Panacea

People-centric cybersecurity in healthcare

# PANACEA Security-by-Design Framework

RINA-C
Martina Bossini Baroggi

Webinar
10th December 2020

# Agenda

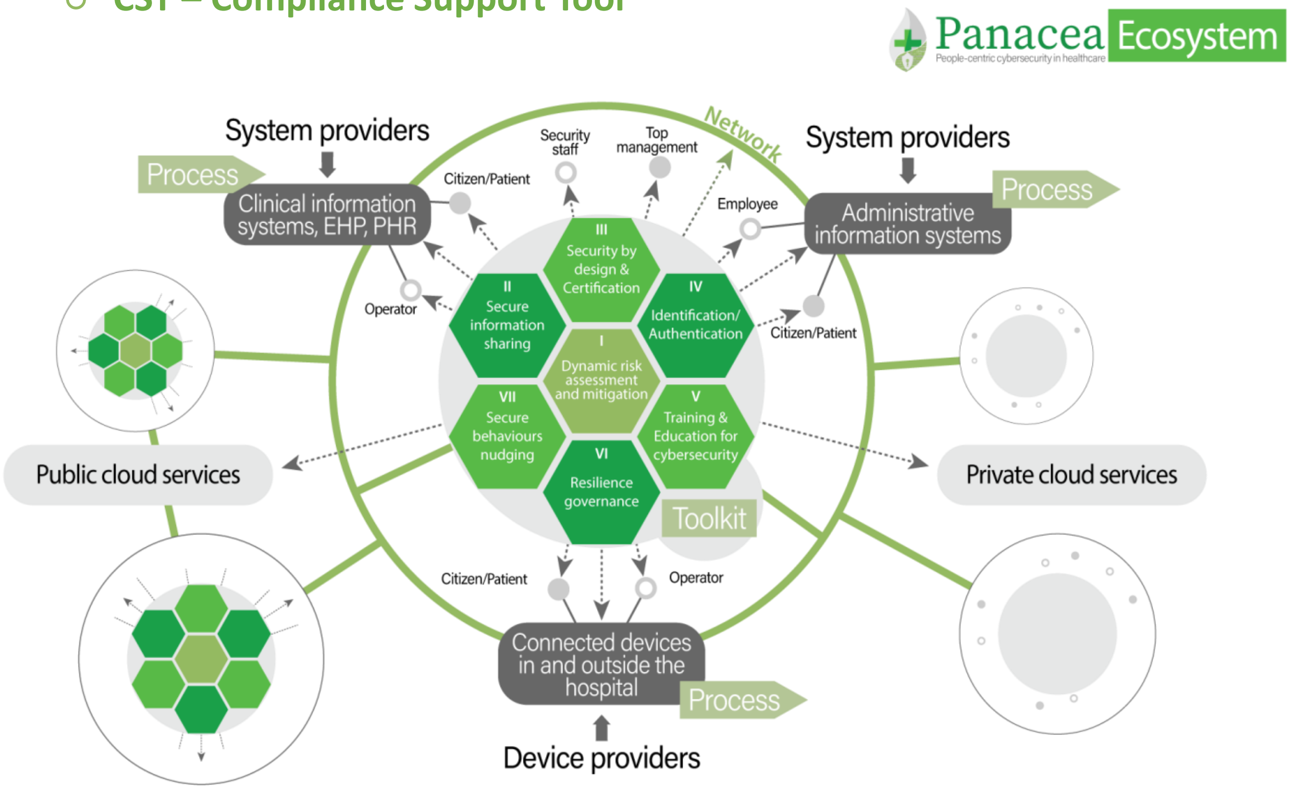
- Healthcare sector context
- PANACEA project response
- Security by Design Approach
- PANACEA Security-by-design Framework
- Innovation points

