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 processes.
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 processes.
A.5.19	Information security in supplier relationships	Yes	Yes	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	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	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	
A.5.24	Information security incident management planning and preparation	Yes	Yes	integrity and the availability of its assets and	Leaflet 'How to identify Security Incident' on intranet to give guidance to endusers. 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	integrity and the availability of its assets and those of its customers, security incidents may	Logical Access Control policy is defined and implemented for restricting access to evidences. SIEM Tool is used for storing evidences.
				occur and must be handled accordingly.	System isolation & forensic procedures are defined and applied in case of incident.
				The NRB must be able to maintain its operations	Business Continuity policy is defined.
				securely in the event of a disaster.	BIA are defined and reviewed regularly.
A.5.29	Information security during disruption	Yes	Yes		BCP are defined and tested regularly ensuring that the security level is
					maintained, even in case of disaster.
				The NRB must be able to maintain its operations	DR procedures are defined and tested regularly.
A.5.30	ICT readiness for business continuity	Yes	Yes	securely in the event of a disaster.	BCP are defined and tested regularly.
A.5.50	Ter reduitess for business continuity	165	163	securely in the event of a disaster.	DR procedures are defined and tested regularly.
				The information processed and the	Compliance policy is defined.
				softwares/services used by NRB may be subject	Inventory of Laws & Regulations is defined and reviewed regularly.
				to laws, regulations and intellectual property	Cryptographic Controls policy is in-line with L&R.
				rights.	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.
A.5.31	Legal, statutory, regulatory and contractual requirements	Yes	Yes		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.
					and chefic for East compliance.
				The information processed and the	Licence Management process is defined.
				softwares/services used by NRB may be subject	Licence inventory tool is implemented to support the process.
				to laws, regulations and intellectual property	General terms and conditions of purchase to inform suppliers on Intellectual
				rights.	property rights.
A.5.32	Intellectual property rights	Yes	Yes		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.
				The records generated/processed by NRB may	Compliance policy is defined.
				be subject to laws, regulations and contractual	Inventory of Laws & Regulations is defined and reviewed regularly.
A.5.33	Protection of records	Yes	Yes	requirements.	The E2E Risk assessment includes evaluation of data type processed and if
					requirements are applicable.
					Privacy and Data Protection policy are defined and applied.
				The information processed and the	Full time DPO is appointed.
				softwares/services used by NRB may be subject	Information Classification policy includes rules and guidance for PII.
A.5.34	Privacy and protection of personal identifiable information (PII)	Yes	Yes	to laws & regulations.	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.
4 5 35	Indones de la contenta de la formación de la f	Vc -	V	External/independant evaluations serve as input	External ISO27001 audits are performed at least annually.
A.5.35	Independent review of information security	Yes	Yes	for continuous improvement.	Annual audits are performed in order to have ISAE 3402 reports.
	Compliance with policies, rules and standards for information security	Yes	Yes	External/independant evaluations serve as input	3-year audit plan carried out by the 3rd line of defense.
A.5.36					

				100	TI CLIDD III III III III III
				NRB manages assets used for the storage and	The CMDB contains all standard operational data.
A.5.37	Documented operating procedures	Yes	Yes	processing of data from NRB and its customers.	· ·
					Specific operational data & procedures are stored in Teams Shares & Sharepoint.
Α6	People controls				jsnarepoint.
7.0				NRB selects personnel for positions with access	HR Process is defined and applied for talent acquisition. It includes specific
				to sensitive systems and data.	checks for screening candidates.
A.6.1	Screening	Yes	Yes		List of critical functions is maintained. Additional checks are performed for
					these functions.
				NRB employs staff for positions with access to	T&C are specifed in multiple documents :
				sensitive systems and data.	- Work regulation
A.6.2	Terms and conditions of employment	Yes	Yes		- General terms and conditions of purchase
	. ,				- Security requirements for external personnel
					- IT Charter
				NRB employs staff for positions with access to	Awareness is raised during the QRM onboarding meeting, and on a regular
A.6.3	Information security awareness, education and training	Yes	Yes	sensitive systems and data.	basis with awareness campaigns via our e-learning platform.
				NRB employs staff for positions with access to	Work regulations and General terms and conditions of purchase include
A.6.4	Disciplinary process	Yes	Yes	sensitive systems and data.	clauses relating to staff failure to comply with security policies or rules.
				NRB employs staff for positions with access to	HR procedudre for employee departure is defined and applied. It includes a
				sensitive systems and data.	contract termination letter sent by registered mail.
A.6.5	Responsibilities after termination or change of employment	Yes	Yes	,	Work regulations, General terms and conditions of purchase and Security
					requirements for external personnel include clauses on confidentiality after
					the end of the contract.
				NRB employs staff for positions with access to	Confidentiality and non-disclosure clauses & requirements are defined in the
				sensitive systems and data.	following agreements and documents :
		.,		,	- Work regulation
A.6.6	Confidentiality or non-disclosure agreements	Yes	Yes		- General terms and conditions of purchase
					- Security requirements for external personnel
					- IT Charter
				Teleworking is a common practice used by NRB	Remote working rules & requirements are defined in the IT Charter.
A.6.7	Remote working	Yes	Yes	employees and co-workers.	Network Security policy is defined and applied for remote access.
					VPN is only allowed for NRB managed devices with MFA authentication.
				NRB employs staff for positions with access to	Personnel are informed at the QRM onboarding meeting and via the leaftlet
	_			sensitive systems and data.	'How to identify and report Security Incident' available on the intranet.
A.6.8	Information security event reporting	Yes	Yes		Security incident management procedure contains detailed information on
					how to report security incident with the support of our ITSM tool.
Α7	Physical controls				
	,			NRB manages buildings where the data of NRB	Physical & Environmental Security policy is defined and applied.
I				and its customers is stored and processed.	Physical perimeter is defined and protected : fences, infra-red intruder
A.7.1	Physical security perimeters	Yes	Yes	and processed.	detection & camera.
					Physical access control is enforced for all entries.
				NRB manages buildings where the data of NRB	Physical & Environmental Security policy is defined and applied.
				and its customers is stored and processed.	Physical access control is enforced for all entries and access to IT Rooms.
					Access Rules for datacenter IT Rooms are defined and applied. Only
A.7.2	Physical entry	Yes	Yes		datacenter personnel have permanent access to IT Rooms.
					Work instructions are defined and implemented for access request to
					buildings and datacenters.
				NRB manages buildings where the data of NRB	Physical & Environmental Security policy is defined and applied.
l				and its customers is stored and processed.	Physical perimeter is defined and protected : fences, infra-red intruder
A.7.3	Securing offices, rooms and facilities	Yes	Yes	and its customers is stored and processed.	detection & camera.
,, .5	Seeding offices, rooms did facilities				Physical access control is enforced for all entries and access to IT Rooms.
1					i nysical access control is emorced for all chilles and access to 11 NOUIIIS.

