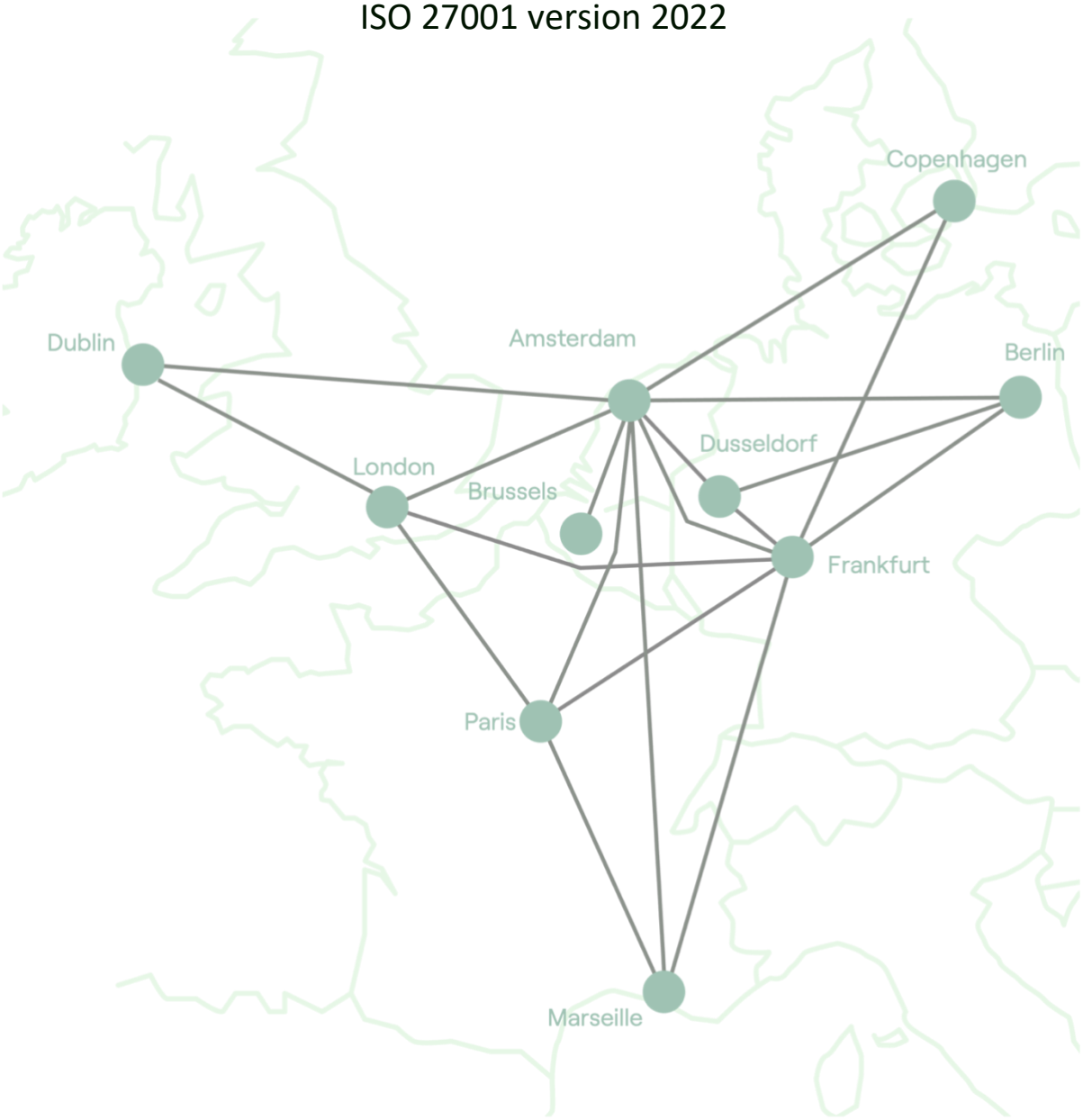
BE THE
INTERNET

Statement of Applicability (SoA)

ISO 27001 version 2022



Company: Broadband Hosting B.V. (NL-ix)

Author: Daniele Menichini

Date: 26 April 2023

Version: 4.1

Table of Contents

1. Introduction

Broadband Hosting B.V. (Hereafter NL-ix) interconnects networks, data centers and applications over a converged exchange fabric. NL-ix has implemented the Information Security Management System (ISMS) and associated controls in accordance with ISO/IEC 27001:2022 (hereafter: ISO 27001).

