Statement of Applicability
Eurofiber Cloud Infra
ISO27001:2022
Version **1.4**
Date **30-6-2025**

	#	Title	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	Y	Y	☐	☐	☑	
	5.2	Information security roles and responsibilities	Y	Y	☐	☐	☑	
	5.3	Segregation of duties	Y	Y	☐	☐	☑	
	5.4	Management responsibilities	Y	Y	☑	☐	☑	
	5.5	Contact with authorities	Y	Y	☐	☑	☑	
	5.6	Contact with special interest groups	Y	Y	☐	☑	☐	
	5.7	Threat intelligence	Y	Y	☐	☑	☐	
	5.8	Information security in project management	Y	Y	☑	☐	☐	
	5.9	Inventory of information and other associated assets	Y	Y	☑	☐	☑	
	5.10	Acceptable use of information and other associated assets	Y	Y	☑	☐	☑	
	5.11	Return of assets	Y	Y	☑	☐	☑	
	5.12	Classification of information	Y	Y	☑	☐	☑	
	5.13	Labelling of information	Y	Y	☑	☐	☐	
	5.14	Information transfer	Y	Y	☑	☐	☑	
	5.15	Access control	Y	Y	☑	☐	☑	
	5.16	Identity management	Y	Y	☑	☐	☑	
	5.17	Authentication information	Y	Y	☑	☐	☑	
	5.18	Access rights	Y	Y	☑	☐	☑	
	5.19	Information security in supplier relationships	Y	Y	☑	☐	☑	
	5.20	Addressing information security within supplier agreements	Y	Y	☑	☐	☑	
	5.21	Managing information security in the information and communication technology (ICT) supply chain	Y	Y	☑	☐	☐	
	5.22	Monitoring, review and change management of supplier services	Y	Y	☑	☐	☐	
	5.23	Information security for use of cloud services	Y	Y	☑	☑	☑	
	5.24	Information security incident management planning and preparation	Y	Y	☑	☑	☐	
	5.25	Assessment and decision on information security events	Y	Y	☑	☐	☑	
	5.26	Response to information security incidents	Y	Y	☑	☐	☐	
	5.27	Learning from information security incidents	Y	Y	☑	☐	☐	
	5.28	Collection of evidence	Y	Y	☑	☑	☐	
	5.29	Information security during disruption	Y	Y	☑	☐	☑	
	5.30	ICT readiness for business continuity	Y	Y	☑	☑	☑	
	5.31	Legal, statutory, regulatory and contractual requirements	Y	Y	☑	☑	☑	
	5.32	Intellectual property rights	Y	Y	☐	☑	☑	
	5.33	Protection of records	Y	Y	☐	☑	☑	
	5.34	Privacy and protection of personal identifiable information (PII)	Y	Y	☑	☑	☑	
	5.35	Independent review of information security	Y	Y	☐	☑	☑	
	5.36	Compliance with policies, rules and standards for information security	Y	Y	☐	☑	☐	
	5.37	Documented operating procedures	Y	Y	☑	☐	☐	
6. People controls	6.1	Screening	Y	Y	☑	☐	☑	
	6.2	Terms and conditions of employment	Y	Y	☑	☐	☐	
	6.3	Information security awareness, education and training	Y	Y	☑	☐	☑	
	6.4	Disciplinary process	Y	Y	☑	☐	☐	
	6.5	Responsibilities after termination or change of employment	Y	Y	☑	☐	☑	
	6.6	Confidentiality or non-disclosure agreements	Y	Y	☑	☑	☑	
	6.7	Remote working	Y	Y	☑	☐	☐	
	6.8	Information security event reporting	Y	Y	☑	☐	☐	

7. Physical controls	7.1	Physical security perimeters	Y	Y	☑	☐	☑	
	7.2	Physical entry	Y	Y	☑	☐	☑	
	7.3	Securing offices, rooms and facilities	Y	Y	☑	☐	☑	
	7.4	Physical security monitoring	Y	Y	☑	☑	☑	
	7.5	Protecting against physical and environmental threats	Y	Y	☑	☐	☑	
	7.6	Working in secure areas	Y	Y	☑	☐	☑	
	7.7	Clear desk and clear screen	Y	Y	☑	☐	☑	
	7.8	Equipment siting and protection	Y	Y	☑	☐	☑	
	7.9	Security of assets off-premises	Y	Y	☑	☐	☑	
	7.10	Storage media	Y	Y	☑	☐	☑	
	7.11	Supporting utilities	Y	Y	☑	☐	☑	
	7.12	Cabling security	Y	Y	☑	☐	☑	
	7.13	Equipment maintenance	Y	Y	☑	☐	☑	
	7.14	Secure disposal or re-use of equipment	Y	Y	☑	☐	☑	
8. Technological controls	8.1	User end point devices	Y	Y	☑	☐	☐	
	8.2	Privileged access rights	Y	Y	☑	☐	☑	
	8.3	Information access restriction	Y	Y	☑	☐	☑	
	8.4	Access to source code	Y	Y	☑	☐	☑	
	8.5	Secure authentication	Y	Y	☑	☐	☑	
	8.6	Capacity management	Y	Y	☑	☐	☑	
	8.7	Protection against malware	Y	Y	☑	☐	☑	
	8.8	Management of technical vulnerabilities	Y	Y	☑	☐	☑	
	8.9	Configuration management	Y	Y	☑	☐	☑	
	8.10	Information deletion	Y	Y	☑	☑	☑	
	8.11	Data masking	Y	Y	☑	☑	☑	
	8.12	Data leakage prevention	Y	Y	☑	☑	☑	
	8.13	Information backup	Y	Y	☑	☐	☑	
	8.14	Redundancy of information processing facilities	Y	Y	☑	☐	☐	
	8.15	Logging	Y	Y	☑	☐	☑	
	8.16	Monitoring activities	Y	Y	☑	☐	☑	
	8.17	Clock synchronization	Y	Y	☑	☐	☑	
	8.18	Use of privileged utility programs	Y	Y	☑	☐	☑	
	8.19	Installation of software on operational systems	Y	Y	☑	☐	☐	
	8.20	Networks security	Y	Y	☑	☐	☑	
	8.21	Security of network services	Y	Y	☑	☐	☑	
	8.22	Segregation of networks	Y	Y	☑	☐	☑	
	8.23	Web filtering	Y	Y	☑	☐	☐	
	8.24	Use of cryptography	Y	Y	☐	☐	☑	
	8.25	Secure development life cycle	Y	Y	☑	☐	☐	
	8.26	Application security requirements	Y	Y	☑	☐	☐	
	8.27	Secure system architecture and engineering principles	Y	Y	☑	☐	☐	
	8.28	Secure coding	Y	Y	☑	☐	☑	
	8.29	Security testing in development and acceptance	Y	Y	☑	☐	☐	
	8.30	Outsourced development	Y	Y	☑	☐	☑	
	8.31	Separation of development, test and production environments	Y	Y	☑	☐	☐	
	8.32	Change management	Y	Y	☑	☐	☐	
	8.33	Test information	Y	Y	☑	☐	☐	
	8.34	Protection of information systems during audit testing	Y	Y	☑	☐	☑	

Statement of Applicability
Eurofiber Cloud Infra
Baseline Informatiebeveiliging Overheid (BIO) 2 version 1.2
