GLOBAL INFORMATION SYSTEM SECURITY POLICY

STATUS : VALIDATED

VERSION : 2,4

PUBLIC	INTERNAL	RESTRICTED	SECRET
X			

BUREAU VERITAS

Shaping a World of Trust

Approvers

Name	Position
Francois VILJOEN	Senior Vice President, Group CIO
Julien ANICOTTE	Group Chief Information Security Officer

Reference documents

Document title	Document Name

Classification

Level	Confidentiality
C1	Public

SUMMARY

GLOSSARY

B

BCP: Business Continuity Plan.

BL: Business Line.

C

CIO: Chief Information Officer.

CISO: Chief Information Security Officer.

G

Global ISSP: Global Information System Security Policy. Current document.

I

ISMS: Information Security Management System.

ISO 27001: An information security management standard. It provides requirements for an information security management system (ISMS).

ISS Policies: Information System Security Policies. Include the Global ISSP and Operational Policies.

O

OG: Operating Group.

S

Services: all kind of services performed by a Supplier for Bureau Veritas, including but not limited to technical assistance, maintenance services, any cloud-based services such as SaaS, IaaS or PaaS. Services can be provided on-site or off-site.

SO: Security Officer.

Supplier: Bidder that has been selected by Bureau Veritas to perform the Services under a Contract.

Supplier's Personnel: employees of the Supplier assigned by the Supplier to the performance of Services.

1. INTRODUCTION

The Global Information System Security Policy defines the reference framework for the information security of Bureau Veritas by highlighting security issues and objectives. It also gives governance principles and fundamental security requirements that apply to Bureau Veritas.

The Global ISSP aims at ensuring the protection of information via the four classification criteria: Availability; Integrity; Confidentiality and Traceability.

1.1. INFORMATION SECURITY, A VITAL ISSUE

Information in all its forms whether written, oral, electronic, processed manually or automatically is a strategic resource on which rely the performance, the sustainability, and the ability of the company to develop its activities and results.

To cope with accidental and malicious threats that could affect its information system security, Bureau Veritas must protect efficiently its information system by implementing suitable security measures, in adequacy with security challenges.

These security measures must allow Bureau Veritas to respect its contractual commitments, legal and regulatory constraints and the continuity of services provided to customers as well as their quality. Furthermore, this contributes the protection and the enhancement of Bureau Veritas' image.

1.2. COMMON OBJECTIVES FOR AN EFFECTIVE PROTECTION

The framework of the Information System Security of Bureau Veritas is defined by the Global ISSP, supported by Operational Policies detailing rules and responsibilities regarding the information security management on specific themes.

Governance principles and common rules formalized in the ISS Policies must ensure the effective protection of information in the scope of Bureau Veritas and the coherence of the information security management system. Also, they must allow capitalizing on implemented security measures and best practices in the different entities and subsidiaries of the organization.

1.2.1. ORGANIZATIONAL PERIMETER

The Global ISSP must be applied to all entities and subsidiaries of Bureau Veritas group worldwide.

ISS Policies must also have an impact on Suppliers. These policies must define fundamental security principles applying to services contracted by Bureau Veritas with Suppliers.

Some subsidiaries or entities of Bureau Veritas may be subject to dedicated and specific security policies due to their activity, the country in which they are located (e.g. local legal constraints), Customer or Suppliers' contractual requirements.

1.2.2. FUNCTIONAL PERIMETER

All resources supporting Bureau Veritas information are included in the Information Security Management System as well as all the ways meant to create, acquire, process, store, distribute or destroy this information on or using:

- Users' equipment (e.g. desktop and laptop computers, smartphones, tablets).
- Operational resources (e.g. servers, printers, telecommunication devices).
- Software (e.g. operating software, databases).
- Paper support.
- Human and organizational resources.

1.2.3. TECHNICAL PERIMETER

ISS Policies must be implemented by Bureau Veritas group and all its entities and subsidiaries. They aim to ensure the applicability regardless of the technical context by not giving details on technologies to implement but only the functional and organizational requirements.

1.2.4. APPROACH

Besides industry's best practices, ISS policies must take into account the following:

- Information risk management: the rules set forth in each policy must be constructed to manage and reduce risks that have a significant impact on business operations and threatening the confidentiality, integrity, availability and traceability of information.
- Compliance: the security rules must enforce assessing compliance requirements with regulation, contractual terms, industry standards, as well as implementing adequate measures to comply.

