Statement of Applicability V5.1

Current as of : 10/2/2025

Section	Information security control	Applicable ?	Implemented ?	Justification for inclusions/exclusions	Selected Controls
A5	**Organizational controls**				
A.5.1	Policies for information security	Yes	Yes	ISMS and other policies are essentials to define the scope, expectations of the interested parties and the company's objectives and rules with regard to information security.	ISMS and other policies approved by Management and published on the Intranet. The policies are regularly reviewed and updated in case of major change that could impact the risk level.
A.5.2	Information security roles and responsibilities	Yes	Yes	The definition of roles and responsibilities is essential for the proper functioning of the ISMS.	The security organisation and responsibilities are defined in the ISMS policy. In the HR job description repository, there are records for the Information Security Manager & the Security Coordinator. Security Relays are listed in 'Liste des contacts/membres CGIS'.
A.5.3	Segregation of duties	Yes	Yes	Some roles are incompatible in the context of NRB activities.	Logical Access Control policy is defined and enforced with the help of our IAM platform. As example, developpers don't have access to production. When applicable, SoD is defined for specific data/platform.
A.5.4	Management responsibilities	Yes	Yes	NRB has employees and co-workers who have access to critical IS and data. They must be informed by the Management about the IS policies & rules.	ISMS and other policies are approved by Management and published on the Intranet. Awareness-raising is done by managers in the event of deviation. News is published on our Intranet in case of important change in a policy.
A.5.5	Contact with authorities	Yes	Yes	Some of the authorities requires incident reporting. The authorities are also a good source for information (guidance, threat, …)	Contact list on the Intranet : 'Liste des contacts majeurs en relation avec la sécurité de l'information en Belgique'. Reporting to authorities is integrated with our Crisis Management process. Integration of some authorities' information in our Threat Management process.
A.5.6	Contact with special interest groups	Yes	Yes	Gathering information about IS from external sources is essential to keep abreast of developments in the field.	Contact list on the Intranet : 'Liste des contacts majeurs en relation avec la sécurité de l'information en Belgique'. ISM member of several interest groups : ISO27K, ISC2, PECB, IBM Xforce, Microsoft, …
A.5.7	Threat intelligence	Yes	Yes	Threats particularly target IT services.	Threat Management process is defined and operated by our Secops department for our internal and mutualized services.
A.5.8	Information security in project management	Yes	Yes	Project management to deliver solutions and services to our customers is one of NRB's core businesses.	Project Management process is defined and implemented. It includes Stage Gates and Security-by-Design.
A.5.9	Inventory of information and other associated assets	Yes	Yes	In order to process its data or those of its customers, assets are used and must be managed and protected.	Information Classification policy to classify assets. Asset Management process & tool to manage assets. Configuration Management DB to store additionnal informations and link assets together.
A.5.10	Acceptable use of information and other associated assets	Yes	Yes	In order to process its data or those of its customers, assets are used and must be managed and protected.	Information Classification policy to give instruction on how to handle assets regarding their sensitivity. IT Charter & Employee awareness to give rules & guidance. Work Regulation to inform employee on their responsibilities. General terms and conditions of purchase to inform third parties on their obligations. Security requirements for external personnel to inform them on their responsibilities.

A.5.11	Return of assets	Yes	Yes	In order to process its data or those of its customers, assets are used and must be managed and protected.	HR Offboarding process includes return of assets. The obligations of external parties are set out in the General terms and conditions of purchase. Security requirements for external personnel to inform them on their responsibilities.
A.5.12	Classification of information	Yes	Yes	Data are processed and must be handled according to their level of confidentiality, integrity and availability.	Information Classification policy & one-pager to define levels and give instructions to end-users. IT Charter to give additional rules & guidance on how to handle & protect information. A specific e-learning module must be followed by all staff.
A.5.13	Labelling of information	Yes	Yes	Data are processed and must be handled according to their level of confidentiality, integrity and availability.	Information Classification policy & Post-it to give instructions to end-users. CIA levels of Business Services are defined in the CMDB. Instructions on the Intranet for end-users on how to label information and protect e-mail using available tools.
