



Space Cybersecurity Digital Consulting

Information security management
Information system audit
Risk management
Security system design





PRIAMOS

An efficient methodology to manage
space cybersecurity risks

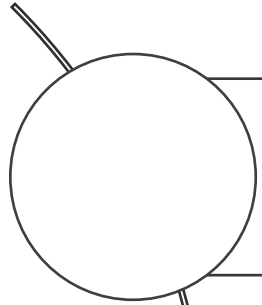
24 April 2024

FOURTH EDITION

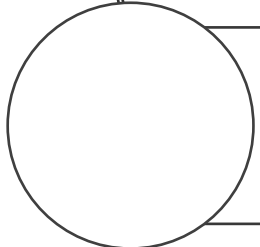
CYSAT[®]

PARIS 2024

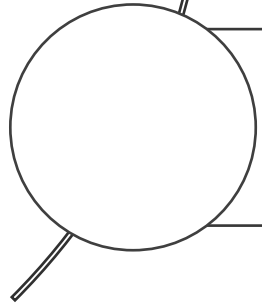
Agenda



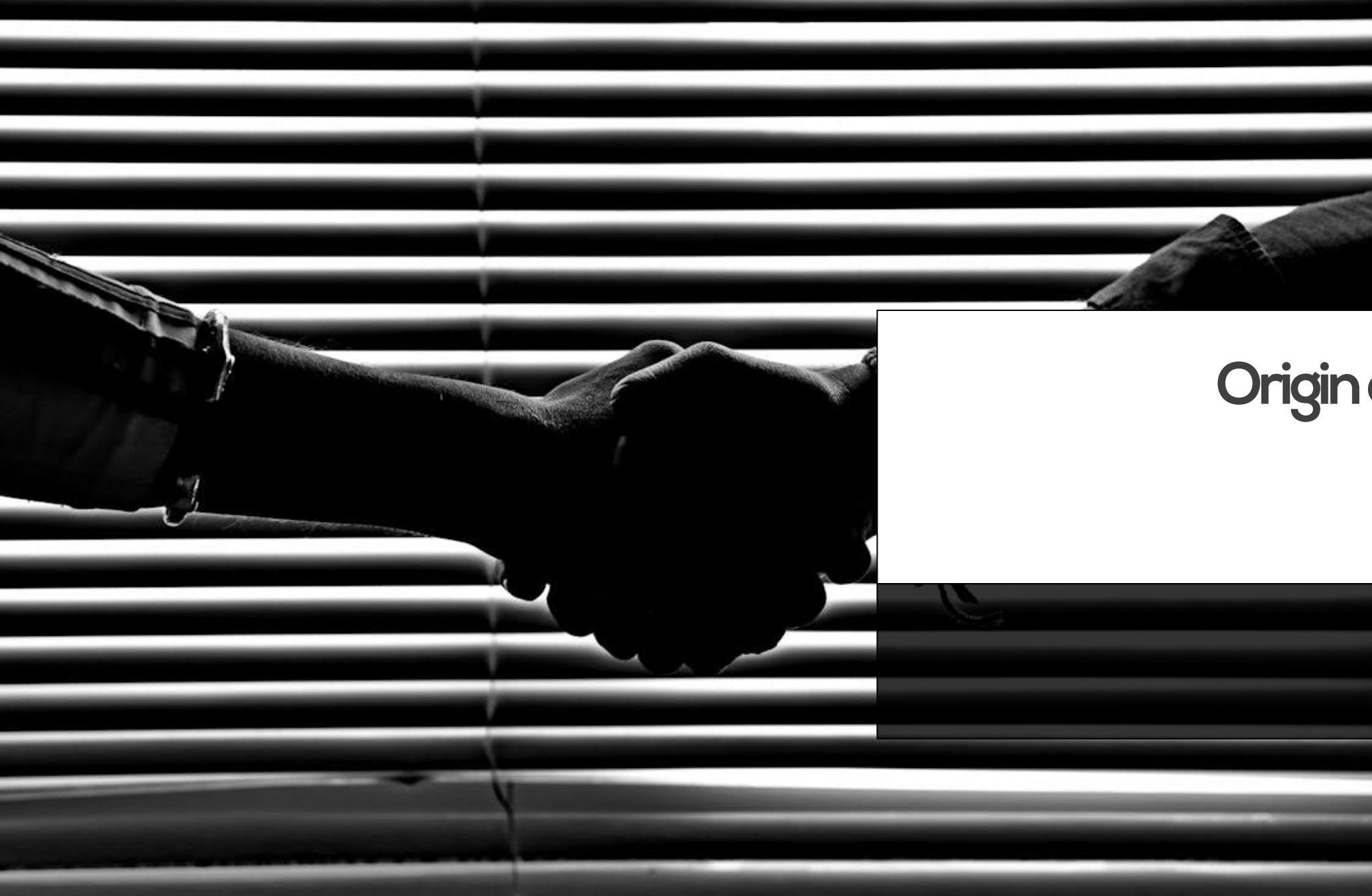
Origin of the project



EBIOS RM methodology



Case study for space industry



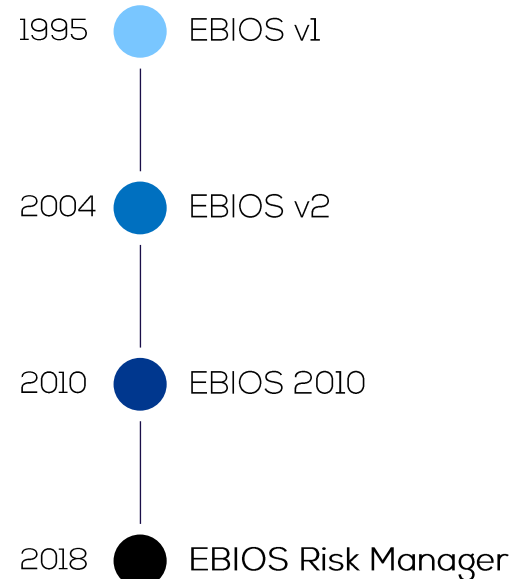
Origin of the project

The origin of the project

EBIOS Risk Manager
Published by National Cybersecurity
Agency of France (ANSSI) with the
support of Club EBIOS.

A risk management method, result
of almost 30 years of evolution

The need:
Complete the study cases
available for EBIOS RM with an ICS
study case.



Club EBIOS has published a call
for tenders last summer to:

- Create a realistic ICS study
case
- Illustrate the complexity and
the problematics faced by ICS
with regards to risks handling
- Show why EBIOS RM is a
relevant method to use

Why us?

Priamos

- **Priamos is a consulting and expertise firm**
 - Protection of information assets