A 2.72 Clear desk and clear screen Yes Yes NRB employs staff for positions with access to sensitive systems and data. A.7.8 Equipment siting and protection Yes Yes NRB manages buildings where the data of NRB equipment in the performance of their duties. A.7.9 Security of assets off-premises Yes Yes NRB manages buildings where the data of NRB equipment in the performance of their duties. A.7.10 Storage media Yes Yes NRB manages buildings where the data of NRB equipment in the performance of their duties. A.7.11 Supporting utilities Yes Yes NRB manages buildings where the data of NRB and its customers is stored and processed. A.7.12 Cabling security Yes Yes NRB manages buildings where the data of NRB and its customers data. NRB manages buildings where the data of NRB and its customers is stored and processed. A.7.12 Cabling security Yes Yes NRB manages buildings where the data of NRB and its customers is stored and processed. A.7.12 Cabling security Yes Yes NRB manages buildings where the data of NRB and its customers is stored and processed. A.7.13 Equipment maintenance Yes Yes Yes NRB manages buildings where the data of NRB and its customers is stored and processed. A.7.14 Secure disposal or re-use of equipment Yes Yes Yes NRB manages buildings where the data of NRB and its customers is stored and processed. A.7.15 A.7.16 Supporting utilities Yes Yes A.7.17 Yes Yes NRB manages buildings where the data of NRB and its customers is stored and processed. A.7.18 Secure disposal or re-use of equipment Yes Yes Yes NRB manages buildings where the data of NRB and its customers is stored and processed. A.7.19 NRB manages buildings where the data of NRB and its customers is stored and processed. A.7.10 Yes A.7.11 Yes A.7.12 Sequence of equipment Yes Yes Yes A.7.12 Sequence of equipment Yes Yes Yes A.7.13 NRB manages buildings where the data of NRB and its customers is stored and processed. A.7.16 Yes A.7.17 Yes A.7.18 Sequence of equipment Yes Yes Yes A.7.18 Yes A.7.19 Yes A.7.19 Yes A.7.19 Yes A.7.10 Yes A	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.
NRB manages buildings where the data of NRB and its customers is stored and processed. A.7.6 Working in secure areas Yes Yes NRB manages buildings where the data of NRB and access Rules for datacenter If Rooms are defined and applied. Physical & Environmental Security policy is defined and applied. Only datacenter perior, of the defendent and applied. It includes rules for or working in DCs. A.7.7 Clear desk and clear screen Yes Yes NRB employs staff for positions with access to sensitive systems and data. A.7.8 Equipment siting and protection Yes Yes NRB manages buildings where the data of NRB and sustomers is stored and processed. A.7.9 Security of assets off-premises Yes Yes Yes Yes NRB manages buildings where the data of NRB and sustomers is stored and processed. A.7.10 Storage media Yes Yes Yes Yes NRB manages buildings where the data of NRB and sustomers is stored and processed. A.7.11 Supporting utilities Yes Yes Yes NRB manages buildings where the data of NRB and customer data. Yes Yes NRB manages buildings where the data of NRB and customer data. Yes Yes Yes NRB manages buildings where the data of NRB and customer data. Yes Yes Yes NRB manages buildings where the data of NRB and customer data. Yes Yes NRB manages buildings where the data of NRB and customer data. Yes Yes NRB manages buildings where the data of NRB and customer data. NRB manages buildings where the data of NRB and customer data. NRB manages buildings where the data of NRB and customer data. NRB manages buildings where the data of NRB and customer data. NRB manages buildings where the data of NRB and customer data. NRB manages buildings where the data of NRB and customer data of NRB and customer data. NRB manages buildings where the data of NRB and customer data of NRB and customer data. NRB manages buildings where the data of NRB and customer data of NRB and customer data of NRB and customer data. NRB manages buildings where the data of NRB and customer data of NRB and customer data.	A.7.5	Protecting against physical and environmental threats	Yes	Yes		The buildings housing the IT rooms are protected against intrusion, fire and environmental risks.
A.7.8 Clear desk and clear screen Yes Yes sensitive systems and data. A.7.8 Equipment siting and protection Ves Yes and soutcomers is stored and processed. A.7.9 Security of assets off-premises Yes Yes Pes PRB employees use off-site equipment in the performance of their duties. A.7.10 Storage media A.7.11 Supporting utilities Yes Yes Yes NRB manages buildings where the data of NRB customers is stored and processed. A.7.12 Cabling security Yes Yes Yes NRB manages buildings where the data of NRB customers is stored and processed. A.7.13 Secure disposal or re-use of equipment Yes Yes Yes NRB manages buildings where the data of NRB customers is stored and processed. A.7.14 Secure disposal or re-use of equipment Yes Yes Yes NRB manages buildings where the data of NRB and its customers is stored and processed. A.7.15 Secure disposal or re-use of equipment Yes Yes NRB manages buildings where the data of NRB and its customers is stored and processed. A.7.16 Secure disposal or re-use of equipment Yes Yes Yes NRB manages buildings where the data of NRB and its customers is stored and processed. A.7.18 Secure disposal or re-use of equipment Yes Yes Yes NRB manages buildings where the data of NRB Physical & Environmental Security policy is defined and applied. A.7.18 Secure disposal or re-use of equipment Yes Yes NRB manages buildings where the data of NRB Physical & Environmental Security policy is defined and applied. A.7.19 Secure disposal or re-use of equipment Yes Yes Yes NRB manages buildings where the data of NRB Physical & Environmental Security policy is defined and applied. A.7.19 Secure disposal or re-use of equipment Yes Yes Yes Yes NRB manages buildings where the data of NRB Physical & Environmental Security policy is defined and applied. A.7.10 Secure disposal or re-use of equipment information. A.7.11 Secure disposal or re-use of equipment information. A.7.12 Yes A.7.13 Secure disposal or re-use of equipment information. A.7.14 Secure disposal or re-use of equipment Yes Yes Yes Yes Yes Yes	A.7.6	Working in secure areas	Yes	Yes	_	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.7.8 Equipment siting and protection Yes Yes NRB manages buildings where the data of NRB 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. Storage media are used to store NRB and customer data. Storage media are used to store NRB and customer data. A.7.10 Storage media Yes Yes Yes NRB manages buildings where the data of NRB official and applied. It includes rules for installing dequipment. A.7.11 Supporting utilities A.7.12 Cabling security Yes Yes NRB manages buildings where the data of NRB and its customers is stored and processed. A.7.13 Equipment maintenance Yes Yes Yes NRB manages buildings where the data of NRB and its customers is stored and processed. A.7.14 Secure disposal or re-use of equipment Yes Yes Yes Storage media are used to store NRB and customer data. NRB manages buildings where the data of NRB and its customers is stored and processed. NRB manages buildings where the data of NRB and its customers is stored and processed. A.7.12 Cabling security Yes Yes NRB manages buildings where the data of NRB and its customers is stored and processed. A.7.13 Equipment maintenance Yes Yes NRB manages buildings where the data of NRB and its customers is stored and processed. A.7.14 Secure disposal or re-use of equipment Yes Yes Yes Storage media are used to store NRB and customer before disposal or re-use is defined. NRB manages buildings where the data of NRB and its customers is stored and processed. A.7.14 Secure disposal or re-use of equipment in DCs. Yes Yes Yes Yes NRB manages buildings where the data of NRB and its customers is stored and processed. A.7.15 A.7.16 Secure disposal or re-use of equipment in DCs. Yes Yes NRB manages buildings where the data of NRB and its customers is stored and processed. A.7.17 A.7.18 Secure disposal or re-use of equipment in DCs. Yes NRB manages buildings where the data of NRB and its customers is stored and processed. A.7.1	A.7.7	Clear desk and clear screen	Yes	Yes		Screen Auto-lock is enforced on systems.