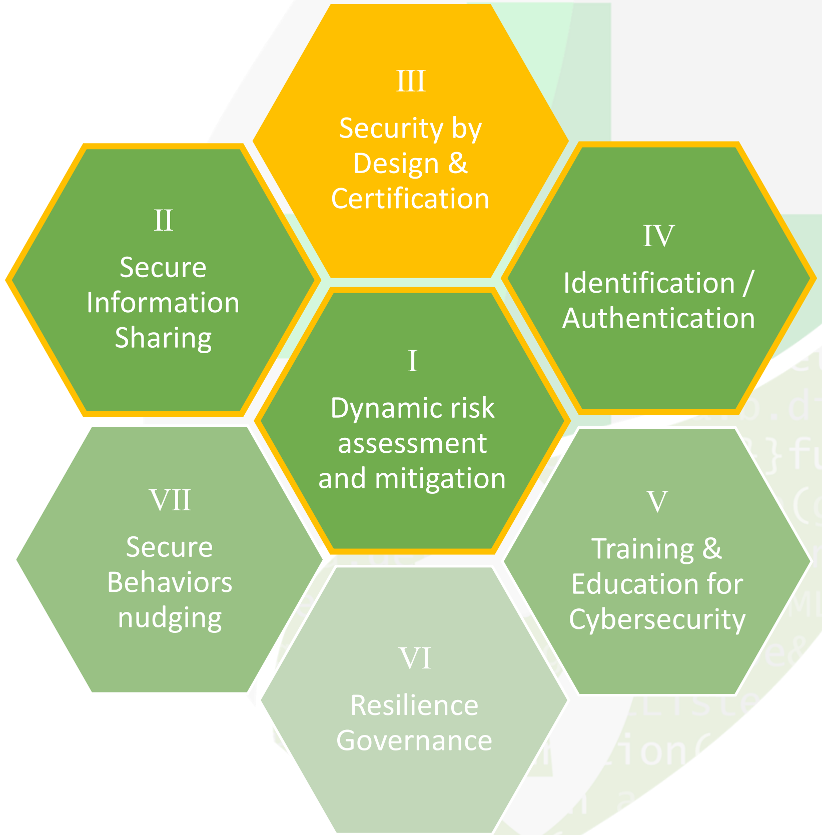
# Healthcare Sector context

- Lack of cyber awareness within healthcare sector
- Immediate and industrywide action
- Development of a programmatic approach to identification, mitigation, and remediation of risk
- Introduction of security aspects (cyber risk)

# PANACEA Project response

- **Security By Design Framework (SbDF),** takes into account a typical assessment and system monitoring audit workflow with the support of specific solutions addressing conformity assessment (through by compliance schemes, CST) and risk assessment (addressing cybersecurity and engineering aspects, SDSP)
  - **SDSP – Secure Design Support Platform**
  - **CST – Compliance Support Tool**


Panacea Ecosystem
People-centric cybersecurity in healthcare
System providers
Process
Clinical information systems, EHP, PHR
Security staff
Top management
Network
Citizen/Patient
Employee
System providers
Administrative information systems
Process
Operator
Citizen/Patient
III
Security by design & Certification
II
Secure information sharing
IV
Identification/ Authentication
I
Dynamic risk assessment and mitigation
VII
Secure behaviours nudging
V
Training & Education for cybersecurity
VI
Resilience governance
Toolkit
Public cloud services
Private cloud services
Citizen/Patient
Operator
Connected devices in and outside the hospital
Process
Device providers


III
Security by Design & Certification
II
Secure Information Sharing
IV
Identification / Authentication
I
Dynamic risk assessment and mitigation
VII
Secure Behaviors nudging
V
Training & Education for Cybersecurity
VI
Resilience Governance

# Security by Design Approach

Security-by-Design Framework (SbDF) has been proposed in order to overcome design limitations of medical devices and medical systems which currently don’t specifically or poorly include security engineering aspects regarding cyber risks.

**Security-by-design:** Approach to software and hardware development that seeks to make systems **as free of vulnerabilities and impervious to attacks as possible** through different measures such as continuous testing, authentication safeguards and adherence to best programming practices.

**Key point:** it is important for a device/system to be **designed from the foundations to be secure**. Therefore, good cyber security measures should be integrated into the design process

# Security by Design Approach

1. Context definition
2. Relevant standards/certification schemes identification
3. Standards mapping, gap analysis and extraction
4. Conformity assessment
5. Risk assessment

