Toetsingskader Informatiebeveiliging cluster 1 t/m 6

(versie 3.0, juli 2017)

IBPDOC3

GEBRUIKERSGROEP IBP IN HET MBO

Kennisnet SURF saMBO-ICT

Verantwoording

Bron:

SURFaudit toetsingskader
Stichting SURF
Februari 2015

Bewerkt door:

Kennisnet / saMBO-ICT

Auteurs

Bart Bosma (SURF)
Ludo Cuijpers (Kennisnet)
Juli 2017

Met dank aan:

Hans Alfons (Vrije Universiteit)
Wim Arendse (Zadkine)
Bram Bogers (Onderwijsgroep Tilburg)
Marcel van Dam (Zadkine)
Elly Dingemanse (Kennisnet)
Esther van der Hei (Nimeto)
Co Klerkx (ROC van Amsterdam)
Ron Veldhoen (Universiteit Twente)

Sommige rechten voorbehouden

Inhoudsopgave

Management samenvatting

Dit document is onderdeel van de producten die opgeleverd onder verantwoording van de Taskforce ibp (Programma Informatiebeveiliging (IB) en Privacy in het mbo).
Het document kan op een vijftal manieren worden gebruikt:

1. **Nulmeting** voor de mbo instelling. Deze meting geeft niet alleen een volwassenheidsniveau aan, op een schaal van 1 (onvolwassen) tot 5 (droom scenario), maar ook de onderdelen waar duidelijk (bewijsbaar) onder de maat wordt gepresteerd.
2. **Baseline voor de mbo sector**. Al dan niet in overleg met OC&W kan een minimaal wenselijk niveau worden bepaald waarbij ook rekening wordt gehouden met aanvullende speerpunten, zoals examinering. Als sector zouden we kunnen kiezen voor volwassenheidsniveau 2 en voor examen specifieke statements, bijvoorbeeld, voor volwassenheidsniveau 3 (bijvoorbeeld autorisatie).
3. **Baseline voor de mbo instelling.** Op basis van de uitkomsten van de nulmeting en de baseline voor de mbo sector kan de mbo instelling haar eigen baseline bepalen, die hoger (ambitieuzer) of lager (inhaalslag) kan worden bepaald.
4. **Benchmark** voor de mbo sector. Eind 2015 krijgen 15 instellingen de mogelijkheid om hier aan deel te nemen. Op basis van de uitkomsten van deze benchmark kunnen door Kennisnet of saMBO-ICT nieuwe initiatieven worden ontplooid.
5. **Aanvulling audit kwaliteitszorg.** Kwaliteitszorg moet kunnen aantonen dat digitale examens voldoen aan allerlei eisen zoals die door de sector in nauw overleg met de Inspectie zijn vastgesteld. Dit toetsingskader toont aan met hard bewijs of een mbo instelling al dan niet voldoet aan de gestelde eisen.
6. **Input accountsverklaring jaarrekening.** Het komt steeds vaker voor dat accountantskantoren inzicht willen hebben in de informatiebeveiliging van een mbo instelling. Dit toetsingskader is afgeleid van een internationaal vastgesteld normenkader (ISO 27001-27002) en dus voor een accountant acceptabel.
7. **Privacy beleid aanzet.** Een aantal statements verzorgen input voor het privacy beleid dat door een mbo instelling vervolgens vorm kan worden gegeven.

Samenhang met andere documenten

De samenhang tussen alle documenten, zoals die geproduceerd worden in opdracht van de taskforce, wordt beschreven in de Roadmap[1].
De verantwoording van dit document is terug te vinden in:

- **Verantwoordingsdocument informatiebeveiliging en privacy in het mbo onderwijs (IBPDOC1):** met name de verantwoording waarom informatiebeveiliging en privacy beleid in de MBO sector wordt geïmplementeerd;
- **Normenkader informatiebeveiliging mbo (IBPDOC2A)**: met name de onderbouwing van het toetsingskader en de verantwoording naar de externe toezichthouders.

[1] Mbo roadmap informatie beveiligingsbeleid voor de mbo sector (IBPDOC5)

1. Beleid en organisatie

Nr.	ISO27002	Controledoelstelling
1.1	5.1.1.1	**Beleidsregels voor informatiebeveiliging**: Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden Gedefinieerd en goedgekeurd door het bestuur.
1.2	5.1.1.2	**Beleidsregels voor informatiebeveiliging**: Het door het bestuur vastgestelde Informatiebeveiligingsbeleid wordt gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.
1.3	5.1.2	**Beoordeling van het Informatiebeveiligingsbeleid:** Het beleid voor informatiebeveiliging behoort met geplande tussenpozen, of als zich significante veranderingen voordoen, te worden beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is.
1.4	6.1.1	**Taken en verantwoordelijkheden informatiebeveiliging**: Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden Gedefinieerd en toegewezen
1.5	6.1.5	**Informatiebeveiliging in projectbeheer:** Informatiebeveiliging behoort aan de orde te komen in projectbeheer, ongeacht het soort project.
1.6	6.2.1.1	**Beleid voor mobiele apparatuur**: Er dient beleid te worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beheren.
1.7	8.2.1	**Classificatie van informatie:** Informatie behoort te worden geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging.
1.8	8.2.2	**Informatie labelen:** Om informatie te labelen behoort een passende reeks procedures te worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.
1.9	10.1.1.1	**Beleid inzake het gebruik van cryptografische beheersmaatregelen:** Ter bescherming van informatie behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld.
1.10	10.1.1.2	**Beleid inzake het gebruik van cryptografische beheersmaatregelen**: Ter bescherming van informatie zijn er tools of applicaties aanwezig waarmee het beleid voor het gebruik van cryptografische beheersmaatregelen wordt geïmplementeerd.
1.11	11.2.5	**Verwijdering van bedrijfsmiddelen:** Apparatuur, informatie en software behoren niet van de locatie te worden meegenomen zonder voorafgaande goedkeuring.
1.12	13.2.1	**Beleid en procedures voor informatietransport:** Ter bescherming van het informatietransport, dat via alle soorten communicatiefaciliteiten verloopt, behoren formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht te zijn.
1.13	13.2.2	**Overeenkomsten over informatietransport:** Overeenkomsten behoren betrekking te hebben op het beveiligd transporteren van bedrijfsinformatie tussen de organisatie en externe partijen.
1.14	14.1.1	**Analyse en specificatie van informatiebeveiligingseisen**: De eisen die verband houden met informatiebeveiliging behoren te worden opgenomen in de eisen voor nieuwe informatiesystemen of voor uitbreidingen van bestaande informatiesystemen.
1.15	15.1.2	**Opnemen van beveiligingsaspecten in leveranciersovereenkomsten:** Alle relevante informatiebeveiligingseisen behoren te worden vastgesteld en overeengekomen met elke leverancier die toegang heeft tot IT-infrastructuurelementen ten behoeve van de informatie van de organisatie, of deze verwerkt, opslaat, communiceert of biedt.
1.16	15.1.3	**Toeleveringsketen van informatie- en communicatietechnologie**: Overeenkomsten met leveranciers behoren eisen te bevatten die betrekking hebben op de informatiebeveiligingsrisico's in verband met de toeleveringsketen van de diensten en producten op het gebied van informatie- en communicatietechnologie.
1.17	16.1.1	**Verantwoordelijkheden en procedures:** Er zijn leidinggevende en -procedures vastgesteld om een snelle, doeltreffende en ordelijke respons op informatiebeveiligingsincidenten te bewerkstelligen.
1.18	16.1.2	**Rapportage van informatiebeveiligingsgebeurtenissen:** Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd.
1.19	18.1.3	**Beschermen van registraties:** Registraties behoren in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfseisen te worden beschermd tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave.
1.20	18.1.4	**Privacy en bescherming van persoonsgegevens:** Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.
1.21	6.1.2	**Scheiding van taken:** Conflicterende taken en verantwoordelijkheden behoren te worden gescheiden om de kans op onbevoegd of onbedoeld wijzigen of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.

1.1 Beleidsregels voor informatiebeveiliging (1)

Cluster: Beleid en organisatie	**ISO 27002 nummer: 5.1.1**

Controledoelstelling: Beleidsregels voor informatiebeveiliging
Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden Gedefinieerd en goedgekeurd door het bestuur.

Tips: Hanteer de "Leidraad Informatiebeveiligingsbeleid XX-V2.0" als uitgangspunt. Controleer het beleid voor de volgende onderdelen op aanwezigheid en juistheid:

1. Inleiding
2. Beleidsuitgangspunten en -principes informatiebeveiliging en privacy
3. Classificatie
4. Wet- en regelgeving
5. Governance informatiebeveiligingsbeleid
6. Melding en afhandeling van incidenten

Toelichting:
Een document met informatiebeveiligingsbeleid moet door de directie worden goedgekeurd en gepubliceerd en kenbaar worden gemaakt aan alle werknemers en relevante externe partijen (Er is beleid voor informatiebeveiliging door het College van Bestuur vastgesteld, gepubliceerd en beoordeeld op basis van inzicht in risico's, kritische bedrijfsprocessen en toewijzing van verantwoordelijkheden.)

Niveaus	**Beheersmaatregel (plus evidence)**	**Audit**
Volwassenheidsniveau 1 (Initieel / ad hoc)	Verantwoordelijkheden en verantwoording t.a.v. informatiebeveiligingsbeleid zijn niet Gedefinieerd.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Er is een algemeen informatiebeveiligingsbeleid of er zijn beleidsstukken en richtlijnen m.b.t. beveiliging gericht op belangrijke delen van de informatievoorziening, maar niet formeel vastgelegd. Men neemt verantwoordelijkheid en men wordt ter verantwoording geroepen, maar deze verantwoordelijkheden zijn niet formeel vastgelegd. **Evidence**: 1. Kopie beschikbare beleidsstukken en richtlijnen.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Het informatiebeveiligingsbeleid is door het bestuur formeel goedgekeurd verantwoordelijkheden zijn belegd, bevoegdheden zijn nog niet volledig belegd. **Evidence in aanvulling op 2**: 1. Kopie informatiebeveiligingsbeleid; 2. Kopie notulen waarin het blijkt dat het informatiebeveiligingsbeleid is goedgekeurd door het management; 3. Organogram waaruit het blijkt dat de verantwoordelijkheden zijn belegd of kopie profielen waarin het blijkt dat de verantwoordelijkheden zijn opgenomen door de medewerkers (Governance); 4. Het Informatiebeveiligingsbeleid voldoet aan best practices, bijvoorbeeld Code voor Informatiebeveiliging (ISO 27001/2).	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	Het beleid wordt gedragen door de organisatie en de bevoegdheden zijn belegd. **Evidence, in aanvulling op 3**: 1. Instelling kan door middel van versiebeheer aantonen dat het Informatiebeveiligingsbeleid periodiek of na een belangrijke verandering in de organisatie, technische infrastructuur of een ingrijpend beveiligingsincident wordt aangepast om te bewerkstelligen dat het geschikt, toereikend en doeltreffend blijft (zie ook 5.1.2.1).	
Volwassenheidsniveau 5 (Geoptimaliseerd)	Beleid wordt tot op het laagste niveau correct geïnterpreteerd en uitgevoerd. Er is een proces ingericht ten behoeve van evaluatie en terugkoppeling, bijv. door periodieke agendering op afdelingsvergadering of werkoverleg. **Evidence, in aanvulling op 4**: 1. Kopie agenda periodiek overleg met informatiebeveiligingsbeleid als standaard agendapunt.	

Controledoelstelling 1.1

Cluster: Beleid en organisatie	**ISO 27002 nummer: 5.1.1**
Controledoelstelling: Beleidsregels voor informatiebeveiliging Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden Gedefinieerd en goedgekeurd door het bestuur.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

1.2 Beleidsregels voor informatiebeveiliging (2)

Cluster: Beleid en organisatie	**ISO 27002 nummer: 5.1.1**
Controledoelstelling: Beleidsregels voor informatiebeveiliging Het door het bestuur vastgestelde Informatiebeveiligingsbeleid wordt gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.	
Tips: onderzoek of er ook met externe partijen wordt gecommuniceerd over het informatiebeveiligings- en privacybeleid van de instelling. Zie ook de SCIPR "Leidraad Informatiebeveiligingsbeleid XX-V2.0.docx".	
Toelichting: Een document met informatiebeveiligingsbeleid moet door de directie worden goedgekeurd en gepubliceerd en kenbaar worden gemaakt aan alle werknemers en relevante externe partijen.	

Niveaus	**Beheersmaatregel (plus evidence)**	**Audit**
Volwassenheidsniveau 1 (Initieel / ad hoc)	Er wordt sporadisch over informatiebeveiligingszaken gecommuniceerd.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Er is beleid, maar slechts initieel bij goedkeuring van het beleid wordt dit ook gecommuniceerd. **Evidence:** 1. Laatste nieuwsbrief of iets dergelijks waarin de goedkeuring van het beleid is gecommuniceerd.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	De medewerkers en **externe partijen** worden regelmatig gewezen op het gepubliceerde informatiebeveiligingsbeleid. Bijvoorbeeld bij aanname van personeel. **Evidence in aanvulling op 2:** 1. Kopie van contract / overeenkomst waarin is verwezen naar het goedgekeurde informatiebeveiligingsbeleid; 2. Kopie van informatie waaruit blijkt dat de medewerkers en externe partijen worden gewezen op het gepubliceerde informatiebeveiligingsbeleid. Bijvoorbeeld interne websites.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	Er wordt via een formele (communicatie infra-) structuur regelmatig gecommuniceerd over op dat moment relevante beveiligingsthema's. Wordt in HR-gesprekken meegenomen. **Evidence in aanvulling op 3:** 1. Kopie van nieuwsbrief met vaste rubriek over informatiebeveiliging (cq. Aantal brieven waarin onderwerp besproken wordt); 2. Kopie agenda waaruit blijkt dat Informatiebeveiliging een vast agendapunt is op de jaargesprekken van medewerkers.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	Er is niet alleen inzicht in actuele behoefte op het gebied van informatiebeveiligingsbeleid maar er wordt ook proactief gecommuniceerd op basis van trends, bijvoorbeeld in een periodiek of informatiebeveiligingsnieuwsbrief. **Evidence in aanvulling op 4:** 1. Kopie van planning Informatiebeveiliging awareness-programma; 2. Kopie van aanwezigheidsregistratie awareness programma.	

Controledoelstelling 1.2

Cluster: Beleid en organisatie	**ISO 27002 nummer: 5.1.1**
Controledoelstelling: Beleidsregels voor informatiebeveiliging Het door het bestuur vastgestelde Informatiebeveiligingsbeleid wordt gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

1.3 Beoordeling van het informatiebeveiligingsbeleid

Cluster: Beleid en organisatie	**ISO 27002 nummer: 5.1.2**
Controledoelstelling: Beoordeling van het informatiebeveiligingsbeleid Het beleid voor informatiebeveiliging behoort met geplande tussenpozen of als zich significante veranderingen voordoen, te worden beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is.	
Tips: het beleid is onderdeel geworden van de PDCA-cyclus. Achterhaal op basis van interviews of dit gerealiseerd is.	
Toelichting: Het informatiebeveiligingsbeleid moet met geplande tussenpozen, of zodra zich belangrijke wijzigingen voordoen, worden beoordeeld om te bewerkstelligen dat het geschikt, toereikend en doeltreffend blijft. (Het informatiebeveiligingsbeleid wordt met geplande tussenpozen of na een belangrijke verandering in de organisatie, technische infrastructuur of een ingrijpend beveiligingsincident, beoordeeld om te bewerkstelligen dat het geschikt, toereikend en doeltreffend blijft.)	

Niveaus	**Beheersmaatregel (plus evidence)**	**Audit**
Volwassenheidsniveau 1 (Initieel / ad hoc)	Onderhoud op informatiebeveiligingsbeleid vindt ad-hoc plaats.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Het informatiebeleid wordt niet met geplande tussenpozen beoordeeld. Indien men het nodig vindt wordt het beleid bijgesteld. **Evidence:** 1. Kopie van enkele voorbeelden (versies) waar bijstellingen zijn doorgevoerd.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Het informatiebeveiligingsbeleid wordt met geplande tussenpozen, of zodra zich belangrijke wijzigingen voordoen, beoordeeld om te bewerkstelligen dat het geschikt, toereikend en doeltreffend blijft. **Evidence in aanvulling op 2:** 1. Kopie planningsagenda; 2. Kopie risicoanalyse met motivatie en actie; inclusief datum en versienummer; 3. Vastlegging van bespreking/goedkeuring van wijzigingen door het verantwoordelijk (top)management, te denken aan het besluitenlijst van het CvB.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	De instelling evalueert het informatiebeveiligingsbeleid periodiek of na een belangrijke verandering in de organisatie, in technische infrastructuur of na een ingrijpend beveiligingsincident en past het beleid aan om te zorgen dat het geschikt, toereikend en doeltreffend blijft. Na bijstelling van het informatiebeveiligingsbeleid wordt, door de verantwoordelijke functionarissen, actie ondernomen om eerder genomen maatregelen weer in overeenstemming te brengen met het bijgestelde beleid. **Evidence in aanvulling op 3:** 1. Kopie van informatiebeveiligingsbeleid met versiebeheer; 2. Verbeterplan.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	Bijstelling van het beleid leidt automatisch tot het bijstellen van bijbehorende processen en procedures. **Evidence:** 1. Kopie van bedrijfsprocessen waaruit blijkt dat de een review van het IB-beleid vast onderdeel uitmaakt van de periodieke evaluatie van het proces.	

Controledoelstelling 1.3

Cluster: Beleid en organisatie	**ISO 27002 nummer: 5.1.2**
Controledoelstelling: Beoordeling van het informatiebeveiligingsbeleid Het beleid voor informatiebeveiliging behoort met geplande tussenpozen of als zich significante veranderingen voordoen, te worden beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

1.4 Beleidsregels voor informatiebeveiliging

Cluster: Beleid en organisatie	**ISO 27002 nummer: 6.1.1**

Controledoelstelling: Beoordeling van het informatiebeveiligingsbeleid
Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden Gedefinieerd en toegewezen.

Tips: Hanteer de "Leidraad Informatiebeveiligingsbeleid XX-V2.0" als uitgangspunt. Controleer de volgende onderdelen op aanwezigheid en juistheid:

1. Inleiding
2. Beleidsuitgangspunten en -principes informatiebeveiliging en privacy
3. Classificatie
4. Wet- en regelgeving
5. **Governance informatiebeveiligingsbeleid**
6. Melding en afhandeling van incidenten

Onderzoek of de governance ook vertaald is in een organogram.

Toelichting:
Alle verantwoordelijkheden voor informatiebeveiliging behoren duidelijk te zijn Gedefinieerd. (Toewijzing vindt plaats in overeenstemming met het beleid. Verantwoordelijkheden worden waar nodig aangevuld met meer gedetailleerde richtlijnen. Lokale verantwoordelijkheden, bijv. t.a.v. continuïteitsplanning, behoren duidelijk te worden Gedefinieerd. Bevoegdheden zijn duidelijk Gedefinieerd en gedocumenteerd.)

Niveaus	**Beheersmaatregel (plus evidence)**	**Audit**
Volwassenheidsniveau 1 (Initieel / ad hoc)	Verantwoordelijkheid en verantwoording zijn niet Gedefinieerd. Medewerkers nemen op eigen initiatief en op reactieve wijze verantwoordelijkheid voor kwesties.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Men neemt verantwoordelijkheid en wordt ter verantwoording geroepen, zelfs als dit niet formeel is geregeld. Bij problemen is echter vaak onduidelijk wie er verantwoordelijk is, en men is geneigd de schuld door te schuiven.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Er is een formele verantwoordelijkheid- en verantwoordingsstructuur en het is duidelijk wie waar verantwoordelijk voor is. Die persoon heeft echter vaak niet de volledige bevoegdheid om zijn verantwoordelijkheden volledig te kunnen uitoefenen. **Evidence:** 1. Kopie van organogram met opgenomen de verantwoordelijkheden en rapportagestructuur; 2. Formele functiebeschrijvingen.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	Er is een aanvaarde structuur voor verantwoordelijkheid en verantwoording en de betreffende personen kunnen zich van hun verantwoordelijkheden kwijten. Positieve actie wordt stelselmatig beloond om de betrokkenen te motiveren. **Evidence in aanvulling op 3:** 1. Kopie van een geaccordeerde mandatenregeling waaruit de bevoegdheden van de beveiligingsfunctionarissen blijkt.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	De verantwoordelijken hebben de vrijheid om, binnen hun mandaat, besluiten en maatregelen te nemen. De verantwoordelijkheidsstructuur is tot op het laagste niveau ingebed in de organisatie. **Evidence in aanvulling op 4:** 1. Kopie van werkinstructies of processchema's waaruit blijkt dat op alle niveaus beveiligingstaken kunnen worden uitgevoerd en hoe eventuele escalaties/opschaling zijn ingeregeld.	

Controledoelstelling 1.4

Cluster: Beleid en organisatie	**ISO 27002 nummer: 6.1.1**
Controledoelstelling: Beoordeling van het informatiebeveiligingsbeleid Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden Gedefinieerd en toegewezen.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

1.5 Informatiebeveiliging in projectbeheer

Cluster: Beleid en organisatie	**ISO 27002 nummer: 6.1.5**

Controledoelstelling: Informatiebeveiliging in projectbeheer
Informatiebeveiliging behoort aan de orde te komen in projectbeheer, ongeacht het soort project.

