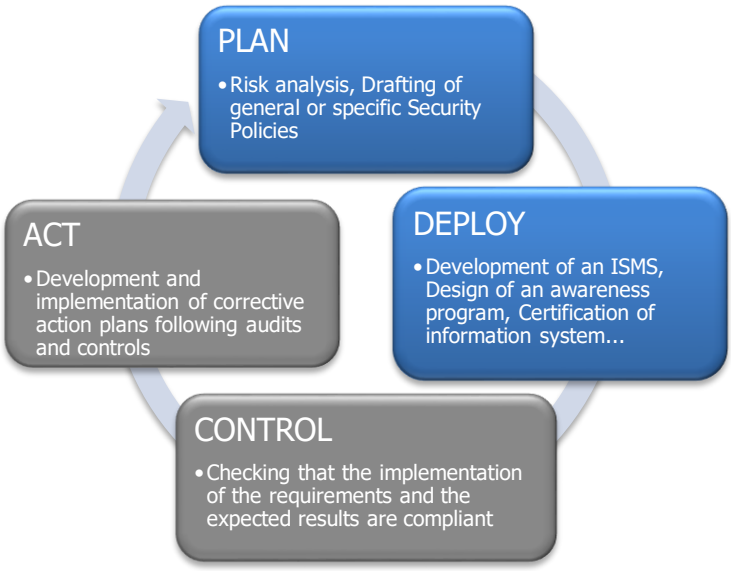
Information Security Management System Policy NRB S.A.

1 Aims

The global approach of the Information Security Management System (ISMS) is to guarantee the sustainability of security in all the processes included in the scope through a PDCA approach. This approach implies industrialisation of Information System security at all levels and involvement with all stakeholders.



This approach takes into account the following restrictions:

- the legal requirements in force in Belgium and in Greece;
- the regulatory requirements;
- the requirements of our customers.

2 Scope of applicability

The information security management system covers:

- Operational management of IT infrastructure, software development, integration and maintenance, consultancy and 'Managed Staffing'.
- NRB's Information System, which enables the activities covered to be carried out.
- NRB data centers located in Herstal.

2.1 Presentation of NRB (Network Research Belgium)

NRB was founded in 1987 and is now one of the major providers of IT services in Belgium.

NRB is in a position to offer a complete range of global ICT services and solutions to support its clients throughout the life cycle of their IT projects. Assuch, NRB sets up and manages a private and hybrid cloud infrastructure. At the same time, NRB designs the architecture and develops, manages, and maintains the applications (mainframe or open systems), whether they are custom-designed or customized and configured from ERP (Enterprise Resource Planning) [SAP], ECM (Enterprise Content

Management) or BI (Business Intelligence) software packages. NRB also offers Consulting and Managed Staffing services. With over 35 years of experience, NRB provides IT solutions and services to the financial sector, the public and social sector at both regional and federal level, the healthcare and public utilities sectors, industry and the biotech sector.

2.2 Internal organisational structure

NRB is organized around three components, namely "Sales", "Delivery" and "Central Services", in order to guarantee its service offering to its clients.

The mission of the Sales entities is:

- to retain current clients and develop a profitable business flow;
- to attract new clients with profitable contracts and boost the growth of NRB

by offering solutions and services provided primarily by NRB's Delivery Services Lines, branches and subsidiaries.

The Sales entities are each responsible for specific market sectors divided by business line. Three transversal entities provide the Sales entities with support services in Bid management and Marketing.

Client Delivery will be structured into "Competence Centers", where employees will be grouped according to their job and areas of expertise. Depending on customers' needs and the business skills required for their projects (products/services), members will be mobilized in multi-disciplinary teams within "Delivery Units".

The Sales entities and Delivery divisions are supported by the Central Functions:

- Finance, Acquisitions & Subsidiaries
- HR & Internal Communication
- Quality & Risk Management
- Secretary General
- Chief Security Officer & Partner Management

2.3 Scope of applicability

2.3.1 Geographic scope

The company, whose headquarters are at Herstal, has a presence in Belgium and Greece.

