Global Information System Security Policy

Group ISMS

Version 2.7
March 2026
Public

SUMMARY

1. Introduction 4
1.1. Information security as a strategic priority 4
1.2. Common objectives for effective protection 4
1.2.1. Organizational perimeter 4
1.2.2. Functional perimeter 5
1.2.3. Technical perimeter 5
1.2.4. Approach 5
1.3. Glossary 6
2. Information System Security Documentation 7
2.1. Structure of the information system security documentation 7
2.2. Implementation of the security policy 8
2.2.1. Lifecycle 8
2.2.2. Applicability 9
2.2.3. Publishing 9
2.2.4. Procedures for handling exemptions and exceptions 9
3. Governance of the Information System Security 10
3.1. Overview of the governance 10
3.2. Global Information Security Officer (Global CISO) of Bureau Veritas 11
3.2.1. Role overview for the Global CISO 11
3.2.2. Responsibilities of the Global CISO 11
3.3. DxS Central Teams 12
3.3.1. DxS Cyber Defense Center (CDC) 12
3.3.1.1. Role overview for the DxS CDC 12
3.3.1.2. Responsibilities of the DxS CDC 12
3.3.2. DxS Digital Trust (DT) 13
3.3.2.1. Role overview for the DxS DT 13
3.3.2.2. Responsibilities of the DxS DT 13
3.3.3. Business Security Officer (BSO) of Bureau Veritas 13
3.3.3.1. Role overview for the BSO 13
3.3.3.2. Responsibilities of the BSO 14
3.3.4. Regional Security Officer (RSO) of Bureau Veritas 14
3.3.4.1. Role overview for the RSO 14
3.3.4.2. Responsibilities of the RSO 14
3.3.5. Field Chief Information Security Officer (FSO) of Bureau Veritas 15

3.3.5.1. Role overview for the FSO 15
3.3.5.2. Responsibilities of the FSO 15
3.4. Support Teams 16
3.4.1. Area Security Officers (ASO) of Bureau Veritas 16
3.4.1.1. Role overview for the ASO 16
3.4.1.2. Responsibilities of the ASO 16
3.4.2. Local Security Correspondents (LSC) of Bureau Veritas 16
3.4.2.1. Role overview for the LSC 16
3.4.2.2. Responsibilities of the LSC 17
3.5. Contact with authorities and special interest groups 17
4. Appendices 18
4.1. Appendix 1: Revision History 18
4.2. Appendix 2: Approvers 18
4.3. Appendix 3: Operational Policies 18
4.4. Appendix 4: Operational Policies 19
4.5. Appendix 5: Functional and Technical guidelines 19

1. Introduction

The **Global Information System Security Policy (Global ISSP)** establishes the overarching framework for information security across Bureau Veritas. It outlines the key security challenges, strategic objectives, governance principles and fundamental security requirements applicable to the entire organization.

Global ISSP aims to ensure effective protection of information in accordance with the four corporate classification criteria:

- Availability
- Integrity
- Confidentiality
- Traceability

1.1. Information security as a strategic priority

Information security is a core strategic matter for Bureau Veritas. Information - in all its forms - is a critical asset that directly supports organizational performance, long-term sustainability and the ability to deliver services and achieve results.

To mitigate accidental or malicious threats that may compromise the security of the information system, Bureau Veritas must implement appropriate, proportional and risk-based measures.

The Information System Security framework at Bureau Veritas is established through the Global ISSP and reinforced by a set of Operational Policies. These policies outline the specific rules and responsibilities related to managing information security across defined thematic areas. Together, the governance principles and common requirements set out in the ISS Policies ensure the effective protection of information assets and maintain the overall coherence of the Information Security Management System (ISMS).

1.2. Common objectives for effective protection

Beyond defining the overall Information System Security framework, the Information System Security Policies also reinforce the coherence of the Information Security Management System (ISMS) by promoting consistent practices across Bureau Veritas. They support alignment throughout all entities and subsidiaries, enabling the organization to build on existing security measures and capitalize on shared best practices.

1.2.1. Organizational perimeter

The Global Information System Security Policy applies to all entities and subsidiaries of the Bureau Veritas Group worldwide. The Information System Security Policies must also extend to Suppliers by defining the fundamental security principles that apply to the services they provide to Bureau Veritas.

Some subsidiaries or entities may additionally be subject to specific security policies due to the nature of their activities, the legal requirements of the countries in which they operate, or contractual obligations imposed by Customers or Suppliers.

1.2.2. Functional perimeter

All resources that support or process Bureau Veritas information fall within the scope of the Information Security Management System (ISMS). This includes all methods and means used to create, acquire, process, store, distribute or dispose of information.

The functional perimeter includes, but is not limited to:

- **User equipment:** Desktop and laptop computers, mobile devices (smartphones, tablets), laboratory terminals and digital equipment, and any end-user computing devices.
- **Operational resources:** Cloud services and platforms, servers, network and telecommunications equipment, printing devices and all infrastructure components, OT equipment, IoT devices and infrastructure (innovation labs).
- **Software:** Operating systems, applications, databases and any software involved in information processing.
- **Physical media:** Paper documents, printed materials, removable media and other tangible information carriers.
- **Human and organizational resources:** Employees, contractors, suppliers, governance structures and operational processes that support information handling.