Tips: Als onderdeel van een project worden de volgende aandachtspunten meegenomen:
- De IBP[2] manager wordt in een vroeg stadium betrokken bij het project.
- Er wordt een IBP-paragraaf opgenomen in het project.
- Er wordt een BIV/PIA uitgevoerd.

Dit is de operationele uitvoer van, bijvoorbeeld, een aanbesteding of een project in het kader van life-cycle management. Zie ook 3.1.14.

Toelichting:
Informatiebeveiliging behoort te worden geïntegreerd in de projectbeheermethode(n) van de organisatie om ervoor te zorgen dat informatiebeveiligingsrisico's worden geïdentificeerd en aangepakt als deel van een project. Dit geldt in het algemeen voor elk project ongeacht het karakter, bijv. een project voor een proces voor kernactiviteiten, IT, 'facility management' en andere ondersteunende processen.

Niveaus	**Beheersmaatregel (plus evidence)**	**Audit**
Volwassenheidsniveau 1 (Initieel / ad hoc)	Aandacht voor informatiebeveiliging is niet geborgd in projectmethodiek. Aandacht vindt plaats uit persoonlijk initiatief of indien het projecten betreft rond beveiligingsmaatregelen.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Informatiebeveiliging blijkt - uit notulen of tekstfragmenten in projectdocumenten – zichtbaar aandacht te besteden aan informatiebeveiliging en privacyaspecten. Formeel geregeld is het nog niet.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	De projectmethodiek beschrijft in proces en producten op welke wijze tijdens projecten met informatiebeveiliging wordt omgegaan. Templates bevatten beveiligingsparagrafen en op verschillende momenten in het project zoals Go / No Go momenten en projectevaluatie wordt de kwaliteit van informatiebeveiliging meegewogen. **Evidence:** 1. Projecttemplates bevatten beveiligingsparagraaf; 2. Methodiek beschrijft vereiste aandacht voor beveiliging; 3. Informatiebeveiligingsfunctionaris heeft adviesfunctie binnen projecten; 4. BIA/PIA zijn verplichte componenten in ieder project.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	Projecten hebben zichtbaar aandacht besteed aan informatiebeveiliging. Kwaliteit van BIA's en PIA's zijn geëvalueerd, in evaluaties is betrokkenheid van de informatiebeveiligingsfunctie mede beoordeeld. **Evidence in aanvulling op 3:** 1. BIA's en PIA's zijn in meerdere projecten uitgevoerd; 2. Advies informatiebeveiligingsfunctionaris is in dossier aanwezig; 3. In projectevaluaties is aandacht voor informatiebeveiliging zichtbaar.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	Informatiebeveiliging heeft in ten minste vijf projecten zichtbaar aandacht gekregen. Leerpunten zijn getrokken en hebben inmiddels tot het bijstellen van de projectaanpak geleid. **Evidence in aanvulling op 4:** 1. Verbeterpunten zijn geformuleerd; 2. Vernieuwde versie projectmethodiek aanwezig; 3. Meerdere projectdeelnemers hebben inmiddels in meerdere projecten zichtbaar aandacht besteed aan informatiebeveiliging.	

[2] **I**nformatie**b**eveiliging en **p**rivacy

Controledoelstelling 1.5

Cluster: Beleid en organisatie	**ISO 27002 nummer: 6.1.5**
Controledoelstelling: Informatiebeveiliging in projectbeheer Informatiebeveiliging behoort aan de orde te komen in projectbeheer, ongeacht het soort project.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

1.6 Beleid voor mobiele apparatuur

Cluster: Beleid en organisatie	**ISO 27002 nummer: 6.2.1**
Controledoelstelling: Beleid voor mobiele apparatuur Er dient beleid te worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beheren.	
Tips: Er is een beleid op het gebied van Bring Your Own Device (BYOD) en Bring Your Company Device (BYCD). Bovendien wordt dit beleid gecontroleerd.	
Toelichting:	

Niveaus	**Beheersmaatregel (plus evidence)**	**Audit**
Volwassenheidsniveau 1 (Initieel / ad hoc)	Verantwoordelijkheid en verantwoording zijn niet gedefinieerd. Medewerkers nemen op eigen initiatief en op reactieve wijze verantwoordelijkheid voor kwesties.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Er is beleid, maar slechts initieel. Bij goedkeuring van het beleid wordt dit ook gecommuniceerd. **Evidence:** 1. Laatste nieuwsbrief, intranet of iets dergelijks, waarin de goedkeuring van het beleid is gecommuniceerd.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Het beleid voor mobiele apparatuur is door het CvB formeel goedgekeurd en ter beschikking gesteld aan de organisatie. **Evidence:** 1. Beleidsdocument betreffende gebruik van mobiele apparatuur; 2. Notulen CvB waarin het blijkt dat het beleid is goedgekeurd.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	Er is een beleid voor het gebruikmaken van mobiele apparatuur met speciale aandacht voor het ervoor waken dat bedrijfsinformatie niet wordt gecompromitteerd. Er is rekening gehouden met de risico's van het werken met mobiele apparatuur in onbeschermde omgevingen. **Evidence in aanvulling op 3:** 1. Bewijs dat alle gebruikers van mobiele apparatuur volgens het beleid handelen.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	Het beleid wordt uitgevoerd volgens en afgestemd op de nieuwste ontwikkelingen betreffende risico's en maatregelen omtrent het gebruik van mobiele apparatuur.	

Controledoelstelling 1.6

Cluster: Beleid en organisatie	**ISO 27002 nummer: 6.2.1**
Controledoelstelling: Beleid voor mobiele apparatuur Er dient beleid te worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beheren.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

1.7 Classificatie van informatie

Cluster: Beleid en organisatie	**ISO 27002 nummer: 8.2.1**
Controledoelstelling: Classificatie van informatie Informatie behoort te worden geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging.	
Tips: er is een beleid waarin de uitgangspunten van de BIV classificatie worden beschreven. De classificaties wordt op Laag, Midden en Hoog niveau beschreven. De beheersmaatregelen worden eveneens op deze schaalverdeling beschreven. Deze classificatie wordt gebruikt en periodiek geëvalueerd.	
Toelichting: Informatie behoort te worden geclassificeerd met betrekking tot de waarde, wettelijke eisen, gevoeligheid en onmisbaarheid voor de organisatie (Classificatie en bijbehorende beheersmaatregelen houden rekening met de behoefte aan het delen van informatie of het beperken ervan en de invloed van deze behoefte op de organisatie. Richtlijnen voor classificatie zijn in overeenstemming met vastgesteld toegangsbeleid.)	

Niveaus	**Beheersmaatregel (plus evidence)**	**Audit**
Volwassenheidsniveau 1 (Initieel / ad hoc)	Classificatie gebeurt niet, of soms, ad hoc of intuïtief bij invoering van een nieuwe registratie of systeem. Initiatief ligt bij projectleider of individuele medewerkers.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Er is een proces van classificatie dat in de praktijk is gegroeid, er zijn werkafspraken en groepen of afdelingen, maar er wordt niet op gestuurd en er is geen overkoepelend beleid. **Evidence**: 1. Kopie van document(en) waaruit blijkt dat er sprake is van: • Classificatie; • Labeling en • Conforme verwerking van informatie. Bijv. een afdelingsclassificatieplan met maatregelentabel.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Er zijn gelijksoortige en gemeenschappelijke procedures en implementaties van dataclassificatie, -labeling en verwerking bij delen van de instelling. Tenminste de concerninformatie wordt systematisch geclassificeerd met betrekking tot de waarde, wettelijke eisen, gevoeligheid en onmisbaarheid voor de organisatie. **Evidence in aanvulling op 2:** 1. Kopie beleid waarin het classificeren van informatie m.b.t. tot waarde, wettelijke eisen, gevoeligheid en onmisbaarheid van de organisatie is opgenomen; 2. Documentatie van uitgevoerde classificatie en proces van totstandkoming; 3. Kopie notulen dat de classificatie is goedgekeurd door management; 4. Kopie van informatie waaruit blijkt dat classificaties periodiek worden gereviewd (data en versienummers).	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	Classificatieproces en uitgevoerde classificaties worden regelmatig geëvalueerd. Ook op afdelings- en gebruikersniveau worden gegevens, bestanden en registraties geclassificeerd. **Evidence in aanvulling op 3:** 1. Procesbeschrijving classificatie en bijbehorende architectuur/maatregelen set; 2. Kopie van informatie waaruit blijkt dat het proces periodiek wordt gereviewd.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	Het classificatie proces, het onderliggende beleid en de implementatierichtlijnen zijn ingericht conform externe best practices en maken onderdeel uit van een gestandaardiseerd en geïntegreerd intern audit en compliance proces. **Evidence in aanvulling op 4:** 1. Kopie waaruit blijkt welke best practice gehanteerd wordt (bijv. "201512-leidraad-classificatie-scipr-2.0.pdf", welke Baseline etc.); 2. Kopie van het interne audit en compliance proces.	

Controledoelstelling 1.7

Cluster: Beleid en organisatie	**ISO 27002 nummer: 8.2.1**
Controledoelstelling: Classificatie van informatie Informatie behoort te worden geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor on-bevoegde bekendmaking of wijziging.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

1.8 Informatie labelen

Cluster: Beleid en organisatie	**ISO 27002 nummer: 8.2.2**

Controledoelstelling: Informatie labelen
Om informatie te labelen behoort een passende reeks procedures te worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.

Tips: de instelling moet kunnen aantonen dat de classificatie daadwerkelijk wordt toegepast. Te denken valt aan:
- Security architectuur document;
- Documenten die voorzien zijn van een 'stempel' vertrouwelijk;
- Aanwezigheid van een vertrouwenspersoon;
- Aanvullende afspraken voor functioneel beheerders i.v.m. vertrouwelijkheid;
- Etc.

Toelichting:
Er behoren geschikte, samenhangende procedures te worden ontwikkeld en geïmplementeerd voor de labeling en verwerking van informatie overeenkomstig het classificatiesysteem dat de organisatie heeft geïmplementeerd. (Procedures voor labelen van informatiebedrijfsmiddelen omvat zowel fysieke als elektronische hulpmiddelen. Het gaat om uitvoer van geclassificeerde gegevens, bestanden en bestandsoverdracht. Het is een hoofdeis voor overeenkomsten waar het delen van informatie wordt vastgelegd. Waar labelen niet mogelijk is kunnen andere manieren van classificatie van informatie worden toegepast, bijvoorbeeld via procedures of meta data.)

Niveaus	**Beheersmaatregel (plus evidence)**	**Audit**
Volwassenheidsniveau 1 (Initieel / ad hoc)	Er wordt niet gelabeld.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	In de praktijk wordt door individuele medewerkers of groepen gebruik gemaakt van classificatie-labels als 'Vertrouwelijk', 'Strikt vertrouwelijk' enz. op rapporten. Er is geen proces of procedure.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Er zijn geschikte, samenhangende procedures ontwikkeld en geïmplementeerd voor de labeling en verwerking van informatie overeenkomstig het classificatiesysteem dat de organisatie heeft geïmplementeerd. **Evidence:** 1. Kopie procedurebeschrijving van het labelen van informatiebedrijfsmiddelen die zowel fysieke als elektronische hulpmiddelen omvatten; 2. Kopie documentatie (e-mail, presentatie, nieuwsbrief) waaruit blijkt dat het procedure bij medewerkers bekend zijn.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	Er is een proces ingericht die waarborgt dat alle informatie wordt geclassificeerd, gelabeld en conform de bijbehorende maatregelen wordt verwerkt. Over dit proces wordt op reguliere basis gerapporteerd. **Evidence in aanvulling op 2:** 1. Kopie van de procesbeschrijving; 2. Kopie van de rapportage waaruit blijkt over welke kritieke informatie de instelling beschikt en wanneer en onder wiens verantwoordelijkheid de dataclassificatie heeft plaatsgevonden en welke maatregelen zijn geïmplementeerd.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	Het classificatie proces, het onderliggende beleid en de implementatierichtlijnen zijn ingericht conform externe best practices en maken onderdeel uit van een gestandaardiseerd en geïntegreerd intern audit en compliance proces. **Evidence in aanvulling op 4:** 1. Voorbeeld van toegepaste best practice.	

Controledoelstelling 1.8

Cluster: Beleid en organisatie	**ISO 27002 nummer: 8.2.2**
Controledoelstelling: Informatie labelen Om informatie te labelen behoort een passende reeks procedures te worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

1.9 Beleid inzake het gebruik van cryptografische beheersmaatregelen (1)

Cluster: Beleid en organisatie	**ISO 27002 nummer: 10.1.1**
Controledoelstelling: Beleid inzake het gebruik van cryptografische beheersmaatregelen Ter bescherming van informatie behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld.	
Tips: Er is een beleid t.a.v. cryptografische beheersmaatregelen.	
Toelichting: Er is beleid ontwikkeld en geïmplementeerd voor het gebruik van cryptografische beheersmaatregelen voor de bescherming van informatie. (Besluiten over het passend zijn van een cryptografische oplossing is onderdeel van het proces risicobeoordeling en de keuze van beheersmaatregelen: wanneer is welk type maatregel passend, voor welk doel en welk bedrijfsproces.)	

Niveaus	**Beheersmaatregel (plus evidence)**	**Audit**
Volwassenheidsniveau 1 (Initieel / ad hoc)	Er is geen beleid dat eisen stelt t.a.v. van het beschermen van informatie met behulp van cryptografie. Bij het aanschaffen van producten vertrouwt men op de aanwezige kennis van de medewerkers of op adviezen van leveranciers.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Er bestaat binnen de organisatie geen formeel beleid dat eisen stelt t.a.v. van het beschermen van informatie met behulp van cryptografie. Cryptografie wordt op afdelingsniveau of in bepaalde bedrijfsprocessen toegepast op basis van individuele expertise. Waar cryptografie gebruikt wordt zal ook documentatie aanwezig zijn. **Evidence**: 1. Kopie van documentatie van gebruikte technologie, inrichting, sleutelbeheer etc.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Er bestaat binnen de organisatie beleid dat eisen stelt t.a.v. van het beschermen van informatie met behulp van cryptografie. **Evidence in aanvulling op 2:** 1. Kopie beleid waarin eisen zijn gesteld voor het beschermen van informatie met behulp van cryptografie; 2. Kopie notulen waaruit blijkt dat het beleid is goedgekeurd door management; 3. Kopie van informatie waaruit blijkt dat de organisatie conform het beleid heeft gewerkt. Denk aan: • Kopie checklist; • Kopie handboek cryptografie (procedures, maatregelen, technieken).	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	Er is een proces ingericht dat waarborgt dat het beleid en de technische en organisatorische eisen m.b.t. cryptografie up-to-date blijven en door de hele organisatie uniform worden toegepast. Dit proces heeft een periodiek karakter, maar wordt ook ingezet bij veranderende omstandigheden (technisch of organisatorisch). Over dit proces wordt op reguliere basis gerapporteerd. **Evidence in aanvulling op 3:** 1. Kopie van de procesbeschrijving; 2. Kopie van de procesrapportage (bijv. na een grote wijziging in infrastructuur of organisatie).	
Volwassenheidsniveau 5 (Geoptimaliseerd)	Het proces is ingericht conform externe best practices. Hierin is opgenomen dat de gebruikte cryptografische algoritmen voor versleuteling als open standaard zijn gedocumenteerd en door onafhankelijke betrouwbare deskundigen zijn getoetst. Het proces maakt onderdeel uit van een gestandaardiseerd en geïntegreerd intern audit en compliance proces. **Evidence in aanvulling op 4:** 1. Kopie waaruit blijkt welke best practice gehanteerd wordt (bijv. welke open standaard of welk Level of Assurance een certificaat moet hebben); 2. Kopie van het interne audit en compliance proces.	

Controledoelstelling 1.9

Cluster: Beleid en organisatie	**ISO 27002 nummer: 10.1.1**
Controledoelstelling: Beleid inzake het gebruik van cryptografische beheersmaatregelen Ter bescherming van informatie behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

1.10 Beleid inzake het gebruik van cryptografische beheersmaatregelen (2)

Cluster: Beleid en organisatie	**ISO 27002 nummer: 10.1.1**
Controledoelstelling: Beleid inzake het gebruik van cryptografische beheersmaatregelen Ter bescherming van informatie zijn er tools of applicaties aanwezig waarmee het beleid voor het gebruik van cryptografische beheersmaatregelen wordt geïmplementeerd.	
Tips: de instelling heeft een of meerder tools aangeschaft in het kader van cryptografische beheersmaatregelen.	
Toelichting: Er is beleid ontwikkeld en geïmplementeerd voor het gebruik van cryptografische beheersmaatregelen voor de bescherming van informatie.	

Niveaus	**Beheersmaatregel (plus evidence)**	**Audit**
Volwassenheidsniveau 1 (Initieel / ad hoc)	Tools of applicaties die informatie beschermen door middel van cryptografie worden op incidentele basis, per geval, aangeschaft.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Er is sprake van een gemeenschappelijke benadering van de tools, voor gelijksoortige toepassingen worden gelijksoortige tools gebruikt., maar die is gebaseerd op oplossingen die door leidende figuren zijn ontwikkeld. Het is niet duidelijk of de tools volledig worden benut en of ze altijd juist worden toegepast (als ze al worden gebruikt). **Evidence:** 1. Kopie toollijst (licentie overzicht software/hardware); 2. Kopie handleidingen voor inrichting en gebruik.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Er zijn tools of applicaties aanwezig die informatie beschermen door middel van cryptografie en deze tools worden ook gebruikt. **Evidence in aanvulling op 2:** 1. Kopie toollijst; 2. Kopie van informatie waaruit het blijkt dat de organisatie tools gebruikt om informatie te beschermen door middel van cryptografie. Te denken aan: • Kopie systeem rapportage; • Kopie productomschrijvingen; • Kopie licentie van de producten (toevoegen bij voorgaande maatregelen).	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	De tools worden ingezet volgens een gestandaardiseerd plan en zijn deels ook geïntegreerd met andere, verwante apparatuur of programmatuur. Er vindt een periodieke evaluatie van de standaard tool set plaats zodat deze up-to-date blijft. Tools worden alleen na formele toestemming (bijvoorbeeld van de CISO) aangeschaft. Bij de inzet van cryptografische producten volgt een afweging van de risico's aangaande locaties, processen en behandelende partijen. Deze werkwijze wordt ook nagevolgd. **Evidence in aanvulling op 3**: 1. Lijst van up-to-date tools met ingangsdata en end-of-life data; 2. Overzicht van geaccordeerde aanschaf/gebruik.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	Op alle afdelingen worden gestandaardiseerde tools gebruikt. De tools zijn volledig geïntegreerd met verwante systemen, zodat processen van begin tot eind worden ondersteund. De toolkeuze is gebaseerd op externe best practices. Rekening houdend met optimale uitwisselingsmogelijkheden met andere organisaties (indien toegestaan). **Evidence in aanvulling op 4:** 1. Overzichtslijst van geïnstalleerde tools in relatie tot de beoogde medewerkers en bedrijfsprocessen voor deze tools; 2. Kopie waaruit blijkt welke best practice gehanteerd wordt (bijv. Welke open standaard of welk Level of Assurance een certificaat moet hebben).	

Controledoelstelling 1.10

Cluster: Beleid en organisatie	**ISO 27002 nummer: 10.1.1**
Controledoelstelling: Beleid inzake het gebruik van cryptografische beheersmaatregelen Ter bescherming van informatie zijn er tools of applicaties aanwezig waarmee het beleid voor het gebruik van cryptografische beheersmaatregelen wordt geïmplementeerd.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

1.11 Verwijdering van bedrijfsmiddelen

Cluster: Beleid en organisatie	**ISO 27002 nummer: 11.2.5**

Controledoelstelling: Verwijdering[3] van bedrijfsmiddelen
Apparatuur, informatie en software behoren niet van de locatie te worden meegenomen zonder voorafgaande goedkeuring.

Tips: apparatuur mag worden meegenomen naar huis. De medewerker gaat akkoord (tekent) met een computerreglement of een Acceptable User Policy (AUP).

Toelichting:
Apparatuur, informatie en programmatuur van de organisatie mogen niet zonder toestemming vooraf van de locatie worden meegenomen. (Er is duidelijk vastgesteld wie vanuit welke rol toestemming hebben om apparatuur mee te nemen of buiten de locatie te gebruiken. Er zijn tijdslimieten en bij inlevering wordt gecontroleerd op de naleving daarvan. Waar nodig wordt geregistreerd wat de locatie verlaat en wanneer het weer wordt teruggebracht.)

Niveaus	Beheersmaatregel (plus evidence)	Audit
Volwassenheidsniveau 1 (Initieel / ad hoc)	Bottom-up wordt bepaald wat wel en wat niet kan worden meegenomen. Er wordt niet altijd een registratie van bijgehouden.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Aan dit onderwerp wordt alleen aandacht besteed in een algemene regeling voor het gebruik van voorzieningen en apparatuur van de organisatie. De feitelijke invulling is per bedrijfsonderdeel verschillend en procedures zijn (al of niet formeel) gebaseerd op de beschikbare kennis en expertise. **Evidence:** 1. Algemene regeling voor het gebruik van voorzieningen en apparatuur van de organisatie.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Apparatuur, informatie en programmatuur van de organisatie worden niet zonder toestemming vooraf van de locatie meegenomen. **Evidence in aanvulling op 2:** 1. Kopie beleid of procedurebeschrijving voor het extern gebruik (of onderhoud) van bedrijfseigendommen (met daarin opgenomen dat apparatuur, informatie en programmatuur van de organisatie niet zonder toestemming vooraf van de locatie mogen worden meegenomen); 2. Kopie geautoriseerd formulier voor het extern gebruik (of onderhoud) van bedrijfseigendommen.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	Het beleid en/of de procedures worden periodiek geëvalueerd. Er wordt gecontroleerd en gestuurd op naleving. **Evidence in aanvulling op 3:** 1. Document waaruit evaluatie blijkt (versiebeheer); 2. Document waaruit blijkt dat controle / naleving plaatsvindt.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	Er wordt gebruik gemaakt van best practices. **Evidence in aanvulling op 4:** 1. Voorbeeld van best practice.	