The NRB data center is located at the company's headquarters in Herstal. NRB also has a data center at Villers-le-Bouillet (30 km from the Herstal site), owned by BelgiumDC, a joint venture in which NRB has a 50 % stake.

NRB S.A. carries out its activities at various operating sites, namely:

- Parc Industriel des Hauts Sarts, 2ème Avenue 65, 4040 Herstal, Belgium
- Interleuvenlaan 10, 3001 Heverlee, Belgium
- Ethnikis Antistasis Street 67, 15231 Chalandri, Greece

The geographic scope of the ISMS includes NRB's data center as well as its operating sites.

NRB's subsidiaries are not included in the scope of the ISMS. Only NRB S.A. falls within the scope of the ISMS.

2.3.2 Human scope

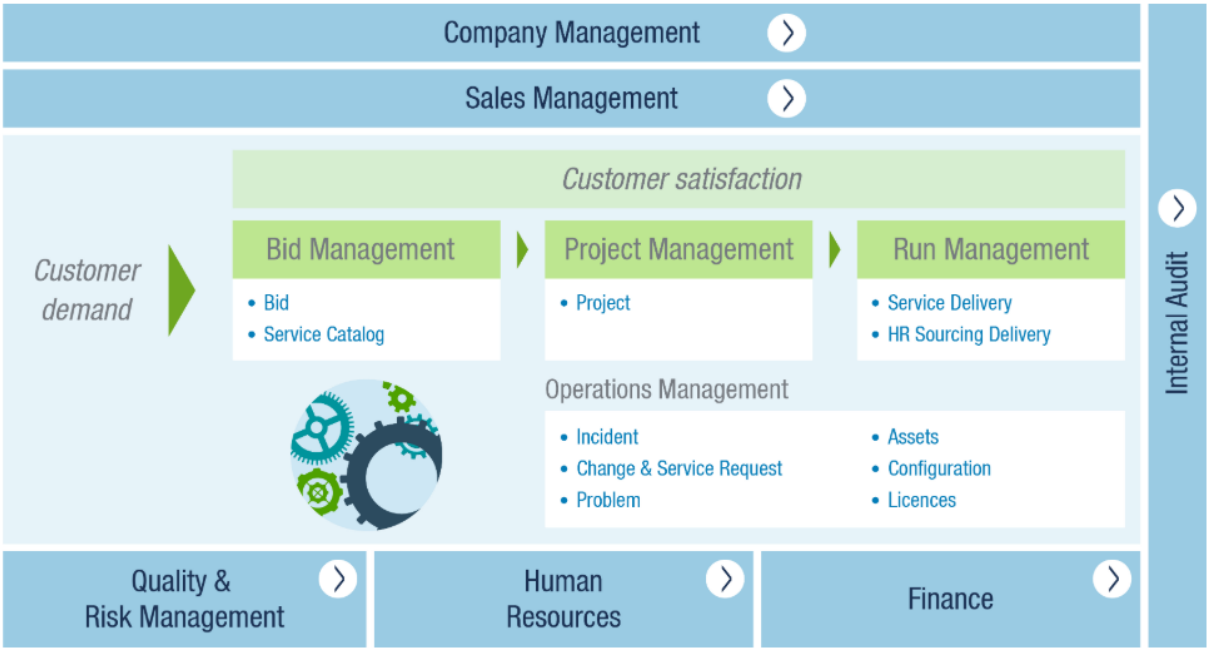
The human scope of the ISMS includes all the NRB teams responsible for the administration of the Data centrer and business services provided by NRB.

The staff included in the certification scope performs tasks that are included in the scope of the ISMS.

2.3.3 Scope and limits of ISMS

2.3.3.1 Scope of the ISMS

NRB is organized around processes. The map below shows the scope of the ISMS, with the various processes:



The scope includes all the services that NRB provides to its clients via the abovementioned processes, with infrastructure equipment owned or leased by NRB, namely:

- server and storage racks
- computer servers
- hosting facilities
- telecom links
- network infrastructure owned by NRB.