 - Protection of personal information
 - Protection of classified defense information
- **Based at Toulouse, France**
- **Founded and owned by Etienne Gérain, cybersecurity expert for space industry**

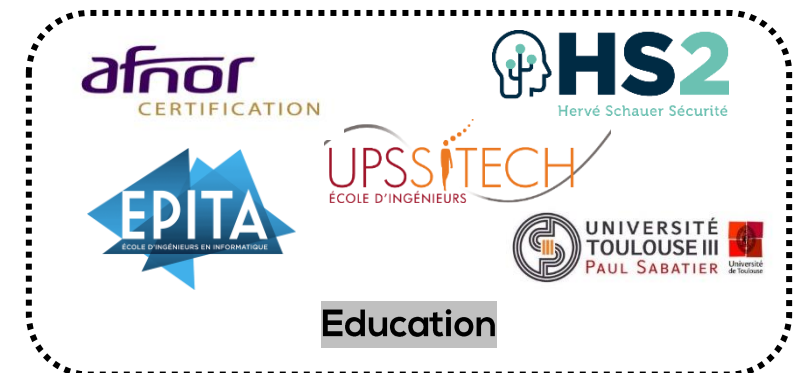
Professional associations



Specialised in security of industrial and defense systems

- **Fields of expertise**
 - **Organization:** Entreprise security and business continuity
 - **Cybersecurity:** Enterprise and industrial systems
 - **Regulatory compliance:** Privacy and Defense
- **Management and technical expertise**
 - Information system security **risk management**
 - Information system security **accreditation**
 - **Executive**, security organization & management systems
 - **Security of architectures** related to information systems
 - **Secure configuration** of hardware and software devices

Clients and partners in industrial sectors and education





Key points on EBIOS RM methodology

EBIOS Risk Manager (EBIOS RM)



Overview

Method and toolbox adaptable for assessing and treating digital risks

Published by National Cybersecurity Agency of France (ANSSI) with the support of Club EBIOS

Compatible with the reference standards in terms of risk management: ISO 27005:2022