- Business objectives: ISS policies, as well as supporting governance must cooperate and coordinate with business to align security strategy with Bureau Veritas objectives and strategy: resilience and data protection.

2. ISS DOCUMENTATION

2.1. STRUCTURE OF THE INFORMATION SYSTEM SECURITY DOCUMENTATION

The information security documentation of Bureau Veritas is formalized as a three levels documentary repository:

- **The Global ISSP** (current document): reference document, establishing challenges, governance principles and fundamental principles of information security for all the Bureau Veritas group, in line with ISO 27001.
- **Operational Policies**: define information security rules by theme applying to Bureau Veritas. Temporary derogations may be granted to entities or subsidiaries if the compliance cannot be ensured. They are validated by the Global CISO of Bureau Veritas.
- **Guides, standards and procedures**: operational documents, supporting activities, compliant with requirements defined in Operational Policies' rules. These documents can be defined at the group level or locally.

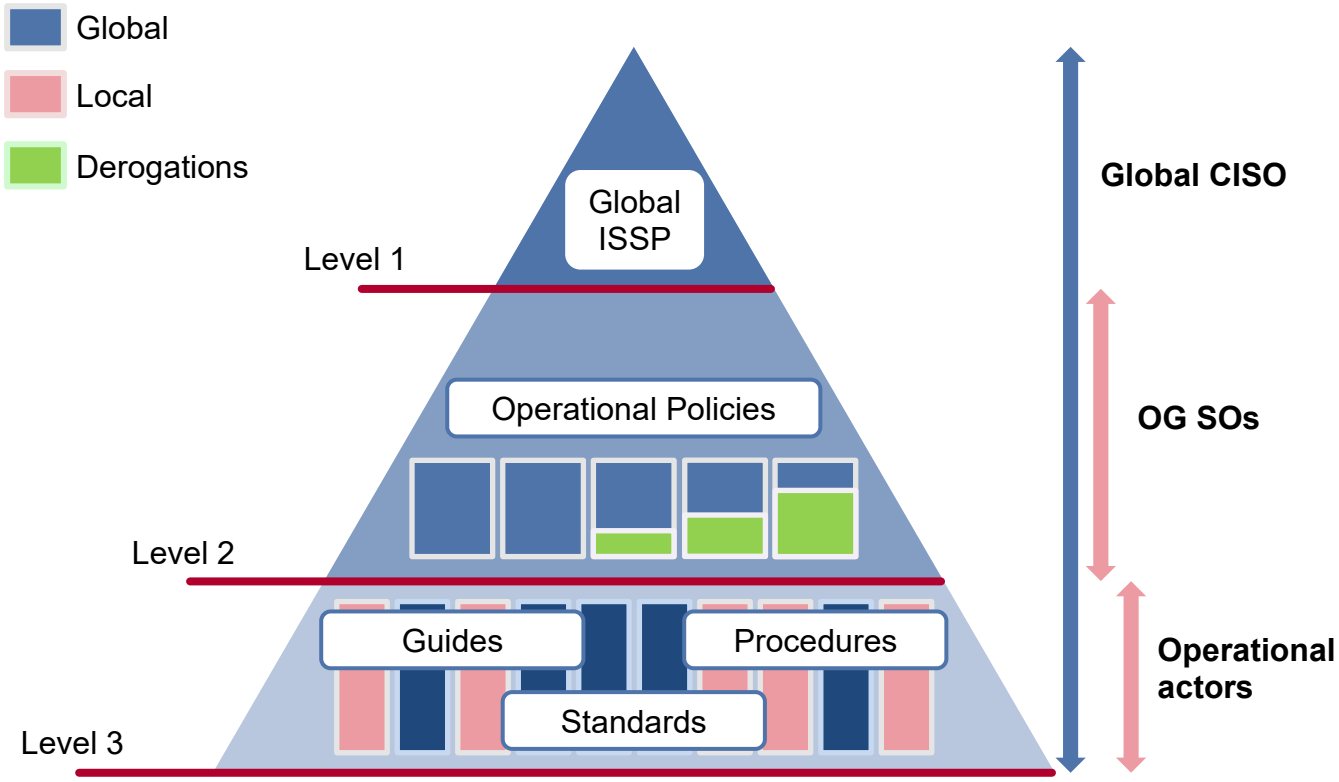

Figure 1 – Documentary repository and responsibilities

2.2. IMPLEMENTATION OF THE SECURITY POLICY

2.2.1. LIFECYCLE

In order to ensure the efficiency and sustainability of ISS Policies over time and their adequacy with Bureau Veritas' security requirements, ISS Policies must be subject to a continuous improvement.