1.2.3. Technical perimeter

Information System Security Policies apply to the entire Bureau Veritas Group, including all its entities and subsidiaries. They are designed to ensure full applicability independent of specific technologies, focusing instead on functional requirements, organizational processes and security principles that remain valid regardless of system architecture or technical solutions

Each entity must implement the controls required by the Information System Security Policies using technologies appropriate to its context, risk level and operational constraints, while ensuring full alignment with the ISMS framework.

1.2.4. Approach

Besides incorporating industry's best practices, Information System Security Policies must consider the following elements:

- **Information Risk Management:** the rules defined in each policy must be designed to manage and reduce risks that could significantly impact business operations or threaten the confidentiality, integrity, availability, or traceability of information.
- **Compliance:** security rules must ensure the assessment of compliance requirements, such as regulatory obligations, contractual commitments, and industry standards, and the implementation of appropriate measures to meet these requirements.
- **Business Objectives:** Information System Security Policies and their supporting governance must collaborate and coordinate closely with the business to ensure that the security strategy is aligned with Bureau Veritas' objectives, particularly regarding performance, resilience and data protection.

1.3. Glossary

A

ASO: Area Security Officer, part of the DxS Team

B

BCM: Business Continuity Management

BSO: Business Security Officer, in charge of clients and critical third parties, part of the DxS Team

C

CISO: Chief Information Security Officer

CAB: Change Advisory Board

D

DxS: Digital x Security Team

DxS CDC: Cyber Defense Center, part of the DxS Team

DxS DT: Digital Trust, part of the DxS Team

F

FSO: Field Security Officer, in charge of Product Lines, part of the DxS Team

I

ISMS: Information Security Management System

ISSP: Information System Security Policy (Global ISSP: Global Information System Security Policy)

IT/IS: Information Technology / Information System(s)

ISO/IEC 27001: International Standard for Information Security Management Systems. The globally recognized standard that defines requirements for establishing, implementing, maintaining and improving an ISMS. Used as the compliance backbone for security governance.

N

NIST: Widely adopted cybersecurity frameworks (NIST CSF, NIST 800-53) used as best-practice references for risk, controls and maturity published by the National Institute of Standards and Technology. U.S. federal agency.

L

LSC: Local Security Correspondent, part of the DxS Team

R

RSO: Region Security Officer, part of the DxS Team

2. Information System Security Documentation

2.1. Structure of the information system security documentation

Bureau Veritas' information security documentation is organized into a three-level governance repository, ensuring consistency, traceability and compliance with ISO/IEC 27001 requirements.

- **Global ISSP (this document):** serves as the reference framework that defines the challenges, governance principles, and fundamental security principles applicable across the entire Bureau Veritas Group, in alignment with ISO 27001.
- **Operational Policies:** establish thematic information security rules applicable to Bureau Veritas. Temporary derogations may be granted to entities or subsidiaries when full compliance cannot be achieved; such derogations must be validated by the Global CISO of Bureau Veritas.
- **Functional and Technical Guidelines:** operational documents that support implementation activities and ensure compliance with the requirements defined in the Operational Policies. These documents may be developed at either the Group level or the local level.