A.5.14	Information transfer	Yes	Yes	Data are processed and must be handled according to their level of confidentiality, integrity and availability.	Information Classification policy & Post-it to give instructions to end-users. IT Charter & Employee awareness to give rules & guidance. General terms and conditions of purchase to inform third parties on their obligations. Security requirements for external personnel to inform them on their responsibilities. Instructions on the Intranet for end-users on how to label information and protect e-mail using available tools.
A.5.15	Access control	Yes	Yes	NRB employees, co-workers and customers have access to data and services managed by NRB.	Logical Access Control policy is defined and implemented. Customer Identity and Access Management policy is defined and implemented for Online Services provided to our Customers. Network Security policy is defined and implemented for accessing our network. All access form untrusted network is subjet to MFA. Access Management Tool is used for automating most of our IAM processses.
A.5.16	Identity management	Yes	Yes	NRB employees, co-workers and customers have access to data and services managed by NRB.	Logical Access Control policy is defined and implemented. Customer Identity and Access Management policy is defined and implemented for Online Services provided to our Customers. Onboarding and Offboarding process is defined and implemented. Workforce Tool to support our IAM processes for external personel. Access Management Tool is used for automating most of our IAM processses.
A.5.17	Authentication information	Yes	Yes	NRB employees, co-workers and customers use passwords to authenticate themselves.	Information Classification policy & Post-it to give instructions to end-users. IT Charter & Employee awareness to give rules & guidance. Password policy for end-users is defined and enforced. Password policy for admins is defined and enforced. Password management tool (Vault) for storing and using securely secret Information.

A.5.18	Access rights	Yes	Yes	NRB employees, co-workers and customers have access to data and services managed by NRB.	Physical & Environmental Security policy is defined and implemented for physical accesses. Logical Access Control policy is defined and implemented for logical accesses. Customer Identity and Access Management policy is defined and implemented for Online Services provided to our Customers. Onboarding and Offboarding process is defined and implemented. Workforce Tool to support our IAM processes for external personel. Access Management Tool is used for automating most of our IAM processses.
A.5.19	Information security in supplier relationships	Yes	Yes	NRB uses subcontractors for its own needs or to provide services to its customers.	Suppliers' relationship policy is defined and implemented. Due diligence procedure for analyzing the risks before contracting with a new critical supplier. General terms and conditions of purchase to inform third parties on their obligations. Security requirements for external personnel to inform them on their responsibilities.
A.5.20	Addressing information security within supplier agreements	Yes	Yes	NRB uses subcontractors for its own needs or to provide services to its customers.	General terms and conditions of purchase to inform third parties on their obligations. Security requirements for external personnel to inform them on their responsibilities.
A.5.21	Managing information security in the information and communication technology (ICT) supply-chain	Yes	Yes	NRB uses subcontractors for its own needs or to provide services to its customers.	Suppliers' relationship policy is defined and implemented. Due diligence procedure for analyzing the risks before contracting with a new supplier. General terms and conditions of purchase to inform third parties on their obligations. Security requirements for external personnel to inform them on their responsibilities.
A.5.22	Monitoring, review and change management of supplier services	Yes	Yes	NRB uses subcontractors for its own needs or to provide services to its customers.	Suppliers' relationship policy including regular review and monitoring is defined and implemented.
A.5.23	Information security for use of cloud services	Yes	Yes	NRB uses Cloud Services for its own needs or to provide services to its customers.	Policy for the use of Cloud Services is defined. Suppliers' relationship policy is defined and implemented. Due diligence procedure for analyzing the risks before contracting with a new supplier.
A.5.24	Information security incident management planning and preparation	Yes	Yes	As NRB is responsible for the confidentiality, the integrity and the availability of its assets and those of its customers, security incidents may occur and must be handled accordingly.	Leaflet 'How to identify Security Incident' on intranet to give guidance to end-users. Security incident management process and procedure are defined. ITSM Tool to support our incident management process and procedure. CGIS Contact list on Intranet to identify Security expert in each domain.
A.5.25	Assessment and decision on information security events	Yes	Yes	As NRB is responsible for the confidentiality, the integrity and the availability of its assets and those of its customers, security incidents may occur and must be handled accordingly.	Security incident management process and procedure are defined. SIEM Tool operated by SecOps to support NRB incident assessement and decision on internal and mutualized services. ITSM Tool to support our incident management process and procedure.