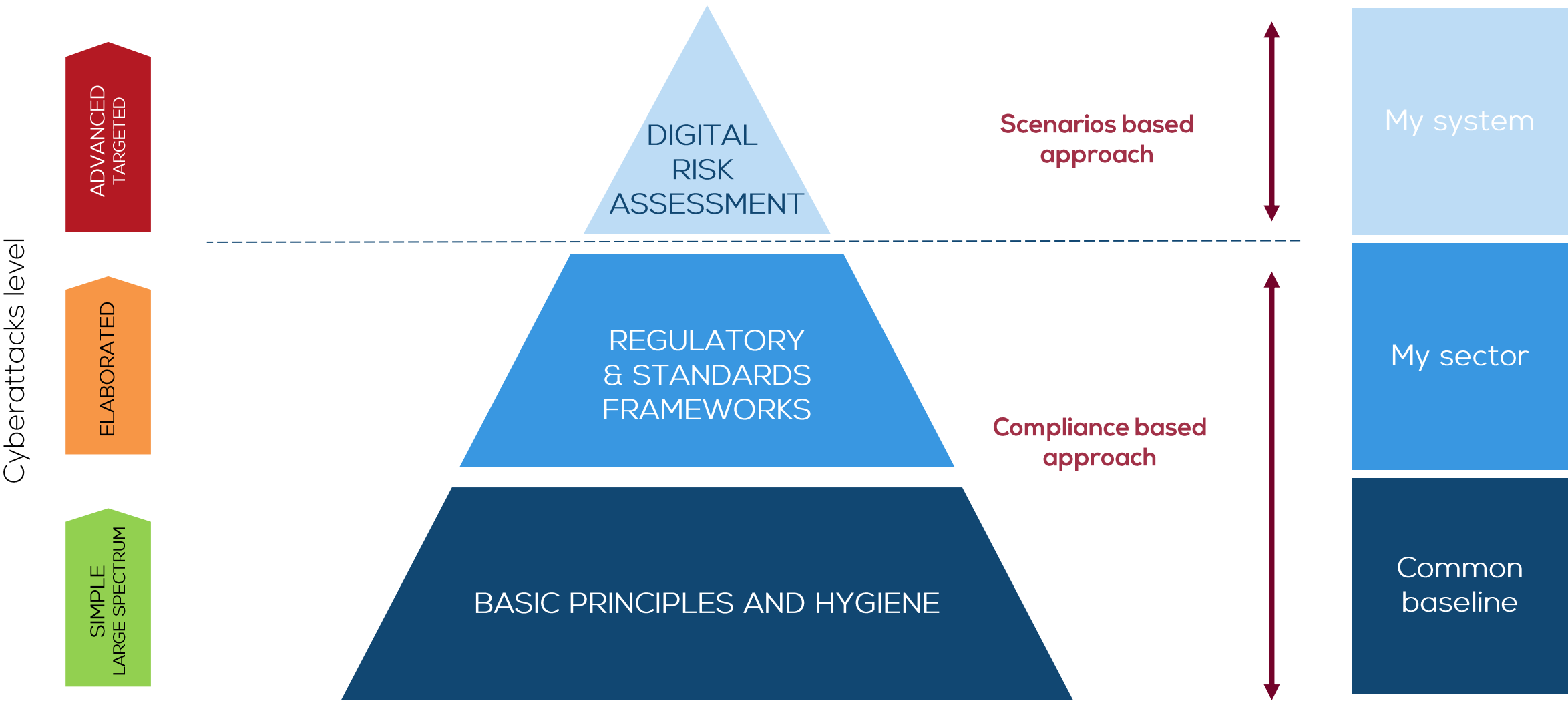
EBIOS RM: What for?

- Setting up or reinforcing a management process of the digital risk within an organization;
- Assess and treat the risks relating to a digital project
- Define the level of security to be achieved for a product or service

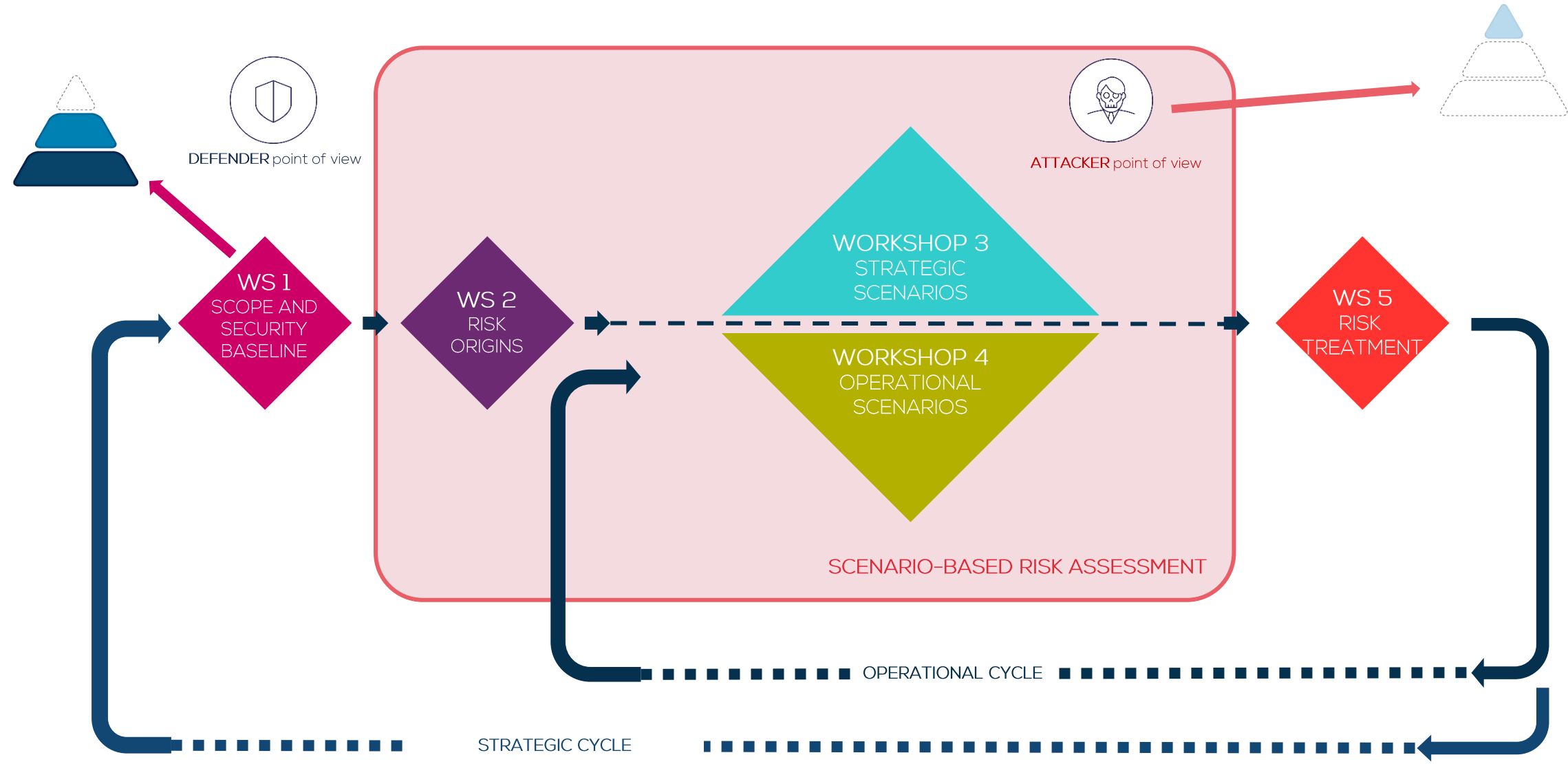
Applicability

For all (private or public organizations, all sectors, sizes etc.)