Date 30-6-2025

	#	Title	Applicable Y/N	Implemented Y/N	Reason inclusion: Risk	Reason inclusion: Legal	Reason inclusion: Contractual	Reason for exclusion
	5.01.01	Verantwoordelijkheden en samenhang voor informatiebeveiliging, de beveiliging van operationele technologie (OT) en de verantwoordelijkheden met betrekking tot de continuïteit van de taakuitvoering van de organisatie, bedrijfscontinuïteitsmanagement (BCM) zijn beschreven en vastgesteld. De toewijzing van verantwoordelijkheid voor ketens van informatiesystemen aan lijnmanagers. De organisatie heeft een informatiebeveiligingsbeleid opgesteld en vastgesteld door de leiding van de organisatie. Dit beleid bevat ten minste de volgende punten: 1. 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. 2. De organisatie van de informatiebeveiligingsfunctie, waaronder verantwoordelijkheden, taken en bevoegdheden. 3. De toewijzing van de verantwoordelijkheden en samenhang van informatiebeveiliging voor ketens van informatiesystemen, de beveiliging van OT, privacybescherming en de verantwoordelijkheden met betrekking tot de continuïteit van de taakuitvoering van organisatie (BCM) aan lijnmanagers. 4. De gemeenschappelijke betrouwbaarheidseisen en normen die op de organisatie van toepassing zijn. 5. De frequentie waarmee het informatiebeveiligingsbeleid wordt geëvalueerd. 6. De bevordering van het beveiligingsbewustzijn.	Y	Y	☑	☐	☑	
	5.01.02	Het informatiebeveiligingsbeleid wordt minimaal jaarlijks en in aansluiting bij de (bestaande) bestuurs- en Planning & Control (P&C)-cycli en externe ontwikkelingen beoordeeld en zo nodig bijgesteld.	Y	Y	☑	☐	☑	
	5.02.01	De leiding van de organisatie heeft vastgelegd wat de verantwoordelijkheden en rollen zijn voor informatiebeveiliging (ook voor OT, BCM en privacybescherming) binnen haar organisatie. Hierbij is specifieke aandacht voor de verantwoordelijkheden en rollen voor het adequaat afhandelen van incidenten. Lijnmanagers en proceseigenaren die verantwoordelijk zijn voor bedrijfsmiddelen zijn ook verantwoordelijk voor de behandeling van risico's die op die bedrijfsmiddelen van toepassing zijn.	Y	Y	☑	☐	☑	
	5.02.02	Er is een CISO aangesteld die bevoegd is om onafhankelijk en zelfstandig te adviseren en te rapporteren aan het bestuur en of het controlerend orgaan over informatiebeveiliging.	Y	Y	☑	☐	☑	
	5.03.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO	Y	Y	☐	☐	☑	
	5.04.01	Bestuur en werknemers moeten regelmatig, scholing volgen om cyberbeveiligingsrisico's te herkennen en te voorkomen en te weten wat men moet doen als er een informatiebeveiligingsincident is. Daarbij tonen bestuurders aan dat zij voldoende kennis en vaardigheden hebben om de gevolgen van informatiebeveiligingsrisico's te beoordelen op de diensten en/of producten die de organisatie levert.	Y	Y	☑	☑	☑	
	5.04.02	De gedragsregels voor het gebruik van bedrijfsmiddelen zijn voor extern personeel en vrijwilligers in het contract vastgelegd volgens de huisregels of interne gedragsregels.	Y	Y	☑	☐	☑	
	5.04.03	Alle medewerkers zijn aantoonbaar gewezen op de gedragsregels voor het gebruik van bedrijfsmiddelen.	Y	Y	☑	☑	☑	
	5.05.01	De organisatie heeft uitgewerkt welke functionarissen met welke (overheids)instanties en toezichthouders formele contacten hebben over informatiebeveiliging. Dit overzicht wordt ten minste jaarlijks geactualiseerd.	Y	Y	☑	☐	☑	
	5.06.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO	Y	Y	☐	☑	☐	
	5.07.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO	Y	Y	☐	☑	☐	
	5.08.01	Bij nieuwe informatiesystemen en bij significante wijzigingen op bestaande informatiesystemen moet een expliciete risicoafweging op basis van de door de organisatie vastgestelde risicomanagementmethodiek worden uitgevoerd, om risico's te identificeren en in voldoende mate te beheersen en ook voor het vaststellen van de beveiligingseisen.	Y	Y	☑	☐	☐	
	5.09.01	Er is een inventaris van bedrijfsmiddelen die van belang zijn voor informatieverwerking, met inbegrip van OT. De inventaris omvat alle eigenschappen die nodig zijn voor het beheer en onderhoud. In de inventaris zijn ook opgenomen: bedrijfsmiddelen op afstand, cloud-omgevingen en bedrijfsmiddelen die regelmatig zijn verbonden met de netwerkinfrastructuur maar niet onder controle van de organisatie staan. De volledigheid en actualiteit van de inventaris wordt periodiek gecontroleerd met tussenpozen die passend zijn voor de frequentie waarmee wijzigingen optreden.	Y	Y	☑	☐	☑	
	5.10.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO	Y	Y	☑	☑	☑	
	5.11.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO	Y	Y	☑	☐	☑	
	5.12.01	Informatie in alle informatiesystemen is door middel van een expliciete risicoafweging geclassificeerd. Hierbij wordt gebruik gemaakt van een vastgestelde impactclassificatiemethodiek die onderdeel is van de vastgestelde risicomanagementmethodiek.	Y	Y	☑	☐	☑	
