Panacea

People-centric cybersecurity in healthcare

PANACEA PAC WORKSHOP
Joint Value proposition
[PANACEA Healthcare Cybersecurity Advisory Services]

4 May 2021

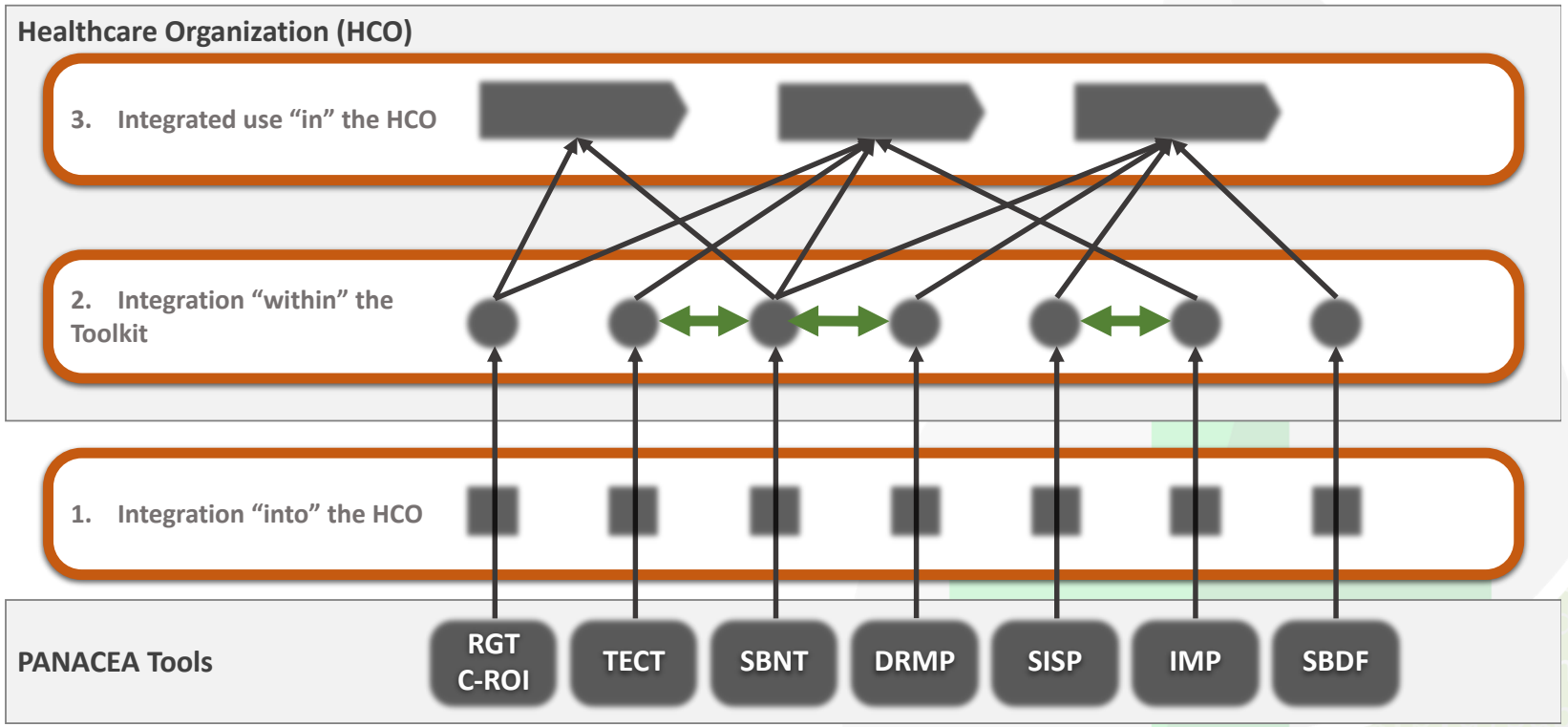
Pasquale Mari
FPG

Funded by the European Union's Horizon 2020
Research and Innovation Programme, under Grant Agreement no 826293