EBIOS RM: How this method combines compliance and risk scenarios

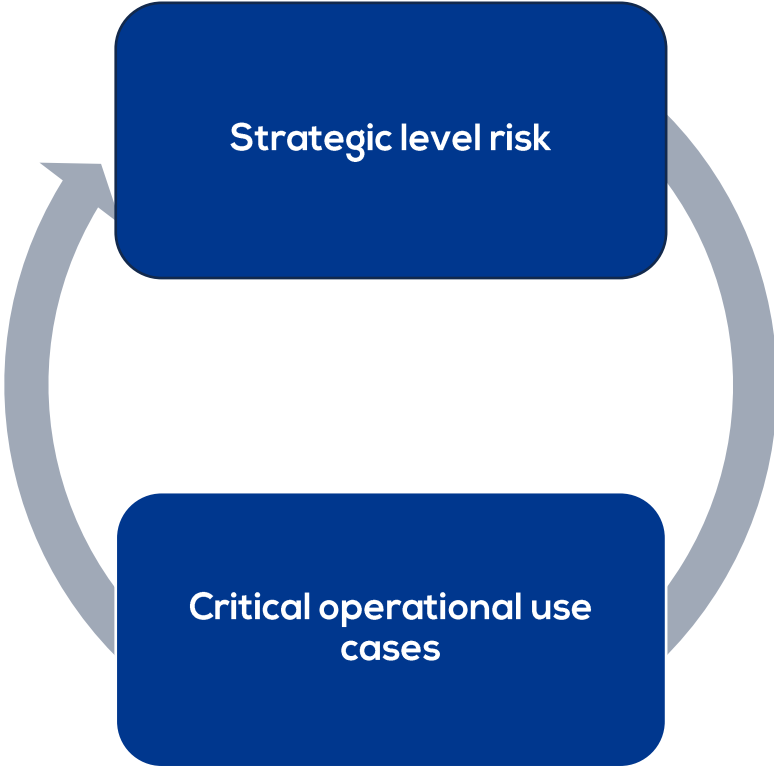


EBIOS RM: Collaborative and agile workshop approach



EBIOS RM:Tailorable for different needs

TARGET OF THE STUDY	MAIN WORKSHOPS TO BE CONDUCTED OR USED				
	1	2	3	4	5
Be in compliance with the digital security reference standards	X				X
Assess the threat level of the ecosystem with respect to the object studied			X		
Identify and analyse the high-level scenarios, integrating the ecosystem		X	X		
Conduct a preliminary risk study in order to identify the priority axes for security improvement	X	X	X		X
Conduct a complete and fine risk study, for example on a security product or for the purpose of a system accreditation	X	X	X	X	X
Direct a security audit and in particular a penetration test			X	X	
Direct the detection and reaction systems, for example at the level of a security operating centre (SOC)			X	X	
Orient crisis management procedures and business continuity plan	X		X	X	



EBIOS RM: Addressing all types of strategic digital risks

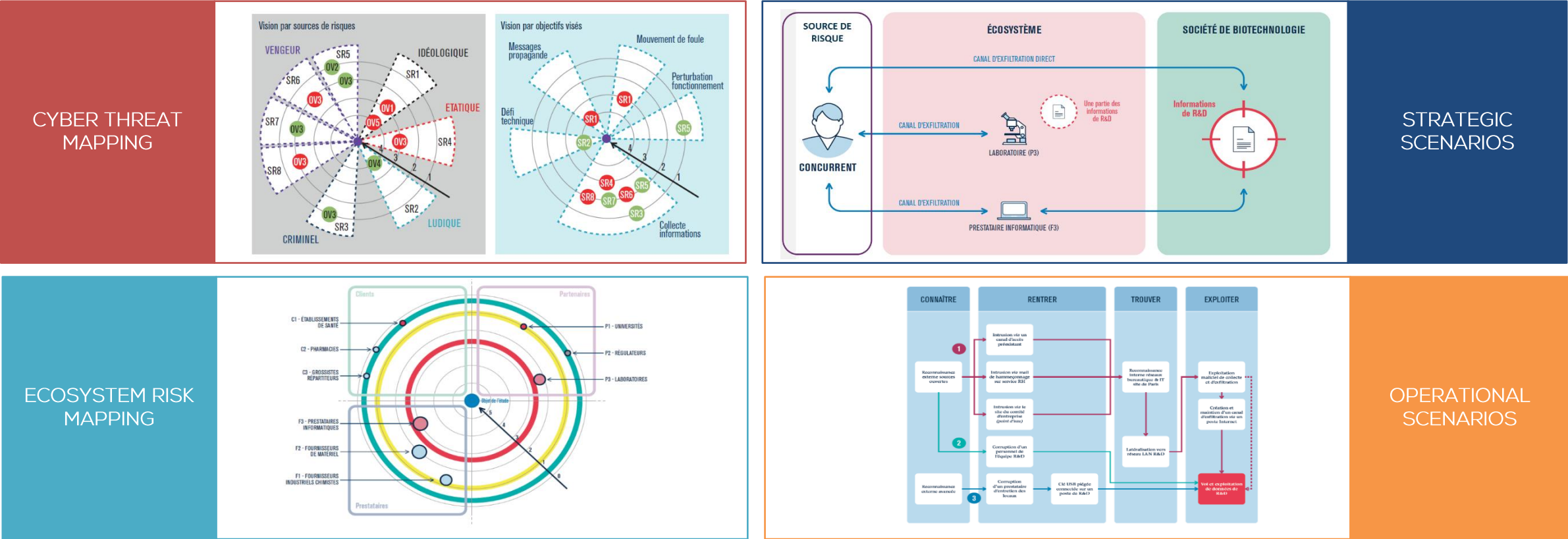
- Disruption of activity, denial or loss of service
- Sabotage, destruction of critical resources
- Human, material or environmental impacts

