Standard technical and organizational security measures applicable to the ISMS of NRB

Overall security and access control organization

Key Control	Overview of technical and organizational measures
(general reference to ISO27K controls domain 5.1.x Information Security Policies) : maturity & ongoing maintenance thereof through ISMS	• Information Security policy is in place and monitored, security objectives are defined in view of the business strategy and information security risk assessment • Privacy and Data Protection policy is in place and monitored
(general reference to ISO27K controls domain 6.1.x Organization of Information Security) : organization and roles & responsibilities	• Security Officer is in place • A network of Information Security Coordinators and 'Relais' is in place, responsibilities are defined • Data Protection Officer is in place • (for project management) Information security objectives are included in project objectives
(general reference to ISO27K controls domain 8.x) Asset Management / Inventory	• Data Classification policy is in place and monitored • An inventory of IT/information assets is in place, asset ownership is defined • IT/information assets are classified in view of their criticality (criteria in Data Classification policy)
(general reference to ISO27K controls domain 18.1.x) Compliance / Compliance monitoring)	• Compliance policy is in place and monitored • (+ implied in continuous improvement ISMS, monitoring of other Information Security policies)
(ISO27K 9.1.x) Access control policy, Access to networks and network services	• Access control policy is in place and monitored, and covers both logical and physical access to information assets • Access to information assets is based on need-to-know / need-to-use principles • Access to NRB network / network services is subject to technical and management controls, to ensure only authorized users can gain access (cf. also further : user management, authentication mechanisms, …) • Use of network services is monitored.
(ISO27K 9.2.x, 9.3.x) User Access Management, Use of secret authentication information	• User registration and de-registration: process to assign, enable and revoke user IDs is defined. The use of shared user IDs is only permitted in exceptional circumstances, when necessary for business or operational reasons • User Access provisioning: access rights are formally assigned to defined users on a need-to-know / need-to-use basis. Access is changed / revoked if users change functions or leave the company. • Privileged access rights are restricted to appropriate personnel (e.g. administrators). Use of privileged access is subject to specific procedures, and activity is logged and monitored • A formal process is in place to allocate secret authentication information to users (mandatory change upon first use, minimum password requirements …).

Key Control	Overview of technical and organizational measures
	Identity verification is in place in case a user's authentication information needs to be renewed / replaced • Users receive instructions on the use of their authentication information (obligation to maintain secrecy/confidentiality thereof, avoiding records, prohibition to share, …) • User access rights are reviewed at regular intervals, and also upon role changes. Access rights are removed or adjusted as required
(ISO27K 9.4.x) System and Application access control	• Access to systems and applications is restricted, in line with the principles defined in the access control policy • Where required, access to systems and applications is subject to secure log-on procedures (authentication process, protection of passwords during log-on procedure, logging & monitoring of failed attempts, termination of idle sessions) • The password management system enforces high-quality passwords (minimum length, type of characters, change of password upon first logon, change of password at regular intervals, restrict re-use of old passwords …) • For privileged users and utility programs, additional security requirements are established, and all activity is logged and monitored (i.e., not only logon process activity) • Application source code and related assets is tightly restricted, and any access to source code libraries is logged and monitored
(ISO27K 10.x) Cryptography	• Our cryptography policy determines the use cases as well as the accepted algorithms and minimum key lengths. These recommendations are in line with the latest recommendations of the security community • Our key and certificate management procedure is based on a workflow with clear R&R for creation, modification and revocation. Certificate data is stored in a secure vault • The data at-rest on our storage bays and the data in transit on networks not managed by NRB are encrypted
(ISO27K 13.x) Communication Security	• The network management policy clearly defines the principles to be applied in the design and management of networks. • The network is divided into domains separated by checkpoints in order to adequately filter north-south traffic and avoid east-west traffic; • Necessary controls (system duplication, SSL, VPN, ...) are applied to preserve the confidentiality, integrity and availability of the network and data

Key Control	Overview of technical and organizational measures
	• Access to the network is subject to technical rules and controls such as 802.1x • The management network is dedicated and is subject to specific requirements and access rules.