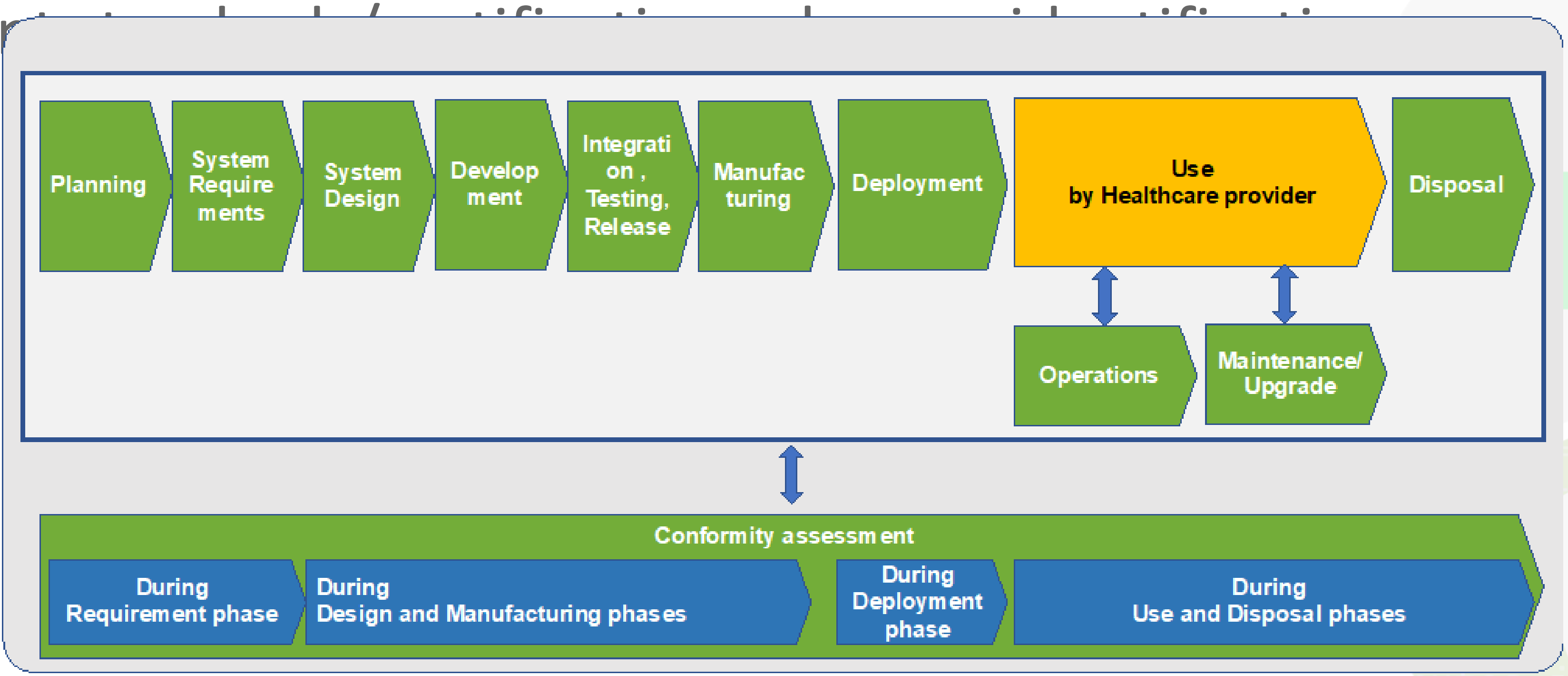
Liaison with ENISA analysis on potential candidates of cybersecurity certification schemes [1]

enisa
European Network
and Information
Security Agency

[1] STANDARDS SUPPORTING CERTIFICATION - Analysis of Standards in Areas Relevant to the Potential EU Candidate Cybersecurity Certification Schemes

# Security by Design Approach

1. **Context definition** **Healthcare Domain, Medical device Lifecycle**
2. Relevan
3. Standa
4. Confor
5. Risk as



[1] STANDARDS SUPPORTING CERTIFICATION - Analysis of Standards in Areas Relevant to the Potential EU Candidate Cybersecurity Certification Schemes