Panacea
People-centric cybersecurity in healthcare

Rationale for a Joint Value Proposition

Joint exploitation as a Consortium is based on **two assets**:

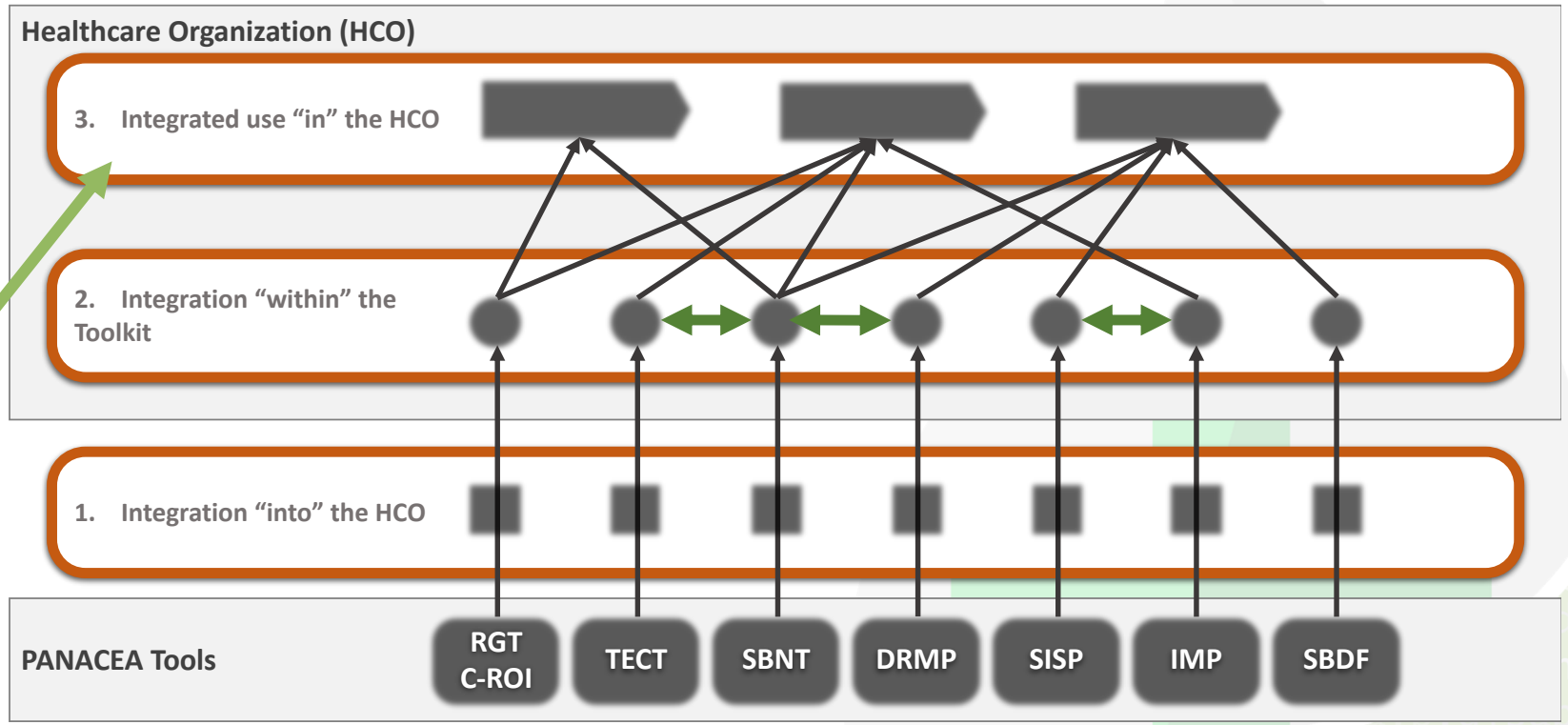


Panacea
People-centric cybersecurity in healthcare

Rationale for a Joint Value Proposition

Joint exploitation as a Consortium is based on **two assets**:

- The **PANACEA Toolkit may be used in an integrated manner**.