[3] Met "verwijdering" wordt bedoeld het "gebruik buiten de instelling".

Controledoelstelling 1.11

Cluster: Beleid en organisatie	**ISO 27002 nummer: 11.2.5**
Controledoelstelling: Verwijdering van bedrijfsmiddelen Apparatuur, informatie en software behoren niet van de locatie te worden meegenomen zonder voorafgaande goedkeuring.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

1.12 Beleid en procedures voor informatietransport

Cluster: Beleid en organisatie	**ISO 27002 nummer: 13.2.1**
Controledoelstelling: Beleid en procedures voor informatietransport Ter bescherming van het informatietransport, dat via alle soorten communicatiefaciliteiten verloopt, behoren formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht te zijn.	
Tips: de instelling heeft een beleid vastgesteld waarin bepaald wordt onder welke voorwaarden er informatie met andere partijen mag worden uitgewisseld. (zie Bijlage 1 Beleid en procedures voor informatietransport).	
Toelichting: Er behoren formeel beleid, formele procedures en formele beheersmaatregelen te zijn vastgesteld om de uitwisseling van informatie via het gebruik van alle typen communicatiefaciliteiten te beschermen. (De uitwisseling tussen organisaties is gebaseerd op formeel uitwisselingsbeleid, in lijn met uitwisselingsovereenkomsten en in overeenstemming met relevante wetgeving. Er zijn procedures en normen vastgesteld ter bescherming van informatie die wordt uitgewisseld.)	

Niveaus	**Beheersmaatregel (plus evidence)**	**Audit**
Volwassenheidsniveau 1 (Initieel / ad hoc)	Er zijn geen richtlijnen voor het beschermen van de uitwisseling van informatie via verschillende communicatiefaciliteiten. Iedere vraag wordt ad-hoc opgelost.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Er is sprake van enige richtlijnen binnen bepaalde bedrijfsonderdelen of bedrijfsprocessen waarbij een vraag die herhaaldelijk terugkomt op gelijke wijze wordt opgelost. **Evidence:** 1. Kopie afdelingsrichtlijn of beschrijving uitwisselingsproces.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Er is formeel beleid en er zijn formele procedures en formele beheersmaatregelen vastgesteld om de uitwisseling van informatie via het gebruik van alle typen communicatiefaciliteiten te beschermen. **Evidence in aanvulling op 2:** 1. Kopie beleid, procedurebeschrijving met beheersingsmaatregelen voor informatie-uitwisseling (geldt voor alle type communicatiefaciliteiten); 2. Kopie Notulen dat het beleid, procedurebeschrijving is goedgekeurd door (gedelegeerd) bestuur; 3. Kopie van informatie waaruit blijkt dat de organisatie conform het beleid heeft uitgevoerd. Denk aan: • Kopie waarin men aantoont dat ze gebruik maken van cryptografische technieken; • Kopie campagne, flyers, e-mails of cursussen waaruit blijkt dat het personeel weet of eraan herinnerd wordt hoe en wanneer ze passende voorzorgen behoren te nemen; 4. Waarneming ter plaatse.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	Er is een gedegen en volledig proces, en er worden interne best practices toegepast. De normen voor ontwikkeling en onderhoud van proces en procedures worden overgenomen en nageleefd. **Evidence in aanvulling op 3:** 1. Rapportage over periodieke review van het beleid, (bijv. toetsing of gebruikte technieken zoals encryptie nog up-to-date[4] zijn).	
Volwassenheidsniveau 5 (Geoptimaliseerd)	De procesdocumentatie is geëvolueerd tot een stelsel van geautomatiseerde workflows. Processen, beleid en procedures zijn gestandaardiseerd en er worden externe best practices en normen toegepast. **Evidence, in aanvulling op 4:** 1. Voorbeeld gestandaardiseerde workflow; best practice.	

[4] Zie bijvoorbeeld: Algorithms, key size and parameters report 2014 en Study on cryptographic protocols van ENISA.

Controledoelstelling 1.12

Cluster: Beleid en organisatie	**ISO 27002 nummer: 13.2.1**
Controledoelstelling: Beleid en procedures voor informatietransport Ter bescherming van het informatietransport, dat via alle soorten communicatiefaciliteiten verloopt, behoren formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht te zijn.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

1.13 Overeenkomsten over informatietransport

Cluster: Beleid en organisatie	**ISO 27002 nummer: 13.2.2**

Controledoelstelling: Overeenkomsten over informatietransport
Overeenkomsten behoren betrekking te hebben op het beveiligd transporteren van bedrijfsinformatie tussen de organisatie en externe partijen.

Tips: er worden contracten en bewerkersovereenkomsten met leveranciers afgesloten waarmee informatie wordt uitgewisseld. Het betreft hier zowel het transport van fysieke documenten (aangetekende stukken) als van digitale informatie.

Toelichting:
Er behoren overeenkomsten te worden vastgesteld voor de uitwisseling van informatie en programmatuur tussen de organisatie en externe partijen.

Niveaus	Beheersmaatregel (plus evidence)	Audit
Volwassenheidsniveau 1 (Initieel / ad hoc)	Op ad-hoc basis worden afspraken gemaakt met externe organisaties over het uitwisselen van informatie.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Met gelijksoortige externe organisaties worden gelijksoortige afspraken gemaakt m.b.t. uitwisseling van informatie. Er is nog geen sprake van een formeel ondertekende overeenkomst.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Er zijn overeenkomsten vastgesteld voor de uitwisseling van informatie en programmatuur tussen de organisatie en externe partijen. **Evidence:** 1. Kopie van de getekende overeenkomst voor de uitwisseling van informatie en programmatuur tussen de organisatie en externe partijen; 2. Kopie beleid of procedurebeschrijving voor de uitwisseling van informatie en programmatuur tussen de organisatie en externe partijen.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	Er vindt regelmatig controle plaats op het naleven van de overeenkomsten. **Evidence in aanvulling op 3:** 1. Controlerapportage.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	Overeenkomsten zijn geëvolueerd naar standaarden die gebaseerd zijn op externe best practices en worden voor verlenging tijdig geëvalueerd en zo nodig bijgesteld. **Evidence in aanvulling op 4:** 1. Overzicht van op dat moment gehanteerde externe best practices (bijv. standaard datacontract, normenkader brancheorganisatie).	

Controledoelstelling 1.13

Cluster: Beleid en organisatie	**ISO 27002 nummer: 13.2.2**
Controledoelstelling: Overeenkomsten over informatietransport Overeenkomsten behoren betrekking te hebben op het beveiligd transporteren van bedrijfsinformatie tussen de organisatie en externe partijen.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

1.14 Analyse en specificatie van informatiebeveiligingseisen

Cluster: Beleid en organisatie	**ISO 27002 nummer: 14.1.1**

Controledoelstelling: Analyse en specificatie van informatiebeveiligingseisen
De eisen die verband houden met informatiebeveiliging behoren te worden opgenomen in de eisen voor nieuwe informatiesystemen of voor uitbreidingen van bestaande informatiesystemen.

Tips: er is beleid dat gebruik kan worden in een programma van eisen bij een aanbesteding. BIV en PIA kunnen hier een onderdeel van zijn. Aanbesteding en life cycle. Systeemeigenaar (proceseigenaar) is verantwoordelijk.
De ICT afdeling is belast met de implementatie. Zie ook hoofdstuk 3.1.5 Informatiebeveiliging in projectbeheer

Toelichting:
In bedrijfseisen voor nieuwe informatiesystemen of uitbreidingen van bestaande informatiesystemen behoren ook eisen voor beveiligingsmaatregelen te worden opgenomen. (Beveiligingseisen en maatregelen zijn een afspiegeling van de waarde van de informatie voor de organisatie, en de mogelijke schade als gevolg van falen of ontbreken van beveiliging.)

Niveaus	Beheersmaatregel (plus evidence)	Audit
Volwassenheidsniveau 1 (Initieel / ad hoc)	Het opnemen van beveiligingsmaatregelen in de bedrijfseisen voor nieuwe of bestaande systemen is geen vanzelfsprekendheid.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Op basis van eerdere ervaringen (voorgedane incidenten), algemene kennis en intuïtie worden soms beveiligingseisen meegenomen in de bedrijfseisen voor een nieuw of bestaand systeem. De feitelijke invulling is per bedrijfsonderdeel verschillend, gebaseerd op de beschikbare kennis en expertise. **Evidence:** 1. Een voorbeeld van een beveiligingsparagraaf in een inrichtingsdocument of change-aanvraag.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	In bedrijfseisen voor nieuwe informatiesystemen of uitbreidingen van bestaande informatiesystemen zijn ook eisen voor beveiligingsmaatregelen opgenomen. **Evidence in aanvulling op 2:** 1. Kopie beleid waarin bedrijfseisen en beveiligingsmaatregelen voor nieuwe informatiesystemen of uitbreiding van bestaande informatiesystemen zijn beschreven; 2. Kopie van het vaste programma van eisen t.a.v. beveiliging; 3. Kopie van informatie waaruit blijkt dat de organisatie conform de vaste programma uitvoeren. Te denken aan: • Kopie checklist voor het beoordelen van bedrijfseisen bij aanschaf of uitbreiding.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	Er is een proces ingericht dat waarborgt dat de beveiligingseisen voor informatiesystemen up-to-date blijven. Dit proces heeft een periodiek karakter, maar wordt ook ingezet bij veranderende omstandigheden (technisch of organisatorisch). Over dit proces wordt op reguliere basis gerapporteerd. **Evidence in aanvulling op 3:** 1. Kopie van de procesbeschrijving; 2. Kopie van de procesrapportage (bijv. na een veranderende omstandigheid).	
Volwassenheidsniveau 5 (Geoptimaliseerd)	Het proces is ingericht conform externe best practices en maakt deel uit van een gestandaardiseerd en geïntegreerd intern audit en compliance proces. **Evidence in aanvulling op 4:** 1. De eisen aan nieuwe systemen zijn gebaseerd op best practices uit de sector en zijn gekoppeld aan vastgestelde maatregelen die in de organisatie gebruikt worden.	

Controledoelstelling 1.14

Cluster: Beleid en organisatie	**ISO 27002 nummer: 14.1.1**
Controledoelstelling: Analyse en specificatie van informatiebeveiligingseisen De eisen die verband houden met informatiebeveiliging behoren te worden opgenomen in de eisen voor nieuwe informatiesystemen of voor uitbreidingen van bestaande informatiesystemen.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

1.15 Opnemen van beveiligingsaspecten in leveranciersover eenkomsten

Cluster: Beleid en organisatie	**ISO 27002 nummer: 15.1.2**

Controledoelstelling: Opnemen van beveiligingsaspecten in leveranciersovereenkomsten
Alle relevante informatiebeveiligingseisen behoren te worden vastgesteld en overeengekomen met elke leverancier die toegang heeft tot IT-infrastructuurelementen ten behoeve van de informatie van de organisatie, of deze verwerkt, opslaat, communiceert of biedt.

Tips: Toegang van systemen door externe medewerkers op het netwerk op de eigen locatie.
Beveiligingsaspecten in de meest brede zin.

a) Omschrijving van de informatie die moet worden verschaft of toegankelijk moet worden en van de methoden om de informatie te verschaffen of toegankelijk te maken;
b) Classificatie van de informatie in overeenstemming met het classificatieschema van de organisatie (zie hoofdstuk 3.1.8); zo nodig ook mapping tussen het eigen schema van de organisatie en het schema van de leverancier;
c) Wettelijke en regelgevende eisen, met inbegrip van gegevensbescherming, rechten van intellectueel eigendom en auteursrecht, en een beschrijving van hoe wordt gewaarborgd dat eraan wordt voldaan;
d) Verplichting van elke contractuele partij om een overeengekomen aantal beheersmaatregelen te implementeren, waaronder toegangsbeveiliging, prestatiebeoordeling, monitoren, rapporteren en auditen;
e) De regels van aanvaardbaar gebruik van informatie, met inbegrip van onaanvaardbaar gebruik indien noodzakelijk;
f) Hetzij een expliciete lijst van leverancierspersoneel dat geautoriseerde toegang heeft of bevoegd is informatie van de organisatie te ontvangen, hetzij procedures of voorwaarden voor autorisatie en het intrekken van de autorisatie, tot toegang tot of ontvangst van informatie van de organisatie door leverancierspersoneel;
g) Beleidsregels betreffende informatiebeveiliging die relevant zijn voor het specifieke contract;
h) Eisen voor incidentbeheer en -procedures (in het bijzonder notificatie en samenwerking tijdens herstel van het incident);
i) Trainings- en bewustzijnseisen voor specifieke procedures en informatiebeveiligingseisen, bijv. voor incidentresponsprocedures, autorisatieprocedures;
j) Relevante regelgeving voor onderaanneming, met inbegrip van de beheersmaatregelen die moeten worden geïmplementeerd;
k) Relevante overeenkomstpartners, met inbegrip van een contactpersoon voor aangelegenheden betreffende informatiebeveiliging;
l) Indien relevant, screeningseisen voor leverancierspersoneel, met inbegrip van verantwoordelijkheden voor het uitvoeren van de screening en notificatieprocedures indien de screening niet is voltooid of de resultaten aanleiding geven tot twijfel of bezorgdheid;
m) Het recht om de processen en beheersmaatregelen van de leverancier in verband met de overeenkomst te auditen;
n) Procedures voor het oplossen van defecten en conflicten;
o) Verplichting van de leverancier om periodiek een onafhankelijk rapport te verstrekken over de doeltreffendheid van beheersmaatregelen, en overeenkomst over tijdige correctie van relevante kwesties die in het rapport aan de orde worden gesteld;
p) Verplichting van de leverancier om te voldoen aan de beveiligingseisen van de organisatie.

Toelichting:
In overeenkomsten met derden waarbij toegang tot, het verwerken van, communicatie van of beheer van informatie of IT-voorzieningen van de organisatie, of toevoeging van producten of diensten aan IT-voorzieningen waarbij sprake is van toegang, behoren alle relevante beveiligingseisen te zijn opgenomen. (Waarborgen dat geen misverstanden bestaan tussen organisatie en derde partij, de organisatie vergewist zich ervan dat de wederzijdse aansprakelijkheid voldoende is afgedekt.)

Niveaus	**Beheersmaatregel (plus evidence)**	**Audit**
Volwassenheidsniveau 1 (Initieel / ad hoc)	Overeenkomsten met derden (zie boven) worden ad hoc beoordeeld door verschillende spelers binnen de organisatie. Een beveiligingsparagraaf is geen vaste praktijk.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Met derden worden vaak voor vergelijkbare activiteiten ook vergelijkbare schriftelijke afspraken gemaakt, waarin relevante beveiligingseisen zijn opgenomen, maar deze zijn grotendeels intuïtief vanwege het individuele karakter van de expertise. Er kan sprake zijn van enige documentatie en een zeker begrip van beleid en procedures. **Evidence:** 1. Kopie van (enkele) schriftelijke afspraken met derden waaruit blijkt dat als er sprake is van toegang, de afspraken voorzien in alle relevante beveiligingseisen.	

Volwassenheidsniveau 3 (Gedefinieerd proces)	In overeenkomsten met derden waarbij toegang tot, het verwerken van, communicatie van of beheer van informatie of IT-voorzieningen van de organisatie, of toevoeging van producten of diensten aan IT-voorzieningen waarbij sprake is van toegang, zijn alle relevante beveiligingseisen opgenomen. **Evidence in aanvulling op 2:** 1. Kopie beleid waarin is opgenomen dat in overeenkomsten met derden waarbij sprake is van het verwerken van, communicatie van of beheer van informatie of IT-voorzieningen van de organisatie, of toevoeging van producten of diensten aan IT-voorzieningen waarbij sprake is van toegang, relevante beveiligingseisen worden beoordeeld en opgenomen; 2. Kopie voorbeeld overeenkomst om aan te tonen dat het is opgenomen.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	Er is een beheersproces, waarbij alle overeenkomsten met derden (etc.) worden beoordeeld door een vast team van deskundigen vanuit relevant perspectief. Niet alleen bij afsluiten, maar ook periodiek worden de beveiligingseisen gereviewd en wordt het passend zijn van maatregelen opnieuw afgezet tegen gewijzigde omstandigheden, de stand der techniek, aanvullende (wettelijke) eisen e.d., tenminste bij verlenging van contracten. **Evidence in aanvulling op 3:** 1. Procesbeschrijving, inkoopbeleid, sourcing-strategie e.d.; 2. Documentatie dat inderdaad review heeft plaatsgevonden.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	Het proces is ingericht conform externe best practices en maakt onderdeel uit van een gestandaardiseerd en geïntegreerd intern audit en compliance proces. **Evidence in aanvulling op 4:** 1. Kopie van het interne audit en compliance proces; 2. Beleidsstuk of visie op contractmanagement; 3. Voorbeeld(en) van toepaste best practices.	

Controledoelstelling 1.15

Cluster: Beleid en organisatie	**ISO 27002 nummer: 15.1.2**
Controledoelstelling: Opnemen van beveiligingsaspecten in leveranciersovereenkomsten Alle relevante informatiebeveiligingseisen behoren te worden vastgesteld en overeengekomen met elke leverancier die toegang heeft tot IT-infrastructuurelementen ten behoeve van de informatie van de organisatie, of deze verwerkt, opslaat, communiceert of biedt.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

1.16 Toeleveringsketen van informatie- en communicatie technologie

Cluster: Beleid en organisatie	**ISO 27002 nummer: 15.1.3**
Controledoelstelling: Toeleveringsketen van informatie- en communicatietechnologie Overeenkomsten met leveranciers behoren eisen te bevatten die betrekking hebben op de informatiebeveiligingsrisico's in verband met de toeleveringsketen van de diensten en producten op het gebied van informatie- en communicatietechnologie.	
Tips: in de bewerkersovereenkomst (privacy bijsluiter), als bijlage bij het contract, moet ook verwezen worden naar subbewerkers. Bovendien moet er periodiek een terugkoppeling gepresenteerd worden in een SLR (Service Level Rapportage) op tenminste de bedrijfskritische applicaties. Zie ook "Leidraad Informatiebeveiligingsbeleid XX-V2.0".	
Toelichting: Met leveranciers die toegang hebben tot bedrijfsmiddelen van de organisatie (applicaties, systemen en/of gegevens) dienen in overeenkomsten eisen gesteld te worden aan toeleveranciers en/of samenwerkingspartners van deze leverancier. De toeleveringsketen van informatie- en communicatietechnologie omvat eveneens dienstverlening op het gebied van 'cloud computing'.	

Niveaus	**Beheersmaatregel (plus evidence)**	**Audit**
Volwassenheidsniveau 1 (Initieel / ad hoc)	Afspraken over de toeleveringsketen van leveranciers worden op ad-hoc basis gemaakt.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	In overeenkomsten met leveranciers worden regelmatig eisen gesteld aan leveranciers in de toeleveringsketen, echter deze zijn doorgaans gebaseerd op eerdere overeenkomsten of samenwerkingen. Er is nog geen sprake van een formeel vastgestelde set eisen of modelcontracten en op naleving wordt niet structureel gestuurd. **Evidence:** 1. Gespreksverslagen met inkopers en/of service level managers; 2. Kopieën van overeenkomsten.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	In overeenkomsten met leveranciers worden eenduidige eisen gesteld aan leveranciers in de toeleveringsketen. De eisen zijn formeel vastgesteld, vastgelegd in overeenkomsten en over naleving worden afspraken gemaakt. **Evidence in aanvulling op 2:** 1. Kopieën van eisen set(s); 2. Kopieën modelcontracten; 3. Verslagen van Service Level besprekingen.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	Er vindt regelmatig controle plaats op het naleven van de overeenkomsten. **Evidence in aanvulling op 3:** 1. Overzichten van toeleveranciers en onderaannemers; 2. Rapportages waaruit compliance van producten en diensten van toeleveranciers en onderaannemers blijkt.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	Overeenkomsten zijn geëvolueerd naar standaarden die gebaseerd zijn op in- en externe best practices en worden voor verlenging tijdig geëvalueerd en zo nodig bijgesteld. **Evidence in aanvulling op 4:** 1. Overzicht van op dat moment gehanteerde externe best practices (zoals standaard datacontract normenkader brancheorganisatie).	

Controledoelstelling 1.16

Cluster: Beleid en organisatie	**ISO 27002 nummer: 15.1.3**
Controledoelstelling: Toeleveringsketen van informatie- en communicatietechnologie Overeenkomsten met leveranciers behoren eisen te bevatten die betrekking hebben op de informatiebeveiligingsrisico's in verband met de toeleveringsketen van de diensten en producten op het gebied van informatie- en communicatietechnologie.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

1.17 Verantwoordelijkheden en procedures

Cluster: Beleid en organisatie	**ISO 27002 nummer: 16.1.1**
Controledoelstelling: Verantwoordelijkheden en procedures Er zijn leidinggevende en -procedures vastgesteld om een snelle, doeltreffende en ordelijke respons op informatiebeveiligingsincidenten te bewerkstelligen.	
Tips: zijn de taken die te maken hebben met informatiebeveiliging opgenomen in de functiebeschrijving van de leidinggevende.	
Toelichting: Er behoren leidinggevende verantwoordelijkheden en procedures te worden vastgesteld om een snelle, doeltreffende en ordelijke reactie op informatiebeveiligingsincidenten te bewerkstelligen. (Er zijn dwingende verantwoordelijkheden en procedures vastgesteld om een snelle, doeltreffende en ordelijke reactie op informatiebeveiligingsincidenten te bewerkstelligen.)	