NRB is a client of its own data center business which hosts the data of the entire company. Its scope includes:

- NRB's internal information system (data and all the resources enabling that data to be processed in any way);
- the data center's administration information system;
- applications owned by NRB (the owner of the data uses NRB's internal shared applications);
- NRB's internal applications;
- data owned by NRB.

2.3.3.2 The limits of the ISMS

Although NRB operates certain aspects of its clients' security, the following are excluded from the scope of the ISMS 27001 and are therefore beyond the scope of ISO 27001 certification:

- NRB's clients' information systems and data;
- equipment and software for which the responsibility of security management is left to clients and suppliers.

If necessary, a detailed up-to-date description of the Information System assets that are included in the scope of the ISMS is available in the CMDB (Configuration Management Database) as well as in the Asset Management Database.

3 Commitment

Mission, vision and values

The vision of NRB describes our ambition, the influence we want to have on society:
NRB shapes the digital future and contributes to a more connected, secure, inclusive and sustainable society. Through impactful and responsible technological solutions, NRB simplifies and enriches everyone's daily life.

The mission determines our reason for being. It explains the markets on which we operate, our goals and our specific features:
NRB supports European private and public sector organizations by taking charge of all their technological needs, while drawing on an in-depth understanding of their businesses.
With the expertise of its employees, a solid technological ecosystem and a sovereign approach, NRB acts as an integrator of complete solutions, enabling its customers to cope with their daily challenges.

As such, and in view of the new risks brought about by the use of technology, it is now inevitable that we must consider the security of the information systems as one of the pillars of our service provision. To demonstrate our ongoing commitment to protecting our clients' information assets, we are engaged in the ISO 27001:2022 certification process.

Given that the security of our services and data is at the heart of our strategic plan, ISO 27001:2022 certification is a valuable asset for the development of the company.

The resulting values are transparent in our relationships with our employees, our partners, our shareholders, society in general and, of course, our customers.

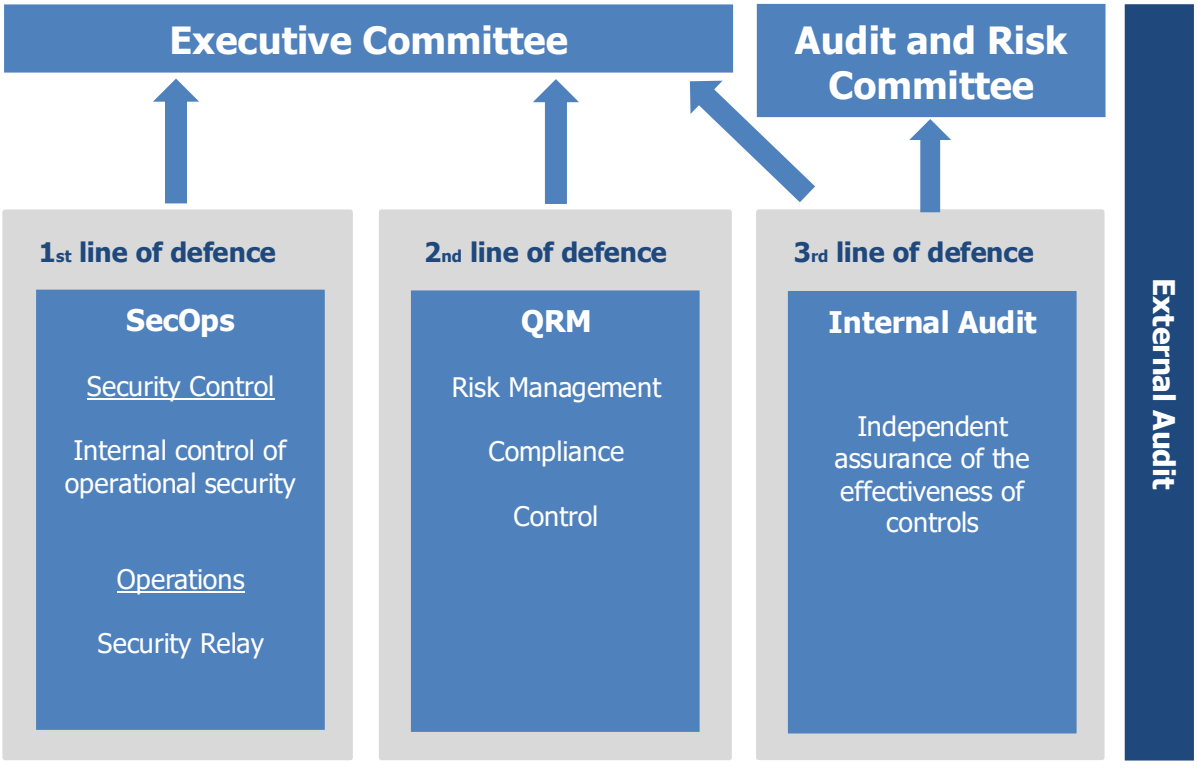
- Integrity : We stand by our commitments, we value transparency and honesty. Guided by our business ethics, we build relationships based on trust and reliability;
- Enthusiasm : We all create a dynamic working environment, and we foster a positive atmosphere. We enjoy what we do together and celebrate success;
- Empathy : We actively listen to understand the needs of colleagues, customers and partners. We collaborate through respectful and authentic relationships;
- Performance : Together, we work to achieve or exceed our goals through efficiency, quality and continuous improvement;
- Ingenuity : By working together, we challenge the standards, and we proactively propose pragmatic and innovative solutions. We overcome obstacles thanks to our curiosity.