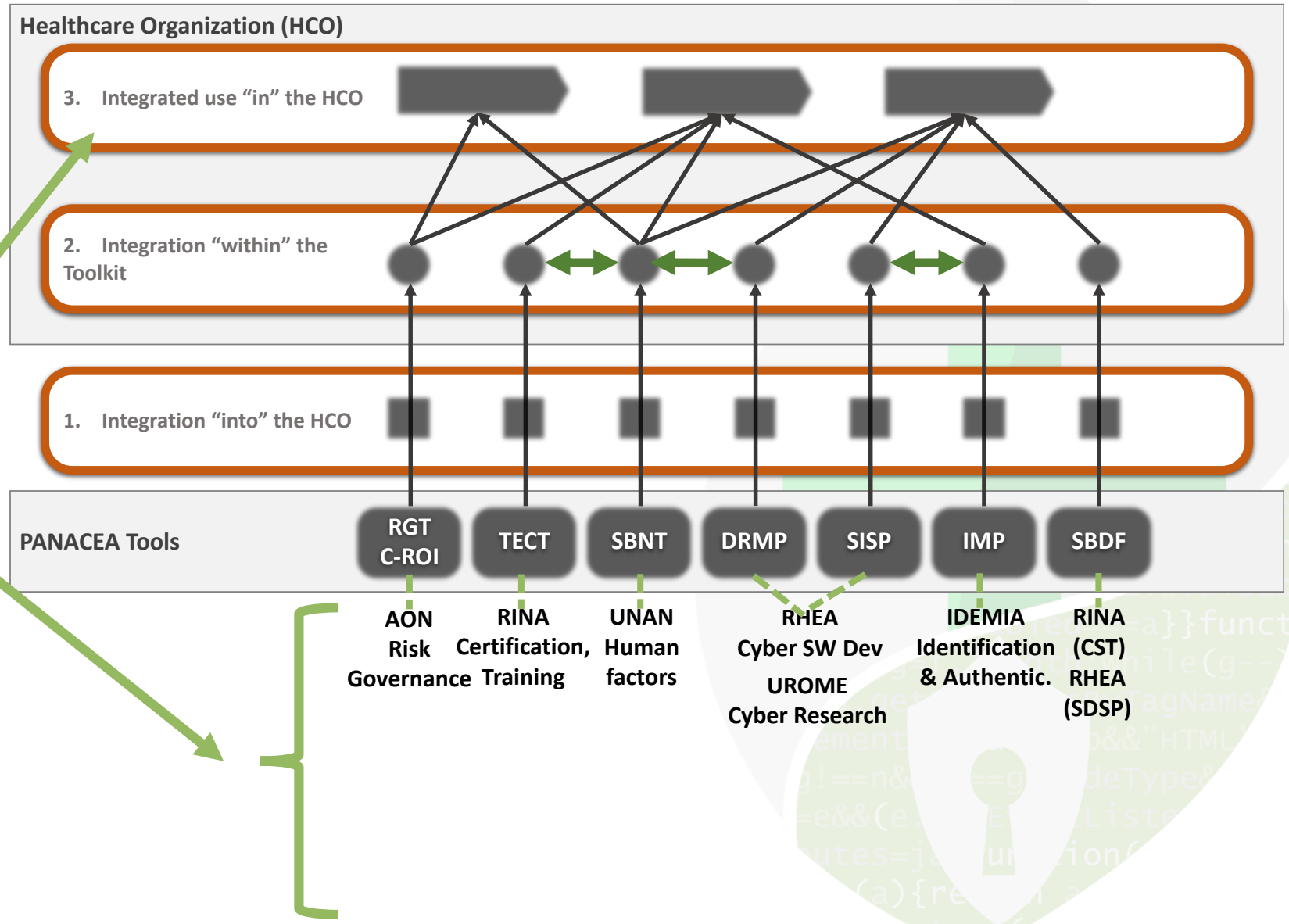


Panacea
People-centric cybersecurity in healthcare

Rationale for a Joint Value Proposition

Joint exploitation as a Consortium is based on **two assets**:

- The **PANACEA Toolkit may be used in an integrated manner**.
- The **PANACEA Consortium includes a collection of multidisciplinary complementary domains of expertise**, including first-hand knowledge of healthcare operational and cybersecurity context.