# Security by Design Approach

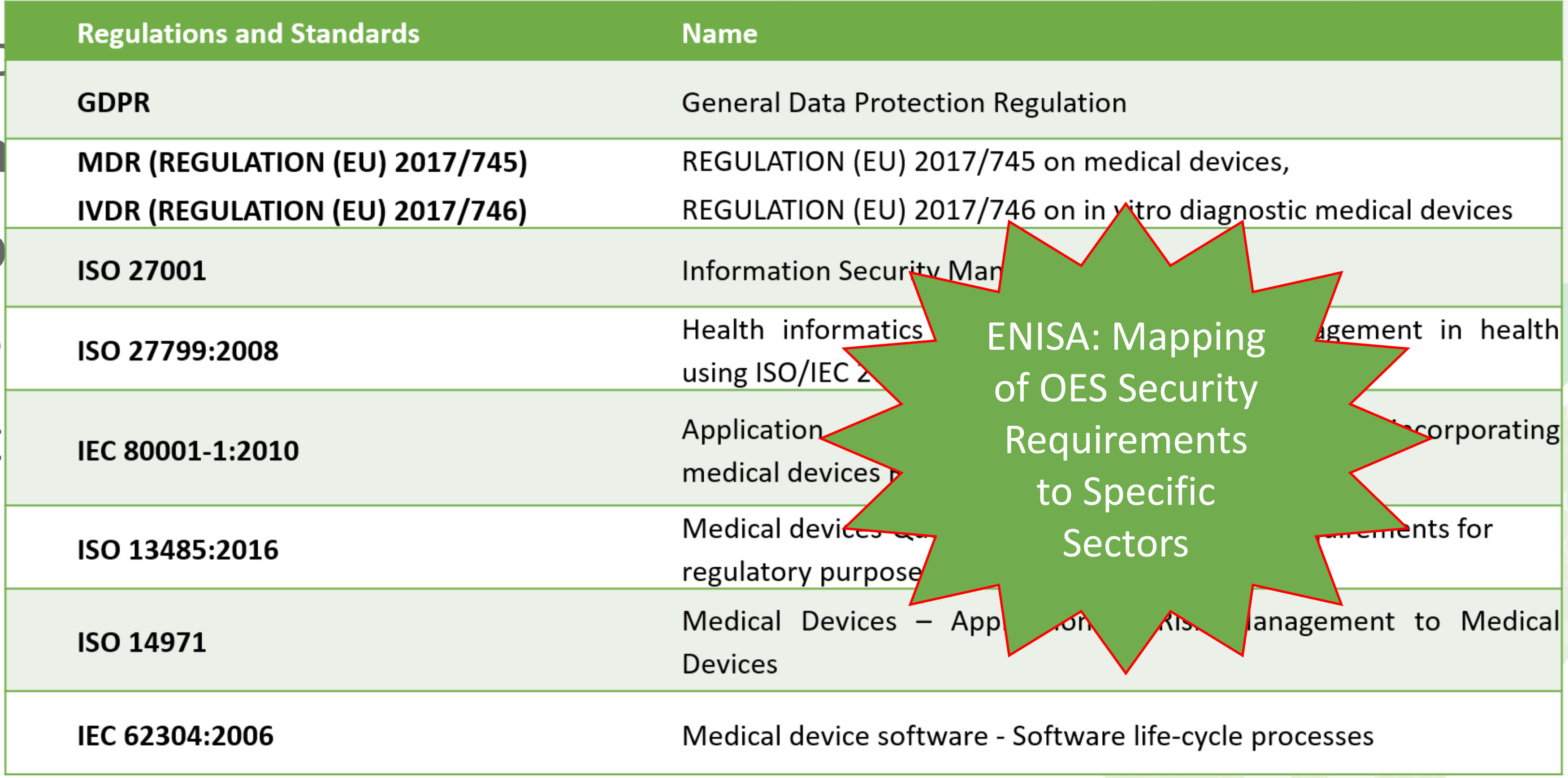
1. Context definitic
2. **Relevant standa**
3. Standards mapp
4. Conformity asse
5. Risk assessment

| Regulations and Standards | Name |
|---|---|
| **GDPR** | General Data Protection Regulation |
| **MDR (REGULATION (EU) 2017/745)**<br>**IVDR (REGULATION (EU) 2017/746)** | REGULATION (EU) 2017/745 on medical devices,<br>REGULATION (EU) 2017/746 on in vitro diagnostic medical devices |
| **ISO 27001** | Information Security Management |
| **ISO 27799:2008** | Health informatics – Information security management in health using ISO/IEC 27002 |
| **IEC 80001-1:2010** | Application of risk management for IT-networks incorporating medical devices Roles, responsibilities and activities |
| **ISO 13485:2016** | Medical devices-Quality management systems-Requirements for regulatory purposes |
| **ISO 14971** | Medical Devices – Application of Risk Management to Medical Devices |
| **IEC 62304:2006** | Medical device software - Software life-cycle processes |

[1] STANDARDS SUPPORTING CERTIFICATION - Analysis of Standards in Areas Relevant to the Potential EU Candidate Cybersecurity Certification Schemes

