Project Title	Protection and privAcy of hospital and health iNfrastructures with smArt Cyber sEcurity and cyber threat toolkit for dAta and people
Project Acronym	PANACEA
Project Number	826293
Type of instrument	Research and Innovation Action
Topic	SU-TDS-02-2018
Starting date of Project	01/01/2019
Duration of the project	36
Website	www.panacearesearch.eu

D1.1 Models of health services and of medical device lifecycle for cybersecurity

Work Package	WP1 User and technical requirements, and scenarios
Lead author	Pasquale Mari (FPG)
Contributors	Silvia Garbin (AON), Raniero Rapone (AON) Fabio Rizzoni (FPG), Giovanni Arcuri (FPG), Matteo Montesi (FPG), Nadia Mores (FPG), Plinio Gianfanelli (FPG), Sabina Magalini (FPG) Annette Denneby (HSE), Muireann Kelleher (HSE) Don Slyne (ICEM), Peter Daly (ICEM) Claude Bauzou (IDEMIA), Sébastien Sohier (IDEMIA) Konstantinos Tsagkos (iSPRINT), Sofoklis Kyriazakos (iSPRINT), Pouyan Ziafati (iSPRINT/LuxAI) Matteo Merialdo (RHEA), Merlin Bieze (RHEA) Daniele Gui (UCSC), Saverio Caruso (UCSC) Lynne Coventry (UNAN) Aimilia Magkanaraki (7HRC), Kallia Anastasopoulou (7HRC), Panagiota Alexoglou (7HRC), Nikos Karamanolakis (7HRC), Kostas Smirlis (7HRC), Irini Kounali (7HRC), Giorgos Mosxovakis (7HRC), Evaggelos Floros (7HRC), Dimitrios Flitzanis (7HRC)
Peer reviewers	Emmanouil Spanakis (FORTH), Vangelis Sakkalis (FORTH) Andrea Mazzù (RINA-C), Ivan Tesfai (RINA-C) Silvia Bonomi (UROME)
Version	V1.0
Due Date	30/04/2019
Submission Date	30/04/2019

Dissemination Level:

x	PU: Public
	CO: Confidential, only for members of the consortium (including the Commission)
	EU-RES. Classified Information: RESTREINT UE (Commission Decision 2005/444/EC)
	EU-CON. Classified Information: CONFIDENTIEL UE (Commission Decision 2005/444/EC)
	EU-SEC. Classified Information: SECRET UE (Commission Decision 2005/444/EC)

The work described in this document has been conducted within the PANACEA project. This project has received funding by the European Union's Horizon 2020 research and innovation programme under grant agreement No. 826293.

Version History

Revision	Date	Editor	Comments
0.1	15/04/2019	Pasquale Mari (FPG)	Document ready for first review
0.2	16/04/2019	Matteo Merialdo (RHEA)	Update of 10.3
0.5	25/04/2019	Matteo Merialdo (RHEA)	Update of Sections 8 and 9, Based on input from Reviewers
0.6	26/04/2019	Pasquale Mari (FPG)	Document ready for final review, amended in all Sections, based on inputs from all the reviewers
1.0	30/04/2019	Pasquale Mari (FPG)	Amendment of Section 4, based in inputs from Reviewers

List of Contributors

The list of contributors to this deliverable are presented in the following table:

Section	Author(s)
1	Pasquale Mari (FPG)
2	Pasquale Mari (FPG)
3	Pasquale Mari (FPG)
4	Pasquale Mari (FPG)
5	Pasquale Mari (FPG)
6	Pasquale Mari (FPG),Fabio Rizzoni (FPG), Matteo Montesi (FPG), Sabina Magalini (FPG) Aimilia Magkanaraki (7HRC), Kallia Anastasopoulou (7HRC), Panagiota Alexoglou (7HRC), Nikos Karamanolakis (7HRC), Kostas Smirlis (7HRC), Irini Kounali (7HRC), Giorgos Mosxovakis (7HRC), Evaggelos Floros (7HRC), Dimitrios Flitzanis (7HRC), Annette Denneby (HSE), Muireann Kelleher (HSE), Don Slyne (ICEM), Peter Daly (ICEM), Daniele Gui (UCSC), Saverio Caruso (UCSC)
7	Pasquale Mari (FPG), Giovanni Arcuri (FPG), Nadia Mores (FPG), Plinio Gianfanelli (FPG), Claude Bauzou (IDEMIA), Sébastien Sohier (IDEMIA), Konstantinos Tsagkos (iSPRINT), Sofoklis Kyriazakos (iSPRINT), Pouyan Ziafati (iSPRINT/LuxAI), Matteo Merialdo (RHEA)
8	Matteo Merialdo (RHEA), Fabio Rizzoni (FPG)
9	Matteo Merialdo (RHEA), Merlin Bieze (RHEA) Silvia Garbin (AON), Raniero Rapone (AON) Lynne Coventry (UNAN)
10	Claude Bauzou (IDEMIA), Sébastien Sohier (IDEMIA), Matteo Merialdo (RHEA), Merlin Bieze (RHEA)
11	Matteo Merialdo (RHEA), Merlin Bieze (RHEA) Silvia Garbin (AON), Raniero Rapone (AON)
12	Pasquale Mari (FPG)
Annex A	Pasquale Mari (FPG)
Annex B	Silvia Garbin (AON), Raniero Rapone (AON)
Annex C	Merlin Bieze (RHEA)

Keywords

Healthcare organizations, Medical devices lifecycle, ICT systems lifecycle, Cybersecurity, Enterprise Architecture, Socio-technical models

Disclaimer

Executive Summary

This document provides a set of models for describing both the entity to be protected from cyber threats (Healthcare organizations, Medical Device Lifecycle, System Development Lifecycle) and the related security system (the Cybersecurity system).

The set of models is named Health Services Models (HSMs) and is made up of four models: a model of the generic healthcare organization (single hospital, group of hospitals and territorial healthcare), a model of Medical Devices lifecycle, a model of Information and Communication Technology (ICT) Systems lifecycle, a model of cybersecurity systems.

The models provide taxonomies for describing the realities in scope.

Each model is made up of three basic elements: ***Entities*** (identifying the components of the reality in scope), ***Catalogues*** (specifying the domain of each entity and providing the relevant taxonomy) and ***Relationships*** (between the Entities).

The first model, named Healthcare Organization Model (HCOM), is made up of four entities:

- **Technological services**, i.e. all the ICT assets, (meaning software applications, hardware infrastructure, medical and non-medical data, workstations, network infrastructure) and all the Medical Devices (e.g. Radiology equipment, Cardiac pacemaker, homecare devices) used, directly and indirectly, to support both healthcare and non-healthcare processes. The Catalogue includes 10 Areas (e.g. Clinical services, Corporate services) articulated in 38 services (e.g. Radiology, Apps for patients, Accounting, Domotics, Clinical reporting, Wearable external medical devices, Staff identification devices, Employee-owned access devices-BYOD, Data Centre and Networking devices)
- **Processes**, i.e. the operational workflows taking place in a healthcare organization. The Catalogue includes 21 Health processes (e.g. Emergency, Operating Room, Clinical Trial, Home care services) and 15 Administrative/Technical processes (e.g. Procurement, Accounting, and Facility Management).
- **Roles**, i.e. the functions of all actors actually operating within a health organization. These include not only internal staff, but also every type of external actor which may interact with the organization. The Catalogue includes 9 Health Roles (e.g. Specialist Medical Practitioners, Nurses), 6 non-health roles (e.g. Administrative front-office) and 3 external roles (Suppliers, Patients, Patient's' related persons)
- **Organizational Functions,** i.e. clusters of organizational units, homogenous per type of contribution that an organizational unit provides to the business. The Catalogue includes 36 Hospital Health functions (e.g. General Surgery), 18 Territorial Health functions (e.g. Hygiene, Ambulance services), 15 Support functions (e.g. Procurement, Information system management).

The second model, named Device Lifecycle Model (DLCM), is made up of three entities:

- **Medical Devices**, i.e. all the Medical Devices which are used to perform healthcare processes. They are classified in 5 types (mobile, stationary, wearable external, implantable, supportive). They are a sub-set of the Technological Services of the Healthcare Organization Model (HCOM).
- **D-Lifecycle Phases**, i.e. the phases of the life of a medical device (D), from the Requirement Definition phase to the Disposal Phase. The lifecycle is made up of 12 phases, including a phase taking care of the conformity and surveillance activities required by the EU regulations
- **D-Roles** i.e. the functions of all actors actually operating during the medical device lifecycle. They include not only manufacturer's roles, but also notified bodies, trust service providers, patients and some of the healthcare provider's roles (as identified in HCOM).

The third model, named Systems Lifecycle Model (SLCM), is made up of three entities:

- **Systems**, i.e. all the Information and Communication Technologies (ICT) assets which are used to perform healthcare processes. They are a sub-set of the Technological Services of the Healthcare Organization Model (HCOM).
- **S-Lifecycle Phases**, i.e. the phases of the life of a System (S), from the Requirement Definition phase to the phase-out Phase. The lifecycle is made up of 11 phases
- **S-Roles**, i.e. the functions of all actors actually operating during the System lifecycle. They include not only suppliers' roles, but also patients and healthcare provider's roles.

The fourth model, named Cybersecurity for Healthcare Model (CSHCM) is made up of four entities:

- **C-Technological services**, i.e. all the technology (software and hardware) which can be used to ensure cybersecurity, both in the healthcare delivery processes and in lifecycles of Medical Devices and Systems; a catalogue of 42 cybersecurity technological solutions has been identified; they are meant to be a complete portfolio of cybersecurity solutions
- **C-Non-technical measures**, i.e. all the non-technical measures which can be used to ensure cybersecurity, both in the healthcare delivery processes and in lifecycles of Medical Devices and Systems. In addition to typical organizational measures (e.g. training), they also include procedures for performing technical activities (e.g. data labelling, phishing simulations). The catalogue includes 26 measures.
- **C-Processes**, i.e. activities that should be executed by an organization to ensure cybersecurity. A catalogue of 21 processes has been identified, based on the activities needed to implement the identify, protect, detect, respond and recover functions of the NIST framework.
- **C-Roles**, i.e. the actors operating in the C-Processes to ensure cybersecurity. Even if the organization is accountable for all the processes, the C-Roles include also external providers. The model leverages on the 52 roles of the NICE Cybersecurity Workforce Framework.

The models have been validated (and then fine-tuned), using them to describe the organization and the cybersecurity status at Gemelli Hospital in Rome (FPG), 7th Health Region of Crete (7HRC) and South-South-West hospital group of public hospitals in Ireland (HSE), the lifecycle of an assistive technology robot (QTrobot) and the lifecycle of a software application for Clinical Trials management at FPG. The results of the validation activity are provided as examples in the document.

Furthermore, the four technical Tools (for dynamic risk assessment & mitigation, secure information sharing, security-by-design & certification, identification & authentication) and the three and non-technical Tools (for training & education, resilience governance, secure behaviours nudging) of the Panacea Toolkit have been mapped into the Cybersecurity for Healthcare Model (CSHCM), making reference to the scope defined for them in the Panacea Description of Action (DOA).

The models are intended to be used to describe Hospitals, Medical Device lifecycle and ICT System lifecycle. This is done through the instantiation of the Catalogues and of the Relationships.

Therefore, in this document 14 ***Instantiation Schemes*** are provided; they consist in guidelines, tables and matrixes for collecting the data needed for the Instantiation. They have been used for the validation activity.

The models are expected to support the Panacea project along all its phases: Toolkit requirements definition, research, development, integration into end-users' realities, testing and validation.

The models could also be used as a standard "map", for instance to compare cybersecurity solutions for Healthcare organizations or to tailor controls of cybersecurity frameworks (e.g. ISO 27001 and NIST) on the specificities of the Healthcare Organizations (Hospitals and territorial Care Centres).

Table of Contents

List of figures

List of tables

1. Introduction

1.1 Purpose of the document

This document is the deliverable associated to the *Task 1.1-Definition of Health Services models*, included in *Work Package 1 - User and technical requirements, and scenarios* of the Panacea Project.

As stated in the Panacea Description of Action (DOA) [DOA1A], the purpose of Task 1.1, and therefore of this document, is to provide:

- a comprehensive map of assets, services and their inter-relations, generalized for the health systems in scope (single hospital, group of hospitals and territorial healthcare) in terms of services/processes, governance models, categories of staff and patients, connected devices, IT architecture, endpoints and their inter-relations; in this document this model is named **Healthcare Organization Model (HCOM)**
- a model of medical devices lifecycle, from design to disposal; in this document this model is named **Device Lifecycle Model (DLCM)**.

Furthermore, even if not explicitly stated in DOA, the purpose of this document is also to provide:

- a model of IT Systems lifecycle, from design to phase-out; in this document this model is named **System Lifecycle Model (SLCM)**
- a model of a cybersecurity system (including technical and non-technical components); in this document this model is named **Cybersecurity for Healthcare Model (CSHCM).**

The collection of these interconnected models in this document is named **Health Services Models (HSMs)**.

The DOA also states that the Task has to insert in the model the components of the Panacea Toolkit (using the high-level architecture from Panacea proposal). Therefore, the document also shows how the Tools of the Panacea Toolkit fit into the HSMs, making reference to their scope, as contained in Panacea proposal.

1.2 Quality assurance

1.2.1 Quality criteria

The Quality Assurance (QA) in the Panacea project relies on the assessment of a work product (i.e. deliverable) according to a list of QA checks established with the Quality Assurance Manager (QAM) - RINA, validated at a project management level and centralized in the [PMP].

For the purpose of the QA of this deliverable, it has been assessed according to the following checklists:

- PEER REVIEW (PR) QA checklist: this deliverable is a report, it then requires a proper peer review according to the checks defined in this checklist. The reviewers have been identified by the QAM following the criteria of independence of evaluation (partners not contributing to the document and task) and robustness in terms of completeness of information, continuity and relevance of the current outcomes with the main related tasks. The peer reviewers identified are:
    - RINA
    - FORTH
    - UROME

1.2.2 Validation process

For the final validation of work products (i.e. deliverables) within the Panacea project, a final QA review process must be used before the issuing of a final version. This QA validation process follows the Quality Review Procedure established with the QAM and validated at project management level in order to guarantee the high-quality level of work products and to validate its adequacy according to the defined quality criteria chosen and defined for each deliverable. The Quality Review Procedure itself and the selection of the QA Review

Committee are described in the [PMP]. The QA validation process is scheduled in the QA Schedule [QASchedule] managed by the QAM.

1.3 Structure of the document

The document is structured in two main parts:

- The first part sets the stage: it describes the methodological approach and how the models have been described, built and validated (Section 4) and establishes the scope of the models and the overall architecture of the models (Section 5):
- The second part provides the key results of the Task 1.1: it describes the Models (Sections 6, 7, 8, 9 and related Annexes A, B, C), their mutual relationships (Section 10) and how they can be applied to real healthcare provider organizations and to real Medical Device lifecycle and System lifecycle. This part also include the application of one of the models for describing the Panacea Solution Toolkit.

Embedded in the second part, many real examples of application of the models are provided: they are the results of the application of the models on the three healthcare providers (FPG, HSE and 7HRC), on a medical device lifecycle case (QTrobot) and on a software application lifecycle case (Clinical Trials management at FPG)[1].

The document ends with a concluding remark Section.

[1] Some examples are provided in a separated confidential document because they contain sensitive information

2. Applicable and Reference Documents

2.1 Applicable Documents (ADs)

The following documents contain requirements applicable to the generation of this document:

Reference	Document Title	Document Reference	Version	Date
[DOA1A]	Panacea Description of the Actions-Annex1 Part A			07/11/2018
[DOA1B]	Panacea Description of the Actions-Annex1 Part B			07/11/2018
[PMP]	PANACEA Project Management Plan		1.0	06/02/2019
[QASchedule]	PANACEA QA Schedule		0.5	01/01/2019

Table 2-1 Applicable Documents

2.2 Reference Documents (RDs)

The following documents have been consulted for the generation of this document:

Reference	Document Title	Document Reference	Version	Date
[Aguilar]	Review and Analysis of Enterprise Architecture Models and Focus IT Architecture	Aguilar Alonso, Igor & José, Carrillo & Verdún, Edmundo & Tovar, Caro. *Review and Analysis of Enterprise Architecture Models and Focus IT Architecture*. Revista de Procesos y Métricas de la TI. 7. 15 - 27. https://www.researchgate.net/publication/288166037_Review_and_Analysis_of_Enterprise_Architecture_Models_and_Focus_IT_Architecture		2010
[APQC]	Healthcare provider process classification framework	APQC-American Productivity & Quality Center, *Healthcare provider process classification framework* https://www.apqc.org/knowledge-base/documents/apqc-process-classification-framework-pcf-healthcare-provider-excel-versi-1	version 7.2.1	12/12/2018
[ARCH]	The Art of Systems Architecting	M. W. Maier, E. Rechtin, *The Art of Systems Architecting*, CRC press		2000

Reference	Document Title	Document Reference	Version	Date
		https://sdincose.org/wp-content/uploads/2017/10/TheArtOfSystemsEngineering_inaugural.pdf		
[AT]	Assistive technologies for people with disabilities: in-depth analysis	Scientific Foresight Unit (STOA) EPRS | European Parliamentary Research Service, European Parliament, *Assistive technologies for people with disabilities: in-depth analysis*, PE 603.218 http://www.europarl.europa.eu/RegData/etudes/IDAN/2018/603218/EPRS_IDA(2018)603218_EN.pdf		January 2018
[AT Rehab]	The Use of Assistive Technology in Rehabilitation and Beyond	M. Oliver, *The Use of Assistive Technology in Rehabilitation and Beyond* https://medicine.utah.edu/pmr/conference/files/2013/Melissa%20Oliver%202013.pdf		Accessed 24 April 2019
[Basten]	EA frameworks, modelling and tools	D. Basten, D. Brons , Chapter 8 of D. F. Ahlemann et al. (eds.), Strategic Enterprise Architecture Management: Challenges, Best Practices, and Future Developments, Management for Professionals, © Springer-Verlag Berlin Heidelberg https://www.researchgate.net/publication/301178632_EA_frameworks_modelling_and_tools		2012
[CNSS]	National Information Assurance (IA) Glossary	CNSS- Committee on National Security Systems of USA *Instruction No. 4009- National Information Assurance (IA) Glossary* https://www.hsdl.org/?view&did=7447		26/04/2010
[COBIT 5]	COBIT 5-A Business Framework For The Governance And management of Enterprise IT	ISACA (Information Systems Audit and Control Association), *COBIT® 5, A Business Framework For The Governance And management of Enterprise IT*		2012

Reference	Document Title	Document Reference	Version	Date
[Davis]	Advancing socio-technical systems thinking: A call for bravery	Davis, M.C., Challenger, R., Jayewardene, D.N.W. & Clegg, C.W. (2014). *Advancing socio-technical systems thinking: A call for bravery*. Applied Ergonomics, 45(2A), 171-180.		2014
[ENISA]	Smart Hospitals: Security and Resilience for Smart Health Service and Infrastructures	ENISA-European Union Agency For Network And Information Security, *Smart Hospitals: Security and Resilience for Smart Health Service and Infrastructures* https://www.researchgate.net/publication/310844589_Smart_Hospitals_Security_and_Resilience_for_Smart_Health_Service_and_Infrastructures_NOVEMBER_2016_Smart_Hospitals_About_ENISA		November 2016
[ENISA TRUST]	Security framework: Guidelines for trust services providers – Part 1	ENISA-Security framework: Guidelines for trust services providers – Part 1 https://www.enisa.europa.eu/publications/tsp1-framework	Version 1.0	December 2013
[ESA ECSS-E-ST-10C]	System engineering general requirements	ECSS-E-ST-10C System engineering general requirements https://ecss.nl/standard/ecss-e-st-10c-rev-1-system-engineering-general-requirements-15-february-2017/	Rev.1	15 February 2017
[EU GDPR]	General Data Protection Regulation	Regulation (EU) 2016/679 of the European Parliament and of the Council 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) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN		27 April 2016

Reference	Document Title	Document Reference	Version	Date
[EU MD REG]	EU Regulation on medical devices	REGULATION (EU) 2017/745 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on *medical devices*, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0745&from=EN		05 April 2017
[Galbraith]	Designing Your Organization Using the Star Model to Solve 5 Critical Design Challenges	A.Kates, J.R. Galbraith, *Designing Your Organization Using the Star Model to Solve 5 Critical Design Challenges*, Jossey-Bass	1st	2007
[Giachetti]	Design of Enterprise Systems: Theory, Architecture, and Methods	R.E. Giachetti, *Design of Enterprise Systems: Theory, Architecture, and Methods*, CRC Press		2010
[Harrel]	Synergistic Security: A Work System Case Study of the Target Breach	M.N. Harrell, Synergistic Security: *A Work System Case Study of the Target Breach, Journal of Cybersecurity Education, Research and Practice*: Vol. 2017 : No. 2 , Article 4. https://digitalcommons.kennesaw.edu/jcerp/vol2017/iss2/4		2017
[IEC MD SW]	"Medical device software – software life cycle processes"	IEC standard 62304, *Medical device software – software life cycle processes*		2015
[IJSIA]	A Classification Scheme for Cybersecurity Model	I. Atoum and A. Otoom, *A Classification Scheme for Cybersecurity Models*, International Journal and Security and its Applications, Vol. 11, No. 1 (2017), pp.109-120 https://www.researchgate.net/publication/315894921_A_Classification_Scheme_for_Cybersecurity_Models		2017
[ILO]	International Standard Classification of 2008 (ISCO 08)	International Labor Office of the International Labor Organisation, *International*		2012

Reference	Document Title	Document Reference	Version	Date
		Standard Classification of 2008 (ISCO 08) https://www.ilo.org/wcmsp5/groups/public/@dgreports/@dcomm/@publ/documents/publication/wcms_172572.pdf		
[ISO/IEC 27001]	Information technology - Security techniques - Information security management systems -- Requirements	https://www.iso.org/standard/54534.html		2013
[ISO/IEC/IEEE 15288]	Systems and software engineering --System life cycle processes	https://www.iso.org/standard/63711.html		2015
[JEA]	Essential Layers, Artifacts, and Dependencies of Enterprise Architecture	Robert Winter and Ronny Fischer, *Essential Layers, Artifacts, and Dependencies of Enterprise Architecture* By Robert Winter and Ronny Fischer, Journal of Enterprise Architecture https://www.alexandria.unisg.ch/213147/1/WiFi07_EssentialLayers_JEA_May2007.pdf		2007
[Leavitt]	Lesson on Leavitt's Diamond Model	Video tutorial https://www.youtube.com/watch?v=u5MevXbAjSo		Accessed 21 April 2019
[MENDES]	Implementing the Service Catalogue Management	.C.Mendes, M.M. Da Silva, *Implementing the Service Catalogue Management Conference: Quality of Information and Communications Technology* (QUATIC), 2010 https://www.researchgate.net/publication/224202028_Implementing_the_Service_Catalogue_Management		2010
[MERRIAM]	Definitions of "measure" and "means"	Merriam-Webster dictionary https://www.merriam-webster.com/dictionary/measure		Accessed 06 April 2019

Reference	Document Title	Document Reference	Version	Date
		https://www.merriam-webster.com/dictionary/means		
[NICE]	National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework	NIST-National Institute of Standards and Technology, *Special Publication 800-181-National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework* https://www.nist.gov/publications/nice-cybersecurity-workforce-framework-national-initiative-cybersecurity-education		August 2017
[NIST]	Framework for Improving Critical Infrastructure Cybersecurity	NIST-National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf	Version 1.1	16 April 2018
[NIST DI]	NIST Special Publication 800-63B	SP 800-63B		June 2017
[NIST SDLC]	The System Development Lifecycle	NIST-National Institute of Standards and Technology, *The System Development Lifecycle* https://csrc.nist.gov/csrc/media/publications/shared/documents/itl-bulletin/itlbul2009-04.pdf		Accessed 06 April 2019
[NIST SP]	Security and Privacy Controls for Federal Information Systems and Organizations	SP 800-53r4 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf	Rev.4	April 2013
[OWASP]	Introduction to the Cyber Defense Matrix	OWASP-Open Web Application Security Project, *Introduction to the Cyber Defense Matrix* https://www.owasp.org/index.php/OWASP_Cyber_Defense_Matrix		Accessed 06 April 2019
[PDIL]	Understanding the Security Vendor Landscape Using the Cyber Defense Matrix	Sounil Yu, *Understanding the Security Vendor Landscape Using the Cyber Defense Matrix*, RSA Conference, San Francisco, SESSION ID: PDIL-W02F		2016

Reference	Document Title	Document Reference	Version	Date
		https://www.rsaconference.com/writable/presentations/file_upload/pdil-w02f_understanding_the_security_vendor_landscape...-final.pdf		
[Robbins]	Organization Theory: structure, design, and applications	S.P. Robbins, Organization Theory: structure, design, and applications, Prentice-Hall International Editions	2nd	1987

Table 2-2 Reference Documents

3. Glossary of Acronyms

Acronym	Description
BLE	Bluetooth Low Energy
CMDB	Configuration Management Data Base
CSHCM	Cybersecurity for Healthcare Model
DLCM	Device Lifecycle Model
DOA	Description of Action
EA	Enterprise Architecture
ENISA	European Union Agency for Network and Information Security
ERP	Enterprise Resource Planning system
FPG	Gemelli University Hospital
HC	Healthcare
HCOM	Healthcare Organization Model
HRO DB	Human Resources and Organization structure Data Base
HSE	South-South-West Hospital Group of the Health Service Executive
HSMs	Health Services Models
ICT	Information and Communication Technology
ILO	International Labour Organization
ISCO	International Standard Classification of Occupations
LAN	Local Area Network
NIST	National Institute of Standards and Technology
OWASP	Open Web Application Security Project
PAC	Project Advisory Committee
PACS	Picture archiving and communication system
PMP	Project Management Plan
QA	Quality Assurance
QAM	Quality Assurance Manager
RIS	Radiology Information System
SAN	Storage Area Network
SLCM	System Development Lifecycle Model
SDO	Standards Developing Organization
7HRC	Seventh Health Region-Crete
TSP	Trust Service Provider
VOIP	Voice over Internet Protocol
VPN	Virtual Private Network

Table 3-1 Table of acronyms

4. Methodology

This Section describes the methodology we used to perform the modelling activity.

Modelling activity followed four main steps, listed here below, and brought to the definition of models:

- Definition of what should be contained in the models
- Definition of the building formalism to be used for representing the models
- Definition of the development process for building the models
- Implementation of the development process and actual building of the models.

The results of the first three steps are contained in next three paragraphs. The results of the last step are provided in the core Sections of this document: Sections from 6 to 9.

4.1 Models content

Health Service Models (HSMs) describes the reality in scope, through a specific set of variables.

To define their content, we considered first what we wanted to model, namely the "object". We defined then the specific use of the model, together with the range of variables we wanted to associate. We searched then for models available in the literature, to understand how they are used in the cybersecurity domain. We finally decided our set of variables, adapting it to the needs of the Panacea project.

There reality in scope includes four "objects" to be modelled:

- The *healthcare provider's organization*;
- The *lifecycle of ICT systems* in the healthcare context and the *lifecycle of Medical Devices*, which involve supplier's and manufacturer's organization processes and people operating on the technical items during their lifecycle;
- The *cybersecurity system*, which can be considered, for modelling purposes, as a separate organization, made up of its own process, people and technologies.

Given the scope and ambition of the Panacea project[2], the models are intended to be used, for instance, to

- Identify which type of workers, as potential target of social engineering, use a given type of software applications or of medical devices;
- Target and track the diffusion of cybersecurity awareness among the different healthcare professions in a hospital or in a health region;
- Identify the formal social groups, different in terms of behaviours that may be influenced by hierarchy or by peers;
- Link the different cybersecurity measures to the types of people, types technological assets and business processes they are intended to protect;
- Link the different cybersecurity measures to the phases of Medical Devices and ICT Systems lifecycle, and to the people operating in the phases.

Given the purpose of the models, all the "objects" should be described taking into consideration both technical components (e.g. ICT and Medical Devices), and non-technical components (e.g. people, organization, processes) and their relationships.

The literature provides two approaches for building these models: Enterprise Architecture (EA) and Socio-Technical-Systems (STS).

[2] The payoff under the Panacea logo states: "people-centric cybersecurity in healthcare"

According to [Giachetti] "an *Enterprise Architecture* is a high-level design of an enterprise, which specifies an enterprise-wide view of the processes, information and organization of the enterprise and how the three views are integrated"

There are many versions of EAs, that differ from each other on the basis of how they disaggregated or aggregate process, information and organization (see, for instance, reviews in [Aguilar], [Basten] and [JEA]). According to [JEA], most Enterprise Architecture frameworks represent an enterprise using five descriptive variables (or layers), shown in following Table 4-1.

Enterprise Architecture layer	Typical artefacts represented on the layer
Business architecture	It represents the fundamental organization of the organization in scope, from a business strategy viewpoint Typical artefacts include: Value networks, relationships to customer and supplier processes, targeted market segments, offered services, organizational goals, strategic projects
Process architecture	it represents the fundamental organization of service development, service creation, and service distribution in the relevant enterprise context Typical artefacts include: Business processes, organizational units, responsibilities, performance indicators, and informational flows
Integration architecture	It represents the fundamental organization of information system components in the relevant enterprise context Typical artefacts include: Enterprise services, application clusters, integration systems and data flows.
Software architecture	It represents the fundamental organization of software artefacts; Typical artefacts include: Software services and data structures
Technology (or infrastructure) architecture	It represents the fundamental organization of computing / telecommunications hardware and networks Typical artefacts include: Computing/telecommunications hardware and networks

Table 4-1 Typical layers of Enterprise Architecture models (adapted from [JEA])

The Enterprise Architecture paradigm fits well for the Cybersecurity Systems. [IJSIA] identifies seven different types of modelling approaches (including the Enterprise Application approach) and compares them according to their capability of satisfying the following nine criteria[3]:

1) Basic security principles: cybersecurity model should support the heart of information security; confidentiality, integrity, and availability;
2) Defence depth: information security must protect information throughout the life span of the information, from the initial creation of the information on through to the final disposal of the information;
3) Defence strategy: proactive models should take proactive decisions in regard to possible incidents such as legislation and proper guidelines and recovery plans. Preventive models trigger prevention actions once a threat is detected;
4) Cybersecurity controls coverage: selecting proper controls and implementing them will help an organization to bring down risk to acceptable levels. A good cybersecurity model should contain risk, administrative, logical and physical control components;
5) Resilience: the ability of the model to be flexible with unseen changes in technology, environment, attack methods, etc. Resilient management systems and processes will provide greater protection against multidimensional attacks;
6) Compliance: a compliance model follows a security standard or a best practice in a cybersecurity domain. Thus, allowing the cybersecurity model to make portable changes between security related standards or cybersecurity models;

[3] The criteria describe the capability of each modelling approach to drive towards effective cybersecurity models of operation

7) Tracking: the model should be able to detect if further modification is needed in security models or cybersecurity strategies;
8) Performance measurement: the ability to measure performance of security initiatives effectively at various organizational levels. It also should audit whether the security policy and strategies are being effectively implemented;
9) Information classification: an important aspect of information security and the risk management is recognizing the value of information and defining appropriate procedures and protection requirements for the information.

[IJSA] conclusion is that the Enterprise Architecture approach fits quite well against all criteria.

However, with respect to our need, the EA approach misses an important variable: People.

The *Socio-Technical Systems (STS)* approach fills this gap. This approach was originally introduced in the 1950s to properly consider technology and the social system within the *work design* (see [Robbins]). *Technology* consists of tools, techniques, procedures, skills, knowledge and devices used by employees to do their job, while the *social system* consists of people who work in the organization and their interrelationships (see [Robbins]).

As for the EAs, there are many STS models. For instance, a model used for organization design is the Galbraith's Star Model (see [Galbraith]), which considers five variables: Strategy, Structure, Processes (which includes information technology), Rewards, and People. A quite recent model (see [Davis]) has been used to analyse crowd events (e.g. Olympics game) and considers six variables: Goals, Processes/Procedures, Technology, Buildings/Infrastructures, and People.

A quite simple STS model is the Leavitt's **Diamond model** (see Figure 4-1), which represents organizations as comprising four key interacting variables, namely (1) task, (2) structure, (3) people and (4) technology (see [Leavitt] and [Harrell]).

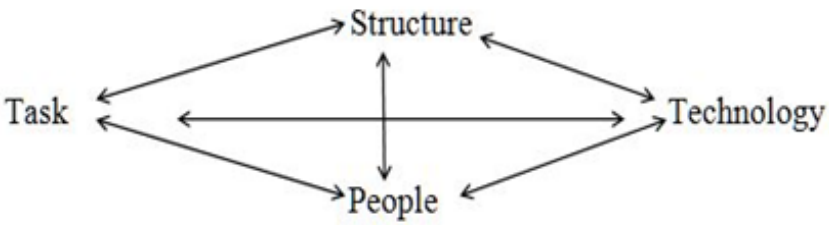

Figure 4-1 Diamond Leavitt model (source [Harrel])

According to [Harrell]: the Structure component of the model includes organizational relationships, workflow systems, or the systems of authority; the Technology component could include anything from a pencil, to a word processor to an entire information system; the People component includes the attitudes of the people, their abilities, or their skills and understanding; the Task component includes all of the things that must be completed to produce goods and services.

The double arrow segments connecting the variables indicate influence and/or need for coherence.

This model was born as a socio-technical model in 1965 to manage organizational change. However, it has recently (2017) been used for describing and analysing cybersecurity situations (see [Harrell]), after adapting the variables (see Figure 4-2).

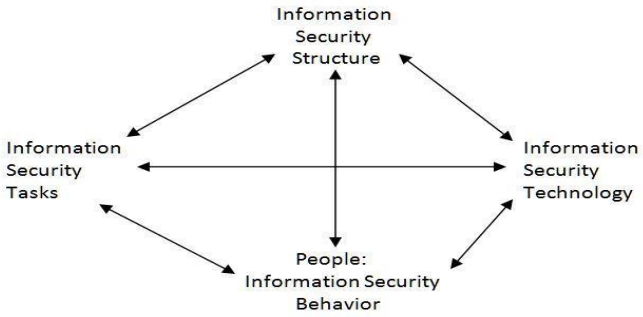

Figure 4-2 Adaptation of Leavitt Diamond model to describe a security context (source [Harrell])

Above analysis shows that both EA and STS are quite flexible approaches: they provide sets of variables that the model designer can configure according to the domain of application.

For Panacea, the models need to allow to describe

- the work contexts where the cybersecurity risk may appear or should be managed
- the technology to be protected
- the work context for designing and implementing the cybersecurity
- the technical and non-technical measures[4] that are in place or could be deployed to ensure cybersecurity.