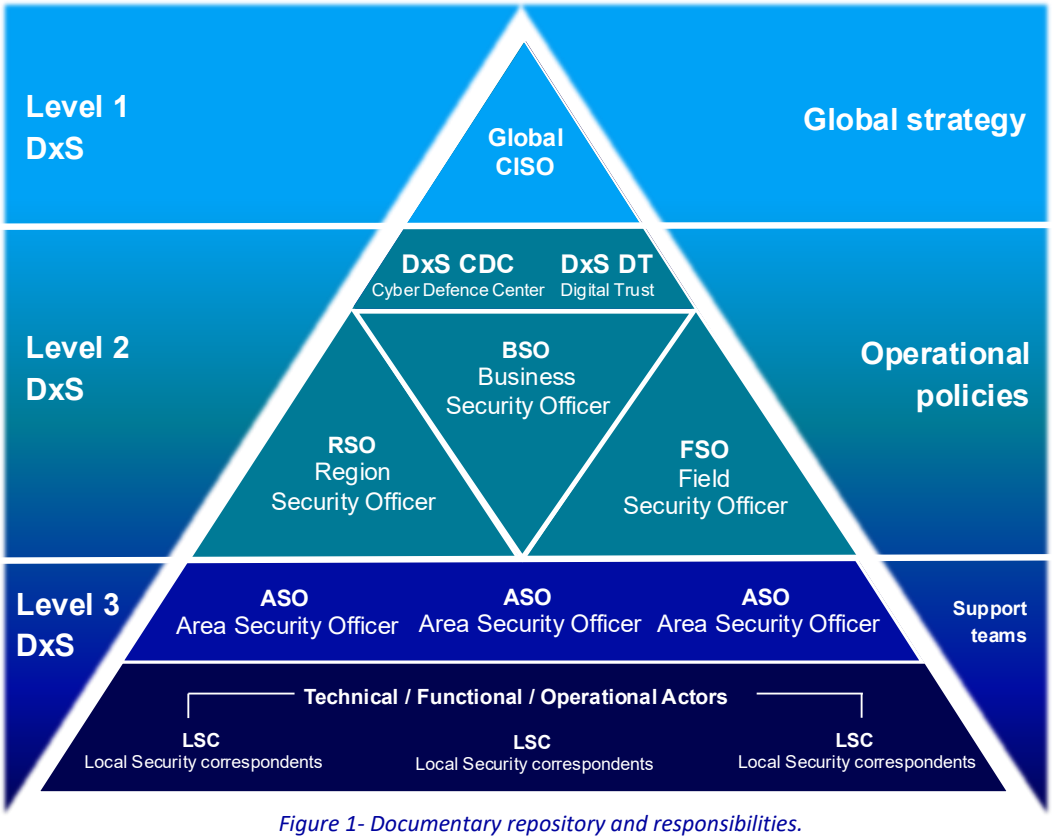

Figure 1- Documentary repository and responsibilities.

2.2. Implementation of the security policy

2.2.1. Lifecycle

To ensure long term effectiveness, relevance, and sustainability of the Information System Security Policies, and their alignment with Bureau Veritas' security requirements, these policies must follow a process of continuous improvement.

This improvement cycle is based on the **Plan–Do–Check–Act (PDCA)** model:

- **Definition and Planning (Plan):** Global CISO defines an action plan that identifies the Information System Security Policies to be updated, the required enhancements, and the associated communication activities.
- **Implementation (Do):** the defined action plan is executed. Improvements are integrated into the applicable Information System Security Policies, and updated versions are shared with the relevant stakeholders for review, feedback, and validation.
- **Control and Monitoring (Check):** this phase assesses the impacts of the updated policies on operational activities. The application and enforcement of the Information System Security Policies are monitored and controlled.
- **Maintenance and Enhancement (Act):** Security Officers and other contributors identify gaps and report them to the Global CISO. This feedback is analyzed to determine necessary improvements, which are then incorporated into the next planning phase.

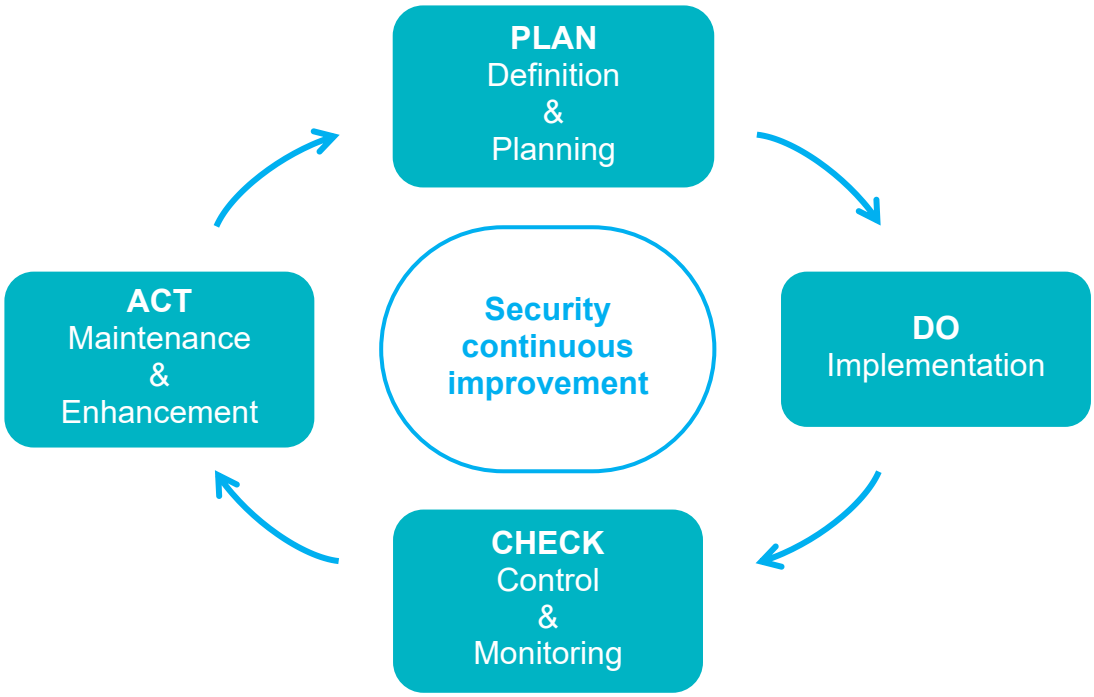

Figure 2 - Continuous improvement lifecycle.

Global ISSP and all Operational Policies must undergo a formal review at least once a year. Requests for updates, whether driven by internal needs, regulatory changes, audit findings or emerging risks, are centralized, assessed and validated by the Global CISO.

Once updated, the Information System Security Policies are submitted to the Executive Management of Bureau Veritas for formal validation and approval, ensuring top-level sponsorship and governance oversight.

The complete lifecycle of Information System Security Policies must be fully integrated into the Information Security Management System (ISMS), with all components of the ISMS documented, maintained, version-controlled, regularly reviewed, and traceable to ensure consistent application, auditability, and alignment with ISO/IEC 27001 requirements.

2.2.2. Applicability

The Information System Security Policies must be implemented, enforced and adhered to across all Bureau Veritas entities and environments without exception.

