Statement of Applicability
Eurofiber Cloud Infra
ISO27001:2022
Version 1.1
Date 10/09/2024

	#	Title	Control (niet afdrukken in de PDF)	Applicable Y/N	Implemented Y/N	Reason inclusion: Risk	Reason inclusion: Legal	Reason inclusion: Contractual	Reason for exclusion
5. Organizational controls	5.1	Policies for information security	Information security policy and topic-specific policies shall be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.	Y	Y	☐	☐	☑	
	5.2	Information security roles and responsibilities	Information security roles and responsibilities shall be defined and allocated according to the organization needs.	Y	Y	☐	☐	☑	
	5.3	Segregation of duties	Conflicting duties and conflicting areas of responsibility shall be segregated.	Y	Y	☐	☐	☑	
	5.4	Management responsibilities	Management shall require all personnel to apply information security in accordance with the established information security policy, top- ic-specific policies and procedures of the organization.	Y	Y	☑	☐	☑	
	5.5	Contact with authorities	The organization shall establish and maintain contact with relevant authorities.	Y	Y	☐	☑	☑	
	5.6	Contact with special interest groups	The organization shall establish and maintain contact with special interest groups or other specialist security forums and professional associations.	Y	Y	☐	☑	☐	
	5.7	Threat intelligence	Information relating to information security threats shall be collected and analysed to produce threat intelligence.	Y	Y	☐	☐	☐	
	5.8	Information security in project management	Information security shall be integrated into project management.	Y	Y	☑	☐	☐	
	5.9	Inventory of information and other associated assets	An inventory of information and other associated assets, including owners, shall be developed and maintained.	Y	Y	☑	☐	☑	
	5.10	Acceptable use of information and other associated assets	Rules for the acceptable use and procedures for handling information and other associated assets shall be identified, documented and implemented.	Y	Y	☑	☐	☑	
	5.11	Return of assets	Personnel and other interested parties as appropriate shall return all the organization's assets in their possession upon change or termination of their employment, contract or agreement.	Y	Y	☑	☐	☑	
	5.12	Classification of information	Information shall be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements.	Y	Y	☑	☐	☑	
	5.13	Labelling of information	An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	Y	Y	☑	☐	☐	
	5.14	Information transfer	Information transfer rules, procedures, or agreements shall be in place for all types of transfer facilities within the organization and between the organization and other parties.	Y	Y	☑	☐	☑	
	5.15	Access control	Rules to physical and logical access to information and other associated assets shall be established and implemented based on business and information security requirements.	Y	Y	☑	☐	☑	
	5.16	Identity management	The full life cycle of identities shall be managed.	Y	Y	☑	☐	☑	
	5.17	Authentication information	Allocation and management of authentication information shall be led by a management process, including advising personnel on appropriate handling of authentication information.	Y	Y	☑	☐	☑	
	5.18	Access rights	Access rights to information and other associated assets shall be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access .	Y	Y	☑	☐	☑	
	5.19	Information security in supplier relationships	Processes and procedures shall be defined and implemented to manage the information security risks associated with the use of supplier's products or services.	Y	Y	☑	☐	☑	
	5.20	Addressing information security within supplier agreements	Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship.	Y	Y	☑	☐	☑	
	5.21	Managing information security in the information and communication technology (ICT) supply chain	Processes and procedures shall be defined and implemented to manage the information security risks associated with the ICT products and services supply chain.	Y	Y	☑	☐	☐	
	5.22	Monitoring, review and change management of supplier services	The organization shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.	Y	Y	☑	☐	☐	
	5.23	Information security for use of cloud services	Processes for acquisition, use, management and exit from cloud services shall be established in accordance with the organization's information security requirements.	Y	Y	☐	☐	☑	
	5.24	Information security incident management planning and preparation	The organization shall plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.	Y	Y	☑	☑	☐	
	5.25	Assessment and decision on information security events	The organization shall assess information security events and decide if they are to be categorized as information security incidents.	Y	Y	☑	☐	☑	
	5.26	Response to information security incidents	Information security incidents shall be responded to in accordance with the documented procedures.	Y	Y	☑	☐	☐	
	5.27	Learning from information security incidents	Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls.	Y	Y	☑	☐	☐	
	5.28	Collection of evidence	The organization shall establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events.	Y	Y	☑	☑	☐	
	5.29	Information security during disruption	The organization shall plan how to maintain information security at an appropriate level during disruption.	Y	Y	☑	☐	☑	