	5.13.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO	Y	Y	☑	☐	☐	

5.14.01	Internetfacing-informatiesystemen en e-mail-berichtenverkeer moeten blijvend voldoen aan de verplichte standaarden, zie hiervoor de website van het Forum Standaardisatie. Hierop wordt gestuurd met de metingen van internet.nl. Daarbij dienen alle onderdelen te worden ingesteld zodat een optimale beveiliging wordt bereikt zonder afbreuk te doen aan de functionaliteit van de geboden dienst.	Y	Y	☑	☐	☐	
5.14.02	Maak bij openbaar webverkeer van gevoelige gegevens gebruik van ten minste publiek vertrouwde Organization Validated (OV)-certificaten. Maak bij intern webverkeer voor gevoelige gegevens gebruik van ten minste publieke vertrouwde OV-certificaten of private PKIo-certificaten. Hogere eisen aan certificaten kunnen voortvloeien uit een risicoanalyse, aansluitvoorwaarden of wetgeving.	Y	Y	☑	☐	☐	
5.14.03	Geavanceerde en/of gekwalificeerde elektronische handtekeningen moeten voldoen aan de Advanced Electronic Signatures (AdES Baseline Profiles), zoals opgenomen in de Lijst open standaarden van Forum Standaardisatie.	Y	Y	☑	☐	☐	
5.14.04	Van alle internetfacing-informatiesystemen, webapplicaties, IP-adressen en API's is een actuele registratie.	Y	Y	☑	☐	☑	
5.14.05	Publiek toegankelijke websites worden bekend gemaakt via Register Internetdomeinen Overheid. Deze informatie wordt ten minste iedere zes maanden geactualiseerd.	Y	Y	☐	☑	☐	
5.15.01	Toegang tot een vertrouwde zone is toegestaan in twee situaties: 1. vanaf geauthentiseerde apparatuur of; 2. vanuit programmatuur die draait binnen een veilige schil.	Y	Y	☑	☐	☐	
5.16.01	Er is een sluitende formele registratie- en afmeldprocedure voor het beheren van gebruikersidentificaties.	Y	Y	☑	☐	☐	
5.16.02	Het gebruiken van groepsaccounts is niet toegestaan, tenzij de proceseigenaar dit motiveert, vastlegt en afstemt met de CISO.	Y	Y	☑	☐	☐	
5.17.01	Pas multi-factorauthenticatie (MFA) ten minste toe voor het primaire aanloggen op de digitale werkomgeving, bij accounts voor via het internet bereikbare voorzieningen en accounts die beheerrechten hebben en in andere situaties waar uit de risicoanalyse blijkt dat dit een passende oplossing is. Pas MFA toe in deze twee vormen: 1. Wachtwoordloze toegang, zoals een pincode in combinatie met een hardware token of persoonlijk uniek certificaat (passkey). 2. Wachtwoordtoegang in combinatie met minimaal een tweede factor. Indien MFA niet mogelijk is voor deze accounts, neem andere mitigerende maatregelen. Betrek de CISO hierbij en laat ze goedkeuren door de proceseigenaar. Combineer waar mogelijk en veilig, MFA met federatieve authenticatievoorzieningen zoals Single Sign On en een Stepping Stone-oplossing. Voor beheer en monitoring van authenticatiegegevens: - geef authenticatie-informatie uit met formele vastgestelde procedures en pas nadat de identiteit van de gebruiker met voldoende zekerheid is vastgesteld; - definieer Use Cases voor misbruik van authenticatiegegevens, monitor deze en neem passende actie bij het optreden ervan. Deze Use Cases omvatten in ieder geval inlogpogingen van ongebruikelijke plekken en pieken in mislukte inlogpogingen.	Y	Y	☑	☐	☐	
5.17.02	De organisatie biedt aan alle medewerkers een wachtwoordmanager of vergelijkbare oplossing aan.	Y	Y	☑	☐	☐	
5.17.03	De eisen aan wachtwoorden moeten geautomatiseerd worden afgedwongen.	Y	Y	☑	☐	☐	
5.18.01	Het maken en aanpassen van accounts met bijzondere rechten wordt gemonitord. Indien deze wijzigingen ongeautoriseerd zijn, is dit een informatiebeveiligingsincident en wordt als zodanig vastgelegd en afgehandeld.	Y	Y	☑	☐	☐	
5.18.02	Alle uitgegeven toegangsrechten worden minimaal eenmaal per jaar beoordeeld. Een risicoafweging bepaalt of dit sneller moet.	Y	Y	☑	☐	☐	
5.19.01	Bij offerteaanvragen waar informatie(voorziening) een rol speelt, zijn informatiebeveiligingseisen (beschikbaarheid, integriteit en vertrouwelijkheid) onderdeel van het hele pakket aan inkoopeisen. De informatiebeveiligingseisen zijn gebaseerd op een expliciete risicoafweging.	Y	Y	☑	☐	☑	

5.20.01	De beveiligingseisen uit de offerteaanvraag worden expliciet opgenomen in de (inkoop)contracten waar de verwerking van informatie een rol speelt.	Y	Y	☑	☑	☑	
5.20.02	Sluit waar mogelijk algemene voorwaarden van leveranciers expliciet uit en neem eventueel aanvullende voorwaarden op. Als uitsluiten niet mogelijk is, beoordeel dan de risico's. Expliciet is gemaakt welke consequenties geaccepteerd worden, welke gemitigeerd moeten zijn en welke voorwaarden niet of nooit geaccepteerd mogen worden bij het aangaan van de overeenkomst.	Y	Y	☑	☑	☑	
5.20.03	In het inkoopcontract wordt opgenomen dat de leverancier aantoont dat hij aan alle gestelde eisen voldoet in opzet, bestaan en werking, op basis van onderzoeken van onafhankelijke derden. Deze onderzoeken hebben een scope die dekkend is voor de gecontracteerde dienstverlening. Hierbij is expliciet aandacht voor de toeleveringsketen en hoe de leverancier zijn leveranciersmanagement ingeregeld heeft, zie overheidsmaatregel 5.21.01. Dit toont de leverancier jaarlijks opnieuw aan.	Y	Y	☑	☑	☑	