This policy has been approved by the NRB Executive Committee, which is committed to providing the means necessary to implement it.

Responsibility for the ISMS is entrusted to the Chief Information Security Officer.
Every employee of NRB is also required to comply with the ISMS Policy.

4 Roles and responsibilities

The governance of the ISMS is based on a structure made up of 3 lines of defence. Steering and communication are carried out through committees.



4.1 First line – SecOps Service

The director of the SecOps department (Chief Security Officer or CSO) is responsible for the first line of defence, that is to say integrating security into operational processes. He liaises with the CISO (Chief Information Security Officer) regarding the second line of defence.

As such, he is responsible for:

- operational security management;
- management of operational security control team and security relays;
- managing the skills of members of the operational security control team;
- alignment of operational security with security policy as defined by the CISO;
- implementation of the security plan and objectives defined by the CISO;
- identification of deviations from the policies, processes and standards defined;
- organization of the security Executive Committee.

4.1.1 Internal control of operational security

The internal security control department is headed by the CSO and supervises operational security activities. This department is responsible for the following activities:

- steering the implementation and improvements of operational security management processes;
- monitoring compliance of the processes implemented;
- steering the resolution of security incidents;
- tracking opened problems following security incidents;
- the implementation and reporting of performance indicators for security measures;
- validation of security operations (SRQ with high risk);
- validation of the compliance of technical procedures and solutions deployed by Delivery;
- technical security tests.

4.1.2 Security relay

The Security Relay is a security expert in a specific technological field. He is in charge of operational security tasks and supports operational security control with his expertise. He:

- reports any deviations from defined standards and processes to SecOps and QRM;
- participates in drafting security procedures in collaboration with SecOps, and security policies with QRM;
- ensures that SecOps and QRM are informed of INTERNAL projects with a security impact carried out by his team, via monthly roadmap reviews;
- ensures that relevant information on projects discussed at monthly roadmap reviews is shared with his team.

4.2 Second line – Service Quality & Risk Management

The Quality & Risk Management manager is responsible for:

- approving the security plan and objectives for validation by the Executive Committee;
- organising and participating in the security management review meeting with the Executive Committee.

4.2.1 Chief Information Security Officer (CISO)

The CISO is the guarantor of the security of NRB's information system. He intervenes across all the Information Systems of the organisation from an organisational and technical point of view, in synergy with the different departments and their different projects.