To do this, it is necessary including in the models the variables shown in next

	"Objects" to be modelled			
Contexts and elements that can be described thanks to the models	**Healthcare provider's organization**	**Medical Device Lifecycle**	**System Lifecycle**	**Cybersecurity System**
Work contexts in which the cybersecurity risk may be appear	• Organizational functions • Process • Roles	• D-Lifecycle phase • D-Roles	• S-Lifecycle phase • S-Roles	
Technology to be protected	• Technological Services used in the processes	• Medical Device involved in the lifecycle is	• System involved in the lifecycle	
Work context for managing the cybersecurity				• C-Processes • C-Roles
Technical and non-technical measures that are in place or could be deployed	• Link between the measures and the context/ technology on which the measures act	• Link between the measures and the context/ technology on which the measures act	• Link between the measures and the context/ technology on which the measures act	• C-Technological Services • Non-Technical measures

[4] The term "measure" stands for "a step planned or taken as a means to an end", and "means" stands for "something useful or helpful to a desired end" (see [MERRIAM]).The distinction between technical and non-technical measures is consistent with the ENISA classification (see [ENISA]):" *Technical measures* rely on ICT and use software for the purpose of automation. Examples of technical measures are the use of technologies such as firewalls, virtual private networks, intrusion detection and prevention systems and vulnerability scanners as well as the use of cryptography. *Organisational measures* include policies, procedures, administrative tools and methods, and measures to create and maintain awareness and are usually implemented manually."

Table 4-2. These variables allow to describe relevant contexts and elements for each one of the four objects that will need to be modelled.

	"Objects" to be modelled			
Contexts and elements that can be described thanks to the models	**Healthcare provider's organization**	**Medical Device Lifecycle**	**System Lifecycle**	**Cybersecurity System**
Work contexts in which the cybersecurity risk may be appear	• Organizational functions • Process • Roles	• D-Lifecycle phase • D-Roles	• S-Lifecycle phase • S-Roles	
Technology to be protected	• Technological Services used in the processes	• Medical Device involved in the lifecycle is	• System involved in the lifecycle	
Work context for managing the cybersecurity				• C-Processes • C-Roles
Technical and non-technical measures that are in place or could be deployed	• Link between the measures and the context/ technology on which the measures act	• Link between the measures and the context/ technology on which the measures act	• Link between the measures and the context/ technology on which the measures act	• C-Technological Services • Non-Technical measures

Table 4-2 Variables of the Health Services Models (HSMs)

In the table, variables are named with the nomenclature that will be used in the HSMs and that will be fully described in Sections from 5 to 10.They are consistent with Panacea variables used in the EA and STS models, described in the above analysis. Making reference, for instance, to the Diamond Model a broad correspondence is the following

- Organizational functions is related to Structure
- Processes and Lifecycle is related to Tasks
- Roles is related to People
- Technological Services and Medical Devices are related to Technology
- Non-Technical measures are also related to Technology (because in the Diamond Model the Technology variable includes every type of tool).

The set of variables that we have selected takes into account both Socio-Technical Systems (STS) approach, and Enterprise Architecture (EA) approach. Our set of variables can be described as follows:

- The set of non-technical[5] variables follows manly the STS approach, because it splits the EA Process layer in three variables (Organizational functions, Process, Roles) to better describe the work context; furthermore, it contains the *Non-technical measures* variable, to take care of the importance of these measures in Panacea toolkit
- With respect to the technology, it follows mainly the EA: even if it is not evident from Table 4-2, the Technology Services variable of our model contains, in its descriptive taxonomy, the distinction between Applications, Data and Infrastructure (see Table 6-1) ; furthermore, it contains the *Medical*

[5] The distinction between "technical", "technological", "technology" and "non-technical" elements or measures is not clear-cut in the models we analysed; in this document we associate the terms "technical"/ "technological"/ "Technology" to the Information and Communication Technologies (ICT) and the Medical Devices and the term "non-technical" to policies, procedures, methods, people, organization, processes

Devices variable, due to the importance of this technological component in Panacea toolkit and in the Healthcare organizations

- With respect to the EA, it includes partially the Business layer (of EA) as an aspect of the Process variable: Panacea is interested in establishing the business priorities of cybersecurity interventions; our models set the basis for this analysis, identifying the processes to be prioritized and providing some metrics to evaluate the processes in terms of cybersecurity criticality (see paragraphs 6.3.2 and 6.3.4)
- With respect to the EA models, they do not describe the interactions between Applications, Data and Infrastructure: this level of detail is already managed by other tools, such as the Configuration Management Data Base (CMBD). See last Section 12 for a discussion on the relationship between our model and CMBDs.
- With respect to STS models, they do not include models of social interrelationships and individual behaviours, but allow to identify the work context where they might happen, profiling the context in terms of relevant attributes (organizational function, process, professional roles involved)[6].

4.2 Models building blocks and graphical representation

Models are constituted by **three building blocks:**

- **Entities**: they are used for describing a given organization, cybersecurity system, lifecycle; Entities include, for instance, Roles, Processes, Technological services (e.g. software applications).
- **Catalogues**: they specify the domain of a the related entity and provide the relevant taxonomy, i.e. a **list of items** classified according to some meaningful criterion (e.g. if the Entity is “Role”, than the Catalogue lists all the possible roles which exist in a Healthcare organization, clustering them in health and non-health roles)
- **Relationships**: they are the links between entities and could also link entities of different models; the links may be
    - **Oriented relationships**, represented as *Entity A* → *Entity B*: it means that A impacts on B, i.e. items of Catalogue A impact[7] on items of Catalogue B; the actual type of impact depends on the nature of the involved Entities; for instance if A is “Cybersecurity non-technical measures” and B is “Roles”, the impact may consist in the fact that the “Training” (an item of Catalogue A) raises the awareness of “Nurses” (an item of Catalogue B);
    - **Non-oriented relationships**, represented as *Entity A* - *Entity B*: it means that A and B may be co-present; for instance, if A is “Role” and B is “Process”, it means that a given Role (e.g. Nurse) can be involved in a given Process (e.g. Emergency department workflow).

Following Figure 4-3 shows **how the building blocks are represented**. In the figure, Entity Z impacts on Entity B.

[6] The modelling of these aspects is in the scope of Work Package 2 “Research on advanced threat modelling, human factors, resilient response and secure interconnectivity” of the Panacea project

[7] “Entity A impacts on Entity B” means that the activation/operation/change of items of Entity A can modify items of Entity B or some attribute of Entity B. For instance if Entity A includes “training for cybersecurity”, and Entity B includes “nurses”, the delivery of the training to the nurses may reduce the vulnerability of the nurses.

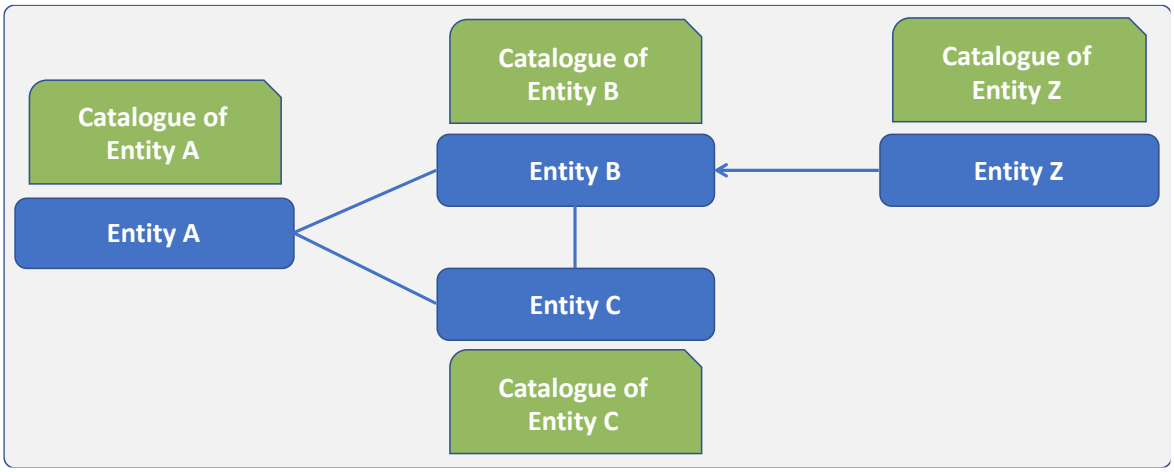

Figure 4-3 Graphical representation of the building blocks of the models

Models are intended to describe a reality, e.g. a given hospital Medical Device lifecycle or IT System lifecycle. This is done through the **instantiation of the Catalogues and of the Relationships.**

Therefore, models have to be complemented with **Instantiation Schemes**, which specify how to build instances of the models. There are two types of Instantiation Schemes.

The first type uses **Instantiation Tables**, to instantiate **Catalogues**.

The typical table has two columns; on the left column there are the items of the catalogue, on the right column there the corresponding items of the instantiated reality; for instance Table 4-3.

Items of the catalogue	Items
Nurse	Clinical Nurse Instructor
	Clinical Nurse Specialist (General)
	Clinical Nurse Specialist (Mental Health)

Table 4-3 An indicative example of Instantiation table

The instantiation may also include attributes, such as the actual number of “Nurses”, in the example above

The second type uses **Instantiation Matrixes**, to instantiate **Relationships**.

For instance, if the relationship is between Entity A and Entity B, then heading of the rows contains the items of Catalogue A, while the heading of the columns contains the items of Catalogue A; the cross contains information appropriate to the relationship; an empty cross means that the items are not related, while an “X” indicates that the two items are actually related; more information can be added, according to the nature of the linked Entities; for instance, the name of the applications used by the Nurses operating in a given process; for instance Table 4-4

		Entity A: ROLES			
		Nurses	**Medical Doctors**	**Administrative Employees**	**Role …**
Entity B: Technological Services	**Application B1**	X			
	Application B2		X	X	
	Application …		X		

Table 4-4 An indicative example of Instantiation Matrix

Matrixes can be **Normative**, if they contain predefined suggested values (see for instance Table 7-6, Table 8-5, Table 10-1, Table 10-2 and Table 10-4).

In Figure 4-4 a summary of the shapes of **Tables and Matrixes is provided**.

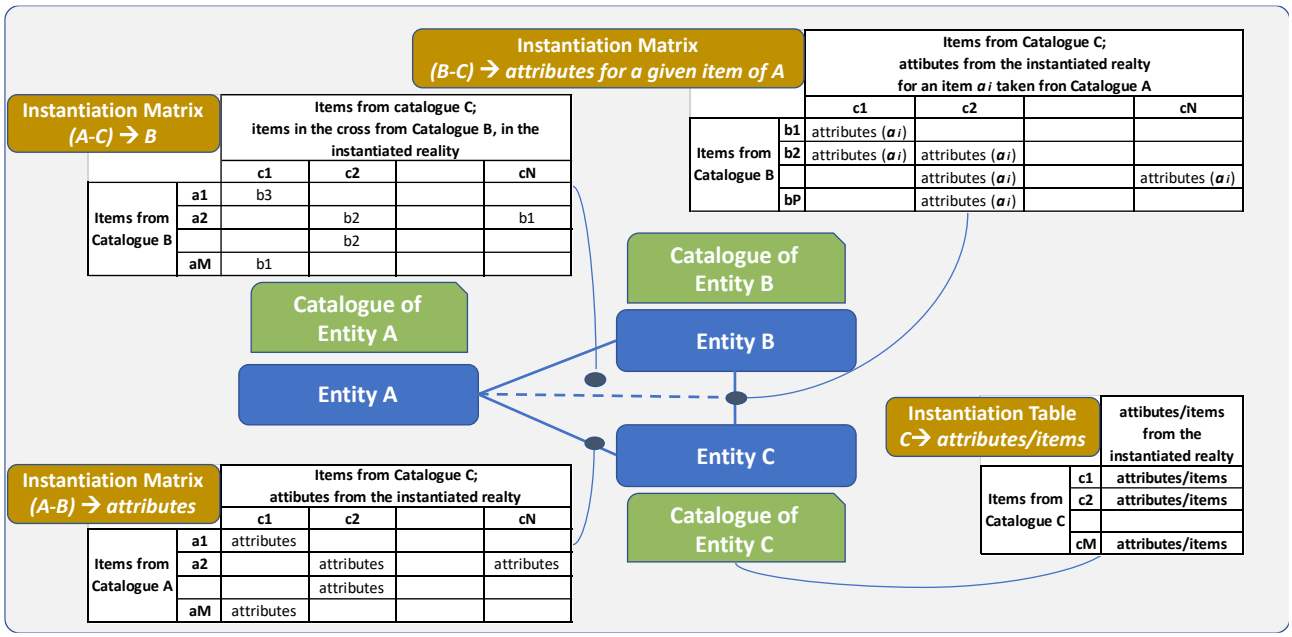

Figure 4-4 Types of Instantiation Tables and Matrixes

Many Instantiation Schemes and examples of instantiations will be provided in following Sections of the Document.

Further schemes will probably be defined during the project, if needed, using the models defined in this document and its taxonomies.

4.3 Models development process and sources

The process performed to identify a robust and useful set of Models has been based on three concepts:

- Go through the cycle "Elaborate → Validate → Fine-tune" and re-validate if needed;
- Leverage the variety and richness of expertise of the Consortium Partners;
- Get input from literature and advice from external experts.

These concepts have been translated into practice following a development process articulated along two integrated paths:

- Logical path (the "what");
- Operational path (the "how").

The logical path consists in following steps:

1) State purpose and requirements for the models;
2) Search for already existing models or parts of models (e.g. taxonomies, lifecycle structures);
3) Define draft models;
4) Define instantiation schemes, to be used to build instances;
5) Test the models on real cases, building the instances;
6) Finalise the models.

The operational path has gone through the following sequence of activities:

1) Task Kick off meeting in Rome with all Task contributors;
2) Prototyping of HCOM by FPG team;
3) Video calls to share the HCOM prototype with all Task contributors;
4) Video calls to launch teams for the definition other Models;
5) Prototyping of DLCM;
6) Prototyping pf SLCM;
7) Two Meetings in Milan to prototype CSHCM;
8) First Instantiation of HCOM and CSHCM in FPG;
9) Meeting in Crete (FPG-7HRC, + HSE in video call) to launch instantiation of HCOM and CSHCM in 7HRC and HSE;
10) Testing of HCOM and CSHCM in FPG, HSE, 7HRC;
11) Testing of DLCM on QT Robot;
12) Testing of SLCM on Clinical Trial software;
13) Video call with ENISA expert to get feedback;
14) Video call with Project Advisory Committee (PAC) members to get feedback;
15) Deliverable drafting and review;
16) Along the entire Task period: video calls to discuss progress, at least one per week

The Task has been performed along the operational path. Each activity of the operational path contributed to implementing the logical steps, as shown in table below.

	Logical steps					
Operational steps	**State purpose and requirements**	**Search for models or parts of models**	**Define draft models**	**Define instantiation schemes**	**Test the models on real cases**	**Finalise the models**
1) Task Kick off meeting in Rome	x					
2) Prototyping of HCOM by FPG	x	x	X			
3) Video calls to share HCOM prototype	x		X			
4) Video calls to launch teams for the definition other Models	x		X			
5) Prototyping of DLCM	x	x	X			
6) Prototyping of SLCM	x	x	X			
7) Two Meetings in Milan to prototype CSHCM	x	x	X			
8) First Instantiation of HCOM and CSHCM in FPG				x		
9) Meeting in Crete				x	x	
10) Testing of HCOM and CSHCM in FPG, HSE, 7HRC						
11) Testing of DLCM on QT Robot				x	x	
12) Testing of SLCM on Clinical Trial software				x	x	
13) Video call with ENISA expert			X			
14) Video call with PAC members						x

Operational steps	Logical steps					
	State purpose and requirements	Search for models or parts of models	Define draft models	Define instantiation schemes	Test the models on real cases	Finalise the models
15) Deliverable drafting and review						x
16) Along the entire Task period: video calls to discuss progress			X	x	x	x

Table 4-5 Models development process

The development process had been based on multiple **sources**

- Relevant literature has been accessed;
- The validation has been done instantiating the models, to describe healthcare organization and cybersecurity status at Gemelli Hospital in Rome (FPG), 7th Health Region of Crete (7HRC) and South-South-West hospital group of public hospitals(HSE), the lifecycle of an assistive robot and the lifecycle of a software application; validation has been done to check four aspects: (1) completeness and (2) non-ambiguity of the taxonomies; (3) usability of the instantiation schemes (are the data available? is it easy to elaborate them to feed tables and matrixes?); (4) feeling of relevance of the models.
- The task has also befitted from the valuable input of following Panacea Project Advisory Committee (PAC) members:
    - Dr. Richard Amlot (Public Health England): Health care governance expert;
    - Dr. Michael Cooke (National University of Ireland Maynooth): Human factors and human-machine interaction expert;
    - Prof. George Cybenko (Thayer School of Engineering, USA): Security of Cyber-physical systems expert; former Founding Editor-in-Chief of IEEE Security & Privacy Journal;
    - Dr. Gabriele Unterberger (Software Centric Srl, Italy): Medical Device Integration, Exploitation of innovative solutions expert ;
    - Dr. Simon Woodworth (University College Cork, Ireland): Clinical Information System expert.
- The task, under the orchestration of FPG (Task Leader), has benefitted from frequent collegial discussions among the Consortium Partners, together with contributions from each Partner, which ensured the involvement of competent staff. End-user Partners, involved clinical managers, ICT officers and officers managing Medical Devices.

5. Health Services Models (HSMs) architecture

5.1 HSMs Purpose

The purposes of the Health Services Models (HSMs) are both internal and external to Panacea Project.

Internal purposes include

- Providing a framework for structuring the user requirements collection: the models are meant to provide end-users with taxonomies, intended to help them in identifying those areas that need effective solutions from the cybersecurity point of view, in particular for what concerns healthcare organizations

(e.g. “need to raise the awareness of Health Services Managers and Medical secretaries”; “need to have easy to use identification and authentication solutions for wearable medical devices”; “need to protect stationary networked medical devices”, “need to have e-learning packages specific for nurses and specific for front-office administrative staff”);

- Providing a common and shared language to describe end users’ socio-technical systems, as well as their demonstration scenarios and use cases;
- Providing a framework where to position Panacea Solution Toolkit components, to make it clear their contributions to cybersecurity, also with respect to the market offering; models contains the “portfolio” of possible technical and non-technical interventions; this makes possible to map the Panacea Tools, and the market offering, into the “portfolio”;
- Providing input for following Panacea Tasks
    - Task 1.2 Definition of Regulatory, End-users and Device Providers requirements;
    - Task 1.3 Definition of Solution Toolkit Technical Requirements;
    - Task 1.4 Scenarios scoping use cases and KPIs definition;
    - Task 2.1 Health Services vulnerabilities, cyber-risk scenarios and current countermeasures;
    - Task 2.2 Human Factors, Threat Models Analysis and Risk Quantification;
    - Task 5.1 Development of governance models, compliance and assurance processes, metrics;
    - Task 6.4 Certification mechanisms.

External purposes are consistent with the Panacea KPI “*2+inputs for standardisation on cybersecurity will be proposed to the relevant SDO Technical Committee*”, and include

- Propose standard models for describing Health Care Organizations, Device lifecycles, System Design Processes and Cybersecurity Systems to map cybersecurity interventions and compare cybersecurity solutions;
- Propose a standard model to support the contextualization of ISO 27001 and the NIST framework for the Healthcare Organizations (Hospitals and territorial Care Centres).

5.2 HSMs Scope

Based on the scope of Task 1.1 (see paragraph 1.1) and on the purpose of the model the scope of the HSMs can be more precisely described along three dimensions

- Threats;
- Measures;
- Threatened assets.

1) **Threats** that may damage highly digitalized processes may include (see [ENISA]): malicious actions, natural phenomena, human errors, system failures, supply chain failures. Within this spectrum of possible threats, the **scope of the HSMs is focused on malicious actions**.

   This scope is coherent with Panacea project mandate, as it stems from the Topic SU-TDS-02-2018, which originated the project:

   - Topic title: *“Toolkit for assessing and reducing **cyber risks** in hospitals and care centres to protect privacy/data/infrastructures”*
   - Topic challenge: *“ICT infrastructures and data have become critical for the functioning of the hospitals and care systems and due to increasing connectivity, the exposure to **risks of cyber-crime** is constantly increasing. Healthcare ICT infrastructures are now considered to be part of the Critical*

Information Infrastructure. ***Cyberattacks*** *are a potential danger to the safety of patients and to the privacy of sensitive health data."*

Cyberattack may be defined as [CNSS]: "*Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself*".

According to [ENISA], **malicious actions** are deliberate acts by a person or an organization including:

- Malware attacks (attacks using a malicious software, such as ransomware, worms, trojans, viruses, rootkits, exploitkits, botnets);
- Hijacking and medjack, to refer to the hijacking of medical devices to create backdoors in hospital networks;
- Medical device tampering;
- Device and data theft;
- Skimming;
- Denial-of-service attacks;
- Social engineering attacks.

Attackers may be internal or external (including suppliers and vendors) to the organization.

2) **Measures,** from the point of view of their **nature,** may include [ENISA]:
   - organisational measures (policies, procedures, administrative tools and methods, and measures to create and maintain awareness);
   - technical measures (which rely on ICT and use software).

   As what concerns the nature of the measures, the scope of HSMs is coherent with the Panacea Toolkit scope, since it includes both organizational and technical measures.

   HSMs is also built to allow the mapping of these measures in **all their cybersecurity phases,** as defined in the NIST Cybersecurity Framework (see [NIST]): Identify, Protect, Detect, Respond, and Recover.

3) **Threatened assets** in the scope of HSMs include
   - The ICT assets and medical devices used in/by a Smart Hospital (as identified in [ENISA]);
   - ICT assets and medical devices used in/by territorial Healthcare organizations;
   - Medical devices during all the phases of their lifecycle, in addition to the "operational" phase;
   - ICT systems during all the phases of their lifecycle, in addition to the "operational" phase;
   - People interacting with above assets (health services staff, providers and patients).

Table below provides a **summary of the HSMs scope**.

Threats	Measures	Threatened Assets
• Malicious actions, originated by external and internal attackers *NOTE: Natural phenomena, Human errors, System failures, Supply chain failures are out of scope*	From the "nature" point of view: • Technical • Organizational From the "cybersecurity phases" point of view • Identify • Protect • Detect • Respond • Recover	• Hospital and Territorial ICT (medical and administrative) assets and medical devices • Medical devices during lifecycle • ICT systems during lifecycle • People (health services medical and non-medical staff, suppliers and patients)

Table 5-1: Scope of Health Services Models (HSMs)

5.3 HSMs overall architecture

The activities performed in Task 1.1 allowed to create an original new set of models.

This Section describes the overall high-level architecture of these models. Following Sections describe each model and their interactions.

HSMs include four inter-related models (see Figure 5-1):

- The **Health Care Organizations Model** (HCOM) describes the generic healthcare provider, in particular describes three types of providers: single Hospital, Group of Hospitals operating with some inter-hospital processes (e.g. procurement managed as a shared service, medical consultations among the hospitals of the Group), Health Region (which includes central functions, hospitals, territorial health service delivery via general practitioners and local healthcare units);
- The **Device Lifecycle Model** (DLCM) describes the generic lifecycle of a Medical Device from the requirement phase to the disposal phase. According to the European regulations (see [EU MD REG]), Medical Device means any device intended by the manufacturer to be used, alone or in combination, for human beings for a broad set of medical purpose, including diagnosis, monitoring, treatment or alleviation of disease, an injury or disability (e.g. Cardiac pacemaker, Computer Tomography scanner, Radiology equipment, High Automation Laboratory System; refer to paragraph 7.1.1 for more examples and more detailed definition);
- The **System Lifecycle Model** (SLCM), Section 8, describes the generic lifecycle of a technological system leveraging healthcare processes (software applications, infrastructures or mix of them) from the requirement phase to the disposal phase;
- The **Cyber-security for Health Care Model** (CSHCM), Section 9, describes the generic set of cybersecurity arrangements, distinguishing between technological and non-technological measures.

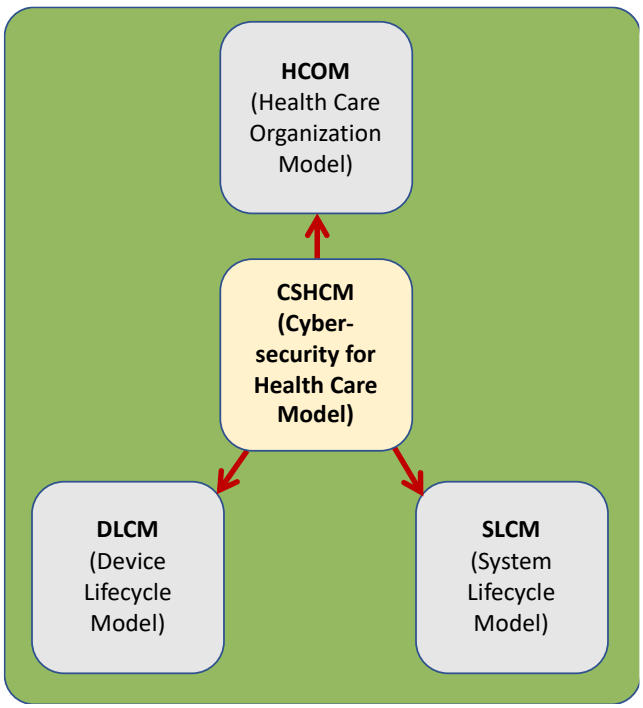

Figure 5-1 Health Services Models (HSMs) high level architecture

The integrated representation of the Models is provided in following Figure 5-2.

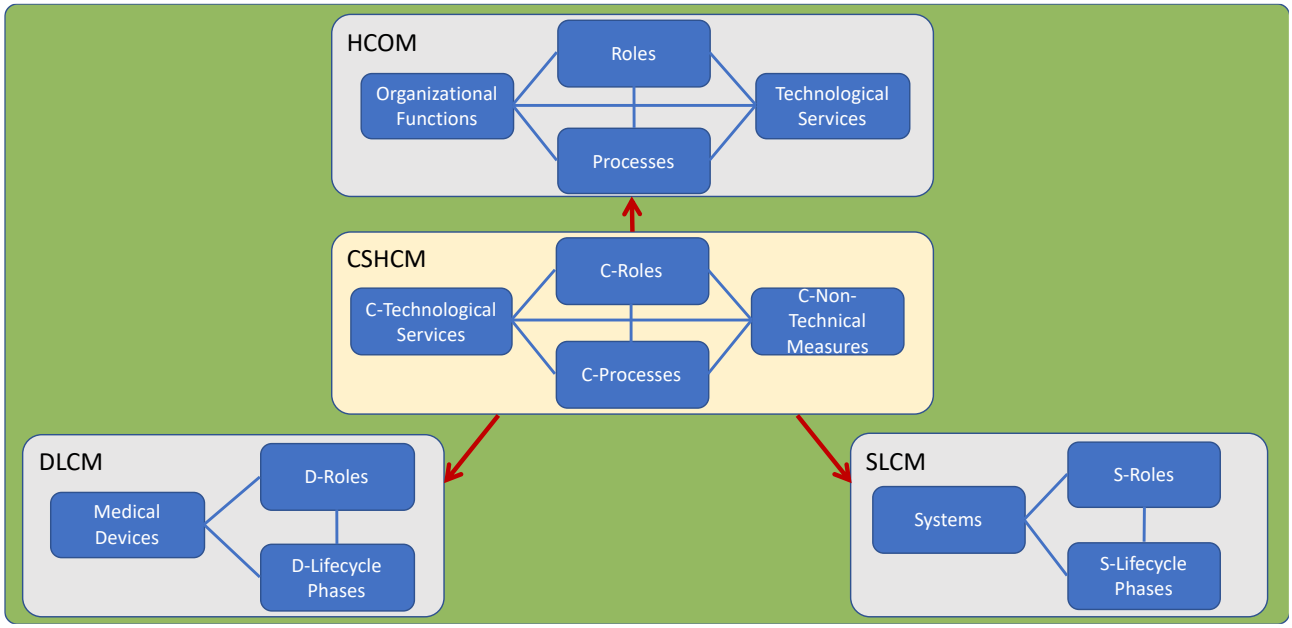

Figure 5-2 Integrated representation of all Health Services Models

For each model the figure shows the relevant Entities and Relationships. Next Sections 6, 7, 8 and 9 describe each one of the four models and their internal instantiation schemes.

The figure also shows that the Entities of the Cybersecurity for Healthcare Model (CSHCM) have impacts on the Entities of the other three models. Details on these three impact relationships are provided in Section 10.

6. Healthcare Organization Model (HCOM)

The HCOM describes the sociotechnical structure of the organization in scope, through **four Entities, four related Catalogues**, and six Relationships, as shown in following Figure. The model is also complemented by **eight instantiation schemes**, described in Section6.3.

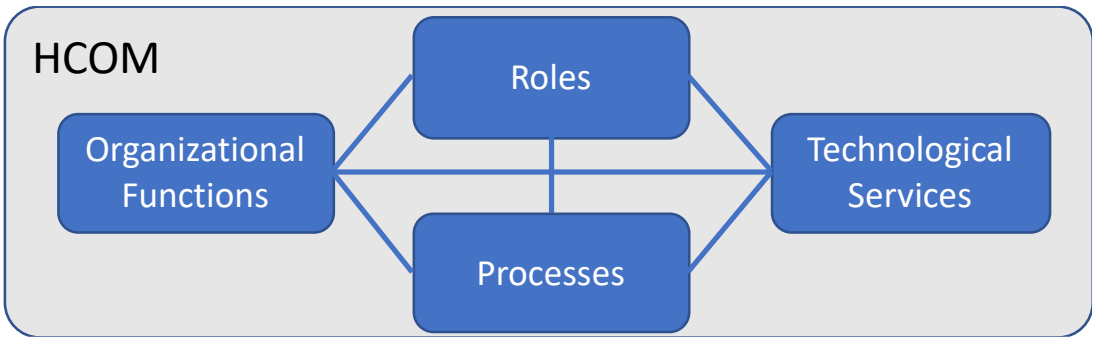

Figure 6-1 Healthcare Organization Model (HCOM): Entities, Catalogues and Relationships

6.1 Entities and Catalogues

6.1.1 Technological Services

Technological services Entity represents all kind of technology (software applications, hardware infrastructure, data, medical devices, workstations) which is used, directly and indirectly, to perform both healthcare and non-healthcare processes.

The related **Technology Services Catalogue** aims at including and classifying every type of technological asset that a cyber-attack may harm, thereby impacting on business continuity, patient safety, data confidentiality or integrity.

The catalogue has been built

- starting from the broad ICT segmentation used in the Enterprise Architecture models, which consists of three layers: application, data, infrastructure;
- customizing application and data layers to the healthcare section: this has been possible by comparing and merging the taxonomies used by the healthcare providers Partners of the Panacea Consortium (FPG, HESE, 7HRC) for describing their ICT assets;
- Adding to the typical ICT assets, the Networked Medical Devices, adopting the classification proposed in [ENISA] and other devices (access devices, identification devices) relevant from the cybersecurity point of view;
- verifying the completeness against the segmentation proposed in [ENISA].

The resulting high-level structure of the Catalogue includes 10 Areas and is shown in Table 6-1.

Type	Area
Applications	Clinical services
	Internet accessible services
	Corporate services
	Facility management services
	Data services
	Infrastructure services

Type	Area
Devices	Networked medical devices
	Identification devices
	Access devices
	Infrastructure

Table 6-1 HCOM Technology Services Catalogue: summary view

Areas are further segmented, leading to **38 different technological services**. The full version of the catalogue is contained in following Table 6-2. In the same Table, for each service is also indicated the ENISA type of asset and examples of systems/devices or functionalities

Type	Area	Service	ENISA type	Examples
Applications	Clinical services	Radiology	Interconnected information systems	PACS, RIS
		Laboratory	Interconnected information systems	Laboratory management system
		Operating room	Interconnected information systems	Surgery list
		Speciality	Interconnected information systems	Cancer, Cardiology, Maternity, Nursing, Intensive care
		Patient administration	Interconnected information systems	Electronic Health Record, Patient Admission and Billing
		Clinical trials management	Interconnected information systems	Patients enrolment management, Clinical trial monitoring
		Hospital Pharmacy Management	Interconnected information systems	Stock management
		Territorial Pharmacy Management	Interconnected information systems	Medicines prescriptions management
		Territorial medical and operational services	Interconnected information systems	Public hygiene Medical Record, Regional Service Desk Outpatient Booking System, GP systems
		Emergency pre-hospital services	Interconnected information systems	Decision support systems for mass casualty management
		Remote clinical services	Remote care assets	Telecare/Teleconsultation Services
	Internet accessible services	Corporate e-mail	Interconnected information systems	Corporate Mail
		Portal	Interconnected information systems	Hospital portal
		Apps for patients	Mobile client devices	On line booking
		Apps for suppliers	Mobile client devices	Facility maintenance incident management
		Apps for internal staff	Mobile client devices	App to communicate illness
	Corporate services	Staff management	Interconnected information systems	Active directory, HR management system, Payroll
		Accounting	Interconnected information systems	General ledger
		Procurement	Interconnected information systems	ERP module for procurement
		Services for staff	Interconnected information systems	Intranet Portal
	Facility management services	Domotics	Building and facilities	Power regulation, Climate regulation, Medical gas supply, Door lock system
		Building and facilities management	Interconnected information systems	Facilities maintenance management, Ticketing
	Data services	Management Reporting	Interconnected information systems	Sistema di ICT Ticketing & Troubleshooting
		Clinical reporting	Interconnected information systems	Emergency room statistics

Type	Area	Service	ENISA type	Examples
		Document Management	Interconnected information systems	Document archiving, Electronic signature
		Data bases	Data	Patients, Suppliers, Epidemiological, Clinical Trial, Documents, CMDB
	Infrastructure services	Data Centre and Networking applications	Interconnected information systems	Monitoring systems, patching delivery systems, centralized management systems, Backup system, VPN
Devices	Networked medical devices	Mobile devices	Networked medical devices	Portable ultrasound devices
		Wearable external devices	Networked medical devices	Wireless temperature counter
		Implantable devices	Networked medical devices	Cardiac pacemaker
		Stationary devices	Networked medical devices	Dialysis medical equipment
		Supportive devices	Networked medical devices	Assistive robot
	Identification devices	Patient identification devices	Identification systems	Bracelets, biometric scanners
		Staff identification devices	Identification systems	Biometric scanners, Smart badges (e.g. ultrasound enabled)
	Access devices	Company-owned access devices	Mobile Client devices (+ Desktop)	Desktop, laptop, smartphone, VOIP telephone, pager, printer
		Employee-owned access devices (BYOD)	Mobile Client devices	Laptop, smartphone, tablet
	Infrastructure	Data Centre and Networking devices	Networking equipment	Server, SAN, Switch, Router
		Networks	Networking equipment	Wired LAN network, wireless LAN network, BLE, RF

Table 6-2 Healthcare Organization Model (HCOM): Catalogue of Technological Services

6.1.2 Processes

Processes Entity represents the operational workflows within a healthcare organization. They involve several and different Organizational Functions, Roles and many Technologies. Processes can include, for instance, Operating Room workflow, the Clinical Trial management workflow, Patient Billing.

The related **Process Catalogue** aims at including and classifying every activity performed by a healthcare provider.

Maps of processes for the healthcare industry are provided by the American Productivity & Quality Center, in [APQC].

We decided to focus, among the whole variety of available processes described by the APQC, on those satisfying the following criteria

- their execution involves use of applications and/or medical devices;
- they capture the specificity of each of the different situations represented by the three Panacea end users;
- They cover the most part of the clinical administrative and technical activities running in the healthcare delivery organizations.

This catalogue contains the most relevant processes in place in the three Panacea end-users, which are quite representative of the healthcare delivery organizations.