# Security by Design Approach

1. Context definitic
2. **Relevant standa**
3. Standards mapp
4. Conformity asse
5. Risk assessment



| Regulations and Standards | Name |
|---|---|
| **GDPR** | General Data Protection Regulation |
| **MDR (REGULATION (EU) 2017/745)**<br>**IVDR (REGULATION (EU) 2017/746)** | REGULATION (EU) 2017/745 on medical devices,<br>REGULATION (EU) 2017/746 on in vitro diagnostic medical devices |
| **ISO 27001** | Information Security Man |
| **ISO 27799:2008** | Health informatics ... gement in health using ISO/IEC 2 |
| **IEC 80001-1:2010** | Application ... corporating medical devices i |
| **ISO 13485:2016** | Medical devices Q ... rements for regulatory purpose |
| **ISO 14971** | Medical Devices – App ... on ... Ris ... anagement to Medical Devices |
| **IEC 62304:2006** | Medical device software - Software life-cycle processes |

ENISA: Mapping of OES Security Requirements to Specific Sectors

[1] STANDARDS SUPPORTING CERTIFICATION - Analysis of Standards in Areas Relevant to the Potential EU Candidate Cybersecurity Certification Schemes

# Security by Design Approach

1. Context definition
2. Relevant standards/certifi
3. **Standards mapping, gap a**
4. Conformity assessment
5. Risk assessment

- **Standards Harmonization**
- **Checklist** extraction:
  the most relevant articles in terms of cybersecurity were extracted in order to define checklists useful to guide the user to assess conformities
- **Taxonomies** extraction:
  assets/vulnerabilities/threats/security controls/scenarios extraction

[1] STANDARDS SUPPORTING CERTIFICATION - Analysis of Standards in Areas Relevant to the Potential EU Candidate Cybersecurity Certification Schemes

# Security by Design Approach

1. Context definition
2. Relevant standards/certification schemes identification
3. Standards mapping, gap analysis and extraction
4. **Conformity assessment**
5. Risk assessment

**CST: Compliance Support Tool**

[1] STANDARDS SUPPORTING CERTIFICATION - Analysis of Standards in Areas Relevant to the Potential EU Candidate Cybersecurity Certification Schemes

# Security by Design Approach

1. Context definition
2. Relevant standards/certification schemes identification
3. Standards mapping, gap analysis and extraction
4. Conformity assessment
5. **Risk assessment**

**SDSP: Secure Design Support Platform**

[1] STANDARDS SUPPORTING CERTIFICATION - Analysis of Standards in Areas Relevant to the Potential EU Candidate Cybersecurity Certification Schemes

# PANACEA Security-by-design Framework

From a technological point of view, the **PANACEA Security-by-design Framework** is composed of two solutions

## Secure Design Support Platform (SDSP)

It will support the security of a medical device/information system in development, by providing a software platform for risk assessment analysis over the system/software in development. Each risk assessment analysis may produce security controls that will lead to new requirements to be embedded in the system in order to improve its resulting security