The objectives of the CISO are translated into management, supervision, and steering activities as presented schematically below:

Security requirements and guidelines

- Defines, in close collaboration with staff, the security policies by including the qualitative and quantitative requirements.
- Maintains security guidelines in operational conditions.
- Monitors compliance with policies and requirements.
- Validates compliance of technical processes and solutions implemented by the SecOps service.

Risk and project management

- Establishes security risk management in line with business strategy and maintains an acceptable threat exposure validated by the Executive Committee.
- Ensures that project specifications are defined and information security risks and requirements are identified.
- Regularly reviews the risks and defines mitigation plans.

Security management and master plan

- Coordinates all security-related actions between the various stakeholders and highlights any information considered important to the Executive Committee.
- Supervises regulatory monitoring.
- Proposes the Security strategy in line with the objectives of NRB.
- Translates the master plan validated in action plan.
- Develops a security dashboard for stakeholders.

Skills and awareness management

- Assists management in defining roles and responsibilities in relation to security.
- Organizes and defines action plans for training, awareness raising and management of the company’s security culture.

Incident management

- Controls the process for handling security incidents.

Resilience

- Defines requirements of the information security and business continuity management system in accordance with the business continuity strategy defined by the Business Continuity Manager.

4.3 Third line – Internal audit

The internal auditor reports administratively and functionally to the Chief Executive Officer, and at the same time to the Audit & Risk Committee (as delegated by the Board of Directors). The internal auditor has direct access to the President of the Audit Committee at all times.

The **mission** of Internal Audit is to provide independent and objective assurance aimed at adding value and improving the operations of NRB. Internal Audit helps the organisation achieve its objectives by providing a systematic and disciplined approach to assessing and improving the effectiveness of the control, risk management and governance processes.

A high-level **three-year audit plan** and an annual audit plan are established in consultation with the Executive Committee and the Audit & Risk Committee, based on a risk assessment.

The **purpose** of Internal Audit is to determine whether risk management, control activities, technology and governance processes, as designed and represented by the management of NRB, are adequate and operate in such a way as to guarantee that:

- risks are identified and managed appropriately;
- interaction with the various governance entities and control functions takes place as required;
- significant financial, management and operating information is accurate, reliable and timely;
- employee actions comply with applicable policies, standards, procedures, laws and regulations;
- resources are acquired economically, used efficiently and protected adequately;
- program and plan objectives are met;
- quality and continuous improvement are fostered in the organisation's control process;
- significant legal or regulatory issues that could affect NRB are recognised and resolved in a timely and appropriate manner.

Opportunities to improve internal controls, operational efficiency and NRB's reputation can also be identified during the audits. They will be communicated to the appropriate management level.

Internal Audit ensures the execution of said internal audit plan and covers the following **areas**:

- operational activities;
- management system certifications (among others, ISO 9001 and ISO 27001);
- financial activities;
- risk management and compliance;
- information and information system management, including security and control aspects;
- all other activities, including human resources and administrative functions.

5 The Committees

5.1 The Executive Committee

Led by the CEO, the Executive Committee is responsible for:

- checking that the ISMS policy is in line with the challenges of NRB;
- monitoring the strategic indicators of the ISMS;
- approving the strategic direction of security (annual plan and security objectives);
- validating budgets and the workforce in relation to security;
- holding a management review including information security aspects as a minimum once a year.

Participants:
The Executive Committee is composed of the Chief Executive Officer (CEO), the Chief Financial Officer (CFO), the Chief HR Officer (CHRO), the Chief Operations Officer – Infrastructure (COO-I), the Chief Operations Officer – Applications (COO-A) and the Chief Commercial Officer (CCO).
The Director of Quality & Risk Management (QRM) is a permanent guest, especially for security-related matters. The Chief Security Officer (CSO) may also be invited as required.

5.2 The Audit & Risk Committee

The Audit & Risk Committee, as delegated by the Board of Directors:

- validates the Internal Audit Charter. The Charter defines the principles, basic roles and responsibilities of the internal audit function within the organisation. The Charter defines the position of the internal audit within the organisation, including the nature of the functional relationship between the internal audit, management (Management Committee), the Board of Directors and the Audit Committee;
- validates the Three-year audit plan;
- reviews the results of all the audits and risks identified;
- monitors the implementation of action plans.