5.20.04	De overheidsorganisatie voert zelfstandig onderzoek uit, ook ter validatie van de rapportages die de leverancier aanlevert. Om dit mogelijk te maken, wordt expliciet opgenomen dat er een mogelijkheid is voor een externe audit. Indien uit het voorgaande restrisico's volgen, beheerst de overheidsorganisatie deze door het toepassen van zijn vastgestelde risicomanagementmethodiek.	Y	Y	☑	☑	☑	
5.20.05	Onderdeel van de afspraken is dat de leverancier transparant is over kwetsbaarheden in de dienstverlening en informatiebeveiligingsincidenten waaronder datalekken. Dit stelt de overheidsorganisatie in staat om passend te reageren onder meer door te rapporteren en mitigerende maatregelen te nemen.	Y	Y	☑	☐	☑	
5.20.06	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	☑	☑	☑	
5.21.01	In het contract is opgenomen dat de leverancier verantwoordelijk is voor het borgen van de gestelde eisen bij de toeleveranciers.	Y	Y	☑	☑	☑	
5.21.02	Voorafgaand aan het afsluiten van de overeenkomst geeft de leverancier inzicht in de keten van toeleveranciers en eventuele risico's daarin. De overheidsorganisatie beoordeelt of de risico's acceptabel zijn.	Y	Y	☑	☑	☑	
5.21.03	De overheidsorganisatie borgt dat de beveiligingseisen aan de leverancier onverminderd van toepassing zijn op de keten van toeleveranciers, tenzij die eisen niet relevant zijn gezien de aard van de dienstverlening door de toeleverancier. Indien informatiebeveiligingseisen zijn uitgesloten, maakt de leverancier dat inzichtelijk, inclusief een onderbouwing.	Y	Y	☑	☑	☑	
5.21.04	Gedurende de looptijd geeft de leverancier veranderingen in de keten van toeleveranciers door, inclusief risico's daarin. Dit omvat minimaal kwetsbaarheden en informatiebeveiligingsincidenten die de dienstverlening aan de overheidsorganisatie kunnen raken.	Y	Y	☑	☐	☑	
5.22.01	Op basis van het door de leverancier aangeleverde bewijsmateriaal, zie overheidsmaatregel 5.20.03, is de proceseigenaar verantwoordelijk voor het jaarlijks beoordelen dat leverancier voldoet aan de gestelde informatiebeveiligingseisen, het vaststellen van eventuele beveiligingsrisico's, het (laten) nemen van mitigerende maatregelen en het accepteren van rest-risico's.	Y	Y	☑	☐	☑	
5.22.02	Er is een actuele registratie van leveranciers en afgesloten contracten.	Y	Y	☐	☑	☐	
5.23.01	Stel beleid op dat toeziet op het inventariseren, classificeren, selecteren, beoordelen en managen van Cloud Service Providers (CSP) en het beëindigen van dienstverlening door CSP's. Implementeer het beleid. Herzie dit beleid minimaal eens per drie jaar. Neem in de contracten op welke situaties aanleiding kunnen zijn tot ontbinding van het contract. Wanneer zich belangrijke wijzigingen bij de leverancier optreden, beoordeel de risico's daarvan en neem passende maatregelen.	Y	Y	☑	☐	☑	
5.24.01	Er is voor alle interne en externe medewerkers een toegankelijk meldloket waar informatiebeveiligingsincidenten kunnen worden gemeld en geregistreerd.	Y	Y	☑	☐	☑	
5.24.02	Er is een meldprocedure waarin de taken en verantwoordelijkheden van het meldloket staan beschreven.	Y	Y	☑	☐	☑	
5.24.03	De proceseigenaar is verantwoordelijk voor het oplossen van informatiebeveiligingsincidenten.	Y	Y	☑	☐	☐	
5.24.04	De proceseigenaar rapporteert maandelijks de opvolging van informatiebeveiligingsincidenten aan de eindverantwoordelijke voor de bedrijfsvoering.	Y	Y	☑	☐	☐	
5.24.05	In de procedure voor informatiebeveiligingsincidenten is er een koppeling gemaakt met crisisbeheersing.	Y	Y	☑	☐	☐	
5.24.06	De beveiliging van toeleveringsketens is onderdeel van de risicoanalyse voor de organisatie. In de risicoanalyse wordt rekening gehouden met: - specifieke kwetsbaarheden van elke rechtstreekse leverancier en dienstverlener; - de algemene kwaliteit van de producten; - de cyberbeveiligingspraktijken van hun leveranciers en dienstverleners, met inbegrip van hun veilige ontwikkelingsprocedures.	Y	Y	☑	☐	☑	
5.24.07	De incidentprocedure is er op ingericht om: - binnen de wettelijke termijn informatiebeveiligingsincidenten te melden bij het nationale Cyber Security Incident Responce Team (CSIRT); - meldingen van het nationale CSIRT te ontvangen, te beoordelen en op te nemen in de risicobehandeling; - betrokkenen binnen de wettelijke termijn op de hoogte te stellen van het incident.	Y	Y	☑	☐	☐	
5.25.01	Informatiebeveiligingsincidenten worden afgedaan via het incidentbeheerproces. Ze worden indien relevant gemeld bij toezichthouders volgens de bepalingen uit de betrokken wet- en regelgeving zoals de Cbw, de Archiefwet en de Algemene verordening gegevensbescherming (AVG).	Y	Y	☑	☐	☐	
5.26.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO	Y	Y	☑	☐	☐	

	5.27.01	Informatiebeveiligingsincidenten worden geanalyseerd om achterliggende oorzaken vast te stellen, verbeteringen te realiseren, om zo toekomstige incidenten te voorkomen.	Y	Y	☑	☐	☐	