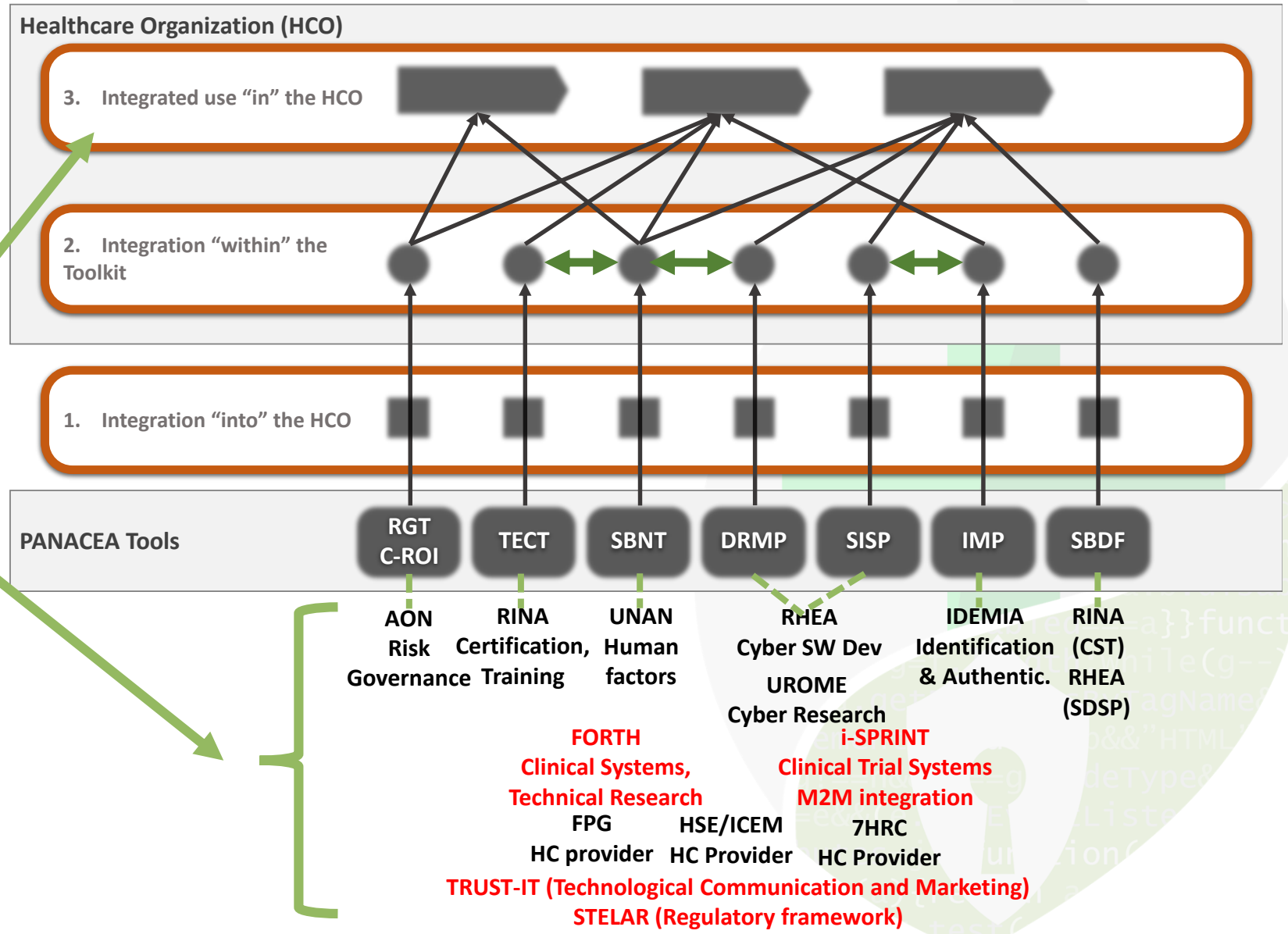


Panacea
People-centric cybersecurity in healthcare

Rationale for a Joint Value Proposition

Joint exploitation as a Consortium is based on **two assets**:

- The **PANACEA Toolkit may be used in an integrated manner**.
- The **PANACEA Consortium includes a collection of multidisciplinary complementary domains of expertise**, including first-hand knowledge of healthcare operational and cybersecurity context.



Business model principles

- Consortium Partners sign a commercial agreement or create a formal entity

PHCAS-PANACEA Healthcare Cybersecurity Advisory Services

- PHCAS has the mission to jointly exploit the expertise and the tools developed during the PANACEA project.
- PHCAS

Provides assessment, certification and advisory services, based on the Partners' multidisciplinary capability, to Healthcare Organizations, in the cybersecurity domain

- PHCAS delivers the services through the Partners, using one or more of the PANACEA Tools
- PHCAS services include the support to the Healthcare Organization in using the PANACEA tools in an integrated manner

Initial Services Portfolio

Service
A. **In Depth Assessment** **B.** **Wide spectrum compliance check** **C.** **Risk Management Capacity Building** **D.** **Staff awareness raising** **E.** **Assistance to Integrated PANACEA toolkit use**

Panacea
People-centric cybersecurity in healthcare

Service A

Service	Content and delivery modality	Output and Benefit for the Client