A.7.10 Security of assets off-premises Yes Yes performance of their duties. A.7.10 Storage media are used to store NRB and customer data. A.7.11 Supporting utilities Yes Yes and its customers is stored and processed. A.7.12 Cabling security Yes Yes and its customers is stored and processed. A.7.13 Equipment maintenance Yes Yes Yes and its customers is stored and processed. A.7.14 Secure disposal or re-use of equipment Yes Yes Yes Yes and its customers is stored and processed. A.7.15 Storage media are used to store NRB and customer data. Laptop are encrypted and Mobile are managed using a MDM solution. A.7.12 A.7.13 A.7.14 Secure disposal or re-use of equipment in DCs. A.7.15 Yes Yes Yes Yes A.7.15 Yes Yes A.7.15 Yes Yes A.7.16 Yes Yes A.7.16 Yes A.7.16 Yes Yes Yes A.7.17 Yes Yes Yes A.7.17 Yes Yes Yes A.7.18 Yes Yes Yes A.7.18 Yes Yes Yes Yes A.7.19 Yes Yes Yes A.7.19 Yes	A.7.8	Equipment siting and protection	Yes	Yes		Datacenter policy is defined and applied. It includes rules for installing equipment in DCs.
A.7.10 Storage media A.7.10 Storage media A.7.10 A.7.10 Storage media A.7.11 A.7.11 A.7.12 A.7.12 Cabling security Yes Yes Yes A.7.13 A.7.13 A.7.13 A.7.14 Secure disposal or re-use of equipment Yes Yes Yes A.7.14 A.7.14 Secure disposal or re-use of equipment Yes Yes Yes A.7.15 A.7.16 A.7.16 A.7.16 A.7.17 A.7.17 A.7.18 A.7.18 A.7.18 A.7.19 A.7.19 A.7.19 A.7.10 A.7.10 A.7.10 A.7.10 A.7.11 A.7.11 A.7.11 A.7.12 A.7.12 A.7.13 A.7.13 A.7.13 A.7.13 A.7.14 A.7.14 A.7.14 A.7.14 A.7.15 A.7.15 A.7.16 A.7.16 A.7.16 A.7.17 A.7.17 A.7.18 A.7.18 A.7.18 A.7.19 A.7.19 A.7.19 A.7.10 A.7.10 A.7.10 A.7.10 A.7.10 A.7.11 A.7.11 A.7.12 A.7.12 A.7.12 A.7.13 A.7.13 A.7.13 A.7.13 A.7.14 A.7.14 A.7.14 A.7.14 A.7.15 A.7.15 A.7.16 A.7.16 A.7.16 A.7.17 A.7.18 A.7.18 A.7.18 A.7.18 A.7.19 A.7.19 A.7.19 A.7.19 A.7.10 A.7.10 A.7.10 A.7.10 A.7.10 A.7.10 A.7.11 A.7.11 A.7.12 A.7.12 A.7.12 A.7.13 A.7.13 A.7.13 A.7.14 A.7.14 A.7.14 A.7.14 A.7.15 A.7.16 A.7.16 A.7.16 A.7.17 A.7.18 A.7.18 A.7.18 A.7.18 A.7.18 A.7.18 A.7.18 A.7.18 A.7.19 A.7.18 A.7.19 A.7.10 A.7.10 A.7.10 A.7.10 A.7.10 A.7.11 A.7.11 A.7.12 A.7.12 A.7.12 A.7.13 A.7.13 A.7.14 A.7.14 A.7.14 A.7.14 A.7.15 A.7.16 A.7.16 A.7.16 A.7.16 A.7.16 A.7.17 A.7.18 A.7.19 A.7.18 A.7.19 A.7.10 A.7.	A.7.9	Security of assets off-premises	Yes	Yes	, ,	
A.7.11 Supporting utilities Yes Yes NRB manages buildings where the data of NRB and its customers is stored and processed. A.7.12 Cabling security Yes Yes Yes NRB manages buildings where the data of NRB and its customers is stored and processed. A.7.13 Equipment maintenance Yes Yes Yes NRB manages buildings where the data of NRB and its customers is stored and processed. Storage media are used to store NRB and customer data. Yes Yes Yes Yes Yes Yes Work instruction to ensure media erasure before disposal or re-use is defined.	A.7.10	Storage media	Yes	Yes		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.
A.7.12 Cabling security Yes Yes and its customers is stored and processed. A.7.13 Equipment maintenance Yes Yes Yes Asset Management process and tool for storing equipment information. Storage media are used to store NRB and customer data. Secure disposal or re-use of equipment Yes	A.7.11	Supporting utilities	Yes	Yes		Physical & Environmental Security policy is defined and applied.
A.7.13 Equipment maintenance Yes Yes and its customers is stored and processed. There is a maintenance contract for every DC supporting utilities. Asset Management process and tool for storing equipment information. 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.	A.7.12	Cabling security	Yes	Yes		, , , , , , , , , , , , , , , , , , , ,
Storage media are used to store NRB and customer data. 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.	A.7.13	Equipment maintenance	Yes	Yes		There is a maintenance contract for every DC supporting utilities.
Encrypted laptop & managed container on mobile.	A.7.14	Secure disposal or re-use of equipment	Yes	Yes		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.
A8 Technological controls	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. Specific 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.
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.

A.B.12 Data making Yes Yes Yes Yes Was analyses assets used for the storage and yes asset to did as from NRB and its customers. A.B.13 Data making Yes Yes Yes Yes Was processing of data from NRB and its customers before disposal or re use is effected. A.B.14 Data making Yes Yes Yes Was processing of data from NRB and its customers before disposal or re use is effected. A.B.15 Data leading prevention Yes Yes Yes Was manages assets used for the storage and processing of data from NRB and its customers before disposal to return to mount or model contained with MSD stableton with the formation of the customers and customers a						
A.B.1.1 Data masking Yes Yes NiB manages assets used for the storage and process methods button with remainder container. A.B.1.2 Data leakage prevention Yes Yes Yes NiB manages assets used for the storage and process methods button the processing of data from NiB and its customers. A.B.1.2 Data leakage prevention Yes Yes Yes NiB manages assets used for the storage and process of the process of the process of the storage and process of the storage and process of the process of the storage and process					NRB manages assets used for the storage and	Work instruction to ensure media erasure before disposal or re-use is
A 8.11 Data making Yes Yes Pes pocessing of data from NRB and its customers of the storage and processing of data from NRB and its customers of the storage and processing of data from NRB and its customers. A 8.12 Data leakage prevention Yes Yes Pes Pes To Data leakage prevention Yes Yes Yes Yes Yes Pes To Data leakage prevention Yes	A.8.10	Information deletion	Yes	Yes	processing of data from NRB and its customers.	