5.3 The security SteerCo

The Security Steering Committee (SteerCo), entity for ISMS tactical monitoring, is led by the Chief Security Officer and meets at least **once a month**.

Objectives:

- to ensure the monitoring of the security program;
- to approve the tactical security strategy;
- to monitor the strategic indicators of the ISMS;
- to monitor important action plans following audits;
- to report information on major security incidents and problems.

Participants:
The members constituting the security Steerco are:

- the Chief Security Officer
- the QRM Manager
- the Chief Information Security Officer (CISO)
- by invitation: Project Manager or security project stakeholders

5.4 The Ops Security SteerCo

The Ops Security SteerCo, the ISMS's operational monitoring body is headed by the CISO and meets at least once every 2 weeks.

Objectives:

- to monitor performance indicators for security measures.
- to follow up on security incidents and problems.
- to monitor action plans following audits.
- to raise security alerts and deviations from policies.
- to pass on security information.

Participants:

The members constituting Ops Security SteerCo are:

- the Chief Information Security Officer
- the Chief Security Officer or his/her representative
- stakeholders, depending on the subjects discussed (Security Control, Internal IT, business lines)

5.5 Recordings of committee meetings

Records are produced for meetings of all these committees.

5.6 RACI

	Executive Committee	QRM Manager	CISO	CSO SecOps	Operational actors	Anyone working for NRB
Propose		C	A/R	R		
Validate	A	C	R	C		
Monitor the application	A		R	R		
Apply/ Observe						A
Maintain		C	A/R	R		
Communicate		A	R	R	C	I

R = responsible = whoever is responsible for carrying out the activity
A = accountable = whoever is ultimately responsible for the activity, i.e. whoever has to account for the progress and quality of the activity
C = consulted = the people who must be consulted
I = informed = the people who must be informed

6 Guiding principles/basic rules

- Engage in responsibilities through the governance of information system security and the Executive Committee;
- Protect data center information from internal and external threats, whether deliberate or accidental;
- Deploy a risk-based approach;
- Develop organisational resilience in a secure manner;
- Reduce exposure to internal and external threats;
- Implement permanent and periodic control of the various security requirements;
- Raise awareness and train staff as a whole;
- Manage the security of the Information System;
- Continually improve skills.

7 Measures and controls implemented

In order to ensure that business and IT activities are harmonised with regard to the security of Information Systems, a risk management process has been implemented. This process is based on the ISO 27005:2018 standard.

Four criteria are used to assess the risks:

- **Confidentiality:** the confidentiality of customer information must be ensured. In addition, access to different parts of the data center must be controlled;
- **Integrity:** the integrity of customer information must be ensured;
- **Availability:** the information must be available to staff maintaining the data center and customers who benefit from its services, as defined in the company procedures and the quality of service obligations towards customers;
- **Proof:** the traceability of access to customer information or to NRB's own information must be ensured.

The details of the security risk analysis methodology used at NRB is documented in the document «Security risk analysis method».

8 Review

This policy must be systematically reviewed annually (date of publication + 1 year).

In addition to annual revision, this policy is amended whenever there is a major change in the organization that impacts on the ISMS, so as to take account of the modifications and thus guarantee optimum maintenance of security risk management.

9 Annexes

9.1 References

Reference documents:

- Security risk analysis method
- ISO/CEI 27001:2022

9.2 Document management

Editor	Thibault Dutrieux			
Updates	Version	Date	Description	
	4.4	12/12/2024	Minor updates with the new NRB's missions, vision and values	
Validation	4.4	16/12/2023	Reread and validated by Emmanuelle Lhermitte	Final
	4.3	21/11/2023	Executive Committee	Final
	4.4	20/12/2024	Executive Committee	Final
Document status	**Approved by the NRB Executive Committee**			