CYBERSECURITY AND PERSONAL DATA PROTECTION

–

GOVERNANCE FRAMEWORK AND MEASURES

March 2026

Table of Contents

1. Purpose and Scope of the Document

This note presents the governance framework, principles, and key measures implemented by Groupe SEB in terms of cybersecurity, information security, and personal data protection. It complements the Universal Registration Document (URD) and the Group's Code of Ethics.

The Group remains committed to a policy of measured transparency towards its stakeholders, by sharing relevant elements of its governance framework and arrangements, while preserving the operational effectiveness of its protective measures.

2. Cybersecurity Governance

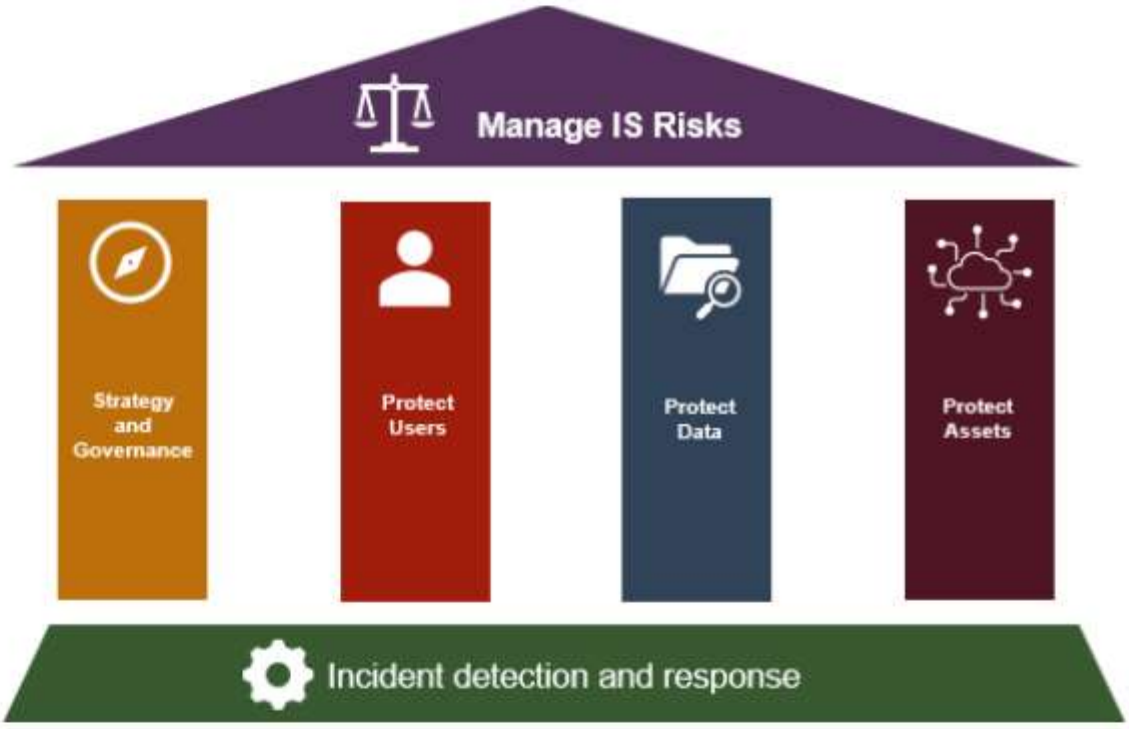
2.1. A dedicated organization

Within the **Information Systems Department** (ISD), **the Information Systems Security Department** (ISSD), headed by the Chief Information Security Officer (CISO), is responsible for overseeing information systems, identifying and assessing risks and defining governance, mobilizing resources, and implementing all policies, processes and systems required to adequately address identified risks.

It therefore relies on an information systems risk analysis, updated on an annual basis. All actions are prioritized according to information systems security risks, in order to focus prevention, detection and remediation resources on the most significant risks.

It is organized into four main pillars:

- Management of cyber strategy and governance
- User protection
- Data protection
- Protection of digital and technical assets



These pillars support the entire information system to ensure its maintenance in secure conditions.

The **ISSD** ensures compliance with various laws and regulatory obligations according to territorial considerations. It acts as the second line of defense by ensuring adherence to the policies it establishes and regularly monitoring the application of policies and the effectiveness of control measures implemented within the Group.