This process of continuous improvement must be cyclical, based on the Plan-Do-Check-Act principle (PDCA):

- **Definition and planning (Plan)**: the Global CISO establishes an action plan including: ISS Policies to update, the needed improvements and the communication phase.
- **Implementation (Do)**: the action plan defined in the previous phase is implemented. Improvements are applied to corresponding ISS Policies; updated policies are communicated to relevant people for feedbacks and validation.
- **Control and monitoring (Check)**: this phase allows identifying impacts on operational activities. Application of the ISS policies is controlled.
- **Maintenance and enhancement (Act)**: Security officers and other stakeholders (e.g. security correspondents) identify the GAPs and inform the Global CISO. Feedback is analyzed to identify needed improvements and feed the coming Plan phase.

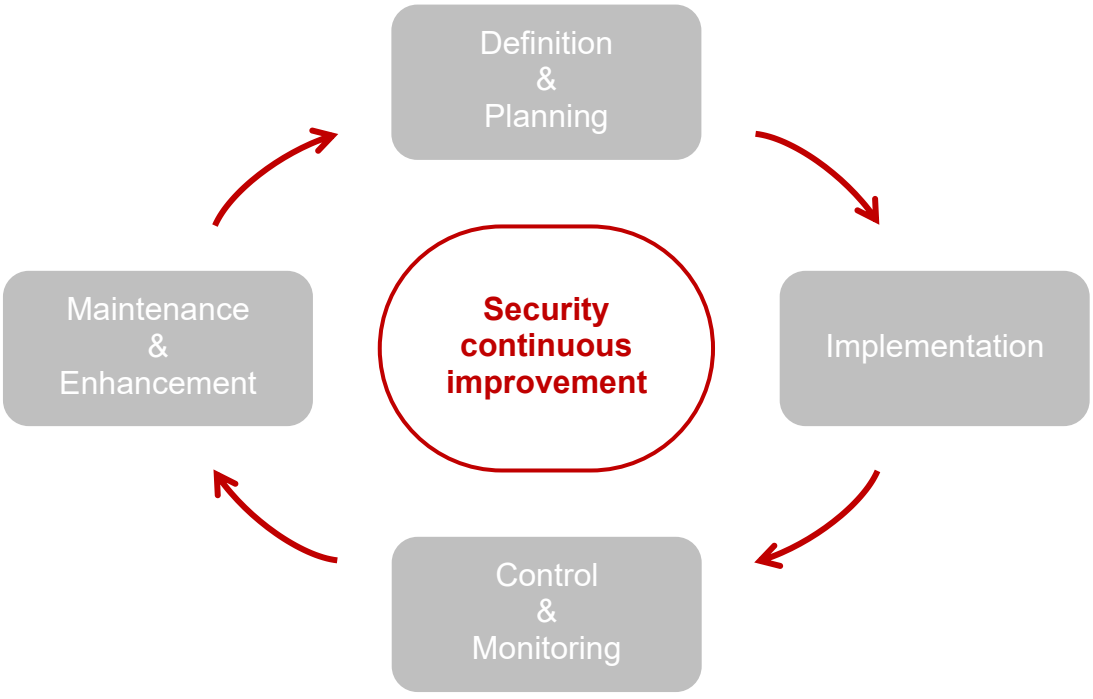

Figure 2 - Continuous improvement lifecycle

The Global ISSP and Operational policies must be reviewed at least once a year. Requests for updates, arising from internal needs or external factors, are centralized and validated by the Global CISO. The updated ISS Policies are submitted for validation to the Executive Management of Bureau Veritas.

The entire lifecycle of ISS Policies must be included in the Information Security Management System (ISMS), ensuring their implementation. The various elements of the ISMS must be formalized and documented in order to ensure the traceability of its operations.

2.2.2. APPLICABILITY

The ISS Policies must be implemented and enforceable.

Non-compliances with the ISS Policies must be subject to formal corrective action plans with a defined completion schedule or derogations.

2.2.3. PUBLISHING

The Global Information System Security Policy must be published publicly on the company's website in order to clearly showcase Bureau Veritas commitment to protect its information as well as customers' information.