Niveaus	**Beheersmaatregel (plus evidence)**	**Audit**
Volwassenheidsniveau 1 (Initieel / ad hoc)	Informatiebeveiligingsincidenten worden ad-hoc afgehandeld. Er zijn geen verantwoordelijkheden belegd.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Er wordt verantwoordelijkheid genomen voor het acteren op een informatiebeveiligingsincident maar deze verantwoordelijkheid is niet altijd formeel duidelijk vastgelegd. Bij problemen/escalaties is echter vaak onduidelijk wie er verantwoordelijk is, en is men geneigd de schuld door te schuiven.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Er zijn leidinggevende verantwoordelijkheden en procedures vastgesteld om een snelle, doeltreffende en ordelijke reactie op informatiebeveiligingsincidenten te bewerkstelligen. **Evidence:** 1. Kopie procedurebeschrijving voor het ontvangen en behandelen van informatiebeveiligingsincidenten; 2. Kopie functieprofielen voor het aantonen van de verantwoordelijkheid; 3. Kopie van informatie waaruit blijkt dat de organisatie conform de procedure uitvoert. Te denken aan: • Kopie laatste 2 incidentenrapportages (versienummer + datum); • Kopie 2 recente incidenten meldingen.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	Niet alleen de verantwoordelijkheden ten aanzien van het reageren op een incident zijn vastgelegd maar ook de volledige bevoegdheden voor het kunnen dragen van deze verantwoordelijkheid zijn toegekend. Met vaste regelmaat wordt over de afgelopen beveiligingsincidenten gerapporteerd, inclusief afhandeling en eventueel escalatie. De directie gebruikt de rapportage als instrument om de incidentafhandeling te verbeteren. **Evidence in aanvulling op 3:** 1. Kopie van de organisatiestructuur en geaccordeerde mandatenregeling of RASCI[5]-schema waaruit de TVB[6]'s van de betrokken medewerkers blijken; 2. Eigen waarneming dat de rapportage beveiligingsincidenten bestaat.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	Verantwoordelijkheidsstructuur en de daarbij toegedeelde bevoegdheden t.a.v. het reageren op beveiligingsincidenten wordt door de hele organisatie gekend en erkend. **Evidence in aanvulling op 4:** 1. Eigen waarneming (steekproef) over bekendheid met de materie bij de medewerkers.	

[5] RASCI: Responsible, Accountable, Support, Consulted, Informed.
[6] TVB's: Taken, Bevoegdheden en Verantwoordelijkheden.

Controledoelstelling 1.17

Cluster: Beleid en organisatie	**ISO 27002 nummer: 16.1.1**
Controledoelstelling: Verantwoordelijkheden en procedures Er zijn leidinggevende en -procedures vastgesteld om een snelle, doeltreffende en ordelijke respons op informatiebeveiligingsincidenten te bewerkstelligen.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

1.18 Rapportage van informatiebeveiligingsgebeurtenissen

Cluster: Beleid en organisatie	**ISO 27002 nummer: 16.1.2**
Controledoelstelling: Rapportage van informatiebeveiligingsgebeurtenissen Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd.	
Tips: er is een goede escalatieprocedure beschikbaar.	
Toelichting: Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd. (Er is een procedure voor het rapporteren van beveiligingsgebeurtenissen vastgesteld, in combinatie met een reactie- en escalatieprocedure voor incidenten, waarin de handelingen worden vastgelegd die moeten worden genomen na het ontvangen van een rapport van een beveiligingsincident.)	

Niveaus	**Beheersmaatregel (plus evidence)**	**Audit**
Volwassenheidsniveau 1 (Initieel / ad hoc)	Incidenten worden soms, en vaak achteraf gemeld.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Incidenten worden gemeld via verschillende formele en informele kanalen. Er is geen formele procedure voor het melden en registreren van incidenten en melden van integriteitsschendingen, maar binnen afdelingen of bepaalde bedrijfsprocessen kunnen wel afspraken gemaakt zijn. Deze zijn gebaseerd op individuele kennis en expertise en soms op beschikbare hulpmiddelen. **Evidence:** 1. Kopie procedurebeschrijving voor het melden en registreren van incidenten op een afdeling of in een bepaald bedrijfsproces.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Er is een vaste procedure voor het melden en registreren van incidenten. 0 **Evidence in aanvulling op 2:** 1. Kopie beleid of procedurebeschrijving voor het melden en registreren van incidenten; 2. Kopie van informatie dat de organisatie conform het beleid of procedurebeschrijving hanteert. Te denken aan: • Kopie twee meest recente rapportages van een informatiebeveiligingsgebeurtenis.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	Op reguliere momenten worden over de afgelopen beveiligingsincidenten gerapporteerd, inclusief kentallen over reacties en escalaties. De directie gebruikt de rapportage als instrument om het incidentenproces te verbeteren. Ervaringen uit de praktijk kunnen eveneens leiden tot aanpassing van de procedures. **Evidence in aanvulling op 3:** 1. Eigen waarneming dat de rapportage beveiligingsincidenten bestaat.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	De incident meldingsprocedure is gebaseerd op best practices en breed in gebruik. De procedure wordt geregeld geëvalueerd en zo nodig bijgesteld. De rapportage maakt onderdeel uit van een gestandaardiseerd en geïntegreerd intern audit en compliance proces. **Evidence in aanvulling op 4:** 1. Kopie waaruit blijkt welke best practice gehanteerd wordt (bijv. ITIL); 2. Eigen waarneming van (communicatie) hulpmiddelen (stickers, pop-up-berichten etc.) die de brede bekendheid ondersteunen; 3. Kopie van het interne audit en compliance proces.	

Controledoelstelling 1.18

Cluster: Beleid en organisatie	**ISO 27002 nummer: 16.1.2**
Controledoelstelling: Rapportage van informatiebeveiligingsgebeurtenissen Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

1.19 Beschermen van registraties

Cluster: Beleid en organisatie	**ISO 27002 nummer: 18.1.3**
Controledoelstelling: Beschermen van registraties Registraties behoren in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfseisen te worden beschermd tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave.	
Tips: hanteer het document met afgesproken bewaartermijnen binnen een instelling (**D**ocumentair **S**tructuur**p**lan - DSP). Dataportabiliteit is een voorwaarde. Fysieke documenten vallen buiten de scope.	
Toelichting: Om registraties te beschermen worden richtlijnen verstrekt voor het bewaren, opslaan, behandelen en verwijderen van registraties en informatie, wordt een bewaarschema opgesteld en wordt een inventarisoverzicht van bronnen van belangrijke informatie bijgehouden.	

Niveaus	**Beheersmaatregel (plus evidence)**	**Audit**
Volwassenheidsniveau 1 (Initieel / ad hoc)	De bescherming van registraties vindt afzonderlijk en ad hoc plaats, al naar gelang de kennis en ervaring van betrokkenen bij die registraties.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Er zijn enige richtlijnen, bewaarschema's en overzichten van bronnen door houders van registraties vastgelegd. Mogelijk vindt deling van kennis plaats en worden ervaringen gedeeld. Geformaliseerd (en structureel) is dit nog niet, het initiatief ligt bij betrokkenen. **Evidence:** 1. Gespreksverslagen met betrokkenen; 2. Kopieën van richtlijnen, bewaarschema's en informatiebronnen.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	De organisatie heeft verantwoordelijkheden voor bescherming van registratie toegekend, richtlijnen en bewaarschema's voor alle registraties vastgesteld en gecommuniceerd naar betrokkenen. **Evidence in aanvulling op 2:** 1. Kopie functiebeschrijvingen betrokkenen; 2. Kopie vastgestelde richtlijnen en bewaarschema's; 3. Kopie communicatiemiddelen waaruit bekendmaking blijkt.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	De vastgestelde richtlijnen en bewaarschema's zijn zichtbaar in gebruik, betrokkenen zijn aantoonbaar bekend met hun rol. De registraties zijn uitputtend geïnventariseerd en van iedere registratie is bekend in hoeverre zij verwerkt worden conform de richtlijnen en bewaarschema's. **Evidence in aanvulling op 3:** 1. Kopie lijst inventarisaties; 2. Kopieën beoordeling compliance; 3. Kopieën actielijsten.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	De bescherming van alle registraties voldoen op ieder moment aan de daaraan gestelde eisen, inventarisoverzichten van informatiebronnen zijn op ieder moment actueel. De compliance is (voor meerdere perioden) door onafhankelijke beoordelaars vastgesteld. **Evidence in aanvulling op 4:** 1. Kopieën van archieflijsten; 2. Kopieën van volledige inventarisoverzichten; 3. Kopieën beheerproces cryptografische sleutels (indien archieven versleuteld zijn); 4. Kopieën van verslagen waaruit toegankelijkheid van data blijkt (leesbaarheid van media en gegevensformaat); 5. Kopieën onafhankelijke compliance rapportages.	

Controledoelstelling 1.19

Cluster: Beleid en organisatie	**ISO 27002 nummer: 18.1.3**
Controledoelstelling: Beschermen van registraties Registraties behoren in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfseisen te worden beschermd tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

1.20 Privacy en bescherming van persoonsgegevens

Cluster: Beleid en organisatie	**ISO 27002 nummer: 18.1.4**	
Controledoelstelling: Privacy en bescherming van persoonsgegevens Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.		
Tips: privacy kan onderdeel zijn van het informatiebeveiligingsbeleid zoals opgenomen in hoofdstuk 3.1.1.		
Toelichting: De bescherming van gegevens en privacy wordt bewerkstelligd overeenkomstig relevante wetgeving, voorschriften en (indien van toepassing) contractuele bepalingen.		
Niveaus	**Beheersmaatregel (plus evidence)**	**Audit**
Volwassenheidsniveau 1 (Initieel / ad hoc)	Er is geen beleid voor bescherming van persoonsgegevens. Voor sommige systemen zijn ad hoc maatregelen genomen.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Er zijn afspraken over maatregelen maar die zijn niet formeel vastgelegd. Ze zijn specifiek ingericht op afdelingsniveau of in een bepaald bedrijfsproces en zijn intuïtief, gebaseerd op individuele kennis en expertise. Evidence (indien beschikbaar): 1. Inrichtings- of procesdocumenten waaruit blijkt dat er specifieke maatregelen genomen zijn.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Er is beleid vastgesteld en dit wordt nageleefd. **Evidence:** 1. Kopie goedgekeurde beleid voor bescherming van persoonsgegevens; 2. Kopie van informatie waaruit blijkt dat het beleid met de medewerkers zijn gecommuniceerd (te denken aan flyers, presentaties); 3. Kopie (/referentie naar) nationale wet- en regelgeving zodat aantoonbaar is dat de organisatie de wet heeft gehanteerd (cross-reference tussen registratie en regelgeving.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	Er is een proces ingericht wat de toepassing van het beleid waarborgt. Daarin wordt onder andere zorg gedragen voor actualisatie van: • Welk CvB lid eindverantwoordelijk is; • Bij welke functionaris de rol/functie van Functionaris voor de Gegevensbescherming (FG) is belegd; • Wie de gegevensverwerkers zijn; • Hoe betrokkenen in staat zijn invloed uit te oefenen op wat er met hun persoonsgegevens gebeurt en hoe daarop wordt toegezien. **Evidence in aanvulling op 3:** 1. Kopie van een actueel overzicht van de procesonderwerpen.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	Het proces en het privacy beleid is ingericht conform externe best practices. Het beleid wordt periodiek geëvalueerd en zo nodig bijgesteld. Men houdt in het proces in de gaten wanneer gebruik, regels en voorschriften veranderen en past het beleid hierop aan. Het proces maakt onderdeel uit van een gestandaardiseerd en geïntegreerd intern audit en compliance proces. **Evidence in aanvulling op 4:** 1. Kopie waaruit blijkt welke best practices gehanteerd worden (bijv. het richtsnoer informatiebeveiliging van het CBP, aangevuld met branche specifieke afspraken); 2. Kopie van het interne audit en compliance proces.	

Controledoelstelling 1.20

Cluster: Beleid en organisatie	**ISO 27002 nummer: 18.1.4**
Controledoelstelling: Privacy en bescherming van persoonsgegevens Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

1.21 Scheiding van taken

Cluster: Beleid en organisatie	**ISO 27002 nummer: 6.1.2**

Controledoelstelling: Scheiding van taken
Conflicterende taken en verantwoordelijkheden behoren te worden gescheiden om de kans op onbevoegd of onbedoeld wijzigen of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.

Tips: scheiden van taken op basis van functies en rollen. Transparantie op het gebied van OTAP en autorisatiematrix. Waarborgen van functiescheiding.

Toelichting:
Conflicterende taken en verantwoordelijkheden zijn gescheiden om de kans op onbevoegd of onbedoeld wijzigen of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.
Binnen de (ICT-) organisatie wordt (voor zover mogelijk) functiescheiding tussen gebruik, ontwikkelen/aanschaffen, beheren en beoordelen van functioneren van systemen gehandhaafd. Autorisaties van gebruikers worden ingeregeld op need-to-know/need-to-act basis vanuit het te ondersteunen bedrijfsproces.

Niveaus	Beheersmaatregel (plus evidence)	Audit
Volwassenheidsniveau 1 (A hoc / initieel)	Verantwoordelijkheid en verantwoording zijn niet Gedefinieerd. Medewerkers nemen op eigen initiatief en op reactieve wijze verantwoordelijkheid voor kwesties. Systemen worden op ad hoc basis aangeschaft geïmplementeerd, beheerd en onderhouden. Er is geen helderheid over wie mag aanschaffen/ontwikkelen, wie beslist over ingebruikname, het feitelijke gebruik, welke beheerinspanning redelijk is en wie aangesproken mag worden op disfunctioneren van een systeem.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Men neemt verantwoordelijkheid en wordt ter verantwoording geroepen, zelfs als dit niet formeel is geregeld. Bij problemen is echter vaak onduidelijk wie er verantwoordelijk is, en men is geneigd de schuld door te schuiven. Gebruikers, ontwikkelaars, beheerders voelen verantwoordelijkheid voor het goed en veilig laten functioneren van een systeem, contacten met eindgebruikers zijn informeel, er worden afspraken gemaakt maar niet vastgelegd. Praktisch zijn er aandachtsgebieden verdeeld, maar is er geen scherpe taakverdeling tussen gebruikers, ontwikkelaars en beheerders (of zij zijn een en dezelfde persoon).	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Er is een formele verantwoordelijkheid- en verantwoordingsstructuur en het is duidelijk wie waar verantwoordelijk voor is. Die persoon heeft echter vaak niet de volledige bevoegdheid om zijn verantwoordelijkheden volledig te kunnen uitoefenen. Afspraken over verantwoordelijkheden gebruikers, ontwikkelaars en beheerders zijn vastgelegd en gecommuniceerd, de communicatie tussen de verschillende belanghebbenden is in procedures en overlegstructuur geregeld. **Evidence:** 1. Procedure beschrijving ontwikkeling/onderhoud/gebruik systeem, waaronder vastgelegde scheiding tussen technisch beheer, applicatiebeheer en functioneel beheer. 2. Verslagen overleggen gebruikers/ontwikkelaars, gebruikers/beheerders, ontwikkelaars/beheerders, etc. 3. Door systeem- en proceseigenaar vastgestelde autorisatieschema's (zowel beheerdersautorisaties als functionele gebruikersautorisaties). 4. Recent overzicht actuele autorisaties.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	Er is een aanvaarde structuur voor verantwoordelijkheid en verantwoording en de betreffende personen kunnen aan hun verantwoordelijkheden voldoen. Positieve actie wordt stelselmatig beloond om de betrokkenen te motiveren. De werking van een systeem wordt stelselmatig geëvalueerd met gebruikers, beheerders en ontwikkelaars. Dit leidt tot planmatige ontwikkeling en onderhoud van het systeem mede op basis van de behoeften van de gebruikers. Zeggenschap en verantwoordelijkheid is voor alle partijen helder in dit proces. Autorisatiesschema's worden periodiek geëvalueerd en geaccordeerd door de systeem- en proceseigenaar. **Evidence in aanvulling op 3:** 1. Vastgelegde afspraken over ontwikkel/beheer/gebruik in het kader van een verbetertraject. 2. Evaluatieverslagen van betrokken groepen.	

	3. Afschrift van een recent door de systeem- en proceseigenaar geaccordeerde autorisatieschema's.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	De verantwoordelijken hebben de vrijheid om besluiten en maatregelen te nemen. De verantwoordelijkheidsstructuur is tot op het laagste niveau ingebed in de organisatie. Functiescheiding en autorisaties worden niet alleen binnen 1 proces of systeem geïmplementeerd, maar ook integraal over de diverse gerelateerde bedrijfsprocessen en systemen van de hele organisatie om onbevoegd gebruik vanuit verschillende processen te voorkomen. Bij voorkeur wordt dit ondersteund door een organisatie breed ingevoerd systeem t.b.v. Role-based Access Control (RBAC) **Evidence in aanvulling op 4:** 1. Overzicht bedrijfsregels in RBAC-systeem. 2. Recent verslag van de (interne) auditor met bevindingen rondom functiescheiding.	

Controledoelstelling 1.21

Cluster: Beleid en organisatie	**ISO 27002 nummer: 6.1.2**
Controledoelstelling: Scheiding van taken Conflicterende taken en verantwoordelijkheden behoren te worden gescheiden om de kans op onbevoegd of onbedoeld wijzigen of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

2. Personeel, studenten en gasten

Nr.	ISO27002	Controledoelstelling
2.1	7.1.2	**Arbeidsvoorwaarden**: De contractuele overeenkomst met medewerkers en contractanten behoort hun verantwoordelijkheden voor informatiebeveiliging en die van de organisatie te vermelden.
2.2	7.2.2	**Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging:** Alle medewerkers van de organisatie en, voor zover relevant, contractanten behoren een passende bewustzijnsopleiding en -training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie.
2.3	9.2.6	**Toegangsrechten intrekken of aanpassen:** De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatie verwerkende faciliteiten behoren bij beëindiging van hun dienstverband, contract of overeenkomst te worden verwijderd, en bij wijzigingen behoren ze te worden aangepast.
2.4	11.2.9	**'Clear desk'- en 'clear screen'-beleid**: Er behoort een 'clear desk'-beleid voor papieren documenten en verwijderbare opslagmedia en een 'clear screen'-beleid voor informatie verwerkende faciliteiten te worden ingesteld.
2.5	13.2.4	**Vertrouwelijkheids- of geheimhoudingsovereenkomst:** Eisen voor vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie betreffende het beschermen van informatie weerspiegelen, behoren te worden vastgesteld, regelmatig te worden beoordeeld en gedocumenteerd.
2.6	16.1.3	**Rapportage van zwakke plekken in de informatiebeveiliging:** Van medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten van de organisatie behoort te worden geëist dat zij de in systemen of diensten waargenomen of vermeende zwakke plekken in de informatiebeveiliging registreren en rapporteren.
2.7	7.1.1	**Screening**: Verificatie van de achtergrond van alle kandidaten voor een dienstverband behoort te worden uitgevoerd in overeenstemming met relevante wet- en regelgeving en ethische overwegingen en behoort in verhouding te staan tot de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend en de vastgestelde risico's te zijn.

2.1 Arbeidsvoorwaarden

Cluster: Personeel, studenten en gasten	**ISO 27002 nummer: 7.1.2**

Controledoelstelling: Arbeidsvoorwaarden
De contractuele overeenkomst met medewerkers en contractanten behoort hun verantwoordelijkheden voor informatiebeveiliging en die van de organisatie te vermelden.

Tips: geen aanvullende opmerkingen

Toelichting:
Als onderdeel van hun contractuele verplichting behoren werknemers, ingehuurd personeel en externe gebruikers de algemene voorwaarden te aanvaarden en te ondertekenen van hun arbeidscontract, waarin hun verantwoordelijkheden en die van de organisatie ten aanzien van informatiebeveiliging behoren te zijn vastgelegd. (Er mag een gedragscode worden gebruikt om de verantwoordelijkheden van gebruikers te dekken ten aanzien van vertrouwelijkheid, gegevensbescherming, ethiek, passend gebruik van voorzieningen enz. Ingehuurde of gedetacheerde gebruikers zijn verbonden met een externe organisatie, die op haar beurt weer verplicht kan zijn om contracten af te sluiten namens de ingehuurde persoon.)