The high-level structure of the Catalogue includes 8 Areas (see Table 6-3), belonging to two broad classes

- **Health processes**, involving the relationship with the patients for care delivery purposes (e.g. operating room, Day hospital/clinic). They include **Hospital specific processes** and **Territorial processes;**
- **Administrative/Technical processes**, which include the patient billing activities and all the activities that make available the resources needed to run the health process (e.g. procurement, human resources management, facility management)[8]

Health Processes
Hospital workflows
Inter-hospital medical consultations
Territorial workflows
Cross-border exchange of patient related data
Emergency pre-hospital workflows
Administrative/Technical processes
Patient billing
Centralized processes
In-Hospital processes

Table 6-3 HCOM Processes Catalogue: summary view

Areas are further segmented, leading to 36 different processes. The full Catalogue is contained in followingTable 6-4, where for some process a note provides clarifications.

Process	**Notes**
Health Processes	
Hospital workflows	
Emergency department workflow	
Hospital admission	
Operating room	
Day hospital/clinic	The patient does not sleep in the hospital
Clinical therapy and diagnosis-Level of care not Involving continuous parameter monitoring	
Clinical therapy and diagnosis-Level of care Involving continuous parameter monitoring	example: Intensive care units
Outpatient	
Visit working hours operations	
Visit after hours	
Diagnostics exams	
Therapy	Dialysis, Chemotherapy, Radiotherapy
Clinical trial management	

[8] Administrative/Technical processes include also a specific class of Centralized processes, which are shared services (e.g. payroll management, procurement) that in multi-hospital organizations, or regional organizations, are provided at a centralized level for the benefit of all the hospitals or all the local health delivery units.

Process	Notes
Pharmaceutical workflows	
Galenic preparation	
Medication preparation	
Hospital pharmacy logistic management	
Medical management of wearable and implantable medical devices	Prescription, Implantation, activation, periodical monitoring, data retrieval are part of this process
Inter-hospital medical consultations	
Territorial workflows	
General Practitioner visit (without primary health record)	
General Practitioner visit (with primary health record)	
Centralized laboratory service	Samples are collected on the territory and analysed in a central laboratory
Home care services	
Cross-border exchange of patient related data	
Emergency pre-hospital workflows	
Emergency call and ambulance transportation	
Administrative/Technical processes	
Patient billing	
Centralized processes	
Human resources (not payroll)	
Human resources (payroll)	
Procurement	
Accounting	
Information and Communication Technology	
Facility management	
Critical infrastructure Incident management	e.g.: incidents related to Devices and Utilities availability
In-Hospital processes	
Human resources (not payroll)	
Human resources (payroll)	
Procurement	
Accounting	
Information and Communication Technology	
Facility management	
Critical infrastructure Incident management	e.g.: incidents related to Devices and Utilities availability

Table 6-4 Healthcare Organization Model (HCOM): Catalogue of Processes

6.1.3 Roles

Roles Entity represents the functions of all actors actually operating in a health organization.

Actors are not only internal staff, but are also external persons which may interact with technology (software applications, IT infrastructure, medical devices) and which consciously or unconsciously may harm the

technology itself and the related data flow. Roles of these actors can be, for instance, Specialist Medical Practitioners, Nurses, Patients, and Suppliers.

The related **Catalogue** refers to Roles in terms of "occupation" and not in terms of "job" or job profiles. According to [ILO]:

- a "job" is a "set of tasks and duties performed, or meant to be performed, by one person, including for an employer or in self-employment";
- "occupation" refers to the kind of work performed in a job. This work can be actually done in "a set of jobs whose main tasks and duties are characterized by high degree of similarity".

For instance, a "nurse" (which is an occupation) may perform a variety of jobs (e.g. in the surgery department, in outpatient service).

From the cybersecurity point of view, we are interested both in "occupation" and in "job" because:

- The "occupation" may be associated to a specific mindset and educational background, thus leading to specific behaviours in the interaction with the technology;
- The "job" is associated to the process in which a worker is actually involved; depending on the process, the worker will interact with specific software applications or medical devices.

For instance, the "nurse" involved in the "operating room" process interacts with the "surgery list" application, while the "nurse" involved in another process will not interact with that application.

In HCOM the Role entity refers to the "occupation". The "job" is taken into consideration by the pair Role-Process.

In order to get a proven and internationally valid list of occupations, we decided to use the International Standard Classification of Occupations, abbreviated as ISCO, which is an international classification under the responsibility of the International Labour Organization (ILO).

The ISCO classification is contained in [ILO] and covers occupations related to many industries. We selected the ones applicable to the Healthcare occupations and grouped them into a set of **15 Roles**. They group a total of **26 ISCO occupations**, which can also be used as **Sub-Roles**, in case a more specific classification is needed.

The Catalogue also includes external roles, regarding **Patients** and **Suppliers**.

The full Catalogue is contained in followingTable 6-5, where the Roles have a two-digit code (e.g. 2.3 for "Nurses") and the Sub-Roles have three-digit code (e.g. 2.3.2 for "Midwifery Professionals"). The Sub-Roles are also ILO-ISCO occupations, which are identified with an ILO-ISCO code (e.g. 222 for "Midwifery Professionals".

Annex A provides definitions and examples of ISCO occupations and, therefore, of the Sub-Roles.

Role code	Roles		Sub-Roles/ ILO-ISCO occupations	ILO-ISCO code
	Managers			
1.1	Health services Managers	1.1.1	Health services Managers	1342
	Health Roles			
2.1	Generalist Medical Practitioners	2.1.1	Generalist Medical Practitioners	2211
2.2	Specialist Medical Practitioners	2.2.1	Specialist Medical Practitioners	2212
2.3	Nurses	2.3.1	Nursing Professionals	2221
		2.3.2	Midwifery Professionals	222

Role code	Roles		Sub-Roles/ ILO-ISCO occupations	ILO-ISCO code
		2.3.3	Nursing and Midwifery Associate Professionals	322
2.4	Paramedical practitioners	2.4.1	Paramedical Practitioners	224
2.5	Medical and Pharmaceutical Technicians	2.5.1	Medical and Pharmaceutical Technicians	321
2.6	Ambulance Workers	2.6.1	Ambulance Workers	3258
2.7	Personal care workers in Health Services	2.7.1	Personal Care Workers in Health Services	53
2.8	Other Heath roles	2.8.1	Traditional and Complementary Medicine Professionals	223
		2.8.2	Other Health Professionals	226
		2.8.3	Traditional and Complementary Medicine Associate Professionals	323
		2.8.4	Other Health Associate Professionals (excluding 3258 Ambulance Workers)	325
	Non-health Roles			
3.1	Technical roles	3.1.1	Science and Engineering Professionals	21
		3.1.2	Science and Engineering Associate Professionals	31
3.2	Administrative back-office roles	3.2.1	Business and Administration Professionals	24
		3.2.2	General and Keyboard Clerks	41
		3.2.3	Numerical and Material Recording Clerks	43
3.3	Administrative front-office roles	3.3.1	Customer Services Clerks	42
3.4	Medical Secretaries	3.4.1	Medical Secretaries	3344
3.5	Information and Communications Technology roles	3.5.1	Information and Communications Technology Professionals	25
		3.5.2	Information and Communications Technicians	35
3.6	Other non-health roles	3.6.1	Legal, Social and Cultural Professionals	26
		3.6.2	Religious Associate Professionals	3413
		3.6.3	Other Clerical Support Workers	44
	External roles			
4.1	Patients	4.1.1	Patients in the healthcare premises	NA
		4.1.2	Patients outside the healthcare premises	NA
4.2	Suppliers	4.2.1	Suppliers operating in the healthcare premises	NA
		4.2.2	Suppliers operating outside the healthcare premises	NA

Table 6-5 Healthcare Organization Model (HCOM): Catalogue of Roles

6.1.4 Organizational Functions

Organizational Functions Entity represents the organizational structure of the healthcare provider.

Organizational structure is usually represented as an organigram or as a list of organizational Units (general term or Offices, or Departments, or Divisions).

However, every actual provider has a very specific and peculiar organigram. This is why the model uses the concept of “organizational function”, as a standard concept that can be applied across different organizations.

A “function” represents the main contribution that an organizational Unit provides to the business. If we consider the units of an organigram at its lowest hierarchical level, normally more than one unit belongs to the same function. Examples of functions are: Surgery, Diagnostic services, Procurement. Surgery may include Units such as General Surgery Department, Cardiac Surgery Department, and Eye Surgery Department.

This **Organizational Functions Catalogue** is specific to the healthcare delivery organizations and results from the functions that are in place at the three Panacea end-users (FPG, HSE, 7HRE). These functions are quite representative of any hospital and territorial healthcare delivery organizations.

The result has been a Catalogue, shown in Table 6-6, of three groups (**Territorial health functions**, **Hospital health functions**, **Support functions) further articulated in 27 Functions** (e.g. 1.1 Prevention), further articulated in **49 Sub-Functions** (e.g. 1.1.1 Hygiene, 1.1.2 Public Health)

1. Territorial health functions
1.1. Prevention
1.1.1. Hygiene
1.1.2. Public Heath
1.1.3. Prevention of chronic-degenerative diseases
1.1.4. Midwifery services
1.2. Diagnosis
1.2.1. Family doctor
1.2.2. Family paediatricians
1.2.3. Specialist doctors
1.2.4. Radio diagnostics
1.2.5. Laboratory diagnostics
1.3. Assistance
1.3.1. Rehabilitation
1.3.2. Assisted medical home living
1.3.3. Mental health assistance
1.3.4. Dependency and addiction assistance
1.4. Emergency
1.4.1. Call centre
1.4.2. Ambulance Services
1.5. Legal and tax medicine
1.6. Drug pharmaceutics
1.10. Other territorial functions
2. Hospital health functions
2.1. Emergency
2.1.1. Emergency Room
2.1.2. Emergency service
2.1.3. Psychiatric assistance

2.2. Anaesthesia
2.3. Intensive therapy
2.4. Surgery
2.5. Medicine
2.6. Rehabilitation
2.7. Diagnostic services
2.7.1. Radio diagnostics
2.7.2. Laboratory diagnostics
2.8. Histopathology
2.9. Outpatient Clinics
2.10 Drug pharmaceutics
2.11.Blood banks
2.12.Ethical Committee
2.13.Other hospital functions
3. Support functions
3.1.Operation Support functions
3.1.1. Hotel services
3.1.2. Admittance
3.2. Administrative support functions
3.2..1. Staff management
3.2.2. Accounting
3.2..3. Procurement
3.2..4. Document Management
3.2..5. Patient Billing
3.3.Technical support functions
3.3.1. Information system management
3.3.2. Medical device management
3.3.3. Facility management
3.4. Communication functions
3.4.1. Media relations
3.4.2. Public relations
3.5. Education and lifelong Learning
3.6. Quality assurance
3.7. Other support functions

Table 6-6 Healthcare Organization Model (HCOM): Catalogue of Organizational Functions

6.2 Relationships

HCOM includes six Entity to Entity relationships.

Following Table 6-7 describes the meaning of each relationship and the key information provided by the instantiation of the relationship:

Entity A	Entity B	Meaning of the relationship between items of A and items of B	What can tell us the instantiation of this relationship
Organizational Functions	Roles	an item of B operates in one or more items of A	Which Roles work in which Organizational Functions
Organizational Functions	Technology Services	an item of A uses one or more items of B	Which Technological Services are used by which Organizational Functions
Organizational Functions	Processes	an item of A contributes to one or more items of B	Which Organizational Functions are involved in which Processes
Roles	Technology Services	an item of A uses one or more items of B	Which Roles have access to which Processes
Roles	Processes	an item of A contributes to one or more items of B	Which Roles operate in which Processes
Technology Services	Processes	an item of A is used in one or more items of B	Which Technological Services are used in which Processes

Table 6-7 HCOM-Meaning of the inter-Entity relationships and of the related instantiations

6.3 Instantiation schemes

Eight instantiation schemes for HCOM are provided in following paragraphs.

They are indicated in Figure 6-2 (instantiations are numbered; numbers are referenced in next paragraphs, included in brackets [ ]).

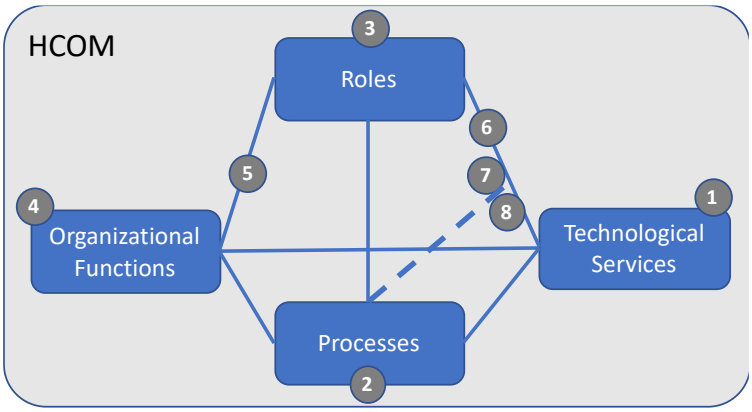

Figure 6-2 Healthcare Organization Model (HCOM): Entities and Instantiation Schemes

6.3.1 Technological Services

The instantiation [1] consists in:

- Associating the actual applications/software systems to the category in the catalogue (in case of big systems, the same software system may be associated to more than one category);
- Specifying the number of Medical Devices per type;
- Specifying the number of Workstations;
- Mapping the key links among systems (to show integration);
- Mapping at high level the available networks (to show integration).

6.3.2 Processes

The instantiation [2] consists in specifying which processes of the Catalogue are operative in the healthcare provider organization.

Each process can be associated to a business priority ranking, which depends on a variety of situational factors[9], to be identified and evaluated by the organization's management. This ranking may support decisions with regard.

If the Healthcare provider has more than one delivery site, the Instantiation Table may show which site is involved in which process (see Table 6-8 for an indicative example):

Process	Hospital 1	Hospital 2	Local Health Unit A	Local Health Unit B
Health Processes				
Hospital workflows				
Emergency department workflow	x	x		x
Operating room	x	x		
…				
Outpatient-Therapy	x	x	x	x
…				

Table 6-8 HCOM: Processes, Instantiation Table (indicative example, for multi-site healthcare provider)

A full and real example of instantiation is provided in following Table 6-9. It refers to the three end-users of the Panacea Consortium.

Process	FPG	7HRC	HSE
Health Processes			
Hospital workflows			
EMERGENCY DEPARTMENT TRIAGE & TREATMENT	x	x	x
Hospital admission			
Operating room	x	x	x
Day hospital/clinic	x		x
Clinical therapy and diagnosis-Level of care not involving continuous parameter monitoring	x	x	x
Clinical therapy and diagnosis-Level of care involving continuous parameter monitoring	x	x	x
Outpatient			
Visit working hours operations	x	x	x
Visit after hours	x	x	
Diagnostics exams	x	x	x
Therapy	x	x	x

[9] For instance, a priority criterion could be the relevance of the process in the territorial context; another criterion could be the reputation a hospital has for that process (e.g. cardiac surgery)

Process	FPG	7HRC	HSE
Clinical trial management	x		x
Pharmaceutical workflows			
Galenic preparation	x	x	x
Medication preparation	x	x	x
Hospital pharmacy logistic management	x	x	x
Medical management of wearable and implantable medical devices	x	x	x
Inter-hospital medical consultations			x
Territorial workflows			
General Practitioner visit (without primary health record)		x	x
General Practitioner visit (with primary health record)		x	x
Centralized laboratory service		x	x
Home care services			
Cross-border exchange of patient related data			x
Emergency pre-hospital workflows	x	x	x
Emergency call and ambulance transportation		x	x
Administrative/Technical processes			
Patient billing	x	x	x
Centralized processes			x
Human resources (not payroll)		x	x
Human resources (payroll)		x	x
Procurement		x	x
Accounting		x	x
Information and Communication Technology		x	x
Facility management		x	x
Critical infrastructure Incident management	x	x	x
In-Hospital processes			
Human resources (not payroll)	x	x	x
Human resources (payroll)	x	x	x
Procurement	x	x	x
Accounting	x	x	x
Information and Communication Technology	x	x	x
Facility management	x	x	x
Critical infrastructure Incident management	x	x	x

Table 6-9 HCOM: Processes, Instantiation Table (real case: FPG, 7HR, HSE)

6.3.3 Roles

The instantiation [3] consists in specifying which roles of the catalogue are associated to the actual professions operating in the organization in scope. It is useful also associating to the roles the number of staff members operating in the Units, to get a quantitative indicator of the relevance of the Units and of the function.

A good source for this instantiation is the Human Resources (HR) data base. It must be noted that, depending on the national regulations and work contracts, the professions may refer to more than one Role of the catalogue. The actual Role may be identified looking at the type of Unit where the professionals actually work.

In the example below, the “Assistente amministrativo” (i.e. Administrative Assistant) are both Administrative back-office roles (249 of them in FPG) and Administrative front-office roles (75 of them):

Hospital AAA: HCOM Roles --->Professional profiles in the Hospital	N. of staff
Administrative back-office roles	**513**
ASSISTENTE AMM.VO	249
COADIUTORE AMM.VO	97
COADIUTORE AMM.VO ESPERTO	7
COLLAB. AMM.VO PROFES.	99
COLLAB. AMM.VO PROFES. ESPERTO	52
COMMESSO	9
Administrative front-office roles	**115**
ASSISTENTE AMM.VO	75
COADIUTORE AMM.VO	24
COADIUTORE AMM.VO ESPERTO	3
COLLAB. AMM.VO PROFES.	5
COLLAB. AMM.VO PROFES. ESPERTO	4
COMMESSO	1
COMMESSO (P)	3

Table 6-10 HCOM: Roles, Instantiation Table (partial, from a real case: FPG)

Another example of instantiation has been impemented at HSE (see Table 6-11).

ROLE	CODE	HOSPITAL ROLE		CODE	COMMUNITI ROLE
Health services Managers	1.1.1	Assistant Director of Midwifery	Health services Managers	1.1.1	Area Director, Nursing
Health services Managers	1.1.1	Assistant Director of Nursing	Health services Managers	1.1.1	Chief Off, Community Healthcare Orgs
Health services Managers	1.1.1	Ast Dir of Nursing, Mental Health Svs	Health services Managers	1.1.1	Director of Community Care
Health services Managers	1.1.1	Assistant Dir of Public Health Nursing	Health services Managers	1.1.1	Director of Counselling - Nat Counselling Svs
Health services Managers	1.1.1	Chief Executive Hospitals	Health services Managers	1.1.1	Director of Nursing, Mental Health Services
Health services Managers	1.1.1	Chief Executive Officer, Hospital Groups	Health services Managers	1.1.1	Director of Public Health Medicine
Health services Managers	1.1.1	Chief Executive/Secretary Managers	Health services Managers	1.1.1	Director of Public Health Medicine
Health services Managers	1.1.1	Chief Finance Officer, Hospital Groups	Health services Managers	1.1.1	Director of Public Health Nursing
Health services Managers	1.1.1	Chief Financial Officer	Health services Managers	1.1.1	Head Svs/Function, Community H.care Orgs
Health services Managers	1.1.1	Chief Information Officer	Health services Managers	1.1.1	Local Health Office Manager (HSE)
Health services Managers	1.1.1	Chief Operations Officer, Hospital Groups	Generalist Medical Practitioners	2.1.1	Area Medical Officer Senior
Health services Managers	1.1.1	Dietician Manager-in-charge	Generalist Medical Practitioners	2.1.1	Community Ophthalmic Physician
Health services Managers	1.1.1	Director of Information Systems	Generalist Medical Practitioners	2.1.1	General Practitioner (GP, Doctor)
Health services Managers	1.1.1	Hosp Group Dir of Nursing & Midwifery	Generalist Medical Practitioners	2.1.1	GP Trainer/Supervisor
Health services Managers	1.1.1	Laboratory Manager	Generalist Medical Practitioners	2.1.1	Medical Officer (Community / District Hospital)
Health services Managers	1.1.1	Radiography Service Manager	Generalist Medical Practitioners	2.2.1	Dental Surgeons (All Categories)
Health services Managers	1.1.1	Technical Services Manager	Generalist Medical Practitioners	2.2.1	Specialist in Public Health Medicine
Generalist Medical Practitioners	2.1.1	Medical Officer - Senior / Principal	Nursing Professionals	2.3.1	Advanced Nurse Practitioner (Mental Health)
Generalist Medical Practitioners	2.1.1	Registrar / Sr Reg / Specialist Reg	Nursing Professionals	2.3.1	Community Mental Health Nurse
Specialist Medical Practitioners	2.2.1	Consultants	Nursing Professionals	2.3.1	Public Health Nurse
Specialist Medical Practitioners	2.2.1	Psychiatrist	Nursing Professionals	2.3.1	Staff Nurse
Paramedical Practitioners	2.2.1	Psychology, Director of	Nursing Professionals	2.3.1	Staff Nurse, Senior
Paramedical Practitioners	2.2.4	Cardiac Physiologist	Nursing Professionals	2.3.1	Staff Nurse, Senior (Mental Health)
Nursing Professionals	2.3.1	Advanced Nurse Practitioner	Other Health Professionals	2.8.2	Community Pharmacist
Nursing Professionals	2.3.1	Clinical Nurse Instructor	Other Health Associate Professionals	2.8.4	Child Care Manager
Nursing Professionals	2.3.1	Clinical Nurse Manager (General)	Other Health Associate Professionals	2.8.4	Community Welfare Officer
Nursing Professionals	2.3.1	Clinical Nurse Manager (Mental Health)	Other Health Associate Professionals	2.8.4	Environmental Health Officer
Nursing Professionals	2.3.1	Clinical Nurse Specialist (General)	Other Health Associate Professionals	2.8.4	Home Help Organiser
Nursing Professionals	2.3.1	Clinical Nurse Specialist (Mental Health)	Other Health Associate Professionals	2.8.4	Social Work Practitioner
Nursing Professionals	2.3.1	Staff Nurse	Other Health Associate Professionals	2.8.4	Social Worker (All Categories)
Nursing Professionals	2.3.1	Staff Nurse, Senior			
Nursing Professionals	2.3.1	Staff Nurse, Senior (Mental Health)			
Medical and Pharmaceutical Technicians	2.5.1	Clinical Photographer			
Medical and Pharmaceutical Technicians	2.5.1	Phlebotomist / Senior			
Medical and Pharmaceutical Technicians	2.5.1	Radiation Therapist			
Medical and Pharmaceutical Technicians	2.5.1	Radiographer			
Ambulance Workers	2.6.1	Ambulance Officer			
Other Health Professionals	2.8.2	Audiologist			
Other Health Professionals	2.8.2	Medical Scientist			
Other Health Professionals	2.8.2	Physicist			
Other Health Professionals	2.8.2	Physiotherapist / Senior			
Other Health Professionals	2.8.2	Psychologist			
Other Health Associate Professionals	2.8.4	Counsellor / Therapist			
Other Health Associate Professionals	2.8.4	Occupational Therapist Manager			
Science and Engineering Professionals	3.1.1	Analytical Chemist			
Science and Engineering Professionals	3.1.1	Biochemist			
Science and Engineering Professionals	3.1.1	Engineering Officer			
Science and Engineering Associate Professionals	3.1.2	Clinical Engineering Technician			
Science and Engineering Associate Professionals	3.1.2	ECG Technician			
Science and Engineering Associate Professionals	3.1.2	Emergency Medical Controller			
Science and Engineering Associate Professionals	3.1.2	Emergency Medical Technician			
Business and Administration Professionals	3.2.1	Catering Supervisor			
Business and Administration Professionals	3.2.1	Head Porter (Porter Supervisor)			
Business and Administration Professionals	3.2.1	Team Leader, Support Services			
General and Keyboard Clerks	3.2.2	Secretary			
Other Clerical Support Workers	3.6.3	Clerical Admin Management Grades			
Other Clerical Support Workers	3.6.3	Clerical Officer			

Table 6-11 HCOM: Roles, Instantiation Table (real case: HSE)

6.3.4 Organizational Functions

The instantiation [4] consists in specifying which organizational Units belong to an organizational function of the Catalogue.

It is useful also associating the number of staff members operating in the Units, to get a quantitative indicator of the relevance of the Units and of the function. In some cases, a Unit may perform two or three types of functions: attribution may be done by prevalence (see example below from FPG: Unit 10A performs Surgery, Medicine and Outpatient clinics, but Medicine is prevalent) or splitting it in two or three parts the Unit.

UNIT	N. of staff	Organizational Function
0J_PRONTO SOCCORSO - OBI	95	2.1. Emergency
0J_RIANIMAZIONE	58	2.3. Intensive therapy

UNIT	N. of staff	Organizational Function
0J_TERAPIA INTENSIVA PEDIATRICA	28	2.3. Intensive therapy
10B_CHIRURGIA ENDOCRINA E METABOLICA	16	2.4. Surgery
10C_CH DIGEST-CH ENDO METAB-DAY SURG	19	2.4. Surgery
-1J_CENTRO EMOTRASFUSIONALE	21	2.5. Medicine
-1J_SERVIZIO EMOTRASFUSIONALE	10	2.5. Medicine
10A_10B_DH+AMB CH ENDO METAB_DH+AMB END MAL METAB	7	2.5. Medicine
10D_ONCOLOGIA PEDIATRICA-DH+AMB ONCOLOGIA PEDIATRICA	23	2.5. Medicine
10E_SOLVENTI 1	22	2.5. Medicine
10L_SOLVENTI 4	16	2.5. Medicine
10M_PAT OBES-DH PAT OBES-ENDOCR-DERM	15	2.5. Medicine
-1V_7A_SERVIZIO MED. FISICA E RIABIL (C/O CEMI)	29	2.6. Rehabilitation
0U_1U_AMBULATORIO - DH MALATTIE INFETTIVE	5	2.9. Outpatient Clinics
0V_AMBULATORIO - DH CONTINUITA' ASSISTENZIALE	11	2.9. Outpatient Clinics
0L_PULIZIE SPOGLIATOI MEDICI	11	3.1. Operation Support functions

Table 6-12 HCOM: Organizational Functions, Instantiation Table (partial, from a real case: FPG)

6.3.5 Roles-Organizational functions

The instantiation [5] consists in specifying which Roles operate in each Organizational Function. At the cross there can be just “X” or the quantity of staff.

Following Table 6-13,Table 6-14 and Table 6-15 provide examples from real cases: HSE and 7HRC have indicated with an “X” the Roles working in each organizational function. FPG has extracted data from the HR Data Base, obtaining the quantification of the Panacea Roles per Panacea Organizational Functions.

	ROLES														
	MANAGERS	HEALTH ROLES								NON-HEALTH ROLES					
HSE	1.1	2.1	2.2	2.3	2.4	2.5	2.6	2.7	2.8	3.1	3.2	3.3	3.4	3.5	3.6
Functions	Health services Managers	Generalist Medical Practitioners	Specialist Medical Practitioners	Nurses	Paramedical practitioners	Medical and Pharmaceutical	Ambulance Workers	Personal care workers in Health	Other Heath roles	Technical roles	Administrative back-office roles	Administrative front-office roles	Medical Secretaries	Information and Communications	Other non-health roles
1. **Territorial health functions**															
1.1. Prevention	X	X	X	X	X	X	X	X						X	
1.2. Diagnosis	X	X	X	X	X	X	X	X							
1.3. Assistance	X	X	X	X	X	X	X		X						
1.4. Emergency	X	X	X	X	X	X	X	X		X					
1.5. Legal and tax medicine	X	X	X	X	X	X	X		X		X	X	X		X
1.6. Drug pharmaceutics	X	X	X	X	X	X	X				X				
1.10. Other territorial functions	X	X	X	X	X	X	X	X	X		X	X			X
2. Hospital health functions															
2.1. Emergency	X	X	X	X	X	X	X								
2.2. Anaesthesia	X	X	X	X	X	X	X								
2.3. Intensive therapy	X	X	X	X	X	X	X								
2.4. Surgery	X	X	X	X	X	X	X								
2.5. Medicine	X	X	X	X	X	X	X								
2.6. Rehabilitation	X	X	X	X	X	X	X		X		X	X			
2.7. Diagnostic services	X	X	X	X	X	X	X								
2.8. Histopathology	X	X	X	X	X	X	X								
2.9. Outpatient Clinics	X	X	X	X	X	X	X								
2.10 Drug store	X	X	X	X	X	X	X								
2.11.Ethical Committee	X	X	X	X	X	X	X		X		X	X			X
2.13.Blood banks	X	X	X	X	X	X	X								
2.14.Other hospital functions	X	X	X	X	X	X	X								
3. Support functions															
3.1.Operation Support functions	X									X	X		X		
3.2. Administrative support functions	X									X	X		X		
3.3.Technical support functions	X									X	X		X	X	
3.4.Communication functions	X									X	X		X		
3.5. Education and lifelong Learning	X									X	X		X		
3.6. Quality assurance	X	X	X	X	X	X	X	X	X	X	X	X	X		X
3.7. Other support functions	X									X	X		X		

Table 6-13 HCOM: Roles-Organizational Functions Relationship, Instantiation Matrix, real case (HSE)

	ROLES														
	MANAGERS	HEALTH ROLES								NON-HEALTH ROLES					
7HRC	1.1	2.1	2.2	2.3	2.4	2.5	2.6	2.7	2.8	3.1	3.2	3.3	3.4	3.5	3.6
Functions	Health services Managers	Generalist Medical Practitioners	Specialist Medical Practitioners	Nurses	Paramedical practitioners	Medical and Pharmaceutical	Ambulance Workers	Personal care workers in Health Services	Other Heath roles	Technical roles *	Administrative back-office roles	Administrative front-office roles	Medical Secretaries	Information and Communications	Other non-health roles
1. **Territorial health functions**															
1.1. Prevention		X	X	X	X			X					X	X	
1.2. Diagnosis		X	X	X	X	X				X			X	X	
1.3. Assistance		X	X	X	X			X					X		
1.4. Emergency		X	X	X	X		X			X					
1.5. Legal and tax medicine		X	X			X								X	
1.6. Drug pharmaceutics						X				X			X	X	
1.10. Other territorial functions														X	
2. Hospital health functions															
2.1. Emergency			X	X	X	X	X			X		X	X	X	
2.2. Anaesthesia			X	X	X	X				X					
2.3. Intensive therapy			X	X	X	X				X			X	X	
2.4. Surgery			X	X	X	X				X			X	X	
2.5. Medicine			X	X						X			X	X	
2.6. Rehabilitation			X	X	X	X	X	X		X			X		
2.7. Diagnostic services			X	X	X	X				X			X	X	
2.8. Histopathology			X		X	X				X			X	X	
2.9. Outpatient Clinics			X	X	X	X				X		X	X	X	
2.10 Drug store			X			X				X			X	X	
2.11.Ethical Committee	X		X										X		
2.13.Blood banks			X		X	X				X			X	X	
2.14.Other hospital functions															
3. Support functions															
3.1.Operation Support functions	X			X	X	X				X	X		X	X	
3.2. Administrative support functions	X		X	X	X	X				X	X		X	X	
3.3.Technical support functions										X		X		X	
3.4.Communication functions															
3.5. Education and lifelong Learning		X	X	X	X	X		X		X	X		X	X	
3.6. Quality assurance	X	X	X	X	X	X				X	X		X	X	
3.7. Other support functions															

*refers to texhnical roles related to maintaining devices, infrastructures etc

Table 6-14 HCOM: Roles-Organizational Functions Relationship, Instantiation Matrix, real case (7HRC)

	Roles	2.1. Emergency	2.2. Anaesthesia	2.3. Intensive therapy	2.4. Surgery	2.5. Medicine	2.6. Rehabilitation	2.7. Diagnostic services	2.8. Histopathology	2.9. Outpatient Clinics	2.10 Drug pharmaceutics	2.11.Blood banks	2.12.Ethical Committee	2.13.Other hospital functions	3.1. Operation Support functions	3.2. Administrative support functions	3.3. Technical support functions	3.4. Communication functions	3.6. Quality assurance	3.7. Other support function	**Total**
1.1	Health services Managers	2	1		1	20	4	29		14	18			6	4	13	14	1	1	11	**139**
2.2	Personal Care Workers in Health Services	9		13	38	50	6	1		36				10	2	1				1	**167**
2.2	Specialist Medical Practitioners	33	149	19	303	429	14	116	13	155	6	1	1	64	1		12	2		5	**1323**
2.3	Nurses	127		312	505	369	41	49	1	487	2	19		170	31	6	5	3		18	**2145**
2.4	Paramedical practitioners						32	6		32										2	**72**
2.5	Medical and Pharmaceutical Technicians				11	35		163	28	19				30			1				**287**
2.8	Other Health roles				11	63	6	3	2	27	1			19		1				1	**134**
3.1	Technical roles	3		7	14	16		15	3	17				11	30		73			114	**303**
3.2	Administrative back-office roles	1	2		28	36	2	20	7	17	14		5	115	28	130	47	10	3	48	**513**
3.3	Administrative front-office roles	41												4	48	3		3		16	**115**
3.5	Information and Communications Technology roles																11				**11**
3.6	Other non-health roles	37		50	70	57	1	15		65				51	77	6	42	1		134	**606**
	Total	**253**	**152**	**401**	**981**	**1075**	**106**	**417**	**54**	**869**	**41**	**20**	**6**	**480**	**221**	**160**	**205**	**20**	**4**	**350**	**5815**

Table 6-15 HCOM: Roles-Organizational Functions Relationship, Instantiation Matrix with n. of staff members, real case (FPG)

6.3.6 Roles-Technological Services

Roles-Technological Services relationship is important from the cybersecurity point of view, because it allows to identify possible vulnerabilities related to the interactions between people and technology (ICT, Medical Devices).

In this paragraph three Instantiation Schemes are described: [6], [7] and [8]

They are intended to facilitate the identification of the level of cybersecurity criticality of the Roles, with respect to the Technological Services.

Each Instantiation Scheme uses a slightly different metrics. It was not in the scope of Task 1.1 to define these metric. However, they are proposed:

- To provide a starting point for further analysis in the project;
- To show a possible use of the HCOM model.

All three metrics consider the criticality level in terms of Access rights and Impact.

The three schemes are complementary. They can be used in sequence.

The first scheme allows to identify, with a quick analysis, the most critical Roles in the entire organization or in wide sub-sections of it (e.g. Hospitals vs territorial Healthcare Units).

After this phase, leveraging on the second and third schemes, the analysis can focus on the processes where the most critical Roles are involved. The scheme considers, in an integrated manner, possible consequences of a cyberattack, analysing the ICT infrastructure at individual application level. The third metric focus on the risks related to personal data, analysing the ICT infrastructure at a more granular level, i.e., the functionality level inside the applications.

Instantiation Scheme [6], first metric

The instantiation consists on specifying the level of **cybersecurity criticality of a role, with respect to the Technology Services in general, without making reference to a specific Process or to a specific Technology Service.**

The criticality is estimated using the following two scores:

- **Overall Access score** (1=very low. 5=very high): it refers to the Roles's level of access to **Technology Services in general**; it is proportional to how much the role can do (Read, Read + Write, Read + Authorize, Read + Write + Authorize), and to the average number of functionalities the role can access;
- **Overall impact score** (A=very low impact, E=very high impact)**:** it refers to the negative **effect on the Healthcare organization** that the user could achieve with malicious intent or if it is a victim of a malicious intent; It relates to the number of systems that a user can access.

Note: a person has an "Authorize" right if he can decide on a "GO/NO GO" in a process; an example is the signature of a medical report triggering a further step in the process; another one is the authorization to launch a laboratory diagnostic process.

Following Table 6-16 provides an example.

