In Focus: Data Security and Cybersecurity | Governance & Standards

Governance

A Security Strategic Committee (bi-yearly basis committee) was initiated in 2025 with the attendance of VP Group Cybersecurity Officer & Group CISO and Group EXCOM members. The main duties of this committee are the following:

- Give an overview of cyber daily life via strategic KPIs and a status on main projects,
- State of Cybersecurity maturity in the Group,
- Review the impact of the implemented Cybersecurity measures on the risks,
- Validation of orientations & decisions by the SEVP Operations & Performance.

Organization

The Group Cybersecurity Directorate (GCD) brings together the Security management of IS/IT (Information Systems/Information Technology), OT (Operational Technologies) and Products & Solutions. It has the strategic and operational objectives of providing and strengthening:

- A unified vision for strategic coherence
- Better risk management
- Proactivity & resilience against cyberattacks
- Optimization of resources and skills
- Acceleration of cyber secured innovation and digital transformation
- Facilitation and monitoring of Regulatory Compliance
- Cost reduction and investment optimization

This decentralized cyber operational function enhances Thales's competitiveness by ensuring integrated cybersecurity across all its information systems and solutions – both those delivered to customers and the means used to build them –, protecting assets and turning cybersecurity into a strategic value driver.

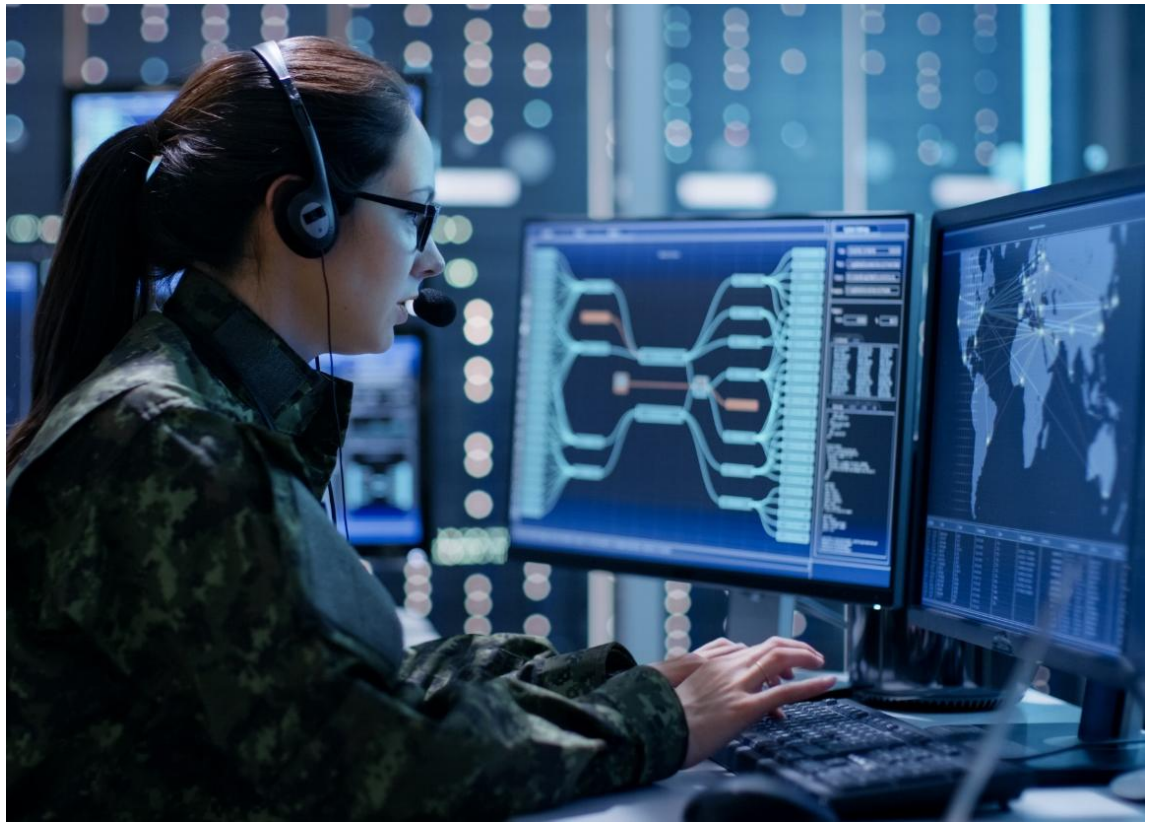
International standards and internal audits

This organization is designed in alignment with internationally recognized standards and best practices. In particular, it reflects the principles of :

- The NIST Cybersecurity Framework (CSF) ;
- The ISO/IEC 27001 standard.

These two frameworks are highlighted because they are among the most recognized internationally, while remaining open to other reference models to support the continuous improvement of our cybersecurity activities and information security systems.

Additionally, the Group internal audit teams perform regular audits both internally and with third-party partners. Thales also maintains a global supplier assessment program to ensure consistent security standards across the supply chain.



In Focus: Data Security and Cybersecurity | Policies & Programs

Key documents

To structure its efforts in Data Security and Cybersecurity, Thales has implemented multiple policies and guidelines:

- Organizational Memo for Cybersecurity
- Personal data protection policy
- Binding Corporate Rules (BCR) on personal data
- Information Systems Security Policy (ISSP)
- Cyber crisis management policy
- Cybersecurity Governance for Products & Solutions
- 9 rules or Cybersecurity Fundamentals Deployment
- Supply Chain Cyber Evaluation Process…

Additionally, all employees are provided with guidance and resources to help them meet their data-related responsibilities, in line with the IT Charter and the Group's Security Policy.