	5.30	ICT readiness for business continuity	ICT readiness shall be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.	Y	Y	☐	☐	☐	
	5.31	Legal, statutory, regulatory and contractual requirements	Legal, statutory, regulatory and contractual requirements relevant to information security and the organization's approach to meet these requirements shall be identified, documented and kept up to date.	Y	Y	☑	☑	☑	
	5.32	Intellectual property rights	The organization shall implement appropriate procedures to protect intellectual property rights.	Y	Y	☐	☑	☑	
	5.33	Protection of records	Records shall be protected from loss, destruction, falsification, unau- thorized access and unauthorized release.	Y	Y	☐	☑	☑	
	5.34	Privacy and protection of personal identifiable information (PII)	The organization shall identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.	Y	Y	☑	☑	☑	
	5.35	Independent review of information security	The organization's approach to managing information security and its implementation including people, processes and technologies shall be reviewed independently at planned intervals, or when significant changes occur.	Y	Y	☐	☐	☑	
	5.36	Compliance with policies, rules and standards for information security	Compliance with the organization's information security policy, top- ic-specific policies, rules and standards shall be regularly reviewed.	Y	Y	☐	☑	☐	
	5.37	Documented operating procedures	Operating procedures for information processing facilities shall be documented and made available to personnel who need them.	Y	Y	☑	☐	☐	
				-	-				
6. People controls	6.1	Screening	Background verification checks on all candidates to become personnel shall be carried out prior to joining the organization and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed, and the perceived	Y	Y	☐	☐	☑	
	6.2	Terms and conditions of employment	The employment contractual agreements shall state the personnel's and the organization's responsibilities for information security.	Y	Y	☑	☐	☐	
	6.3	Information security awareness, education and training	Personnel of the organization and relevant interested parties shall receive appropriate information security awareness, education and training and regular updates of the organization's information security policy, topic-specific policies and procedures, as relevant for their job function.	Y	Y	☐	☐	☐	
	6.4	Disciplinary process	A disciplinary process shall be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation.	Y	Y	☑	☐	☐	
	6.5	Responsibilities after termination or change of employment	Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, enforced and communicated to relevant personnel and other interested parties.	Y	Y	☐	☐	☑	
	6.6	Confidentiality or non-disclosure agreements	Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.	Y	Y	☑	☑	☑	
	6.7	Remote working	Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises.	Y	Y	☑	☐	☐	
	6.8	Information security event reporting	The organization shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.	Y	Y	☑	☐	☐	
				-	-				
7. Physical controls	7.1	Physical security perimeters	Security perimeters shall be defined and used to protect areas that contain information and other associated assets.	Y	Y	☑	☐	☑	
	7.2	Physical entry	Secure areas shall be protected by appropriate entry controls and access points.	Y	Y	☑	☐	☑	
	7.3	Securing offices, rooms and facilities	Physical security for offices, rooms and facilities shall be designed and implemented.	Y	Y	☑	☐	☑	
	7.4	Physical security monitoring	Premises shall be continuously monitored for unauthorized physical access.	Y	Y	☐	☐	☑	
	7.5	Protecting against physical and environmental threats	Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure shall be designed and implemented.	Y	Y	☑	☐	☑	
	7.6	Working in secure areas	Security measures for working in secure areas shall be designed and implemented.	Y	Y	☑	☐	☑	
	7.7	Clear desk and clear screen	Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities shall be defined and appropriately enforced.	Y	Y	☑	☐	☑	
	7.8	Equipment siting and protection	Equipment shall be sited securely and protected.	Y	Y	☑	☐	☑	
	7.9	Security of assets off-premises	Off-site assets shall be protected.	Y	Y	☑	☐	☑	
	7.10	Storage media	Storage media shall be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements.	Y	Y	☑	☐	☑	
	7.11	Supporting utilities	Information processing facilities shall be protected from power failures and other disruptions caused by failures in supporting utilities.	Y	Y	☑	☐	☑	
	7.12	Cabling security	Cables carrying power, data or supporting information services shall be protected from interception, interference or damage.	Y	Y	☑	☐	☑	
	7.13	Equipment maintenance	Equipment shall be maintained correctly to ensure availability, integrity and confidentiality of information.	Y	Y	☑	☐	☑	
	7.14	Secure disposal or re-use of equipment	Items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	Y	Y	☑	☐	☑	
				-	-				
	8.1	User end point devices	Information stored on, processed by or accessible via user end point devices shall be protected.	Y	Y	☑	☐	☐	
	8.2	Privileged access rights	The allocation and use of privileged access rights shall be restricted and managed.	Y	Y	☑	☐	☑	
	8.3	Information access restriction	Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access .	Y	Y	☑	☐	☑	