Niveaus	Beheersmaatregel (plus evidence)	Audit
Volwassenheidsniveau 1 (Initieel / ad hoc)	Er zijn geen afspraken vastgelegd, werknemers handelen op eigen initiatief, het is niet duidelijk wat de verantwoordelijkheden zijn, de algemene voorwaarden zijn niet algemeen bekend. Processen en werkwijzen voor aanvaarding van eigen verantwoordelijkheden en die van de organisatie door werknemers, ingehuurd personeel en externe gebruikers ten aanzien van informatiebeveiliging worden op ad-hoc basis benaderd. Er is geen sprake van een vastomlijnd proces of beleid.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Er zijn afspraken maar die zijn niet schriftelijk vastgelegd of ondertekend. Er verschijnen gelijksoortige en gemeenschappelijke processen voor aanvaarding van eigen verantwoordelijkheden en die van de organisatie door werknemers, ingehuurd personeel en externe gebruikers ten aanzien van informatiebeveiliging, maar deze zijn grotendeels intuïtief vanwege het individuele karakter van de expertise. Bepaalde aspecten van het proces zijn reproduceerbaar vanwege die individuele expertise, en er kan sprake zijn van enige documentatie en een zeker begrip van beleid en procedures. **Evidence**: 1. Kopie van mogelijk beschikbaar beleid en procedures; 2. Kopie van gedragscode(s) voor informatiebeveiliging.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Er zijn organisatie breed afspraken die door medewerkers moeten worden ondertekend. Langzaamaan worden steeds vaker best practices toegepast voor aanvaarding van eigen verantwoordelijkheden en die van de organisatie door werknemers, ingehuurd personeel en externe gebruikers ten aanzien van informatiebeveiliging. Voor alle belangrijke activiteiten worden proces, beleid en procedures Gedefinieerd en gedocumenteerd. **Evidence in aanvulling op 2:** 1. Kopie cao, regelingen personeel, beleid, procesbeschrijving waarin de organisatie brede afspraken zijn opgenomen; 2. Kopie werkinstructies/ gedragscode; 3. Kopie arbeidscontract indien de algemene voorwaarden m.b.t. informatiebeveiliging daarin zijn vastgelegd.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	Langzaamaan worden steeds vaker best practices toegepast voor aanvaarding van eigen verantwoordelijkheden en die van de organisatie door werknemers, ingehuurd personeel en externe gebruikers ten aanzien van informatiebeveiliging. Voor alle belangrijke activiteiten worden proces, beleid en procedures Gedefinieerd en gedocumenteerd. Periodiek vindt evaluatie plaats (PDCA). **Evidence in aanvulling op 3:** 1. Informatie over periodieke evaluatie en herziening van proces en procedures.	

Volwassenheidsniveau 5 (Geoptimaliseerd)	Er worden externe best practices en normen toegepast voor aanvaarding van eigen verantwoordelijkheden en die van de organisatie ten aanzien van informatiebeveiliging. De procesdocumentatie is geëvolueerd tot een stelsel van geautomatiseerde workflows. Processen, beleid en procedures zijn gestandaardiseerd en geïntegreerd, ten behoeve van een effectief beheer en verbeteringen in alle stadia. **Evidence in aanvulling op 4:** 1. Kopie beleid waaruit blijkt dat externe best practices zijn opgenomen; 2. Kopie beschrijving workflow proces(sen); 3. Kopie procesgegevens workflow.	

Controledoelstelling 2.1

Cluster: Personeel, studenten en gasten	**ISO 27002 nummer: 7.1.2**
Controledoelstelling: Arbeidsvoorwaarden De contractuele overeenkomst met medewerkers en contractanten behoort hun verantwoordelijkheden voor informatiebeveiliging en die van de organisatie te vermelden.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

2.2 Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging

Cluster: Personeel, studenten en gasten	**ISO 27002 nummer: 7.2.2**

Controledoelstelling: Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging
Alle medewerkers van de organisatie en, voor zover relevant, contractanten behoren een passende bewustzijnsopleiding en -training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie.

Tips: geen aanvullende opmerkingen

Toelichting:
Alle werknemers van de organisatie en, voor zover van toepassing, ingehuurd personeel en externe gebruikers, behoren geschikte training en regelmatige bijscholing te krijgen met betrekking tot beleid en procedures van de organisatie, voor zover relevant voor hun functie. (Bewustmakingstraining, bijv. een introductieprogramma waarin de verwachtingen van de organisatie worden behandeld voordat toegang wordt verleend tot informatie of diensten. Voortgezette en/of periodieke bewustwordingsprogramma's voor relevante groepen gebruikers.)

Niveaus	Beheersmaatregel (plus evidence)	Audit
Volwassenheidsniveau 1 (Initieel / ad hoc)	Het is niet duidelijk welke procedures gelden en voor wie dit relevant is.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Voor kritieke terreinen zijn minimale eisen t.a.v. vaardigheden vastgesteld. Training wordt pas aangeboden als daar behoefte aan blijkt te bestaan en niet op basis van een overeengekomen plan; de opleiding bestaat deels uit informele praktijktraining. **Evidence:** 1. Kopie van vaardigheidseisen die gesteld worden aan functies voor informatiebeveiliging; 2. Kopie van (informele) praktijktrainingen voor informatiebeveiliging.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Op alle terreinen zijn de benodigde vaardigheden bekend en benoemd. Er is een formeel opleidingsplan opgesteld, de formele training gaat echter nog uit van afzonderlijke initiatieven. **Evidence in aanvulling op 2:** 1. Kopie recente opleidingsplan; 2. Kopie lijst met opgestelde cursussen en bijscholingen; 3. Kopie documentatie (nieuwsbrief, flyers of aankondigingen) m.b.t. het aanmelden van de cursussen; 4. Kopie enkele materialen van recente cursussen.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	Voor alle terreinen worden de vaardigheidsvereisten stelselmatig bijgehouden; op alle kritieke gebieden is de deskundigheidsbevordering gewaarborgd en certificering wordt aangemoedigd. Er worden volwaardige trainingstechnieken toegepast. **Evidence: in aanvulling op niveau 3:** 1. Trainingstechnieken worden toegepast conform het opleidingsplan, en kennisdeling wordt bevorderd (recente training). Alle personen met specifieke kennis worden hierbij betrokken en de effectiviteit van het opleidingsplan wordt beoordeeld (evaluatie training)	
Volwassenheidsniveau 5 (Geoptimaliseerd)	De organisatie hanteert een formeel proces voor het stimuleren van voortdurende vaardigheidsverbetering, gebaseerd op heldere persoonlijke en organisatie brede doelstellingen. Training en opleiding ondersteunen externe best practices en het gebruik van geavanceerde concepten en technieken. Kennisdeling is onderdeel van de bedrijfscultuur en vervat in geïntegreerde bedrijfssystemen. Advies wordt ingewonnen van externe deskundigen en vooraanstaande sectorgenoten. **Evidence in aanvulling op 4:** 1. Cursussen en trainingen voldoen aan externe best practices en het gebruik van geavanceerde concepten en technieken m.b.t. informatiebeveiliging; 2. Kopie adviezen van externe deskundigen m.b.t. informatiebeveiliging.	

Controledoelstelling 2.2

Cluster: Personeel, studenten en gasten	**ISO 27002 nummer: 7.2.2**
Controledoelstelling: Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging Alle medewerkers van de organisatie en, voor zover relevant, contractanten behoren een passende bewustzijnsopleiding en -training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

2.3 Toegangsrechten intrekken of aanpassen

Cluster: Personeel, studenten en gasten	**ISO 27002 nummer: 9.2.6**

Controledoelstelling: Toegangsrechten intrekken of aanpassen
De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatie verwerkende faciliteiten behoren bij beëindiging van hun dienstverband, contract of overeenkomst te worden verwijderd, en bij wijzigingen behoren ze te worden aangepast.

Tips: de autorisatiematrix is voor dit statement cruciaal. Met name de medewerkers die uit dienst zijn getreden moeten worden ge-audit. Het betreft hier medewerkers en externen die een nieuwe rol of functie krijgen (life cycle) en de medewerkers en externen die de instelling verlaten (de-provisioning). Studenten worden niet meegenomen, omdat zij geen groot risico vormen in het kader van informatiebeveiliging (zie Cyberdriegingsbeeld 2016).
Zie ook hoofdstuk 3.5.1.

Toelichting:
De toegangsrechten van alle werknemers, ingehuurd personeel en externe gebruikers tot informatie en IT-voorzieningen worden geblokkeerd bij beëindiging van het dienstverband, het contract of de overeenkomst, of ze worden na wijziging aangepast. (Bij beëindiging of wijziging van een rol of functie worden de toegangsrechten beoordeeld, en indien nodig ingetrokken of gewijzigd. Het gaat om fysieke en logische toegangsmiddelen (sleutels, accounts, medewerkerskaart, abonnementen).)

Niveaus	Beheersmaatregel (plus evidence)	Audit
Volwassenheidsniveau 1 (Initieel / ad hoc)	De toegangsrechten worden ad hoc gewijzigd of ingetrokken, wanneer er toevallig iemand aan denkt.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Er verschijnen gelijksoortige en gemeenschappelijke processen, maar deze zijn grotendeels intuïtief vanwege het individuele karakter van de expertise. Bepaalde aspecten van het proces zijn reproduceerbaar vanwege die individuele expertise, en er kan sprake zijn van enige documentatie en een zeker begrip van beleid en procedures. **Evidence:** 1. Kopie van procesbeschrijving(en) voor intrekken/wijzigen van toegangsrechten bij functiewijziging/beëindiging aanstelling; 2. Kopie van voorbeelden van mutaties van toegangsrechten.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Voor de belangrijkste autorisaties is een procedure beschreven en wordt op een vaste manier gewerkt, met vaste termijnen en instelling brede communicatie over autorisatieprocedures. **Evidence in aanvulling op 2:** 1. Kopie procedurebeschrijving omtrent de toegangsrechten (inclusief blokkering van toegangsrechten); 2. Kopie van informatie dat de organisatie conform de procedure heeft gewerkt; zoals wijzigingsformulieren, e-mails; 3. Kopie van informatie waaruit blijkt dat de blokkering van toegang conform het beleid is; 4. Kopie van informatie waaruit blijkt dat het proces is gecommuniceerd/ geïmplementeerd. Te denken aan e-mails, nieuwsbrief.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	Er is een gedegen en volledig proces, en er worden interne best practices toegepast. Op alle gebieden zijn er vaste procedures ingeregeld en de acties op de verschillende deelgebieden zijn gecoördineerd. Er vinden regelmatige controles plaats op de autorisatietabellen. Alle aspecten van het proces zijn gedocumenteerd en reproduceerbaar. Beleidsvoorschriften zijn goedgekeurd en bekrachtigd door het management. De normen voor ontwikkeling en onderhoud van proces en procedures worden overgenomen en nageleefd. **Evidence in aanvulling op 3:** 1. Uit kopie beleid blijkt dat PDCA-cyclus is vastgesteld en taken zijn belegd; 2. Kopie van goedkeuring/vaststelling beleid door CvB/RvB/RvT.	

Volwassenheidsniveau 5 (Geoptimaliseerd)	Er worden externe best practices en normen toegepast. De procesdocumentatie is geëvolueerd tot een stelsel van geautomatiseerde workflows. Processen, beleid en procedures zijn gestandaardiseerd en geïntegreerd, ten behoeve van een effectief beheer en verbeteringen in alle stadia. **Evidence in aanvulling op 4:** 1. Kopie beleid/procesbeschrijving/proces waaruit blijkt dat externe normen worden toegepast; 2. Kopie beschrijvingen van geautomatiseerde workflows; 3. Testen van de procesinformatie uit de workflow van n mutaties (op basis van aantal mutaties per tijdeenheid per jaar) of wordt voldaan aan opgesteld en goedgekeurd beleid.	

Controledoelstelling 2.3

Cluster: Personeel, studenten en gasten	**ISO 27002 nummer: 9.2.6**
Controledoelstelling: Toegangsrechten intrekken of aanpassen De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatie verwerkende faciliteiten behoren bij beëindiging van hun dienstverband, contract of overeenkomst te worden verwijderd, en bij wijzigingen behoren ze te worden aangepast.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

2.4 'Clear desk'- en 'clear screen'-beleid

Cluster: Personeel, studenten en gasten	**ISO 27002 nummer: 11.2.9**	
Controledoelstelling: 'Clear desk'- en 'clear screen'-beleid Er behoort een 'clear desk'-beleid voor papieren documenten en verwijderbare opslagmedia en een 'clear screen'-beleid voor informatie verwerkende faciliteiten te worden ingesteld.		
Tips: een audit kan ook plaatsvinden op afvalpapier. Het komt (kwam) vaak voor dat waardedocumenten in een afvalbak werden gegooid zonder dat informatie onleesbaar is (was) gemaakt.		
Toelichting: Er behoort een "clear desk"-beleid voor papier en verwijderbare opslagmedia en een "clear screen"-beleid voor IT-voorzieningen te worden ingesteld.		
Niveaus	**Beheersmaatregel (plus evidence)**	**Audit**
Volwassenheidsniveau 1 (Initieel / ad hoc)	Processen en werkwijzen worden op ad-hoc basis / per leidinggevende benaderd. Er is geen sprake van een vastomlijnd proces of beleid.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Er zijn binnen groepen afspraken praktijkafspraken gemaakt, daar is over gecommuniceerd op operationeel-tactisch niveau.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Er zijn instelling breed afspraken vastgelegd en er wordt gecommuniceerd over nut en noodzaak van clear desk en clear screen. Clear screen wordt waar mogelijk en nodig afgedwongen op basis van baseline en best practice. **Evidence:** 1. Kopie 'Clear desk'- en 'clear screen'-beleid; 2. Kopie e-mails, flyers, of nieuwsbrief waaruit het blijkt dat de organisatie met de eindgebruikers heeft gecommuniceerd omtrent het volgende: • Elke dag dossiers opbergen bij vertrek naar huis; • PC vergrendelen bij verlaten van werkplek.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	**Evidence in aanvulling op 3:** 1. Er is een gedegen en volledig proces, PDCA belegd, en er worden interne best practices toegepast. Alle aspecten van het proces zijn gedocumenteerd en reproduceerbaar. Beleidsvoorschriften zijn goedgekeurd en bekrachtigd door het management. Er vinden regelmatige controles plaats op de effectiviteit van de beveiligingsmaatregelen.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	**Evidence in aanvulling op 4:** 1. Er worden externe best practices en normen toegepast. De procesdocumentatie is geëvolueerd tot een stelsel van geautomatiseerde workflows. Processen, beleid en procedures zijn gestandaardiseerd en geïntegreerd, ten behoeve van een effectief beheer en verbeteringen in alle stadia.	

Controledoelstelling 2.4

Cluster: Personeel, studenten en gasten	**ISO 27002 nummer: 11.2.9**
Controledoelstelling: 'Clear desk'- en 'clear screen'-beleid Er behoort een 'clear desk'-beleid voor papieren documenten en verwijderbare opslagmedia en een 'clear screen'-beleid voor informatie verwerkende faciliteiten te worden ingesteld.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

2.5 Vertrouwelijkheids- of geheimhoudingsovereenkomst

Cluster: Personeel, studenten en gasten	**ISO 27002 nummer: 13.2.4**

Controledoelstelling: Vertrouwelijkheids- of geheimhoudingsovereenkomst
Eisen voor vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie betreffende het beschermen van informatie weerspiegelen, behoren te worden vastgesteld, regelmatig te worden beoordeeld en gedocumenteerd.

Tips: geheimhoudingsovereenkomst beoordelen. Onderzoek met name de deelnemersadministratie. T.a.v. de geheimhouding kan ook verwezen worden naar de cao.

Toelichting:
Eisen voor vertrouwelijkheid of geheimhoudingsovereenkomst die een weerslag vormen van de behoefte van de organisatie aan bescherming van informatie behoren te worden vastgesteld en regelmatig te worden beoordeeld. (Vertrouwelijkheidseisen (o.a. een geheimhoudingsovereenkomst) vormen een weerslag van de behoefte van de organisatie aan bescherming van informatie binnen juridisch afdwingbare voorwaarden. Denk bij die eisen aan o.a.: welke informatie, looptijd, eigendom van informatie, toegelaten gebruik, wat te doen bij inbreuk e.d.).

Niveaus	Beheersmaatregel (plus evidence)	Audit
Volwassenheidsniveau 1 (Initieel / ad hoc)	Eisen voor vertrouwelijkheid of een geheimhoudingsovereenkomst van personeel/studenten en gasten zijn niet vastgelegd. Organisatieonderdelen nemen op basis van eigen inzicht maatregelen voor geheimhouding.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Er verschijnen gelijksoortige en gemeenschappelijke processen voor de vertrouwelijkheid van gegevens voor personeel/studenten en gasten, maar deze zijn grotendeels intuïtief vanwege het individuele karakter van de expertise. Bepaalde aspecten van het proces zijn reproduceerbaar vanwege die individuele expertie, en er kan sprake zijn van enige documentatie en een zeker begrip van beleid en procedures. **Evidence:** 1. Kopie van (vastgestelde/beschreven) processen.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Eisen voor vertrouwelijkheid of geheimhouding overeenkomst die een weerslag vormen van de behoefte van de organisatie aan bescherming van informatie zijn vastgesteld en worden regelmatig beoordeeld. Langzaamaan worden steeds vaker best practices toegepast voor de vertrouwelijkheid van gegevens voor personeel/studenten en gasten. Voor alle belangrijke activiteiten worden proces, beleid en procedures Gedefinieerd en gedocumenteerd. **Evidence in aanvulling op 2:** 1. Kopie beleidsbeschrijving met opgenomen de volgende punten: • Benodigde handelingen wanneer een overeenkomst begint of eindigt, • Eigendom van de informatie, vakgeheimen en intellectueel eigendom, en hoe dit verband houdt met de bescherming van vertrouwelijke informatie; 2. Kopie vertrouwelijkheid of geheimhoudingsovereenkomst die wordt gebruikt in de organisatie; 3. Kopie risicoanalyse waarin is beschreven wat de verwachte looptijd van een vertrouwelijkheids- of geheimhoudingsovereenkomst is, waaronder gevallen waar de vertrouwelijkheid mogelijk onbeperkt moet worden aangehouden.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	Er is een gedegen en volledig proces vastgelegd in beleid voor de vertrouwelijkheid van gegevens voor personeel/studenten en gasten, en er worden interne richtlijnen toegepast. Alle aspecten van het proces zijn gedocumenteerd en reproduceerbaar. Beleidsvoorschriften zijn goedgekeurd en bekrachtigd door het management. De normen voor ontwikkeling en onderhoud van proces en procedures worden overgenomen en nageleefd. **Evidence in aanvulling op 3:** 1. Kopie goedkeuring/vaststelling beleid door MT/CvB; 2. Kopie voorbeelden van actuele geheimhoudingsovereenkomst(en) of gedragscode(s); 3. Kopie planningsagenda of kopie verslaglegging waaruit blijkt dat het beleid regelmatig wordt beoordeeld. Datum en versienummers.	

Volwassenheidsniveau 5 (Geoptimaliseerd)	Het beleid voor geheimhouding van vertrouwelijke gegevens is in overeenstemming met externe regelgeving en wettelijke voorschriften. De procesdocumentatie is geëvolueerd tot een stelsel van geautomatiseerde workflows. Processen, beleid en procedures zijn gestandaardiseerd en geïntegreerd, ten behoeve van een effectief beheer en verbeteringen in alle stadia. **Evidence in aanvulling op 4:** 1. Kopie notitie waarin het beleid voor geheimhouding wordt getoetst en afgestemd met externe wet- en regelgeving.	

Controledoelstelling 2.5

Cluster: Personeel, studenten en gasten	**ISO 27002 nummer: 13.2.4**
Controledoelstelling: Vertrouwelijkheids- of geheimhoudingsovereenkomst Eisen voor vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie betreffende het beschermen van informatie weerspiegelen, behoren te worden vastgesteld, regelmatig te worden beoordeeld en gedocumenteerd.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

2.6 Rapportage van zwakke plekken in de informatiebeveiliging

Cluster: Personeel, studenten en gasten	**ISO 27002 nummer: 16.1.3**
Controledoelstelling: Rapportage van zwakke plekken in de informatiebeveiliging Van medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten van de organisatie behoort te worden geëist dat zij de in systemen of diensten waargenomen of vermeende zwakke plekken in de informatiebeveiliging registreren en rapporteren.	
Tips: werknemers moeten zwakke plekken melden. Een "Responsible Disclosure" beleid is dan wenselijk. Zie de SURF Beleidsnotitie Modelbeleid en procedure responsible disclosure.[7]	
Toelichting: Van alle werknemers, ingehuurd personeel en externe gebruikers van informatiesystemen en -diensten behoort te worden geëist dat zij alle waargenomen of verdachte zwakke plekken in systemen of diensten registreren en rapporteren (Gebruikers worden geïnformeerd dat zelf testen op zwakke plekken uitgelegd kan worden als potentieel misbruik. Het zou ook schade kunnen veroorzaken en leiden tot wettelijke aansprakelijkheid.)	

Niveaus	**Beheersmaatregel (plus evidence)**	**Audit**
Volwassenheidsniveau 1 (Initieel / ad hoc)	Medewerkers (c.s.) weten niet welke incidenten ze moeten melden en hoe dat dan moet.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Medewerkers weten dat zij incidenten moeten melden maar de meeste weten niet hoe dat moet en wanneer dat moet. Men realiseert zich dat er iets gedaan moet worden. Het management communiceert over de algemene kwesties. **Evidence:** 1. Kopie van notulen/notitie waarin de noodzaak wordt vastgesteld dat personen alle waargenomen of verdachte zwakke plekken in systemen of diensten dienen te registreren en rapporteren; 2. Kopie van (voorbeeld)meldingen.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Medewerkers weten dat zij incidenten moeten melden en het is bekend waar zij dat moeten doen. Men begrijpt dat ingrijpen noodzakelijk is. De communicatie door het management kent een meer formele, vaste structuur. **Evidence in aanvulling op 2:** 1. Kopie overzicht welke meldpunten er aanwezig zijn; 2. Kopie nieuwsbrief, e-mail, waaruit blijkt dat het is gecommuniceerd met alle werknemers, ingehuurd personeel en externe gebruikers en laat zien dat de organisatie awareness bevordert; 3. Kopie van de laatste 2 meldingen.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	Medewerkers worden er regelmatig op gewezen dat zij incidenten moeten melden en krijgen ook terugkoppeling van gemelde incidenten. Men heeft een goed beeld van wat er nodig is. Er worden volwaardige communicatietechnieken en standaard communicatietools ingezet. **Evidence in aanvulling op 3:** 1. Kopie opvolgingsacties; 2. Het incidentproces en de communicatie daarover wordt periodiek geëvalueerd (PDCA).	
Volwassenheidsniveau 5 (Geoptimaliseerd)	Medewerkers melden incidenten op een afgesproken manier en geven ook feedback over de werking van het proces. Men heeft diepgaand inzicht in zowel actuele als toekomstige behoeften. Er wordt proactief gecommuniceerd over kwesties op basis van trends. Volwaardige communicatietechnieken worden ingezet, alsmede geïntegreerd communicatietools. Best practices worden toegepast. **Evidence in aanvulling op 4:** 1. Toegepaste best practices.	