Role		Professional profile in the instantiated organization	Operational environment	Overall access	Overall impact
2.3.1	Nursing Professionals	Advanced Nurse Practitioner	Hospital	C	3
2.3.1	Nursing Professionals	Clinical Nurse Specialist (Mental Health)	Hospital	B	1
2.3.1	Nursing Professionals	Advanced Nurse Practitioner	Territorial Health Unit	C	2
2.3.1	Nursing Professionals	Community Mental Health Nurse	Territorial Health Unit	A	1

Table 6-16 HCOM: Criticality per Role and Technological Services in general, Instantiation Table, with the first metric (adapted excerpt from a real case)

For each Role (in this case the Nursing Professionals), thanks to the Instantiation Table described in paragraph 6.3.3, the actual four Professional profiles are listed.

The table, besides Roles and Professional profiles, includes also an indication of the operational environment.

Operational environment is a key parameter because it could determine different scores (listed in the columns of Overall Access and Overall Impact) for similar professional profiles.

For instance, the Advanced Nurse Practitioner has a lower impact score in the Health unit environment with respect to the Hospital environment.

For each Professional profile, the ICT Department and the Manager of the Nurses have estimated the criticality scores. Criticality scores are associated to different colors, as it's evident in the columns of Overall access and Overall impact. Colors give an immediate visual indication of the level of criticality. As a whole, Nurses in the Hospital seem to be at a medium level of criticality, higher than the Nurses operating in the territorial Health Units.

Instantiation Scheme [7], second metric

The instantiation consists in specifying the **level of cybersecurity criticality of a role**, **in relation to a specific process and to the technological assets (applications, medical devices) currently used by the role in the process.**

The criticality is estimated using the following two scores:

- **Access score** (1=very low. 5=very high): it refers to the level of access to **the specific technological asset in the context of the process**; ; it is proportional to how much the role can do (Read, Read +

Write, Read + Authorize, Read + Write + Authorize), and to the number of **functionalities for the specific technological asset**, the role can access;

- **Impact score** (A=very low impact, E=very high impact)**:** it refers to the negative **effect on the process** that the user could achieve with malicious intent or if it is a victim of a malicious intent; It is evaluated in terms of loss of confidentiality, data integrity, production flow continuity.

Following Table 6-17 provides an example.

Technology services used in the Emergency department workflow	Nursing Professionals	Specialist Medical Practitioner	Paramedical Practitioner	Business and Administration Professional	Medical Imaging Technician
Admission Transfer Discharge-AAA system	5E	1E	1E	5E	
Radiology Picture Archiving Communication System-BBB system	2E	5E			5E
Emergency Medical Record-CCC system	2D	4E	4E	1B	

Table 6-17 HCOM: Criticality per Role- Technological Service-Process, Instantiation Matrix, with the second metric (adapted excerpt from a real case)

The Table refers to the "Emergency department workflow", which involves five Roles[10]. The applications on the left have been identified with the instantiation scheme described in paragraph 6.3.1. The Table shows the criticality scores associated to the pairs Role-Technology Service. For instance, the Nursing Professional Role is very critical with regard to the Admission Transfer Discharge-AAA system.

Instantiation Scheme [8], third metric

The instantiation, and the relate metrics, is quite similar to the previous scheme [7], but is applied at **a more analytical level** (**each functionality of the Technology Service**) and takes into account the **types of data managed by the functionality.**

The criticality is estimated using following two scores:

- **Access score**: it refers to the level of access to **the specific technological asset in the context of the process**; the level of access is described in terms of "Read, Read + Write, Read + Authorize, Read + Write + Authorize", with regard to the **specific functionality of the Technological service which is analysed;**
- **GDPR Criticality**: the type of data are classified in two categories: EU General Data Protection Regulation (GDPR) article 9 (i.e. very critical). Other data (i.e. less critical, from the point of view of the personal data.

Following Table 6-18 provides an example.

Process: AAA		ROLES			
		HEALTH ROLES		NON-HEALTH ROLES	
		2.2	2.5	3.3	3.5
Technological Services	Functionality	Specialist Medical Practitioners	Medical and Pharmaceutical Technicians	Administrative front-office roles	Information and Communications Technology roles
Laboratory system-xxx System	scheduling	9,RWA			
Laboratory system-xxx System	acceptance of samples		9,RA		

[10] It shows, as an example, three of the applications used in the process

Table 6-18 HCOM: Criticality per Role- Technological Service-Process, Instantiation Matrix, with the third metrics (adapted excerpt from a real case)

The reading of the table is similar to the reading of previous Table 6-17. Main differences consist in the presence of the column “Functionality” and in the metrics: 9, RWA means that

- the Nurse, when access the “scheduling” functionality of the Laboratory system xxx, can do everything (Read, Write, Authorize)
- the scheduling functionality treats personal data, classified as Article 9 of the GDPR.

The concept of “GDPR Criticality” has been introduced as it is a mandatory aspect according to the GDPR; in this context it is necessary to consider the high importance that the GDPR associates to the **"special category of personal data", identified in Art.9** (see [EU GDPR]).

Applications used within a hospital contain and treat both non-personal (e.g. financial data, contractual data) and personal data. The processing of personal data is governed by the GDPR.

“Personal data” means any information relating to an identified or identifiable natural person (“data subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person” (art. 4 GDPR).

Among the personal data, the GDPR identifies "special category of personal data" (art. 9).

The personal data included in this category are:

- data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership;
- genetic data (“genetic data means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question”, as per art. 4 GDPR);
- biometric data for the purpose of uniquely identifying a natural person (“biometric data means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data”, as per art. 4 GDPR);
- data concerning health (“data concerning health means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status”, as per Art. 4 GDPR);
- data concerning a natural person’s sex life or sexual orientation.

These special data reveal much more information about the patient than common personal data.

So, a potential data breach, (as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed – art. 4 GDPR) would have a strong impact on the privacy of data subjects.

For this reason, the GDPR establishes a special process to protect these data, more rigid than the common one.

7. Device Lifecycle Model (DLCM)

The DLCM describes the life of medical devices through **three Entities[11], three related Catalogues**, as shown in following Figure 7-1. The model also complemented by **two instantiation schemes**, described in Section 7.3.

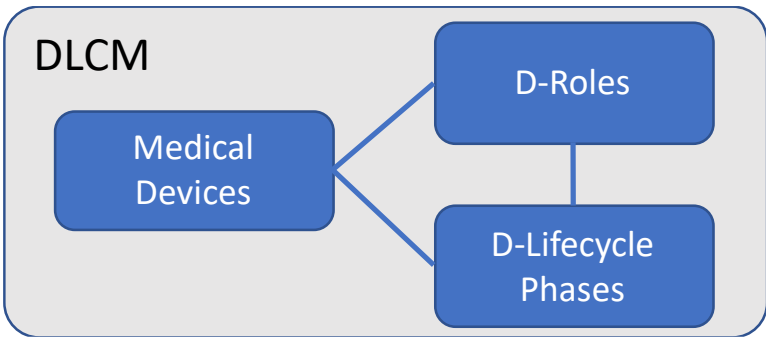

Figure 7-1 Device Lifecycle Model (DLCM): Entities, Catalogues and Relationships

7.1 Entities and Catalogues

7.1.1 Medical Devices

Medical Devices entity represents all the Medical Devices which are used to perform healthcare processes.

According to [EU MD REG], "*medical device* means any instrument, apparatus, appliance, software, implant, reagent, material or other article intended by the manufacturer to be used, alone or in combination, for human beings for one or more of the following specific medical purposes:

- diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease,
- diagnosis, monitoring, treatment, alleviation of, or compensation for, an injury or disability,
- investigation, replacement or modification of the anatomy or of a physiological or pathological process or state,
- providing information by means of in vitro examination of specimens derived from the human body, including organ, blood and tissue donation,

and which does not achieve its principal intended action by pharmacological, immunological or metabolic means, in or on the human body, but which may be assisted in its function by such means".

For Panacea project purposes, the Medical Devices in scope are a sub-set of above cases, relevant from the cybersecurity perspective: they must be networked, i.e. they transmit and/or receive data from other devices or ICT systems.

The Entity also includes assistive technology devices (which are designed to improve the functional capabilities of people with disabilities, see [AT] and [AT Rehab]), even if not all of them can be classified as Medical Devices (see [AT]), because they may share similar cybersecurity issues.

The DLCM adopts an already available categorization of Medical Devices, consistent with above requirements. It is provided in [ENISA]. Categories and examples are listed in following Table 7-1.

[11] The letter "D" stands for "Devices", to distinguish the entities from the HCOM ones

Macro-category	Category	Examples of Medical Devices
Networked medical devices	Mobile	Portable ultrasound devices
		Portable echocardiographic devices
		Portable insulin pump
	Wearable external	Wireless temperature counter
	Implantable	Cardiac pacemaker
	Stationary	High Automation Laboratory System
		Patient Ventilation system
		Infusion medical equipment
		Dialysis medical equipment
		Central Station Patient Monitoring
		Computer Tomography scanner
		Radiology equipment
		Chemotherapy dispensing station
		Life support machine
	Supportive	Assistive robot

Table 7-1 Device Lifecycle Model (DLCM): Medical Devices Catalogue

7.1.2 D-Lifecycle Phases

D-Lifecycle Phases entity represents the entire set of phases of the life of a medical device, from the Requirement Definition phase to the Disposal Phase. The lifecycle also includes the “Use” phase, i.e. the period during which a device is used for healthcare purposes.

The lifecycle adopted in the model has been designed in compliance with:

- the directions foreseen by the “Regulation (EU) 2017/745 of the European Parliament and of the Council on medical devices” (see [EU MD REG]) with regard to conformity assessment along the life of the Medical Devices;
- the IEC standard on “Medical device software – software life cycle processes” (see [IEC MD SW]).

Furthermore, the lifecycle intends to be generic enough to include the high variety of medical devices, belonging to different Classes (related to the level of potential hazard inherent in the type of device concerned), and with different mix of software-hardware composition.

A graphical representation of the Medical Devices lifecycle is shown in Figure 7-2 below.

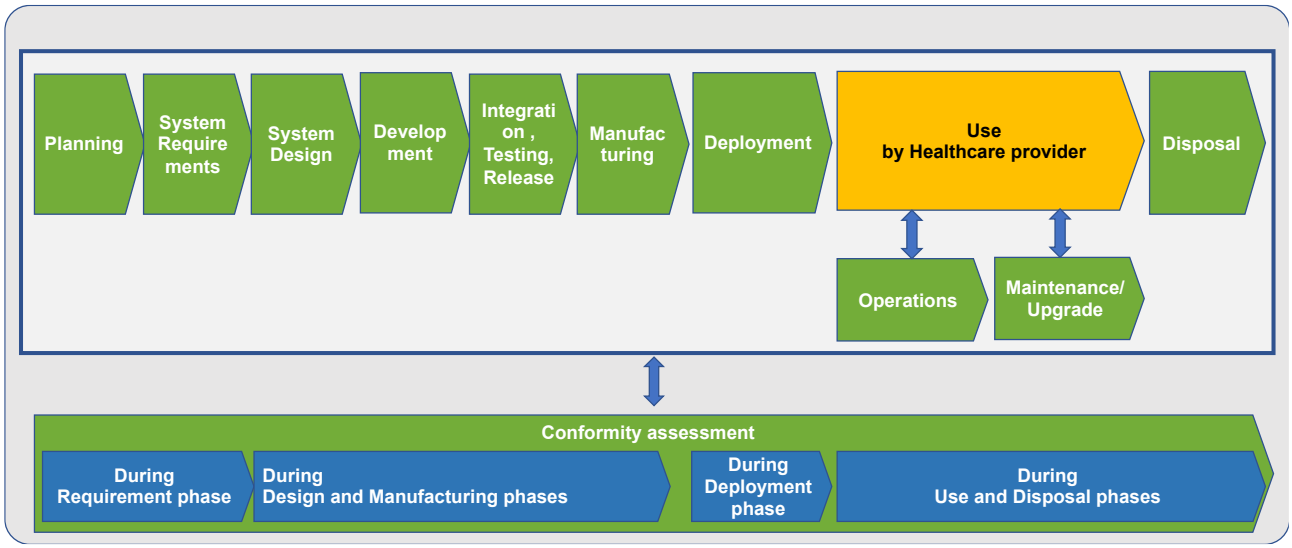

Figure 7-2 Device Lifecycle Model (DLCM): Lifecycle Phases

It is worth noting that the lifecycle refers:

- To a **new product** in the first phases of design and development (until Integration, Testing, Release);
- To an **individual item** during the manufacturing phase and in the deployment phase, when the individual item is delivered to a healthcare provider;
- To an **individual item** also in following phases, if the device is non-personal (e.g. radiology equipment);
- To an **individual AND personalized item**, from the Deployment phase, if the device is personal;
- To **both ICT and non-ICT**[12] components of the Medical Devices.

Following Figure 7-3 provides some details on the activities performed in terms of Conformity during the entire lifecycle of the Medical Device.

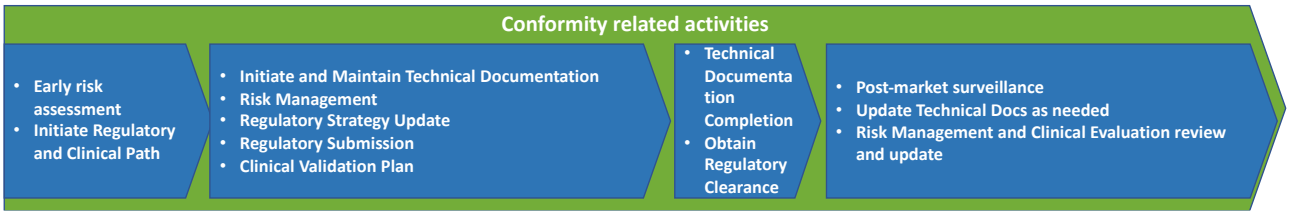

Figure 7-3 Device Lifecycle Model (DLCM): Conformity related activities

7.1.3 D-Roles

D-Roles Entity represents the functions of all actors currently operating during the medical device lifecycle. They include not only internal staff, but also every type of external actor who has a role during the lifecycle and that consciously or unconsciously may harm the devices and the related data flow or may put the basis for device vulnerabilities.

[12] E.g. mechanical, electrical, radiological components

D-Roles Catalogue includes all the Roles involved during the lifecycle include three main categories: Manufacturers, Third Parties, User organizations, meaning the Healthcare Providers. It also includes a sub-set of the HCOM Roles Catalogue (e.g. Technical staff and device users).

The catalogue is built

- selecting the roles from the HCOM catalogue, that may be involved during the lifecycle[13],
- selecting the roles from the SLCM roles catalogue (see paragraph 8.1.3);
- adding the manufacturer's roles, needed to develop, manufacture and deploy the medical devices
- adding roles related to the regulations and to the need to identify the individual medical device

In particular:

- There are specific Roles related to the conformity regulatory duties: Manufacturer's Conformity Responsible Person, Notified Body (to assess the conformity of the device before being placed on the market), Healthcare provider's Medical Devices Surveillance Responsible Person;
- The role of Trust Service Provider (TSP), in general provides customers with electronic security services to customers (see [ENISA TRUST]), such as electronic time stamps, and electronic authentication. In the context of the Medical Device lifecycle, the TSP responses to the need to identify the individual medical device and is intended to provide, for instance, services for:
    - Preventing Security breach (as device cloning …);
    - Identifying a device by its Unique ID;
    - Ensuring an end to end communication with the device via its crypto keys.

The resulting Catalogue includes 16 Roles, as shown in Table 7-2 below.

Manufacturer
System architect
Research & Development Specialist
Hardware architect
Software developer
Legal advisor
Maintenance staff
Data analyst
Conformity Responsible Person
Third Party
Trust Service Provider
Notified Body
Healthcare provider
Specialist Medical Practitioners (e.g. Radiologist)
Medical and Pharmaceutical Technicians (e.g. Medical Imaging Technicians)
Nurses
Patients
Technical Roles (Device Dept. Engineer/Technician)
Technical Roles (Medical Devices Surveillance Responsible Person)

Table 7-2 Device Lifecycle Model (DLCM): Roles Catalogue

[13] Not only the Medical Device Manufacturer, but also the Healthcare providers. Hey are involved not only during the "use" Phase, but also to provide requirements and to get training; Patients may be involved for the same reason

7.2 Relationships

DLCM includes three Entity to Entity relationships.

Following Table 7-3 describes the meaning of each relationship and the key information provided by the instantiation of the relationship:

Entity A	Entity B	Meaning of the relationship between items of A and items of B	What can tell us the instantiation of this relationship
Medical Devices	Roles	an item of B operates in the lifecycle of one or more items of A	For a given medical device X, which set of roles operates in the lifecycle For another medical device, Y, a different set of roles may operate in the lifecycle
Medical Devices	D-Lifecycle Phases	an item of B (a lifecycle phase) is applicable to one or more items of A	For a given medical device X, which set of phases is included in its lifecycle For another medical device, Y, a different set of phases may be included
D-Roles	D-Lifecycle Phases	an item of A operates in one or more items of B (lifecycle phases)	Which Roles operate in which Phases

Table 7-3 DLCM-Meaning of the inter-Entity relationships and of the related instantiations

7.3 Instantiation schemes

Two of the possible instantiation schemes for DLCM are provided in following paragraphs

They are indicated in Figure 7-4 (instantiations are numbered; numbers are referenced in next paragraphs, include in brackets [ ]).

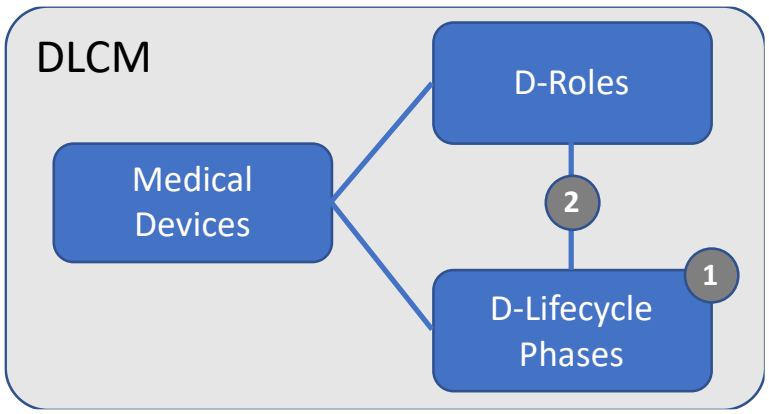

Figure 7-4 Device Lifecycle Model (DLCM): Entities and Instantiation Schemes

7.3.1 D-Lifecycle Phases

The instantiation [1] consists in specifying, for a given Medical Device

- which phases are actually done, making reference to the generic D-Lifecycle;
- which steps are done in each phase.

The example shown in Table 7-4 below refers to the real case of the QTRobot.

QTRobot[14] is a humanoid robot, built and designed to assist in teaching new skills to children with autism spectrum disorder or daily functioning for elder people who live at home, helping them to benefit more from educational sessions.

The robot can be connected in a network and can be remotely programmed/controlled. Data transmitted include the history of the educational programs-games, and particularly time of the day, duration of each game, game results, etc., as well as user's data such as his/her emotion during the game and reaction time of the user.

The instantiation has consisted in the description of the Lifecycle[15].

Phase →	Requirement definition	Design	Prototyping	Manufacturing	Deployment	Use	Maintenance	Upgrade	Data exchange with Manufacturer	Disposal
Steps	Survey literature	2D design - QTrobot HW interface	QTrobot HW MVP by additive manufacturing	Injection moulding	Configuration	Following documentation	Shipment back to local distributor	In case of QTrobot HW: replacement with a new device	User Consent and Terms and Conditions	Send back to manufacturer or recycling centres
	Survey target clients	2D design - QTrobot SW user interface	QTrobot SW MVP	PCB production	Shipment to client	Troubleshooting Q&A	Repair by distributor or replacement	Releasing QTrobot SW update	Automatic data acquisition	
	Competition Analysis	Feedback loop from clients and adjustments of core interfaces	Feedback loop from clients and adjustments of QTrobot HW & SW MVPs	Series-A production & Quality Control	Kick-off call and Setup		Quality control	Acceptance by user and installation	Surveys	
	Regulatory Analysis	QTrobot SW architecture design	Product Certification tests and finalization of Bill of Materials	Mass Production			Shipment to client	Documentation and troubleshooting		
	Analysis of functional and non-functional requirements	QTrobot HW 3D design								

[14] QTRobot is designed and produced by LuxAI S.A., which is a company specializing in disruptive robotic solutions for education, health-care and entertainment. LuxAI S.A. is subcontractor of iSPRINT in the Panacea Project, as planned in the DOA (see [DOA1B]).

[15] The "conformity related activities" do not appear in the matrix because the QTRobot is an assistive technology device not obliged to certification.

Phase →	Requirement definition	Design	Prototyping	Manufacturing	Deployment	Use	Maintenance	Upgrade	Data exchange with Manufacturer	Disposal
	Requirement Specification									

Table 7-4 DLCM: D-Lifecycle Catalogue, Instantiation Table, real case (QTRobot)

7.3.2 D-Lifecycle Phases/D-Roles

The Instantiation [2] consists in specifying which of the Phases of the Catalogue apply to the category of Medical Devices (or to a specific Medical Device), which Roles are involved and which activities each Role performs in the Phase.

The instantiation scheme uses two normative matrixes:

- A **Role-Phase involvement matrix**, where an "X" proposes that the Role may operate in the Phase (see Table 7-5);
- A **Role-Phase activity matrix** (see Table 7-6), that describes the purpose of each phase and proposes the activity that each Role may perform, if the "X" is present on the previous matrix.

Both matrixes have already been prepared. They contain hypothesis of Role involvement and activity, to be used as starting point on the Medical Device for which the instantiation is done.

Roles	Conformity Assessment	Planning	System analysis & Requirements	System Design	Development	Integration, Testing, Release	Manufacturing	Deployment	Operations	Maintenance/Upgrade	Disposal
MANUFACTURER SIDE											
System architect		X	X	X	X	X	X	X		X	X
Research & Development Specialist		X	X	X	X						
Hardware architects			X	X	X	X	X	X		X	
Software architect			X	X	X	X				X	
Software developer					X	X				X	
Legal advisor		X	X				X	X		X	X
Maintenance staff			X		X					X	X
Data analyst			X	X	X					X	
Conformity Responsible Person	X										
THIRD PARTIES											
Trust Service Provider		X	X	X	X	x	X	X	X	X	X

Notified Body	X										
HC ORGANIZATION SIDE											
Specialist Medical Practitioners	X		X	X	X	X		X	X	X	X
Nurses			X	X	X	X		X	X	X	X
Patients			X		X	X		X	X	X	X
Device Dept. Engineer/technician			X		X	X		X	X	X	X
MD Surveillance Responsible Person	X										

Table 7-5 DLCM: Role-Phase involvement matrix

Roles/Phases	**Conformity Assessment**
Purpose -->	The Phase interacts which all the other phases of the Lifecycle. Purpose of the phase is to ensure that the product complies with the regulations. The phase includes conformity assessment (before the product is placed on the market), certification (CE marking), post-market surveillance. The overall responsible for these activities is the Manufacturer, with the involvement of the Notified Body (for conformity assessment) and of the user organization for post-market surveillance.
Conformity Responsible Person	Takes care of the Manufacturer's responsibility
Notified Body	Are officially designated by their national authority and carry out the procedures for conformity assessment vs applicable legislation, when a third party is required. They are mainly involved during Design and Manufacturing Phases
Specialist Medical Practitioners	Notify events relevant from the surveillance point of view
MD Surveillance Responsible Person	Collaborates with the Manufacturer, collecting and providing data for surveillance purposes
Roles/Phases	**Planning**
Purpose -->	Purpose of this first phase is to find out the scope of the needs of the customer and determine high-level solutions. Resources, costs, time, benefits and other items should be considered here. This process determines the scope of the project management and technical activities, identifies process outputs, project tasks and deliverables, establishes schedules for project task conduct, including achievement criteria, and required resources to accomplish project tasks.
System Architect	Develops information technology (IT) rules and system requirements that describe baseline and target architectures encompassing software and hardware components of the device. Within this phase, he may define an high-level preliminary overview of the system to better define the scope and close the contract.
Trust service provider	May be involved in this phase as a consultant on the preliminary definition of the system
Research & Development Specialist	Conducts systems (software and hardware) engineering research to develop new capabilities if needed. He may be involved in his phase as a consultant on the preliminary definition of the system
Legal Advisor	Provides legal advice and recommendations on relevant topics related to laws and regulations. Provides support from a contractual perspective.
Roles/Phases	**System Analysis & Requirements**
Purpose -->	In this phase, detailed user and system requirements are elicited from the users/customer and other stakeholders, the requirements are further analysed and refined, and plans and processes for managing the requirements throughout the rest of the system/device life cycle are developed.
System Architect	Develops system requirements (software and hardware) that describe baseline and target system architectures.
Research & Development Specialist	Conducts systems (software and hardware) engineering research to develop new capabilities if needed. He may be involved in his phase as a consultant on the preliminary definition of the system
Hardware architects	Develops hardware (ICT and non-ICT) requirements that describe baseline and target hardware architectures.

Software architect	Develops software requirements that describe baseline and target software architectures.
Maintenance staff	Device maintenance is fundamental, in particular for life-critical devices. Maintenance experts will need to be involved in this phase.
Legal advisor	Provides legal advice and recommendations on relevant topics related to laws and regulations. Provides support from a contractual perspective.
Data Analyst	Examines planned data flows of the device from multiple disparate sources with the goal of providing security and privacy insight.
Trust service provider	Involved in this phase for defining the workflow processes requested, and the level of security required.
Specialist Medical Practitioners	May contribute to the specifications of the requirements from a user point of view
Nurses	May contribute to the specifications of the requirements from a user point of view
Patients	May contribute to the specifications of the requirements from a user point of view
Device Dept. technician	Contributes to the specification of the requirements from a technical point of view (from the customer side, hence considering the specifics of the healthcare organization)
Roles/Phases	**System Design**
Purpose -->	Once the requirements are expressed and folded into a management process, a system architecture can be described. The architecture will be the foundation for further development, integration, testing, operation, interfacing, and improvement of the system as time goes on.
System Architect	Develops system architecture (software, hardware and their interfaces) fulfilling the requirements baseline. Depending on the device, a software architect may be involved.
Research & Development Specialist	Conducts systems (software and hardware) engineering research to develop new capabilities if needed. He may be involved in his phase as a consultant on the definition of the system
Hardware architects	Develop the detailed hardware (ICT and non-ICT) architecture of the device, in collaboration with the system architect.
Software architect	Develop the detailed software architecture of the device, in collaboration with the system architect.
Data Analyst	Designs and implements custom algorithms, workflow processes, and layouts for modelling, data mining, and research purposes. Constrained devices may need a specialist approach for data management.
Trust service provider	Develops system architecture (software, hardware and their interfaces) fulfilling the requirements baseline for Trusted server according to the devices constraints. Depending on the device, the trusted provider may be involved.
Specialist Medical Practitioners	May contribute to provide feedback on the architecture from a user point of view
Nurses	May contribute to provide feedback on the architecture from a user point of view
Roles/Phases	**Development**
Purpose -->	At this point in the system life cycle, a complete and comprehensive description of what and how the system is expected to perform has been developed along with an architectural representation to guide the actual design and development of the hardware, software, networking, and interfaces. From an hardware perspective, the development usually aims on producing prototypes of the components of the device.
System Architect	Guides the development of the device (hardware and software components and the interfaces)
Research & Development Specialist	Conducts systems (software and hardware) engineering research to develop new capabilities if needed. He may be involved in his phase as a consultant on the development of the system
Hardware architects	Guides the development and production of the hardware (ICT and non-ICT) components (including prototypes) of the device
Software architect	Guides the development of the software components of the device
Software developer	Under the guidance of the system architect (depending on the device, also a software architect may be involved), develops the software on board the device
Maintenance staff	Device maintenance is fundamental, in particular for life-critical devices. Maintenance experts will need to be involved in this phase.

Data Analyst	Contributes to the software development of the device. Constrained devices may need a specialistic approach for data management.
Trust service provider	Under the guidance of the system architect (depending on the device, also a software architect may be involved), develops the Trusted Services (e.g. key management, personalization, device authentication,…).
Specialist Medical Practitioners	may contribute to the set-up of the final prototype
Nurses	may contribute to the set-up of the final prototype
Nurses	may contribute to the set-up of the final prototype
Device Dept. technician	Contributes to the monitoring of the development from a technical point of view (from the customer side, hence considering the specifics of the healthcare organization)
Roles/Phases	**Integration, Testing, Release**
Purpose -->	During the design and development phase, all of the system's subsystems are developed. In the device integration phase, the device's components and their interfaces are integrated into an operational whole: different hardware components are integrated and their software is installed to be tested. The integration sub-phase is usually followed by a testing phase, to assess the compliance of the system with respect to the system requirements. The result of this phase is usually a limited number of prototypes of the device, ready for mass-production.
System Architect	Supervises the integration and the testing of the device to assess coverage of the requirements.
Hardware architects	Supervise the integration and the testing of the device to assess coverage of the requirements.
Software architect	Supervises the integration and the testing of the device to assess coverage of the requirements.
Software developer	Follows the integration and the testing of the device to assess coverage of the requirements.
Trust service provider	Involved in the end-to-end testing of the devices to assess coverage of the requirements.
Specialist Medical Practitioners	May contribute to the testing
Nurses	May contribute to the testing
Patients	May contribute to the testing
Device Dept. technician	Contributes to the integration and testing sub-phases from a technical point of view (from the customer side, hence considering the specifics of the healthcare organization)
Roles/Phases	**Manufacturing**
Purpose -->	The device has been successfully developed and tested and it is ready for mass production (which could be assigned to a third-party company). During this phase it is fundamental to monitor that the quality of the device does not reduce due to mass production.
System Architect	The system architect usually follows the mass manufacturing in order to provide guidance with respect to the specifications and to assess that the specifications are correctly followed.
Hardware architects	The hardware architects usually monitor the mass manufacturing in order to provide guidance with respect to the specifications and to assess that the specifications are correctly followed.
Legal advisor	In case of third-party companies involved in the manufacturing, the legal department of the producer may need to provide legal monitoring over the compliance of the manufacturing contract.
Trust service provider	The Trust service provider may be involved during the manufacturing process, especially if trusted services are used for the personalisation of the devices, to put or get the Unique ID, and/or personalize the Crypto keys, needed for data exchanges.
Roles/Phases	**Deployment**
Purpose -->	Once the system is verified and mass-manufactured in the previous phases, it needs to be deployed in the target environment. This could involve deployment over humans, or integration in complex IT infrastructure, or both.
System Architect	Follows the integration and the testing of the device to assessment coverage of the requirements.
Hardware architect	Follows the integration and the testing of the device to assessment coverage of the requirements.
Legal advisor	Provides legal advice and recommendations on relevant topics related to laws and regulations. Provides support from a contractual perspective.

Trust service provider	Involved in the deployment, ensure that the device is correctly identified, and authorized to work in healthcare area.
Specialist Medical Practitioners	Depending on the device, may be involved in the deployment
Nurses	Depending on the device, may be involved in the deployment
Patients	Depending on the device, may be involved in the deployment
Device Dept. technician	Contributes to the monitoring of the deployment from a technical point of view (from the customer side, hence considering the specifics of the healthcare organization). Will be involved in the integration (if needed) with the existing IT infrastructure.
Roles/Phases	**Operations**
Purpose -->	The purpose of the Operation Phase is to use the device(s) in order to deliver their services. Conditions may greatly vary depending on the device category and nature.
Trust service provider	May be involved in operations, if services are needed during this phase (e.g. authentication of the device, authentication of data coming from the device,…)
Specialist Medical Practitioners	Depending on the device, may be involved in the operation phase
Nurses	Depending on the device, may be involved in the operation phase
Patients	Depending on the device, may be involved in the operation phase
Device Dept. technician	Contributes to the monitoring of the operation phase. Activities may vary depending on the nature of the device and the related contract. For example, devices connected to the IT infrastructure of the hospital may need specific attention for this Role, while wearable and not connected devices may not involve the role
Roles/Phases	**Maintenance / Upgrade**
Purpose -->	Maintenance is a critical phase of the life-cycle: it must be properly resourced from a supplier and a customer point of view. Maintenance procedure (for example, organized with framework such as ITIL) must be defined and implemented. Because the technological underpinnings of a system are constantly changing, product improvements and upgrades, including the insertion of new technologies, must be planned for.
System Architect	May be involved in maintenance, depending on the request. Very likely involved to manage upgrade requests.
Hardware architect	May be involved in maintenance, depending on the request. Very likely involved to manage upgrade requests.
Software Developer	May be involved in maintenance, depending on the request. Very likely involved to manage upgrade requests.
Maintenance staff	Provides technical support to customers (depending on the case, it may be the end user or the healthcare institute) who need assistance utilizing the device.
Legal advisor	Provides legal advice and recommendations on relevant topics related to laws and regulations. Provides support from a contractual perspective.
Data Analyst	Examines data from multiple disparate sources with the goal of providing security and privacy insight. Designs and implements custom algorithms, workflow processes, and layouts for complex, enterprise-scale data sets used for modelling, data mining, and research purposes. Data analyst may be involved in the upgrade phase is the customers requires an update of the underlying data schemas of the devices.
Trust service provider	Execute Maintenance / Upgrade requested by the owner of the devices. identify the device by his unique ID, push the Maintenance / Upgrade software updates through a secured connection. Ensure that the device is correctly updated and may activate the device in the healthcare area.
Specialist Medical Practitioners	May contribute to define needed upgrades or request for maintenance
Nurses	May contribute to define needed upgrades or request for maintenance
Patients	May contribute to define needed upgrades or request for maintenance
Device Dept. technician	May contribute to define needed upgrades or request for maintenance

Roles/Phases	Disposal
Purpose -->	In the retirement stage, the devices and their related services are removed from operation. System Engineering activities in this stage are primarily focused on ensuring that disposal requirements are satisfied, from a technical and legal perspective.
System Architect	May be involved if specific technical information are needed during the disposal phase.
Maintenance staff	The task may be assigned to a sub-role of the maintenance staff, dedicated to the actual collection and disposal of the devices and related services.
Legal advisor	Provides legal advice and recommendations on relevant topics related to laws and regulations. Provides support from a contractual perspective.
Trust service provider	Depending on the device, this Role may be involved in the disposal (for example, for devices connected to the IT infrastructure)
Device Dept. technician	Depending on the device, this Role may be involved in the disposal (for example, for devices connected to the IT infrastructure)
Specialist Medical Practitioners	Involved in case of substitution of implantable device
Nurses	Involved in case of substitution of implantable device
Patients	Involved in case of substitution of implantable device

Table 7-6 DLCM: Role-Phase activity matrix

8. System Lifecycle Model (SLCM)

The SLCM (System Lifecycle Model) describes the life of a System through **three Entities, three related Catalogues and three Relationships**, as shown in Figure 8-1. The model is also complemented by **one instantiation scheme**, described in Section 8.3.

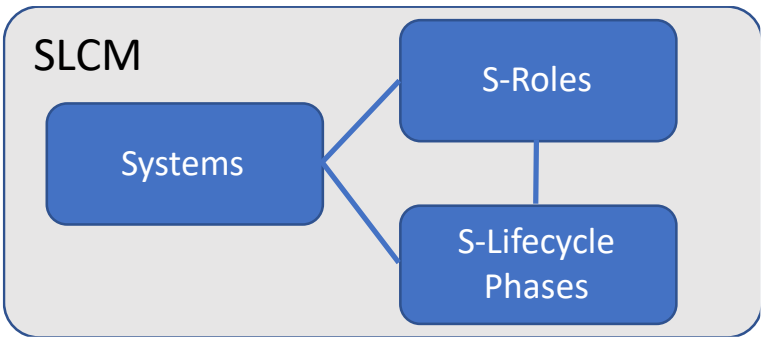

Figure 8-1 System Lifecycle Model (SLCM): Entities, Catalogues and Relationships

Note: the letter "S" (in *Lifecycle* and in *Roles*) stands for "System", to distinguish the entities from the HCOM ones.