This Statement of Applicability (SoA) specifies which objectives and controls of ISO 27001 are applicable to the service delivery of NL-ix:

- The applicable standards contain a reference to a page in which the application of that standard is explained.
- The standards that do not apply contain a justification for the exclusion.

1.1. Scope

The scope of the ISMS encompasses:

- Information
  - Company documentation
  - Employee information
- Information systems (applications)
- Services
  - Peering
  - Transit
  - Wave
  - MPLS
  - Cloud
  - SaaS
  - Elastic Interconnect
- Location
  - Röntgenlaan 75, Zoetermeer
  - Barbara Strozzilaan 251, Amsterdam
- Employees
- Customers
- All processes (Strategic, Tactical, Operational)

Excluded from the scope are customer data and customer information systems. These are the responsibility of the customer.

1.2. Document control

Version	Date	Description
1.0	7 August 2020	*First version of the SOA*
2.0	3 February 2021	*Final version before the official audit*
3.0	15 March 2022	*Added to the scope the development activities*
3.1	25 April 2022	*Changed style based on the new branding*
4.0	9 November 2023	*Updated based on version 2022 of the standard*
4.1	26 April 2024	*Updated information security controls*

2. Mandatory controls

2.1. Context of the organization

Understanding the organization and its context
The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system.
Understanding the needs and expectations of interested parties
The organization shall determine: a) interested parties that are relevant to the information security management system; b) the relevant requirements of these interested parties; c) which of these requirements will be addressed through the information security management system.
Determining the scope of the information security management system
The organization shall determine the boundaries and applicability of the information security management system to establish its scope. When determining this scope, the organization shall consider: a) the external and internal issues referred to in "*Understanding the organization and its context*"; b) the requirements referred to in "*Understanding the needs and expectations of interested parties*"; c) interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations. The scope shall be available as documented information.
Information security management system
The organization shall establish, implement, maintain and continually improve an information security management system, including the processes needed and their interactions, in accordance with the requirements of this document.

2.2. Leadership

Leadership and commitment

Top management shall demonstrate leadership and commitment with respect to the information security management system by:
a) ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization;
b) ensuring the integration of the information security management system requirements into the organization's processes;
c) ensuring that the resources needed for the information security management system are available;
d) communicating the importance of effective information security management and of conforming to the information security management system requirements;
e) ensuring that the information security management system achieves its intended outcome(s);
f) directing and supporting persons to contribute to the effectiveness of the information security management system;
g) promoting continual improvement; and
h) supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.

Policy

Top management shall establish an information security policy that:
a) is appropriate to the purpose of the organization;
b) includes information security objectives (see 6.2) or provides the framework for setting information security objectives;
c) includes a commitment to satisfy applicable requirements related to information security;
d) includes a commitment to continual improvement of the information security management system.
The information security policy shall:
e) be available as documented information;
f) be communicated within the organization;
g) be available to interested parties, as appropriate.

Organizational roles, responsibilities and authorities

Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated within the organization.

Top management shall assign the responsibility and authority for:
a) ensuring that the information security management system conforms to the requirements of this document;
b) reporting on the performance of the information security management system to top management.

2.3. Planning

Actions to address risks and opportunities

General

When planning for the information security management system, the organization shall consider the issues and the requirements referred and determine the risks and opportunities that need to be addressed to:
a) ensure the information security management system can achieve its intended outcome(s);
b) prevent, or reduce, undesired effects;
c) achieve continual improvement.
The organization shall plan:
d) actions to address these risks and opportunities; and
e) how to
    1) integrate and implement the actions into its information security management system processes; and
    2) evaluate the effectiveness of these actions.