	5.27.02	De analyses van informatiebeveiligingsincidenten, inclusief de achterliggende oorzaken en de verbeteringen worden breed gedeeld met relevante partners om herhaling en toekomstige incidenten te voorkomen.	Y	Y	☑	☐	☑	
	5.28.01	De bewaartermijn van een (vermoedelijk) informatiebeveiligingsincident en alle informatie om het incident te analyseren en op te lossen, is minimaal drie jaar. Dit betreft onder meer de informatie benodigd voor de analyse (waaronder logging), de oplossing en het advies.	Y	Y	☑	☑	☐	
	5.29.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO	Y	Y	☑	☐	☑	
	5.30.01	De proceseigenaar test jaarlijks continuïteitsplannen op werking, volledigheid en actualiteit, om de plannen te verbeteren.	Y	Y	☑	☐	☑	
	5.30.02	Binnen de inventarisatie van beheersmaatregel 5.12, identificeert de proceseigenaar kritieke systemen op basis van de vastgestelde risicomanagementmethodiek en een expliciete risicoafweging. De proceseigenaar actualiseert dit overzicht ten minste eens per drie jaar.	Y	Y	☑	☐	☐	
	5.31.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO	Y	Y	☑	☑	☑	
	5.32.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO	Y	Y	☐	☑	☑	
	5.33.01	De proceseigenaar heeft voor alle informatie(systemen) in selectielijsten de bewaartermijn vastgelegd, rekening houdend met de eigen bedrijfsdoelstellingen en wet- en regeling, zoals de archiefwet en privacywetgeving. De proceseigenaar heeft deze termijnen ook praktisch ingeregeld en toetst periodiek de werking hiervan.	Y	Y	☑	☑	☐	
	5.34.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO	Y	Y	☑	☑	☑	
	5.35.01	Er is een werkend ISMS volgens NEN-EN-ISO/IEC ISO 27001.	Y	Y	☑	☐	☐	
	5.35.02	Er is een vastgesteld auditplan waarin jaarlijks keuzes worden gemaakt voor welke systemen welk soort beveiligingsaudits worden uitgevoerd.	Y	Y	☑	☐	☐	
	5.36.01	In de P&C-cyclus en als onderdeel van de plan-do-check-act (PDCA)-cyclus wordt gerapporteerd over informatiebeveiliging onder coördinatie van de CISO. Dit resulteert in een jaarlijks af te geven In Control Verklaring (ICV), of een vergelijkbaar instrument, over de gehele informatiebeveiliging van de overheidsorganisatie. De ICV of het vergelijkbare instrument kan ook onderdeel zijn van de formele verantwoording.	Y	Y	☑	☐	☐	
	5.37.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO	Y	Y	☑	☐	☐	
	6.01.01	Elke organisatie heeft een vastgesteld screeningsbeleid. Bij indiensttreding en bij functiewijziging kan op basis van een risicoafweging een Verklaring Omtrent het Gedrag (VOG) gevraagd worden.	Y	Y	☑	☐	☑	
	6.02.01	Alle medewerkers (intern en extern) zijn bij hun aanstelling of functiewisseling gewezen op hun verantwoordelijkheden voor informatiebeveiliging. De voor hen geldende regelingen en instructies voor informatiebeveiliging zijn eenvoudig toegankelijk.	Y	Y	☑	☑	☑	
	6.03.01	Alle medewerkers, lijnmanagers en bestuurders hebben de verantwoordelijkheid bedrijfsinformatie te beschermen. Iedereen kent de regels van en verplichtingen voor informatiebeveiliging en daar waar relevant de speciale eisen voor gerubriceerde omgevingen.	Y	Y	☑	☑	☑	
	6.03.02	Alle medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten hebben binnen drie maanden na indiensttreding aantoonbaar een training I-bewustzijn succesvol gevolgd.	Y	Y	☑	☐	☑	
	6.03.03	Het management benadrukt bij aanstelling en interne overplaatsing en bijvoorbeeld in werkoverleggen of in personeelsgesprekken bij zijn medewerkers en contractanten het belang van opleiding en training op het gebied van informatiebeveiliging. Het management stimuleert hen actief deze periodiek te volgen.	Y	Y	☑	☐	☑	
	6.04.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO	Y	Y	☑	☐	☐	
	6.05.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO	Y	Y	☑	☐	☑	
	6.06.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO	Y	Y	☑	☑	☑	
	6.07.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO	Y	Y	☑	☐	☐	
	6.08.01	Alle medewerkers (intern en extern) hebben aantoonbaar kennisgenomen van de meldingsprocedure van informatiebeveiligingsincidenten.	Y	Y	☑	☑	☑	

	7.01.01	Er wordt voor het inrichten van beveiligde zones gebruik gemaakt van standaarden.	Y	Y	☑	☐	☐	
	7.01.02	Kritieke informatie of informatiesystemen zijn nooit via één beveiligde zone te bereiken.	Y	Y	☑	☐	☑	
	7.02.01	In geval van concrete beveiligingsrisico's worden waarschuwingen, volgens onderlinge afspraken, verzonden aan de relevante collega's binnen het beveiligingsdomein van de overheid.	Y	Y	☑	☐	☐	
	7.03.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO	Y	Y	☑	☑	☑	
	7.04.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO	Y	Y	☑	☐	☑	
	7.05.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO	Y	Y	☑	☐	☑	
	7.06.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO	Y	Y	☑	☐	☑	
	7.07.01	Bij het gebruik van een chipcardtoken voor toegang tot systemen wordt bij het verwijderen van het token de toegangsbeveiligingsvergrendeling automatisch geactiveerd.	Y	Y	☑	☐	☐	