Any non-compliance with the Information System Security Policies must be formally recorded, trigger the creation of a corrective action plan, include a defined completion schedule with assigned responsibilities and follow up steps, and, when necessary, be covered by a validated derogation in accordance with the established governance process.

2.2.3. Publishing

The Global Information System Security Policy (Global ISSP) must be published publicly on the company website to demonstrate Bureau Veritas' commitment to protecting both its own information and that of its customers.

In contrast, Operational Policies are published internally only and must remain accessible exclusively to authorized Bureau Veritas users.

All Policy updates must be accompanied by formal communication to relevant stakeholders, ensuring they are informed of the changes, effective dates and any required actions.

2.2.4. Procedures for handling exemptions and exceptions

All components of the Bureau Veritas Information System are required to comply with the Information System Security Policies and associated standards. However, situations may arise in which full compliance with certain rules cannot be achieved. In such cases, a formal derogation process must be established and applied to manage, document, and monitor any exemptions or exceptions. Derogation requests must be reviewed and approved by Global CISO.

3. Governance of the Information System Security

3.1. Overview of the governance

The governance of the Information Security Management System establishes the structure of the Bureau Veritas information security stream and defines the roles and responsibilities of all stakeholders involved (Global CISO, RSO, BSO, FSO, Area Security Officers, etc.).

This governance framework provides direction and oversight for the information security stream by defining mandatory processes, coordinating activities, and supplying the necessary support materials (such as Policies, training programs, awareness content and operational guidelines).

Governance also encompasses all roles contributing to the effective operation and continuous improvement of information security within business activities, control functions, project ownership and project management. Its purpose is to ensure consistent implementation of security requirements, alignment with regulatory and internal standards and adherence to Bureau Veritas' risk management principles.

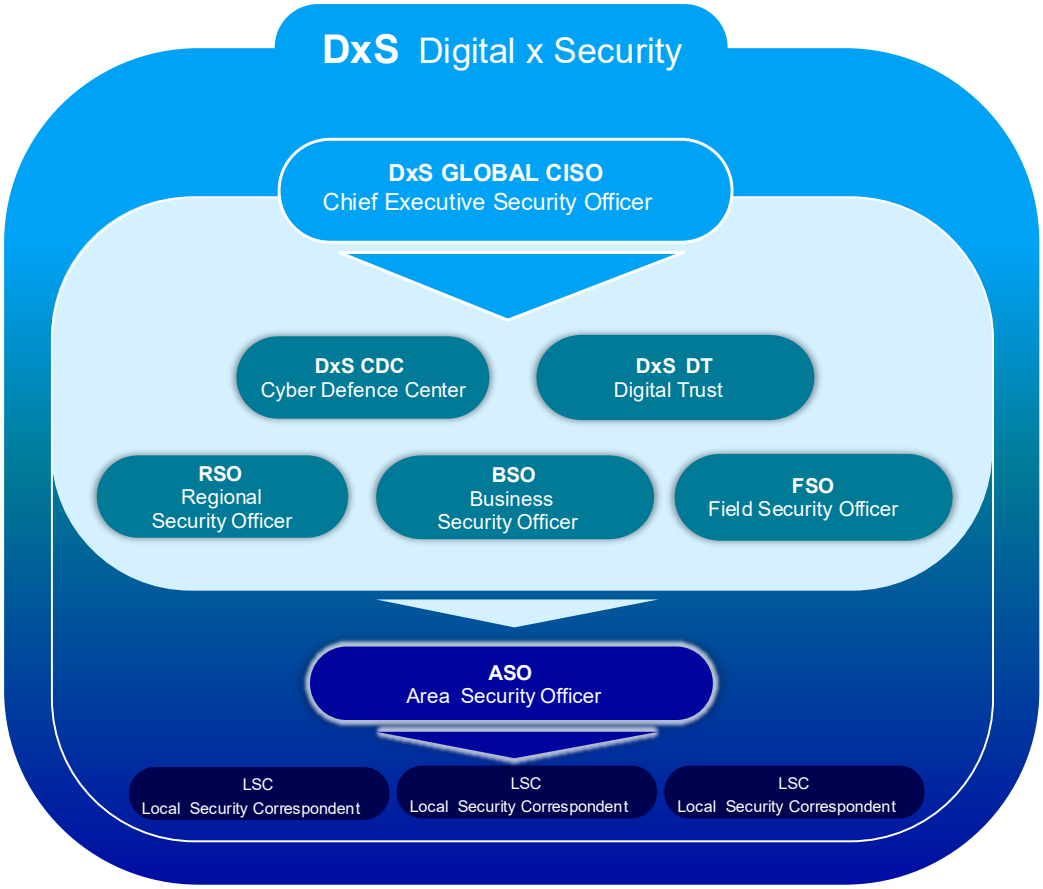

Figure 3 - Organization of the DxS governance of Bureau Veritas.