[7] https://www.surf.nl/kennisbank/2015/beleidsnotitie-modelbeleid-en-procedure-responisible-disclosure.html

Controledoelstelling 2.6

Cluster: Personeel, studenten en gasten	**ISO 27002 nummer: 16.1.3**
Controledoelstelling: Rapportage van zwakke plekken in de informatiebeveiliging Van medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten van de organisatie behoort te worden geëist dat zij de in systemen of diensten waargenomen of vermeende zwakke plekken in de informatiebeveiliging registreren en rapporteren.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

2.7 Screening

Cluster: Personeel, studenten en gasten	**ISO 27002 nummer: 7.1.1**
Controledoelstelling: Screening: Verificatie van de achtergrond van alle kandidaten voor een dienstverband behoort te worden uitgevoerd in overeenstemming met relevante wet- en regelgeving en ethische overwegingen en behoort in verhouding te staan tot de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend en de vastgestelde risico's te zijn.	
Tips: instelling moet een screeningsbeleid hebben waarvan de verklaring Omtrent Gedrag (VOG) een onderdeel is. Dit moet ook overlegd worden door tijdelijke externe medewerkers. In sommige sectoren (mbo, po, vo) is dit een verplichting.	
Toelichting: Verificatie van de achtergrond van alle kandidaten voor een dienstverband wordt uitgevoerd in overeenstemming met relevante wet- en regelgeving en ethische overwegingen en staat in verhouding tot de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend en de vastgestelde risico's.	

Niveaus	**Beheersmaatregel (plus evidence)**	**Audit**
Volwassenheidsniveau 1 (A hoc / initieel)	Processen en werkwijzen worden op ad-hoc basis benaderd. Er is geen sprake van een vastomlijnd proces of beleid. Er is geen beleid. Verificatie van de achtergrond van kandidaten gebeurt ad hoc als leidinggevende of HR-medewerker daar aan denkt en het in gang zet.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Er verschijnen gelijksoortige en gemeenschappelijke processen en vanwege het individuele karakter van de expertise zijn bepaalde aspecten van het proces reproduceerbaar. Er kan sprake zijn van enige documentatie en een zeker begrip van beleid en procedures. Er is geen expliciet beleid, binnen de organisatie zijn meerdere mensen zich bewust van mogelijkheid en nut van screening voor functies met toegang tot gevoelige gegevens. Als referenties beschikbaar zijn worden deze ook nagegaan. **Evidence:** 1. Gespreksverslag HR /Leidinggevenden. 2. Door HR aangegeven aantallen uitgevoerde achtergrondverificaties per jaar.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Voor alle belangrijke activiteiten worden proces, beleid en procedures Gedefinieerd en gedocumenteerd. Langzaamaan worden steeds vaker best practices toegepast. Criteria voor functies waarbij achtergrond checks worden uitgevoerd zijn beschreven. Verificatie van achtergrond is (als optie) opgenomen in de beschrijving van het aanstellingsproces. **Evidence in aanvulling op 2:** 1. Procesbeschrijving aanstelling waarin verificatie achtergrond is opgenomen. 2. Beschrijving (criteria voor) functies waarbij achtergrond verificatie vereist is. 3. Beschrijving van de inhoud van een achtergrond verificatie (afhankelijk van soort functie). 4. Voorbeeld van vacaturetekst waaruit blijkt dat achtergrond verificatie onderdeel uitmaakt van de sollicitatieprocedure.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	Er is een gedegen en volledig proces en er worden interne best practices toegepast. Alle aspecten van het proces zijn gedocumenteerd en reproduceerbaar. Beleidsvoorschriften zijn goedgekeurd en bekrachtigd door het management. De normen voor ontwikkeling en onderhoud van proces en procedures worden overgenomen en nageleefd. De toepassing van procedures rondom achtergrond verificatie worden regelmatig getoetst op hun effectiviteit en op de validiteit van de vastgestelde criteria. **Evidence in aanvulling op 3:** 1. Jaarverslag afdeling HR waaruit blijkt dat achtergrond verificatie wordt geëvalueerd.	

Volwassenheidsniveau 5 (Geoptimaliseerd)	Er worden externe best practices en normen toegepast. De procesdocumentatie si geëvolueerd tot een stelsel van geautomatiseerde workflows. Processen, beleid en procedures zijn gestandaardiseerd en geïntegreerd, ten behoeve van een effectief beheer en verbeteringen in alle stadia. De toepassing van procedures rondom achtergrond verificatie is afgestemd met andere organisaties in de sector. **Evidence in aanvulling op 4:** 1. Jaarverslag afdeling HR of notulen sector-overleg waaruit blijkt dat achtergrond verificatie wordt afgestemd met de sector.	

Controledoelstelling 2.7

Cluster: Personeel, studenten en gasten	**ISO 27002 nummer: 7.1.1**
Controledoelstelling: Screening: Verificatie van de achtergrond van alle kandidaten voor een dienstverband behoort te worden uitgevoerd in overeenstemming met relevante wet- en regelgeving en ethische overwegingen en behoort in verhouding te staan tot de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend en de vastgestelde risico's te zijn.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

3. Ruimten en apparatuur

Nr.	ISO27002	Controledoelstelling
3.1	6.2.1.2	**Beleid voor mobiele apparatuur:** Er dienen beveiligingsmaatregelen te worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beperken.
3.2	8.3.2	**Verwijderen van media:** Media behoren op een veilige en beveiligde manier te worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures.
3.3	11.1.1	**Fysieke beveiligingszone:** Beveiligingszones behoren te worden Gedefinieerd en gebruikt om gebieden te beschermen die gevoelige of essentiële informatie en informatie verwerkende faciliteiten bevatten.
3.4	11.1.2	**Fysieke toegangsbeveiliging:** Beveiligde gebieden behoren te worden beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.
3.5	11.1.3	**Kantoren, ruimten en faciliteiten beveiligen:** Voor kantoren, ruimten en faciliteiten behoort fysieke beveiliging te worden ontworpen en toegepast.
3.6	11.1.4	**Beschermen tegen bedreigingen van buitenaf:** Tegen natuurrampen, kwaadwillige aanvallen of ongelukken behoort fysieke bescherming te worden ontworpen en toegepast.
3.7	11.1.5	**Werken in beveiligde gebieden:** Voor het werken in beveiligde gebieden behoren procedures te worden ontwikkeld en toegepast.
3.8	11.1.6	**Laad- en loslocatie:** Toegangspunten zoals laad- en loslocaties en andere punten waar onbevoegde personen het terrein kunnen betreden, behoren te worden beheerst, en zo mogelijk te worden afgeschermd van informatie verwerkende faciliteiten om onbevoegde toegang te vermijden.
3.9	11.2.1	**Plaatsing en bescherming van apparatuur:** Apparatuur behoort zo te worden geplaatst en beschermd dat risico's van bedreigingen en gevaren van buitenaf, alsook de kans op onbevoegde toegang worden verkleind.
3.10	11.2.2	**Nutsvoorzieningen:** Apparatuur behoort te worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door ontregelingen in nutsvoorzieningen.
3.11	11.2.3	**Beveiliging van bekabeling:** Voedings- en telecommunicatiekabels voor het versturen van gegevens of die informatiediensten ondersteunen, behoren te worden beschermd tegen interceptie, verstoring of schade.
3.12	11.2.4	**Onderhoud van apparatuur:** Apparatuur behoort correct te worden onderhouden om de continue beschikbaarheid en integriteit ervan te waarborgen.
3.13	11.2.6	**Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein:** Bedrijfsmiddelen die zich buiten het terrein bevinden, behoren te worden beveiligd, waarbij rekening behoort te worden gehouden met de verschillende risico's van werken buiten het terrein van de organisatie.
3.14	11.2.7	**Veilig verwijderen of hergebruiken van apparatuur:** Alle onderdelen van de apparatuur die opslagmedia bevatten, behoren te worden geverifieerd om te waarborgen dat gevoelige gegevens en in licentie gegeven software voorafgaand aan verwijdering of hergebruik zijn verwijderd of betrouwbaar veilig zijn overschreven.
3.15	12.4.4	**Kloksynchronisatie:** De klokken van alle relevante informatie verwerkende systemen binnen een organisatie of beveiligingsdomein behoren te worden gesynchroniseerd met één referentietijdbron.

3.1 Beleid voor mobiele apparatuur

Cluster: Ruimten en apparatuur	**ISO 27002 nummer: 6.2.1.2**
Controledoelstelling: Beleid voor mobiele apparatuur Er dienen beveiligingsmaatregelen te worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beperken.	
Tips: de apparatuur van de organisatie wordt geregistreerd; sommige instellingen registreren ook de eigen apparatuur (BYOD). Dit wordt beschreven in een beleidsdocument (bijv. de AUP).	
Toelichting: Een gestolen of verloren mobiel apparaat, het afluisteren of onderscheppen van draadloze communicatie, onbeveiligde privé (mobiele) apparaten en malware kunnen bedrijfsinformatie compromitteren.	

Niveaus	**Beheersmaatregel (plus evidence)**	**Audit**
Volwassenheidsniveau 1 (Initieel / ad hoc)	Beveiligingsmaatregelen zijn niet beschreven, iedere gebruiker van mobiele middelen zet de mobiele middelen naar eigen inzicht in. Daar waar sprake is van beveiliging van middelen wordt deze ad hoc door beheerders ingericht alvorens de apparatuur en programmatuur beschikbaar te stellen. De richtlijnen en toelichtingen die mogelijk aanwezig zijn worden niet consequent verspreid.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Er zijn beveiligingsmaatregelen beschreven en deels zijn technische middelen beschikbaar voor beveiliging van mobiele apparatuur. Ook is er een standaard inrichting die doorgaans gehanteerd wordt (verplicht wachtwoord, gereguleerde installatiemogelijkheden, versleutelingsprogrammatuur en anti-diefstal kabels) alvorens een middel wordt uitgeleverd. Geformaliseerd en gestandaardiseerd zijn deze werkwijzen niet.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Mobiele apparatuur wordt met gestandaardiseerde, veilige, inrichting uitgeleverd. Alle mobiele apparaten en toepassingen (ook die middelen in eigendom van de gebruiker) worden geregistreerd, afspraken rondom het gebruik van de middelen wordt consequent aan gebruikers meegegeven. **Evidence:** 1. Kopie beheerprocedures mobiele middelen; 2. Kopie communicatiemateriaal (mogelijk als onderdeel van of aanvullend op ICT-gedragsregels); 3. Kopie inventarislijst mobiele middelen.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	Gebruikers en beheerders zijn bekend met de afspraken en technische middelen ter beveiliging van mobiele middelen. Controle op gebruik vindt plaats en bij overtreding of uitzondering volgt analyse en passende reactie. **Evidence in aanvulling op 3:** 1. Kopie handleidingen technische beveiligingsmiddelen (zoals van tools voor e-mail versleuteling, geheugenencryptie, back-up voorzieningen); 2. Interviews waaruit blijkt dat de ICT-medewerkers bekwaam zijn in het beheer van mobiele middelen; 3. Incidentrapportages specifiek rond mobiele middelen zijn aanwezig; 4. Kopieën rapportages gebruik van mobiele middelen; 5. Evaluatie van standaards en tools heeft plaatsgevonden.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	Het beheer van mobiele middelen is geautomatiseerd en eveneens van toepassing op apparatuur van medewerkers zelf. Gegevens van verloren apparaten kunnen op afstand worden gewist, standaards en tools zijn ten minste twee keer geëvalueerd. De maatregelen sluiten naadloos aan op de eisen en behoeften van organisatie en medewerkers. **Evidence in aanvulling op 4:** 1. Geautomatiseerde beheerprocedures zijn gedocumenteerd; 2. Evaluatierapporten zijn aanwezig.	

Controledoelstelling 3.1

Cluster: Ruimten en apparatuur	**ISO 27002 nummer: 6.2.1.2**
Controledoelstelling: Beleid voor mobiele apparatuur Er dienen beveiligingsmaatregelen te worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beperken.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

3.2 Verwijderen van media

Cluster: Ruimten en apparatuur	**ISO 27002 nummer: 8.3.2**
Controledoelstelling: Verwijderen[8] van media Media behoren op een veilige en beveiligde manier te worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures.	
Tips: geen aanvullende opmerkingen	
Toelichting: Media behoren op een veilige en beveiligde manier te worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures. (Hoofdstuk 3.2.3 gaat over opslag voorzieningen in een apparaat bijv. harde schijf, hoofdstuk 3.14 is gericht op mobiele/verwijderbare media, zoals USB sticks, geheugenkaarten, externe harddisks, disks, cards, en tapes).	

Niveaus	**Beheersmaatregel (plus evidence)**	**Audit**
Volwassenheidsniveau 1 (Initieel / ad hoc)	Naar eigen inzicht, op individueel niveau.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Werkafspraken, op operationeel niveau binnen bepaalde groepen (bottom-up).	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Aantoonbaar gebruik van best practices. Beleid, proces- / procedurebeschrijvingen zijn aanwezig en vindbaar, communicatie hierover heeft plaatsgevonden. **Evidence:** 1. Kopie procedurebeschrijving voor verwijderen van media; 2. Kopie van informatie waaruit blijkt dat de organisatie conform de procedurebeschrijving heeft uitgevoerd. Te denken aan: • Kopie contractovereenkomst met een goedgekeurde verwijderbedrijf; • Kopie checklist bij het verwijderen van media; • Kopie van een registerlijst met alle verwijderde media's.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	**Evidence in aanvulling op 3:** 1. Er is een gedegen en volledig proces, PDCA belegd, en er worden interne best practices toegepast. Alle aspecten van het proces zijn gedocumenteerd en reproduceerbaar. Beleidsvoorschriften zijn goedgekeurd en bekrachtigd door het management. Er vinden regelmatige controles plaats op de effectiviteit van de beveiligingsmaatregelen.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	**Evidence in aanvulling op 4:** 1. Er worden externe best practices en normen toegepast. De procesdocumentatie is geëvolueerd tot een stelsel van geautomatiseerde workflows. Processen, beleid en procedures zijn gestandaardiseerd en geïntegreerd, ten behoeve van een effectief beheer en verbeteringen in alle stadia.	

[8] "verwijderen" betekent hier "vernietigen"

Controledoelstelling 3.2

Cluster: Ruimten en apparatuur	**ISO 27002 nummer: 8.3.2**
Controledoelstelling: Verwijderen van media Media behoren op een veilige en beveiligde manier te worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

3.3 Fysieke beveiligingszone

Cluster: Ruimten en apparatuur	**ISO 27002 nummer: 11.1.1**

Controledoelstelling: Fysieke beveiligingszone
Beveiligingszones behoren te worden Gedefinieerd en gebruikt om gebieden te beschermen die gevoelige of essentiële informatie en informatie verwerkende faciliteiten bevatten.

Tips: gebruik van pasjes, die vervolgens gelogd worden. Maar ook een sleutelplan. De rechten van de huishoudelijke dienst kunnen als onderzoekvraag worden meegenomen. In scope zijn bijv. ICT-ruimten, archiefruimten, etc.

Toelichting:
Er behoren toegangsbeveiligingen (barrières zoals toegangspoorten met kaartsloten of een bemande receptie) te worden aangebracht om ruimten te beschermen waar zich informatie en IT-voorzieningen bevinden. (Denk daarbij aan serverruimte, back up-ruimte, (MER) OTAP-straat en patchruimtes (SER). Denk ook aan kasten met persoonsdossiers, afgedrukte tentamenvragen, enz.)

Niveaus	Beheersmaatregel (plus evidence)	Audit
Volwassenheidsniveau 1 (Initieel / ad hoc)	Toegangsbeveiliging wordt naar bevind van zaken aangebracht door individuele medewerkers.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Er zijn praktijkafspraken gemaakt over toegangsbeveiligingsmaatregelen, op operationeel niveau.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Er is beleid en/of PvA voor het gebruik en de standaardisatie van toegangsbeveiligingsmaatregelen. Instrumenten worden gebruikt voor hun fundamentele doeleinden, wellicht niet helemaal in overeenstemming met beleid, architectuur en/of geïntegreerd. **Evidence:** 1. Kopie overzicht van ruimten met specifieke toegangsbeveiliging, waarbij is aangetoond dat er toegangsbeveiligingen zijn; 2. Waarneming ter plaatse.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	Er is een gedegen en volledig proces, PDCA belegd, en er worden interne best practices toegepast. Alle aspecten van het proces zijn gedocumenteerd en reproduceerbaar. Beleidsvoorschriften zijn goedgekeurd en bekrachtigd door het management. Er vinden regelmatige controles plaats op de effectiviteit van de beveiligingsmaatregelen. **Evidence in aanvulling op 3:** 1. Verslagen van controles op de effectiviteit van de toegangsbeveiliging.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	Er worden externe best practices en normen toegepast. De procesdocumentatie is geëvolueerd tot een stelsel van geautomatiseerde workflows. Processen, beleid en procedures zijn gestandaardiseerd en geïntegreerd, ten behoeve van een effectief beheer en verbeteringen in alle stadia. **Evidence in aanvulling op 4:** 1. Periodieke (jaarlijks/twee jaarlijks) evaluaties van de effectiviteit van de toegangsbeveiliging; 2. Eventueel verbeterplannen.	

Controledoelstelling 3.3

Cluster: Ruimten en apparatuur	**ISO 27002 nummer: 11.1.1**
Controledoelstelling: Fysieke beveiligingszone Beveiligingszones behoren te worden Gedefinieerd en gebruikt om gebieden te beschermen die gevoelige of essentiële informatie en informatie verwerkende faciliteiten bevatten.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

3.4 Fysieke toegangsbeveiliging

Cluster: Ruimten en apparatuur	**ISO 27002 nummer: 11.1**

Controledoelstelling: Fysieke toegangsbeveiliging
Beveiligde gebieden behoren te worden beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.

Tips: plattegrond met zone classificatie. ICT-ruimten zijn alleen toegankelijk voor geautoriseerde medewerkers (geen conciërges, facilitaire beheerders en onderhoudspersoneel).

Toelichting:
Beveiligde zones behoren te worden beschermd door geschikte toegangsbeveiliging, om te bewerkstelligen dat alleen bevoegd personeel wordt toegelaten. (Het gaat hier eigenlijk om een classificatie van fysieke ruimte. Er wordt een indeling in zones voorgesteld, van openbaar (publiek toegankelijk), voor studenten, voor afdelingen/medewerkers (kantoorruimte), voor medewerkers t.b.v. werkzaamheden met speciale bevoegdheden (ruimte met kluis, infrastructuur, gevaarlijke stoffen).)

Niveaus	Beheersmaatregel (plus evidence)	Audit
Volwassenheidsniveau 1 (Initieel / ad hoc)	Er is geen algemene regeling. Per zone zijn maatregelen genomen op individueel initiatief, maar niet noodzakelijk afgestemd op het belang van die zone of ruimte voor de organisatie/afdeling als geheel.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Zones en ruimtes zijn beschermd ongeveer in overeenstemming met hun belang voor de organisatie. De maatregelen sets per zone zijn niet op elkaar afgestemd, maar per afdeling zijn praktijkafspraken gemaakt.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Op basis van best practices is de toegangsbeveiliging tot de beveiligde zones op grote lijnen uniform ingericht, gekoppeld aan het belang van die zone voor de organisatie. Er is een 'masterplan' toegangsbeveiliging of vergelijkbaar document, er is een Plan van Aanpak, en er zijn procesbeschrijvingen/procedures gepubliceerd en/of gecommuniceerd. **Evidence:** 1. Kopie beschrijving waarin is beschreven de inrichting van toegangsbeveiliging tot de beveiligde zones; 2. Kopie van informatie waaruit blijkt dat het beleid/procedure geüpdate wordt aan het actuele belang. Denk aan; • Twee meeste recente rapportages of analyses (datum en versienummer).	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	Er is een gedegen en volledig proces, PDCA belegd, en er worden interne best practices toegepast. Alle aspecten van het proces zijn gedocumenteerd en reproduceerbaar. Beleidsvoorschriften zijn goedgekeurd en bekrachtigd door het management. Er vinden regelmatige controles plaats op de effectiviteit van de beveiligingsmaatregelen. **Evidence in aanvulling op 3:** 1. Verslagen van audits op de effectiviteit van de beveiligingsmaatregelen.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	Er worden externe best practices en normen toegepast. De procesdocumentatie is geëvolueerd tot een stelsel van geautomatiseerde workflows. Processen, beleid en procedures zijn gestandaardiseerd en geïntegreerd, ten behoeve van een effectief beheer en verbeteringen in alle stadia. **Evidence in aanvulling op 4:** 1. Evaluaties van proces rond de beveiligingsmaatregelen.	