Information security risk assessment

The organization shall define and apply an information security risk assessment process that:
a) establishes and maintains information security risk criteria that include:
    1) the risk acceptance criteria; and
    2) criteria for performing information security risk assessments;
b) ensures that repeated information security risk assessments produce consistent, valid and comparable results;
c) identifies the information security risks:
    1) apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information security management system; and
    2) identify the risk owners;
d) analyses the information security risks:
    1) assess the potential consequences that would result if the risks identified were to materialize;
    2) assess the realistic likelihood of the occurrence of the risks identified and
    3) determine the levels of risk;
e) evaluates the information security risks:

1) compare the results of risk analysis with the risk criteria established
2) prioritize the analysed risks for risk treatment.

The organization shall retain documented information about the information security risk assessment Process.

Information security risk treatment

The organization shall define and apply an information security risk treatment process to:
a) select appropriate information security risk treatment options, taking account of the risk assessment results;
b) determine all controls that are necessary to implement the information security risk treatment option(s) chosen;
c) compare the controls above with those in Annex A and verify that no
necessary controls have been omitted;
d) produce a Statement of Applicability that contains:
the necessary controls, justification for their inclusion; whether the necessary controls are implemented or not; and the justification for excluding any of the Annex A controls.
e) formulate an information security risk treatment plan; and
f) obtain risk owners' approval of the information security risk treatment plan and acceptance of the residual information security risks.
The organization shall retain documented information about the information security risk treatment process

Information security objectives and planning to achieve them

The organization shall establish information security objectives at relevant functions and levels. The information security objectives shall:
a) be consistent with the information security policy;
b) be measurable (if practicable);
c) take into account applicable information security requirements, and results from risk assessment and risk treatment;
d) be monitored;
e) be communicated;
f) be updated as appropriate;
g) be available as documented information.
The organization shall retain documented information on the information security objectives.
When planning how to achieve its information security objectives, the organization shall determine:
h) what will be done;
i) what resources will be required;
j) who will be responsible;

k) when it will be completed; and
l) how the results will be evaluated.

Planning of changes

When the organization determines the need for changes to the information security management system, the changes shall be carried out in a planned manner.

2.4. Support

Resources
The organization shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the information security management system.
Competence
The organization shall: a) determine the necessary competence of person(s) doing work under its control that affects its information security performance; b) ensure that these persons are competent on the basis of appropriate education, training, or experience; c) where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken; and d) retain appropriate documented information as evidence of competence.
Awareness
Persons doing work under the organization's control shall be aware of: a) the information security policy; b) their contribution to the effectiveness of the information security management system, including the benefits of improved information security performance; and c) the implications of not conforming with the information security management system requirements.
Communication
The organization shall determine the need for internal and external communications relevant to the information security management system including: a) on what to communicate; b) when to communicate; c) with whom to communicate; d) how to communicate.
Documented information
General

The organization's information security management system shall include:
a) documented information required by this document; and
b) documented information determined by the organization as being necessary for the effectiveness of the information security management system.

Creating and updating

When creating and updating documented information the organization shall ensure appropriate:
a) identification and description (e.g. a title, date, author, or reference number);
b) format (e.g. language, software version, graphics) and media (e.g. paper, electronic); and
c) review and approval for suitability and adequacy.

Control of documented information

Documented information required by the information security management system and by this document shall be controlled to ensure:
a) it is available and suitable for use, where and when it is needed; and
b) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).
For the control of documented information, the organization shall address the following activities, as applicable:
c) distribution, access, retrieval and use;
d) storage and preservation, including the preservation of legibility;
e) control of changes (e.g. version control); and
f) retention and disposition.
Documented information of external origin, determined by the organization to be necessary for the planning and operation of the information security management system, shall be identified as appropriate, and controlled.

2.5. Operation

Operational planning and control
The organization shall plan, implement and control the processes needed to meet requirements, and to implement the actions determined in Planning, by: — establishing criteria for the processes; — implementing control of the processes in accordance with the criteria. Documented information shall be available to the extent necessary to have confidence that the processes have been carried out as planned. The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary. The organization shall ensure that externally provided processes, products or services that are relevant to the information security management system are controlled.
Information security risk assessment
The organization shall perform information security risk assessments at planned intervals or when significant changes are proposed or occur. The organization shall retain documented information of the results of the information security risk assessments.
Information security risk treatment
The organization shall implement the information security risk treatment plan. The organization shall retain documented information of the results of the information security risk treatment.