	8.4	Access to source code	Read and write access to source code, development tools and software libraries shall be appropriately managed.	Y	Y	☑	☐	☑	
	8.5	Secure authentication	Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access .	Y	Y	☑	☐	☑	
	8.6	Capacity management	The use of resources shall be monitored and adjusted in line with current and expected capacity requirements.	Y	Y	☑	☐	☑	
	8.7	Protection against malware	Protection against malware shall be implemented and supported by appropriate user awareness.	Y	Y	☑	☐	☑	
	8.8	Management of technical vulnerabilities	Information about technical vulnerabilities of information systems in use shall be obtained, the organization's exposure to such vulnerabilities shall be evaluated and appropriate measures shall be taken.	Y	Y	☑	☐	☑	
	8.9	Configuration management	Configurations, including security configurations, of hardware, software, services and networks shall be established, documented, implemented, monitored and reviewed.	Y	Y	☐	☐	☐	

8. Technological controls	8.10	Information deletion	Information stored in information systems, devices or in any other storage media shall be deleted when no longer required.	Y	Y	☐	☐	☐	
	8.11	Data masking	Data masking shall be used in accordance with the organization's topic-specific policy on access and other related topic-specific policies, and business requirements, taking applicable legislation into consideration.	Y	Y	☐	☐	☐	
	8.12	Data leakage prevention	Data leakage prevention measures shall be applied to systems, networks and any other devices that process, store or transmit sensitive information.	Y	Y	☐	☐	☑	
	8.13	Information backup	Backup copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.	Y	Y	☑	☐	☑	
	8.14	Redundancy of information processing facilities	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	Y	Y	☑	☐	☐	
	8.15	Logging	Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analysed.	Y	Y	☑	☐	☑	
	8.16	Monitoring activities	Networks, systems and applications shall be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.	Y	Y	☐	☐	☑	
	8.17	Clock synchronization	The clocks of information processing systems used by the organization shall be synchronized to approved time sources.	Y	Y	☑	☐	☑	
	8.18	Use of privileged utility programs	The use of utility programs that can be capable of overriding system and applications shall be restricted and tightly led.	Y	Y	☑	☐	☑	
	8.19	Installation of software on operational systems	Procedures and measures shall be implemented to securely manage software installation on operational systems.	Y	Y	☑	☐	☐	
	8.20	Networks security	Networks and network devices shall be secured, managed and led to protect information in systems and applications.	Y	Y	☑	☐	☑	
	8.21	Security of network services	Security mechanisms, service levels and service requirements of network services shall be identified, implemented and monitored.	Y	Y	☑	☐	☑	
	8.22	Segregation of networks	Groups of information services, users and information systems shall be segregated in the organization's networks.	Y	Y	☑	☐	☑	
	8.23	Web filtering	Access to external websites shall be managed to reduce exposure to malicious content.	Y	Y	☐	☐	☐	
	8.24	Use of cryptography	Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented.	Y	Y	☐	☐	☑	
	8.25	Secure development life cycle	Rules for the secure development of software and systems shall be established and applied.	Y	Y	☑	☐	☐	
	8.26	Application security requirements	Information security requirements shall be identified, specified and approved when developing or acquiring applications.	Y	Y	☑	☐	☐	
	8.27	Secure system architecture and engineering principles	Principles for engineering secure systems shall be established, documented, maintained and applied to any information system development activities.	Y	Y	☑	☐	☐	
	8.28	Secure coding	Secure coding principles shall be applied to software development.	Y	Y	☐	☐	☐	
	8.29	Security testing in development and acceptance	Security testing processes shall be defined and implemented in the development life cycle.	Y	Y	☑	☐	☐	
	8.30	Outsourced development	The organization shall direct, monitor and review the activities related to outsourced system development.	Y	Y	☑	☐	☐	
	8.31	Separation of development, test and production environments	Development, testing and production environments shall be separated and secured.	Y	Y	☑	☐	☐	
	8.32	Change management	Changes to information processing facilities and information systems shall be subject to change management procedures.	Y	Y	☑	☐	☐	
	8.33	Test information	Test information shall be appropriately selected, protected and managed.	Y	Y	☑	☐	☐	
	8.34	Protection of information systems during audit testing	Audit tests and other assurance activities involving assessment of operational systems shall be planned and agreed between the tester and appropriate management.	Y	Y	☑	☐	☑	

Statement of Applicability
Eurofiber Cloud Infra
Baseline Informatiebeveiliging Overheid (BIO) version 1.0.4zv - BBN2
Date 10/09/2024

	#	Title	Applicable Y/N	Implemented Y/N	Reason inclusion: Risk	Reason inclusion: Legal	Reason inclusion: Contractual	Reason for exclusion