A. **In Depth Assessment**	The service is a one-off service, articulated in two steps, providing **1) Assessment of the vulnerabilities** of the Hospital from the cybersecurity point of view and its **cybersecurity readiness, for systems, medical devices and staff.** Its scope includes: • Maturity of the Governance Processes (RGT) • Maturity of Governance Organization (RGT) • Quality of procurement process from the cybersecurity point of view (SbDF) • Vulnerabilities of network and related human layer (DRMP+SBNT) • Staff vulnerability to phishing (FPG expertise) • Strength of Identification & Authentication measures (IDEMIA expertise) • Cybersecurity of Medical Devices (SbDF) **2) Definition of a prioritized portfolio of measures** (also based on DRMP) and an estimate of the investment needed to raise the compliance level (C-ROI). PHCAS team works with an internal client team; PHCAS sets-up with the client the emulation environment to apply the DRMP on areas deserving specific in depth analysis; PHCAS team uses PANACEA tools to perform the assessment. Contract agreement may be: • One-off, fixed price • Fixed price Subscription, including periodical assessment and a yearly amount of person days that the client can use for support in implementing the portfolio	**Output** The client gets a **Repor**t including • an **assessment** covering • all “targets” (applications, medical devices, network, staff) • the measures to protect the ”targets” • a **set of recommended and prioritized improvement measures**, and an indication of the **required investment** **Benefit** The benefit for the client is to get a complete and “in depth” picture of its compliance level and vulnerabilities, allowing to **plan a consistent and optimal portfolio of interventions**