2.6. Performance evaluation

Monitoring, measurement, analysis and evaluation

The organization shall determine:
a) what needs to be monitored and measured, including information security processes and controls;
b) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results. The methods selected should produce comparable and reproducible results to be considered valid;
c) when the monitoring and measuring shall be performed;
d) who shall monitor and measure;
e) when the results from monitoring and measurement shall be analysed and evaluated;
f) who shall analyse and evaluate these results.
Documented information shall be available as evidence of the results.
The organization shall evaluate the information security performance and the effectiveness of the information security management system.

Internal audit

General

The organization shall conduct internal audits at planned intervals to provide information on whether the information security management system:
a) conforms to
    1) the organization's own requirements for its information security management system;
    2) the requirements of this document;
b) is effectively implemented and maintained.

Internal audit programme

The organization shall plan, establish, implement and maintain an audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting.
When establishing the internal audit programme(s), the organization shall consider the importance of the processes concerned and the results of previous audits.
The organization shall:
a) define the audit criteria and scope for each audit;
b) select auditors and conduct audits that ensure objectivity and the impartiality of the audit process;

c) ensure that the results of the audits are reported to relevant management;
Documented information shall be available as evidence of the implementation of the audit programme(s) and the audit results.

Management review

General

Top management shall review the organization's information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness.

Management review inputs

The management review shall include consideration of:
a) the status of actions from previous management reviews;
b) changes in external and internal issues that are relevant to the information security management system;
c) changes in needs and expectations of interested parties that are relevant to the information security management system;
d) feedback on the information security performance, including trends in:
    1) nonconformities and corrective actions;
    2) monitoring and measurement results;
    3) audit results;
    4) fulfilment of information security objectives;
e) feedback from interested parties;
f) results of risk assessment and status of risk treatment plan;
g) opportunities for continual improvement.

Management review results

The results of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the information security management system.
Documented information shall be available as evidence of the results of management reviews.

2.7. Improvement

Continual improvement
The organization shall continually improve the suitability, adequacy and effectiveness of the information security management system.
Nonconformity and corrective action
When a nonconformity occurs, the organization shall: a) react to the nonconformity, and as applicable: 1) take action to control and correct it; 2) deal with the consequences; b) evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere, by: 1) reviewing the nonconformity; 2) determining the causes of the nonconformity; and 3) determining if similar nonconformities exist, or could potentially occur; c) implement any action needed; d) review the effectiveness of any corrective action taken; and e) make changes to the information security management system, if necessary. Corrective actions shall be appropriate to the effects of the nonconformities encountered. Documented information shall be available as evidence of: f) the nature of the nonconformities and any subsequent actions taken, g) the results of any corrective action.

3. Information security controls

3.1. Organizational controls

1. **Policies for information security**	Information security policy and topic-specific policies shall be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.	In scope: **Yes** ☒ LR ☐ CO ☒ BR/BP ☐ RRA
2. **Information security roles and responsibilities**	Information security roles and responsibilities shall be defined and allocated according to the organization needs.	In scope: **Yes** ☒ LR ☒ CO ☒ BR/BP ☐ RRA
3. **Segregation of duties**	Conflicting duties and conflicting areas of responsibility shall be segregated.	In scope: **Yes** ☒ LR ☐ CO ☒ BR/BP ☒ RRA
4. **Management responsibilities**	Management shall require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization.	In scope: **Yes** ☒ LR ☐ CO ☒ BR/BP ☐ RRA
5. **Contact with authorities**	The organization shall establish and maintain contact with relevant authorities.	In scope: **Yes**