A.5.26	Response to information security incidents	Yes	Yes	As NRB is responsible for the confidentiality, the integrity and the availability of its assets and those of its customers, security incidents may occur and must be handled accordingly.	Security incident management process and procedure are defined. Multiple Incident Response Playbooks are defined, applied and regularly tested & improved.
A.5.27	Learning from information security incidents	Yes	Yes	As NRB is responsible for the confidentiality, the integrity and the availability of its assets and those of its customers, security incidents may occur and must be handled accordingly.	Security incident management process and procedure are defined. Incident Report Template is used for reporting on each major or important security incident. Problem management process for determing the root cause of each major/important/recurring security incident.

A.5.28	Collection of evidence	Yes	Yes	As NRB is responsible for the confidentiality, the integrity and the availability of its assets and those of its customers, security incidents may occur and must be handled accordingly.	Logical Access Control policy is defined and implemented for restricting access to evidences. SIEM Tool is used for storing evidences. System isolation & forensic procedures are defined and applied in case of incident.
A.5.29	Information security during disruption	Yes	Yes	The NRB must be able to maintain its operations securely in the event of a disaster.	Business Continuity policy is defined. BIA are defined and reviewed regularly. BCP are defined and tested regularly ensuring that the security level is maintained, even in case of disaster. DR procedures are defined and tested regularly.
A.5.30	ICT readiness for business continuity	Yes	Yes	The NRB must be able to maintain its operations securely in the event of a disaster.	BIA are defined and reviewed regularly. BCP are defined and tested regularly. DR procedures are defined and tested regularly.
A.5.31	Legal, statutory, regulatory and contractual requirements	Yes	Yes	The information processed and the softwares/services used by NRB may be subject to laws, regulations and intellectual property rights.	Compliance policy is defined. Inventory of Laws & Regulations is defined and reviewed regularly. Cryptographic Controls policy is in-line with L&R. Bid phase of the E2E Risk assessment includes evaluation of applicable L&R. Privacy-by-Design & Security-by-Design processes are defined and applied to ensure compliance with applicable L&R. General terms and conditions of purchase to inform third parties on their obligations. Due diligence procedure for analyzing the risks before contracting with a new supplier includes the analysis of applicable L&R. Online Services Terms & Conditions of Use defines the R&R between NRB and the client for L&R compliance.
A.5.32	Intellectual property rights	Yes	Yes	The information processed and the softwares/services used by NRB may be subject to laws, regulations and intellectual property rights.	Licence Management process is defined. Licence inventory tool is implemented to support the process. General terms and conditions of purchase to inform suppliers on Intellectual property rights. Sales Terms and Conditions to inform customers on Intellectual property rights. Software Licensing Management SLM Services for managing licence on our Private Cloud platform. IT Charter to give rules & guidance on using ressources subject to Intellectual property rights.
A.5.33	Protection of records	Yes	Yes	The records generated/processed by NRB may be subject to laws, regulations and contractual requirements.	Compliance policy is defined. Inventory of Laws & Regulations is defined and reviewed regularly. The E2E Risk assessment includes evaluation of data type processed and if requirements are applicable. Privacy and Data Protection policy are defined and applied.
A.5.34	Privacy and protection of personal identifiable information (PII)	Yes	Yes	The information processed and the softwares/services used by NRB may be subject to laws & regulations.	Full time DPO is appointed. Information Classification policy includes rules and guidance for PII. Privacy and Data Protection policy are defined and applied. The E2E Risk assessment includes evaluation of data type processed and if requirements are applicable. Privacy-by-Design is applied when applicable.
A.5.35	Independent review of information security	Yes	Yes	External/independant evaluations serve as input for continuous improvement.	External ISO27001 audits are performed at least annually. Annual audits are performed in order to have ISAE 3402 reports.
A.5.36	Compliance with policies, rules and standards for information security	Yes	Yes	External/independant evaluations serve as input for continuous improvement.	3-year audit plan carried out by the 3rd line of defense. Annual pentest mission performed by appointed 3rd party.