8.1 Entities and Catalogues

8.1.1 Systems

Systems entity represents all the systems supporting healthcare processes. These are identified in Section 6.1.2, while Technological Services are identified in Section 6.3.1. From the Technological Services list it is possible to extract a set of assets (systems), classified as from [ENISA], supporting the Services and hence, the related healthcare processes. The system classification from [ENISA] also encompasses Networked Medical Devices: these devices are technically Systems, but due to their importance in the context of the PANACEA project, their relevance in the healthcare sector and their singularity in terms of manufacturing and diffusion, there are analysed on a separate instance in Section 7. In general, Section 8 provides a taxonomy for systems supporting healthcare processes.

Systems Catalogue is shown in the following Table 8-1; hey include all Technological Services from HCOM (Section 6.1.1), without the Medical Devices; they are listed with a focus on the different categories of systems as from [ENISA] taxonomy.

Type	Area	Service	System Category	Examples
Applications	Clinical services	Radiology	Interconnected information systems	PACS, RIS
		Laboratory	Interconnected information systems	Laboratory management system
		Surgery	Interconnected information systems	Surgery list
		Speciality	Interconnected information systems	Cancer, Cardiology, Histology, Maternity, Nursing, Intensive care
		Patient administration	Interconnected information systems	Electronic Health Record, Patient Admission and Billing
		Clinical trials management	Interconnected information systems	
		Hospital Pharmacy Management	Interconnected information systems	Stock management
		Territorial Pharmacy Management	Interconnected information systems	Medicines prescriptions management

Type	Area	Service	System Category	Examples
		Territorial medical and operational services	Interconnected information systems	Public hygiene Medical Record, Regional Service Desk Outpatient Booking System, GP systems
		Emergency pre-hospital services	Interconnected information systems	Decision support systems for mass casualty management
		Remote clinical services	Remote care assets	Telecare/Teleconsultation Services
	Internet accessible services	Corporate e-mail	Interconnected information systems	Corporate Mail
		Portal	Interconnected information systems	
		Apps for patients	Mobile client devices	On line booking
		Apps for suppliers	Mobile client devices	Facility maintenance incident management
		Apps for internal staff	Mobile client devices	App to communicate illness
	Corporate services	Staff management	Interconnected information systems	Active directory, HR management system, Payroll
		Accounting	Interconnected information systems	General ledger, Oracle
		Procurement	Interconnected information systems	Oracle
		Services for staff	Interconnected information systems	Intranet Portal
	Facility management services	Domotics	Building and facilities	Power regulation, Climate regulation, Medical gas supply, Door lock system
		Building and facilities management	Interconnected information systems	Facilities maintenance management, Ticketing
	Data services	Management Reporting	Interconnected information systems	Sistema di ICT Ticketing & Troubleshooting
		Clinical reporting	Interconnected information systems	Emergency room statistics
		Document Management	Interconnected information systems	Biometric scanners,
		Data bases	Data	Patients, Suppliers, Epidemiological, Clinical Trial, Documents, CMDB
	Infrastructure services	Data Centre and Networking applications	Interconnected information systems	Monitoring systems, patching delivery systems, centralized management systems, Backup system, VPN
Devices	Identification devices	Patient identification devices	Identification systems	Bracelets, biometric scanners
		Staff identification devices	Identification systems	Biometric scanners, Smart badges (e.g. ultrasound enabled)
	Access devices	Company-owned access devices	Mobile Client devices (+ Desktop)	Desktop, laptop, smartphone, VOIP telephone, pagers
		Employee-owned access devices (BYOD)	Mobile Client devices	Laptop, smartphone, tablet
	Infrastructure	Data Centre and Networking devices	Networking equipment	Server, SAN, Switch, Router
		Networks	Networking equipment	Wired LAN network, wireless LAN network, BLE, BT, RF

Table 8-1 System Lifecycle Model (SLCM): Systems Catalogue and Categories

8.1.2 S-Lifecycle

S-Lifecycle Phases Entity represents the entire set of phases of the life of a system, from the Requirement Definition phase to the Disposal/Phase-out Phase. The lifecycle also includes the “Operational” phase, i.e. the period during which the system is used by the healthcare organization.

A graphical representation of the System lifecycle is shown in Figure 8-2 below.

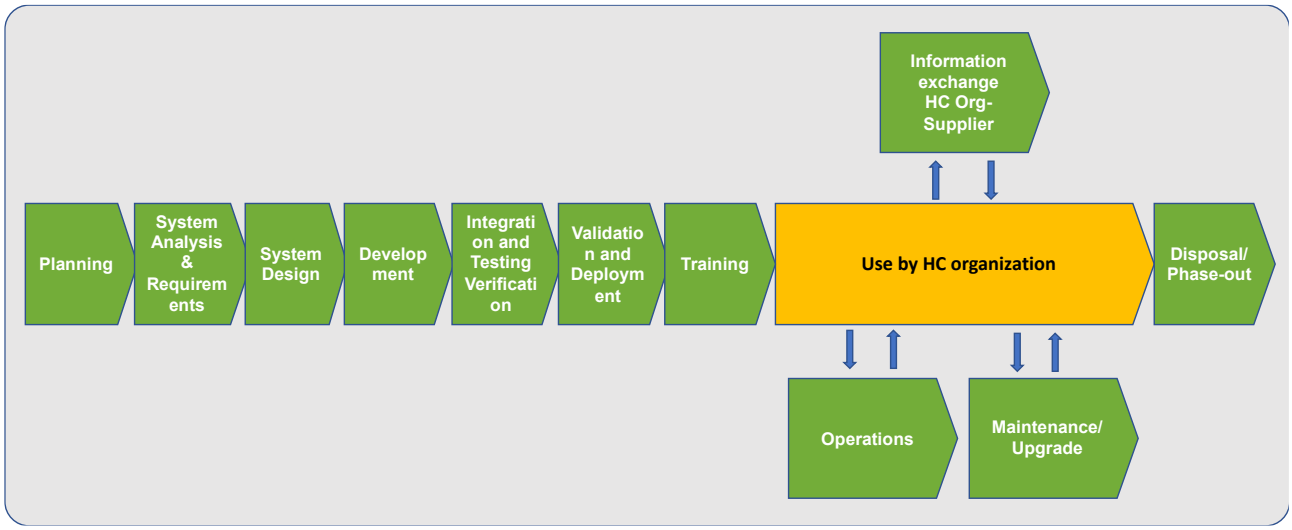

Figure 8-2 System Lifecycle Model (DLCM): Lifecycle Phases

The Phases are based on [NIST SLDC], adapted to take into account the perspective of the end-users, collected via interviews to the IT managers of FPG, 7HRC and HSE. In particular, the phase named "Implementation" in [NIST LC], has been split in two phases (Integration & Verification and Validation & Deployment) and a Training phase has been added.

Purpose and content of each phase are described in Section 8.3.1.

8.1.3 S-Roles

S-Roles Entity represents the actors actually involved in the different phases of the system lifecycle. They include not only staff of the healthcare organization leveraging the operational system, but also every type of actor which has a role during its lifecycle and, consciously or unconsciously, may harm it, or may put the basis for system vulnerabilities.

S-Roles Catalogue includes a sub-set of the HCOM Roles Catalogue from paragraph 6.1.3 (e.g. IT staff and system users).

In the following Table 8-2, Roles for systems in the healthcare domain are identified. The list is a combination of Roles from [NICE] and Roles identified in HCOM (paragraph 9.1.4).

SYSTEM SUPPLIER SIDE	HC ORGANIZATION SIDE
Software Developer	**Managers**
Enterprise Architect	Health services Managers
Security Architect	**Health Roles**
Research & Development Specialist	Generalist Medical Practitioners
Systems Requirements Planner	Specialist Medical Practitioners
System Testing and Evaluation Specialist	Nurses
Systems Developer	Paramedical practitioners
Data Analyst	Medical and Pharmaceutical Technicians
Technical Support Specialist	Ambulance Workers
Network Operations Specialist	Personal care workers in Health Services

SYSTEM SUPPLIER SIDE	HC ORGANIZATION SIDE
Legal Advisor	Other Health roles
Privacy Officer/Privacy Compliance Manager	**Non-health Roles**
Program Manager	Technical roles
IT Project Manager	Administrative back-office roles
Product Support Manager	Administrative front-office roles
Product Instructor	Medical Secretaries
Product Instructional Curriculum Developer	Information and Communications Technology roles
	Other non-health roles
	External roles
	Patients

Table 8-2 System Lifecycle Model (DLCM): Roles Catalogue

System Supplier side Roles are consistent with [NICE] and they are also included in the CSHCM catalogue of Roles.

Healthcare organization Roles are taken from the HCOM Catalogue of Roles.

8.2 Relationships

DLCM includes three Entity to Entity relationships.

Following Table 8-3 describes the meaning of each relationship and the key information provided by the instantiation of the relationship:

Entity A	Entity B	Meaning of the relationship between items of A and items of B	What can tell us the instantiation of this relationship
Systems	S-Roles	an item of B operates in the lifecycle of one or more items of A	For a given System X, which set of roles operates in the lifecycle For another System, Y, a different set of roles may operate in the lifecycle
Systems	S-Lifecycle Phases	an item of B (a lifecycle phase) is applicable to one or more items of A	For a given System X, which set of phases is included in its lifecycle For another medical device, Y, a different set of phases may be included
S-Roles	S-Lifecycle Phases	an item of A operates in one or more items of B (lifecycle phases)	Which Roles operate in which Phases

Table 8-3 DLCM-Meaning of the inter-Entity relationships and of the related instantiations

8.3 Instantiation schemes

One of the possible instantiation schemes for DLCM (see Figure 8-3) is provided in following paragraph.

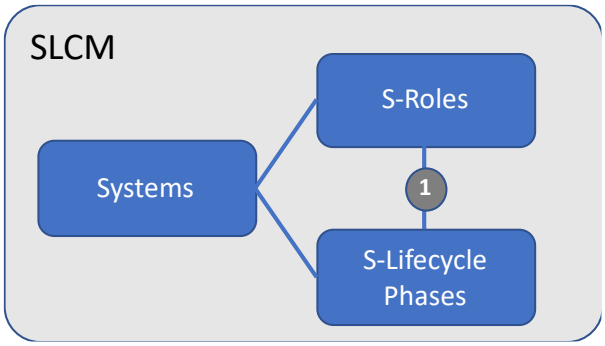

Figure 8-3 System Lifecycle Model (DLCM): Entities and Instantiation Schemes Lifecycle Phases/D-Roles

8.3.1 Catalogue 3: S-Roles – S-Lifecycle Phases

The instantiation (identified with 1 in Figure 8-3) applies to a given category of Systems (as from Table 8-1) or to a specific System A. It consists in specifying which of the Phases from Figure 8-2 apply to the category (or specifically to A), which S-Roles from Table 8-2 are involved and which activities each Role performs in the Phase.

The instantiation scheme consists in

- A **Role-Phase involvement matrix**, where an "X" indicates that the Role may be involved in the Phase
- A **Role-Phase activity matrix**, detailing the activity that the Role may perform in the specific Phase, if the combination is identified in the previously listed matrix

Aforementioned matrixes have been developed and are provided in following Table 8-4 and Table 8-5.

They contain hypothesis of Role involvement in the system life-cycle and related detailed activities, to be used as starting point on the specific healthcare system ***A*** for which the instantiation is done. They are consistent with [NIST SDLC], [ISO/IEC/IEEE 15288] and Table 6-5 from the HCOM model.

Lifecycle Phases / Roles	Planning	System Analysis & Requirements	System Design	Development	Integration & Verification	Deployment & Validation	Training	Operations	Maintenance / Upgrade	Information exchange	Disposal
SYSTEM SUPPLIER SIDE											
Software Developer				X	X	X			X		
System Architect	X	X	X	X	X	X			X		
Security Architect		X	X	X	X	X			X		
Research & Development Specialist	X	X	X	X							
Systems Requirements Planner		X			X	X					
System Testing and Evaluation Specialist					X	X			X		
Systems Developer				X	X	X			X		
Data Analyst		X	X	X						X	

Roles \ Lifecycle Phases	Planning	System Analysis & Requirements	System Design	Development	Integration & Verification	Deployment & Validation	Training	Operations	Maintenance / Upgrade	Information exchange	Disposal
Technical Support Specialist						X		X	X		X
Network Operations Specialist			X		X	X		X			X
Legal Advisor	X					X			X		X
Privacy Officer/Privacy Compliance Manager		X				X				X	
Program Manager	X										X
IT Project Manager	X	X	X	X	X	X	X		X	X	X
Product Support Manager								X	X	X	X
Product Instructor							X				
Product Instructional Curriculum Developer							X				
HC ORGANIZATION SIDE											
Managers											
Health services Managers	X	X	X	X	X	X	X	X	X	X	X
Health Roles											
Generalist Medical Practitioners		X				X	X				
Specialist Medical Practitioners		X				X	X				
Nurses		X				X	X				
Paramedical practitioners		X				X	X				
Medical and Pharmaceutical Technicians		X				X	X				
Ambulance Workers		X				X	X				
Personal care workers in Health Services		X				X	X				
Other Health roles		X				X	X				
Non-health Roles											
Technical roles		X				X	X				
Administrative back-office roles		X				X	X				
Administrative front-office roles		X				X	X				
Medical Secretaries		X				X	X				
Information and Communications Technology roles	X	X	X	X	X	X	X	X	X	X	X
Other non-health roles		X				X	X				
External roles											
Patients		X									

Table 8-4 System Lifecycle Model (SLCM): Role-Phase involvement matrix

Phase ==> / Roles	Planning
Purpose ==>	Purpose of this first phase is to find out the scope of the needs of the customer and determine high-level solutions. Resources, costs, time, benefits and other items should be considered here. This process determines the scope of the project management and technical activities, identifies process outputs, project tasks and deliverables, establishes schedules for project task conduct, including achievement criteria, and required resources to accomplish project tasks.
System Architect	Develops information technology (IT) rules and system requirements that describe baseline and target architectures. Within this phase, he may define a high-level preliminary overview of the system to better define the scope and main features and close the contract.
Research & Development Specialist	Conducts software and systems engineering and software systems research to develop new capabilities. He may be involved in his phase as a consultant on the preliminary definition of the system
Legal Advisor	Provides legal advice and recommendations on relevant topics related to law. Provides support from a contractual perspective.
Program Manager	Leads, coordinates, communicates, integrates, and is accountable for the overall success of the program, ensuring alignment with agency or enterprise priorities.
IT Project Manager	Directly manages information technology projects. Usually follows the entire project from Planning to Disposal.
Health services Managers	Usually initiates the project and monitors the entire lifecycle
Information and Communications Technology roles	May be involved in the initial definition of the scope and the constraints of the new system
Phase ==> / Roles	**System Analysis & Requirements**
Purpose -->	In this phase, detailed user and system requirements are elicited from the user and other stakeholders, the requirements are further analyzed and refined, and plans and processes for managing the requirements throughout the rest of the system life cycle are developed.
System Architect	Develops information technology (IT) rules and system requirements that describe baseline and target architectures.
Security Architect	Ensures that the stakeholder security requirements necessary to protect the organization's mission and business processes are adequately addressed in all aspects of the system architecture including reference models and segment and solution architectures.
Research & Development Specialist	Conducts software and systems engineering and software systems research to develop new capabilities. He may be involved in his phase as a consultant on the preliminary definition of the system
Systems Requirements Planner	Consults with customers to evaluate functional requirements and translate functional requirements into technical solutions.
Data Analyst	Examines data from multiple disparate sources with the goal of providing security and privacy insight. Designs and implements custom algorithms, workflow processes, and layouts for complex, enterprise-scale data sets used for modelling, data mining, and research purposes.
Privacy Officer/Privacy Compliance Manager	Develops and oversees privacy compliance program and privacy program staff, supporting privacy compliance, governance/policy, and incident response needs of privacy and security executives and their teams.
IT Project Manager	Directly manages information technology projects. Usually follows the entire project from Planning to Disposal.
Health services Managers	Contributes to the specifications of the requirements from a user point of view and follows up on monitoring the project
Generalist Medical Practitioners	May contribute to the specifications of the requirements from a user point of view
Specialist Medical Practitioners	May contribute to the specifications of the requirements from a user point of view
Nurses	May contribute to the specifications of the requirements from a user point of view
Paramedical practitioners	May contribute to the specifications of the requirements from a user point of view
Medical and Pharmaceutical Technicians	May contribute to the specifications of the requirements from a user point of view
Ambulance Workers	May contribute to the specifications of the requirements from a user point of view

Personal care workers in Health Services	May contribute to the specifications of the requirements from a user point of view
Other Health roles	May contribute to the specifications of the requirements from a user point of view
Technical roles	May contribute to the specifications of the requirements from a user point of view
Administrative back-office roles	May contribute to the specifications of the requirements from a user point of view
Administrative front-office roles	May contribute to the specifications of the requirements from a user point of view
Medical Secretaries	May contribute to the specifications of the requirements from a user point of view
Information and Communications Technology roles	Contributes to the specifications of the requirements from an infrastructure and constraints point of view
Other non-health roles	May contribute to the specifications of the requirements from a user point of view
Patients	May contribute to the specifications of the requirements from a user point of view
Phase ==> Roles	**System Design**
Purpose -->	Once the requirements are expressed and folded into a management process, a system architecture can be described. The architecture will be the foundation for further development, integration, testing, operation, interfacing, and improvement of the system as time goes on.
System Architect	Develops information technology (IT) rules and system requirements that describe baseline and target architectures.
Security Architect	Ensures that the stakeholder security requirements necessary to protect the organization's mission and business processes are adequately addressed in all aspects of the system architecture including reference models and segment and solution architectures.
Research & Development Specialist	Conducts software and systems engineering and software systems research to develop new capabilities. He may be involved in his phase as a consultant on the preliminary definition of the system.
Network Operations Specialist	Plans, implements, and operates network services/systems, to include hardware and virtual environments. In this phase, their contribution is usually to provide inputs for the system architecture.
Data Analyst	Examines data from multiple disparate sources with the goal of providing security and privacy insight. Designs and implements custom algorithms, workflow processes, and layouts for complex, enterprise-scale data sets used for modelling, data mining, and research purposes.
IT Project Manager	Directly manages information technology projects. Usually follows the entire project from Planning to Disposal.
Health services Managers	Usually involved in periodic architectural reviews (for example, Preliminary Design Review, Architectural Review) to monitor the progresses.
Information and Communications Technology roles	Usually involved in periodic architectural reviews (for example, Preliminary Design Review, Architectural Review) to help Health services Managers monitor the progresses.
Phase ==> Roles	**Development**
Purpose -->	At this point in the system life cycle, a complete and comprehensive description of what and how the system is expected to perform has been developed along with an architectural representation to guide the actual design and development of the hardware, software, networking, and interfaces.
Software Developer	Develops, creates, maintains, and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs.
System Architect	Develops information technology (IT) rules and system requirements that describe baseline and target architectures.
Security Architect	Ensures that the stakeholder security requirements necessary to protect the organization's mission and business processes are adequately addressed in all aspects of the system architecture including reference models and segment and solution architectures.
Research & Development Specialist	Conducts software and systems engineering and software systems research to develop new capabilities. He may be involved in his phase as a consultant on the preliminary definition of the system.
Systems Developer	Designs, develops, tests, and evaluates information systems throughout the systems development life cycle.

Data Analyst	Examines data from multiple disparate sources with the goal of providing security and privacy insight. Designs and implements custom algorithms, workflow processes, and layouts for complex, enterprise-scale data sets used for modelling, data mining, and research purposes.
IT Project Manager	Directly manages information technology projects. Usually follows the entire project from Planning to Disposal.
Health services Managers	Usually involved in periodic reviews to monitor the progresses.
Information and Communications Technology roles	Usually involved in periodic reviews to help Health services Managers monitoring the progresses.
Phase ==> Roles	**Integration and Verification**
Purpose ==>	During the design and development phase, all of the system's subsystems are complete. In the system integration phase, the system's components and its interfaces with other systems or networks are integrated into an operational whole. The integration sub phase is usually followed by a technical requirements verification phase, to assess the compliance of the system with respect to the system requirements.
Software Developer	Develops, creates, maintains, and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs.
System Architect	Develops information technology (IT) rules and system requirements that describe baseline and target architectures.
Security Architect	Ensures that the stakeholder security requirements necessary to protect the organization's mission and business processes are adequately addressed in all aspects of the system architecture including reference models and segment and solution architectures.
Systems Requirements Planner	Consults with customers to evaluate functional requirements and translate functional requirements into technical solutions. During this phase, this Role may be involved for the requirements verification.
Network Operations Specialist	Plans, implements, and operates network services/systems, to include hardware and virtual environments.
System Testing and Evaluation Specialist	Plans, prepares, and executes tests of systems to evaluate results against specifications and requirements as well as analyze/report test results.
Systems Developer	Designs, develops, tests, and evaluates information systems throughout the systems development life cycle.
IT Project Manager	Directly manages information technology projects. Usually follows the entire project from Planning to Disposal.
Health services Managers	Usually involved in periodic reviews to monitor the progresses.
Information and Communications Technology roles	Usually involved in periodic reviews to help Health services Managers monitor the progresses.
Phase ==> Roles	**Deployment & Validation**
Purpose ==>	Once the system is verified in the previous phase, it needs to be deployed in the operational environment (for example, an existing network or IT infrastructure) and validated. Validation refers on the testing activities to assess if the system is fulfilling its purpose from a stakeholders point of view. Testing at this phase also involves properties such as reliability, security, and interoperability.
Software Developer	Develops, creates, maintains, and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs.
System Architect	Develops information technology (IT) rules and system requirements that describe baseline and target architectures.
Security Architect	Ensures that the stakeholder security requirements necessary to protect the organization's mission and business processes are adequately addressed in all aspects of the system architecture including reference models and segment and solution architectures.
Systems Requirements Planner	Consults with customers to evaluate functional requirements and translate functional requirements into technical solutions.
System Testing and Evaluation Specialist	Plans, prepares, and executes tests of systems to evaluate results against specifications and requirements as well as analyse/report test results.
Systems Developer	Designs, develops, tests, and evaluates information systems throughout the systems development life cycle.
Technical Support Specialist	Provides technical support to customers who need assistance utilizing client-level hardware and software in accordance with established or approved organizational process components (i.e., Master Incident Management Plan, when applicable).
Network Operations Specialist	Plans, implements, and operates network services/systems, to include hardware and virtual environments.
Legal Advisor	Provides legal advice and recommendations on relevant topics related to law. Provides support from a contractual perspective

Privacy Officer/Privacy Compliance Manager	Develops and oversees privacy compliance program and privacy program staff, supporting privacy compliance, governance/policy, and incident response needs of privacy and security executives and their teams.
IT Project Manager	Directly manages information technology projects. Usually follows the entire project from Planning to Disposal.
Health services Managers	Involved in system validation.
Generalist Medical Practitioners	Possibly involved in system validation
Specialist Medical Practitioners	Possibly involved in system validation
Nurses	Possibly involved in system validation
Paramedical practitioners	Possibly involved in system validation
Medical and Pharmaceutical Technicians	Possibly involved in system validation
Ambulance Workers	Possibly involved in system validation
Personal care workers in Health Services	Possibly involved in system validation
Other Health roles	Possibly involved in system validation
Technical roles	Possibly involved in system validation
Administrative back-office roles	Possibly involved in system validation
Administrative front-office roles	Possibly involved in system validation
Medical Secretaries	Possibly involved in system validation
Information and Communications Technology roles	Involved in system validation
Other non-health roles	Possibly involved in system validation
Phase ==> Roles	**Training**
Purpose -->	The training phase is a fundamental step of the life-cycle, in particular for health care system. All health care personnel involved in the usage of the system at an operational stage needs to be properly involved in trainings.
IT Project Manager	Directly manages information technology projects. Usually follows the entire project from Planning to Disposal.
Product Support Manager	Manages the package of support functions required to field and maintain the readiness and operational capability of systems and components.
Product Instructor	Develops and conducts training or education of personnel.
Product Instructional Curriculum Developer	Develops, plans, coordinates, and evaluates cyber training/education courses, methods, and techniques based on instructional needs.
Health services Managers	Involved in project monitoring and overseeing and managing the training activities from a customer perspective
Generalist Medical Practitioners	Possibly involved in the trainings
Specialist Medical Practitioners	Possibly involved in the trainings
Nurses	Possibly involved in the trainings
Paramedical practitioners	Possibly involved in the trainings
Medical and Pharmaceutical Technicians	Possibly involved in the trainings
Ambulance Workers	Possibly involved in the trainings
Personal care workers in Health Services	Possibly involved in the trainings
Other Health roles	Possibly involved in the trainings
Technical roles	Possibly involved in the trainings
Administrative back-office roles	Possibly involved in the trainings
Administrative front-office roles	Possibly involved in the trainings
Medical Secretaries	Possibly involved in the trainings

Information and Communications Technology roles	Involved in training in order to support the operational phase.
Other non-health roles	Possibly involved in the trainings
Phase ==> Roles	**Operations**
Purpose -->	The purpose of the Operation Phase is to use the system in order to deliver its services. Personnel is assigned to operate the system, and monitors the services and operator-system performance. In order to sustain services it identifies and analyses operational problems in relation to agreements, stakeholder requirements and organizational constraints.
IT Project Manager	Directly manages information technology projects. Usually follows the entire project from Planning to Disposal.
Product Support Manager	Manages the package of support functions required to field and maintain the readiness and operational capability of systems and components.
Technical Support Specialist	Provides technical support to customers who need assistance utilizing client-level hardware and software in accordance with established or approved organizational process components (i.e., Master Incident Management Plan, when applicable).
Network Operations Specialist	Plans, implements, and operates network services/systems, to include hardware and virtual environments.
Health services Managers	Involved in project monitoring and overseeing.
Information and Communications Technology roles	Supporting the delivery of the services provided by the system to the user.
Phase ==> Roles	**Maintenance / Upgrade**
Purpose -->	Maintenance is a critical phase of the life-cycle: it must be properly resourced from a supplier and a customer point of view. Maintenance procedure (for example, organized with framework such as ITIL) must be defined and implemented. Because the technological underpinnings of a system are constantly changing, product improvements and upgrades, including the insertion of new technologies, must be planned for.
Software Developer	Develops, creates, maintains, and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs.
System Architect	Develops information technology (IT) rules and system requirements that describe baseline and target architectures.
Security Architect	Ensures that the stakeholder security requirements necessary to protect the organization's mission and business processes are adequately addressed in all aspects of the system architecture including reference models and segment and solution architectures.
System Testing and Evaluation Specialist	Plans, prepares, and executes tests of systems to evaluate results against specifications and requirements as well as analyze/report test results.
Systems Developer	Designs, develops, tests, and evaluates information systems throughout the systems development life cycle.
Data Analyst	Examines data from multiple disparate sources with the goal of providing security and privacy insight. Designs and implements custom algorithms, workflow processes, and layouts for complex, enterprise-scale data sets used for modelling, data mining, and research purposes. Data analyst may be involved in the upgrade phase is the customers requires an update of the underlying data schemas of the systems.
Legal Advisor	Provides legal advice and recommendations on relevant topics related to law. Provides support from a contractual perspective, relevant in case of dispute between the supplier and the customer.
IT Project Manager	Directly manages information technology projects. Usually follows the entire project from Planning to Disposal.
Product Support Manager	Manages the package of support functions required to field and maintain the readiness and operational capability of systems and components.
Technical Support Specialist	Provides technical support to customers who need assistance utilizing client-level hardware and software in accordance with established or approved organizational process components (i.e., Master Incident Management Plan, when applicable).
Health services Managers	Managers oversee the maintenance operations and may trigger upgrade requests to the supplier.
Information and Communications Technology roles	Depending on the set-up and the contract, customer IT support may be involved in some maintenance operations (first level support, for example).

Phase ==> / Roles	Information exchange HC Organization-Supplier
Purpose -->	This phase could be considered as part of the upgrade phase: it is dedicated to the exchanges between the customer and the supplier with respect to refinements and updates on the data format in order to adapt to changing legal and user requirements. It is particularly relevant in health care organizations due to the high quantity of personal data usually involved and the average frequency of data format may change due to regulations and policies.
Data Analyst	Examines data from multiple disparate sources with the goal of providing security and privacy insight. Designs and implements custom algorithms, workflow processes, and layouts for complex, enterprise-scale data sets used for modelling, data mining, and research purposes.
Privacy Officer/Privacy Compliance Manager	Develops and oversees privacy compliance program and privacy program staff, supporting privacy compliance, governance/policy, and incident response needs of privacy and security executives and their teams.
IT Project Manager	Directly manages information technology projects. Usually follows the entire project from Planning to Disposal.
Product Support Manager	Manages the package of support functions required to field and maintain the readiness and operational capability of systems and components.
Health services Managers	Managers may trigger data format change requests to the supplier.
Information and Communications Technology roles	IT staff of the customer may be involved on defining the data format changes, or they may be required in order to test data format changes within the operational environment.
Phase ==> / Roles	**Disposal**
Purpose -->	In the retirement stage, the System and its related services are removed from operation. System Engineering activities in this stage are primarily focused on ensuring that disposal requirements are satisfied, from a technical and legal perspective.
Technical Support Specialist	Provides technical support to customers who need assistance utilizing client-level hardware and software in accordance with established or approved organizational process components (i.e., Master Incident Management Plan, when applicable).
Network Operations Specialist	Plans, implements, and operates network services/systems, to include hardware and virtual environments.
Legal Advisor	Provides legal advice and recommendations on relevant topics related to law. Provides support from a contractual perspective
Program Manager	Leads, coordinates, communicates, integrates, and is accountable for the overall success of the program, ensuring alignment with agency or enterprise priorities.
IT Project Manager	Directly manages information technology projects. Usually follows the entire project from Planning to Disposal.
Product Support Manager	Manages the package of support functions required to field and maintain the readiness and operational capability of systems and components.
Health services Managers	Manages of the customer must follow the disposal phase in order to assess the closure of the contract and validate the proper removal of it from the infrastructure
Information and Communications Technology roles	Being a delicate phase, customer IT support must follow it in order to assess that the overall infrastructure is not impacted by the removal of the system and the is no risk of data breaches.

Table 8-5 System Lifecycle Model (SLCM): Role-Phase activity matrix

The above matrixes have been validated at FPG on a "Clinical Trial" system.

The system is an application currently under ad hoc development, performed by an external supplier, activated via an already existing framework contract.

The application consists in a workflow, connecting several actors and already accessing already existing data bases. For instance, it accesses the patient data base to provide a list of patients to be considered as candidate for enrolment in the clinical trial.

The result of the Instantiation is shown in following Table 8-6. Yellow cells indicate which roles have actually been involved or are planned to be involved.

Roles/Phases	Planning	System Analysis & Requirements	System Design	Development	Integration and Verification	Validation & Deployment	Training	Operations	Maintenance / Upgrade	Information exchange HC Organization-Supplier	Disposal
SUPPLIER SIDE											
Software Developer				X	X	X			X		
Enterprise Architect	X	X	X	X	X	X			X		
Security Architect		X	X	X	X	X			X		
Research & Development Specialist	X	X	X	X							
Systems Requirements Planner		X			X	X					
System Testing and Evaluation Specialist					X	X			X		
Systems Developer				X	X	X			X		
Data Analyst		X	X	X						X	
Technical Support Specialist						X		X	X		X
Network Operations Specialist			X		X	X		X			X
Legal Advisor	X					X			X		X
Privacy Officer/Privacy Compliance Manager		X				X				X	
Program Manager	X										X
IT Project Manager	X	X	X	X	X	X	X		X	X	X
Product Support Manager								X	X	X	X
Product Instructor							X				
Product Instructional Curriculum Developer							X				
HC ORGANIZATION SIDE											
Managers											
Health services Managers	X	x	X	X	X	X		X			
Health Roles											
Generalist Medical Practitioners		X				X	X				
Specialist Medical Practitioners		X				X	X	X			
Nurses		X				X	X	X			
Paramedical practitioners		X				X	X	X			
Medical and Pharmaceutical Technicians		X				X	X				
Ambulance Workers		X				X	X				
Personal care workers in Health Services		X				X	X				
Other Health roles		X				X	X				
Non-health Roles											
Technical roles		X				X	X				
Administrative back-office roles		X					X	X			
Administrative front-office roles											
Medical Secretaries		X				X	X				
Information and Communications Technology roles	X	X	X	X	X	X	X	X	X	X	X
Other non-health roles		X				X	X				
Privacy Officer/Privacy Compliance Manager	x										
Program Manager											
IT Project Manager staff	x	x	x			x				x	x
External roles											
Patients											

Table 8-6 Roles vs System Lifecycle Phases, Instantiation on a Clinical Trial Application

Previously depicted instantiations will be useful in PANACEA to identify possible areas of introduction of cyber vulnerabilities during the system lifecycle, and, as consequence on which phase and roles, focus the development of technical and non-technical measures.

9. Cybersecurity for Healthcare Model (CSHCM)

The CSHCM (Cybersecurity for Healthcare Model) describes the sub-system of a healthcare organization dedicated to take care of the cybersecurity of the organization itself. It is composed of **four Entities[16], four related Catalogues and six Relationships** as shown in following Figure 9-1. The model is also complemented by **four instantiation schemes**, described in Section 9.3.

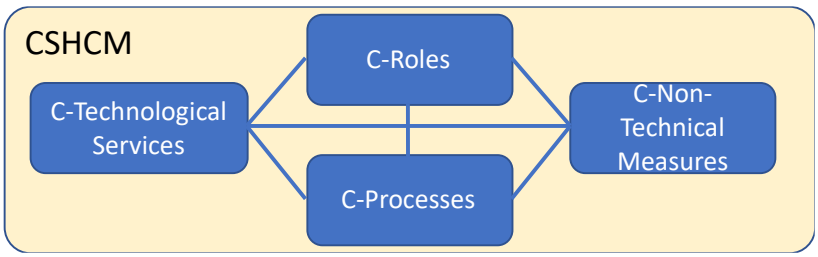

Figure 9-1 Cybersecurity for Healthcare Model (CSHCM): Entities, Catalogues and Relationships

9.1 Entities and Catalogues

9.1.1 C-Technological Services

C-Technological services Entity represents the technology elements (software and hardware) which can be used to ensure cybersecurity, both in the healthcare delivery processes and in lifecycles of Medical Devices and Systems.

C-Technological services Catalogue has been built aiming at setting up a **cybersecurity solutions portfolio**. The method to find out an exhaustive list of technological solutions for cybersecurity has been based on the concept of the Cyber Defence Matrix, created by the OWASP-Open Web Application Security Project (see [OWASP] and [PDIL]).

The Cyber Defense Matrix, as shown in Table 9-1, has two dimensions. The first dimension captures the five operational functions of the NIST Cybersecurity Framework ([NIST]). The second dimension captures the categories of assets that we try to secure.