A 8.11 Date masking by the services of the storage and processing of data from NBB and its existomers. The workfore includes built, stress and processing of data from NBB and its existomers. The workfore includes built, stress and processing of data from NBB and its existomers. The workfore includes built, stress includes built, stress and processing of data from NBB and its existomers. The workfore includes built, stress and processing of data from NBB and its existomers. The workfore includes built, stress the subject to the Straight and processing of data from NBB and its existomers. The workfore includes built process. The workfore includes built, stress of the Straight and processing of data from NBB and its existomers. The NBB must be able to maintain its opportunity of the storage and processing of data from NBB and its existomers. The NBB must be able to maintain its opportunity of the storage and processing of data from NBB and its existomers. The NBB must be able to maintain its opportunity of the storage and processing of data from NBB and its existomers. The NBB must be able to maintain its opportunity of the storage and processing of data from NBB and its existomers. The NBB must be able to maintain its opportunity of the storage and processing of data from NBB and its existomers. The NBB must be able to maintain its opportunity of the storage and processing of data from NBB and its existomers. The NBB must be able to maintain its opportunity of the storage and processing of data from NBB and its existomers. The Radian from NBB and its existomers are required to maintain to opportunity of the storage and processing of data from NBB and its existomers. The required in the storage and processing of data from NBB and its existomers. The required in the storage and processing of data from NBB and its existomers. The required in the storage and processing of data from NBB and its existomers. The required in the storage and processing of data from NBB and its existomers. The required process is only all	7.110120	inioinidaen deieaen				Laptop are encrypted and Mobile are managed using a MDM solution with
A 8.11 Data masking Yes Pes processing of data from NBB and its customers. A 8.12 Data leakage prevention Pessage of the storage and processing of data from NBB and its customers. In Instructions to the line framethy one by a beginning the storage and processing of data from NBB and its customers. In Instructions on the intranet for end-users to law to label information and processing of data from NBB and its customers. In Instructions on the intranet for end-users on low to label information and processing of data from NBB and its customers. In Instructions on the intranet for end-users on low to label information and process. The end using warded tools (Microsoft body left processing of data from NBB and its customers.) A 8.13 Information backup Yes Yes Pessage and processing of data from NBB and its customers. A 8.14 Redundancy of information processing facilities Yes Yes Pessage and Pes						
A 8.12 Data leakage prevention Ves Ves NRB manages assets used for the storage and processing of data from NRB and its customers. If Charter & Employee awareness to per level & guidance for end-users on how to label information and protect e- mail using wailable tools, (Microsoft Purview). Specific Self-Wild cases to self-test data definition. A 8.13 Information backup Ves Ves Wes NRB manages assets used for the storage and protect e- mail using wailable tools, (Microsoft Purview). Specific Self-Wild cases to store that self-tribution. A 8.14 Redundancy of information processing facilities Ves Ves NRB manages assets used for the storage and processing of data from NRB and its customers. Securely in the event of a disaster. Barrier are regularly updated and applied. At least two back-up copies, with a third more regularly updated in deeded. Disaster Recovery strategy is defined and applied. At least two back-up copies, with a third more regularly updated in deeded. Disaster Recovery strategy is defined and applied. At least two back-up copies, with a third more regularly updated in deeded. Disaster Recovery strategy is defined and implemented - Technical Recovery strategy is defined and implemented - Technical Recovery Plans are regularly updated and tested. Der are regularly updated and tested disaster regularly updated and tested. Der are regularly updated and correlated in our SEM. Security events and alerts are analyzed on the protection of log data. A 8.16 Monitoring activities Ves Ves Ves Ves NRB employees, co-workers and customers. NRB. N					NRB manages assets used for the storage and	Data masking is performed using the 'Normal Change' workflow (defined in
A 8.12 Data leakage prevention Yes Yes Will manages assets used for the storage and processing of data from NRB and its customers. Instructions to neth users on how to bable information and processing of data from NRB and its customers. Instructions to the Instruction on the Instruction to the Instru	A.8.11	Data masking	Yes	Yes	processing of data from NRB and its customers.	our Change Management process). The workflow includes build, test and risk
A 8.12 Data leakage prevention Per Services of data from NRB and its customers in contract for and users to detect data editionation and protect entail using available tools (Micropot Puriew). Specific Silful Aucessos to detect data editionation and protect entail using available tools (Micropot Puriew). Specific Silful Aucessos to detect data editionation and protect entail using available tools (Micropot Puriew). Specific Silful Aucessos to detect data editionation and protect entail using available tools (Micropot Puriew). Specific Silful Aucessos to detect data editionation and protect entail using available tools (Micropot Puriew). Specific Silful Aucessos to detect data editionation and protect entail using available tools (Micropot Puriew). Specific Silful Aucessos to detect data editionation and protect entail using available tools (Micropot Puriew). Specific Silful Aucessos to detect data editionation and protect entail using available tools (Micropot Puriew). Specific Silful Aucessos to detect data edition and protect on extending the protection of						analysis phases.
A.8.12 Data leakage prevention Ves Ves Pes Instructions on the intranse for end-users on how to label information and processing protect er multiple available took (officers) Planeway. Specific SEM userases to defect data exilitation. A.8.13 Information backup Ves Yes Pes Pes NRB manages assets used for the storage and processing of data from NRB and its customers. NRB and its customers of the storage and processing of data from NRB and its customers. NRB employees, co-workers and customers have access to data and existence of the storage and processing of data from NRB and its customers. NRB employees, co-workers and customers have access to data and processing of data from NRB and its customers. NRB employees, co-workers and customers have access to data and processing of data from NRB and its customers. NRB employees and least set of the storage and processing of data from NRB and its customers. NRB employees are set of data from NRB and its customers. NRB employees and least set on Standard processing of data from NRB and its customers. NRB employees are set of data and correlated in our SIEM. Security events and alerts are analyzed and escaled as required by our Sectors team. Using are stored and correlated in our SIEM. Security events and alerts are analyzed and escaled as a required by our Sectors team. Security incident are handled following our Security incident Management process. The work of the storage and processing of data from NRB and its customers. NRB employees are all our sections teams analyzed and escaled as required by our Sectors team. Security incident are analyzed and escaled as required by our Sectors team. Security incident are handled following our Security incident Management process. The work of the storage and processing of data from NRB and its customers. NRB employees are all our sections teams are allowed on end-user works according events to our Settlem's team of a sonay section to elevate the section of sonay are allowed on end-user works according to the customers are allowe					NRB manages assets used for the storage and	Information Classification policy & Post-it to give instructions to end-users.
