

Impact Analysis of AI Regulation in the Navigation Sector

AAE Webinar

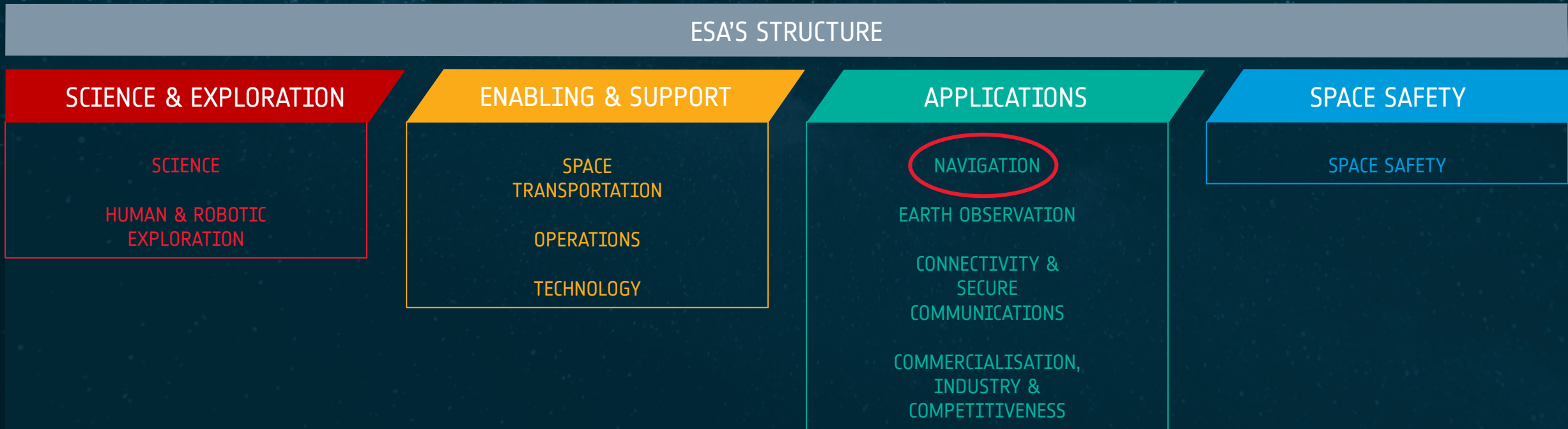
Ora Buch Kornreich

ESA ESTEC

13/04/2026

1. A Brief Introduction to the European Space Agency

WHO	23 Member States, 2500+ staff members and total workforce of 6000+
WHY	For the peaceful use of space, benefiting all
WHERE	HQ in Paris, seven sites across Europe & Spaceport in Kourou
BUDGET	€8.26 billion = €15 (one cinema ticket) per European a year



GALILEO

- ◆ The world's most precise satellite navigation system.
- ◆ Designed and developed by ESA on behalf of the EU.
- ◆ Serving four billion smartphone users around the globe.
- ◆ 34 satellites in orbit and four to be launched
- ◆ 12 Galileo Second Generation satellites in production.

FUTURE NAV

- ◆ **CELESTE:** In-Orbit-Demonstration mission of low Earth orbit PNT services
- ◆ **GENESIS:** A single satellite flying four key Earth-measuring technologies

EGNOS

- ◆ First pan-European satellite navigation system, most notably used for civil aviation.
- ◆ Joint project of ESA, the European Commission, EUSPA and Eurocontrol.
- ◆ Augments the US GPS system, and soon Galileo, over Europe and makes it suitable for safety-critical applications.
- ◆ Three satellites in GEO.

HORIZON EUROPE – H2020

- ◆ Supporting the future construction and evolution of EGNOS and GALILEO, which focus on R&D for new versions of these programmes
- ◆ Also provide opportunities for the development of new applications for the use of these Systems in different market segments.

2. ESA's Cyber Internal Audit Unit



- ◆ The team oversees the work of Cyber Internal Auditors operating in the supply chain (Prime contractors, subcontractors, etc.)
- ◆ Coordinating around 100 annual cyber audits
- ◆ **Main objective:** evaluation of the level of compliance of the information security management system and the security measures implemented by the different actors
- ◆ Review of the defined security requirements, the security policies, guides and guidelines established by the European Union and the different Member States involved.
- ◆ Special emphasis on the monitoring of international safety standards.

3. Impact of AI Regulations on the Navigation Programmes

Where is AI in space-related cybersecurity?

- ◆ Authentication mechanisms
- ◆ Encryption methods
- ◆ Mechanisms in satellites' software
- ◆ Supply chain mechanisms
- ◆ Organisational operations

→ New ethics guidelines, regulations and risk-management standards to consider

3. Impact of AI Regulations on the Navigation Programmes

The EU AI Act

- ◆ Does NOT apply to
 - ◆ AI systems or models specifically developed and put into service for the **sole purpose of scientific research and development**
 - ◆ Any research, testing or development activity regarding AI systems or AI models **prior to their being placed on the market or put into service**
 - ◆ **Most** of the contracts we monitor fall in either of these scenarios
 - ◆ **But** some do cover services in operation → some risks during the development, integration and testing activities
- We have developed a set of mandatory guidelines to check compliance during the audit such as:
- ◆ **Identify whether an AI Policy exists within the organisation**
 - ◆ **Identify critical potential vulnerabilities in the software used (if involving AI)**
 - ◆ **Clarify whether the software was developed in-house or acquired**

3. Impact of AI Regulations on the Navigation Programmes

Framework for AI good cybersecurity practices (FAICP)

- ◆ Divided in 3 levels
- ◆ Level I (cybersecurity foundations): basic cybersecurity practices for all information and communication technology (ICT) systems that support AI
- ◆ Level II (AI-specific): AI system-related cybersecurity (characteristics, processes, and controls associated with AI)
- ◆ Level III (sectoral AI): best practices for industry professionals, focusing on high-risk AI-systems as identified in the AI Act.
- ◆ ENISA's questionnaire integrated in the audit framework

NIST AI Risk Management Framework (AI RMF)

- ◆ Voluntary use but included in the audit
- ◆ Principles used to implement the cyber internal audit

The ISO42001 Standard

- ◆ framework for establishing, implementing, maintaining, and continually improving AI management systems within organisations
- ◆ addresses the unique management challenges posed by AI systems (e.g. transparency, explainability) to ensure their responsible use and development
- ◆ pivotal for integrating AI systems within organisational processes
- ◆ Compliance is analysed during the audit and maturity evaluated. Gaps identified → vulnerabilities result in recommendations to remedy them



EUROPEAN SPACE AGENCY

Thank you!



Follow ESA on social
media!
Explore more on esa.int



ELEVATING THE FUTURE OF EUROPE