Operational policies on the other hand are published internally. They must be accessible only for all Bureau Veritas employees.

Every updates to the policies must be followed by a communication to relevant stakeholders to inform them of the new changes.

2.2.4. PROCEDURES FOR HANDLING EXEMPTIONS AND EXCEPTIONS

All components of Bureau Veritas Information System are expected to comply with the ISS policies and standards. Nonetheless, in various cases, compliance with some rules cannot be achieved for various reasons. The derogation procedure for managing, documenting and monitoring these exemptions and exceptions must be formalized and implemented.

Derogation requests must be reviewed and approved by the Global CISO, compliance team or OG/SO of the requesting entity.

3. GOVERNANCE OF THE INFORMATION SYSTEM SECURITY

3.1. OVERVIEW OF THE GOVERNANCE

The governance of the information system security aims at defining the structure of the information security stream of Bureau Veritas as well as roles and responsibilities of all relevant people composing this structure (Global CISO, OG SOs, Information Security Team, etc.).

Through this governance, the goal is to frame the activity of the information system security stream of Bureau Veritas, by defining relevant processes, animating the stream and providing the needed material (ISS Policies, training and awareness supports, guides).

The governance also includes any relevant role for the animation of the information system security within business activities, control functions, project ownership and management.

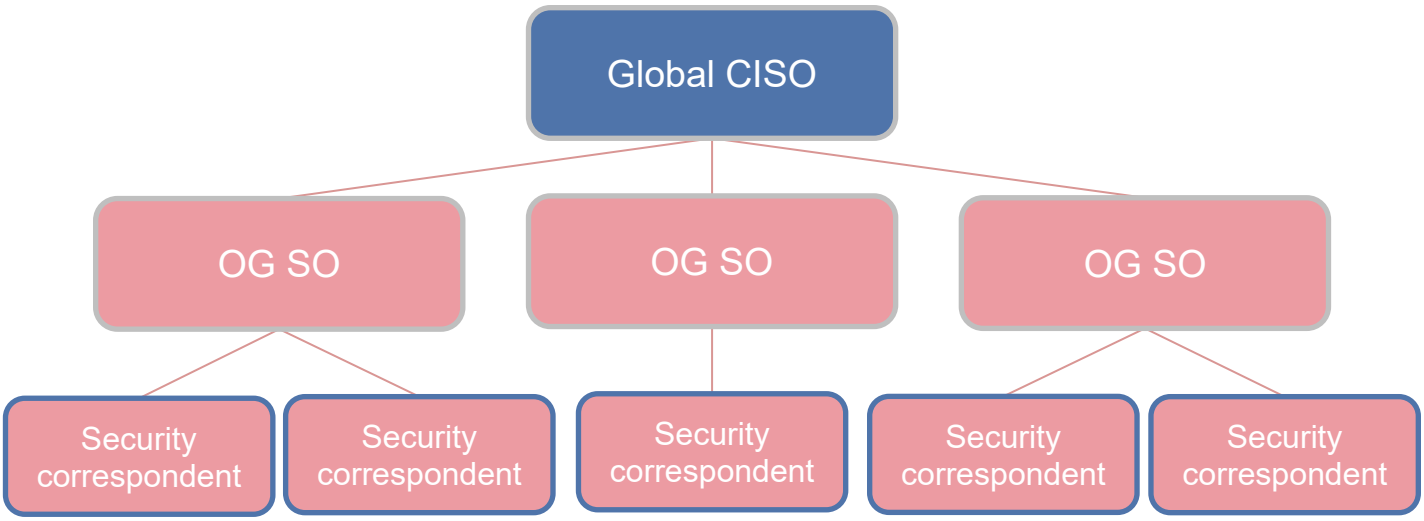

Figure 3 - Organization of the ISS governance of Bureau Veritas

3.2. THE GLOBAL CHIEF INFORMATION SECURITY OFFICER (GLOBAL CISO) OF BUREAU VERITAS

3.2.1. PRESENTATION OF THE GLOBAL CISO

The Global CISO of Bureau Veritas is the guarantor of the security and the continuity of the information system of Bureau Veritas group, its entities and its subsidiaries. As such, he is in charge of the Information Security Management System of Bureau Veritas.

The Global CISO carries out his duties within Bureau Veritas and alongside Suppliers, Customers and external third-parties (e.g. government entities, certification bodies).