The ISSD is made up of a governance team and an operational security team.

The **operational security team** addresses the security needs expressed by the governance team by selecting a range of partners for support on cybersecurity topics and equipping itself with recognized tools and solutions for incident protection and detection. Within its structure, there is a dedicated sub-organization to ensure security event detection and response (Security Operations Center - SOC & Computer Emergency Response Team - CERT).

2.2. Framework and mission

The **ISSD**'s primary mission is to define the strategy and evolution of the existing security framework in order to address the organization's information systems security challenges. Framework evolution proposals are based on strategy, risk mapping, and regulatory compliance. The security framework is structured in alignment with recommendations from reference authorities such as the National Institute of Standards and Technology (NIST) and the International Organization for Standardization (ISO), and applicable standards for the Group. The NIST Cybersecurity Framework is structured around six domains:

- Governance
- Identification
- Protection
- Detection
- Response
- Recovery, which includes resilience and crisis management aspects

This approach relies on two principles: **defense in depth** and **security by design**.

It applies to three scopes: IT, Operational Technology (OT), and Internet of Things (IoT) for Groupe SEB's connected products.

The Directorate promotes the following values in its actions:

- **Collaboration:** Security should be embodied by all users of Groupe SEB's information systems, particularly IT teams.
- **Transparency:** Rules must be known to be enforced.
- **Simplicity:** Rules should be simple for effective implementation.

The vision of the cybersecurity directorate is to establish a fair and agile information systems security that supports the innovation and evolution of Groupe SEB.

2.3. Governance and supervision

The Executive Committee of the Information Systems Department (ExCom) is informed on a monthly basis of the cybersecurity status within the Group. A detailed presentation is made to the ExCom at least on a semi-annual basis. Cybersecurity challenges are integrated into the Group's risk mapping and are monitored within the framework of internal control and risk management processes.

Regarding data protection requirements, the Director of Information Systems Security or Chief Information Security Officer (CISO) collaborates with the Data Protection Officer (DPO), the Legal Department, the Compliance Department, and the HR Administration Department. This collaboration between the IT department, CISO, DPO, Legal, Compliance, and Internal Audit ensures comprehensive coverage of cybersecurity, information security, and personal data protection issues.

The ISSD also works in partnership with the Internal Audit service to validate security-related controls and their annual review plan.

2.4. Cyber Awareness and Culture

Cybersecurity is everyone's responsibility. All newcomers to the Group are made aware of cybersecurity challenges through a welcome kit available in both French and English. All employees are also informed by email of emerging situational risks, whether originating from within the Group, from its partners, or from its broader environment.

The Information Systems Security Directorate also collaborates with the Group's Learning & Development team to provide targeted training for the most sensitive professions and organizes several phishing tests annually to raise employee awareness of increasingly sophisticated hacker techniques. The framework also includes the Group's partners and subcontractors in the prevention of information systems security risks.

3. Threat Monitoring and Incident Response

3.1. Preparing to better respond

In the context of increasing cyber threats and cyberattacks worldwide, Groupe SEB initiated information systems security enhancement plans as early as 2020. Detection and response capabilities to cyberattacks have been significantly strengthened. A security master plan was implemented in 2022, outlining the Group's cybersecurity trajectory until 2026. This plan addressed both IT and OT systems. A new plan covering the period from 2026 to 2030 is currently being developed.

Additionally, new projects are subject to security by design strategy. For website or connected object projects, penetration tests are conducted before production deployment.

The Group closely monitors recommendations and alerts issued by competent cybersecurity authorities and reference organizations to counter increasingly sophisticated attack modes that could affect business continuity or data confidentiality.

Each year, the Executive Committee of Groupe SEB and the teams from the Industry, ISD and Marketing departments take part in a cyber crisis management exercise, enabling them to train for potential crises and strengthen collaboration between Group Management, business lines, functions and Information Systems teams.

3.2. A dedicated incident response framework

Groupe SEB is equipped with a Security Operation Center (SOC) that enables advanced detection of vulnerabilities and threats, as well as quick identification of weak signals, to respond to potential cyberattacks and limit their occurrence or impacts.

This comprehensive service is equipped with human resources, tools and processes that enable Groupe SEB to ensure its capacity to detect, analyze and contain security incidents as swiftly as possible, in order to limit their potential impact. These tools include a SIEM (Security Information and Event Management) system, which centralizes and correlates security event logs across the IT environment, and an EDR (Endpoint Detection and Response) solution, which monitors and responds to threats at the device level.