	5.1.1.1	Er is een informatiebeveiligingsbeleid opgesteld door de organisatie. Dit beleid is vastgesteld door de leiding van de organisatie en bevat tenminste de volgende punten: a)de strategische uitgangspunten en randvoorwaarden die de organisatie hanteert voor informatiebeveiliging en in het bijzonder de inbedding in, en afstemming op het algemene beveiligingsbeleid en het informatievoorzieningsbeleid; b)de organisatie van de informatiebeveiligingsfunctie, waaronder verantwoordelijkheden, taken en bevoegdheden; c)de toewijzing van de verantwoordelijkheden voor ketens van informatiesystemen aan lijnmanagers; d)de gemeenschappelijke betrouwbaarheidseisen en normen die op de organisatie van toepassing zijn; e)de frequentie waarmee het informatiebeveiligingsbeleid wordt geëvalueerd; f)de bevordering van het beveiligingsbewustzijn.	Y	Y	☐	☐	☑	
	5.1.2.1	Het informatiebeveiligingsbeleid wordt periodiek en in aansluiting bij de (bestaande) bestuurs- en P&C-cycli en externe ontwikkelingen beoordeeld en zo nodig bijgesteld.	Y	Y	☐	☐	☑	
	6.1.1.1	De leiding van de organisatie heeft vastgelegd wat de verantwoordelijkheden en rollen zijn op het gebied van informatiebeveiliging binnen haar organisatie.	Y	Y	☐	☐	☑	
	6.1.1.2	De verantwoordelijkheden en rollen ten aanzien van informatiebeveiliging zijn gebaseerd op relevante voorschriften en wetten.	Y	Y	☐	☐	☑	
	6.1.1.3	De rol en verantwoordelijkheden van de Chief Information Security Officer (CISO) zijn in een CISO-functieprofiel vastgelegd.	Y	Y	☐	☐	☑	
	6.1.1.4	Er is een CISO aangesteld conform een vastgesteld CISO-functieprofiel.	Y	Y	☐	☐	☑	
	6.1.2.1	Er zijn maatregelen getroffen die onbedoelde of ongeautoriseerde toegang tot bedrijfsmiddelen waarnemen of voorkomen.	Y	Y	☑	☐	☑	
	6.1.3.1	Er is door de organisatie uitgewerkt wie met welke (overheids)instanties en toezichthouders contact heeft ten aanzien van informatiebeveiligingsaangelegenheden (vergunningen/incidenten/calamiteiten) en welke eisen voor deze aangelegenheden relevant zijn.	Y	Y	☑	☑	☑	
	6.1.3.2	Het contactoverzicht wordt jaarlijks geactualiseerd.	Y	Y	☐	☐	☑	
	6.2.1.1	Mobiele apparatuur is zo ingericht dat bedrijfsinformatie niet onbevoegd wordt opgeslagen ('zero footprint'). Als zero footprint (nog) niet realiseerbaar is, biedt een mobiel apparaat (zoals een laptop, tablet en smartphone) de mogelijkheid om de toegang te beschermen door middel van een toegangsbeveiligingsmechanisme en, indien vertrouwelijke gegevens worden opgeslagen, versleuteling van die gegevens. In het geval van opslag van vertrouwelijke informatie moet op deze mobiele apparatuur 'wissen op afstand' mogelijk zijn.	Y	Y	☑	☐	☐	
	6.2.1.2	Bij de inzet van mobiele apparatuur zijn minimaal de volgende aspecten geïmplementeerd: a) In bewustwordingsprogramma's komen gedragsaspecten van veilig mobiel werken aan de orde. b) Het device maakt deel uit van patchmanagement en hardening. c) Er wordt gebruik gemaakt van Mobile Device Management MDM of van Mobile Application Management (MAM)-oplossingen. d) Gebruikers tekenen een gebruikersovereenkomst voor mobiel werken, waarmee zij verklaren zich bewust te zijn van de gevaren van mobiel werken en verklaren dit veilig te zullen doen. Deze verklaring heeft betrekking op alle mobiele apparatuur die de medewerker zakelijk gebruikt. e) Periodiek wordt getoetst of de punten in lid a), b) en c) worden nageleefd.	Y	Y	☑	☐	☐	
	7.1.1.1	Elke organisatie heeft een vastgesteld screeningsbeleid. Bij indiensttreding en bij functiewijziging kan een Verklaring Omtrent het Gedrag (VOG) gevraagd	Y	Y	☑	☐	☑	
	7.1.2.1	Alle medewerkers (intern en extern) zijn bij hun aanstelling of functiewisseling gewezen op hun verantwoordelijkheden ten aanzien van informatiebeveiliging. De voor hen geldende regelingen en instructies ten aanzien van informatiebeveiliging zijn eenvoudig toegankelijk.	Y	Y	☑	☑	☑	
	7.2.1.1	Er is aansluiting bij een klokkenluidersregeling, zodat iedereen in staat is om anoniem en veilig beveiligingsissues te kunnen melden.	Y	Y	☐	☑	☑	
	7.2.2.1	Alle medewerkers hebben de verantwoordelijkheid bedrijfsinformatie te beschermen. Iedereen kent de regels en verplichtingen met betrekking tot informatiebeveiliging en daar waar relevant de speciale eisen voor gerubriceerde omgevingen	Y	Y	☑	☑	☑	
	7.2.2.2	Alle medewerkers en contractanten die gebruikmaken van de informatiesystemen- en diensten hebben binnen drie maanden na indiensttreding een training I-bewustzijn succesvol gevolgd.	Y	Y	☑	☐	☑	
	7.2.2.3	Het management benadrukt bij aanstelling en interne overplaatsing en bijvoorbeeld in werkoverleggen of in personeelsgesprekken bij haar medewerkers en contractanten het belang van opleiding en training op het gebied van informatiebeveiliging en stimuleert hen actief deze periodiek te volgen.	Y	Y	☑	☐	☑	
	8.1.3.1	Alle medewerkers zijn aantoonbaar gewezen op de gedragsregels voor het gebruik van bedrijfsmiddelen.	Y	Y	☑	☑	☑	
	8.1.3.2	De gedragsregels voor het gebruik van bedrijfsmiddelen zijn voor extern personeel in het contract vastgelegd overeenkomstig de huisregels of gedragsregels.	Y	Y	☑	☐	☑	
	8.2.1.1	De informatie in alle informatiesystemen is door middel van een expliciete risicoafweging geclassificeerd, zodat duidelijk is welke bescherming nodig is.	Y	Y	☑	☐	☑	
	8.3.1.1	Er is een verwijderinstructie waarin is opgenomen dat van verwijderbare media die hergebruikbaar zijn en die de organisatie verlaten de onnodige inhoud onherstelbaar verwijderd is (ISO 27002 – implementatierichtlijn 8.3.1.a).	Y	Y	☑	☐	☐	