- Fraud, falsification
- Abuse of use, identity alteration or theft

- Data or intellectual property theft
- Espionage, Economic intelligence

- Activism, agitation, propaganda
- Influence, destabilization, damage to image or reputation
- Strategic pre-positioning

EBIOS RM: Understandable deliverables at each step



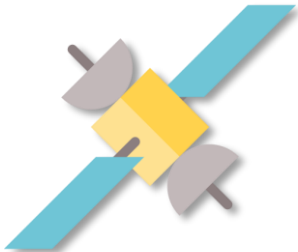
Critical systems/activities using EBIOS RM



5G digital risk assessment



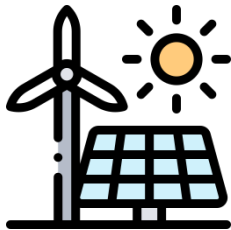
French Covid-19 management IS



Galileo GNSS



Air transport
Cybersecurity



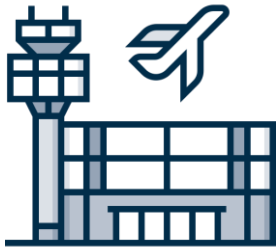
Energy sector Essential IS
identification



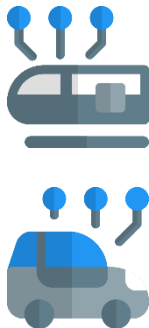
Supply chain security
for defence critical
assets



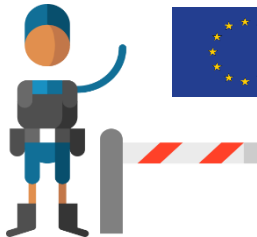
CyberNB CI-SOC
reference method



Airspace surveillance and territorial
integrity



Autonomous
connected vehicles



EU external borders
protection



Case study for space industry

The case study : The space system CHEM-ICS

Mission of the system

- Control the pesticide concentration on the ground
- Real time system
- Provision of reports and maps representing the concentration of the pesticides studied

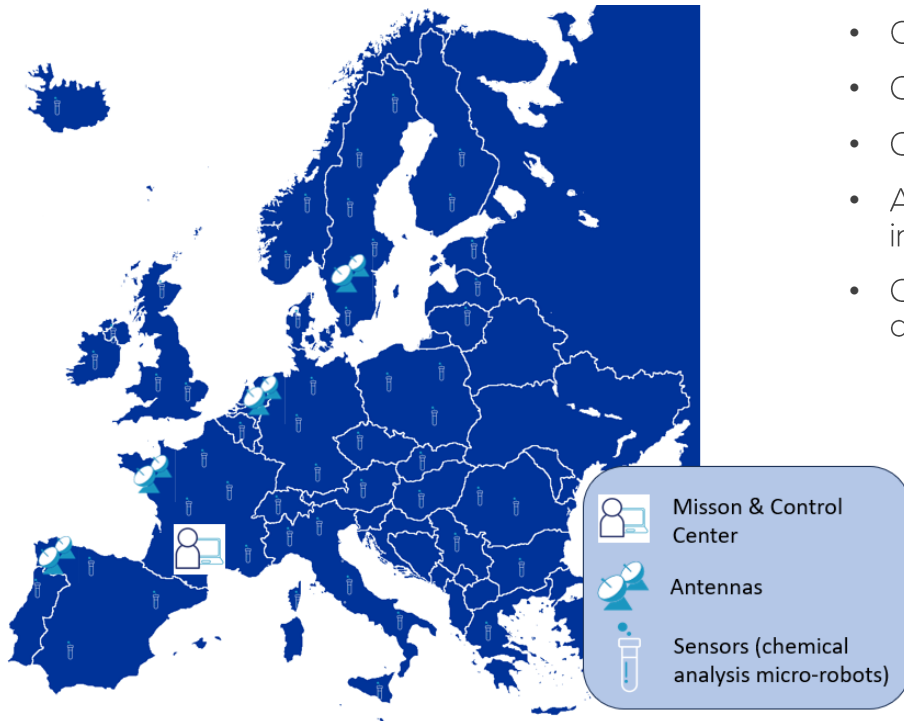
Challenges

- Ensure the operability of the constellation
- Ensure data freshness
- Maximize the number of clients
- Guarantee data integrity