	NIST Functions				
Asset categories	**IDENTIFY**	**PROTECT**	**DETECT**	**RESPOND**	**RECOVER**
Devices					
Applications					
Networks					
Data					
Users					

[16] the letter "C" stands for "Cybersecurity", to distinguish the entities from the HCOM ones

Table 9-1 Structure of the Cyber Defense Matrix (source: [OWASP])

OWASP used the matrix for vendor analysis, putting at the crosses of the two dimensions the cybersecurity products of the vendors (see [PDIL]).

In Panacea, we contextualized the Defense Matrix by adopting as second dimension (asset categories) the Technological Services classes defined in HCOM (Table 6-2), plus users and vendors/suppliers.

Then, we used the **Cyber Defense Matrix** as an exploratory tool to build a "**Cybersecurity Portfolio of Technological solutions**".

The result is the Matrix shown in Table 10-1, which leverages on the 42 Technology Services listed and described in Table 9-2 below (in alphabetical order). Each of the Technology Service in Table 9-2 is provided by a description and a reference source. In several cases, the source is based on the experience of the PANACEA Consortium collaborating to this deliverable.

#	Cyber-Technology Service	Definition	Source
1	Anti-Virus System (AV)	Defend against know signatures of virus, malware, and suspicious network activity	PANACEA Consortium, [NIST]
2	Application tampering detection System	Detection of application tampering	PANACEA Consortium, [NIST]
3	Audit trail System	Enables replay of events on a timeline, helps investigations	PANACEA Consortium, [NIST]
4	Authentication services	Provision authentication for connected devices	PANACEA Consortium, [NIST]
5	Configuration and systems management	Provision/configure desktops, servers or mobile devices, and then manage the change of configuration settings, software, and increasingly the files and data on those elements on an ongoing basis.	https://www.gartner.com/it-glossary/cm-configuration-management/
6	Data encryption System	Encryption of data to ensure confidentiality	PANACEA Consortium, [NIST]
7	Data loss prevention System (DLP)	Designed to detect and prevent violations to corporate policies regarding the use, storage, and transmission of sensitive data	https://www.optiv.com/cybersecurity-dictionary/dlp
8	Data monitoring System	Monitor data to detect unauthorized access either directly or laterally.	PANACEA Consortium, [NIST]
9	Data recovery System (backup/restore)	Details the backup plan, backup software can be employed for this. Restore functionality needs to be taken into account separately	PANACEA Consortium, [NIST]
10	Device authentication System	After device identification, the device authentication applies trust rules to provide authentication levels that govern device accessibility within the cyber-infrastructure	PANACEA Consortium, [NIST DI]
11	Device blacklisting System	Blacklist devices based on a signature (e.g. MAC, SN, vendor, etc)	PANACEA Consortium, [NIST DI]
12	Device identification System	Provision the identification of devices as they are connecting to the network, Multiple levels as trust can apply	PANACEA Consortium, [NIST DI]

#	Cyber-Technology Service	Definition	Source
13	Dynamic Application Security Testing System (DAST)	Detect conditions indicative of a security vulnerability in an application in its running state. Most DAST solutions test only the exposed HTTP and HTML interfaces of Web-enabled applications; however, some solutions are designed specifically for non-Web protocol and data malformation (for example, remote procedure call, Session Initiation Protocol [SIP] and so on).	https://www.gartner.com/it-glossary/dynamic-application-security-testing-dast/
14	Endpoint control System	Detection of devices at the point of connection, e.g. USB devices, network plugin	PANACEA Consortium, [NIST]
15	Factory reset System	Reset the device to the original factory settings, this might introduce different issues though	PANACEA Consortium, [NIST]
16	Firewall System (FW)	A firewall can screen and keep out unwanted network traffic and ward off outside intrusion into a private network.	https://www.gartner.com/it-glossary/firewall/
17	Firmware reset System	In case of device compromise reset the control chip to a trusted firmware	PANACEA Consortium, [NIST]
18	Full Packet Capture System (PCAP)	Network Packet capture	PANACEA Consortium, [NIST]
19	Host Intrusion Prevention System (HISP)	monitors a single host for suspicious activity by analysing events occurring within that host	https://blog.malwarebytes.com/101/2013/05/whatiships/
20	Identification and authentication System	Provision for user identification and authentication	PANACEA Consortium, [NIST]
21	Identity and access management System (IAM)	IAM addresses the mission-critical need to ensure appropriate access to resources across increasingly heterogeneous technology environments, and to meet increasingly rigorous compliance requirements.	https://www.gartner.com/it-glossary/identity-and-access-management-iam/
22	Image recovery System	Recover a desktop device by reverting to a previously stored save image	PANACEA Consortium, [NIST]
23	Incident management System	Incident management system that allows coordination on ongoing cyber threats in an effort to provide a consolidated and promptly response	PANACEA Consortium, [NIST]
24	Interactive Application Security Testing System (IAST)	Instruments the application binary which can enable both DAST-like confirmation of exploit success and SAST-like coverage of the application code. In some cases, IAST allows security testing as part of general application testing process which provides significant benefits to DevOps approaches.	https://www.optiv.com/cybersecurity-dictionary/iast
25	Intrusion Detection System (IDS)	a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered	https://searchsecurity.techtarget.com/definition/intrusion-detection-system
26	Intrusion Prevention System (IPS)	A network security/threat prevention technology that examines network traffic flows to detect and prevent vulnerability exploits.	https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips
27	Netflow System	Collect and record IP traffic	PANACEA Consortium, [NIST]
28	Physical Access behavioural analytics System	Analytics to gain information to spot suspicious patterns in user physical access requests	PANACEA Consortium, [NIST]

#	Cyber-Technology Service	Definition	Source
29	Physical access control system	System that relies on the user identification system to authenticate or deny physical access requests (e.g. door, gate, etc)	PANACEA Consortium, [NIST]
30	Risk Assessment System (RAS)	A system that follows standardized risk assessment methodologies to support an expert into performing a risk assessment.	PANACEA Consortium, [NIST]
31	Runtime Application Self-Protection Service (RASP)	Built right into an application, or added into an application's runtime environment or underlying operating system. By instrumenting an application's code from this position, RASP is capable of monitoring application behaviour while it is running and can take real-time actions to minimize malicious exploits.	https://www.optiv.com/cybersecurity-dictionary/rasp
32	Secure Remote Access System (SRA)	Secure Remote Access (SRA) allows users to remotely access restricted network resources via a secure and authenticated pathway by encrypting all network traffic and giving the appearance that the user is on the local network, regardless of geographic location.	http://www.vads.com/integrated-ict-services/managed-ict/secure-remote-access-sra/
33	Security By Design Assessment System (SDAS)	Tool to support security engineering by assessing the applicability of security requirements on a software system that is still under development or already deployed.	PANACEA Consortium, [NIST]
34	Static Application Security Testing System (SAST)	Analyse application source code, byte code and binaries for coding and design conditions that are indicative of security vulnerabilities.	https://www.gartner.com/it-glossary/static-application-security-testing-sast/
35	Structural vulnerability assessment System	assessment of the current or future cyber infrastructure	PANACEA Consortium, [NIST]
36	Threat analysis System	dynamic or static threat analysis	PANACEA Consortium, [NIST]
37	Threat detection System	Detect devices that are blacklisted and isolate	PANACEA Consortium, [NIST]
38	User behavioural analytics System	Analytics to gain information to spot suspicious patterns in user access requests to resource	PANACEA Consortium, [NIST]
39	User identification system	System that identifies users based on e.g. identity card, physical attributes or pin code	PANACEA Consortium, [NIST]
40	Video surveillance System	Video surveillance in support of physical security	PANACEA Consortium, [NIST]
41	Web application firewall System (WAF)	An application firewall for HTTP applications. It applies a set of rules to an HTTP conversation. Generally, these rules cover common attacks such as cross-site scripting (XSS) and SQL injection.	https://www.owasp.org/index.php/Web_Application_Firewall
42	Web fraud detection System	Detection of web fraud detection	PANACEA Consortium, [NIST]

Table 9-2 Cybersecurity for Healthcare Model (CSHCM): C-Technology Services catalogue

9.1.2 C-Non-technical measures

C-Non-technical measures Entity represents all the non-technological measures which can be used to mitigate security risks, both in the healthcare delivery processes and in lifecycles of Medical Devices and Systems. In addition to typical organizational measures (e.g. training), they also include procedures for performing technical activities (e.g. data labelling, phishing simulations).

C-Non-technical measures Catalogue includes a large set of non-technical security measures, encompassing procedures, governance actions and training.

The Non-technical measures identified in CSHCM represent a set of means to reduce potential cybersecurity risks.

The method to find out an exhaustive list of Non-technical measures for cybersecurity has been based on two main sources:

- Frameworks, regulation, standards evaluating the cybersecurity capacity of organizations and/or recommending best practices for implementing cybersecurity and effective governance (ISO/IEC 27001:2013, ISO 31000:2018, NIST SP 800-53 rev.4, GDPR, COBIT5))
- Consortium members experience (AON for Insurance Schemes, UNAN for “Nudging” guidelines)

Table 9-3 and Table 9-4 below provide the Catalogue, relevant sources and details:

Security measure class	Security measure type
Governance	Governance priorities
Training and/or education packages	Initial learning interventions
	Refresher learning interventions
	Performance support systems
“Nudging” guidelines	Identify the behaviors you wish staff to exhibit to protect against the 5 currently most common cyberattacks
	Method to detect problematic behaviors or lack of security behaviors within each team/group
	Security Behavior and Barriers Workshop
	Nudge workshops
	Develop procedural intervention
	Implement and monitor effectiveness
Insurance schemes	First Party coverage (about the insured's own damage)
	Third Party coverage (third party liability protection, such as clients or partners)
Communication plans	Media Communication plan (for reputation & Brand)
	GDPR related communication plan
	Establish cyber threat information sharing with other health care organizations
Security Risk Management Plan	Security Risk life cycle plan: Security Role and Responsibility Plan
	Risk Mitigation Plan
Standard Operating Procedures	Event classification and Cyber Security Incident Management
Technical processes	Data labeling
	Phishing Simulations

and/or procedures	Phishing Awareness
	Applicable (data) legislation
	Device eradication
	Account block
	Investigation
	Outsourced monitoring

Table 9-3 Cybersecurity for Healthcare Model (CSHCM): C-Non-Technical Measures catalogue

Security Measure Class	Type	Description	Reference
Governance	Governance priorities	Assessment of the Information Security Management System (ISMS) below the Cyber Security Governance (for more details **see Table on Governance Measures**)	COBIT5, NIST SP 800-53 rev.4, ISO/IEC 27001:2013
Training and/or education packages	Initial learning interventions	Learning content, assessments and delivery methods designed specifically for each target audience (may include online learning).	ISO/IEC 27001:2013, NIST SP 800-53 rev.4
	Refresher learning interventions	Delivered periodically, based on analysis of knowledge and skill fade, following initial learning intervention (likely to include online learning)	
	Performance support systems	Support mechanisms in the workplace which routinely remind and guide on CS threats and processes	
"Nudging" guidelines	Identify the behaviors you wish staff to exhibit to protect against the 5 currently most common cyberattacks	Be aware of the behaviors you wish different staff groups to adhere to and ensure that this is a) clear in the ISP b) being followed.	Consortium members experience (UNAN)
	Method to detect problematic behaviors or lack of security behaviors within each team/group	Identify meaningful groupings of people with similar roles and access to data and devices to baseline behaviors and identify problematic behaviors. Involve staff in identifying current behavior levels to identify behaviors which are falling behind. All staff should be included as they will all have some cybersecurity behaviors they are expected to exhibit.	
	Security Behavior and Barriers Workshop	Involve staff in understand what is influencing insecure behaviors. Work with staff groupings to identify local "influencers" of behaviors using the MINDSPACE framework	
	Nudge workshops	Involve staff in identifying possible nudges/interventions to remove these barriers and facilitate secure behaviors	
	Develop preferred intervention	For example: Tagging external e-mails to make them recognizable to staff may make staff think before responding to a phishing email.	
	Implement and monitor effectiveness	Any changes should be monitored for effectiveness	
Insurance schemes	First Party coverage (about the insured's own damage)	Support and cover direct costs of IT's operational recovery.	Consortium members experience (AON)
		Support and cover cost of Forensic Analysis post Incident	
		Support and cover cost of Media Communication issues related to the company Brand and notifications to the customers.	

	Third Party coverage (third party liability protection, such as clients or partners)	Communication Costs of the GDPR obligations.	
Communication plans	Media Communication plan (for reputation & Brand)	Media channel costs and services in order to mitigate reputational and brand issues	GDPR, NIST SP 800-53 rev.4, ISO/IEC 27001:2013
	GDPR related communication plan	Support and cover cost GDPR related communication to perform to the government and thirty parts (Customers Notifications)	
	Establish cyber threat information sharing with other health care organizations	Share up to data information about any attempted attacks	
Security Risk Management Plan	Security Risk life cycle plan: Security Role and Responsibility Plan	Internal and external (consulting service) Audit of Security Governance and Policy implementation checks	NIST SP 800-53 rev.4, ISO/IEC 27001:2013, ISO 31000:2018
		Periodic Security Awareness Campaign/Assessment (es. phishing campaign, etc.)	
		Periodic Cyber Risk Assessment	
		Periodic Vulnerability and Penetration testing	
	Risk Mitigation Plan	Patching management plan (Priority, time, costs of patch implementation)	
		Security Policy updating	
		Security Best practices implementation plan or upgrade	
Standard Operating Procedures	Event classification and Cyber Security Incident Management	Security operation center procedure	ISO/IEC 27001:2013, NIST 800-53 rev.4
		Identification and management flow of anomalies	
		Escalation plan	
		Action plan and mitigation procedures.	
Technical processes and/or procedures	Data labeling	Labels or tags that detail the data in such a way that classification, data search and data categorization can be automated	ISO/IEC 27001:2013, NIST 800-53 rev.4
	Phishing Simulations	Run simulation on users to determine vulnerability and raise awareness	
	Phishing Awareness	Increase awareness of phishing attacks, in doing so protecting the cyber infrastructure	
	Applicable (data) legislation	Legislative framework applicable to the cyber domain, it will govern amongst other things the level of deployable detection and response measures	
	Device eradication	Once a device is compromised beyond recovery it needs to be redacted in a safe way	
	Account block	Block user accounts, this can be a centralized system or part of Identity management	
	Investigation	Investigative team employing a plethora of tools to investigate a cyber incident after the fact.	
	Outsourced monitoring	Rely on vendor monitoring of provided services	

Table 9-4 Cybersecurity for Healthcare Model (CSHCM): C-Non-Technical Measures catalogue, with descriptions and sources

The following Table 9-5 provides more details on the Governance measures, relating them to the relevant NIST Function. Table 9-5 provides details on the controls from COBIT, ISO/IEC and NIST.

NIST FUNCTIONS	#	Governance Measures	Classification	COBIT 5	ISO/IEC 27001:2013	NIST SP 800-53 Rev. 4
IDENTIFY	1	Roles and responsibilities regarding cybersecurity risk management are defined and made known for all personnel and for relevant third parties (e.g. supplier, customers, partners)	Governance risks	APO01.02, DSS06.03	A.6.1.1	CP-2, PS-7, PM-11
	2	Data security policies are identified, approved by management, published end communicated to internal and external parties	Governance risks	APO01.03, EDM01.01, EDM01.02	A.5.1.1	1 controls from all families
	3	Legal requirements for cybersecurity & privacy are identified, documented and kept up to date	Governance risks	MEA03.01, MEA03.04	A.18.1	1 controls from all families (except PM-1)
	4	Governance and risk management processes include the management of cybersecurity risks	Governance risks	DSS04.02		PM-9, PM-11
	5	Cyber threats, both internal and external, are identified, analysed and reported	Governance risks	APO12.01, APO12.02, APO12.03, APO12.04		RA-3, SI-5, PM-12, PM-16
	6	Cyber risk responses are identified and prioritised	Governance risks	APO12.05, APO13.02		PM-4, PM-9
	7	Cyber risk tolerance, acceptable cyber risk assessment methodologies, cyber risk mitigation strategies are clearly identified and expressed	Governance risks	APO12.06		PM-9
PROTECT	8	Physical access to sensitive information data is protected and authorization credentials are identified	Governance risks	DSS01.04, DSS05.05	A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3	PE-2, PE-3, PE-4, PE-5, PE-6, PE-9
	9	All cybersecurity related employees of the organization received appropriate awareness education and training and regular updates in cybersecurity policies and procedures	Governance risks	APO07.03, BAI05.07	A.7.2.2	AT-2, PM-13
	10	Competences of cybersecurity related personnel are regularly verified	Governance risks	APO07.02, DSS06.03	A.6.1.1, A.7.2.2	AT-3, PM-13
	11	Incident Response, Incident Recovery and Disaster Recovery plans are designed and managed in the event of cyberattacks	Governance risks	DSS04.03	A.16.1.1, A.17.1.1, A.17.1.2	CP-2, IR-8
	12	Response and recovery plans following cyberattacks are verified over time	Governance risks		A.17.1.3	CP-4, IR-3, PM-14
	13	Cybersecurity policies are included in personnel management processes (e.g. screening, layoff)	Governance risks	APO07.01, APO07.02, APO07.03, APO07.04, APO07.05	A.7.1.1, A.7.3.1, A.8.1.4	PS Family
DETECT	14	Criteria and procedures to report cybersecurity problems are identified and implemented	Governance risks	DSS03.01		AC-4, CA-3, CM-2, SI-4

NIST FUNCTIONS	#	Governance Measures	Classification	COBIT 5	ISO/IEC 27001:2013	NIST SP 800-53 Rev. 4
	15	Preventive, detective and corrective measures are implemented and maintained in place through a continuous monitoring process	Governance risks	DSS05.01	A.6.1.1	CA-2, CA-7, PM-14
	16	Cybersecurity monitoring processes are verified and improved over time	Governance risks	APO11.06, DSS04.05	A.16.1.6	CA-2, CA-7, PL-2, RA-5, SI-4, PM-14
	17	Cybersecurity management responsibilities and procedures are identified to ensure a quick and effective response to information security incidents	Governance risks		A.6.1.1, A.16.1.1	CP-2, CP-3, IR-3, IR-8
	18	Information security events are reported through appropriate management channels	Governance risks	APO12.06	A.16.1.2	AU-6, CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4
RESPOND	19	Cybersecurity coordination within the organisation is consistent with the response plans	Governance risks			CP-2, IR-4, IR-8
	20	Roles and responsibilities regarding cybersecurity in response to information security incidents are defined	Governance risks		A.6.1.1, A.16.1.1	CP-2, CP-3, IR-3, IR-8
	21	Information security incidents are resolved in accordance with documented procedures	Governance risks		A.16.1.5	IR-4
	22	Information security incidents are resolved through detection prevention and recovery plans to reduce the likelihood or impact of future incidents	Governance risks		A.12.2.1, A.16.1.5	IR-4
RECOVER	23	Contingency planning and cyber incident response are identified and updated	Governance risks			CP-2, IR-4, IR-8
	24	Incident recovery activities are communicated to interested parties within the organisation	Governance risks			CP-2, IR-4

Table 9-5 Cybersecurity for Healthcare Model (CSHCM): C-Non-Technical Measures catalogue: focus on Governance measures

9.1.3 C-Processes

C-Processes Entity represents all the activities that should be executed by an organization to ensure proper cybersecurity management. Making reference to the NIST framework (see [NIST], they include the NIST categories, which are the breakdown of the NIST functions (Identify, Protect, Detect, Respond and Recover).

C-Processes Catalogue is derived from the NIST framework (see [NIST]). CSHCM Processes correspond to NIST *categories* (they have been renamed for consistency with the HCM). See Table 9-6 below.

CSHCM Functions	#	CSHCM Processes	Description
IDENTIFY **Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities: inventorying assets**	1	Asset Management	The data, personnel, devices and systems and facilities required by the organisation are identified and managed in accordance with the organisation's business objectives and risk strategy
	2	Business Environment Assessment	The organisation's mission, objectives, activities and actors involved are understood and evaluated in terms of priorities. This

CSHCM Functions	#	CSHCM Processes	Description
and vulnerabilities, measuring attack surface, risk profiling			information influences cybersecurity roles, responsibilities and cyber risk management.
	3	Governance	Cybersecurity policies and procedures shall be identified.
	4	Risk Assessment	The organisation understands the cyber risk inherent in the operations (including mission, functions, image or reputation), assets and individuals, including risks associated to the supply chain
	5	Risk Management Strategy	The organization's priorities and requirements and risk tolerance are defined and used to support cyber risk decisions. The scope of the strategy also include the supply chain
PROTECT **Develop and implement appropriate safeguards to ensure delivery of critical services: preventing or limiting impact, patching, containing, isolating, hardening, managing access, vulnerability remediation**	6	Access Control	Access to cybersecurity assets and related resources is limited to personnel, processes, devices, activities and transactions actually authorized
	7	Awareness and Training	Personnel and third parties are educated and trained on cybersecurity and receive adequate preparation, consistent with policies, procedures and agreements.
	8	Data Security	Data is stored and managed in accordance with the organisation's cyber risk management strategy to ensure the integrity, confidentiality and availability of the information.
	9	Information Protection Processes and Procedures implementation	Cybersecurity policies are implemented and adapted over time (which address the purpose, scope, roles and responsibilities, commitment on the part of the management and coordination between the different parties)
	10	Maintenance	Maintenance of information control systems shall be carried out in accordance with existing policies and procedures
	11	Protective Technology	Technical cybersecurity solutions are managed to ensure the security and resilience of systems and assets, in accordance with the relevant policies, procedures and agreements.
DETECT **Develop and implement appropriate activities to identify the occurrence of a cybersecurity event: discovering events, triggering on anomalies, hunting for intrusions, security analytics**	12	Anomalies and Events	Unexpected cyber activities are detected in a timely manner and their potential impact is analysed
	13	Security Continuous Monitoring	Information systems and assets are periodically monitored to identify cybersecurity events and to verify the effectiveness of protection measures.
	14	Detection Processes	Monitoring processes and procedures shall be adopted, maintained and verified over time to ensure a timely and adequate understanding of security events.
RESPOND **Develop and implement appropriate activities to take action regarding a detected cybersecurity incident: acting on events, eradicating intrusion footholds, assessing damage, coordinating, reconstructing events forensically**	15	Response Planning	Response procedures and processes are executed and maintained to ensure timely response to detected cybersecurity events.
	16	Communications	Response activities are coordinated with internal and external parts, to include possible support from law enforcement agencies or law enforcement agencies.
	17	Analysis	Analyses are conducted to ensure adequate response and support for recovery activities
	18	Mitigation	Response activities are improved by incorporating lesson learned from previous monitoring and response activities
	19	Improvements	Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.
RECOVER **Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident: returning**	20	Recovery Planning	Restoration processes and procedures are executed and maintained to ensure timely recovery of systems or assets involved in a cybersecurity event.
	21	Improvements	Organizational response activities, Restoration plans and related processes have been improved taking into account lessons learned for future activities.

CSHCM Functions	#	CSHCM Processes	Description
to normal operations, restoring services, documenting lessons learned	22	Communications	Incident recovery activities are coordinated with internal and external parties, such as victims, ISPs, owners of attacked systems, vendors, CERT/CSIRTs, etc.

Table 9-6 Cybersecurity for Healthcare Model (CSHCM): C-Processes

9.1.4 C-Roles

C-Roles Entity represents the Actors operating in the C-Processes to ensure cyber security. Even if the organization is accountable for all the processes, the C-Roles also include external providers.

C-Roles Catalogue is based on the NIST National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, which provides a very comprehensive catalogue of roles (see [NICE]).

Roles are divided into 7 categories.

- Security provision
- Operate and Maintain
- Oversee and Govern
- Protect and Defend
- Analyse
- Collect
- Operate
- Investigate

The full list of the 52 Roles is provided in following Table 9-7. Detailed description of each Role is provided in Annex C-Cybersecurity Roles

It is understood that not all roles will be played in an organization by dedicated job positions. Some roles will be combined into one job position, or distributed across different positions; furthermore, some roles may not be applicable.

Category	#	Specialty Area	Work Role
Securely Provision (SP)	**1**	Risk Management (RSK)	Authorizing Official/Designating Representative
	2		Security Control Assessor
	3	Software Development (DEV)	Software Developer
	4		Secure Software Assessor
	5	Systems Architecture (ARC)	Enterprise Architect
	6		Security Architect
	7	Technology R&D (TRD)	Research & Development Specialist
	8	Systems Requirements Planning (SRP)	Systems Requirements Planner
	9	Test and Evaluation (TST)	System Testing and Evaluation Specialist
	10	Systems Development (SYS)	Information Systems Security Developer
	11		Systems Developer
Operate and Maintain (OM)	**12**	Data Administration (DTA)	Database Administrator
	13		Data Analyst

Category	#	Specialty Area	Work Role
	14	Knowledge Management (KMG)	Knowledge Manager
	15	Customer Service and Technical Support (STS)	Technical Support Specialist
	16	Network Services (NET)	Network Operations Specialist
	17	Systems Administration (ADM)	System Administrator
	18	Systems Analysis (ANA)	Systems Security Analyst
Oversee and Govern (OV)	19	Legal Advice and Advocacy (LGA)	Cyber Legal Advisor
	20		Privacy Officer/Privacy Compliance Manager
	21	Training, Education, and Awareness (TEA)	Cyber Instructional Curriculum Developer
	22		Cyber Instructor
	23	Cybersecurity Management (MGT)	Information Systems Security Manager
	24		Communications Security (COMSEC) Manager
	25	Strategic Planning and Policy (SPP)	Cyber Workforce Developer and Manager
	26		Cyber Policy and Strategy Planner
	27	Executive Cyber Leadership (EXL)	Executive Cyber Leadership
	28	Program/Project Management (PMA) and Acquisition	Program Manager
	29		IT Project Manager
	30		Product Support Manager
	31		IT Investment/Portfolio Manager
	32		IT Program Auditor
Protect and Defend (PR)	33	Cyber Defense Analysis (CDA)	Cyber Defense Analyst
	34	Cyber Defense Infrastructure Support (INF)	Cyber Defense Infrastructure Support Specialist
	35	Incident Response (CIR)	Cyber Defense Incident Responder
	36	Vulnerability Assessment and Management (VAM)	Vulnerability Assessment Analyst
Analyze (AN)	37	Threat Analysis (TWA)	Threat/Warning Analyst
	38	Exploitation Analysis (EXP)	Exploitation Analyst
	39	All-Source Analysis (ASA)	All-Source Analyst
	40		Mission Assessment Specialist
	41	Targets (TGT)	Target Developer
	42		Target Network Analyst
	43	Language Analysis (LNG)	Multi-Disciplined Language Analyst
Collect and Operate (CO)	44	Collection Operations (CLO)	All Source-Collection Manager
	45		All Source-Collection Requirements Manager
	46	Cyber Operational Planning (OPL)	Cyber Intel Planner
	47		Cyber Ops Planner
	48		Partner Integration Planner
	49	Cyber Operations (OPS)	Cyber Operator
Investigate (IN)	50	Cyber Investigation (INV)	Cyber Crime Investigator
	51		Law Enforcement /CounterIntelligence Forensics Analyst

Category	#	Specialty Area	Work Role
	52	Digital Forensics (FOR)	Cyber Defense Forensics Analyst

Table 9-7 Cybersecurity for Healthcare Model (CSHCM): C-Roles

9.2 Relationships

CSHCM includes six Entity to Entity relationships.

Following Table 9-8 describes the meaning of each relationship and the key information provided by the instantiation of the relationship:

Entity A	Entity B	Meaning of the relationship between items of A and items of B	What can tell us the instantiation of this relationship
C-Technological Services	C-Roles	an item of B may use (or take care of) one or more items of A	Which Roles may work on which Technological Services
C-Technological Services	C-Non-Technical Measures	an item of B may be used in conjunction with one or more items of A	Which Technological Services may be synergic with which Non-Technical Measure
C-Technological Services	C-Processes	an item of A is used in one or more processes of B	Which Technological Services are used in which Processes
C-Roles	C-Non-Technical Measures	an item of A may use (or take care of) one or more items of B	Which Roles operate to design and deliver which Non-Technical Measure
C-Roles	C-Processes	an item of A contributes to one or more items of B	Which Roles operate in which Processes
C-Non-Technical Measures	C-Processes	an item of A is used in one or more items of B	Which Non-Technical Measure are used in which Processes

Table 9-8 CSHCM- Meaning of the inter-Entity relationships and of the related instantiations

9.3 Instantiation schemes

Four of the possible instantiation schemes for DLCM are provided in following paragraphs

They are indicated in Figure 9-2 (instantiations are numbered; numbers are referenced in next paragraphs, included in brackets [ ]).

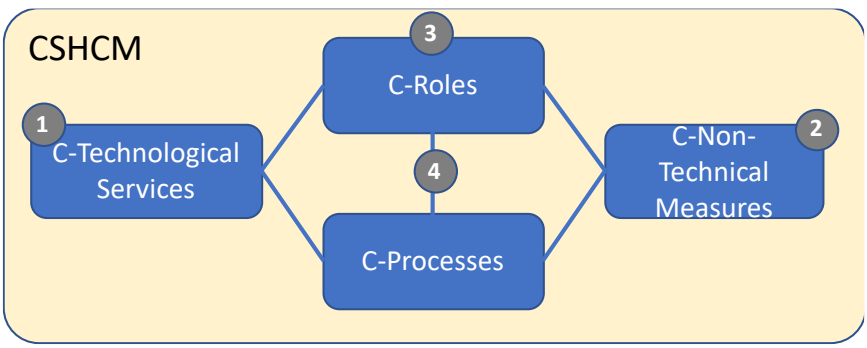

Figure 9-2 Cybersecurity for Healthcare Model (CSHCM): Entities and Instantiation Schemes

9.3.1 C-Technological Services

The instantiation [1] of the C-Technological Services in the context of a specific healthcare organization consists in specifying which of the 42 Cybersecurity Technological Services of the CSHCM catalogue are implemented in full or partially or none on the organization. A colour code may be used to provide immediate visibility of the status: Red (not covered), Yellow (partially covered), Green (covered), as shown in Table 9-9 below in an example.

.

#	Cybersecurity Technological Service	Organization XXX Status (Green=covered; Yellow=Partially covered; Red=Not covered)
1	Anti Virus (AV)	kaspersky
2	Application tampering detection	Application log files
3	Audit trail	no
4	Authentication services	mac authentication on cisco ise
5	Configuration and systems management	cmdb, sdas, data center system as domain controller, sccm
	…	…
17	Full Pack Capture (PCAP)	wireshark, only for troubleshooting

Table 9-9 C-Technological Services_Instantiation Table, Example (adapted from a real case)

9.3.2 C-Non-Technical Measures

The instantiation [2] consists in specifying which of the 36 Cybersecurity Non-Technical Measures of the CSHCM catalogue (Table 9-3) are covered in full or partially or none in the healthcare organization. A colour code may be used to provide immediate visibility of the status: Red (not covered), Yellow (partially covered), Green (covered), as shown below in an example of instantiation, referred to only one class of Non-Technical measures.

Class	Types	Description	Organization XXX Status (Green=covered; Yellow=Partially covered; Red=Not covered)
Standard Operating Procedures	Event classification and Cyber Security Incident Management	Security operation center procedure	In the process of implementing
		Identification and management flow of anomalies	no action taken
		Escalation plan	no action taken
		Action plan and mitigation procedures.	YES

Table 9-10 C-Non-Technical Measures_Instantiation Table, Example (adapted from a real case)

9.3.3 C-Roles

The instantiation [3] consists in specifying which of the 52 Cybersecurity Roles are covered in the healthcare organization in scope.

A percentage scale can be used to indicate the level of coverage of the role by the staff (or suppliers) of the organization in scope

0%	not covered
25%	low actions taken, but no designated role of a specific Staff
50%	some actions taken, but no designated role of a specific Staff
75%	many actions taken, but not to a full extended of this role
100%	all actions taken for this role, designated Staff for this role

See in Table 9-10 below an example of instantiation. It shows some of the rows of the full Instantiation Table, which is made up of 52 rows. The table shows that three work roles of the CSHCM Catalogue are all fully covered, even if there is some dependence on the external supplier: the fact that there is no internal development capability may be a risk.

					Organization XXX Positions playing Cybersecurity roles			
Category	**Specialty Area**	**Work Role Id**	**Work Role**	**Work Role Description**	**IT Staff**	**Application Vendor**	**DPO**	**Manager**
Securely Provision (SP)	Risk Management (RSK)	SP-RSK-001	Authorizing Official/Designating Representative	Senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation (CNSSI 4009).				100%
	Risk Management (RSK)	SP-RSK-002	Security Control Assessor	Conducts independent comprehensive assessments of the management, operational, and technical security controls and control enhancements employed within or inherited by an information technology (IT) system to determine the overall effectiveness of the controls (as defined in NIST SP 800-37).	25%	100%		
	Software Development (DEV)	SP-DEV-001	Software Developer	Develops, creates, maintains, and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs.	0%	100%		

Table 9-11 C-Roles_Instantiation Table_Example , Example (adapted from a real case)

9.3.4 C-Roles and C-Processes

This instantiation [4] integrates the previous ones, supporting a more detailed analysis over the organization. It can be used to more deeply check which activities are actually performed in the organization, going through the NIST Functions.

The instantiation is supported by a map providing the relationship between the Roles (C-Roles) from [NICE] and the [NIST] categories (or CSHCM Processes).

The map crosses the 52 C-Roles (belonging to 7 categories, as explained in Section 9.1.4) with the C-Process (see Section 9.1.3), specifying which Roles are involved in each Process.

To build the map, as first step the relationship between the seven Role Categories and the five NIST functions has been summarized elaborating material form [NICE], in following Table 9-12.

NICE Role Category	NIST Function				
	IDENTIFY (ID)	PROTECT (PR)	DETECT (DE)	RESPOND (RS)	RECOVER (RC)
Security Provision	X	X			
Operate and Maintain		X	X		
Oversee and Govern	X	X	X		X
Protect and Defend		X	X	X	
Analyze	X		X	X	
Collect and Operate		X	X	X	
Investigate			X	X	X

Table 9-12 Relationship between cybersecurity role categories and NIST Functions (source: elaboration of [NICE] content)

To introduce a more meaningful mapping and granularity at the level of 52 C-Roles and 21 C-Processes, the tasks of each role have been taken into account (as part of the NICE role definitions, [NICE]) and mapped onto the C-Process. The result is the matrix shown as Table 9-13below.

In the matrix, the C-Roles are the rows, while the C.Process are the columns. Each process is identified with a number; the corresponding name of the process can be read in Table 9-14.

The matrix shows for each role, in which process operates; this is indicated with a coloured cell. For instance, the Role “Secure Software Assessor” (the forth from the top) is not involved in the processes from 12 to 21; is mainly involved in the Identify and Protect set of processes, apart from processes 3, 5 and 7.

The matrix can be used as a tool to plot the current situation of the hospitals cybersecurity roles expressed in the taxonomy of the NICE cybersecurity workforce and in relationships with the C-Processes.

It allows, for instance, to produce a consistent set of job descriptions (for the internal staff) and contractual agreements with the external security suppliers.