	7.08.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO	Y	Y	☑	☐	☑	
	7.09.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO	Y	Y	☑	☐	☑	
	7.10.01	Er is een verwijderinstructie waarin is opgenomen dat van verwijderbare media die herbruikbaar zijn en die de organisatie verlaten, de bedrijfsgevoelige inhoud onherstelbaar verwijderd is.	Y	Y	☑	☐	☐	
	7.10.02	Voor het wissen van alle data op het medium, wordt data onherstelbaar verwijderd of onbeschikbaar gemaakt. Er wordt gecontroleerd of alle data onherstelbaar verwijderd is. Hiervan wordt verslag gemaakt. Er wordt bij voorkeur gebruik gemaakt van producten waarvoor de Unit Weerbaarheid van het Nationaal Bureau voor Verbindingsbeveiliging (NBV) een positief inzetadvies afgegeven heeft.	Y	Y	☑	☐	☑	
	7.10.03	Het gebruik van koeriers of transporteurs voor transport van geclassificeerde informatie voldoet aan vooraf opgestelde betrouwbaarheidseisen.	Y	Y	☑	☐	☐	
	7.11.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO	Y	Y	☑	☐	☑	
	7.12.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO	Y	Y	☑	☐	☑	
	7.13.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO	Y	Y	☑	☐	☑	
	7.14.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO	Y	Y	☑	☐	☑	
	8.01.01	Mobiele apparatuur is zo ingericht dat bedrijfsinformatie niet standaard op het gebruikersdevice wordt opgeslagen ('zero footprint'). Als (near) zero footprint (nog) niet realiseerbaar is, biedt een mobiel apparaat (zoals een laptop, tablet en smartphone) de mogelijkheid om de toegang te beschermen met een toegangsbeveiligingsmechanisme met minimaal versleuteling van de gegevens. Op mobiele apparatuur moet 'wissen op afstand' mogelijk zijn.	Y	Y	☑	☐	☐	
	8.01.02	Bij de inzet van mobiele apparatuur zijn minimaal de volgende aspecten geïmplementeerd: - In bewustwordingsprogramma's komen gedragsaspecten van veilig mobiel werken aan de orde. - Het apparaat maakt deel uit van patchmanagement en hardening. - Er wordt gebruik gemaakt van Mobile Device Management (MDM)- of Mobile Application Management (MAM)-oplossingen. - 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. Periodiek wordt getoetst of de punten in lid 1., 2. en 3. worden nageleefd.	Y	Y	☑	☐	☐	
	8.02.01	De toegewezen of gebruikte speciale bevoegdheden worden in opzet, bestaan en werking minimaal ieder kwartaal beoordeeld.	Y	Y	☑	☐	☐	
	8.03.01	Er zijn maatregelen genomen die het fysiek en/of logisch isoleren van informatie met specifiek belang waarborgen.	Y	Y	☑	☐	☐	
	8.03.02	Gebruikers kunnen alleen die informatie met specifiek belang inzien en verwerken die ze nodig hebben voor de uitoefening van hun taak.	Y	Y	☑	☐	☐	
	8.04.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO	Y	Y	☑	☐	☑	
	8.05.01	Voor het verlenen van toegang tot het netwerk aan externe leveranciers wordt vooraf een risicoafweging gemaakt. De risicoafweging bepaalt onder welke voorwaarden en voor hoelang de leveranciers toegang krijgen. Uit een registratie blijkt hoe de rechten zijn toegekend.	Y	Y	☑	☐	☑	
	8.06.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO	Y	Y	☑	☐	☑	
	8.07.01	Het downloaden van bestanden is beheerst en beperkt op basis van het risico en need-of-use. De antimalware-software moet altijd alle downloads beoordelen.	Y	Y	☑	☐	☐	
	8.07.02	Gebruikers zijn voorgelicht over de risico's van surfgedrag en het klikken op onbekende links.	Y	Y	☑	☐	☐	
	8.07.03	De gebruikte antimalware-software en bijbehorende herstelsoftware zijn actueel en wordt ondersteund door periodieke updates.	Y	Y	☑	☐	☐	
	8.07.04	De malwarescan wordt uitgevoerd op: - alle omgevingen, bijvoorbeeld op (mail)servers, (desktop)computers en bij de toegangsverlening tot het netwerk van de organisatie; - alle gedownloade content voorafgaand aan executie of opslag; - alle bestanden die via netwerken of via elke vorm van opslagmedium zijn ontvangen, vóór gebruik of opslag in de eigen omgeving.	Y	Y	☑	☐	☐	
	8.08.01	Als de kans op misbruik en de verwachte schade beide hoog zijn (bijvoorbeeld met de NCSC-Inschalingsmatrix beveiligingsadviezen of leveranciersbeveiligingsadviezen), worden passende mitigerende maatregelen zo snel mogelijk, maar uiterlijk binnen een week getroffen.	Y	Y	☑	☐	☐	
	8.08.02	Op basis van een expliciete risicoafweging wordt bepaald op welke wijze mitigerende maatregelen getroffen worden.	Y	Y	☑	☐	☐	
	8.08.03	In de tussentijd of als installatie binnen een week niet mogelijk is, worden op basis van een expliciete risicoafweging mitigerende maatregelen getroffen.	Y	Y	☑	☐	☐	

8.08.04	Informatiesystemen worden bij voorkeur jaarlijks gecontroleerd op technische naleving van beveiligingsnormen en risico's van de feitelijke veiligheid. Dit kan bijvoorbeeld door (geautomatiseerde) kwetsbaarheidsanalyses, penetratietesten of red-teamingstesten. Internetfacing-informatiesystemen worden bij voorkeur continue getest op zwakheden en kwetsbaarheden.	Y	Y	☑	☐	☐	