A.5.37	Documented operating procedures	Yes	Yes	NRB manages assets used for the storage and processing of data from NRB and its customers.	The CMDB contains all standard operational data. The Intranet contains all standard procedures. Specific operational data & procedures are stored in Teams Shares & Sharepoint.
A6	**People controls**				
A.6.1	Screening	Yes	Yes	NRB selects personnel for positions with access to sensitive systems and data.	HR Process is defined and applied for talent acquisition. It includes specific checks for screening candidates. List of critical functions is maintained. Additional checks are performed for these functions.
A.6.2	Terms and conditions of employment	Yes	Yes	NRB employs staff for positions with access to sensitive systems and data.	T&C are specifed in multiple documents : - Work regulation - General terms and conditions of purchase - Security requirements for external personnel - IT Charter
A.6.3	Information security awareness, education and training	Yes	Yes	NRB employs staff for positions with access to sensitive systems and data.	Awareness is raised during the QRM onboarding meeting, and on a regular basis with awareness campaigns via our e-learning platform.
A.6.4	Disciplinary process	Yes	Yes	NRB employs staff for positions with access to sensitive systems and data.	Work regulations and General terms and conditions of purchase include clauses relating to staff failure to comply with security policies or rules.
A.6.5	Responsibilities after termination or change of employment	Yes	Yes	NRB employs staff for positions with access to sensitive systems and data.	HR procedudre for employee departure is defined and applied. It includes a contract termination letter sent by registered mail. Work regulations, General terms and conditions of purchase and Security requirements for external personnel include clauses on confidentiality after the end of the contract.
A.6.6	Confidentiality or non-disclosure agreements	Yes	Yes	NRB employs staff for positions with access to sensitive systems and data.	Confidentiality and non-disclosure clauses & requirements are defined in the following agreements and documents : - Work regulation - General terms and conditions of purchase - Security requirements for external personnel - IT Charter
A.6.7	Remote working	Yes	Yes	Teleworking is a common practice used by NRB employees and co-workers.	Remote working rules & requirements are defined in the IT Charter. Network Security policy is defined and applied for remote access. VPN is only allowed for NRB managed devices with MFA authentication.
A.6.8	Information security event reporting	Yes	Yes	NRB employs staff for positions with access to sensitive systems and data.	Personnel are informed at the QRM onboarding meeting and via the leaftlet 'How to identify and report Security Incident' available on the intranet. Security incident management procedure contains detailed information on how to report security incident with the support of our ITSM tool.
A7	**Physical controls**				
A.7.1	Physical security perimeters	Yes	Yes	NRB manages buildings where the data of NRB and its customers is stored and processed.	Physical & Environmental Security policy is defined and applied. Physical perimeter is defined and protected : fences, infra-red intruder detection & camera. Physical access control is enforced for all entries.
A.7.2	Physical entry	Yes	Yes	NRB manages buildings where the data of NRB and its customers is stored and processed.	Physical & Environmental Security policy is defined and applied. Physical access control is enforced for all entries and access to IT Rooms. Access Rules for datacenter IT Rooms are defined and applied. Only datacenter personnel have permanent access to IT Rooms. Work instructions are defined and implemented for access request to buildings and datacenters.
A.7.3	Securing offices, rooms and facilities	Yes	Yes	NRB manages buildings where the data of NRB and its customers is stored and processed.	Physical & Environmental Security policy is defined and applied. Physical perimeter is defined and protected : fences, infra-red intruder detection & camera. Physical access control is enforced for all entries and access to IT Rooms.

A.7.4	Physical security monitoring	Yes	Yes	NRB manages buildings where the data of NRB and its customers is stored and processed.	Physical & Environmental Security policy is defined and applied. Onsite 24/7 guards or Intruder detection and alarms with guards on-call.
A.7.5	Protecting against physical and environmental threats	Yes	Yes	NRB manages buildings where the data of NRB and its customers is stored and processed.	Physical & Environmental Security policy is defined and applied. The buildings housing the IT rooms are protected against intrusion, fire and environmental risks. Physical access control for all entries and access to IT Rooms.