A 8.13 Information backup A 8.13 Information backup A 8.14 Redundancy of information processing facilities A 8.15 Redundancy of information processing facilities A 8.16 Redundancy of information processing facilities A 8.17 Logging Yes Yes Yes Yes Yes Yes A 8.18 Redundancy of information processing facilities Yes Yes Yes Yes Yes A 8.19 Redundancy of information processing facilities Yes Yes Yes Yes Yes Yes Yes					processing of data from NRB and its customers.	IT Charter & Employee awareness to give rules & guidance.
A.8.13 Information backup Yes Yes Yes NRB manages assets used for the storage and processing of data from NRB and fix customers. The NRB must be able to maintain its operations of the event of a disaster. Redundancy of information processing facilities Yes Yes Yes Yes NRB employees, co-workers and customers NRB manages assets used for the storage and public entire the process of the process	Δ & 12	Data leakage prevention	Voc	Voc		Instructions on the Intranet for end-users on how to label information and
A 8.13 Information backup Yes Yes Yes Yes Yes Yes Yes Ye	A.0.12	Data leakage prevention	103	103		protect e-mail using available tools (Microsoft Purview).
A 8.14 Redundancy of information processing facilities A 8.14 Redundancy of information processing facilities A 8.15 Redundancy of information processing facilities A 8.16 Redundancy of information processing facilities A 8.17 Logging A 8.18 Monitoring activities A 8.18 Lise of privileged utility programs A 8.19 Lise of privileged utility programs A 8.19 Installation of software on operational systems A 8.10 New or case stored that processing of data from NRB and its customers. A 8.10 New or case stored and services to data and services managed by NRB. A 8.11 Lise of privileged utility programs A 8.12 Security of programs A 8.13 New or case stored and services managed by NRB. A 8.14 Use of privileged utility programs A 8.15 Security events and services managed by NRB. A 8.16 Nonitoring activities A 8.17 Clock synchronization A 8.18 New or case stored by the ENP of Source is sensitive systems and data. A 8.19 Installation of software on operational systems A 8.10 New or case stored by the ENP of Source is sensitive systems and data. A 8.10 New or case stored and services managed by NRB. A 8.11 New or case stored by the ENP of Source is sensitive systems and data. A 8.12 Security or case of the storage and processing of data from NRB and its customers. A 8.15 New or case stored by the ENP of Source is sensitive systems and data. A 8.16 New or case stored by the ENP of Source is sensitive systems and data. A 8.17 New or case stored by the ENP of Source is sensitive systems and data. A 8.18 New or case stored by the ENP of Source is sensitive systems and data. A 8.19 New or case stored and services of the storage and processing of data from NRB and its customers. A 8.20 New or case stored is sensitive systems and data. A 8.21 Security of network services A 8.22 Security of network services A 8.23 Security of network services A 8.24 Security of network services A 8.25 Secu						Specific SIEM usecases to detect data exfiltration.
Regular restore testing for different platform are performed. A 8.14 Redundancy of information processing facilities Yes Yes Yes NRB must be able to maintain its operations. Bit first a seleptory on at least 2 generalised datacenters. Business Continuity policy is defined and applied. Bit first a seleptory on at least 2 generalised tradeactions. Bit first a seleptory on at least 2 generalised datacenters. Business Continuity policy is defined and applied. Bit first a seleptory on at least 2 generalised selected and selected. Bit first a selective of a disaster. Bit first a selective of a selective					NRB manages assets used for the storage and	Backup policy is defined and applied. At least two back-up copies, with a third
Regular restore testing for different platform are performed. A 8.14 Redundancy of information processing facilities Yes Yes Yes NRB must be able to maintain its operations. Miss first is deployed and least 2 generallent datacenters. Business Continuity policy is defined and applied. Bit Air or regularly voidated. BCP are regularly updated. BCP are regularly updated. BCP are regularly updated and implemented - Technical Recovery Plans are regularly updated and implemented - Technical Recovery Plans are regularly updated and implemented - Technical Recovery Plans are regularly updated and applied of the protection of log data. A 8.15 Logging Yes Yes Yes Yes NRB employees, co-workers and customers have access to data and services managed by NRB. Logs are stored and correlated in our SEM. Security events and alerts are analyzed and escalated as required by our SecOps team. Logs are stored and correlated in our SEM. Security events and alerts are analyzed and escalated as required by our SecOps team. A 8.16 AS DO Clock synchronization Yes Yes Yes NRB employees, co-workers and customers have access to data and services managed by NRB. Logs are stored and correlated in our SEM. Security events and alerts are analyzed and escalated as required by our SecOps team. A 8.18 Use of privileged utility programs Yes Yes NRB employees, co-workers and customers have access to data and services managed by NRB. NRB employees, co-workers and customers NRB employees, co-workers and customers logs and correlated in our SEM. Security events and alerts are analyzed and escalated as required by our SecOps team. NRB employees, co-workers and customers NRB em	A.8.13	Information backup	Yes	Yes	_	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
A 8.14 Redundancy of Information processing facilities Yes Yes NBB employees, co-workers and customers have access to data and services managed by NRB. A 8.15 Logging Yes Yes NBB employees, co-workers and customers have access to data and services managed by NRB. RBB employees, co-workers and customers have access to data and services managed by NRB. RBB employees, co-workers and customers have access to data and services managed by NRB. RBB employees, co-workers and customers have access to data and services managed by NRB. RBB employees, co-workers and customers have access to data and services managed by NRB. RBB employees, co-workers and customers have access to data and services managed by NRB. RBB employees, co-workers and customers have access to data and services managed by NRB. RBB employees, co-workers and customers have access to data and services managed by NRB. RBB employees, co-workers and customers have access to data and services managed by NRB. RBB employees, co-workers and customers have access to data and services managed by NRB. RBB employees, co-workers and customers have access to data and services managed by NRB. RBB employees, co-workers and customers have access to data and services managed by NRB. RBB employees, co-workers and customers have access to data and services managed by NRB. RBB employees, co-workers and customers have access to data and services managed by NRB. RBB employees, co-workers and customers have access to data and services managed by NRB. RBB employees, co-workers and customers have access to data and services managed by NRB. RBB employees, co-workers and customers have access to data and services managed by NRB. RBB employees, co-workers and customers have access to data and services managed by NRB. RBB employees, co-workers and customers have access to data and services managed by NRB. RBB employees, co-workers and customers have access to data and services managed by NRB. Security events and alerts are analyzed and escalated as require		'				