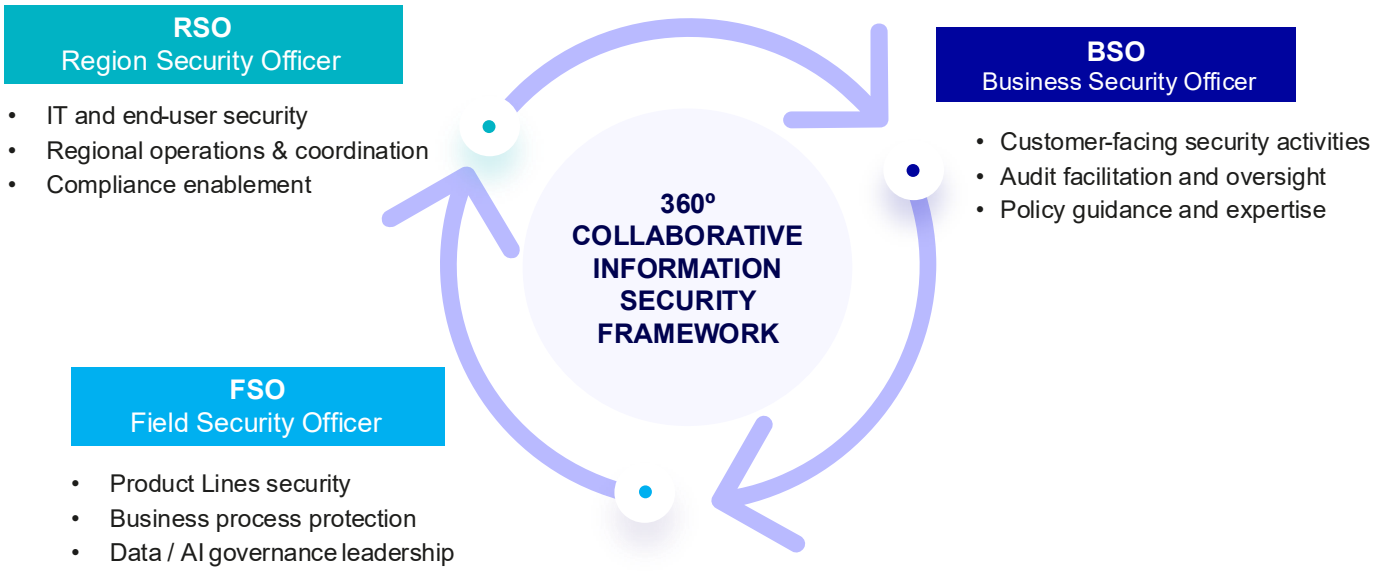

Figure 4 - Information security governance framework

3.2. Global Information Security Officer (Global CISO) of Bureau Veritas

3.2.1. Role overview for the Global CISO

The Global Information Security Officer (Global CISO) is responsible for ensuring the protection, resilience, and continuity of Bureau Veritas' information systems across the Group, its entities and its subsidiaries.

As the accountable owner of the Information Security Management System (ISMS), Global CISO provides strategic direction, governance oversight, and ensures alignment with internal and regulatory security requirements.

The Global CISO performs these responsibilities in coordination with internal stakeholders and external parties such as suppliers, customers, governmental bodies and certification authorities.

3.2.2. Responsibilities of the Global CISO

The Global CISO of Bureau Veritas oversees the implementation, performance and continuous improvement of the Information Security Management System. The key responsibilities include:

- **Establish and maintain** the organizational framework and operating conditions of the Bureau Veritas information security stream.
- **Define and coordinate** global security training and awareness initiatives.
- **Validate and approve** the appointment of Central Teams and Support Teams members.
- **Produce, consolidate and review** global information security dashboards and key performance / risk indicators from Central Teams, Security Officers and Security Correspondents reports.
- **Develop, maintain and update** Policies and ensure they reflect regulatory and organizational requirements.
- **Obtain Executive Management approval** for Policies and strategic security directives.
- **Ensure enforcement and provide guidance** for the implementation of Policies across the Group, entities and subsidiaries.

- **Monitor compliance** with Policies and ensure deviations are formally managed and justified.
- **Review and approve derogations** to Policies when they involve global impact or critical risk.
- **Plan and oversee** internal and external audits on information security matters, ensuring the implementation of corrective actions derived from audit recommendations.
- **Advise, approve and supervise** local security audit activities in coordination with Central Teams and Support Teams.
- **Participate in Change Advisory Boards (CAB)**, particularly for changes with significant or critical impact on Bureau Veritas' information systems.
- **Oversee incident management processes**, ensuring efficient crisis management and coordination with relevant stakeholders.
- **Supervise the implementation, maintenance and periodic testing** of the Business Continuity Management (BCM) processes related to information systems.

3.3. DxS Central Teams

The DxS Central Teams are responsible for implementing, disseminating and operationalizing the security policies and strategies defined by the Global Information Security Officer (Global CISO). They form the core operational and governance capabilities that protect, govern and enable Bureau Veritas' digital ecosystem.

Their structure consists of two central teams, DxS Cyber Defense Center (DxS CDC) and DxS Digital Trust (DxS DT), working in close coordination with other security actors, ensuring effective support and alignment across all specialized security functions.

The following sections describe each Central Team and outline their respective responsibilities.