A.7.6	Working in secure areas	Yes	Yes	NRB manages buildings where the data of NRB and its customers is stored and processed.	Physical & Environmental Security policy is defined and applied. Physical access policy is defined and applied. Access Rules for datacenter IT Rooms are defined and applied. Only datacenter personnel have permanent access to IT Rooms. Datacenter policy is defined and applied. It includes rules for working in DCs. A safety, health and environment sheet is posted in the buildings and DCs.
A.7.7	Clear desk and clear screen	Yes	Yes	NRB employs staff for positions with access to sensitive systems and data.	Clear desk & clean screen policy is defined and applied. Screen Auto-lock is enforced on systems. A specific e-learning module must be followed by all staff.
A.7.8	Equipment siting and protection	Yes	Yes	NRB manages buildings where the data of NRB and its customers is stored and processed.	Datacenter policy is defined and applied. It includes rules for installing equipment in DCs. DC Environmental monitoring is performed.
A.7.9	Security of assets off-premises	Yes	Yes	NRB employees use off-site equipment in the performance of their duties.	IT charter contains rules aimed at protecting personnel equipment. Laptop are encrypted and Mobile are managed using a MDM solution.
A.7.10	Storage media	Yes	Yes	Storage media are used to store NRB and customer data.	Access Rules for datacenter IT Rooms are defined and applied. Only datacenter personnel have permanent access to IT Rooms. Work instruction IMACD includes rules for the installation & removal of ICT equipment in DCs. Work instruction to ensure media erasure before disposal or re-use is defined. Information Classification policy & Post-it and IT Charter contain rules and guidance for the use of storage media. USB port are blocked on laptops.
A.7.11	Supporting utilities	Yes	Yes	NRB manages buildings where the data of NRB and its customers is stored and processed.	Physical & Environmental Security policy is defined and applied. All supporting utilities for DCs are redundant.
A.7.12	Cabling security	Yes	Yes	NRB manages buildings where the data of NRB and its customers is stored and processed.	Physical & Environmental Security policy is defined and applied. Datacenter policy is defined and applied. It includes rules for cabling in DCs.
A.7.13	Equipment maintenance	Yes	Yes	NRB manages buildings where the data of NRB and its customers is stored and processed.	Physical & Environmental Security policy is defined and applied. There is a maintenance contract for every DC supporting utilities. Asset Management process and tool for storing equipment information.
A.7.14	Secure disposal or re-use of equipment	Yes	Yes	Storage media are used to store NRB and customer data.	Work instruction IMACD includes rules for the installation & removal of ICT equipment in DCs. Work instruction to ensure media erasure before disposal or re-use is defined. ICT equipment disposal is performed by a specific team. Encrypted laptop & managed container on mobile.
A8	**Technological controls**				

A.8.1	User end point devices	Yes	Yes	Desktops, laptops and mobile devices are used by NRB employees and co-workers.	IT Charter to give rules & guidance on protecting user endpoint devices. Desktop/Laptop are secured and managed by NRB. As such, Desktop/Laptop : - are hardened; - have USB ports disabled for storage devices; - have up-to-date antivirus and EDR reporting alerts to a SIEM/SOC; - have a centrally managed local firewall; - benefit from the latest published and applicable security patches; - are scanned regularly to detect unwanted software; - are encrypted. Additionally, users are not local admin and the local admin account is deleted. MDM solution is deployed on smartphone connecting to NRB resources with the use of a secure container for professional applications.
A.8.2	Privileged access rights	Yes	Yes	NRB employs staff for positions with access to sensitive systems and data.	Logical Access Control policy is defined and applied (RBAC model for attributing privileged rights). Specific admin accounts is mandatory for admin tasks. Admins tasks are only possible from specific and secured VLANs. Governance & requirements are defined and applied for the management of privileged accounts. Specifc password policy is enforced for admin accounts. A secure Vault is used for the storage of Secret information.
A.8.3	Information access restriction	Yes	Yes	NRB employs staff for positions with access to sensitive systems and data.	Network security policy & Logical Access Control policy are defined and applied (RBAC model for attributing rights). Admins tasks are only possible from specific and secured VLANs. Our Access Management tool (IAM support tool) is used to automate the assignment of rights according to user roles (RBAC model). Network & User Access Control is enforced to allow only registered devices and users on internal ressources & VLANs (Conditional Access, 802.1X, ...)