Controledoelstelling 3.4

Cluster: Ruimten en apparatuur	**ISO 27002 nummer: 11.1**
Controledoelstelling: Fysieke toegangsbeveiliging Beveiligde gebieden behoren te worden beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

3.5 Kantoren, ruimten en faciliteiten beveiligen

Cluster: Ruimten en apparatuur	**ISO 27002 nummer: 11.1.3**	
Controledoelstelling: Kantoren, ruimten en faciliteiten beveiligen Voor kantoren, ruimten en faciliteiten behoort fysieke beveiliging te worden ontworpen en toegepast.		
Tips: controle op examenruimten is wenselijk. Onderzoek ook de rechten van externen. Scope: Alleen ICT-ruimten of aan ICT gerelateerde ruimten.		
Toelichting: Er behoort fysieke beveiliging van kantoren, ruimten en faciliteiten te worden ontworpen en toegepast.		
Niveaus	**Beheersmaatregel (plus evidence)**	**Audit**
Volwassenheidsniveau 1 (Initieel / ad hoc)	Er zijn afsluitbare ruimtes. Sleutelbeheer op afdelingsniveau.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Er zijn praktijkafspraken over de verantwoordelijkheid van fysieke beveiliging van ruimtes en voorzieningen met bedrijf kritische gegevens, apparatuur, infrastructurele of facilitaire voorzieningen. Verantwoordelijkheden en bevoegdheden zijn niet eenduidig vastgelegd.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Best practices worden toegepast. Beleid, proces en procedures zijn Gedefinieerd en gedocumenteerd, bevoegdheden en verantwoordelijkheden zijn vastgelegd. **Evidence:** 1. Kopie overzicht van ruimten met specifieke toegangsbeveiliging; 2. Kopie van adresboeken en interne telefoongidsen van de organisatie waarin locaties worden aangeduid met gevoelige IT-voorzieningen, behoren niet vrij toegankelijk te zijn voor bezoekers; 3. Waarneming ter plaatse.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	Er is een gedegen en volledig proces, PDCA belegd, en er worden interne best practices toegepast. Alle aspecten van het proces zijn gedocumenteerd en reproduceerbaar. Beleidsvoorschriften zijn goedgekeurd en bekrachtigd door het management. Er vinden regelmatige controles plaats op de effectiviteit van de beveiligingsmaatregelen. **Evidence in aanvulling op 3:** 1. Verslagen van tests op de effectiviteit van de maatregelen.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	Er worden externe best practices en normen toegepast. De procesdocumentatie is geëvolueerd tot een stelsel van geautomatiseerde workflows. Processen, beleid en procedures zijn gestandaardiseerd en geïntegreerd, ten behoeve van een effectief beheer en verbeteringen in alle stadia. **Evidence in aanvulling op 4:** 1. Evaluaties van het proces rond de fysieke beveiliging.	

Controledoelstelling 3.5

Cluster: Ruimten en apparatuur	**ISO 27002 nummer: 11.1.3**
Controledoelstelling: Kantoren, ruimten en faciliteiten beveiligen Voor kantoren, ruimten en faciliteiten behoort fysieke beveiliging te worden ontworpen en toegepast.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

3.6 Beschermen tegen bedreigingen van buitenaf

Cluster: Ruimten en apparatuur	**ISO 27002 nummer: 11.1.4**	
Controledoelstelling: Beschermen tegen bedreigingen van buitenaf Tegen natuurrampen, kwaadwillige aanvallen of ongelukken behoort fysieke bescherming te worden ontworpen en toegepast.		
Tips: beleid opnemen in 3.1.1. Kern is het inwinnen van specialistisch advies. BCM en (bijvoorbeeld) ARBO-specialisten.		
Toelichting: Er behoort fysieke beveiliging van kantoren, ruimten en faciliteiten te worden ontworpen en toegepast.		
Niveaus	**Beheersmaatregel (plus evidence)**	**Audit**
Volwassenheidsniveau 1 (Initieel / ad hoc)	Fysieke beveiligingsmaatregelen zijn bottom-up door gebouwenbeheer of facilitaire dienst getroffen, en op basis van externe eisen (brandweer, verzekering).	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Fysieke beveiligingsmaatregelen worden periodiek geïnspecteerd, bijvoorbeeld op initiatief van brandweer en verzekering (reactief).	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Best practices worden toegepast. Beleid, proces en procedures zijn vastgelegd. O.a. fysieke beveiligingsmaatregelen worden periodiek geïnspecteerd op initiatief van centraal verantwoordelijke stafafdeling. Er is een plan van aanpak t.b.v. implementatieaanbevelingen, er zijn management notulen waaruit blijkt dat risico's zijn geaccepteerd en/of maatregelen worden aangepast. **Evidence:** 1. Kopie beleid, procedurebeschrijving waarin beheersingsmaatregelen de fysieke bescherming tegen schade door brand, overstroming, aardschokken, explosies, oproer en andere vorm van natuurlijke of menselijke calamiteiten zijn beschreven; 2. Kopie van informatie waaruit blijkt dat beheersmaatregelen zijn geïmplementeerd om het risico van mogelijke gevaren te minimaliseren, bijvoorbeeld • Overzicht waar alle brandmelders en brandblusser staan; • Waarneming ter plaatse • Kopie plan van aanpak voor het oplossen tijdens menselijk calamiteiten • Kopie testrapporten van beveiligingsmiddelen.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	**Evidence in aanvulling op 3:** 1. Er is een gedegen en volledig proces, PDCA belegd, en er worden interne best practices toegepast. Alle aspecten van het proces zijn gedocumenteerd en reproduceerbaar. Beleidsvoorschriften zijn goedgekeurd en bekrachtigd door het management. Er vinden regelmatige controles plaats op de effectiviteit van de beveiligingsmaatregelen.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	**Evidence in aanvulling op 4:** 1. Er worden externe best practices en normen toegepast. De procesdocumentatie is geëvolueerd tot een stelsel van geautomatiseerde workflows. Processen, beleid en procedures zijn gestandaardiseerd en geïntegreerd, ten behoeve van een effectief beheer en verbeteringen in alle stadia.	

Controledoelstelling 3.6

Cluster: Ruimten en apparatuur	**ISO 27002 nummer: 11.1.4**
Controledoelstelling: Beschermen tegen bedreigingen van buitenaf Tegen natuurrampen, kwaadwillige aanvallen of ongelukken behoort fysieke bescherming te worden ontworpen en toegepast.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

3.7 Werken in beveiligde gebieden

Cluster: Ruimten en apparatuur	**ISO 27002 nummer: 11.1.5**
Controledoelstelling: Werken in beveiligde gebieden Voor het werken in beveiligde gebieden behoren procedures te worden ontwikkeld en toegepast.	
Tips: het betreft hier werken in MER, SER, serverruimten e.d. ARBO kan hier aanvullende informatie opleveren.	
Toelichting: Er behoren een fysieke bescherming en richtlijnen voor werken in beveiligde ruimten te worden ontworpen en toegepast. Er moeten altijd 2 mensen aanwezig zijn (m.n. buiten kantooruren) vanwege ARBO/BHV.	

Niveaus	Beheersmaatregel (plus evidence)	Audit
Volwassenheidsniveau 1 (Initieel / ad hoc)	Processen en werkwijzen worden op ad-hoc basis benaderd. Er is geen sprake van een vastomlijnd proces of beleid.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Er zijn praktijkafspraken gemaakt. Medewerkers werken op basis van individuele instructies.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Best practices worden toegepast. Er is beleid, proces en procedures zijn vastgelegd. Voor belangrijke ruimtes zijn procedures en werkinstructies vastgesteld en gecommuniceerd. **Evidence:** 1. Kopie procedure/ werkinstructies/ richtlijnen voor werken in beveiligde ruimtes; 2. Kopie van informatie waaruit blijkt dat de procedure, werkinstructies of richtlijnen is gecommuniceerd met de medewerkers. Denk aan; • Kopie intranet waarin de "op te vragen informatie" m.b.t. fysieke maatregelen voor belangrijke ruimtes is beschreven; 3. Kopie van informatie waaruit blijkt dat voor alle belangrijke ruimtes fysieke maatregelen zijn getroffen; 4. Waarneming ter plaatse.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	**Evidence in aanvulling op 3:** 1. Er is een gedegen en volledig proces, PDCA belegd, en er worden interne best practices toegepast. Alle aspecten van het proces zijn gedocumenteerd en reproduceerbaar. Beleidsvoorschriften zijn goedgekeurd en bekrachtigd door het management. Er vinden regelmatige controles plaats op de effectiviteit van de beveiligingsmaatregelen.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	**Evidence in aanvulling op 4:** 1. Er worden externe best practices en normen toegepast. De procesdocumentatie is geëvolueerd tot een stelsel van geautomatiseerde workflows. Processen, beleid en procedures zijn gestandaardiseerd en geïntegreerd, ten behoeve van een effectief beheer en verbeteringen in alle stadia.	

Controledoelstelling 3.7

Cluster: Ruimten en apparatuur	**ISO 27002 nummer: 11.1.5**
Controledoelstelling: Werken in beveiligde gebieden Voor het werken in beveiligde gebieden behoren procedures te worden ontwikkeld en toegepast.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

3.8 Laad- en loslocatie

Cluster: Ruimten en apparatuur	**ISO 27002 nummer: 11.1.6**

Controledoelstelling: Laad- en loslocatie
Toegangspunten zoals laad- en loslocaties en andere punten waar onbevoegde personen het terrein kunnen betreden, behoren te worden beheerst, en zo mogelijk te worden afgeschermd van informatie verwerkende faciliteiten om onbevoegde toegang te vermijden.

Tips: nieuwe notebooks kunnen gestolen worden of voorzien worden van ongewenste software. Denk ook aan terreurdreiging.

Toelichting:
De toegangspunten zoals gebieden voor laden en lossen en andere punten waar onbevoegden het terrein kunnen betreden, worden beheerst en indien mogelijk afgeschermd van IT-voorzieningen, om onbevoegde toegang te voorkomen. (Onderwijsinstellingen zijn per definitie publiek toegankelijk. Beveiliging van laad/lospunten zijn vooral gericht op het voorkomen van diefstal van geleverde of af te voeren goederen.)

Niveaus	**Beheersmaatregel (plus evidence)**	**Audit**
Volwassenheidsniveau 1 (Initieel / ad hoc)	Ontvangst bij Laad en losruimtes wordt geïmproviseerd. toezicht is afhankelijk van situatie en individuele inschatting.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Toezicht en bewaking van laad- en losruimtes is in de praktijk belegd. Er is geen formeel beleid, wel praktijkafspraken op operationeel niveau.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Best practices worden toegepast. Beleid, proces en procedures zijn vastgelegd. O.a. het proces toezicht en bewaking van laad- en losruimtes is belegd. Er is een vastgesteld protocol voor goederenontvangst. **Evidence:** 1. Kopie procedurebeschrijving voor openbare toegang en gebieden voor laden en lossen; 2. Kopie van informatie waaruit blijkt dat de organisatie conform de procedurebeschrijving werken, te denken aan: • Kopie van een registratieboek; • Kopie overzicht waar fysieke beveiligingstools (bijv. camera's) zijn geplaatst bij openbare toegang en gebieden voor laden en lossen; 3. Waarneming ter plaatse.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	**Evidence in aanvulling op 3:** 1. Er is een gedegen en volledig proces, PDCA belegd, en er worden interne best practices toegepast. Alle aspecten van het proces zijn gedocumenteerd en reproduceerbaar. Beleidsvoorschriften zijn goedgekeurd en bekrachtigd door het management. Er vinden regelmatige controles plaats op de effectiviteit van de beveiligingsmaatregelen.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	**Evidence in aanvulling op 4:** 1. Er worden externe best practices en normen toegepast. De procesdocumentatie is geëvolueerd tot een stelsel van geautomatiseerde workflows. Processen, beleid en procedures zijn gestandaardiseerd en geïntegreerd, ten behoeve van een effectief beheer en verbeteringen in alle stadia.	

Controledoelstelling 3.8

Cluster: Ruimten en apparatuur	**ISO 27002 nummer: 11.1.6**
Controledoelstelling: Laad- en loslocatie Toegangspunten zoals laad- en loslocaties en andere punten waar onbevoegde personen het terrein kunnen betreden, behoren te worden beheerst, en zo mogelijk te worden afgeschermd van informatie verwerkende faciliteiten om onbevoegde toegang te vermijden.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

3.9 Plaatsing en bescherming van apparatuur

Cluster: Ruimten en apparatuur	**ISO 27002 nummer: 11.2.1**
Controledoelstelling: Plaatsing en bescherming van apparatuur Apparatuur behoort zo te worden geplaatst en beschermd dat risico's van bedreigingen en gevaren van buitenaf, alsook de kans op onbevoegde toegang worden verkleind.	
Tips: aantal aandachtspunten: • Plaats waardevolle apparatuur niet in het zicht. • Schroef desktops vast. • Blindeer ramen van ruimten waar computers staan indien die gelokaliseerd zijn aan de straatkant.	
Toelichting: Apparatuur behoort zo te worden geplaatst en beschermd dat risico's van schade en storing van buitenaf en de gelegenheid voor onbevoegde toegang wordt verminderd	

Niveaus	**Beheersmaatregel (plus evidence)**	**Audit**
Volwassenheidsniveau 1 (Initieel / ad hoc)	Plaatsing en beschermingsmaatregelen van bedrijf kritische apparatuur wordt bottom-up en op basis van individuele beoordeling uitgevoerd.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Plaatsing en beschermingsmaatregelen van bedrijf kritische apparatuur geschiedt op basis van praktijkafspraken op operationeel niveau.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Er is beleid en/of een PvA opgesteld waarin het proces en de instrumenten voor plaatsing van bedrijf kritische apparatuur zoveel mogelijk te standaardiseren en te automatiseren. Instrumenten worden gebruikt voor fundamentele doeleinden, mogelijk niet volledig in lijn met architectuur en mogelijk niet volledig geïntegreerd. **Evidence:** 1. Kopie plan van aanpak waarin de beheersingsmaatregelen om het risico van mogelijk gevaren te minimaliseren; 2. Kopie van informatie waaruit blijkt dat bedrijf kritische apparatuur is geplaatst en beschermd tegen schade en storing van buitenaf en de gelegenheid voor onbevoegde toegang. Te denken aan: • kopie overzicht van ruimten met specifieke toegangsbeveiliging; 3. Waarneming ter plaatse.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	**Evidence in aanvulling op 3:** 1. Er is een gedegen en volledig proces, PDCA belegd, en er worden interne best practices toegepast. Alle aspecten van het proces zijn gedocumenteerd en reproduceerbaar. Beleidsvoorschriften zijn goedgekeurd en bekrachtigd door het management. Er vinden regelmatige controles plaats op de effectiviteit van de beveiligingsmaatregelen.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	**Evidence in aanvulling op 4:** 1. Er worden externe best practices en normen toegepast. De procesdocumentatie is geëvolueerd tot een stelsel van geautomatiseerde workflows. Processen, beleid en procedures zijn gestandaardiseerd en geïntegreerd, ten behoeve van een effectief beheer en verbeteringen in alle stadia.	

Controledoelstelling 3.9

Cluster: Ruimten en apparatuur	**ISO 27002 nummer: 11.2.1**
Controledoelstelling: Plaatsing en bescherming van apparatuur Apparatuur behoort zo te worden geplaatst en beschermd dat risico's van bedreigingen en gevaren van buitenaf, alsook de kans op onbevoegde toegang worden verkleind.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

3.10 Nutsvoorzieningen

Cluster: Ruimten en apparatuur	**ISO 27002 nummer: 11.2.2**
Controledoelstelling: Nutsvoorzieningen Apparatuur behoort te worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door ontregelingen in nutsvoorzieningen.	
Tips: beoordeel o.a. noodstroomvoorzieningen zoals aanwezigheid UPS (Uninterruptible Power Supply). Scope: vitale apparatuur.	
Toelichting: Apparatuur behoort te worden beschermd tegen stroomuitval en andere storingen door onderbreking van nutsvoorzieningen.	

Niveaus	**Beheersmaatregel (plus evidence)**	**Audit**
Volwassenheidsniveau 1 (Initieel / ad hoc)	Op basis van best effort, bottom-up zijn een aantal tools geïnstalleerd, bijvoorbeeld een UPS in een patchkast.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Beschermingsmaatregelen zijn op operationeel niveau geïmplementeerd. Tools zijn gedocumenteerd, praktijkafspraken zijn gemaakt.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Apparatuur is technisch/geautomatiseerd beschermd tegen stroomuitval en andere storingen door onderbreking van nutsvoorzieningen op basis van beleid en/of plan van aanpak. De gebruikte tooling is wellicht niet geheel in lijn met architectuur, beleid of PvA, en wellicht niet geheel geïntegreerd. **Evidence:** 1. Kopie beleid of plan van aanpak waarin is beschreven hoe de apparatuur is bescherm tegen stroomuitval en andere storingen door onderbrekingen van nutvoorzieningen; 2. Kopie van informatie waaruit blijkt dat de apparatuur is beschermd tegen stroomuitval en andere storingen. Te denken aan: • Kopie onderhoudscontract voor inspectie nutsvoorzieningen; • Kopie testrapporten m.b.t. nutvoorzieningen; • Kopie nutsvoorzieningen vs. verbruik van de systemen; 3. Waarneming ter plaatse.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	**Evidence in aanvulling op 3:** 1. Er is een gedegen en volledig proces, PDCA belegd, en er worden interne best practices toegepast. Alle aspecten van het proces zijn gedocumenteerd en reproduceerbaar. Beleidsvoorschriften zijn goedgekeurd en bekrachtigd door het management. Er vinden regelmatige controles plaats op de effectiviteit van de beveiligingsmaatregelen.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	**Evidence in aanvulling op 4:** 1. Er worden externe best practices en normen toegepast. De procesdocumentatie is geëvolueerd tot een stelsel van geautomatiseerde workflows. Processen, beleid en procedures zijn gestandaardiseerd en geïntegreerd, ten behoeve van een effectief beheer en verbeteringen in alle stadia.	

Controledoelstelling 3.10

Cluster: Ruimten en apparatuur	**ISO 27002 nummer: 11.2.2**
Controledoelstelling: Nutsvoorzieningen Apparatuur behoort te worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door ontregelingen in nutsvoorzieningen.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

3.11 Beveiliging van bekabeling

Cluster: Beleid en organisatie	**ISO 27002 nummer: 11.2.3**	
Controledoelstelling: Beveiliging van bekabeling Voedings- en telecommunicatiekabels voor het versturen van gegevens of die informatiediensten ondersteunen, behoren te worden beschermd tegen interceptie, verstoring of schade.		
Tips: geen aanvullende opmerkingen.		
Toelichting: Voedings- en telecommunicatiekabels die voor dataverkeer of ondersteunende informatiediensten worden gebruikt, behoren tegen interceptie of beschadiging te worden beschermd,		
Niveaus	**Beheersmaatregel (plus evidence)**	**Audit**
Volwassenheidsniveau 1 (Initieel / ad hoc)	Er zijn bottom-up enige beschermingsmaatregelen getroffen.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Er zijn op operationeel niveau werkafspraken omtrent gebruik en beschermingsmaatregelen voor bekabeling.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Er is gedocumenteerd welke typen/standaarden voedings- en telecommunicatiekabels die voor dataverkeer of ondersteunende informatiediensten worden gebruikt, en hoe deze tegen interceptie of beschadiging worden beschermd. Standaardgebruik, maar wellicht niet volledig conform architectuur en integratie policy. **Evidence:** 1. Kopie beleid of plan van aanpak waarin de beheersingsmaatregelen zijn beschreven voor beveiligen van voedings- en telecommunicatiekabels die voor dataverkeer of ondersteunende informatiediensten worden gebruikt tegen interceptie of beschadiging; 2. Kopie van informatie waaruit blijkt dat de organisatie conform het beleid of plan van aanpak hebben uitgevoerd. Te denken aan: • Kopie testrapporten m.b.t. voedings- en telecommunicatiekabels; 3. Waarneming ter plaatse.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	**Evidence in aanvulling op 3:** 1. Er is een gedegen en volledig proces, PDCA belegd, en er worden interne best practices toegepast. Alle aspecten van het proces zijn gedocumenteerd en reproduceerbaar. Beleidsvoorschriften zijn goedgekeurd en bekrachtigd door het management. Er vinden regelmatige controles plaats op de effectiviteit van de beveiligingsmaatregelen.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	**Evidence in aanvulling op 4:** 1. Er worden externe best practices en normen toegepast. De procesdocumentatie is geëvolueerd tot een stelsel van geautomatiseerde workflows. Processen, beleid en procedures zijn gestandaardiseerd en geïntegreerd, ten behoeve van een effectief beheer en verbeteringen in alle stadia.	

Controledoelstelling 3.11

Cluster: Beleid en organisatie	**ISO 27002 nummer: 11.2.3**
Controledoelstelling: Beveiliging van bekabeling Voedings- en telecommunicatiekabels voor het versturen van gegevens of die informatiediensten ondersteunen, behoren te worden beschermd tegen interceptie, verstoring of schade.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

3.12 Onderhoud van apparatuur

Cluster: Ruimten en apparatuur	**ISO 27002 nummer: 11.2.4**
Controledoelstelling: Onderhoud van apparatuur Apparatuur behoort correct te worden onderhouden om de continue beschikbaarheid en integriteit ervan te waarborgen.	
Tips: scope: IT-infrastructuur. Onderhoudscontracten (SLA en SLR) moeten op orde zijn.	
Toelichting: Apparatuur behoort op correcte wijze te worden onderhouden, om te waarborgen dat deze voortdurend beschikbaar is en in goede staat verkeert.	