3.3.1. DxS Cyber Defense Center (CDC)

3.3.1.1. Role overview for the DxS CDC

The DxS Cyber Defense Center (DxS CDC) serves as Bureau Veritas' central hub for digital defense. It operates as a centralized capability dedicated to protecting the Group's digital assets through continuous monitoring, detection, analysis, and response to cybersecurity threats. In line with the structure shown, DxS CDC delivers key defensive functions including Detect & Respond, Core Security, Emergency Response, Threat Intelligence, and Digital Resilience. Through these coordinated capabilities, the CDC maintains a unified view of cyber risks and ensures a consistent and resilient security posture across the organization.

The CDC operates in alignment with the policies and strategic orientations defined by the Global CISO and contributes directly to the effective implementation of the Information Security Management System (ISMS). It works closely with internal stakeholders and external partners to ensure cybersecurity activities across the Group remain coordinated, compliant, and continuously improved.

3.3.1.2. Responsibilities of the DxS CDC

The CDC oversees the execution and continuous enhancement of cybersecurity operations across Bureau Veritas. The main responsibilities include:

- **Operate and coordinate** global cybersecurity monitoring, detection and analysis activities to ensure timely identification of threats across BV's digital ecosystem.
- **Manage and maintain** core protection services, including network, endpoint, application, cloud and data security controls.
- **Conduct and enhance** vulnerability management activities, ensuring vulnerabilities are detected, prioritized and remediated according to risk.
- **Execute and support** incident response processes, including containment, eradication, recovery and

post-incident analysis.

- **Implement access-centric protection controls**, ensuring that identities, systems and services have the appropriate access and privileges across BV environments.
- **Produce and review** global cybersecurity dashboards, key performance indicators and security reports for operational and executive visibility.
- **Collect, analyse and share** threat intelligence to anticipate evolving threats and support proactive decision-making.
- **Perform security assessments** and coordinate penetration testing and forensic investigations when required.

3.3.2. DxS Digital Trust (DT)

3.3.2.1. Role overview for the DxS DT

The DxS Digital Trust (DxS DT) is the governance, risk and compliance capability responsible for ensuring that Bureau Veritas' digital ecosystem aligns with international standards, regulatory obligations and internal security policies. It provides the governance structures, control frameworks and compliance oversight required to maintain digital trust across the Group.

The team operates in alignment with the Global CISO and collaborates with business, IT and regional stakeholders to ensure that governance, risk and compliance activities remain consistent, auditable and continuously improved.

3.3.2.2. Responsibilities of the DxS DT

The DxS Digital Trust Team oversees the development, implementation and continuous improvement of governance, risk and compliance practices across Bureau Veritas. The main responsibilities include:

- **Define and maintain** security governance frameworks, policies and controls aligned with international standards and regulatory requirements.
- **Identify, assess and manage digital risks,** ensuring that risk treatment activities are documented, monitored and aligned with Group priorities.
- **Monitor and report** compliance with security policies, customer obligations, regulatory frameworks and contractual requirements.
- **Support and coordinate** internal and external audits, certifications and regulatory inspections, ensuring evidence, controls and processes are audit-ready.
- **Manage exceptions, deviations and risk acceptances**, ensuring decisions are justified, documented and formally approved.
- **Develop and deliver** cybersecurity awareness, training and behaviour-change initiatives to strengthen the Group's digital trust culture.
- **Advise and collaborate** with business, IT and regional teams, enabling secure-by-design practices and supporting customer trust activities.
- **Ensure continuous improvement** of governance, compliance and risk management processes as part of the Information Security Management System (ISMS).

3.3.3. Business Security Officer (BSO) of Bureau Veritas

3.3.3.1. Role overview for the BSO

The **Business Security Officer (BSO)** acts as the primary interface between cybersecurity and the business, ensuring that security requirements are embedded into day-to-day operations, decision-making and customer engagements.

The BSO enables secure business growth by aligning security practices with commercial objectives, maintaining compliance with regulatory and contractual obligations and promoting a risk-aware culture across their perimeter.

Working at the intersection of business, IT and security functions, the BSO ensures the effective implementation of the Policies, supports digital trust activities and contributes to the operational performance of the Information Security Management System (ISMS).

3.3.3.2. Responsibilities of the BSO

The main responsibilities of the BSO include:

- **Enforce DxS security Policies** within their business perimeter, ensuring adherence to controls, procedures and operational standards.
- **Monitor and report key security indicators**, risks, incidents and compliance status to DxS Central Teams and the Global CISO.
- **Manage and document security exceptions**, derogations and risk acceptances, ensuring decisions are justified and traceable.
- **Support audits and certifications**, ensuring evidence, controls and processes are maintained and audit-ready.
- **Support business continuity requirements**, ensuring proper maintenance and readiness of BCP activities within their scope.
- **Assess and oversee security practices** in business operations, projects and IT/IS activities, ensuring alignment with security requirements.
- **Facilitate customer and business engagements**, supporting responses to security questionnaires, due-diligence reviews and digital trust requirements.
- **Promote cybersecurity awareness** by supporting training initiatives and embedding secure-by-default behaviors in their perimeter.
- **Advise management** on security risks, controls and mitigation options to support informed and risk-aware decision-making.
- **Collaborate with Legal, Finance, Communications, Human Resources and DxS Central Teams** on regulatory, contractual and customer-driven security requirements.