## Compliance Support Tool (CST)

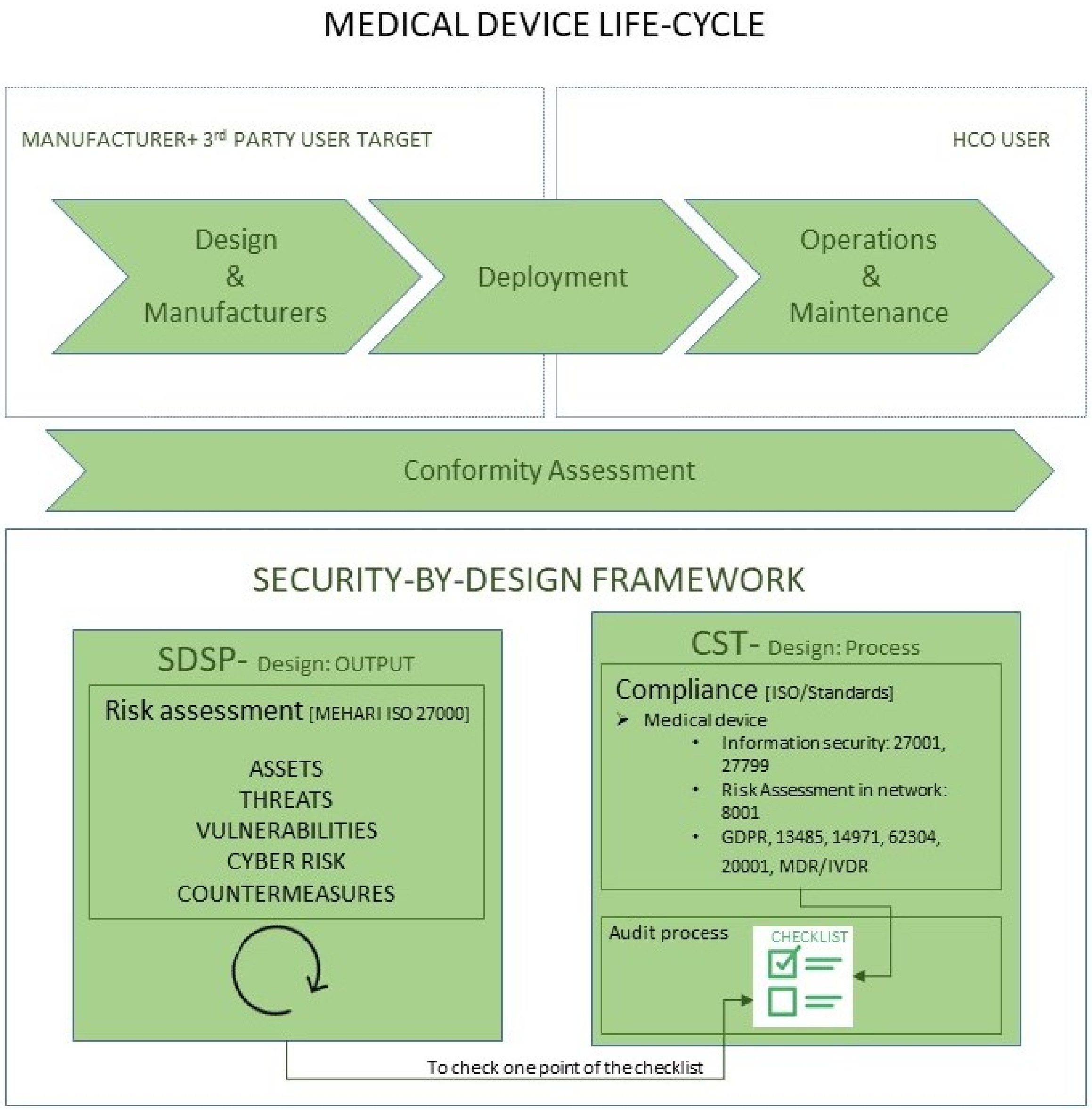
It will support the quality assurance process during the whole lifecycle of a medical device/system, in order to put in place an assessment audit of the process supporting health devices/systems providers/quality responsible, ensuring compliance to current standards in the health sector.

# PANACEA Security-by-design Framework

- Introduction of security aspects (cyber risk) since the beginning of the initial design process: from requirements phase to deployment phase and till the operational phase

- Design PROCESS: The CST covers the compliance through the whole process.

- Design contextualized OUTPUT: The SDSP supports the user to perform the risk assessment in each phase of medical device life-cycle.



MEDICAL DEVICE LIFE-CYCLE

MANUFACTURER+ 3rd PARTY USER TARGET

HCO USER

Design & Manufacturers

Deployment

Operations & Maintenance

Conformity Assessment

SECURITY-BY-DESIGN FRAMEWORK

SDSP- Design: OUTPUT

Risk assessment [MEHARI ISO 27000]

ASSETS
THREATS
VULNERABILITIES
CYBER RISK
COUNTERMEASURES

CST- Design: Process

Compliance [ISO/Standards]

- Medical device
  - Information security: 27001, 27799
  - Risk Assessment in network: 8001
  - GDPR, 13485, 14971, 62304, 20001, MDR/IVDR

Audit process

CHECKLIST

To check one point of the checklist

# Innovation points

- Development of a tool (CST) that will support the user to verify the compliance to standards relevant for cyber security during the whole life-cycle of a medical device or eHealth application;
- Development of a tool (SDSP) that will provide a risk-based approach to refine the security controls of a medical device/system during its development;
- Extraction of taxonomies (vulnerabilities/threats/security controls) from health care most relevant standards in order to take into consideration during risk assessments scenarios specific for this sector;
- Security-by-design principles support through the analysis of the security level/scenarios will support manufacturers in decision-making of possible security controls to implement during software/system engineering early phases;
- Security-by-design Framework takes into consideration the ENISA approach and guidelines for the analysis of potential candidates of certification schemes.