A.B.14 Redundancy of information processing facilities **Pes*** **Pes*** **Pes*** **Pes*** **NBB employees, co-workers and customers have access to data and services managed by NRB. **AB.15					The NRB must be able to maintain its operations	
A.B.14 Redundancy of information processing facilities A.B.15 Redundancy of information processing facilities A.B.16 Redundancy of information processing facilities A.B.17 Logging A.B.18 Personal Sequency A.B.18 Personal Sequency A.B.19 A result of the sequency A.B.19 Logging A.B.19 Logging A.B.19 Logging A.B.19 Logging A.B.19 Logging A.B.19 Logging A.B.10 Redundancy of information processing facilities A.B.10 Redundancy of information processing facilities A.B.10 Redundancy of information processing facilities A.B.110 Logging A.B.111 Logging A.B.111 Logging A.B.112 Logging A.B.112 Logging A.B.113 Logging A.B.114 Logging A.B.115 Logging A.B.115 Logging A.B.117 Clock synchronization A.B.118 Logging A.B.118 Logging A.B.119 Logging A.B.119 Logging A.B.110 Logging A.B.110 Logging A.B.110 Logging A.B.110 Logging A.B.110 Logging A.B.110 Logging A.B.111 Logging A.B.110 Logging A.B					·	, ,
A.8.15 Logging Yes Yes NRB employees, co-workers and customers logical Access Control policy is defined and implemented - Technical Recovery Plans are regularly updated and tested. Logging A.8.15 Logging Yes Yes NRB. A.8.16 NRB employees, co-workers and customers have access to data and services managed by NRB. A.8.16 NRB employees, co-workers and customers have access to data and services managed by NRB. A.8.17 Clock synchronization Yes Yes Logs produced must be exploitable. A.8.18 Use of privileged utility programs Yes Yes Yes Sensitive systems and data. A.8.19 Installation of software on operational systems Yes Yes Yes Yes Yes Yes Yes Yes Yes Ye	4 0 14	Dodundanay of information and a first	Vc -	V		
A 8.15 A 8.16 A 8.17 A 8.18 A 8.19 A 8.10 A 8.10	A.8.14	Redundancy of information processing facilities	res	res		, ,
A.8.15 A.8.16 A.8.16 A.8.17 Clock synchronization A.8.18 Use of privileged utility programs Yes Yes Yes A.8.19 Installation of software on operational systems A.8.19 A.8.19 A.8.19 A.8.10 A.8.10 A.8.10 A.8.10 A.8.10 A.8.10 A.8.10 A.8.10 A.8.10 A.8.11 A.8.11 A.8.12 A.8.12 A.8.13 A.8.12 A.8.13 A.8.14 A.8.15 A.8.15 A.8.16 A.8.16 A.8.17 A.8.18 A.8.18 A.8.17 A.8.18 A.8.18 A.8.18 A.8.19 A.8.18 A.8.19 A.8.18 A.8.10 A.8						,
A.8.15 Logging Yes Yes NRB employees, co-workers and customers have access to data and services managed by NRB. NRB employees, co-workers and customers and policy is defined and applied for the protection of log data. NRB employees, co-workers and customers have access to data and services managed by NRB. NRB employees, co-workers and customers have access to data and services managed by RRB. NRB employees, co-workers and customers have access to data and services managed by RRB. NRB employees, co-workers and customers have access to data and services managed by RRB. A.8.17 Clock synchronization Yes Yes Logs produced must be exploitable. NRB employs staff for positions with access to Data The Infrastructure (based on Internet and GPS source) is implemented. NRB employs staff for positions with access to Security events and alerts are analyzed and escalated as required by our Secotypt incident are handled following our Security incident and services are handled following our Security incident are handled following our Security incident are handled followi						,
A.8.15 A.8.16 A.8.17 A.8.17 A.8.18 A.8.18 A.8.18 A.8.18 A.8.19 A.8.10 A.8.19 A.8.10 A.8.19 A.8.10 A.8.19 A.8.10 A.8.11 A.8.11 A.8.11 A.8.11 A.8.12 A.8.11 A.8.12 A.8.12 A.8.13 A.8.13 A.8.14 A.8.15 A.8.15 A.8.15 A.8.16 A.8.16 A.8.17 A.8.17 A.8.18 A.8.18 A.8.18 A.8.18 A.8.18 A.8.18 A.8.18 A.8.19 A.8.18 A.8.19 A.8.19 A.8.10 A.8.10					NRB employees, co-workers and customers	
A.8.16 Monitoring activities A.8.17 Monitoring activities A.8.18 Use of privileged utility programs A.8.19 Installation of software on operational systems A.8.19 Installation of software on operational systems A.8.19 A.8.10 Networks security A.8.10 A.8.10 A.8.10 Networks security A.8.110 A	A 0.15	Logging	Voc	Voc	have access to data and services managed by	data.
A.8.16 Monitoring activities	A.8.15	Logging	res	res	NRB.	Logs are stored and correlated in our SIEM. Security events and alerts are
A.8.16 Monitoring activities Yes Yes NRB. A.8.17 Clock synchronization Yes Yes Yes Logs produced must be exploitable. A.8.18 Use of privileged utility programs A.8.18 A.8.18 A.8.19 Installation of software on operational systems A.8.20 A.8.20 A.8.20 A.8.20 A.8.21 A.8.21 A.8.21 A.8.21 A.8.21 A.8.30 A.8.31 A.8.31 A.8.32 A.8.32 A.8.32 A.8.33 A.8.34 A.8.35 A.8.35 A.8.35 A.8.35 A.8.35 A.8.36 A.8.36 A.8.37 A.8.38 A.8.39 A.8.39 A.8.30 A.8.						analyzed and escalated as required by our SecOps team.
A.8.17 Clock synchronization Yes Yes NRB. Clock synchronization Yes Yes Logs produced must be exploitable. A.8.17 Clock synchronization Yes Yes Logs produced must be exploitable. A.8.18 Use of privileged utility programs Yes Yes Yes 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. NRB manages assets used for the storage and processing of data from NRB and its customers. NRB manages assets used for the storage and processing of data from NRB and its customers. Solvant center is used to deploy standard software on WKS. No admin rights are allowed on end-user workfations, 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 Network Security Policy is defined and applied. Network Security Policy is defined and paplied.					NRB employees, co-workers and customers	Logs are stored and correlated in our SIEM. Security events and alerts are
A.8.17 Clock synchronization A.8.18 Use of privileged utility programs A.8.19 Installation of software on operational systems A.8.19 Installation of software on operational systems A.8.19 A.8.19 Installation of software on operational systems A.8.19 A.8.19 Security incident are handled following our Security Incident Management process. A.8.19 A.8.19 Installation of software on operational systems A.8.10 A.8.10 A.8.10 Security of networks security A.8.10 A.8.10 Security of networks security A.8.10 A.8.10 Security of network services A.8.10 A.8.10 Security incident are handled following our Security Incident Management processing of the storage and processing of data from NRB and its customers. A.8.10 A.	Λ 9 16	Monitoring activities	Voc	Voc	have access to data and services managed by	analyzed and escalated as required by our SecOps team.