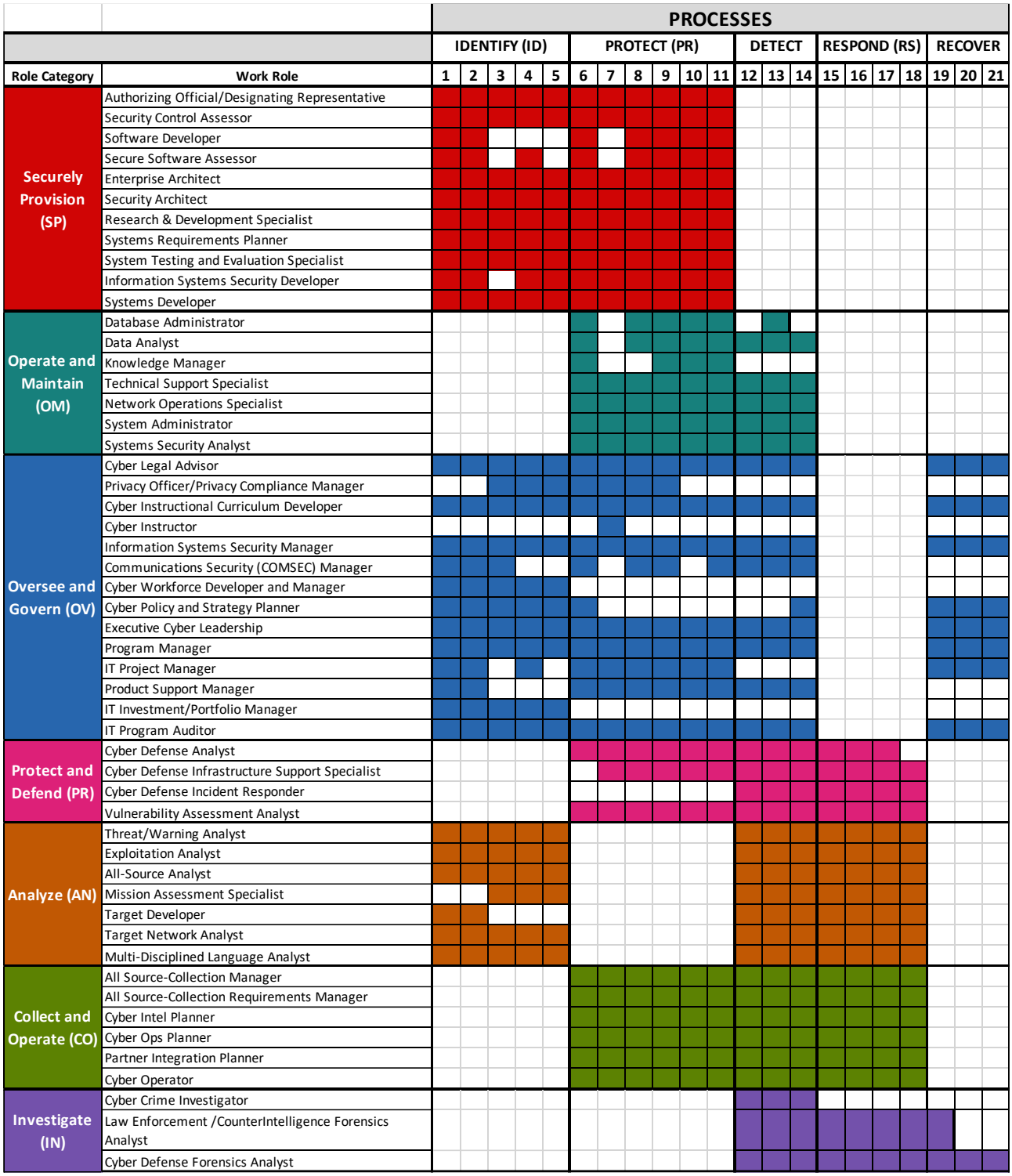

Table 9-13 C-Roles-C-Processes_Matrix Instantiation scheme

NIST FUNCTION	#	C-Processes
IDENTIFY (ID) **Develop an organizational understanding to**	1	Asset Management (ID.AM)
	2	Business Environment (ID.BE)

manage cybersecurity risk to systems, people, assets, data, and capabilities.	3	Governance (ID.GV)
	4	Risk Assessment (ID.RA)
	5	Risk Management Strategy (ID.RM)
PROTECT (PR) **Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.**	6	Identity Management, Authentication and Access Control (PR.AC)
	7	Awareness and Training (PR.AT)
	8	Data Security (PR.DS)
	9	Information Protection Processes and Procedures (PR.IP)
	10	Maintenance (PR.MA)
	11	Protective Technology (PR.PT)
DETECT (DE) **Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.**	12	Anomalies and Events (DE.AE)
	13	Security Continuous Monitoring (DE.CM)
	14	Detection Processes (DE.DP)
RESPOND (RS) **Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.**	15	Response Planning (RS.RP)
	16	Communications (RS.CO)
	17	Analysis (RS.AN)
	18	Mitigation (RS.MI)
RECOVER (RC) **Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.**	19	Recovery Planning (RC.RP)
	20	Improvements (RC.IM)
	21	Communications (RC.CO)

Table 9-14 C-Processes list

10. Cross-models relationships and matrixes

In view of the next Tasks of the Panacea Project, the most important cross-models relationships are the ones between CSHCM and each one of the three other models.

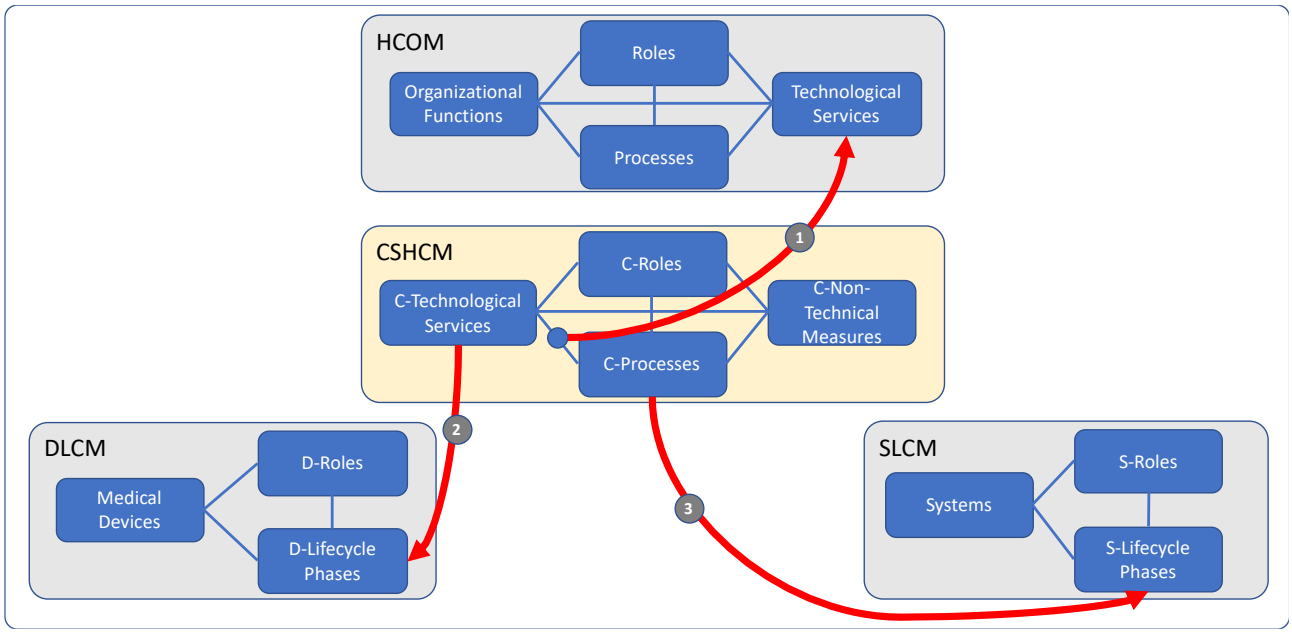

Figure 10-1 Cross-Models Instantiations

In this section the key relationships, shown and numbered in Figure 10-1 above, are described in terms of instantiation schemes

10.1 CSHCM-HCOM

The Instantiation Scheme [1] describes the relationship involving three Entities: Technological Services of HCOM, C-Processes and C-Technological Services of CSHCM. The scheme allows to answer the question: *given a category of assets (e.g. the Data) in a hospital, which type of C-Technological Service should be in place to properly perform processes related to each C-Macroprocess (e.g. Respond)?*

A useful scheme for answering this question is the Defence Matrix already introduced in paragraph 9.1.1.

The Defence Matrix is shown in following Table 10-1.

On left, the first two columns describe the assets to be protected:

- The first column classifies them according a simple taxonomy, used by OWASP, which includes also staff, suppliers (of services) and vendors (of products).
- The second column leverages on the [ENISA] taxonomy.

Remaining columns are the NIST functions, i.e. the C-Processes of CSHCM.

At the cross between rows (the assets) and columns (the Macroprocesses), are positioned the 42 Technology Services listed in Table 9-2.

The meaning of this positioning is that a given technology (e.g. the Intranet Detection System) is used in a given Macroprocess (Respond) to defend a given type of asset (the Networking equipment).

Numbers in the matrix identify the service and it is the same of the C-Technological Services Catalogue

The Matrix can be used to visualise the coverage of an organization's cybersecurity portfolio.

The matrix has already been used by end-users of the Consortium for describing their coverage.

<table>
<tr><th colspan="2" rowspan="2">ASSETS</th><th colspan="6">NIST Cybersecurity Framework Functions - CSHCM Macroprocesses</th></tr>
<tr><th colspan="5">Structural Awareness</th><th>Situational Awareness</th></tr>
<tr><th>Asset categories</th><th>ENISA asset types</th><th colspan="3">IDENTIFY (ID)</th><th colspan="2">PROTECT (PR)</th><th>DETECT (DE)</th><th>RESPOND (RS)</th><th>RECOVER (RC)</th></tr>
<tr><td rowspan="5">Devices</td><td>Networked medical devices (e.g. IOMT)</td><td rowspan="11">30. Risk Assessment System (RAS)</td><td rowspan="6">5. Configuration and systems management System</td><td rowspan="4">12. Device identification System</td><td rowspan="11">21 Identity and access management System (IAM)

32 Secure Remote Access System (SRA)</td><td></td><td rowspan="5">14 Endpoint control System
37 Threat detection System</td><td rowspan="5">11 Device blacklisting System</td><td>17 Firmware reset System</td></tr>
<tr><td>Identification systems</td><td>19. Host Intrusion Prevention System (HISP)</td><td></td></tr>
<tr><td>Desktop and mobile devices</td><td>1. Anti Virus System (AV)</td><td>22 Image recovery System</td></tr>
<tr><td>Mobile Client devices (BYOD)</td><td></td><td>15 Factory reset System</td></tr>
<tr><td>Remote care system assets</td><td>36 Threat analysis System
35 Structural vulnerability assessment System
10 Device authentication System</td><td>17 Firmware reset System</td></tr>
<tr><td>Applications</td><td>Interconnected information systems</td><td>33. Security By Design Assessment System (SDAS)</td><td>34 Static Application Security Testing System(SAST)
13 Dynamic Application Security Testing System (DAST)
24 Interactive Application Security Testing System (IAST)
31 Runtime Application Self-Protection Service(RASP)
41 Web application firewall System (WAF)</td><td>42 Web fraud detection System</td><td>23 Incident management System</td><td></td></tr>
<tr><td>Networks</td><td>Networking equipment</td><td>27. NetFlow System</td><td>16 Firewall (FW)
26 Intrusion Prevention System (IPS)</td><td>25 Intrusion Detection System (IDS)</td><td>18 Full Pack Capture System (PCAP)</td><td></td></tr>
<tr><td>Data</td><td>Data</td><td colspan="2"></td><td>6 Data encryption System
7 Data loss prevention System (DLP)</td><td>8 Data monitoring System</td><td></td><td>9 Data recovery System (backup /restore)</td></tr>
<tr><td>Users</td><td>Identification systems</td><td colspan="2">20. Identification and</td><td>3 Audit trail System</td><td>38 User behavioral</td><td></td><td></td></tr>
</table>

			authentication System Phishing Simulations			analytics System		
infrastructure	Building and facilities		39. User identification system	29. Physical access control system		28 Physical Access behavioural analytics System 40 Video surveillance System		
Vendors (product suppliers) Service suppliers	Interconnected information systems		4. Authentication services					

Table 10-1 CSHCM-HCOM_Defence Matrix

10.2 CSHCM-DLCM

There are many possible relationships between the CSHCM and the DLCM.

Considering that Panacea project will look for solutions to manage the Medical Device identification, an important link is between the **Device Identification technologies** of the **Cybersecurity Technology Services** list (items 10, 11, 12, 17: see paragraph 9.1.1) and the **phases of the life of a Medical Device**.

The relationship is based on two concepts:

- There are two types of identification solutions: Tamper proof ID, Software ID;
- The identification solution is born from the start of the Medical Device lifecycle and the management of the solution varies according three “stages”.

Figure below shows where the three stages of the identification solution position themselves with respect to the Medical Device Lifecycle.

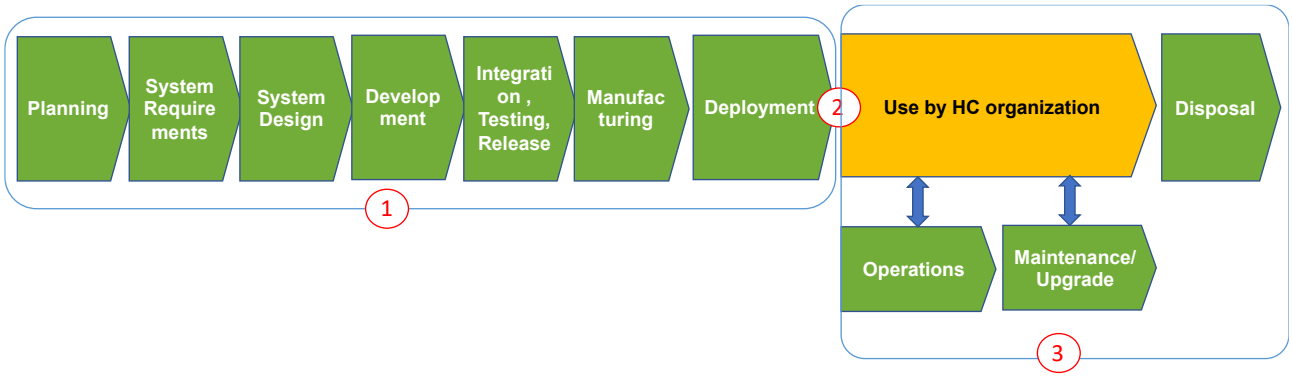

Figure 10-2 CSHC-DLCM: stages of the identification solution

The activities per stage and per type of solution are described in following table.

Identification solution	Stage 1	Stage 2	Stage 3
Tamper proof ID	The personalization of the secure element of the device could be the following: • During the System on Chip (SoC) design step, an ID and/or Crypto keys are personalized via Trusted Provisioning service, held by the SoC Manufacturing or by a third parties. The SoC is locked and protected. It cannot be personalized without access of the Trusted Service. • During the SoC Manufacturing, the chip is identified and unlocked by the Trusted Provisioning Service only, • During the device manufacturing, the device is identified and personalized via the Secure ID of the secure element, thanks to the Trusted Provisioning Service.	The HC provider enrolls the device as secure device and manages API (Application Programming Interface) to manage the secure devices through external secure server management if the device is personal, part of the deployment phase includes personalization; when a device is used for multiple patients (one after the other), the device is re-deployed and thus re-personalized.	In the field, the device is used (including standard usage, maintenance and upgrade) via the Trusted Provisioning Service. This means that the device can be used in the connected hospital, because it is identified as a trusted device. All actions as maintenance, upgrade … can only be authorized / controlled by the Trusted Provisioning service The Trusted Provisioning Services could be located • in an external Trusted area (e.g. owned by the security service provider) and accessed through the Cybersecurity area of the hospital • Or within the hospital
Software ID	In this case, there is no secured component, but the software used in the device is personalized with an unique ID and with Crypto keys. Each device is unique and identified by his unique ID. The data provisioning is secured by the Crypto Keys, used for authentication, data transfer … Theses keys could be transferred to Hospitals Admin and/or kept into Trusted Provisioning Service.	The manufacturer transfers security keys to the HC provider IT Dept and put in place Keys Management System to authenticate the device and track operations. Mitigate the risk by strengthening keys protection through the hospital IT system	All actions as maintenance, upgrade … can be managed by the Keys Management System hosted in hospital, or also by a Trusted Provisioning service. Mitigate the risk by strengthening keys protection through the hospital IT system

Table 10-2 CSHCM-DLCM_activities per stage and per type of identification solution

10.3 CSHCM-SLCM

A relationship between CSHCM and SLCM consists in the link between the Phases of the System Lifecycle and the Cybersecurity functions (taken from the NIST framework). The link identifies which functions from the NIST Framework *could* be involved (from the perspective of the healthcare organization and the system supplier) during the life-time of a complex system as described in Section 8.

This link is described in Table 10-4.

The connections are consistent with following sources:

- Security and Privacy Controls for Federal Information Systems and Organizations SP 800-53, [NIST SP]
- NIST Cybersecurity Framework, [NIST]

The connections have been identified starting from SP 800-53, where controls relevant for the Information Systems security are clearly identified and clearly associated in a table to the NIST Sub-categories. An excerpt of this table is shown in Table 10-3 below.

Function	Category	Subcategory	All SP 800-53 Controls
Protect	**Information Protection Processes and Procedures (PR.IP):** Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained	CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10
		PR.IP-2: A System Development Life Cycle to manage systems is implemented	PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, SI-12, SI-13, SI-14, SI-16, SI-17
		PR.IP-3: Configuration change control processes are in place	CM-3, CM-4, SA-10
		PR.IP-4: Backups of information are conducted, maintained, and tested periodically	CP-4, CP-6, CP-9
		PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	PE-10, PE-12, PE-13, PE-14, PE-15, PE-18
		PR.IP-6: Data is destroyed according to policy	MP-6
		PR.IP-7: Protection processes are continuously improved	CA-2, CA-7, CP-2, IR-8, PL-2, PM-6
		PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties	AC-21, CA-7, SI-4
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	CP-2, CP-7, CP-12, CP-13, IR-7, IR-8, IR-9, PE-17
		PR.IP-10: Response and recovery plans are tested	CP-4, IR-3, PM-14
		PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21

Function	Category	Subcategory	All SP 800-53 Controls
		PR.IP-12: A vulnerability management plan is developed and implemented	RA-3, RA-5, SI-2

Table 10-3 Extract from [NIST SP]: relationship between NIST functions and NIST security controls

For instance, NIST sub-category "*PR.IP-2: A System Development Life Cycle to manage systems is implemented"* (part of category "*Information Protection Processes and Procedure*"s) is linked to the following SP 800-53 security controls

PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, SI-12, SI-13, SI-14, SI-16, SI-17.

In the SP 800-53 aforementioned controls are not explicitly associated to the lifecycle phases. Therefore, they have been analysed to find their conceptual relationship with the system development life-cycle in different phases.

For instance, the SA-4 control (which is one of the controls related to the NIST category*" Information Protection Processes and Procedures*," corresponding to CSHCM process with the same name) states (see [NIST SP]):

> *The organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs:*
>
> - *Security functional **requirements**;*
> - *Security strength **requirements**;*
> - *Security assurance **requirements**;*
> - *Security-related documentation **requirements**;*
> - ***Requirements** for protecting security-related documentation;*
> - *Description of the information system development environment and environment in which the system is intended to operate; and*
> - *Acceptance criteria*

This shows that there is a link between the "*System Analysis & Requirements*" phase of the lifecycle and the "*Information Protection Processes and Procedures*" process.

The same operation has been performed with all other SP 800-53 security controls, in order to find the ones with a logic relationship to one or more phases of the system development life-cycle and hence find the link from the phases to the NIST categories and, therefore, to the CSHCM processes.

Lifecycle Phases → CSHCM Processes ↓	Planning	System Analysis & Requirements	System Design	Development	Integration & Verification	Deployment & Validation	Training	Operations	Maintenance / Upgrade	Information exchange HC Organization-Supplier	Disposal
Asset Management		**X**	**X**					**X**			

Lifecycle Phases → CSHCM Processes ↓	Planning	System Analysis & Requirements	System Design	Development	Integration & Verification	Deployment & Validation	Training	Operations	Maintenance / Upgrade	Information exchange HC Organization-Supplier	Disposal
Business Environment Assessment	X	X									
Governance		X				X					
Risk Assessment		X	X			X		X			
Risk Management Strategy											
Access Control								X			
Awareness and Training							X				
Data Security								X		X	
Information Protection Processes and Procedures	X	X	X	X	X	X					X
Maintenance									X		
Protective Technology								X			
Anomalies and Events								X			
Security Continuous Monitoring								X			

Lifecycle Phases → CSHCM Processes ↓	Planning	System Analysis & Requirements	System Design	Development	Integration & Verification	Deployment & Validation	Training	Operations	Maintenance / Upgrade	Information exchange HC Organization-Supplier	Disposal
Detection Processes								X			
Response Planning								X			
Communications								X			
Analysis								X			
Mitigation								X			
Recovery Planning								X			
Improvements								X			
Communications								X			

Table 10-4 CSHCM-SLCM_C-Processes vs S-Lifecycle Phases

11. Panacea Toolkit in the HSMs

11.1 Technical Tools

CSHCM Technological Services measures have been mapped with the four technical tools of the Panacea Toolkit, making reference to their high-level scope defined in the Panacea Description of Action (DOA),

- Dynamic Risk Assessment and Mitigation;
- Secure Information Sharing;
- Security by Design & Certification;
- Identification/ Authentication.

In order to assess the positioning of the Panacea Toolkit with respect to the Technological Services identified in Section 9.1.1.

Table 11-1 below provides the result of this mapping and shows that Panacea Toolkit is expect to provide strong contribution to 2 out 42 Cybersecurity Technological Services (plus partial contribution for other 4. It must be noted that Panacea Toolkit is focused on the Identify and Protect Functions of the NIST Framework and doesn't aims at providing solutions for the three remaining Functions.

#	Cyber Technological Services	Dynamic Risk Assessment and Mitigation	Secure Information Sharing	Security by Design & Certification	Identification/ Authentication	Remarks
1	Anti-Virus System (AV)					
2	Application tampering detection System					
3	Audit trail System					
4	Authentication services				X	
5	Configuration and systems management (CSM)	X (partial)				Partially covered as part of the information from the CSM can be used as a basis for the dynamic risk assessment
6	Data encryption System		X			
7	Data loss prevention System (DLP)	X	X			
8	Data monitoring System					
9	Data recovery System (backup/restore)					
10	Device authentication System				X	
11	Device blacklisting System	X (partial)				Partially covered, some Devices could be blacklisted automatically based on identified risk
12	Device identification System				X	
13	Dynamic Application Security Testing System (DAST)	X				
14	Endpoint control System	X			X	
15	Factory reset System					
16	Firewall System (FW)					
17	Firmware reset System					
18	Full Pack Capture System (PCAP)					
19	Host Intrusion Prevention System (HISP)					
20	Identification and authentication System				X	
21	Identity and access management System (IAM)				X	
22	Image recovery System	X (to be				

#	Cyber Technological Services	Dynamic Risk Assessment and Mitigation	Secure Information Sharing	Security by Design & Certification	Identification/ Authentication	Remarks
		explored)				
23	Incident management System		X (partial)			Partially covered, an IMS can be used as the basis for threat data that can be useful as input for the dynamic risk assessment
24	Interactive Application Security Testing System (IAST)			X		
25	Intrusion Detection System (IDS)					
26	Intrusion Prevention System (IPS)					
27	Netflow System					
28	Physical Access behavioural analytics System	X (to be explored)				
29	Physical access control system				X	
30	Risk Assessment System (RAS)	X				
31	Runtime Application Self-Protection Service (RASP)					
32	Secure Remote Access System (SRA)					
33	Security By Design Assessment System (SDAS)			X		
34	Static Application Security Testing System (SAST)			X		
35	Structural vulnerability assessment System	X				
36	Threat analysis System	X				
37	Threat detection System	X				
38	User behavioural analytics System	X				
39	User identification system				X	
40	Video surveillance System					
41	Web application firewall System (WAF)					
42	Web fraud detection System					

Table 11-1 Mapping of Panacea Technical tools with the security measures identified in CSHCM

11.2 Non-Technical Tools

CSHCM Non-technical mitigation measures have been mapped with the three organizational tools of the Panacea Toolkit, making reference to their high-level scope defined in the Panacea Description of Action (DOA),

- Training and Education for Cybersecurity;
- Resilience Governance;
- Secure Behaviours Nudging.

in order to assess the positioning of the Panacea Toolkit with respect to the CSHCM non-technical measures identified in Section 9.1.2.

Table 11-2 below provides the result of this mapping and shows that Panacea Toolkit is expect to provide contribution to all the Types of measures.

Class	Types	Training and Education for Cybersecurity	Resilience Governance	Secure Behaviors Nudging
Governance	Controls		X	
Training and/or education packages	Initial learning interventions	X		
	Refresher learning interventions	X		
	Performance support systems	X		
"Nudging" guidelines	Identify the behaviors you wish staff to exhibit to protect against the 5 currently most common cyberattacks			X
	Method to detect problematic behaviors or lack of security behaviors within each team/group			X
	Security Behavior and Barriers Workshop			X
	Nudge workshops			X
	Develop preferred intervention			X
	Implement and monitor effectiveness			X
Insurance schemes	First Party coverage (about the insured's own damage)		X	
	Third Party coverage (third party liability protection, such as clients or partners)		X	
Communication plans	Media Communication plan (for reputation & Brand)		X	
	GDPR related communication plan		X	
	Establish cyber threat information sharing with other health care organizations		X	
Security Risk Management Plan	Security Risk life cycle plan: Security Role and Responsibility Plan		X	
	Risk Mitigation Plan		X	
Standard Operating Procedures	Event classification and Cyber Security Incident Management		X	
Technical processes and/or procedures	Data labeling		X	
	Phishing Simulations	X		
	Phishing Awareness	X		
	Applicable (data) legislation		X	
	Device eradication		X	
	Account block		X	
	Investigation			X
	Outsourced monitoring			X

Table 11-2 Mapping of Panacea Non-Technical tools with the security measures identified in CSHCM

12. Conclusions

The Panacea team in charge of the production of this Deliverable, has had many opportunities to share the "work in progress" and the intermediate output, both with Consortium and non -Consortium experts.

This had allowed the Team to timely collect feedback and frequent questions, aiming at

- better positioning the models in the realm of the models;
- better qualifying the fact that these models are a high level representation of the reality;
- understanding how the model can practically be used;
- understanding what can be done with these models.

This final section tries to answer those questions and hence properly wrap-up the deliverable.

1) Which types of models are the HSMs?

HSMs, as a whole, make up an architectural model, which describes both the reality to be protected (Healthcare organizations, Medical Device Lifecycle, System Development Lifecycle) and the related defence system (the Cybersecurity system).

Its main purpose is to support the Panacea project.

According to [ARCH], **architectural models in a project fill many roles**, including:

- Communication with client, users, and builders;
- Maintenance of system integrity through coordination of design activities;
- Assisting design by providing templates, and organizing and recording decisions.

The HSMs described in this document fill all these roles. Thanks to its taxonomies and instantiation schemes, it provides a clear link between the Toolkit to be developed and the realities on which the Toolkit should operate

These descriptions can be used in all the phases of the project:

- During the toolkit requirements definition, facilitating the interaction with end users and other stakeholders, through specific context descriptions
- During the research and Development activities, allowing to easily identify real cases where to develop ideas and test prototypes
- During the Integration into end-users' realities, allowing the identification of meaningful scenarios, relevant both for the project and for the end-users

2) How the HCOM relates to the real organizational components?

HCOM provides a summary representation of the reality, allowing to grasp its essential aspects.

HCOM' link with the reality is mediated by the data bases normally available in the organizations: ICT asset register (or Configuration Management Database -CMDB), Medical Devices register, and the HR Database.

The relationship between HCOM and the reality can be represented in a picture structured in three layers (see next Figure 12-1[17]):

- Layer 1: is the reality, made up of individual persons, workstations, Medical Devices, software programs, data bases, servers, cables, switches, …

[17] Legend: TS=Technological Services, S=Service, P=Processes, R=Roles, F=Organizational Functions

- Layer 2: provides a very precise representation of the lower layer; for the most part of the reality[18], it t provides a 1:1 representation, which may be contained in
    - the Configuration Management Data Base (CMDB), which registers the assets for the most part individually, in part as small clusters and shows the logical connections among the assets; CMBD is normally organized linking together all the assets which contribute to the so called "services"[19]
    - the Human Resources Data Base (HR DB), which registers Individual staff and their position in the organigram
- Layer 3: is the layer where HCOM are positioned; it provides a summary representation of the reality; it lists all the "services" of the CMDB, but at the same time it identifies all the other assets in terms of clusters (e.g. Patient Data); as for the staff, it is clustered in the layer per Role and per Organizational Functions; the layer it also introduces the Processes, as an entity to which the other entities can be referred.

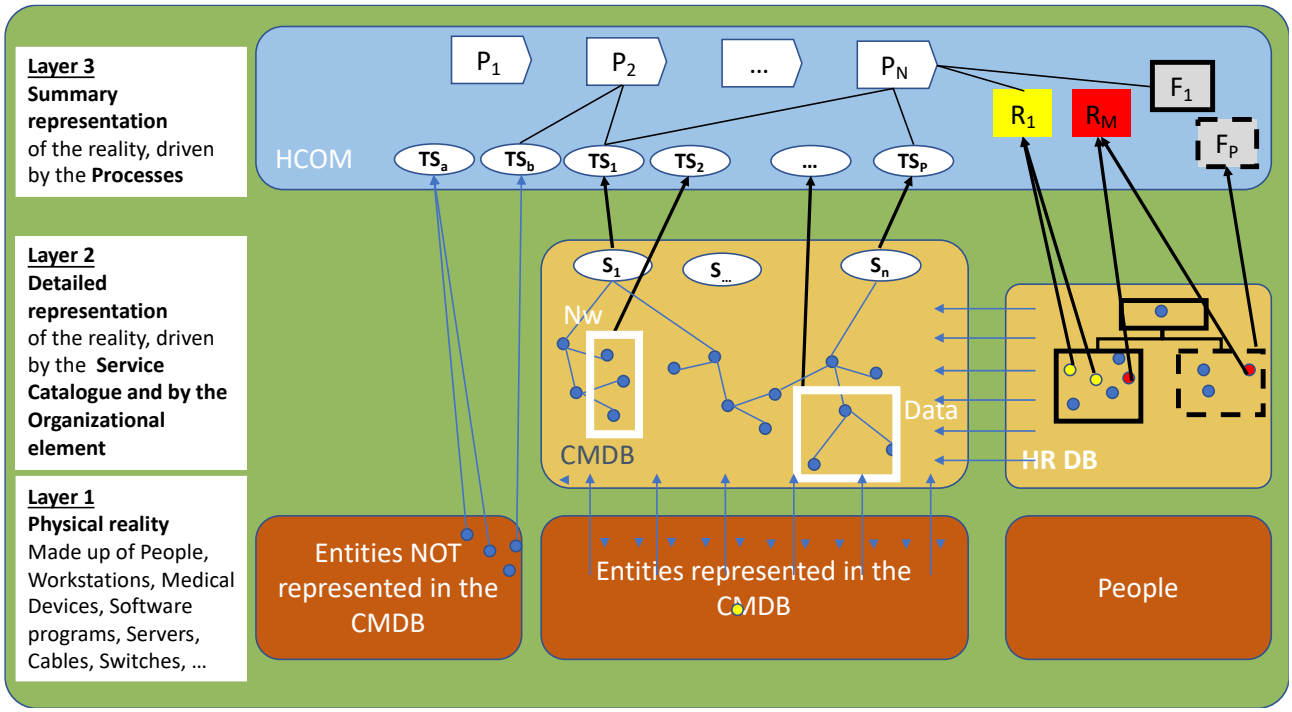

Figure 12-1 HCOM relationship with real entities and resource Data Bases (e.g. CMDB, HR DB)

3) How the models can be used?

From an operational point of view, each model is made up of a set of lists (the Catalogues), tables and matrixes, which have been shown and described in the previous sections of this document.

The full set of Catalogues, Instantiation Tables and Instantiation Matrixes has been put on the sheets of an Excel file.

[18] For instance, it may happen that groups of Medical Devices are not included in the CMDB because they are connected in a local dedicated network, ad not to the network of the hospital. HCOM includes also these assets, not individually, but as clusters

[19] "Service" is what is seen by the users, but each service is built through the cooperation of many assets (applications, servers, data bases, etc.); for instance, the CMDB of FPG has some 300 services. Services are listed in a Service Catalogue (see [MENDES]

The instantiation of a reality, as emerged during the execution of Task 1.1, can count on already available sources, which normally include:

- Human Resources Data Base (HR DB), which contains also organigrams at Unit level, the list of the individual staff member with indication of their job profile and the Unit in which they work;
- Medical Device register;
- A register of all the ICT assets or a Configuration Management Data Base (CMDB), which contains the not only the register of all the ICT assets, but also shows logical connections among these assets.

For some Matrixes and Tables there are not yet existing sources. Interviews with ICT managers, Information Security Officer, Risk Manager, Director of Health operations, staff operating in the processes may fill the informational gap.

Table and Matrixes have already been used during Task 1.1, to instantiate the models at FPG, HSE and 7HRC. The non-confidential results are shown in the document to explain the most part of the instantiation schemes. Some of them are confidential and are delivered as a separate document: they are related to instantiation of the Technology Services catalogue, see 6.3.1, of the criticality analysis, see 6.3.6, and of the Cybersecurity for Healthcare Model (CSHCM), see 9.3.

4) For which purposes the models are expected to be used?