Secure Operations

Key Control	Overview of technical and organizational measures
(general reference to ISO27K controls domain 11.1.x Secure Areas) : physical security perimeter, access controls, ...	• Overall building security includes physical barriers, a badge-based access control, video surveillance, … • Access to identified 'secure areas' (e.g. data centre) is further restricted to authorized personnel only. Any visitors (e.g. technical staff from suppliers) are identified up-front (white list principle), and receive temporary access only
(general reference to ISO27K controls domain 11.2.x Equipment handling) : equipment protection, maintenance, removal/disposal practices, ...	• Equipment is held in areas that are protected against environmental threats (fire, water, theft, …) • Procedures for the secure removal and disposal of information assets are established and monitored
(ISO27K 12.1.x) Operational procedures and responsibilities	• Operating procedures are documented and available to all users who need them. The procedures cover system installation / configurations, backup and recovery management, scheduling (if applicable), error handling, overall monitoring • Formal change management is set up to handle changes to infrastructure / procedures / organization in a standardized manner (documentation, authorization, testing & final approval, implementation) • Emergency changes are subject to explicit review and approval • Capacity management/Performance monitoring is defined and operational (projections for future capacity requirements, deletion of obsolete data, multiple performance optimization measures) • Development, Test and Operational environments are separated. Procedures for transferring software between these environments are established and monitored. • Preventive and detective measures against malware are operational.
(ISO27K 12.3.x) Backup, archiving and destruction principles are defined and implemented, and tested on a regular basis	• Physical backup procedures are defined, monitored and tested regularly • Logical backup and restore procedures are defined, monitored and tested regularly • Archiving procedures are defined and monitored • Backup information is subject to physical and environmental protection

Key Control	Overview of technical and organizational measures
	• Destruction of backups and archives is conducted as per defined procedures
(ISO27K 12.4.x) Event logging	• Event logging is established - both overall & specifically for administrator activity (overall logs capture events, administrator logs full detail of activity)
(ISO27K 12.5.1) (System) Software installation is subject to standardized and secure practices	• Only administrators have the authorization and access profiles to conduct system software installation or upgrades • Installations are subject to formal procedures, that enforce adequate testing prior to actual installation • A rollback strategy is defined for any system software upgrade
(ISO27K 12.6.1) Technical vulnerability management	• Preventive and detective measures against technical vulnerabilities are operational (starting from an inventory of IT assets and risk-based classification thereof) • A patching schedule is defined and adhered to • If new vulnerabilities are identified, a risk assessment takes place and actions defined • Restrictions on software installation by users are in place
(ISO27K 16.1.x) Incident Management	• Incident Management policy and procedures are established and monitored, roles & responsibilities are defined • The incident handling process includes principles and guidance on escalation and reporting, the assessment & response mechanism, lessons-learned practices, documentation requirements • Specifically for (potential) security and privacy-related incidents, additional escalation and analysis requirements are established

Secure Development

Key Control	Overview of technical and organizational measures
(ISO27K 14.1.1) Security requirements analysis and specifications	• Information security requirements are defined for any new information system / application being considered for implementation / development (including e.g. authentication and access principles depending on the criticality of the information, logging requirements, training of to-be users, …) • Additional security requirements are defined and implemented for any new system / application that makes use of public infrastructure / networks (including e.g. extra authentication steps, encryption, confirmation processes for data integrity, …) • Additional security requirements are defined and implemented for any new system / application that involves operational transactions (including e.g.

Key Control	Overview of technical and organizational measures
	electronic signatures, authentication, privacy considerations, encryption of communication, …)
(ISO27K 14.2.x) Secure development	• A secure development policy is established and monitored • Secure Development training is provided to all developers, covering secure design, coding and testing principles and practices. • Development, Test and Operational environments are separated. Procedures for transferring software between these environments are established and monitored. • Formal change control procedures are applied for any changes to systems / applications : authority levels are defined & adhered to, version control is applied • Testing and test acceptance procedures are defined and adhered to – at different stages of development, and ultimately in formal user acceptance testing (including explicit testing of security and other 'non-functional' requirements), • Specifically when underlying operating platforms are changed, also all critical applications using these platforms are reviewed and tested • Specifically when NRB uses other suppliers to assist in development activities (partial or full outsourcing), secure development practices (design, coding, testing) are enforced contractually.
(ISO27K 14.3.1) Protection of test data	• Development, Test and Operational environments are separated. Procedures for transferring software between these environments are established and monitored. • Test data is selected based on testing needs – only under exceptional circumstances will operational data be used in test (or development) environments (such operational data is deleted once testing is completed) • Test environments are subject to standard access control procedures