3.3.4. Regional Security Officer (RSO) of Bureau Veritas

3.3.4.1. Role overview for the RSO

The **Regional Security Officer (RSO)** acts as the primary security representative within a defined regional scope and ensures the operational implementation of the Policies and security practices across the regions. The RSO provides a vital link between regional business teams, IT/IS functions and the DxS Central Teams, ensuring alignment with security requirements and supporting the resilience and continuity of business operations.

The RSO represents the regions in the global cybersecurity governance model by reporting relevant security information, contributing to the translation of operational Policies into local procedures and supporting the Global CISO in maintaining a consistent level of security across Bureau Veritas.

3.3.4.2. Responsibilities of the RSO

The main responsibilities of the RSO include:

- **Implement and enforce DxS security Policies** across their regional scope, ensuring consistent application of controls and operational standards. Monitor indicators, events and report regional security risks and compliance status to the Global CISO.
- **Manage and document derogations**, exceptions and risk acceptance within their region, ensuring proper justification and traceability.

- **Supervise and coordinate Area Security Officers (ASO)** and support Local Security Correspondents (LSC) to ensure aligned execution of security activities across all countries in the region.
- **Ensure consistent implementation of security processes** and contribute to translating DxS operational Policies into local requirements, collaborate with business, IT/IS and compliance functions.
- **Support incident management** by coordinating regional responses, aligning with DxS crisis management requirements, and ensuring proper escalation.
- **Configure and manage regional cybersecurity training** and phishing campaigns, using the Group-designated awareness platform and aligning with the annual DxS DT Training and Awareness Plan or local needs.
- **Support internal and external audits**, provide regional oversight, facilitating evidence collection and ensuring corrective actions are implemented.
- **Participate in governance forums**, including Change Advisory Boards (CAB), for changes affecting regional information systems.

3.3.5. Field Chief Information Security Officer (FSO) of Bureau Veritas

3.3.5.1. Role overview for the FSO

The Field Security Officer (FSO) ensures that cybersecurity is embedded across Bureau Veritas Product Lines by translating Group cyber strategy into operational execution.

The FSO aligns security controls with business priorities, regulatory requirements, and performance targets, acting as the cybersecurity liaison between Product Lines, DxS Central Teams and foundational IT functions.

The FSO defines and maintains cyber perimeters for each Product Line, drives the implementation of required controls and monitors performance to strengthen resilience, compliance and operational continuity.

3.3.5.2. Responsibilities of the FSO

The main responsibilities of the FSO include:

- **Implement and enforce** security Policies and directives across assigned Product Lines, ensuring consistent control application and operational readiness.
- **Define and maintain** the cybersecurity perimeter for each Product Line, clarifying scope, ownership and control responsibilities.
- **Translate product-specific risks into actionable controls** and escalate systemic or cross-line risks through established governance channels.
- **Align Product Line practices** with applicable standards and frameworks (e.g., ISO/IEC 27001, NIST) within the defined scope, ensuring audit-ready evidence and documentation.
- **Oversee security posture** across Product Line applications, data flows and processes; coordinate remediation, hardening and vulnerability management with accountable teams.
- **Support incident management and recovery**, ensuring Product Lines meet resilience, response and testing expectations.
- **Embed security-by-design** in product development and industrialization, participating in planning gates, reviews and acceptance activities.
- **Establish, monitor and report KPIs** for Product Line cybersecurity and track corrective actions to closure.
- **Facilitate feedback loops** from Product Lines to continuously improve Policies, control guidance and operational playbooks.

3.4. Support Teams

3.4.1. Area Security Officers (ASO) of Bureau Veritas

3.4.1.1. Role overview for the ASO

Area Security Officers (ASO) act as the operational cybersecurity leads within their assigned region. ASOs ensure the implementation of DxS Policies and controls, support local business and IT/IS teams and maintain alignment with the Regional Security Officer (RSO).

ASOs coordinate the network of Local Security Correspondents (LSC) to achieve consistent execution of security practices, incident readiness and compliance within their perimeter.

ASOs contribute to Group cybersecurity governance by reporting local risk and compliance status, facilitating audits and translating DxS directives into executable country procedures. ASOs are appointed according to Group procedures by the Global CISO or delegated authority and operate under the functional oversight of the RSO.

3.4.1.2. Responsibilities of the ASO

The main responsibilities of the ASO include:

- **Implement and enforce DxS security Policies** within their area, ensuring operational alignment with regional and Group requirements.
- **Produce local dashboards and reports**, monitor indicators, and escalate significant risks, deviations and events to the RSO. Maintain visibility over in-scope assets, applications and third parties.
- **Coordinate and guide** and manage and document exceptions, derogations and risk acceptances, ensuring proper justification and traceability.
- **Local Security Correspondents (LSC)** to ensure consistent execution of controls, evidence collection and timely reporting. Support vulnerability and patch management.
- **Promote regional cybersecurity training** and awareness initiatives, ensuring local execution of programs and campaigns.
- **Coordinate access and identity hygiene activities**, including periodic access reviews and enforcement of privileged access controls.
- **Support local incident management**, ensuring triage, escalation to the RSO and implementation of corrective actions.
- **Maintain and test the business continuity** strategy for their scope, ensuring readiness and alignment with Group expectations.
- **Act as the primary security point of contact** for local business, IT/IS and operational teams, supporting customer and supplier-related security requirements.