A.8.17 Clock synchronization A.8.18 Use of privileged utility programs Yes Yes NRB employs staff for positions with access to sensitive systems and data. NRB manages assets used for the storage and processing of data from NRB and its customers. NRB manages assets used for the storage and processing of data from NRB and its customers. NRB manages assets used for the storage and processing of data from NRB and its customers. NRB manages assets used for the storage and processing of data from NRB and its customers. NRB manages assets used for the storage and processing of data from NRB and its customers. NRB manages assets used for the storage and processing of data from NRB and its customers. NRB manages assets used for the storage and processing of data from NRB and its customers. NRB manages assets used for the storage and processing of data from NRB and its customers. NRB manages assets used for the storage and processing of data from NRB and its customers. NRB manages assets used for the storage and processing of data from NRB and its customers. NRB manages assets used for the storage and processing of data from NRB and its customers. NRB manages assets used for the storage and processing of data from NRB and its customers. NRB manages assets used for the storage and processing of data from NRB and its customers. NRB manages assets used for the storage and processing of data from NRB and its customers. NRB manages assets used for the storage and processing of data from NRB and its customers. NRB manages assets used for the storage and processing of data from NRB and its customers. NRB manages assets used for the storage and processing of data from NRB and its customers. NRB manages assets used for the storage and processing of data from NRB and its customers. NRB manages assets used for the storage and processing of data from NRB and its customers. NRB manages assets used for the storage and processing of data from NRB and its customers. NRB manages assets used for the storage and pro	A.0.10	Widilitoring activities	162	162	NRB.	Security incident are handled following our Security Incident Management
A.8.17 Lock synchronization Yes Yes NRB employs staff for positions with access to sensitive systems and data. NRB employs staff for positions with access to sensitive systems and data. NRB manages assets used for the storage and processing of data from NRB and its customers. A.8.19 Installation of software on operational systems Yes Yes Yes Yes Yes NRB manages assets used for the storage and processing of data from NRB and its customers. A.8.20 Networks security NRB manages assets used for the storage and processing of data from NRB and its customers. NRB manages assets used for the storage and processing of data from NRB and its customers. 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 Network Security Policy is defined and applied. Network Security Policy is defined and applied. Network Architecture diagrams are updated regularly. Network Architecture diagrams are updated regularly. Network Security Policy is defined and applied. Network Security Policy is defined and						process.
A.8.18 Use of privileged utility programs Yes Yes NRB employs staff for positions with access to sensitive systems and data. NRB manages assets used for the storage and processing of data from NRB and its customers. A.8.19 Installation of software on operational systems A.8.20 Networks security Yes NRB manages assets used for the storage and processing of data from NRB and its customers. NRB manages assets used for the storage and processing of data from NRB and its customers. NRB software on operational 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 in the storage and processing of data from NRB and its customers. A.8.20 Network Security Policy is defined and applied. Network Security Policy is defined and applied. Network Architecture diagrams are updated regularly. Network Informations are stored in specific tools and the CMDB. Network Security Policy is defined and applied.	Δ 8 17	Clack synchronization	Vec	Yos	Logs produced must be exploitable.	A robust NTP infrastructure (based on Internet and GPS source) is
A.8.18 Use of privileged utility programs Yes Yes NRB manages assets used for the storage and processing of data from NRB and its customers. A.8.19 Installation of software on operational systems Yes Yes Yes Yes Yes Yes Yes	7.0.17	CIOCK SYNCHIONIZATION	163	163		implemented.
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 operational systems Yes Yes Yes Yes NRB manages assets used for the storage and processing of data from NRB and its customers. 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. NRB manages assets used for the storage and processing of data from NRB and its customers. NRB manages assets used for the storage and processing of data from NRB and its customers. NRB manages assets used for the storage and processing of data from NRB and its customers. NRB manages assets used for the storage and processing of data from NRB and its customers. NRB manages assets used for the storage and processing of data from NRB and its customers. NRB manages assets used for the storage and processing of data from NRB and its customers. NRB manages assets used for the storage and processing of data from NRB and its customers. NRB manages assets used for the storage and processing of data from NRB and its customers. NREWORK Security Policy is defined and applied. Network Security Policy is defined and applied.					NRB employs staff for positions with access to	Use of privileged utility program are detected by the EDR on servers
Security events and alerts are analyzed and escalated as required by our Secops team. NRB manages assets used for the storage and processing of data from NRB and its customers. A.8.19 Installation of software on operational systems Yes Yes Yes Yes NRB manages assets used for the storage and processing of data from NRB and its customers. 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. NRB manages assets used for the storage and processing of data from NRB and its customers. NRB manages assets used for the storage and processing of data from NRB and its customers. NRB manages assets used for the storage and processing of data from NRB and its customers. NRB manages assets used for the storage and processing of data from NRB and its customers. NRB manages assets used for the storage and processing of data from NRB and its customers. NRB manages assets used for the storage and processing of data from NRB and its customers. Network Security Policy is defined and applied. Network 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. Workflow (defined in our Change Management process). The workflow includes build, test and risk analysis phases. Workflow (defined in our Change Management process). The workflow includes build, test and risk analysis phases. Workflow (defined in our Change Management process). The workflow includes build, test and risk analysis phases. Workflow (defined in our Change Management process). The workflow includes b	Δ 8 18	Use of privileged utility programs	Yes	Yes	sensitive systems and data.	forwarding events to our SIEM/SOC.
NRB manages assets used for the storage and processing of data from NRB and its customers. A.8.19 Installation of software on operational systems Yes Yes Yes Yes NRB manages assets used for the storage and processing of data from NRB and its customers. 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 Network Security Policy is defined and applied. Network Architecture diagrams are updated regularly. Network Architecture diagrams are updated regularly. Network Informations are stored in specific tools and the CMDB. Network Security Policy is defined and applied.	70.10	ose of privileged delity programs	103	103		Security events and alerts are analyzed and escalated as required by our
processing of data from NRB and its customers. A.8.19 Installation of software on operational systems Yes Yes Yes Yes Yes Yes Yes						SecOps team.
A.8.19 Installation of software on operational systems Yes Yes Yes Yes Yes Yes Yes					_	, ,
A.8.19 Installation of software on operational systems Yes Yes Yes Yes Yes Yes Yes Yes Yes Ye					processing of data from NRB and its customers.	workflow (defined in our Change Management process). The workflow
A.8.19 Installation of software on operational systems Yes Yes Yes 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 NRB manages assets used for the storage and Network Security Policy is defined and applied. Network Architecture diagrams are updated regularly. Network informations are stored in specific tools and the CMDB. NRB manages assets used for the storage and Processing of data from NRB and its customers. NRB manages assets used for the storage and Processing of data from NRB and its customers. NRB manages assets used for the storage and Processing of data from NRB and its customers. Network Security Policy is defined and applied.						includes build, test and risk analysis phases.