A.8.4	Access to source code	Yes	Yes	NRB's activities and services include software development.	Infrastructure Standard for Software Development is defined and applied to secure access to our code repositories.
A.8.5	Secure authentication	Yes	Yes	NRB employs staff for positions with access to sensitive systems and data.	Network security policy & Logical Access Control policy are defined and applied to ensure proper authentication of devices and users. MFA is enforced for all access from untrusted network.
A.8.6	Capacity management	Yes	Yes	NRB manages assets used for the storage and processing of data from NRB and its customers.	Single point of knowledge in teams are identified in BIA. Capacity reports are produced on Mainframe and on NRB private Cloud, in order to forecast future requirements.
A.8.7	Protection against malware	Yes	Yes	NRB manages assets used for the storage and processing of data from NRB and its customers.	Antimalware policy is defined and applied. Antimalware and EDR are installed on servers & workstations, reporting alerts to a SIEM/SOC. Antimalware and EDR are installed on Mail/Web Gateways.
A.8.8	Management of technical vulnerabilities	Yes	Yes	NRB manages assets used for the storage and processing of data from NRB and its customers.	Technical Vulnerability Management policy is defined and applied. Vulnerability Management process is defined and implemented. Threat Management process is defined and implemented. Automated regular vulnerability scanning is performed. Regular (at least once a year) pentests are performed.
A.8.9	Configuration management	Yes	Yes	NRB manages assets used for the storage and processing of data from NRB and its customers.	Technical Vulnerability Management policy is defined and applied. System hardening is performed by default. Regular compliance scanning is performed. Regular (at least once a year) pentests are performed.

A.8.10	Information deletion	Yes	Yes	NRB manages assets used for the storage and processing of data from NRB and its customers.	Work instruction to ensure media erasure before disposal or re-use is defined. Laptop are encrypted and Mobile are managed using a MDM solution with erasable container.
A.8.11	Data masking	Yes	Yes	NRB manages assets used for the storage and processing of data from NRB and its customers.	Data masking is performed using the 'Normal Change' workflow (defined in our Change Management process). The workflow includes build, test and risk analysis phases.
A.8.12	Data leakage prevention	Yes	Yes	NRB manages assets used for the storage and processing of data from NRB and its customers.	Information Classification policy & Post-it to give instructions to end-users. IT Charter & Employee awareness to give rules & guidance. Instructions on the Intranet for end-users on how to label information and protect e-mail using available tools (Microsoft Purview). Specific SIEM usecases to detect data exfiltration.
A.8.13	Information backup	Yes	Yes	NRB manages assets used for the storage and processing of data from NRB and its customers.	Backup policy is defined and applied. At least two back-up copies, with a third immutable copy on request. Regular restore testing for different platform are performed.
A.8.14	Redundancy of information processing facilities	Yes	Yes	The NRB must be able to maintain its operations securely in the event of a disaster.	NRB infra is deployed on at least 2 georesilient datacenters. Business Continuity policy is defined and applied. BIA are regularly updated. BCP are regularly tested and updated if needed. Disaster Recovery strategy is defined and implemented - Technical Recovery Plans are regularly updated and tested.
A.8.15	Logging	Yes	Yes	NRB employees, co-workers and customers have access to data and services managed by NRB.	Logical Access Control policy is defined and applied for the protection of log data. Logs are stored and correlated in our SIEM. Security events and alerts are analyzed and escalated as required by our SecOps team.
A.8.16	Monitoring activities	Yes	Yes	NRB employees, co-workers and customers have access to data and services managed by NRB.	Logs are stored and correlated in our SIEM. Security events and alerts are analyzed and escalated as required by our SecOps team. Security incident are handled following our Security Incident Management process.
A.8.17	Clock synchronization	Yes	Yes	Logs produced must be exploitable.	A robust NTP infrastructure (based on Internet and GPS source) is implemented.
A.8.18	Use of privileged utility programs	Yes	Yes	NRB employs staff for positions with access to sensitive systems and data.	Use of privileged utility program are detected by the EDR on servers forwarding events to our SIEM/SOC. Security events and alerts are analyzed and escalated as required by our SecOps team.