	8.3.2.1	Media die vertrouwelijke informatie bevatten, zijn opgeslagen op een plek die niet toegankelijk is voor onbevoegden.	Y	Y	☑	☐	☑	
	8.3.2.2	Verwijdering vindt plaats op een veilige manier, bijvoorbeeld door verbranding of versnippering. Verwijdering van alleen gegevens is ook mogelijk door het wissen van de gegevens voordat de media worden gebruikt voor een andere toepassing in de organisatie (ISO 27002 – implementatierichtlijn 8.3.2.a).	Y	Y	☑	☐	☑	
	8.3.2.3	Voor het wissen van alle data op het medium, wordt de data onherstelbaar verwijderd, bijvoorbeeld door minimaal twee keer te overschrijven met vaste data en één keer met random data. Er wordt gecontroleerd of alle data onherstelbaar verwijderd is.	Y	Y	☑	☐	☑	
	8.3.3.1	Er is een vastgestelde procedure voor het fysiek transport van media.	Y	Y	☑	☐	☐	
	8.3.3.2	Het gebruik van koeriers of transporteurs voor transport van op BBN2 of hoger geclassificeerde informatie voldoet aan vooraf opgestelde	Y	Y	☑	☐	☐	
	9.1.2.1	Alleen geauthenticeerde apparatuur kan toegang krijgen tot een vertrouwde zone.	Y	Y	☑	☐	☐	
	9.1.2.2	Gebruikers met eigen of ongeauthenticeerde apparatuur (Bring Your Own Device) krijgen alleen toegang tot een onvertrouwde zone.	Y	Y	☑	☐	☐	
	9.2.1.1	Er is een sluitende formele registratie- en afmeldprocedure voor het beheren van gebruikersidentificaties.	Y	Y	☑	☑	☐	
	9.2.1.2	Het gebruiken van groepsaccounts is niet toegestaan tenzij dit wordt gemotiveerd en vastgelegd door de proceseigenaar.	Y	Y	☑	☐	☐	
	9.2.2.1	Er is uitsluitend toegang verleend tot informatiesystemen na autorisatie door een bevoegde functionaris.	Y	Y	☑	☐	☐	
	9.2.2.2	Op basis van een risicoafweging is bepaald waar en op welke wijze functiescheiding wordt toegepast en welke toegangsrechten worden gegeven.	Y	Y	☑	☐	☐	
	9.2.2.3	Er is een actueel mandaatregister of er zijn functieprofielen waaruit blijkt welke personen bevoegdheden hebben voor het verlenen van toegangsrechten.	Y	Y	☐	☑	☐	
	9.2.3.1	De uitgegeven speciale bevoegdheden worden minimaal ieder kwartaal beoordeeld.	Y	Y	☑	☐	☐	
	9.2.5.1	Alle uitgegeven toegangsrechten worden minimaal eenmaal per jaar beoordeeld.	Y	Y	☑	☐	☐	
	9.2.5.2	De opvolging van bevindingen is gedocumenteerd en wordt behandeld als beveiligingsincident.	Y	Y	☑	☐	☑	
	9.2.6.3	Alle uitgegeven toegangsrechten worden minimaal eenmaal per halfjaar beoordeeld.	Y	Y	☑	☐	☐	
	9.3.1.1	Medewerkers worden ondersteund in het beheren van hun wachtwoorden door het beschikbaar stellen van een wachtwoordenkluis.	Y	Y	☑	☐	☐	
	9.4.1.1	Er zijn maatregelen genomen die het fysiek en/of logisch isoleren van informatie met specifiek belang waarborgen.	Y	Y	☑	☐	☐	
	9.4.1.2	Gebruikers kunnen alleen die informatie met specifiek belang inzien en verwerken die ze nodig hebben voor de uitoefening van hun taak.	Y	Y	☑	☐	☐	
	9.4.2.1	Als vanuit een onvertrouwde zone toegang wordt verleend naar een vertrouwde zone, gebeurt dit alleen op basis van minimaal two-factor authenticatie.	Y	Y	☑	☐	☐	
	9.4.2.2	Voor het verlenen van toegang tot het netwerk door externe leveranciers wordt vooraf een risicoafweging gemaakt. De risicoafweging bepaalt onder welke voorwaarden de leveranciers toegang krijgen. Uit een registratie blijkt hoe de rechten zijn toegekend.	Y	Y	☑	☐	☑	
	9.4.3.1	Als er geen gebruik wordt gemaakt van two-factor authenticatie, is de wachtwoordlengte minimaal 8 posities en complex van samenstelling. Vanaf een wachtwoordlengte van 20 posities vervalt de complexiteitseis. Het aantal foutieve inlogpogingen is maximaal 10. De tijdsduur dat een account wordt geblokkeerd na overschrijding van het aantal keer foutief inloggen, is vastgelegd.	Y	Y	☑	☐	☐	
	9.4.3.2	In situaties waar geen two-factor authenticatie mogelijk is, wordt minimaal halfjaarlijks het wachtwoord verniewd (zie ook 9.4.2.1.).	Y	Y	☑	☐	☐	
	9.4.3.3	De eisen aan wachtwoorden moeten geautomatiseerd worden afgedwongen.	Y	Y	☑	☐	☐	
	9.4.3.4	Initiële wachtwoorden en wachtwoorden die gereset zijn, hebben een maximale geldigheidsduur van een werkdag en moeten bij het eerste gebruik worden	Y	Y	☑	☐	☐	
	9.4.3.5	Wachtwoorden die voldoen aan het wachtwoordbeleid hebben een maximale geldigheidsduur van een jaar. Daar waar het beleid niet toepasbaar is, geldt een maximale geldigheidsduur van 6 maanden.	Y	Y	☑	☐	☐	
	9.4.4.1	Alleen bevoegd personeel heeft toegang tot systeemhulpmiddelen.	Y	Y	☑	☐	☐	
	9.4.4.2	Het gebruik van systeemhulpmiddelen wordt gelogd. De logging is een halfjaar beschikbaar voor onderzoek.	Y	Y	☑	☐	☐	
	10.1.1.1	In het cryptografiebeleid zijn minimaal de volgende onderwerpen uitgewerkt: (a) Wanneer cryptografie ingezet wordt. (b) Wie verantwoordelijk is voor de implementatie. (c) Wie verantwoordelijk is voor het sleutelbeheer. (d) Welke normen als basis dienen voor cryptografie en de wijze waarop de normen van het Forum worden toegepast. (e) De wijze waarop het beschermingsniveau vastgesteld wordt. (f) Bij communicatie tussen organisaties wordt het beleid onderling vastgesteld.	Y	Y	☑	☐	☐	
	10.1.1.2	Cryptografische toepassingen voldoen aan passende standaarden.	Y	Y	☑	☐	☐	
	10.1.2.1	Ingeval van PKI-overheid certificaten: hanteer de PKI-Overheid-eisen t.a.v. het sleutelbeheer. In overige situaties: hanteer de standaard ISO-11770 voor het beheer van cryptografische sleutels.	Y	Y	☑	☑	☐	
	10.1.2.2	Er zijn (contractuele) afspraken over reservevoorzieningen van een alternatieve leverancier als uit risicoafweging blijkt dat deze noodzakelijk zijn.	Y	Y	☑	☐	☐	