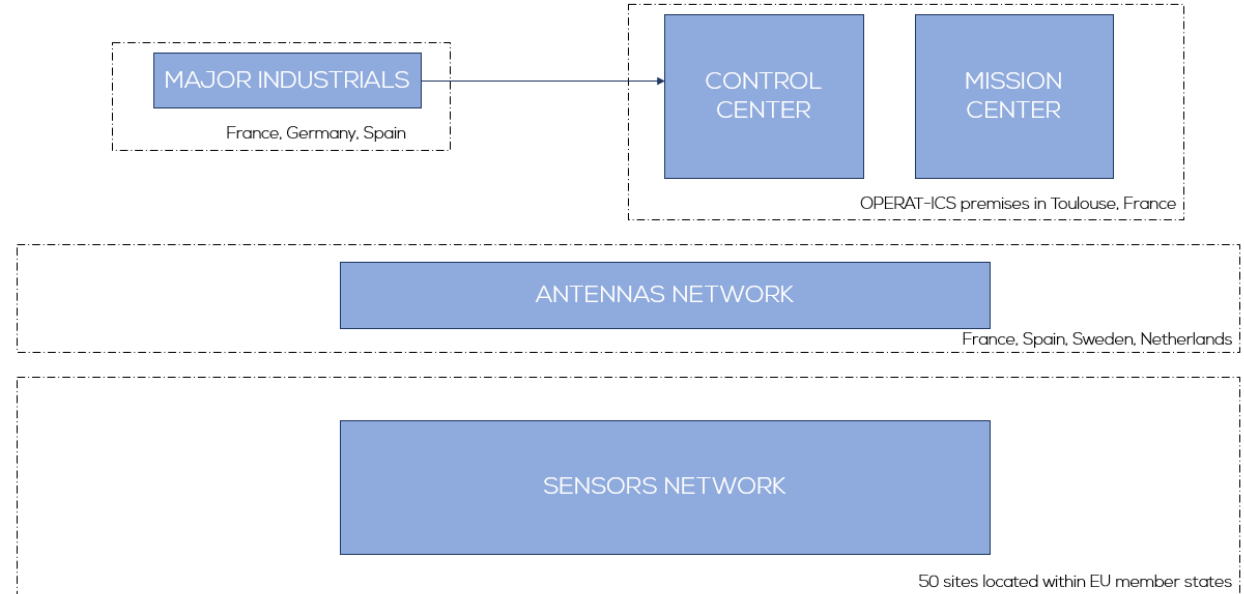
Composition

- Space segment
- Ground segment
 - Control Center
 - Mission Center
 - Antennas
 - Sensors