8.08.05	Internetfacing-informatiesystemen hebben een verplichte (bij voorkeur geautomatiseerde) penetratietest bij iedere nieuwe release of major update. Als daar bevindingen met een hoog risico uitkomen die niet op een andere manier gemitigeerd kunnen worden, mag het systeem niet in productie. Alle internetfacing-informatiesystemen worden minimaal jaarlijks getest op zwakheden en kwetsbaarheden.	Y	Y	☑	☐	☐	
8.08.06	Een Coordinated Vulnerability Disclosure (CVD)-procedure is ingericht en gepubliceerd volgens de NCSC-leidraad of NEN-EN-ISO/IEC 29147:2020 Vulnerability disclosure. Informatie afkomstig uit de Coordinated Vulnerability Disclosure (CVD)-meldingen is onderdeel van de incidentrapportage.	Y	Y	☑	☐	☐	
8.09.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO	Y	Y	☑	☐	☑	
8.10.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO	Y	Y	☑	☑	☑	
8.11.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO	Y	Y	☑	☑	☑	
8.12.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO	Y	Y	☑	☑	☑	
8.13.01	Er is een back-upbeleid waarin de eisen voor het bewaren en beschermen zijn gedefinieerd en vastgesteld. Er moet speciale aandacht zijn voor het beschermen van de back-up tegen ransomware-aanvallen en genomen maatregelen om de integriteit van de back-up te behouden.	Y	Y	☑	☐	☐	
8.13.02	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	☑	☐	☐	
8.13.03	Het back-upproces voorziet in de 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	☑	☐	☑	
8.13.04	De herstelprocedure wordt minimaal jaarlijks getest of na een grote wijziging, om de goede werking te waarborgen als deze in noodgevallen uitgevoerd moet worden.	Y	Y	☑	☐	☐	
8.14.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO	Y	Y	☑	☐	☐	
8.15.01	Een logregel bevat minimaal: - Actie: de gebeurtenis of handeling die heeft plaatsgevonden. - Object: waarop de gebeurtenis of handeling effect had (bijvoorbeeld welk bestand, proces of systeem). - Resultaat: het resultaat van de gebeurtenis of handeling. - Oorsprong: het apparaat of de netwerklocatie van waaruit de gebeurtenis of handeling in gang is gezet. - Actor: identificatie van de persoon die of het proces dat de gebeurtenis in gang heeft gezet. - Tijdstempel: datum en tijdstip waarop de gebeurtenis of handeling plaatsvond.	Y	Y	☑	☐	☐	
8.15.02	Een logregel bevat nooit gegevens die tot het doorbreken van de beveiliging kunnen leiden.	Y	Y	☑	☐	☐	
8.15.03	Er is een overzicht van logbestanden die worden gegenereerd.	Y	Y	☑	☐	☐	
8.15.04	De bewaartermijn van logbestanden en gegevens in het Security Incident en Event Monitoring (SIEM) worden risicogericht bepaald, rekening houdend met het scenario dat aanvallers langdurig binnen zijn.	Y	Y	☑	☐	☐	
8.15.05	Oneigenlijk wijzigen, verwijderen of pogingen daartoe van loggegevens worden zo snel mogelijk gemeld als informatiebeveiligingsincident via de procedure voor informatiebeveiligingsincidenten volgens beheersmaatregel 5.24.	Y	Y	☑	☐	☐	
8.15.06	Op basis van een expliciete risicoafweging bepaalt de organisatie de periodieke toetsing op het ongewijzigd bestaan van logbestanden gedurende de bewaartermijn. Toetsing wordt uitgevoerd door een onafhankelijke functionaris (ten opzichte van de uitvoering).	Y	Y	☑	☐	☐	
8.16.01	Bij ontdekte nieuwe dreigingen (aanvallen) via overheidsmaatregel 8.16.3 worden deze binnen geldende juridische kaders verplicht gedeeld met de daarvoor aangewezen Computer Emergency Response Team (CERT).	Y	Y	☑	☐	☐	
8.16.02	Het SIEM- en/of het SOC-monitoring-proces hebben eenduidige regels over wanneer een incident moet worden gerapporteerd aan het verantwoordelijke management.	Y	Y	☑	☐	☑	
8.16.03	De informatieverwerkende omgeving wordt gemonitord met een detectie- en response-oplossing, waarmee aanvallen kunnen worden gedetecteerd en afwijkingen adequaat en tijdig worden behandeld.	Y	Y	☑	☐	☐	
8.16.04	Actieve netwerkcomponenten zijn voorzien van logging en monitoring van die logging om afwijkende gebeurtenissen te kunnen waarnemen en daarop te reageren.	Y	Y	☑	☐	☐	
8.17.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO	Y	Y	☑	☐	☑	
8.18.01	Alleen bevoegd personeel heeft op die momenten dat toegang strikt noodzakelijk is toegang tot systeemhulpmiddelen.	Y	Y	☑	☐	☐	
8.18.02	Het gebruik van systeemhulpmiddelen wordt gelogd. De logging is een halfjaar beschikbaar voor onderzoek.	Y	Y	☑	☐	☐	
8.19.01	Het risico van installatie door gebruikers van niet geautoriseerde software moet worden beheerst.	Y	Y	☑	☐	☐	
8.20.01	Netwerkcomponenten moeten minimaal voldoen aan het vertrouwelijkheidsniveau van het netwerk waarvan ze onderdeel zijn.	Y	Y	☑	☐	☐	
8.20.02	Toegang tot beheerinterfaces van netwerkcomponenten moet (zo veel als mogelijk en risicogericht) gescheiden zijn van het gebruikersnetwerk.	Y	Y	☑	☐	☐	

8.21.01	In koppelpunten met externe of onvertrouwde zones en vanwege netwerksegmentatie 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 te mitigeren.	Y	Y	☑	☐	☑	