11.1.1.1	Er wordt voor het inrichten van beveiligde zones gebruik gemaakt van standaarden.	Y	Y	☑	☐	☐	
11.1.2.1	In geval van concrete beveiligingsrisico's worden waarschuwingen, conform onderlinge afspraken, verzonden aan de relevante collega's binnen het beveiligingsdomein van de overheid.	Y	Y	☑	☐	☐	
11.1.3.1	Sleutelbeheer is ingericht op basis van een sleutelplan.	Y	Y	☑	☐	☐	
11.1.4.1	De organisatie heeft gelnventariseerd welke papieren archieven en apparatuur bedrijfskritisch zijn. Tegen bedreigingen van buitenaf zijn beveiligingsmaatregelen genomen op basis van een expliciete risicoafweging.	Y	Y	☑	☑	☐	
11.1.4.2	Bij huisvesting van IT-apparatuur wordt rekening gehouden met de kans op gevolgen van rampen veroorzaakt door de natuur en menselijk handelen.	Y	Y	☑	☐	☐	
11.2.9.1	Een onbemensde werkplek is altijd vergrendeld.	Y	Y	☑	☐	☐	
11.2.9.2	Informatie wordt automatisch onloegankelijk gemaakt met bijvoorbeeld een screensaver na een inactiviteit van maximaal 15 minuten.	Y	Y	☑	☐	☐	
11.2.9.3	Sessies op remote desktops worden op het remote platform vergrendeld na een vastgestelde periode.	Y	Y	☑	☐	☐	
11.2.9.4	Het overnemen van sessies op remote werkplekken op een andere werkplek is alleen mogelijk via dezelfde beveiligde loginprocedure als waarmee de sessie is gecreëerd. Na een expliciete risicoafweging mag hiervan worden afgeweken.	Y	Y	☑	☐	☐	
11.2.9.5	Bij het gebruik van een chipcardtoken voor toegang tot systemen wordt bij het verwijderen van de token de toegangsbeveiligingslock automatisch geactiveerd.	Y	Y	☑	☐	☐	
12.1.2.1	In de procedure voor wijzigingenbeheer is minimaal aandacht besteed aan: (a) het administreren van wijzigingen; (b) risicoafweging van mogelijke gevolgen van de wijzigingen; (c) goedkeuringsprocedure voor wijzigingen.	Y	Y	☑	☐	☑	
12.1.4.1	In de productieomgeving wordt niet getest. Alleen met voorafgaande goedkeuring door de proceseigenaar en schriftelijke vastlegging hiervan, kan hiervan worden afgeweken.	Y	Y	☑	☐	☐	
12.1.4.2	Wijzigingen in de productieomgeving worden altijd getest voordat zij in productie gebracht worden. Alleen met voorafgaande goedkeuring door de proceseigenaar en schriftelijke vastlegging hiervan, kan hiervan worden afgeweken.	Y	Y	☑	☐	☐	
12.2.1.1	Het downloaden van bestanden is beheerst en beperkt op basis van risico en need-of-use.	Y	Y	☑	☐	☐	
12.2.1.2	Gebruikers zijn voorgelicht over de risico's ten aanzien van surfgedrag en het klikken op onbekende links.	Y	Y	☑	☐	☐	
12.2.1.3	De gebruikte antimalwaresoftware en bijbehorende herstelsoftware is actueel en wordt ondersteund door periodieke updates.	Y	Y	☑	☐	☐	
12.2.1.4	Computers en media worden als voorzorgsmaatregel routinematig gescand. De uitgevoerde scan behoort te omvatten: (a) Alle bestanden die via netwerken of via elke vorm van opslagmedium zijn ontvangen, vóór gebruik op malware scannen. (b) Bijlagen en downloads vóór gebruik.	Y	Y	☑	☐	☐	
12.2.1.5	De malware scan wordt op verschillende omgevingen uitgevoerd, bijv. op mailservers, desktopcomputers en bij de toegang tot het netwerk van de organisatie.	Y	Y	☑	☐	☐	
12.3.1.1	Er is een back-up beleid waarin de eisen voor het bewaren en beschermen zijn gedefinieerd en vastgesteld.	Y	Y	☑	☐	☐	
12.3.1.2	Op basis van een expliciete risicoafweging is bepaald wat het maximaal toegestane dataverlies is en wat de maximale hersteltijd is na een incident.	Y	Y	☑	☐	☐	
12.3.1.3	2 In het back-upbeleid staan minimaal de volgende eisen: (a) Dataverlies bedraagt maximaal 28 uur. (b) Hersteltijd in geval van incidenten is maximaal 16 werkuren (twee dagen van 8 uur) in 85% van de gevallen.	Y	Y	☑	☐	☑	
12.3.1.4	Het back-up proces voorziet in opslag van de back-up op een locatie, waarbij een incident op de ene locatie niet kan leiden tot schade op de andere.	Y	Y	☑	☐	☑	
12.3.1.5	De restore procedure wordt minimaal jaarlijks getest of na een grote wijziging om de goede werking te waarborgen als deze in noodgevallen uitgevoerd moet	Y	Y	☑	☐	☐	
12.4.1.1	Een logregel bevat minimaal: (a) de gebeurtenis; (b) de benodigde informatie die nodig is om het incident met hoge mate van zekerheid te herleiden tot een natuurlijk persoon; (c) het gebruikte apparaat; (d) het resultaat van de handeling; (e) een datum en tijdstip van de gebeurtenis.	Y	Y	☑	☐	☐	
12.4.1.2	Een logregel bevat in geen geval gegevens die tot het doorbreken van de beveiliging kunnen leiden.	Y	Y	☑	☐	☐	
12.4.1.3	De informatieverwerkende omgeving wordt gemonitord door een SIEM en/of SOC middels detectie-voorzieningen, zoals het Nationaal Detectie Netwerk (alleen voor rijksoverheidsorganisaties). Deze worden ingezet op basis van een risico-inschatting, mede aan de hand van de aard van de te beschermen gegevens en informatiesystemen, zodat aanvallen kunnen worden gedetecteerd.	Y	Y	☑	☐	☐	
12.4.1.4	Bij ontdekte nieuwe dreigingen (aanvallen) via 12.4.1.3 worden deze binnen geldende juridische kaders verplicht gedeeld binnen de overheid, waaronder met het NCSC (alleen voor rijksoverheidsorganisaties) of via de sectorale CERT (voor andere overheidsorganisaties), middels (bij voorkeur geautomatiseerde) threat intelligence sharing mechanismen.	Y	Y	☑	☐	☐	
12.4.1.5	De SIEM en/of SOC hebben heldere regels over wanneer een incident moet worden gerapporteerd aan het verantwoordelijk management.	Y	Y	☑	☐	☑	