The full set of Health Services Models (HSMs)

- In Panacea Project, will be used
  - To elicit and clearly map end user requirements, taking care not only of FPG, 7HRC and HSE needs but also of other healthcare end users, medical device manufacturers, software developers and system integrators;
  - To describe and select the best scenarios for testing the Panacea Toolkit at FPG, 7HRC and HSE;
  - To tailor the Toolkit on the specificities of the Healthcare Organizations (e.g. on the different types of staff and of medical devices).
- Outside Panacea Project, could be used as a standard ”descriptive model” or “taxonomy”, for instance
  - To describe and compare cybersecurity solutions for Healthcare organizations;
  - To tailor controls of cybersecurity frameworks (e.g. ISO 27001 and NIST) on the specificities of the Healthcare Organizations (Hospitals and territorial Care Centres);

Annex A-ILO/ISCO occupations (definitions and examples)

	Roles		Sub-Roles/ ILO-ISCO occupations	ILO-ISCO code	Definition (according to [ILO] document)	Examples (from [ILO] document)
	Managers					
1.1	Health services Managers	1.1.1	Health services Managers	1342	Health services managers plan, direct, coordinate and evaluate the provision of clinical and community health care services in hospitals, clinics, public health agencies and similar organizations.	Chief public health officer Clinical director Community health care coordinator Director of nursing Health facility administrator Hospital matron Medical administrator
	Health Roles					
2.1	Generalist Medical Practitioners	2.1.1	Generalist Medical Practitioners	2211	Generalist medical practitioners (including family and primary care doctors) diagnose, treat and prevent illness, disease, injury and other physical and mental impairments and maintain general health in humans through application of the principles and procedures of modern medicine. They do not limit their practice to certain disease categories or methods of treatment and may assume responsibility for the provision of continuing and comprehensive medical care to individuals, families and communities.	District medical doctor–therapist Family medical practitioner General practitioner Medical doctor (general) Medical officer (general) Physician (general) Primary health care physician Resident medical officer specializing in general practice
2.2	Specialist Medical Practitioners	2.2.1	Specialist Medical Practitioners	2212	Specialist medical practitioners (medical doctors) diagnose, treat and prevent illness, disease, injury and other physical and mental impairments in humans, using specialized testing, diagnostic, medical, surgical, physical and psychiatric techniques through application of the principles and procedures of modern medicine. They specialize in certain disease categories, types of patient or methods of treatment and may conduct medical education and research in their chosen areas of specialization.	Anaesthetist Cardiologist Emergency medicine specialist Gynaecologist Obstetrician Ophthalmologist Paediatrician Pathologist Preventive medicine specialist Psychiatrist Radiation oncologist Radiologist Resident medical officer in specialist training Specialist medical practitioner (public health) Specialist physician (internal medicine) Specialist physician (nuclear medicine) Surgeon

	Roles		Sub-Roles/ ILO-ISCO occupations	ILO-ISCO code	Definition (according to [ILO] document)	Examples (from [ILO] document)
2.3	Nurses	2.3.1	Nursing Professionals	2221	Nursing professionals provide treatment, support and care services for people who are in need of nursing care due to the effects of ageing, injury, illness or other physical or mental impairment, or potential risks to health. They assume responsibility for the planning and management of the care of patients, including the supervision of other health care workers, working autonomously or in teams with medical doctors and others in the practical application of preventive and curative measures.	Clinical nurse consultant District nurse Nurse anaesthetist Nurse educator Nurse practitioner Operating theatre nurse Professional nurse Public health nurse Specialist nurse
2.3		2.3.2	Midwifery Professionals	222	Midwifery professionals plan, manage, provide and evaluate midwifery care services before, during and after pregnancy and childbirth. They provide delivery care for reducing health risks to women and newborn children, working autonomously or in teams with other health care providers.	Professional midwife
2.3		2.3.3	Nursing and Midwifery Associate Professionals	322	Nursing and midwifery associate professionals provide basic nursing and personal care for people who are physically or mentally ill, disabled or infirm, and for others in need of care due to potential risks to health including before, during and after childbirth. They generally work under the supervision of, and in support of, implementation of health care, treatment and referrals plans established by medical, nursing, midwifery and other health professionals.	Assistant nurse Associate professional nurse Enrolled nurse Practical nurse Assistant midwife Traditional midwife Assistant midwife Traditional midwife
2.4	Paramedical practitioners	2.4.1	Paramedical Practitioners	224	Paramedical practitioners provide advisory, diagnostic, curative and preventive medical services more limited in scope and complexity than those carried out by medical doctors. They work autonomously or with limited supervision of medical doctors, and apply advanced clinical procedures for treating and preventing diseases, injuries and other physical or mental impairments common to specific communities.	Advanced care paramedic Clinical officer (paramedical) Feldscher Primary care paramedic Surgical technician
2.5	Medical and Pharmaceutical Technicians	2.5.1	Medical and Pharmaceutical Technicians	321	Medical and pharmaceutical technicians perform technical tasks to assist in diagnosis and treatment of illness, disease, injuries and impairments.	Medical Imaging Technicians Therapeutic Equipment Technicians Medical and Pathology Laboratory Technicians Pharmaceutical Technicians and Assistants Medical and Dental Prosthetic Technicians

	Roles		Sub-Roles/ ILO-ISCO occupations	ILO-ISCO code	Definition (according to [ILO] document)	Examples (from [ILO] document)
2.6	Ambulance Workers	2.6.1	Ambulance Workers	3258	Ambulance workers provide emergency health care to patients who are injured, sick, infirm or otherwise physically or mentally impaired prior to and during transport to medical facilities. Tasks may include recording information on patients' conditions and treatments provided in medical record-keeping systems.	Ambulance officer Ambulance paramedic Emergency medical technician Emergency paramedic
2.7	Personal care workers in Health Services	2.7.1	Personal Care Workers in Health Services	53	Personal care workers in health services provide personal care and assistance with mobility and activities of daily living to patients and elderly, convalescent and disabled people in health care and residential settings.	Health Care Assistants Home-based Personal Care Workers
2.8	Other Heath roles	2.8.1	Traditional and Complementary Medicine Professionals	223	Traditional and complementary medicine professionals examine patients; prevent and treat illness, disease, injury and other physical and mental impairments; and maintain general health in humans by applying knowledge, skills and practices acquired through extensive study of the theories, beliefs and experiences originating in specific cultures.	Acupuncturist Ayurvedic practitioner Chinese herbal medicine practitioner Homeopath Naturopath
2.8		2.8.2	Other Health Professionals	226	Other health professionals provide health services related to dentistry, pharmacy, environmental health and hygiene, occupational health and safety, physiotherapy, nutrition, hearing, speech, vision and rehabilitation therapies. This minor group includes all human health professionals except doctors, traditional and complementary medicine practitioners, nurses, midwives and paramedical professionals.	Dentists Pharmacists Environmental and Occupational Health and Hygiene Professionals 2264 Physiotherapists Dieticians and Nutritionists Audiologists and Speech Therapists Optometrists and Ophthalmic OpticiansHealth Professionals Not Elsewhere Classified
2.8		2.8.3	Traditional and Complementary Medicine Associate Professionals	323	Traditional and complementary medicine associate professionals prevent, care for and treat human physical and mental illnesses, disorders and injuries using herbal and other therapies based on theories, beliefs and experiences originating in specific cultures. They administer treatments using traditional techniques and medicaments, either acting independently or according to therapeutic care plans established by a traditional medicine or other health professional.	Acupuncture technician Ayurvedic technician Bonesetter Herbalist Homeopathy technician Scraping and cupping therapist Village healer Witch doctor

	Roles		Sub-Roles/ ILO-ISCO occupations	ILO-ISCO code	Definition (according to [ILO] document)	Examples (from [ILO] document)
2.8		2.8.4	Other Health Associate Professionals (excluding 3258 Ambulance Workers)	325	Other health associate professionals perform technical tasks and provide support services in dentistry, medical records administration, community health, the correction of reduced visual acuity, physiotherapy, environmental health, emergency medical treatment and other activities to support and promote human health.	Dental Assistants and Therapists Medical Records and Health Information Technicians Community Health Workers Dispensing Opticians Physiotherapy Technicians and Assistants Medical Assistants Environmental and Occupational Health Inspectors and Associates Health Associate Professionals Not Elsewhere Classified
	Non-health Roles					
3.1	Technical roles	3.1.1	Science and Engineering Professionals	21	Science and engineering professionals conduct research; improve or develop concepts, theories and operational methods; or apply scientific knowledge relating to fields such as physics, astronomy, meteorology, chemistry, geophysics, geology, biology, ecology, pharmacology, medicine, mathematics, statistics, architecture, engineering, design and technology.	Civil Engineers Electrical Engineers Electronics Engineers Building Architects
3.1		3.1.2	Science and Engineering Associate Professionals	31	Physical and engineering science technicians perform technical tasks to aid in research on and the practical application of concepts, principles and operational methods particular to physical sciences including such areas as engineering, technical drawing or economic efficiency of production processes.	Civil Engineering Technicians Electrical Engineering Technicians Electronics Engineering Technicians Mechanical Engineering Technicians Chemical Engineering Technicians
3.2	Administrative back-office roles	3.2.1	Business and Administration Professionals	24	Business and administration professionals perform analytical, conceptual and practical tasks to provide services in financial matters, human resource development, public relations, marketing and sales in the technical, medical, information and communications technology areas; and conduct reviews of organizational structures, methods and systems as well as quantitative analyses of information affecting investment programmes.	Accountant Auditor Administration Professionals (Organization and methods analyst, Human resource expert Job analyst Training officer
3.2		3.2.2	General and Keyboard Clerks	41	General and keyboard clerks record, organize, store and retrieve information and perform a wide range of clerical and administrative tasks according to established procedures.	General Office Clerks Secretaries (general) Keyboard Operators
3.2		3.2.3	Numerical and Material Recording Clerks	43	Material recording and transport clerks keep records of goods produced, purchased, stocked and dispatched, and of materials needed at specified production dates, or keep records of operational aspects and coordinate the timing of passenger and freight transport.	Payroll Clerks Stock Clerks

	Roles		Sub-Roles/ ILO-ISCO occupations	ILO-ISCO code	Definition (according to [ILO] document)	Examples (from [ILO] document)
3.3	Administrative front-office roles	3.3.1	Customer Services Clerks	42	Customer services clerks deal with clients in connection with money-handling operations, travel arrangements, requests for information, making appointments, operating telephone switchboards, and interviewing for surveys or to complete applications for eligibility for services.	Customer contact centre information clerk Answering service operator
3.4	Medical Secretaries	3.4.1	Medical Secretaries	3344	Medical secretaries, using specialized knowledge of medical terminology and health care delivery procedures, assist health professionals and other workers by performing a variety of communication, documentation, administrative and internal coordination functions, to support health workers in medical facilities and other health-care related organizations.	Dental secretary Hospital ward secretary Medical insurance billing secretary Medical office administrative assistant ▪ Medical practice manager Medical secretary Medical stenographer Medical transcriptionist Pathology secretary Patient care secretary Medical laboratory secretary
3.5	Information and Communications Technology roles	3.5.1	Information and Communications Technology Professionals	25	Information and communications technology professionals conduct research; plan, design, write, test, provide advice and improve information technology systems, hardware, software and related concepts for specific applications; develop associated documentation including principles, policies and procedures; and design, develop, control, maintain and support databases and other information systems to ensure optimal performance and data integrity and security.	Software and Applications Developers and Analysts Database and Network Professionals
3.5		3.5.2	Information and Communications Technicians	35	Information and communications technicians provide support for the day-to-day running of computer systems, communications systems and networks, and perform technical tasks related to telecommunications, broadcast image and sound as well as other types of telecommunications signals on land, sea or in aircraft.	Information and Communications Technology Operations Technicians Information and Communications Technology User Support Technicians Computer Network and Systems Technicians Web Technician Engineering technician (telecommunications)
3.6	Other non-health roles	3.6.1	Legal, Social and Cultural Professionals	26	Legal, social and cultural professionals conduct research; improve or develop concepts, theories and operational methods; or apply knowledge relating to the law, storage and retrieval of information and artefacts, psychology, social welfare, politics, economics, history, religion, languages, sociology, other social sciences, and arts and entertainment.	Legal Professionals Social and Religious Professionals (Imam, Priest, Rabbi)

	Roles		Sub-Roles/ ILO-ISCO occupations	ILO-ISCO code	Definition (according to [ILO] document)	Examples (from [ILO] document)
3.6		3.6.2	Religious Associate Professionals	3413	Religious associate professionals provide support to ministers of religion or to a religious community, undertake religious works, preach and propagate the teachings of a particular religion and endeavour to improve well-being through the power of faith and spiritual advice.	Faith healer ay preacher Monk Nun
3.6		3.6.3	Other Clerical Support Workers	44	Other clerical support workers sort and deliver mail, file documents, prepare information for processing, maintain personnel records, check material for consistency with original source material, assist persons who cannot read or write, and perform various other specialized clerical duties.	Personnel Clerks

Annex B-Governance reference controls

Following three details of the controls indicated in Table 9-3 and related to the Cybersecurity governance (non-technical) measures. They refer to COBIT 5, ISO/IEC 27001:2013 and NIST SP 800-53 Rev. 4.

COBIT 5	
Control ID	*Description*
APO01.02	Establish, agree on and communicate roles and responsibilities of IT personnel, as well as other stakeholders with responsibilities for enterprise IT, that clearly reflect overall business needs and IT objectives and relevant personnel's authority, responsibilities and accountability
APO01.03	Maintain the enablers of the management system and control environment for enterprise IT, and ensure that they are integrated and aligned with the enterprise's governance and management philosophy and operating style. These enablers include the clear communication of expectations/requirements. The management system should encourage cross-divisional co-operation and teamwork, promote compliance and continuous improvement, and handle process deviations (including failure)
APO07.01	Evaluate staffing requirements on a regular basis or upon major changes to the enterprise or operational or IT environments to ensure that the enterprise has sufficient human resources to support enterprise goals and objectives. Staffing includes both internal and external resource
APO07.02	Identify key IT personnel while minimizing reliance on a single individual performing a critical job function through knowledge capture (documentation), knowledge sharing, succession planning and staff backup
APO07.03	Define and manage the skills and competencies required of personnel. Regularly verify that personnel have the competencies to fulfil their roles on the basis of their education, training and/or experience, and verify that these competencies are being maintained, using qualification and certification programmes where appropriate. Provide employees with ongoing learning and opportunities to maintain their knowledge, skills and competencies at a level required to achieve enterprise goals
APO07.04	Perform timely performance evaluations on a regular basis against individual objectives derived from the enterprise's goals, established standards, specific job responsibilities, and the skills and competency framework. Employees should receive coaching on performance and conduct whenever appropriate
APO07.05	Understand and track the current and future demand for business and IT human resources with responsibilities for enterprise IT. Identify shortfalls and provide input into sourcing plans, enterprise and IT recruitment processes sourcing plans, and business and IT recruitment processes
APO11.06	Maintain and regularly communicate an overall quality plan that promotes continuous improvement. This should include the need for, and benefits of, continuous improvement. Collect and analyses data about the QMS and improve its effectiveness. Correct non-conformities to prevent recurrence. Promote a culture of quality and continual improvement
APO12.02	Develop useful information to support risk decisions that take into account the business relevance of risk factors
APO12.03	Maintain an inventory of known risk and risk attributes (including expected frequency, potential impact and responses) and of related resources, capabilities and current control activities
APO12.04	Provide information on the current state of IT-related exposures and opportunities in a timely manner to all required stakeholders for appropriate response
APO12.05	Manage opportunities to reduce risk to an acceptable level as a portfolio
APO12.06	Respond in a timely manner with effective measures to limit the magnitude of loss from IT-related events
APO13.02	Maintain an information security plan that describes how information security risk is to be managed and aligned with the enterprise strategy and enterprise architecture. Ensure that recommendations for implementing security improvements are based on approved business cases and implemented as an integral part of services and solutions development, then operated as an integral part of business operation
BAI05.07	Sustain changes through effective training of new staff, ongoing communication campaigns, continued top management commitment, adoption monitoring and sharing of lessons learned across the enterprise
DSS01.04	Maintain measures for protection against environmental factors. Install specialized equipment and devices to monitor and control the environment
DSS03.01	Define and implement criteria and procedures to report problems identified, including problem classification, categorization and prioritization

DSS04.02	Evaluate business continuity management options and choose a cost-effective and viable continuity strategy that will ensure enterprise recovery and continuity in the face of a disaster or other major incident or disruption
DSS04.03	Develop a business continuity plan (BCP) based on the strategy that documents the procedures and information in readiness for use in an incident to enable the enterprise to continue its critical activities
DSS04.05	Conduct a management review of the continuity capability at regular intervals to ensure its continued suitability, adequacy and effectiveness. Manage changes to the plan in accordance with the change control process to ensure that the continuity plan is kept up to date and continually reflects actual business requirements
DSS05.01	Implement and maintain preventive, detective and corrective measures in place (especially up-to-date security patches and virus control) across the enterprise to protect information systems and technology from malware (e.g., viruses, worms, spyware, spam)
DSS05.05	Define and implement procedures to grant, limit and revoke access to premises, buildings and areas according to business needs, including emergencies. Access to premises, buildings and areas should be justified, authorized, logged and monitored. This should apply to all persons entering the premises, including staff, temporary staff, clients, vendors, visitors or any other third party
DSS06.03	Manage the business roles, responsibilities, levels of authority and segregation of duties needed to support the business process objectives. Authorize access to any formation assets related to business information processes, including those under the custody of the business, IT and third parties. This ensures that the business knows where the data are and who is handling data on its behalf
EDM01.01	Continually identify and engage with the enterprise's stakeholders, document an understanding of the requirements, and make a judgement on the current and future design of governance of enterprise IT.
EDM01.02	Inform leaders and obtain their support, buy-in and commitment. Guide the structures, processes and practices for the governance of IT in line with agreed-on governance design principles, decision-making models and authority levels. Define the information required for informed decision making.
MEA03.02	Review and adjust policies, principles, standards, procedures and methodologies to ensure that legal, regulatory and contractual requirements are addressed and communicated. Consider industry standards, codes of good practice, and good practice guidance for adoption and adaptation
MEA03.04	Obtain and report assurance of compliance and adherence with policies, principles, standards, procedures and methodologies. Confirm that corrective actions to address compliance gaps are closed in a timely manner

ISO/IEC 27001:2013	
Control ID	*Description*
A.5.1.1	A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.
A.6.1.1	All information security responsibilities shall be defined and allocated.
A.7.1.1	Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.
A.7.2.2	All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.
A.7.3.1	Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced.
A.8.1.4	All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement.
A.11.1.1	Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.
A.11.1.2	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.
A.11.1.4	Physical protection against natural disasters, malicious attack or accidents shall be designed and applied.

A.11.1.6	Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.
A.11.2.3	Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage.
A.12.2.1	Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.
A.16.1.1	Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.
A.16.1.2	Information security events shall be reported through appropriate management channels as quickly as possible.
A.16.1.5	Information security incidents shall be responded to in accordance with the documented procedures.
A.16.1.6	Knowledge gained from analyzing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.
A.17.1.1	The organization shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.
A.17.1.2	The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.
A.17.1.3	The organization shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.
A.18.1.1	All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization.
A.18.1.2	Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.
A.18.1.3	Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislatory, regulatory, contractual and business requirements.
A.18.1.4	Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.
A.18.1.5	Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.

NIST SP 800-53 Rev. 4	
Control ID	*Description*
AC-4	Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information.
AT-2	Organizations determine the appropriate content of security awareness training and security awareness techniques based on the specific organizational requirements and the information systems to which personnel have authorized access.
AT-3	Organizations determine the appropriate content of security training based on the assigned roles and responsibilities of individuals and the specific security requirements of organizations and the information systems to which personnel have authorized access. Such training can include for example, policies, procedures, tools, and artifacts for the organizational security roles defined.
AU-6	Audit review, analysis, and reporting covers information security-related auditing performed by organizations including, for example, auditing that results from monitoring of account usage, remote access, wireless connectivity, mobile device connection, configuration settings, system component inventory, use of maintenance tools and nonlocal maintenance, physical access, temperature and humidity, equipment delivery and removal, communications at the information system boundaries, use of mobile code, and use of VoIP.
CA-2	The organization develops a security assessment plan that describes the scope of the assessment including: security controls and control enhancements under assessment; assessment procedures to be used to determine security control effectiveness; and assessment environment, assessment team, and assessment roles and responsibilities. Assesses the security controls in the information system and its environment of operation to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements; produces a security assessment report that documents the results of the assessment; and provides the results of the security control assessment.

CA-3	The organization authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements; documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated.
CA-7	Continuous monitoring programs facilitate ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions. Continuous monitoring programs also allow organizations to maintain the security authorizations of information systems and common controls over time in highly dynamic environments of operation with changing mission/business needs, threats, vulnerabilities, and technologies.
CM-2	The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.
CP-2	Organizations can ensure that the necessary contingency planning activities are in place and activated in the event of a security incident. They develop a contingency plan for the information system that addresses contingency roles, responsibilities, assigned individuals with contact information.
CP-3	Contingency training provided by organizations is linked to the assigned roles and responsibilities of organizational personnel to ensure that the appropriate content and level of detail is included in such training.
CP-4	The organization tests the contingency plan to determine the effectiveness of the plans and the organizational readiness to execute the plan.
IR-3	Organizations test incident response capabilities to determine the overall effectiveness of the capabilities and to identify potential weaknesses or deficiencies.
IR-4	The organization implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; coordinates incident handling activities with contingency planning activities; and incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implements the resulting changes accordingly.
IR-8	The organizations develop and implement a coordinated approach to incident response. Organizational missions, business functions, strategies, goals, and objectives for incident response help to determine the structure of incident response capabilities.
PE-2	This control applies to organizational employees and visitors. Individuals with permanent physical access authorization credentials are not considered visitors. Authorization credentials include, for example, badges, identification cards, and smart cards. Organizations determine the strength of authorization credentials needed (including level of forge-proof badges, smart cards, or identification cards) consistent with federal standards, policies, and procedures.
PE-3	The organization verifies individual access authorizations before granting access to the facility and determines the types of facility guards needed including, for example, professional physical security staff or other personnel such as administrative staff or information system users.
PE-4	The organization controls physical access to information system distribution and transmission lines help to prevent accidental damage, disruption, and physical tampering.
PE-5	The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.
PE-6	The organization monitors physical access to the facility where the information system resides to detect and respond to physical security incidents.
PE-9	The organization protects power equipment and power cabling for the information system from damage and destruction.
PL-2	The organization develops a security plan for the information system that provides an overview of the security requirements for the system; distributes copies of the security plan and communicates subsequent changes to the plan; updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments and protects the security plan from unauthorized disclosure and modification.
PM-11	The organization defines mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations and determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until achievable protection needs are obtained.
PM-12	The organization implements an insider threat program that includes a cross-discipline insider threat incident handling team. Insider threat programs include security controls to detect and prevent malicious insider activity through the centralized integration and analysis of both technical and non-technical information to identify potential insider threat concerns.
PM-13	The organization establishes an information security workforce development and improvement program. Information security workforce development and improvement programs are complementary to organizational security awareness and training programs.
PM-14	The organization implements a process for ensuring that organizational plans for conducting security testing, training, and monitoring activities associated with organizational information systems are developed and maintained and continue to be executed in a timely manner.

PM-16	The organization implements a threat awareness program that includes a cross-organization information-sharing capability. One of the best techniques to address this concern is for organizations to share threat information. This can include, for example, sharing threat events that organizations have experienced, mitigations that organizations have found are effective against certain types of threats, threat intelligence.
PM-4	Organizations view plans of action and milestones from an organizational perspective, prioritizing risk response actions and ensuring consistency with the goals and objectives of the organization.
PM-9	The organization implements the risk management strategy consistently across the organization and reviews and updates the risk management strategy to address organizational changes.
PS-7	Organizations define the transfers and terminations deemed reportable by security-related characteristics that include, for example, functions, roles, and nature of credentials/privileges associated with individuals transferred or terminated.
RA-3	Risk assessments take into account threats, vulnerabilities, likelihood, and impact to organizational operations and assets, individuals, other organizations, and the operation and use of information systems. Risk assessments also take into account risk from external parties.
RA-5	Security categorization of information systems guides the frequency and comprehensiveness of vulnerability scans. Organizations determine the required vulnerability scanning for all information system components, ensuring that potential sources of vulnerabilities such as networked printers, scanners, and copiers are not overlooked.
SI-4	Organizations can monitor information systems, for example, by observing audit activities in real time or by observing other system aspects such as access patterns, characteristics of access, and other actions. Information system monitoring is an integral part of organizational continuous monitoring and incident response programs.
SI-5	The organization disseminates security alerts, advisories, and directives to external organizations, that include, for example, external mission/business partners, supply chain partners, external service providers, and other peer/supporting organizations.

Annex C-Cybersecurity Roles

Following table provides a description of the Cybersecurity Roles from the [NICE] framework and mentioned in Section 9.1.4

NIST - NICE Cybersecurity Workforce Framework				
Category	**Specialty Area**	**Work Role Id**	**Work Role**	**Work Role Description**
Securely Provision (SP)	Risk Management (RSK)	SP-RSK-001	Authorizing Official/Designating Representative	Senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation (CNSSI 4009).
	Risk Management (RSK)	SP-RSK-002	Security Control Assessor	Conducts independent comprehensive assessments of the management, operational, and technical security controls and control enhancements employed within or inherited by an information technology (IT) system to determine the overall effectiveness of the controls (as defined in NIST SP 800-37).
	Software Development (DEV)	SP-DEV-001	Software Developer	Develops, creates, maintains, and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs.
	Software Development (DEV)	SP-DEV-002	Secure Software Assessor	Analyzes the security of new or existing computer applications, software, or specialized utility programs and provides actionable results.
	Systems Architecture (ARC)	SP-ARC-001	Enterprise Architect	Develops and maintains business, systems, and information processes to support enterprise mission needs; develops information technology (IT) rules and requirements that describe baseline and target architectures.
	Systems Architecture (ARC)	SP-ARC-002	Security Architect	Ensures that the stakeholder security requirements necessary to protect the organization's mission and business processes are adequately addressed in all aspects of enterprise architecture including reference models, segment and solution architectures, and the resulting systems supporting those missions and business processes.
	Technology R&D (TRD)	SP-TRD-001	Research & Development Specialist	Conducts software and systems engineering and software systems research to develop new capabilities, ensuring cybersecurity is fully integrated. Conducts comprehensive technology research to evaluate potential vulnerabilities in cyberspace systems.
	Systems Requirements Planning (SRP)	SP-SRP-001	Systems Requirements Planner	Consults with customers to evaluate functional requirements and translate functional requirements into technical solutions.
	Test and Evaluation (TST)	SP-TST-001	System Testing and Evaluation Specialist	Plans, prepares, and executes tests of systems to evaluate results against specifications and requirements as well as analyze/report test results.
	Systems Development (SYS)	SP-SYS-001	Information Systems Security Developer	Designs, develops, tests, and evaluates information system security throughout the systems development life cycle.
	Systems Development (SYS)	SP-SYS-002	Systems Developer	Designs, develops, tests, and evaluates information systems throughout the systems development life cycle.
Operate and Maintain (OM)	Data Administration (DTA)	OM-DTA-001	Database Administrator	Administers databases and/or data management systems that allow for the secure storage, query, protection, and utilization of data.
	Data Administration (DTA)	OM-DTA-002	Data Analyst	Examines data from multiple disparate sources with the goal of providing security and privacy insight. Designs and implements custom algorithms, workflow processes, and layouts for complex, enterprise-scale data sets used for modeling, data mining, and research purposes.
	Knowledge Management (KMG)	OM-KMG-001	Knowledge Manager	Responsible for the management and administration of processes and tools that enable the organization to identify,

NIST - NICE Cybersecurity Workforce Framework				
Category	**Specialty Area**	**Work Role Id**	**Work Role**	**Work Role Description**
				document, and access intellectual capital and information content.
	Customer Service and Technical Support (STS)	OM-STS-001	Technical Support Specialist	Provides technical support to customers who need assistance utilizing client-level hardware and software in accordance with established or approved organizational process components (i.e., Master Incident Management Plan, when applicable).
	Network Services (NET)	OM-NET-001	Network Operations Specialist	Plans, implements, and operates network services/systems, to include hardware and virtual environments.
	Systems Administration (ADM)	OM-ADM-001	System Administrator	Responsible for setting up and maintaining a system or specific components of a system (e.g. for example, installing, configuring, and updating hardware and software; establishing and managing user accounts; overseeing or conducting backup and recovery tasks; implementing operational and technical security controls; and adhering to organizational security policies and procedures).
	Systems Analysis (ANA)	OM-ANA-001	Systems Security Analyst	Responsible for the analysis and development of the integration, testing, operations, and maintenance of systems security.
Oversee and Govern (OV)	Legal Advice and Advocacy (LGA)	OV-LGA-001	Cyber Legal Advisor	Provides legal advice and recommendations on relevant topics related to cyber law.
	Legal Advice and Advocacy (LGA)	OV-LGA-002	Privacy Officer/Privacy Compliance Manager	Develops and oversees privacy compliance program and privacy program staff, supporting privacy compliance, governance/policy, and incident response needs of privacy and security executives and their teams.
	Training, Education, and Awareness (TEA)	OV-TEA-001	Cyber Instructional Curriculum Developer	Develops, plans, coordinates, and evaluates cyber training/education courses, methods, and techniques based on instructional needs.
	Training, Education, and Awareness (TEA)	OV-TEA-002	Cyber Instructor	Develops and conducts training or education of personnel within cyber domain.
	Cybersecurity Management (MGT)	OV-MGT-001	Information Systems Security Manager	Responsible for the cybersecurity of a program, organization, system, or enclave.
	Cybersecurity Management (MGT)	OV-MGT-002	Communications Security (COMSEC) Manager	Individual who manages the Communications Security (COMSEC) resources of an organization (CNSSI 4009) or key custodian for a Crypto Key Management System (CKMS).
	Strategic Planning and Policy (SPP)	OV-SPP-001	Cyber Workforce Developer and Manager	Develops cyberspace workforce plans, strategies, and guidance to support cyberspace workforce manpower, personnel, training and education requirements and to address changes to cyberspace policy, doctrine, materiel, force structure, and education and training requirements.
	Strategic Planning and Policy (SPP)	OV-SPP-002	Cyber Policy and Strategy Planner	Develops and maintains cybersecurity plans, strategy, and policy to support and align with organizational cybersecurity initiatives and regulatory compliance.
	Executive Cyber Leadership (EXL)	OV-EXL-001	Executive Cyber Leadership	Executes decision-making authorities and establishes vision and direction for an organization's cyber and cyber-related resources and/or operations.
	Program/Project Management (PMA) and Acquisition	OV-PMA-001	Program Manager	Leads, coordinates, communicates, integrates, and is accountable for the overall success of the program, ensuring alignment with agency or enterprise priorities.
	Program/Project Management (PMA) and Acquisition	OV-PMA-002	IT Project Manager	Directly manages information technology projects.

NIST - NICE Cybersecurity Workforce Framework				
Category	**Specialty Area**	**Work Role Id**	**Work Role**	**Work Role Description**
	Program/Project Management (PMA) and Acquisition	OV-PMA-003	Product Support Manager	Manages the package of support functions required to field and maintain the readiness and operational capability of systems and components.
	Program/Project Management (PMA) and Acquisition	OV-PMA-004	IT Investment/Portfolio Manager	Manages a portfolio of IT investments that align with the overall needs of mission and enterprise priorities.
	Program/Project Management (PMA) and Acquisition	OV-PMA-005	IT Program Auditor	Conducts evaluations of an IT program or its individual components to determine compliance with published standards.
Protect and Defend (PR)	Cyber Defense Analysis (CDA)	PR-CDA-001	Cyber Defense Analyst	Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats.
	Cyber Defense Infrastructure Support (INF)	PR-INF-001	Cyber Defense Infrastructure Support Specialist	Tests, implements, deploys, maintains, and administers the infrastructure hardware and software.
	Incident Response (CIR)	PR-CIR-001	Cyber Defense Incident Responder	Investigates, analyzes, and responds to cyber incidents within the network environment or enclave.
	Vulnerability Assessment and Management (VAM)	PR-VAM-001	Vulnerability Assessment Analyst	Performs assessments of systems and networks within the network environment or enclave and identifies where those systems/networks deviate from acceptable configurations, enclave policy, or local policy. Measures effectiveness of defense-in-depth architecture against known vulnerabilities.
Analyze (AN)	Threat Analysis (TWA)	AN-TWA-001	Threat/Warning Analyst	Develops cyber indicators to maintain awareness of the status of the highly dynamic operating environment. Collects, processes, analyzes, and disseminates cyber threat/warning assessments.
	Exploitation Analysis (EXP)	AN-EXP-001	Exploitation Analyst	Collaborates to identify access and collection gaps that can be satisfied through cyber collection and/or preparation activities. Leverages all authorized resources and analytic techniques to penetrate targeted networks.
	All-Source Analysis (ASA)	AN-ASA-001	All-Source Analyst	Analyzes data/information from one or multiple sources to conduct preparation of the environment, respond to requests for information, and submit intelligence collection and production requirements in support of planning and operations.

NIST - NICE Cybersecurity Workforce Framework				
Category	**Specialty Area**	**Work Role Id**	**Work Role**	**Work Role Description**
	All-Source Analysis (ASA)	AN-ASA-002	Mission Assessment Specialist	Develops assessment plans and measures of performance/effectiveness. Conducts strategic and operational effectiveness assessments as required for cyber events. Determines whether systems performed as expected and provides input to the determination of operational effectiveness.
	Targets (TGT)	AN-TGT-001	Target Developer	Performs target system analysis, builds and/or maintains electronic target folders to include inputs from environment preparation, and/or internal or external intelligence sources. Coordinates with partner target activities and intelligence organizations, and presents candidate targets for vetting and validation.
	Targets (TGT)	AN-TGT-002	Target Network Analyst	Conducts advanced analysis of collection and open-source data to ensure target continuity; to profile targets and their activities; and develop techniques to gain more target information. Determines how targets communicate, move, operate and live based on knowledge of target technologies, digital networks, and the applications on them.
	Language Analysis (LNG)	AN-LNG-001	Multi-Disciplined Language Analyst	Applies language and culture expertise with target/threat and technical knowledge to process, analyze, and/or disseminate intelligence information derived from language, voice and/or graphic material. Creates and maintains language-specific databases and working aids to support cyber action execution and ensure critical knowledge sharing. Provides subject matter expertise in foreign language-intensive or interdisciplinary projects.
Collect and Operate (CO)	Collection Operations (CLO)	CO-CLO-001	All Source-Collection Manager	Identifies collection authorities and environment; incorporates priority information requirements into collection management; develops concepts to meet leadership's intent. Determines capabilities of available collection assets, identifies new collection capabilities; and constructs and disseminates collection plans. Monitors execution of tasked collection to ensure effective execution of the collection plan.

NIST - NICE Cybersecurity Workforce Framework				
Category	**Specialty Area**	**Work Role Id**	**Work Role**	**Work Role Description**
	Collection Operations (CLO)	CO-CLO-002	All Source-Collection Requirements Manager	Evaluates collection operations and develops effects-based collection requirements strategies using available sources and methods to improve collection. Develops, processes, validates, and coordinates submission of collection requirements. Evaluates performance of collection assets and collection operations.
	Cyber Operational Planning (OPL)	CO-OPL-001	Cyber Intel Planner	Develops detailed intelligence plans to satisfy cyber operations requirements. Collaborates with cyber operations planners to identify, validate, and levy requirements for collection and analysis. Participates in targeting selection, validation, synchronization, and execution of cyber actions. Synchronizes intelligence activities to support organization objectives in cyberspace.
	Cyber Operational Planning (OPL)	CO-OPL-002	Cyber Ops Planner	Develops detailed plans for the conduct or support of the applicable range of cyber operations through collaboration with other planners, operators and/or analysts. Participates in targeting selection, validation, synchronization, and enables integration during the execution of cyber actions.
	Cyber Operational Planning (OPL)	CO-OPL-003	Partner Integration Planner	Works to advance cooperation across organizational or national borders between cyber operations partners. Aids the integration of partner cyber teams by providing guidance, resources, and collaboration to develop best practices and facilitate organizational support for achieving objectives in integrated cyber actions.
	Cyber Operations (OPS)	CO-OPS-001	Cyber Operator	Conducts collection, processing, and/or geolocation of systems to exploit, locate, and/or track targets of interest. Performs network navigation, tactical forensic analysis, and, when directed, executes on-net operations.
Investigate (IN)	Cyber Investigation (INV)	IN-INV-001	Cyber Crime Investigator	Identifies, collects, examines, and preserves evidence using controlled and documented analytical and investigative techniques.
	Cyber Investigation (INV)	IN-FOR-001	Law Enforcement /CounterIntelligence Forensics Analyst	Conducts detailed investigations on computer-based crimes establishing documentary or physical evidence, to include digital media and logs associated with cyber intrusion incidents.

NIST - NICE Cybersecurity Workforce Framework				
Category	**Specialty Area**	**Work Role Id**	**Work Role**	**Work Role Description**
	Digital Forensics (FOR)	IN-FOR-002	Cyber Defense Forensics Analyst	Analyzes digital evidence and investigates computer security incidents to derive useful information in support of system/network vulnerability mitigation.