A.8.19	Installation of software on operational systems	Yes	Yes	NRB manages assets used for the storage and processing of data from NRB and its customers.	Installation of software on systems is performed using the 'Normal Change' workflow (defined in our Change Management process). The workflow includes build, test and risk analysis phases. SW installation on systems is only authorized to admins (RBAC). NRB Software Center is used to deploy standard software on WKS. No admin rights are allowed on end-user workstations, installation of non-standard software on WKS is only allowed using a special tool to elevate privilege and monitor activities. Activities are reviewed regularly to identify deviation.
A.8.20	Networks security	Yes	Yes	NRB manages assets used for the storage and processing of data from NRB and its customers.	Network Security Policy is defined and applied. Network Architecture diagrams are updated regularly. Network informations are stored in specific tools and the CMDB.
A.8.21	Security of network services	Yes	Yes	NRB manages assets used for the storage and processing of data from NRB and its customers.	Network Security Policy is defined and applied. Secure Network Services are implemented and monitored (VPN/DNS/DDoS protection).

A.8.22	Segregation of networks	Yes	Yes	NRB manages assets used for the storage and processing of data from NRB and its customers.	Network Security Policy is defined and applied. Network Architecture diagrams are updated regularly. Network informations are stored in specific tools and the CMDB. Unified firewall management tool is used to store information, implement rules and verify compliance.
A.8.23	Web filtering	Yes	Yes	NRB assets have connections to untrusted ressources.	Web Proxy gateway is implemented for internet access. Local workstation URL filtering is implemented for internet access.
A.8.24	Use of cryptography	Yes	Yes	NRB manages assets used for the storage and processing of data from NRB and its customers.	Cryptographic Controls policy is defined and applied. Certificate Management policy is defined and applied. Certificate Management procedure is defined and implemented. CMDB and Secure Vault for storing certificate information.
A.8.25	Secure development life cycle	Yes	Yes	NRB's activities and services include systems & software development.	Secure Systems Development Life Cycle policy is defined and applied.
A.8.26	Application security requirements	Yes	Yes	NRB's activities and services include systems & software development.	Project Management process is defined and implemented. It includes Stage Gates and Security-by-Design to ensure that requirements are identified, implemented and tested.
A.8.27	Secure system architecture and engineering principles	Yes	Yes	NRB's activities and services include systems & software development.	Project Management process is defined and implemented. It includes Stage Gate, high- and low-level designs and Security-by-Design.
A.8.28	Secure coding	Yes	Yes	NRB's activities and services include systems & software development.	Secure Systems Development Life Cycle policy is defined and applied. Security testing is implemented either using tools and manual tests.
A.8.29	Security testing in development and acceptance	Yes	Yes	NRB's activities and services include systems & software development.	Project Management process is defined and implemented. It includes Stage Gates and Security-by-Design. Security testing is implemented either using tools and manual tests.
A.8.30	Outsourced development	Yes	Yes	NRB's activities and services include systems & software development.	General terms and conditions of purchase contains specific clauses on outsourced development. Project Management process is defined and implemented. It includes Stage Gates and Security-by-Design.
A.8.31	Separation of development, test and production environments	Yes	Yes	NRB manages assets used for the storage and processing of data from NRB and its customers.	Infrastructure Standard for Software Development is defined and applied. Project Management process is defined and implemented. It includes Stage Gates and Security-by-Design. Network Security Policy is defined and applied. Network Architecture diagrams are updated regularly.
A.8.32	Change management	Yes	Yes	NRB manages assets used for the storage and processing of data from NRB and its customers.	Change Management process is defined and implemented. The workflow for 'Normal Change' includes build, test and risk analysis phases. ITSM tool to support our Change Management process.
A.8.33	Test information	Yes	Yes	NRB's activities and services include systems & software development.	Duplication of data between environment is performed using the 'Normal Change' workflow (defined in our Change Management process). The workflow includes formal approval and risk analysis phases. Project Management process which includes Stage Gates and Security-by-Design which includes analysis on the use of test data.
A.8.34	Protection of information systems during audit testing	Yes	Yes	NRB manages assets used for the storage and processing of data from NRB and its customers.	Technical audit autorisation form must be filled by each involved parties prior each audit.