12.4.2.1	Er is een overzicht van logbestanden die worden gegenereerd.	Y	Y	☑	☐	☐	
12.4.2.2	Ten behoeve van de loganalyse is op basis van een expliciete risicoafweging de bewaarperiode van de logging bepaald. Binnen deze periode is de beschikbaarheid van de loginformatie gewaarborgd.	Y	Y	☑	☐	☐	
12.4.2.3	Er is een (onafhankelijke) interne audit procedure die minimaal half jaarlijks toetst op het ongewijzigd bestaan van logbestanden.	Y	Y	☑	☐	☐	
12.4.2.4	Oneigenlijk wijzigen, verwijderen of pogingen daartoe van loggegevens worden zo snel mogelijk gemeld als beveiligingsincident via de procedure voor informatiebeveiligingsincidenten conform hoofdstuk 16.	Y	Y	☑	☐	☐	
12.6.1.1	Als de kans op misbruik en de verwachte schade beide hoog zijn (NCSC classificatie kwetsbaarheidswaarschuwingen), worden patches zo snel mogelijk, maar uiterlijk binnen een week geïnstalleerd. In de tussentijd worden op basis van een expliciete risicoafweging mitigerende maatregelen getroffen.	Y	Y	☑	☐	☐	
12.6.2.1	Gebruikers kunnen op hun werkomgeving niets zelf installeren, anders dan via de ICT-leverancier wordt aangeboden of wordt toegestaan (whitelist).	Y	Y	☑	☐	☐	
13.1.2.1	Het dataverkeer dat de organisatie binnenkomt of uitgaat wordt bewaakt / geanalyseerd op kwaadaardige elementen middels detectievoorzieningen (zoals beschreven in de richtlijn voor implementatie van detectieoplossingen), zoals het Nationaal Detectie Netwerk (alleen voor rijksoverheidsorganisaties) of GDI, die worden ingezet op basis van een risico-inschatting, mede aan de hand van de aard van de te beschermen gegevens en informatiesystemen.	Y	Y	☑	☐	☐	
13.1.2.2	Bij ontdekte nieuwe dreigingen vanuit 13.1.2.1 worden deze, rekening houdend met de geldende juridische kaders, verplicht gedeeld binnen de overheid, waaronder met het NCSC (alleen voor rijksoverheidsorganisaties) of de sectorale CERT, bij voorkeur door geautomatiseerde mechanismen (threat intelligence	Y	Y	☑	☐	☐	
13.1.2.3	Bij draadloze verbindingen zoals wifi en bij bedrade verbindingen buiten het gecontroleerd gebied wordt gebruik gemaakt van encryptiemiddelen waarvoor het NBV een positief inzetadvies heeft afgegeven.	Y	Y	☑	☐	☐	
13.1.2.4	In koppelpunten met externe of onvertrouwde zones zijn maatregelen getroffen om mogelijke aanvallen die de beschikbaarheid van de informatievoorziening negatief beïnvloeden (bijvoorbeeld DDoS-aanvallen, Distributed Denial of Service attacks) te signaleren en hierop te reageren.	Y	Y	☑	☐	☑	
13.1.3.1	Alle gescheiden groepen hebben een gedefinieerd beveiligingsniveau.	Y	Y	☑	☐	☐	
13.2.3.1	Voor de beveiliging van elektronische (e-mail)berichten gelden de vastgestelde open standaarden tegen phishing en afluisteren op de 'pas toe of leg uit'-lijst van het Forum. Voor beveiliging van websiteverkeer gelden de open standaarden tegen afluisteren op de 'pas toe of leg uit'-lijst van het Forum.	Y	Y	☑	☐	☐	
13.2.3.2	Voor veilige berichtenuitwisseling met basisregistraties wordt, conform de 'pas toe of leg uit'-lijst van het Forum, gebruik gemaakt van de actuele versie van Digikoppeling.	Y	Y	☑	☐	☐	
13.2.3.3	Maak gebruik van PKIoverheid-certificaten bij web- en mailverkeer van gevoelige gegevens. Gevoelige gegevens zijn onder andere digitale documenten binnen de overheid waar gebruikers rechten aan kunnen ontlenen.	Y	Y	☑	☐	☐	
13.2.3.4	Om zekerheid te bieden over de integriteit van het elektronische bericht, wordt voor elektronische handtekeningen gebruik gemaakt van de AdES Baseline Profile standaard.	Y	Y	☑	☐	☐	
14.1.1.1	Bij nieuwe informatiesystemen en bij wijzigingen op bestaande informatiesystemen moet een expliciete risicoafweging worden uitgevoerd ten behoeve van het vaststellen van de beveiligingseisen, uitgaande van de BIO.	Y	Y	☑	☐	☐	
14.2.1.1	De gangbare principes rondom 'security by design' zijn uitgangspunt voor de ontwikkeling van software en systemen.	Y	Y	☑	☐	☐	
14.2.2.1	Wijzigingsbeheer vindt plaats op basis van een algemeen geaccepteerd beheerframework.	Y	Y	☑	☐	☐	
14.2.5.1	Zie overheidsmaatregel 14.2.1.1	Y	Y	☑	☐	☐	
14.2.6.1	Systeemontwikkelomgevingen worden passend beveiligd op basis van een expliciete risicoafweging.	Y	Y	☑	☐	☐	
14.2.7.1	Een voorwaarde voor uitbestedingstrajecten is een expliciete risicoafweging. De noodzakelijke beveiligingsmaatregelen die daaruit volgen worden aan de leverancier opgelegd.	Y	Y	☑	☐	☑	
14.2.9.1	Voor acceptatietesten van systemen worden gestructureerde testmethodieken gebruikt. De testen worden bij voorkeur geautomatiseerd uitgevoerd.	Y	Y	☑	☐	☑	
14.2.9.2	Van de resultaten van de testen wordt verslag gemaakt.	Y	Y	☑	☐	☑	
15.1.1.1	Bij offerteaanvragen waar informatie(voorziening) een rol speelt, worden eisen ten aanzien van informatiebeveiliging (beschikbaarheid, integriteit en vertrouwelijkheid) benoemd. Deze eisen zijn gebaseerd op een expliciete risicoafweging.	Y	Y	☑	☐	☑	
15.1.1.2	Op basis van een expliciete risicoafweging worden de beheersmaatregelen met betrekking tot leverancierstoegang tot bedrijfsinformatie vastgesteld.	Y	Y	☑	☑	☑	
15.1.1.3	Met alle leveranciers die als verwerker voor of namens de organisatie persoonsgegevens verwerken, worden verwerkersovereenkomsten gesloten waarin alle wettelijk vereiste afspraken zijn vastgesteld.	Y	Y	☑	☑	☑	
15.1.2.1	De beveiligingseisen uit de offerteaanvraag worden expliciet opgenomen in de (inkoop)contracten waar informatie een rol speelt.	Y	Y	☑	☑	☑	