		☒ LR ☐ CO ☒ BR/BP ☐ RRA
6. **Contact with special interest groups**	The organization shall establish and maintain contact with special interest groups or other specialist security forums and professional associations.	In scope: **Yes** ☒ LR ☐ CO ☒ BR/BP ☐ RRA
7. **Threat intelligence**	Information relating to information security threats shall be collected and analysed to produce threat intelligence.	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☐ RRA
8. **Information security in project management**	Information security shall be integrated into project management.	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☐ RRA
9. **Inventory of information and other associated assets**	An inventory of information and other associated assets, including owners, shall be developed and maintained.	In scope: **Yes** ☒ LR ☐ CO ☒ BR/BP ☐ RRA
10. **Acceptable use of information and other associated assets**	Rules for the acceptable use and procedures for handling information and other associated assets shall be identified, documented and implemented.	In scope: **Yes**

		☒ LR ☐ CO ☒ BR/BP ☒ RRA
11. **Return of assets**	Personnel and other interested parties as appropriate shall return all the organization's assets in their possession upon change or termination of their employment, contract or agreement.	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☐ RRA
12. **Classification of information**	Information shall be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements.	In scope: **Yes** ☒ LR ☐ CO ☒ BR/BP ☐ RRA
13. **Labelling of information**	An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☐ RRA
14. **Information transfer**	Information transfer rules, procedures, or agreements shall be in place for all types of transfer facilities within the organization and between the organization and other parties.	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☐ RRA
15. **Access control**	Rules to control physical and logical access to information and other associated assets shall be established and implemented based on business and information security requirements.	In scope: **Yes**

		☐ LR ☐ CO ☒ BR/BP ☒ RRA
16. **Identity management**	The full life cycle of identities shall be managed.	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☒ RRA
17. **Authentication information**	Allocation and management of authentication information shall be controlled by a management process, including advising personnel on appropriate handling of authentication information.	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☐ RRA
18. **Access rights**	Access rights to information and other associated assets shall be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control.	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☐ RRA
19. **Information security in supplier relationships**	Processes and procedures shall be defined and implemented to manage the information security risks associated with the use of supplier's products or services.	In scope: **Yes** ☐ LR ☒ CO ☒ BR/BP ☒ RRA
20. **Addressing information security within supplier agreements**	Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship.	In scope: **Yes**

		☐ LR ☒ CO ☒ BR/BP ☒ RRA
21. **Managing information security in the information and communication technology (ICT) supply chain**	Processes and procedures shall be defined and implemented to manage the information security risks associated with the ICT products and services supply chain.	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☒ RRA
22. **Monitoring, review and change management of supplier services**	The organization shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☒ RRA
23. **Information security for use of cloud services**	Processes for acquisition, use, management and exit from cloud services shall be established in accordance with the organization's information security requirements.	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☒ RRA
24. **Information security incident management planning and preparation**	The organization shall plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.	In scope: **Yes** ☒ LR ☐ CO ☒ BR/BP ☒ RRA
25. **Assessment and decision on information security events**	The organization shall assess information security events and decide if they are to be categorized as information security incidents	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☐ RRA

26. **Response to information security incidents**	Information security incidents shall be responded to in accordance with the documented procedures.	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☐ RRA
27. **Learning from information security incidents**	Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls.	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☐ RRA
28. **Collection of evidence**	The organization shall establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events.	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☐ RRA
29. **Information security during disruption**	The organization shall plan how to maintain information security at an appropriate level during disruption.	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☐ RRA
30. **ICT readiness for business continuity**	ICT readiness shall be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements	In scope: **Yes** ☒ LR ☒ CO ☒ BR/BP ☒ RRA
31. **Legal, statutory, regulatory and contractual requirements**	Legal, statutory, regulatory and contractual requirements relevant to information security and the organization's approach to meet these	In scope: **Yes**

	requirements shall be identified, documented and kept up to date.	☒ LR ☐ CO ☒ BR/BP ☐ RRA
32. **Intellectual property rights**	The organization shall implement appropriate procedures to protect intellectual property rights.	In scope: Yes ☒ LR ☐ CO ☒ BR/BP ☐ RRA
33. **Protection of records**	Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release.	In scope: Yes ☐ LR ☐ CO ☒ BR/BP ☐ RRA
34. **Privacy and protection of personal identifiable information (PII)**	The organization shall identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.	In scope: **Yes** ☒ LR ☒ CO ☒ BR/BP ☐ RRA
35. **Independent review of information security**	The organization's approach to managing information security and its implementation including people, processes and technologies shall be reviewed independently at planned intervals, or when significant changes occur.	In scope: **Yes** ☒ LR ☐ CO ☒ BR/BP ☐ RRA