Panacea
People-centric cybersecurity in healthcare

Service B

Service	Content and Delivery modality	Output and Benefit for the Client
B. Wide spectrum compliance check	The service is a one-off service, articulated in three steps, providing: 1) a check of the compliance of the Hospital vs the more diffused cybersecurity standards and to the certification schemes or indications from EU/National authorities relevant for the client 2) recommendations on how to fill the gaps 3) assistance in implementing the recommendations The first step is performed by RINA, based on a Certification scheme developed during the PANACEA project Second and third steps are delivered by a wider team, including the PHCAS partners relevant w.r.t. the result of the first step Contract agreement may be: • One-off, fixed price	**Output** The client gets a **Repor**t including the recommendations to reach compliance. The client also gets multidisciplinary advice on how to implement the recommendations **Benefit** The benefit for the client is to be **prepared to pass certification** (e.g. Joint Commission International) and/or **satisfy requests/indications from EU/National bodies** (e.g. NIS, Procurement Guidelines for Cybersecurity In Hospitals)

Panacea
People-centric cybersecurity in healthcare

Service C

Service	Content and Delivery modality	Output and Benefit for the Client
C. Risk Management Capacity Building	The service is a one-off service, articulated in four steps, providing: 1) Assessment of current capacity, through assessment of • Maturity of the Governance Processes (RGT) • Maturity of Governance Organization (RGT) • Skill assessment (based on results from other EU projects participated by PANACEA Partners) 2) Recommendations on how to fill the gaps 3) Assistance in implementing the recommendations in terms of (if applicable) • Governance Organization model upgrade (RGT) • Adoption of relevant PANACEA tools (C-ROI, DRMP, SbDF, SBNT, TECT) based on the Implementation Guidelines developed during the PANACEA project • Staff competency building/strengthening (based on results from other EU projects participated by PANACEA Partners) 4) Assistance until the capability is sufficiently acquired. The first step is performed mainly by AON (based on RGT) and RHEA Remaining steps are delivered by a wider team, including the PHCAS partners relevant wrt the result of the first step Contract agreement may be: • One-off, fixed price	**Output** The client gets a **Report** including the recommendations to set-up/upgrade the capability. The client also gets multidisciplinary advice on how to implement the recommendations **Benefit** The benefit for the client is to **rapidly set-up a cybersecurity management capability**

Service D

Service	Content and Delivery modality	Output and Benefit or the Client
D. **Staff awareness raising**	The service is a one-off service, articulated in four steps, providing: 1) Assessment of current awareness through • Identification of weakness topics and target population (SBNT) • Staff vulnerability to phishing (FPG expertise) 2) Design/Customization of applicable solutions (SBNT, TECT, IMP H2M, SISP) 3) Implementation of designed solutions 4) Result evaluation (TECT) and recommendation on how to stabilize or improve the results obtained. The first step is performed mainly by UNAN with the support of FPG Remaining steps are delivered by a wider team, including the PHCAS partners relevant wrt the result of the first step. The clients sets-up a team (at least CISO+HR) to drive the service Contract agreement may be: • One-off, fixed price • One-off, fixed price+ success fee (related to the awareness improvement reached, as assessed by the evaluation step)	**Output** The client gets a **Repor**t on the current status of cybersecurity awareness The client also gets design and implementation of measures **Benefit** The benefit for the client is to **rapidly improve staff awareness**

Service E

Service	Content and Delivery modality	Output and Benefit or the Client
E. Assistance to Integrated PANACEA toolkit use	In case the client has already adopted all (or most of) Panacea tools, this service consists assisting the client in their combined use. Examples of integrated use cases include: • To cope with frequent selection and deployment of new technology • To limit human errors due to multi-use and time pressure • To ensure secure Smart-working • To decide cybersecurity investments • To contrast stream of fake pandemic related messages • To ensure secure rapid on-boarding of new staff in clinical activities • To ensure secure Telemedicine • To ensure secure upgrade to sanitary purposes of non-sanitary host structures In general, the service is delivered by a team involving many PHCAS partners The clients sets-up a team to drive the service. Contract agreement may be: • One-off, fixed price, every time the intervention is required • Fixed price Subscription, including a yearly amount of person days that the client can use to get the services when needed	**Output** The client gets an end-to-end service to cope with recurrent problems **Benefit** Benefit for the client is to **do best use of PANACEA toolkit** to cope a variety of **situations requiring a multidimensional approach**