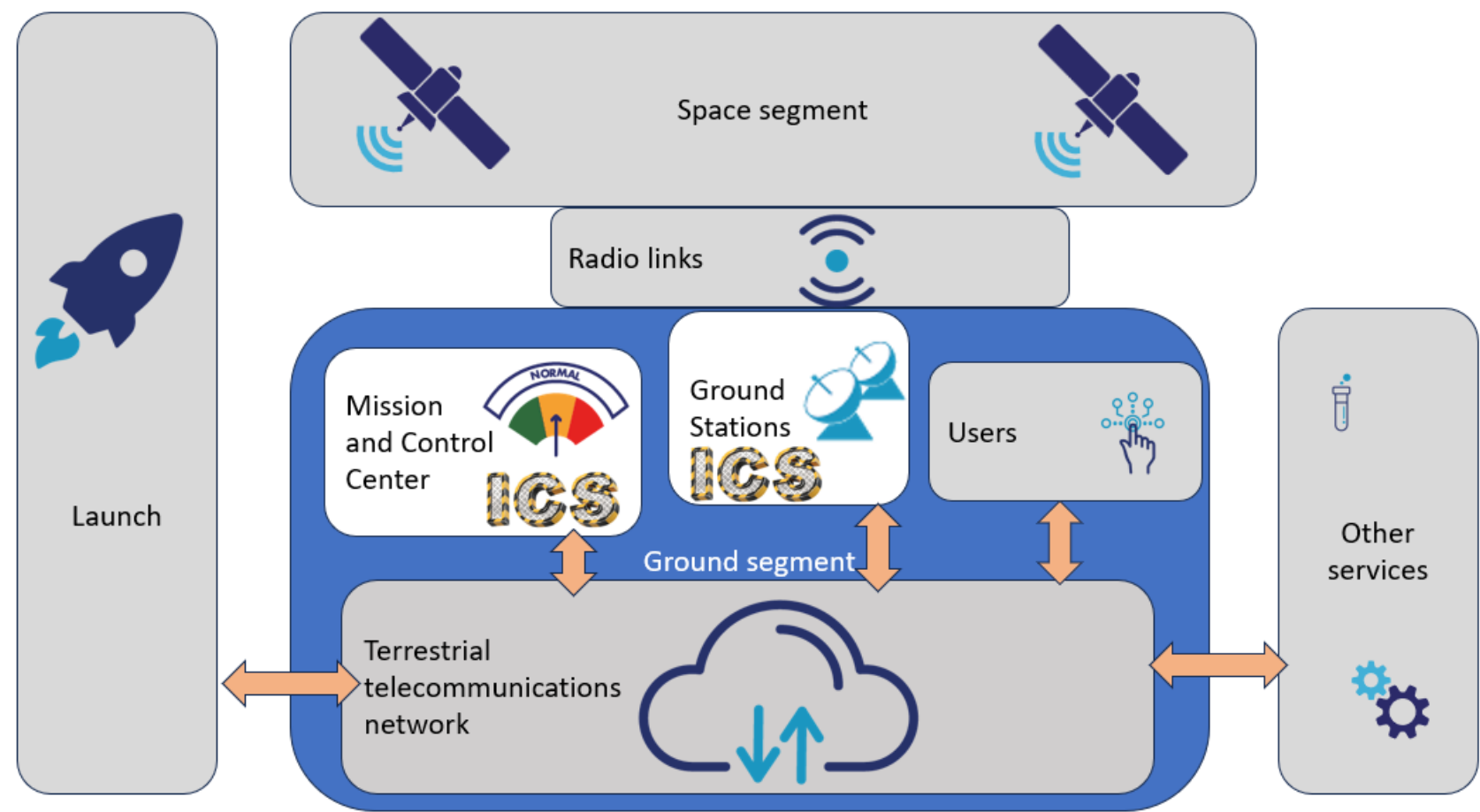
Ecosystem and hosting entities



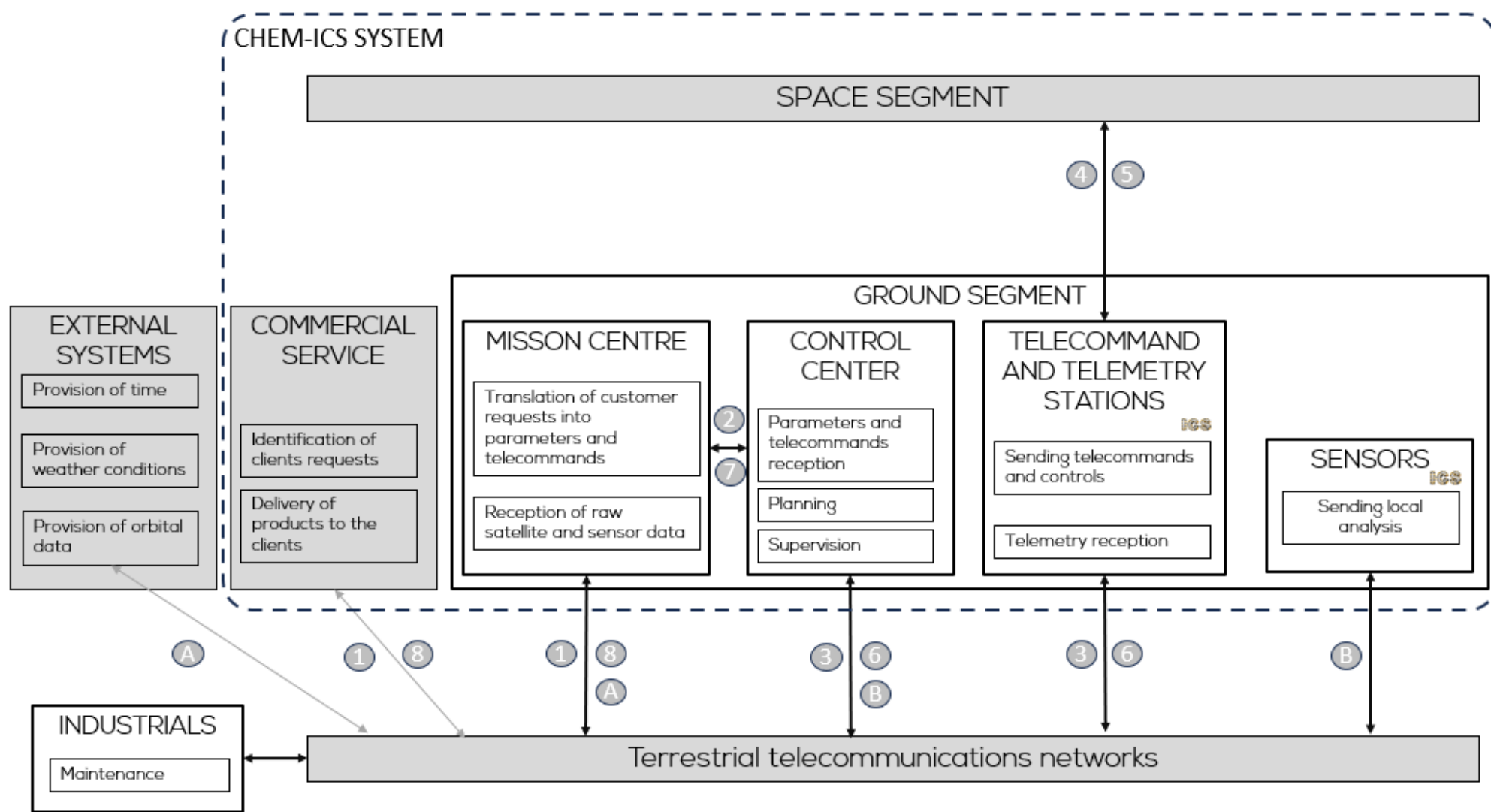
- AGRONOM-ICS: Owner of the CHEM-ICS system, Marketing of services.
- OPERAT-ICS: Operator of the CHEM-ICS system.
- CONSULT-ICS: Design, initial technical specifications, Consulting Architect
- CONSORT-ICS: Detailed Design, Realization, Deployment, Maintenance.
- ANTENN-ICS: Development, production, maintenance of ground antennas system for the space industry
- CHEMIROB-ICS: Development, production and distribution of microrobot systems and chemical analysis automation systems, Software developments