3.4.2. Local Security Correspondents (LSC) of Bureau Veritas

3.4.2.1. Role overview for the LSC

Local Security Correspondents (LSC) are the first-line operational points for cybersecurity at site, regional or business unit level. Under the coordination of the Area Security Officer (ASO), LSCs execute day-to-day security activities, collect evidence for controls, support incident response and promote awareness.

LSCs ensure that local operational practices follow DxS Policies and that deviations or issues are promptly escalated to the ASO.

3.4.2.2. Responsibilities of the LSC

The main responsibilities of the LSC include:

- **Execute assigned security controls** according to DxS Policies and local procedures defined by the ASO.
- **Maintain and provide evidence** of control performance, logs and local documentation to the ASO as required.
- **Support vulnerability and patch management**, validating deployment status with local IT and reporting delays or blocking issues.
- **Assist with access-related hygiene activities**, including periodic access reviews and joiner-mover-leaver enforcement.
- **Support endpoint protection, encryption and mobile device management** by performing local hygiene checks and validations.
- **Act as the local contact for security events**, performing initial triage and escalating incidents to the ASO according to procedure.
- **Assist in containment actions and evidence collection** during incident response under ASO or DxS Central Teams guidance.
- **Support business continuity and disaster recovery exercises**, preparing local inputs, executing tests and gathering required evidence.
- **Deliver or facilitate awareness and training sessions** for local teams and support execution of regional awareness programs.
- **Adapt DxS directives into local work instructions** for installation, operation and event handling when guided by the ASO.
- **Promote secure operational practices** and raise improvement opportunities to the ASO.
- **Prepare local evidence for audits**, participate in walkthroughs when requested and support users' assessments.
- **Maintain an inventory of in-scope local third parties** and support supplier due-diligence questionnaires and follow-ups.
- **Provide timely reporting** of metrics, issues and status updates to the ASO for consolidation.
- **Escalate risks, non-conformities and policy deviations** to the ASO without delay.

3.5. Contact with authorities and special interest groups

Where appropriate, Bureau Veritas and its subsidiaries establish and maintain contact with competent authorities. When relevant, Bureau Veritas should also maintain contact with special interest groups, specialist security forums and professional associations.

Maintaining these relationships may be required for compliance purposes such as notifying authorities of security incidents or data breaches. In addition, participation in specialist forums and professional associations helps the company anticipate developments in the cybersecurity field and prepare for changes. These connections can also provide valuable support or advice when dealing with complex or challenging situations.

4. Appendices

4.1. Appendix 1: Revision History

Version	Author	Description	Date
1.5	ISS Compliance	Appointment of the Group CISO	12/01/2017
2.0	ISS Compliance	Update of the content to comply with group strategy	27/03/2017
2.1	ISS Compliance	Update of the security roles Update of the frequency of policy review Adding a new operational policy to the appendix	19/12/2019
2.2	ISS Compliance	Adding policies creation approach Adding publishing requirements	19/03/2021
2.3	ISS Compliance	Annual review Adding requirement for handling derogations	07/04/2022
2.4	ISS Compliance	Annual review	20/04/2023
2.5	ISS Compliance	Annual review	30/04/2024
2.6	ISS Compliance	Annual Review ISO 27001:2022 adoption	09/04/2025
2.7	DxS Digital Trust	Content review to align with the new 2026 organization and roles.	16/03/2026

4.2. Appendix 2: Approvers

Name	Position
Julien ANICOTTE	Global Chief Information Security Officer

4.3. Appendix 3: Document Title

Document title	Document Name
Global Information System Security Policy	BV_GISSP_Global Information System Security Policy

4.4. Appendix 4: Operational Policies

The **operational Policies** completing the Global ISSP (GISSP) on thematic subjects for Bureau Veritas are:

- Human Resources security
- Classification of information
- Management of IT traces
- Logical access control
- Media handling
- Suppliers' relationships
- Network security
- Development and maintenance of applications
- Physical security
- Activity Continuity
- Operations security
- User equipment
- Management of security incidents
- Cloud security
- Data governance
- Generative AI
- Global IS/IT Charter

4.5. Appendix 5: Functional and Technical guidelines

The **functional guidelines** completing the Global ISSP (GISSP) on thematic subjects for Bureau Veritas are:

- ISS cyber threat data breach Policy
- Contact list French authorities
- BV ISO27001 internal process
- ISS ISO27001 certification guideline
- Physical security recommendations
- ISS Security by Design guidelines
- Security derogation request
- ISS Security questionnaires guidelines
- Cyber@BV user profiles for IAM and BV solutions
- Classification visuals
- Cyber@BV NIST framework process
- M&A and Carve out process
- M&A and Carve out checklist
- Third Party Risk Management and best practices

The **technical guidelines** completing the Global ISSP (GISSP) on thematic subjects for Bureau Veritas are:

- AWS KMS for Bureau Veritas
- Cybersecurity guidelines for Software Development
- Security requirements for web development
- Security best practices for SSL/TLS protocols and ciphers
- Software Licensing and Security
- AWS Golden Rules
- Digital travel recommendations