15.1.2.2	In de inkoopcontracten worden expliciet prestatie-indicatoren en de bijbehorende verantwoordingsrapportages opgenomen.	Y	Y	☑	☑	☑	
15.1.2.3	In situaties waarin contractvoorwaarden worden opgelegd door leveranciers, is voorafgaand aan het tekenen van het contract met een risicoafweging helder gemaakt wat de consequenties hiervan zijn voor de organisatie. Expliciet is gemaakt welke consequenties geaccepteerd worden en welke gemitigeerd moeten zijn bij het aangaan van de overeenkomst.	Y	Y	☑	☑	☑	
15.1.2.4	Ter waarborging van vertrouwelijkheid of geheimhouding worden bij IT-inkopen standaardvoorwaarden voor inkoop gehanteerd.	Y	Y	☑	☑	☑	
15.1.2.5	Voordat een contract wordt afgesloten, wordt in een risicoafweging bepaald of de afhankelijkheid van een leverancier beheersbaar is. Een vast onderdeel van het contract is een expliciete uitwerking van de exit-strategie.	Y	Y	☑	☑	☑	
15.1.2.6	In inkoopcontracten wordt expliciet de mogelijkheid van een externe audit opgenomen waarmee de betrouwbaarheid van de geleverde dienst kan worden getoetst. Een audit is niet nodig als de contractant door middel van certificering aantoont dat de gewenste betrouwbaarheid van de dienst is gebo rgd.	Y	Y	☑	☑	☑	
15.1.3.1	Leveranciers moeten hun keten van toeleveranciers bekendmaken en transparant zijn over de maatregelen die zij genomen hebben om de aan hen opgelegde eisen ook door te vertalen naar hun toeleveranciers.	Y	Y	☑	☑	☑	
15.2.1.1	Jaarlijks wordt de prestatie van leveranciers op het gebied van informatiebeveiliging beoordeeld op vooraf vastgestelde prestatie-indicatoren, zoals in het contract opgenomen is.	Y	Y	☑	☐	☑	
16.1.2.1	Er is een meldloket waar beveiligingsincidenten kunnen worden gemeld.	Y	Y	☑	☐	☑	
16.1.2.2	Er is een meldprocedure waarin de taken en verantwoordelijkheden van het meldloket staan beschreven.	Y	Y	☑	☐	☑	
16.1.2.3	Alle medewerkers en contractanten hebben aantoonbaar kennis genomen van de meldingsprocedure van incidenten.	Y	Y	☑	☑	☑	
16.1.2.4	Incidenten worden zo snel mogelijk, maar in ieder geval binnen 24 uur na bekendwording, intern gemeld.	Y	Y	☑	☐	☑	
16.1.2.5	De proceseigenaar is verantwoordelijk voor het oplossen van beveiligingsincidenten.	Y	Y	☑	☐	☐	
16.1.2.6	De opvolging van incidenten wordt maandelijks gerapporteerd aan de verantwoordelijke.	Y	Y	☑	☐	☐	
16.1.2.7	Informatie afkomstig uit de Coordinated Vulnerability Disclosure (CVD) procedure is onderdeel van de incidentrapportage .	Y	Y	☑	☐	☐	
16.1.3.1	Een Coordinated Vulnerability Disclosure (CVD) procedure is gepubliceerd en ingericht.	Y	Y	☑	☐	☐	
16.1.4.1	Informatiebeveiligingsincidenten die hebben geleid tot een vermoedelijk of mogelijk opzettelijke inbreuk op de beschikbaarheid, vertrouwelijkheid of integriteit van informatieverwerkende systemen, behoren zo snel mogelijk (binnen 72 uur) al dan niet geautomatiseerd te worden gemeld aan het NCSC (alleen voor rijksoverheidsorganisaties) of de sectorale CERT.	Y	Y	☑	☐	☐	
16.1.6.1	Beveiligingsincidenten worden geanalyseerd met als doel te leren en toekomstige beveiligingsincidenten te voorkomen.	Y	Y	☑	☐	☐	
16.1.6.2	De analyses van de beveiligingsincidenten worden gedeeld met de relevante partners om herhaling en toekomstige incidenten te voorkomen.	Y	Y	☑	☐	☑	
16.1.7.1	In geval van een (vermoed) informatiebeveiligingsincident is de bewaartermijn van de gelogde incidentinformatie minimaal drie jaar.	Y	Y	☐	☑	☐	
17.1.3.1	Continuïteitsplannen worden jaarlijks getest op geldigheid en bruikbaarheid.	Y	Y	☑	☐	☑	
17.1.3.2	Door het uitvoeren van een expliciete risicoafweging worden de bedrijfskritische procesonderdelen met hun bijbehorende betrouwbaarheidseisen	Y	Y	☑	☐	☐	
17.1.3.3	De dienstverlening van de bedrijfskritische onderdelen wordt bij calamiteiten uiterlijk binnen een week hersteld.	Y	Y	☑	☐	☑	
18.1.3.1	De proceseigenaar heeft per soort informatie inzichtelijk gemaakt wat de bewaartermijn is.	Y	Y	☑	☑	☐	
18.1.4.1	In overeenstemming met de AVG heeft iedere organisatie een Functionaris Gegevensbescherming (FG) met voldoende mandaat om zijn/haar functie uit te	Y	Y	☐	☑	☐	
18.1.4.2	Organisaties controleren regelmatig de naleving van de privacyregels en informatieverwerking en -procedures binnen hun verantwoordelijkheidsgebied aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.	Y	Y	☐	☑	☐	
18.1.5.1	Cryptografische beheersmaatregelen moeten expliciet aansluiten bij de standaarden op de 'pas toe of leg uit'-lijst van het Forum.	Y	Y	☑	☐	☐	
18.2.1.1	Er is een information security management system (ISMS) waarmee aantoonbaar de gehele Plan-Do-Check-Act cyclus op gestructureerde wijze wordt afgedekt.	Y	Y	☑	☐	☐	
18.2.1.2	Er is een vastgesteld auditplan waarin jaarlijks keuzes worden gemaakt voor welke systemen welk soort beveiligingsaudits worden uitgevoerd.	Y	Y	☑	☐	☐	
18.2.2.1	In de P&C-cyclus wordt gerapporteerd over informatiebeveiliging, resulterend in een jaarlijks af te geven In Control Verklaring (ICV) over de informatiebeveiliging. Indien voldoende herkenbaar kan de ICV voor informatiebeveiliging onderdeel zijn van de reguliere, generieke verantwoording.	Y	Y	☑	☐	☐	
18.2.3.1	Informatiesystemen worden jaarlijks gecontroleerd op technische naleving van beveiligingsnormen en risico's ten aanzien van de feitelijke veiligheid. Dit kan bijvoorbeeld door (geautomatiseerde) kwetsbaarheidsanalyses of penetratietesten.	Y	Y	☑	☐	☐	