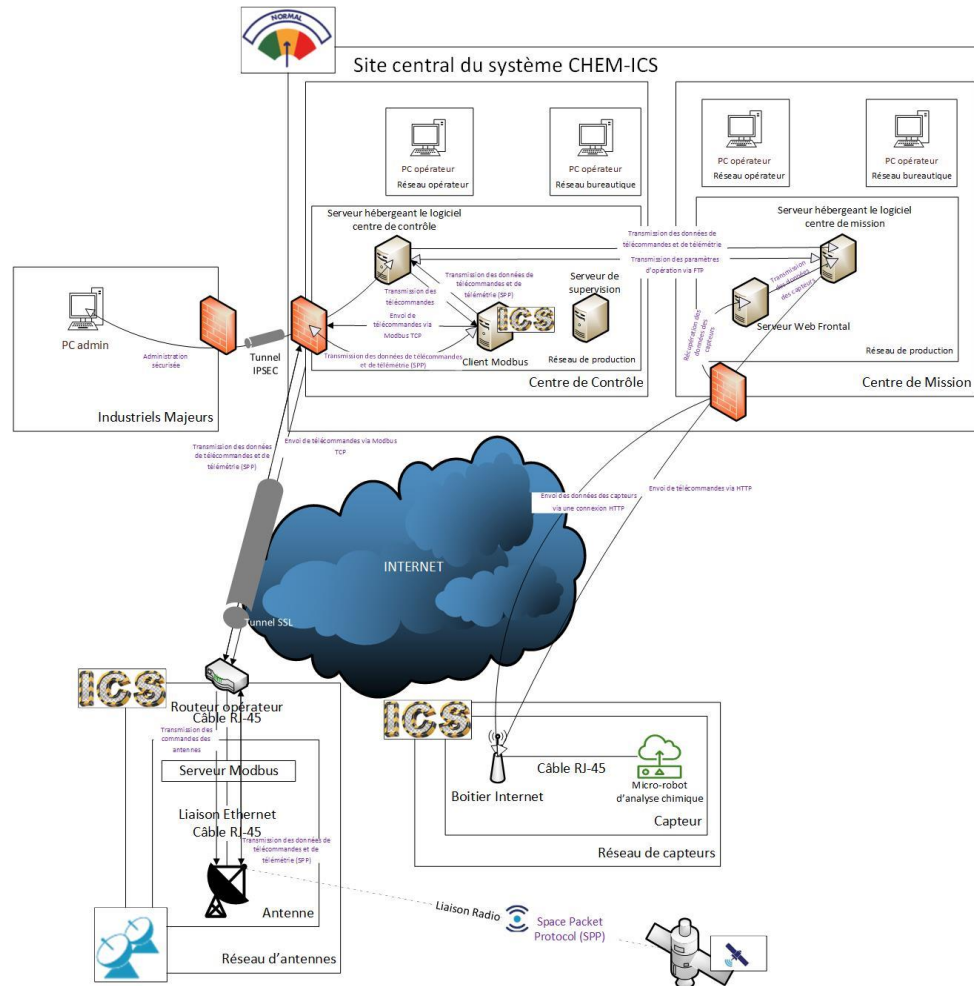
Overview of CHEM-ICS



Functional description



Detailed description and weaknesses to assess



Some weaknesses highlighted

- Multi-sites system,
- Obsolete products difficult to replace short-term,
- Difficulty to update or replace (certified) COTS,
- Difficulty updating in limited timeframes,
- Rogue IT,
- Non reliable sub-contractors,
- Use of a public interconnection service,
- High turn-over of specialists implying know-how loss,
- Real-time constraints and prioritization of choices linked to operational safety to the detriment of security,
- Uncontrolled switch to degraded mode for operational/real-time safety requirements,
- Long and expensive development cycles,
- Complex operations with risks of physical damages.

Interest for the space community



- Representative of the industrial context and its problematics (IoT integration, real time constraints, etc.) as well as of the space context



- Space cybersecurity awareness for startups, small and medium sized company and the New Space domain.



- Training for space experts nonspecialised in cybersecurity



- EBIOS RM is ISO 27005:2022 compatible
- Adapted to space contexts



- Good study case to onboard new people on space projects as it provides a vision on a simpler system than in real life



- Training for cybersecurity experts nonspecialised in the space domain



Space Cybersecurity Digital Consulting

Information security management

Information system audit

Risk management

Security system design

Thank you for your attention

Eva Soussi

+33 6 09 37 51 37

eva.soussi@priamos.fr

<https://www.priamos.fr/>