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 Yes NRB manages assets used for the storage and processing of data from NRB and its customers. Network Architecture diagrams are updated regularly. Network Architecture diagrams are updated regularly. Network informations are stored in specific tools and the CMDB. NRB manages assets used for the storage and processing of data from NRB and its customers. Security of network services Yes Yes Yes Yes Yes Yes Yes						, , , , , , , , , , , , , , , , , , , ,
A.8.20 Networks security Yes Yes NRB manages assets used for the storage and processing of data from NRB and its customers. NRB manages assets used for the storage and processing of data from NRB and its customers. NRB manages assets used for the storage and processing of data from NRB and its customers. Network Architecture diagrams are updated regularly. Network Architecture diagrams are updated regularly. Network informations are stored in specific tools and the CMDB. Network Security Policy is defined and applied. Network informations are stored in specific tools and the CMDB. Network Security Policy is defined and applied. Secure Network Services are implemented and monitored (VPN/DNS/DDOS)	A.8.19	Installation of software on operational systems	Yes	Yes		NRB Software Center is used to deploy standard software on WKS.
A.8.20 Networks security Yes Yes Yes NRB manages assets used for the storage and processing of data from NRB and its customers. NRB manages assets used for the storage and processing of data from NRB and its customers. NRB manages assets used for the storage and processing of data from NRB and its customers. NRB manages assets used for the storage and network informations are stored in specific tools and the CMDB. NRB manages assets used for the storage and processing of data from NRB and its customers. Network Architecture diagrams are updated regularly. Network Informations are stored in specific tools and the CMDB. NRB manages assets used for the storage and processing of data from NRB and its customers. Security Policy is defined and applied. Secure Network Services are implemented and monitored (VPN/DNS/DDoS)						No admin rights are allowed on end-user workstations, installation of non-
A.8.20 Networks security Yes Yes Yes NRB manages assets used for the storage and processing of data from NRB and its customers. NRB manages assets used for the storage and processing of data from NRB and its customers. NRB manages assets used for the storage and Network Architecture diagrams are updated regularly. Network informations are stored in specific tools and the CMDB. NRB manages assets used for the storage and Processing of data from NRB and its customers. Network Security Policy is defined and applied. Network Security Policy is defined and applied. Secure Network Services are implemented and monitored (VPN/DNS/DDoS)						standard software on WKS is only allowed using a special tool to elevate
A.8.20 Networks security Yes Yes NRB manages assets used for the storage and processing of data from NRB and its customers. NRB manages assets used for the storage and processing of data from NRB and its customers. NRB manages assets used for the storage and Network Architecture diagrams are updated regularly. Network informations are stored in specific tools and the CMDB. NRB manages assets used for the storage and processing of data from NRB and its customers. NRB manages assets used for the storage and processing of data from NRB and its customers. Secure Network Services are implemented and monitored (VPN/DNS/DDoS						privilege and monitor activities. Activities are reviewed regularly to identify
A.8.20 Networks security Yes Yes processing of data from NRB and its customers. Network Architecture diagrams are updated regularly. Network informations are stored in specific tools and the CMDB. NRB manages assets used for the storage and processing of data from NRB and its customers. Network Architecture diagrams are updated regularly. Network Security Policy is defined and applied. Secure Network Services are implemented and monitored (VPN/DNS/DDOS)						
Network informations are stored in specific tools and the CMDB. NRB manages assets used for the storage and processing of data from NRB and its customers. Security of network services Yes Network informations are stored in specific tools and the CMDB. Network Security Policy is defined and applied. Secure Network Services are implemented and monitored (VPN/DNS/DDoS)					_	, , ,
NRB manages assets used for the storage and processing of data from NRB and its customers. Security of network services Yes Yes NRB manages assets used for the storage and processing of data from NRB and its customers. Secure Network Services are implemented and monitored (VPN/DNS/DDoS	A.8.20	Networks security	Yes	Yes	processing of data from NRB and its customers.	, , ,
A.8.21 Security of network services Yes Processing of data from NRB and its customers. Secure Network Services are implemented and monitored (VPN/DNS/DDoS						· · · · · · · · · · · · · · · · · · ·
,					_	
protection).	A.8.21	Security of network services	Yes	Yes	processing of data from NRB and its customers.	, , , ,
						protection).

NRB manages assets used for the storage and processing of data from NRB and its customers. Network Architecture diagram	ned and annlied
	s are updated regularly.
	red in specific tools and the CMDB.
	cool is used to store information, implement
rules and verify compliance.	oor is used to store information, implement
NRR ascets have connections to untrusted Wigh Provy gateway is implem	ented for internet access
	is implemented for internet access.
NRB manages assets used for the storage and	<u> </u>
processing of data from NRR and its customers. Cartificate Management policy	• •
USE OF CRYPTOGRADIN YES YES YES	edure is defined and implemented.
CMDB and Secure Vault for sto	·
NRB's activities and services include systems & Secure Systems Development	0
A.8.25 Secure development life cycle Yes Yes software development.	Life Cycle policy is defined and applied.
	is defined and implemented. It includes Stage
	to ensure that requirements are identified,
Application security requirements fes software development. Gates and security-by-besign implemented and tested.	to chaire that requirements are identified,
NRR's activities and services include systems & Project Management process	is defined and implemented. It includes Stage
A.8.27 Secure system architecture and engineering principles Yes Yes software development.	
NRB's activities and services include systems & Secure Systems Development	
1 A.8.28 Secure coding Yes Yes	d either using tools and manual tests.
	is defined and implemented. It includes Stage
A.8.29 Security testing in development and acceptance Yes Yes software development. Gates and Security-by-Design.	s defined and implemented. It includes stage
odice and occurry by occupant	d either using tools and manual tests.
	of purchase contains specific clauses on
software development	or parenase contains specific clauses on
LAX30 Voltsourced development yes yes .	is defined and implemented. It includes Stage
Gates and Security-by-Design.	s defined and implemented. It includes stage
	ftware Development is defined and applied.
	is defined and implemented. It includes Stage
Gates and Security-hy-Design	s defined and implemented. It includes stage
A.8.31 Separation of development, test and production environments Yes Yes Network Security Policy is defi	ned and annlied
Network Architecture diagram	• •
Network Architecture diagram	s are updated regularly.
NRB manages assets used for the storage and Change Management process	is defined and implemented. The workflow for
processing of data from NRR and its customers 'Normal Change' includes built	I, test and risk analysis phases.
A.8.32 Change management Yes Yes ITSM tool to support our Change	· ·
This is to the support our claim.	0
NRB's activities and services include systems & Duplication of data between e	nvironment is performed using the 'Normal
	our Change Management process). The
worlflow includes formal anni	
LAX33 Lest Information Yes Yes	which includes Stage Gates and Security-by-
Design which includes analysis	
NRB manages assets used for the storage and Technical audit autorisation fo	rm must be filled by each involved parties prior
NRB manages assets used for the storage and Protection of information systems during audit testing Yes Yes processing of data from NRB and its customers. each audit.	rm must be filled by each involved parties prior