36. **Compliance with policies, rules and standards for information security**	Compliance with the organization's information security policy, topic-specific policies, rules and standards shall be regularly reviewed.	In scope: Yes ☐ LR ☐ CO ☒ BR/BP ☐ RRA
37. **Documented operating procedures**	Operating procedures for information processing facilities shall be documented and made available to personnel who need them.	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☒ RRA

Legend (reasons for control selection)

- *LR: legal requirements*
- *CO: contractual obligations*
- *BR/BP: business requirements/adopted best practices*
- *RRA: results of risk assessment*

3.2. People controls

1. **Screening**	Background verification checks on all candidates to become personnel shall be carried out prior to joining the organization and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	In scope: **Yes** ☒ LR ☐ CO ☒ BR/BP ☐ RRA
2. **Terms and conditions of employment**	The employment contractual agreements shall state the personnel's and the organization's responsibilities for information security.	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☐ RRA
3. **Information security awareness, education and training**	Personnel of the organization and relevant interested parties shall receive appropriate information security awareness, education and training and regular updates of the organization's information security policy, topic-specific policies and procedures, as relevant for their job function.	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☒ RRA
4. **Disciplinary process**	A disciplinary process shall be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation.	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☐ RRA
5. **Responsibilities after termination or change of employment**	Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, enforced and communicated to relevant personnel and other interested parties.	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☐ RRA

6. **Confidentiality or non-disclosure agreements**	Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☒ RRA
7. **Remote working**	Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises.	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☐ RRA
8. **Information security event reporting**	The organization shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☒ RRA

Legend (reasons for control selection)

- *LR: legal requirements*
- *CO: contractual obligations*
- *BR/BP: business requirements/adopted best practices*
- *RRA: results of risk assessment*

3.3. Physical controls

1. **Physical security perimeters**	Security perimeters shall be defined and used to protect areas that contain information and other associated assets.	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☐ RRA
2. **Physical entry**	Secure areas shall be protected by appropriate entry controls and access points.	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☐ RRA
3. **Securing offices, rooms and facilities**	Physical security for offices, rooms and facilities shall be designed and implemented.	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☐ RRA
4. **Physical security monitoring**	Premises shall be continuously monitored for unauthorized physical access.	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☐ RRA
5. **Protecting against physical and environmental threats**	Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure shall be designed and implemented.	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☒ RRA
6. Working in secure areas	Security measures for working in secure areas shall be designed and implemented.	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☐ RRA

7. **Clear desk and clear screen**	Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities shall be defined and appropriately enforced.	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☐ RRA
8. **Equipment siting and protection**	Equipment shall be sited securely and protected.	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☒ RRA
9. **Security of assets off-premises**	Off-site assets shall be protected.	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☐ RRA
10. **Storage media**	Storage media shall be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements.	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☐ RRA
11. **Supporting utilities**	Information processing facilities shall be protected from power failures and other disruptions caused by failures in supporting utilities.	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☒ RRA
12. **Cabling security**	Cables carrying power, data or supporting information services shall be protected from interception, interference or damage.	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☒ RRA

13. **Equipment maintenance**	Equipment shall be maintained correctly to ensure availability, integrity and confidentiality of information.	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☒ RRA
14. **Secure disposal or re-use of equipment**	Items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☒ RRA

Legend (reasons for control selection)

- *LR: legal requirements*
- *CO: contractual obligations*
- *BR/BP: business requirements/adopted best practices*
- *RRA: results of risk assessment*