In parallel, to test the system's effectiveness, "Red teaming" exercises are conducted. In these exercises, professional ethical hackers from a specialized company attempt to breach the Group's cyber defenses. These exercises are conducted in coordination with the Group's Internal Audit team.

All these measures are subject to regular reviews and improvements. The results of controls and exercises feed into a continuous improvement process that strengthens the Group's security posture.

The Information Systems Security Directorate also oversees the implementation and testing of Business Continuity Plans, defines Business Continuity Plans with the business teams, and has designated a cyber crisis management process for Groupe SEB.

4. Information Security and Data Protection

4.1. Protection of Information Assets

The companies and entities of Groupe SEB own a vast array of information distributed across various media (paper, digital, etc.). Overall, businesses are increasingly exposed to acts of information theft. The main threats include cybercrime and industrial espionage. The growing use of outsourcing, the increased use of information and communication technologies such as cloud, SaaS solutions, remote work, mobility, the often-blurred line between professional and private life, and the use of artificial intelligence all contribute to the rise of these threats. In this context, Groupe SEB implements technical and organizational solutions to ensure the security of its entire information heritage.

A particular effort may be undertaken to protect information with a higher level of confidentiality or that falls under specific legal frameworks, including personal data described below.

4.2. Third-Party Risk Management

The Group pays special attention to managing third-party risks. Suppliers, service providers, and partners with access to the Group's information systems or data are subject to specific measures, including security and confidentiality contractual clauses, risk-proportional evaluations (due diligence), escalation and notification requirements in case of incidents, as well as periodic access reviews.

These provisions particularly apply to cloud services, SaaS, IT outsourcing, and projects involving connected devices.

4.3. Personal Data Protection

Groupe SEB's policy on personal data protection is founded on a common framework applicable to all markets in which the Group operates and to all individuals whose personal data is processed (including consumers, clients, employees, and partners). This Group-wide standard is based on the General Data Protection Regulation (GDPR) and incorporates local regulations when they diverge from or complement the European framework. It is anchored in the Group's policies that define governance and compliance rules regarding personal data protection.

Personal data protection is a major priority for Groupe SEB. It is a fundamental pillar of its commitment to compliance and trust for its consumers, clients, employees, and partners. The protection and respect for the confidentiality of personal data are highlighted as key themes in the Group's Ethics Code. The Group's practices are based on the key principles of personal data regulations, reflected in its internal policies and standards.

Individuals whose personal data is processed by the Group have rights (including the right to access, delete or modify their data), in accordance with the framework defined by applicable legislation. They must also rely on secure and confidential management of their personal data.

To ensure compliance with these principles, the Group:

- Implements technical and organizational measures that limit data access to only those who need it, both internally and for external parties.
- Enforces security and confidentiality prerequisites in all contracts with suppliers or third-party providers, ensuring they meet at least the Group's standards for personal data protection.
- Deploys an alert mechanism that involves data privacy and cybersecurity teams as soon as there is a suspected incident, to conduct an analysis. In confirmed incidents, a task force is established to address the incident and develop a remediation plan and impact analysis for continuous improvement.
- Strives to integrate the principles of privacy by design and privacy by default in the development of its projects, products, and services involving personal data.

4.4. A Networked Organization

The governance of personal data protection within the Group is centered around the Data Protection Officer (DPO), who acts independently, and a compliance function specialized in personal data protection within the Group Compliance department. These central roles are supported by an international network of DPOs and Privacy Relays to:

- Ensure the consistent application of Group rules and processes for personal data protection;
- Assist entities in implementing applicable regulatory requirements;
- Strengthen the culture of personal data protection within the business operations.

5. Management, Indicators, and Continuous Improvement

The Group relies on several monitoring indicators to measure the effectiveness of its awareness and protection initiatives, including the frequency of crisis management exercises, the reach of awareness campaigns, the frequency of phishing tests, the proportion of employees trained in cybersecurity issues, and the presence of incident review processes and remediation plans.

Groupe SEB is committed to a continuous improvement approach for its cybersecurity, information security, and personal data protection measures. This approach aims to continually adjust the level of risk management in response to technological, regulatory, and threat landscape developments.