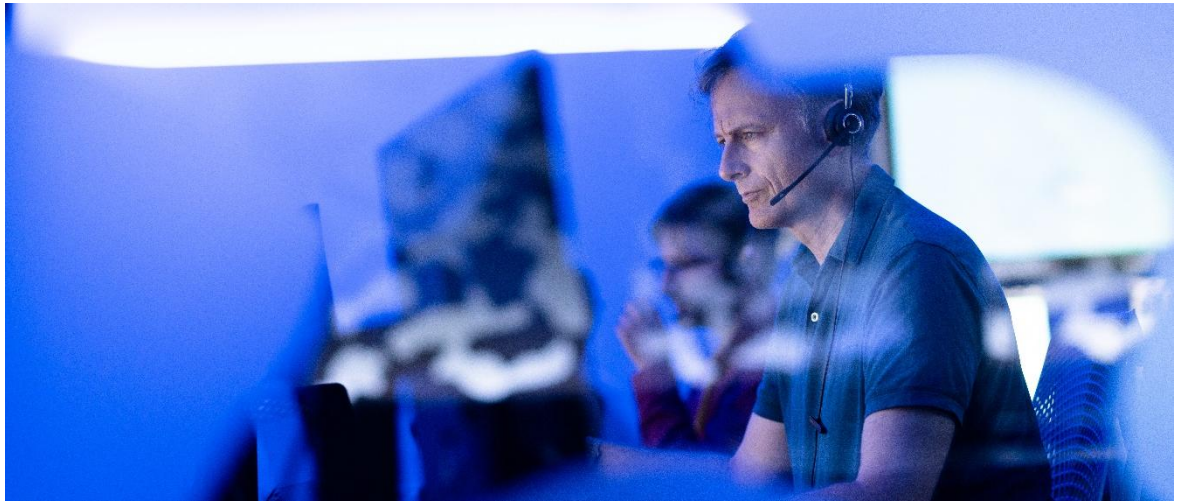
See also (on Thales' website):
Binding Corporate Rules
Personal data protection policy
Data security solutions
Data protection: how to comply with ANSSI's recommendations?

Training and Cybersecurity Academy

Training programs include e-learning modules and face-to-face sessions covering cybersecurity and data security/protection.

The Cybersecurity Academy features dedicated colleges for IS/IT and Product & Solutions Security, empowering Thales teams and partners to master evolving cybersecurity challenges through cutting-edge training and certification. Each college offers specialized skills and tailored learning paths fully aligned with the Group's overall strategy.

As part of the Group's commitment to being a learning company, Thales defines and prioritizes essential cybersecurity skills and implements a continuously improving three-year roadmap built on four key pillars: Governance & Strategic Alignment, Training & Certification, Community & Collaboration, and Performance & Cyber Culture. This structured approach ensures sustainable development and excellence in cybersecurity capabilities across Thales.



Cybersecurity incidents

A group instruction sets the framework for the preparation and management of Cyber crises: crisis exercises are regularly organized & 5 e-learning training modules are available to all group employees.

Thales oversees the monitoring of its products, solutions, and/or clients through its Security Operations Centers (SOCs). Incident handling is carried out under the authority of the CERT. The Group's commitment at Thales to partners and clients is to respond to their information requests through a single point of contact, ensuring compliance with international and local regulations.

- The PSIRT is centrally structured to coordinate PSIRTs organized by GBU and by country, according to our activities.
- The CERT and PSIRTs rely on a central Cyber Threat Intelligence (CTI) function that provides enhanced technical knowledge of threats relevant to the industrial sectors served by Thales, as well as current geopolitical developments

For more details, please refer to the Computer Emergency Response Team on Thales' website.

In Focus: Data Security and Cybersecurity | Group Product Security

Product Security Commitment

Thales integrates cybersecurity as a design, development, deployment and operations requirement for its products, solutions and services. The objective is to protect the Group's customers, their operations and critical infrastructure against cyber risks, throughout their life cycle, including after delivery (vulnerabilities, patches, advice, updates). This ambition is in line with the Group's cybersecurity strategy and Thales's brand and market positioning, which are based on TRUST. In this context, a Central Governance of Cybersecurity has been created.

Organization

Within the Group Cybersecurity Directorate (GCD), the Group Chief Product Security Officer (GPSO) is in charge to define and steer the Cybersecurity governance of Thales Products & Solutions.

It ensures end-to-end security across the project and product lifecycle – from offering to decommissioning – by establishing common guidelines, rules and policies, supporting their deployment, and promoting Product Security practices internally and externally.

All these missions are made possible by:

1. Relying on the Thales CPSOs (Chief Product Security Officers), CSAs (Cyber Security Authorities), COLs (Cyber Operation Leaders) and Cyber HoDs (Head of Discipline Cybersecurity) network as described in the Group Cybersecurity Governance for Solutions.

2. Following a Product Security Framework based on three pillars (Governance, End-to-End Solution Development Life Cycle, Cyber Assurance) dispatched in ten sub-activities that make up "Product Security by Thales".

3. Providing a dedicated 3/5 year-based Master Plan (CERBERUS) intended to fuels the Product Security Framework.

Group Product Security Office has been built **based on a 3 pillars framework, broken down into 10 areas of action**

+

The Framework is fueled with a **master plan defined each 5 years** called CERBERUS which **combines Thales strategy, global trends and several applicable regulations**

- **C = Cybersecurity** (protecting products from digital threats)
- **E = Efficiency** (over all Solutions lifecycle)
- **R = Risks** (assessing risks and vulnerabilities to identify improvement measures)
- **B = Blueprint** (defining a clear roadmap for PS)
- **E = Education** (addressing human aspects and talent development)
- **R = Recover** (ensuring a rapid and effective response to security incidents and crisis)
- **U = Unity** (promoting collaboration across all departments with a shared vision)
- **S = Services** (promoting Thales Cyber Services to counter the silo's effect)