3.4. Technological controls

1. **User end point devices**	Information stored on, processed by or accessible via user end point devices shall be protected.	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☒ RRA
2. **Privileged access rights**	The allocation and use of privileged access rights shall be restricted and managed.	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☐ RRA
3. **Information access restriction**	Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access control.	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☐ RRA
4. **Access to source code**	Read and write access to source code, development tools and software libraries shall be appropriately managed.	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☐ RRA
5. **Secure authentication**	Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access control.	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☒ RRA
6. **Capacity management**	The use of resources shall be monitored and adjusted in line with current and expected capacity requirements.	In scope: **Yes** ☒ LR ☐ CO ☒ BR/BP ☒ RRA
7. **Protection against malware**	Protection against malware shall be implemented and supported by appropriate user awareness.	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☒ RRA

8. **Management of technical vulnerabilities**	Information about technical vulnerabilities of information systems in use shall be obtained, the organization's exposure to such vulnerabilities shall be evaluated and appropriate measures shall be taken.	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☒ RRA
9. Configuration management	Configurations, including security configurations, of hardware, software, services and networks shall be established, documented, implemented, monitored and reviewed.	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☒ RRA
10. **Information deletion**	Information stored in information systems, devices or in any other storage media shall be deleted when no longer required.	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☐ RRA
11. **Data masking**	Data masking shall be used in accordance with the organization's topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration.	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☒ RRA
12. **Data leakage prevention**	Data leakage prevention measures shall be applied to systems, networks and any other devices that process, store or transmit sensitive information.	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☒ RRA
13. **Information backup**	Backup copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☐ RRA

14. **Redundancy of information processing facilities**	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	In scope: **Yes** ☒ LR ☐ CO ☒ BR/BP ☒ RRA
15. Logging	Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analysed.	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☐ RRA
16. **Monitoring activities**	Networks, systems and applications shall be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☐ RRA
17. **Clock synchronization**	The clocks of information processing systems used by the organization shall be synchronized to approved time sources.	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☐ RRA
18. **Use of privileged utility programs**	The use of utility programs that can be capable of overriding system and application controls shall be restricted and tightly controlled.	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☐ RRA
19. **Installation of software on operational systems**	Procedures and measures shall be implemented to securely manage software installation on operational systems.	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☒ RRA
20. Networks security	Networks and network devices shall be secured, managed and controlled to protect information in systems and applications.	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☒ RRA

21. **Security of network services**	Security mechanisms, service levels and service requirements of network services shall be identified, implemented and monitored.	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☐ RRA
22. **Segregation of networks**	Groups of information services, users and information systems shall be segregated in the organization's networks.	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☒ RRA
23. **Web filtering**	Access to external websites shall be managed to reduce exposure to malicious content.	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☐ RRA
24. **Use of cryptography**	Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☐ RRA
25. **Secure development life cycle**	Rules for the secure development of software and systems shall be established and applied.	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☒ RRA
26. **Application security requirements**	Information security requirements shall be identified, specified and approved when developing or acquiring applications.	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☐ RRA
27. **Secure system architecture and engineering principles**	Principles for engineering secure systems shall be established, documented, maintained and applied to any information system development activities.	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☐ RRA

28. **Secure coding**	Secure coding principles shall be applied to software development.	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☐ RRA
29. **Security testing in development and acceptance**	Security testing processes shall be defined and implemented in the development life cycle.	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☒ RRA
30. Outsourced development	The organization shall direct, monitor and review the activities related to outsourced system development.	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☐ RRA
31. **Separation of development, test and production environments**	Development, testing and production environments shall be separated and secured.	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☒ RRA
32. Change management	Changes to information processing facilities and information systems shall be subject to change management procedures	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☒ RRA
33. **Test information**	Test information shall be appropriately selected, protected and managed.	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☐ RRA
34. **Protection of information systems during audit testing**	Audit tests and other assurance activities involving assessment of operational systems shall be planned and agreed between the tester and appropriate management.	In scope: **Yes** ☐ LR ☐ CO ☒ BR/BP ☐ RRA

Legend (reasons for control selection)

- *LR: legal requirements*

- *CO: contractual obligations*
- *BR/BP: business requirements/adopted best practices*
- *RRA: results of risk assessment*