8.21.02	Het dataverkeer van of naar de vertrouwde omgeving, wordt bewaakt/geanalyseerd op verdacht verkeer met detectievoorzieningen.	Y	Y	☑	☐	☐	
8.21.03	Bij ontdekte nieuwe dreigingen vanuit overheidsmaatregel 8.21.02 worden deze doorgeleid, rekening houdend met de geldende juridische kaders gedeeld binnen de overheid.	Y	Y	☑	☐	☐	
8.21.04	Bij transport van gegevens over draadloze verbindingen zoals wifi en bij bedrade verbindingen buiten het gecontroleerd gebied worden de gegevens versleuteld met uitzondering van metagegevens die noodzakelijk zijn om het transport tot stand te laten komen. De inrichting van de versleuteling is risicogericht en houdt rekening met de noodzakelijke beschermingstermijn en -niveau. Hierbij wordt bij voorkeur gebruik gemaakt van encryptiemiddelen waarvoor de Unit Weerbaarheid van de Algemene Inlichtingen en Veiligheidsdienst (AIVD) een positief inzetadvies heeft afgegeven. Heeft de Unit Weerbaarheid geen geadviseerde encryptiemiddelen, wordt in overleg met de CISO een andere geschikte versleutelingsmethodiek gekozen en ingericht.	Y	Y	☑	☐	☐	
8.22.01	Alle gescheiden groepen hebben een gedefinieerd beveiligingsniveau.	Y	Y	☑	☐	☐	
8.23.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO	Y	Y	☑	☐	☐	
8.24.01	In het cryptografiebeleid zijn minimaal de volgende onderwerpen uitgewerkt: - Wanneer cryptografie ingezet wordt. - Wie verantwoordelijk is voor de implementatie. - Wie verantwoordelijk is voor het sleutelbeheer. - Hoe geregistreerd wordt waar welke cryptografie toegepast wordt. - Welke normen als basis dienen voor cryptografie en de wijze waarop de normen van het Forum Standaardisatie worden toegepast. - De wijze waarop het beschermingsniveau vastgesteld wordt. - Bij communicatie tussen organisaties wordt het beleid onderling vastgesteld.	Y	Y	☑	☐	☐	
8.24.02	Cryptografische beheersmaatregelen zijn opgenomen in de inventaris van de bedrijfsmiddelen. Voor alle cryptografische beheersmaatregelen is vastgesteld waar ze worden ingezet, wie er voor verantwoordelijk is en hoe ze actueel worden gehouden.	Y	Y	☐	☐	☑	
8.24.03	Cryptografische toepassingen voldoen aan passende standaarden van het Forum Standaardisatie.	Y	Y	☑	☐	☐	
8.24.05	Er zijn (contractuele) afspraken over reservecertificaten van een alternatieve leverancier als uit de risicoafweging blijkt dat deze noodzakelijk zijn als onderdeel van gereedheid voor bedrijfscontinuïteit (beheersmaatregel 5.30).	Y	Y	☑	☐	☐	
8.25.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO	Y	Y	☑	☐	☐	
8.26.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO	Y	Y	☑	☐	☐	
8.27.01	Architectuurprincipes zoals ‘security by design’ en ‘security by default’ voor het ontwerpen van beveiliging van informatiesystemen worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle activiteiten over het ontwikkelen van informatiesystemen.	Y	Y	☑	☐	☐	
8.28.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO	Y	Y	☑	☐	☑	
8.29.01	Voor acceptatietesten van systemen worden gestructureerde testmethodieken gebruikt. De testen worden bij voorkeur geautomatiseerd uitgevoerd. Van de resultaten van de testen wordt verslag gemaakt.	Y	Y	☑	☐	☑	
8.30.01	Interne maatregelen voor systeemontwikkeling zijn onverkort van toepassing op uitbestede ontwikkeling, aangevuld met maatregelen die volgen vanuit uitbestedingen.	Y	Y	☑	☐	☑	
8.31.01	In de productieomgeving wordt niet getest. Alleen met voorafgaande goedkeuring door de proceseigenaar kan hiervan worden afgeweken.	Y	Y	☑	☐	☐	
8.31.02	Significante wijzigingen in de productieomgeving worden altijd getest voordat zij in productie gebracht worden. Alleen met voorafgaande goedkeuring door de proceseigenaar kan hiervan worden afgeweken.	Y	Y	☑	☐	☐	
8.32.01	In het wijzigingsbeheerproces is minimaal aandacht besteed aan: - het administreren van wijzigingen, met de resultaten van het testplan; - een risicoafweging van mogelijke gevolgen van de wijzigingen, inclusief een beschreven rollbackplan; - de goedkeuringsprocedure voor wijzigingen.	Y	Y	☑	☐	☑	
8.32.02	Wijzigingsbeheer vindt plaats op basis van een algemeen geaccepteerd beheerraamwerk.	Y	Y	☑	☐	☐	
8.33.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO	Y	Y	☑	☐	☐	
8.34.01	Geen overheidsmaatregel, zie deel 1 Kader BIO2, verplichtingen BIO	Y	Y	☑	☐	☑	

Statement of Applicability
Eurofiber Cloud Infra
ISO27017:2021
Date 30-6-2025

	#	Title	Applicable Y/N	Implemented Y/N	Reason inclusion: Risk	Reason inclusion: Legal	Reason inclusion: Contractual	Reason for exclusion
	CLD.6.3.1	Shared roles and responsibilities within a cloud computing environment	Y	Y	☑	☐	☑	
	CLD.8.1.5	Removal of cloud service customer assets	Y	Y	☑	☐	☑	
	CLD.9.5.1	Segregation in virtual computing environments	Y	Y	☑	☐	☑	
	CLD.9.5.2	Virtual machine hardening	Y	Y	☑	☐	☑	
	CLD.12.1.5	Administrator's operational security	Y	Y	☑	☐	☑	
	CLD.12.4.5	Monitoring of Cloud Services	Y	Y	☑	☐	☑	
	CLD.13.1.4	Alignment of security management for virtual and physical networks	Y	Y	☑	☐	☑	