3.2.2. ASSIGNMENTS OF THE GLOBAL CISO

The Global CISO of Bureau Veritas is in charge of the Information Security Management System of the organization and its maintenance in operational conditions. As part of this duty, his missions are:

- Formalize, coordinate and maintain in operational conditions the organization of the information system security stream of Bureau Veritas.
- Define training and awareness campaigns.
- Approve the appointment of OG SOs.
- Produce global security dashboards, centralize indicators from OG SOs and perform global analysis of information system security performance.
- Develop and update ISS Policies.
- Get Executive Management approval for ISS Policies.
- Enforce and accompany ISS Policies implementation within the Bureau Veritas group, its entities and subsidiaries.
- Monitor the compliance with the ISS Policies within the Bureau Veritas group.
- Handle derogations to ISS Policies with a global scope or a critical impact.
- Plan and oversee audits on the information system for security purposes and follow the corrective action plan built with audits' recommendations.
- Approve, advise and monitor local information security audits with the OG SO;
- Participate to Change Advisory Boards (CAB), in particular for changes with a critical or a large impact on the Bureau Veritas information system.
- Monitor the implementation and the maintenance in operational conditions of the security incident management process of Bureau Veritas and its regular testing, in particular for ensuring the efficiency of the crisis management plan and the crisis unit.
- Monitor the implementation and the maintenance in operational conditions of the Business Continuity Plan of Bureau Veritas and its regular testing.

3.3. OPERATIONAL GROUP SECURITY OFFICERS (OG SO) OF BUREAU VERITAS

3.3.1. PRESENTATION OF THE OG SO

OG Security Officers are the guarantors of the security and the continuity of the information system of Bureau Veritas at OG level. They are appointed at OG level and will be trusted partners for the central team.

Their main duties are the execution and supervision of the information security activities on their scope within businesses and technical teams, but also to ensure the implementation of global initiatives on their respective scope, especially the application of policies and compliance frameworks.

3.3.2. ASSIGNMENTS OF OG SO

OG Security Officers of Bureau Veritas are in charge of the implementation of Information Security Management System and its maintenance in operational conditions within their respective scope. As part of their duty, their missions are:

- Report important information to the Global CISO.
- Enforce the implementation of ISS Policies.
- Handle derogations to ISS Policies on their scope.
- Ensure that good security practices are followed.
- Define dedicated training and awareness campaigns.
- Produce local security dashboards, analyze security indicators and send them to the Global CISO.
- Coordinate local security actions.
- Contribute, with businesses and IT/IS Departments, to the transcription of Operational Policies into technical procedures (e.g. installation, operation, event handling), guides and standards.
- Approve, advise and monitor local information security audits with the Global CISO.
- Participate to Change Advisory Boards (CAB) for changes on the information system impacting their scope.
- Ensure the maintenance in operational conditions of the security incident management process on their scope.
- Ensure the maintenance in operational conditions of the Business Continuity Plan on their scope.

3.4. LOCAL SECURITY CORRESPONDENTS

In addition to the Global CISO and OG SOs described above, the information security organization involves local security correspondents.

OG Security Officers identify and supervise Local security correspondents within entities, subsidiaries, departments, businesses, and wherever necessary. Local Security correspondents assist the OG SOs in their missions, implement information security on their scope or develop projects based on specific security needs.

3.5. CONTACT WITH AUTHORITIES AND SPECIAL INTEREST GROUPS

Where appropriate, Bureau Veritas and its subsidiaries establishes and maintains contact with appropriate authorities.

Moreover, when relevant, Bureau Veritas should establish and maintain contact also with special interest groups or other specialist security forums and professional associations.

Having established contact channels with the parties mentioned above can be necessary for compliance (e.g. notifying relevant authorities of a data breach). In addition, special interest groups or other specialist security forums and professional associations can help the company anticipate development of the cybersecurity field and prepare for change and evolution. These connections might also come in handy in case support / advice is required when faced with a challenging situation.

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
4.4	ISS Compliance	Annual review	20/04/2023

4.2. APPENDIX 2: OPERATIONAL POLICIES

The Operational Policies completing the Global ISSP on thematic subjects for Bureau Veritas are:

- Human Resource Security
- Classification of Information
- Logical Access Control
- Physical Security
- Operations Security
- Management of IT Traces
- Media Handling
- Users' Equipment
- Network Security
- Cloud Security
- Development and Maintenance of Applications
- Suppliers Relationship
- Management of Security Incidents
- Activity Continuity