Niveaus	**Beheersmaatregel (plus evidence)**	**Audit**
Volwassenheidsniveau 1 (Initieel / ad hoc)	Verantwoordelijkheid en verantwoording zijn niet Gedefinieerd. Medewerkers nemen op eigen initiatief en op reactieve wijze verantwoordelijkheid voor kwesties. Het is onduidelijk welke onderhoudscontracten van toepassing zijn.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Men neemt verantwoordelijkheid en wordt ter verantwoording geroepen, ook als dit niet formeel is geregeld. Bij problemen is onduidelijk wie er verantwoordelijk is. Er is sprake van standaard onderhoudscontracten.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Er is een formele verantwoordelijkheid- en verantwoordingsstructuur (RASCI) en het is duidelijk wie waar verantwoordelijk voor is. Onderhoudscontracten zijn specifiek toegespitst op het belang van de apparatuur voor de organisatie. **Evidence:** 1. Kopie beleid voor classificatie, waarborgen en onderhouden van apparatuur; 2. Kopie van formele verantwoordelijkheid- en verantwoordingstructuur; 3. Kopie onderhoudscontracten van belangrijke apparatuur; 4. Kopie twee meeste recente rapporten die door een onderhoudsbedrijf zijn afgegeven.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	**Evidence in aanvulling op 3:** 1. Er is een gedegen en volledig proces, PDCA belegd, en er worden interne best practices toegepast. Alle aspecten van het proces zijn gedocumenteerd en reproduceerbaar. Beleidsvoorschriften zijn goedgekeurd en bekrachtigd door het management. Er vinden regelmatige controles plaats op de effectiviteit van de beveiligingsmaatregelen.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	**Evidence in aanvulling op 4:** 1. Er worden externe best practices en normen toegepast. Onderhoudsprocedures en contracten worden op elkaar afgestemd en geoptimaliseerd.	

Controledoelstelling 3.12

Cluster: Ruimten en apparatuur	**ISO 27002 nummer: 11.2.4**
Controledoelstelling: Onderhoud van apparatuur Apparatuur behoort correct te worden onderhouden om de continue beschikbaarheid en integriteit ervan te waarborgen.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

3.13 Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein

Cluster: Ruimten en apparatuur	**ISO 27002 nummer: 11.2.6**

Controledoelstelling: Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein
Bedrijfsmiddelen die zich buiten het terrein bevinden, behoren te worden beveiligd, waarbij rekening behoort te worden gehouden met de verschillende risico's van werken buiten het terrein van de organisatie.

Tips: afspraken opnemen in AUP.

Toelichting:
Apparatuur buiten de terreinen behoort te worden beveiligd waarbij rekening wordt gehouden met de diverse risico's van werken buiten het terrein van de organisatie. (Denk hier aan beveiligde/beheerde werkplekken en notebooks. Mobiele apparatuur en BYOD worden in toegangsbeleid meegenomen.)

Niveaus	Beheersmaatregel (plus evidence)	Audit
Volwassenheidsniveau 1 (Initieel / ad hoc)	Beveiliging van beheerde werkplek/notebooks vindt by default / op individueel niveau plaats.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Bedrijfsmiddelen die worden verstrekt of uitgeleend, worden in de praktijk op uniforme wijze beveiligd.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Best practices worden toegepast. Beleid, proces en procedures zijn gedocumenteerd voor alle sleutelposities. **Evidence:** 1. Kopie beleid of procedurebeschrijving voor beveiligen van apparatuur buiten de terreinen; 2. Kopie van informatie waaruit blijkt dat de organisatie uitleen conform het beleid of procedurebeschrijving uitvoert. Denk bijvoorbeeld aan: • Kopie verzekeringsovereenkomst; • Kopie e-mails, nieuwsbrief waaruit blijkt dat de medewerkers (organisatie) op de hoogte zijn gebracht over het beleid; 3. Waarneming ter plaatse.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	**Evidence in aanvulling op 3:** 1. Er is een gedegen en volledig proces, PDCA belegd, en er worden interne best practices toegepast. Alle aspecten van het proces zijn gedocumenteerd en reproduceerbaar. Beleidsvoorschriften zijn goedgekeurd en bekrachtigd door het management. Er vinden regelmatige controles plaats op de effectiviteit van de beveiligingsmaatregelen.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	**Evidence in aanvulling op 4:** 1. Er worden externe best practices en normen toegepast. De procesdocumentatie is geëvolueerd tot een stelsel van geautomatiseerde workflows. Processen, beleid en procedures zijn gestandaardiseerd en geïntegreerd, ten behoeve van een effectief beheer en verbeteringen in alle stadia.	

Controledoelstelling 3.13

Cluster: Ruimten en apparatuur	**ISO 27002 nummer: 11.2.6**
Controledoelstelling: Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein Bedrijfsmiddelen die zich buiten het terrein bevinden, behoren te worden beveiligd, waarbij rekening behoort te worden gehouden met de verschillende risico's van werken buiten het terrein van de organisatie.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

3.14 Veilig verwijderen of hergebruiken van apparatuur

Cluster: Ruimten en apparatuur	**ISO 27002 nummer: 11.2.7**

Controledoelstelling: Veilig verwijderen of hergebruiken van apparatuur
Alle onderdelen van de apparatuur die opslagmedia bevatten, behoren te worden geverifieerd om te waarborgen dat gevoelige gegevens en in licentie gegeven software voorafgaand aan verwijdering of hergebruik zijn verwijderd of betrouwbaar veilig zijn overschreven.

Tips: het betreft hier afvoer van apparatuur.

Toelichting:
Alle apparatuur die opslagmedia bevat, behoort te worden gecontroleerd om te bewerkstelligen dat alle gevoelige gegevens en in licentie gebruikte programmatuur zijn verwijderd of veilig zijn overschreven voordat de apparatuur wordt verwijderd. (Dit betreft informatie op zowel servers, werkplekken, beheerde/geleende notebooks, tablets, smartphones en ook eigen devices die worden hergebruikt of voor hergebruik worden afgevoerd.

Niveaus	Beheersmaatregel (plus evidence)	Audit
Volwassenheidsniveau 1 (Initieel / ad hoc)	Individuele medewerkers classificeren zelf de gegevens die ze op mobiele media opslaan.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Er zijn praktijkafspraken hoe het afvoeren en hergebruik van bedrijfsmiddelen is geregeld.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Best practices worden toegepast. Beleid, proces en procedures zijn gedocumenteerd voor alle sleutelposities. Afvoer en/of schonen van beheerde apparatuur door leveranciers is contractueel vastgelegd. **Evidence:** 1. Kopie beleid of procedurebeschrijving voor veilig verwijderen of hergebruiken van apparatuur; Certificaten; 2. Kopie van informatie waaruit blijkt dat de organisatie conform het beleid heeft uitgevoerd. Te denken aan: • Checklist die worden gebruikt bij het controleren van "veilig verwijderen of hergebruiken van apparatuur" en • Kopie van een aantal ingevulde checklists;	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	**Evidence in aanvulling op 3:** 1. Er is een gedegen en volledig proces, PDCA belegd, en er worden interne best practices toegepast. Alle aspecten van het proces zijn gedocumenteerd en reproduceerbaar. Beleidsvoorschriften zijn goedgekeurd en bekrachtigd door het management. Er vinden regelmatige controles plaats op de effectiviteit van de beveiligingsmaatregelen.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	**Evidence in aanvulling op 4:** 1. Er worden externe best practices en normen toegepast. De procesdocumentatie is geëvolueerd tot een stelsel van geautomatiseerde workflows. Processen, beleid en procedures zijn gestandaardiseerd en geïntegreerd, ten behoeve van een effectief beheer en verbeteringen in alle stadia.	

Controledoelstelling 3.14

Cluster: Ruimten en apparatuur	**ISO 27002 nummer: 11.2.7**
Controledoelstelling: Veilig verwijderen of hergebruiken van apparatuur Alle onderdelen van de apparatuur die opslagmedia bevatten, behoren te worden geverifieerd om te waarborgen dat gevoelige gegevens en in licentie gegeven software voorafgaand aan verwijdering of hergebruik zijn verwijderd of betrouwbaar veilig zijn overschreven.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

3.15 Kloksynchronisatie

Cluster: Ruimten en apparatuur	**ISO 27002 nummer: 12.4.4**
Controledoelstelling: Kloksynchronisatie De klokken van alle relevante informatie verwerkende systemen binnen een organisatie of beveiligingsdomein behoren te worden gesynchroniseerd met één referentietijdbron.	
Tips: De systeemklokken van alle relevante infrastructuur componenten (zoals switches, servers, werkstations en appliances) dienen geautomatiseerd gesynchroniseerd te worden met een betrouwbare bron. In het beheerde netwerk moet een redundant uitgevoerde NTP[9]-bron geplaatst te zijn waarmee elke infrastructuur component zijn systeemklok synchroniseert. Deze NTP-bron synchroniseert op zijn beurt met een geautoriseerde NTP-bron van het internet.	
Toelichting: De klokken van alle relevante informatiesystemen binnen een organisatie of beveiligingsdomein behoren te worden gesynchroniseerd met een overeengekomen nauwkeurige tijdsbron.	

Niveaus	**Beheersmaatregel (plus evidence)**	**Audit**
Volwassenheidsniveau 1 (Initieel / ad hoc)	Operationeel, by default.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Bottom-up, praktijkafspraken over gemaakt op operationeel niveau.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	De klokken van relevante informatiesystemen worden gesynchroniseerd met een overeengekomen nauwkeurige tijdsbron. **Evidence:** 1. Kopie beleid en procedurebeschrijving voor de synchronisatie van systeemklokken; 2. Kopie van informatie waaruit blijkt dat de klokken van alle relevante informatiesystemen binnen de organisatie of beveiligingsdomein zijn gesynchroniseerd met overeengekomen nauwkeurige tijdbron. Denk aan: • Kopie van welke tijdbron (v.b. conform Coordinated Universal Time) die de organisatie gebruikt voor synchronisatie; 3. Kopie van informatie waaruit blijkt dat de synchronisatie regelmatig plaatsvindt. Denk aan: • Schermprint van het proces synchronisatie.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	**Evidence in aanvulling op 3:** 1. Er is een gedegen en volledig proces, PDCA belegd, en er worden interne best practices toegepast. Alle aspecten van het proces zijn gedocumenteerd en reproduceerbaar. Beleidsvoorschriften zijn goedgekeurd en bekrachtigd door het management. Er vinden regelmatige controles plaats op de effectiviteit van de beveiligingsmaatregelen.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	**Evidence in aanvulling op 4:** 1. Er worden externe best practices en normen toegepast. De procesdocumentatie is geëvolueerd tot een stelsel van geautomatiseerde workflows. Processen, beleid en procedures zijn gestandaardiseerd en geïntegreerd, ten behoeve van een effectief beheer en verbeteringen in alle stadia.	

[9] NTP: network time protocol

Controledoelstelling 3.15

Cluster: Ruimten en apparatuur	**ISO 27002 nummer: 12.4.4**
Controledoelstelling: Kloksynchronisatie De klokken van alle relevante informatie verwerkende systemen binnen een organisatie of beveiligingsdomein behoren te worden gesynchroniseerd met één referentietijdbron.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

4. Continuïteit

Nr.	ISO27002	Controledoelstelling
4.1	12.1.2	**Wijzigingsbeheer:** Veranderingen in de organisatie, bedrijfsprocessen, informatie verwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging behoren te worden beheerst.
4.2	12.1.4	**Scheiding van ontwikkel-, test- en productieomgevingen** Ontwikkel-, test- en productieomgevingen behoren te worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen.
4.3	12.2.1.1	**Beheersmaatregelen tegen malware:** Ter bescherming tegen malware behoren beheersmaatregelen voor detectie, preventie en herstel te worden geïmplementeerd.
4.4	12.2.1.2	**Beheersmaatregelen tegen malware:** Er zijn geschikte procedures ingevoerd om het bewustzijn van de gebruikers te vergroten ten aanzien van het gevaar van virussen en dergelijke.
4.5	12.3.1.1	**Back-up van informatie:** Regelmatig behoren back-upkopieën van informatie, software en systeemafbeeldingen te worden gemaakt.
4.6	12.3.1.2	**Back-up van informatie:** Gemaakte back-ups worden regelmatig getest conform het back-up beleid.
4.7	12.5.1	**Software installeren op operationele systemen:** Om het op operationele systemen installeren van software te beheersen behoren procedures te worden geïmplementeerd.
4.8	12.6.1	**Beheer van technische kwetsbaarheden:** Informatie over technische kwetsbaarheden van informatiesystemen die worden gebruikt behoort tijdig te worden verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden te worden geëvalueerd en passende maatregelen te worden genomen om het risico dat ermee samenhangt aan te pakken.
4.9	12.6.2	**Beperkingen voor het installeren van software:** Voor het door gebruikers installeren van software behoren regels te worden vastgesteld en te worden geïmplementeerd.
4.10	14.2.6	**Beveiligde ontwikkelomgeving:** Organisaties behoren beveiligde ontwikkelomgevingen vast te stellen en passend te beveiligen voor verrichtingen op het gebied van systeemontwikkeling en integratie, die betrekking hebben op de gehele levenscyclus van de systeemontwikkeling.
4.11	15.2.2	**Beheer van veranderingen in dienstverlening van leveranciers:** Veranderingen in de dienstverlening van leveranciers, met inbegrip van handhaving en verbetering van bestaande beleidslijnen, procedures en beheersmaatregelen voor informatiebeveiliging, behoren te worden, beheerd, rekening houdend met de criticaliteit van bedrijfsinformatie, betrokken systemen en processen en herbeoordeling van risico's.
4.12	16.1.4	**Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen:** Informatiebeveiligingsgebeurtenissen behoren te worden beoordeeld en er behoort te worden geoordeeld of zij moeten worden geclassificeerd als informatiebeveiliging incidenten.
4.13	16.1.5	**Respons op informatiebeveiligingsincidenten:** Op informatiebeveiligingsincidenten behoort te worden gereageerd in overeenstemming met de gedocumenteerde procedures.
4.14	17.1.2	**Informatiebeveiligingscontinuïteit implementeren:** De organisatie behoort processen, procedures en beheersmaatregelen vast te stellen, te documenteren, te implementeren en te handhaven om het vereiste niveau van continuïteit voor informatiebeveiliging tijdens een ongunstige situatie te waarborgen.
4.15	17.2.1	**Beschikbaarheid van informatie verwerkende faciliteiten:** Informatie verwerkende faciliteiten behoren met voldoende redundantie te worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.

4.1 Wijzigingsbeheer

Cluster: Continuïteit	**ISO 27002 nummer: 12.1.2**	
Controledoelstelling: Wijzigingsbeheer Veranderingen in de organisatie, bedrijfsprocessen, informatie verwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging behoren te worden beheerst.		
Tips: geen aanvullende opmerkingen.		
Toelichting: Wijzigingen in IT-voorzieningen en informatiesystemen behoren te worden beheerst.		
Niveaus	**Beheersmaatregel (plus evidence)**	**Audit**
Volwassenheidsniveau 1 (Initieel / ad hoc)	Wijzigingen worden op ad-hoc basis benaderd. Er is geen sprake van een vast-omlijnd proces of beleid. Er vindt geen impact analyse plaats.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Er verschijnen gelijksoortige en gemeenschappelijke processen, maar deze zijn grotendeels intuïtief vanwege het individuele karakter van de expertise. Bepaalde aspecten van het proces zijn reproduceerbaar vanwege die individuele expertise, en er kan sprake zijn van enige documentatie en een zeker begrip van beleid en procedures. Er vindt een beperkte impactanalyse plaats, alleen binnen het eigen expertise domein.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Er is in elk geval voor de concernsystemen een samenhangend wijzigingsproces ingericht en vastgesteld, waarin wijzigingsvoorstellen op hun impact beoordeeld worden. De wijzigingen worden volgens een vaste procedure afgehandeld. Voor veel voorkomende wijzigingen zijn standaardprocedures ingericht. **Evidence:** 1. Beschrijving van organisatie m.b.t. OTAP; 2. Kopie procesbeschrijving "change managementproces"; 3. Kopie van informatie waaruit blijkt dat de organisatie conform de procesbeschrijving heeft uitgevoerd. Te denken aan: • Kopie gehanteerde RFC-formulier (lijncontrole); • Kopie impactanalyse van de wijziging (lijncontrole); • Kopie acceptatieformulier , inclusief testuitkomsten (lijncontrole); • Schermprint van de change die van ontwikkelomgeving naar productie omgeving wordt geïmplementeerd (lijncontrole).	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	Er is een gedegen en volledig wijzigingsproces voor alle informatiesystemen en er worden interne best practice toegepast. Alle aspecten van het proces zijn gedocumenteerd en reproduceerbaar. Er vindt periodieke verslaglegging plaats m.b.t. aard, impact en resultaten van wijzigingen. Zo nodig wordt het proces bijgesteld. Er is een algemene wijzigingskalender waar grote wijzigingen in gepland en gegroepeerd zijn. **Evidence in aanvulling op 3:** 1. Aantoonbare revisies van de procedures, verslagen van resultaten van wijzigingen (wel/niet succesvol, reden van succes/falen, vervolgactie); 2. Kopie recente wijzigingskalender (jaar/kwartaal).	
Volwassenheidsniveau 5 (Geoptimaliseerd)	Er worden externe best practice en normen toegepast. De procesdocumentatie is geëvolueerd tot een stelsel van geautomatiseerde workflows. Processen, beleid en procedures zijn gestandaardiseerd en geïntegreerd, ten behoeve van een effectief beheer en verbeteringen in alle stadia. **Evidence in aanvulling op 3:** 1. Procesdocumentatie met workflow statistieken; 2. Overzicht van gebruikte “best practice” voor verbetering eigen processen.	

Controledoelstelling 4.1

Cluster: Continuïteit	**ISO 27002 nummer: 12.1.2**
Controledoelstelling: Wijzigingsbeheer Veranderingen in de organisatie, bedrijfsprocessen, informatie verwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging behoren te worden beheerst.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

4.2 Scheiding van ontwikkel-, test- en productieomgevingen

Cluster: Continuïteit	**ISO 27002 nummer: 12.1.4**
Controledoelstelling: Scheiding van ontwikkel-, test- en productieomgevingen Ontwikkel-, test- en productieomgevingen behoren te worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen.	
Tips: audit aanpassen aan SaaS applicaties.	
Toelichting: Het scheidingsniveau tussen productie-, test- en ontwikkelomgevingen dat nodig is om operationele problemen te voorkomen behoort te worden geïdentificeerd en geïmplementeerd.	

Niveaus	Beheersmaatregel (plus evidence)	Audit
Volwassenheidsniveau 1 (Initieel / ad hoc)	Er is geen OTAP-beleid, omgevingen worden aangemaakt en gebruikt zoals beheerders en gebruikers dat verstandig achten.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Voor de grote concernsystemen is naast iedere productieomgeving is minstens één testomgeving aanwezig en in gebruik. Indien de organisatie zelf ontwikkelingen doet is een aparte ontwikkelomgeving in gebruik. Op initiatief van gebruikers en beheerders worden tests uitgevoerd voordat programmatuur naar productie wordt overgezet. **Evidence:** 1. Kopie schema's applicatieomgevingen; 2. Kopie testbevindingen.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Het OTAP-beleid is uitgeschreven rekening houdend met het vereiste scheidingsniveau met daarin de benodigde omgevingen per applicatie. De werkwijze rond promotie (testen, overzetten) van programmatuur is aanwezig waarin tevens vastgelegd is wie geautoriseerd is toestemming tot installatie in productie te geven. **Evidence als 2 plus:** 1. Kopie OTAP-beleid; 2. Kopie transport-aanvraagformulieren (change requests); 3. Kopie lijst geautoriseerd opdrachtgevers.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	De OTAP omgevingen zijn conform beleid ingericht en worden overeenkomstig het beleid gebruikt. **Evidence in aanvulling op 3:** 1. Omgevingen zijn herkenbaar gescheiden, zoals door afwijkende gebruikers-ID's en/of ander schermopbouw/-kleuren; 2. Transporten vinden geautomatiseerd plaats; 3. Testomgevingen bevatten geanonimiseerde gegevens; 4. Ontwikkelaars hebben geen schrijfrechten op productie; 5. Ontwikkeltools zijn niet op productie aanwezig.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	Omgevingen zijn op ieder moment is de juiste omgeving, met de juiste test data, beschikbaar. Beheer is verregaand geautomatiseerd. **Evidence in aanvulling op 4:** 1. Kosten van inrichting en beheer van omgevingen zijn bekend; 2. Omgevingen kunnen geautomatiseerd naar behoefte opgebouwd en afgebouwd worden.	

Controledoelstelling 4.2

Cluster: Continuïteit	**ISO 27002 nummer: 12.1.4**
Controledoelstelling: Scheiding van ontwikkel-, test- en productieomgevingen Ontwikkel-, test- en productieomgevingen behoren te worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

4.3 Beheersmaatregelen tegen malware

Cluster: Continuïteit	**ISO 27002 nummer: 12.2.1.1**
Controledoelstelling: Beheersmaatregelen tegen malware Ter bescherming tegen malware behoren beheersmaatregelen voor detectie, preventie en herstel te worden geïmplementeerd.	
Tips: vragen die gesteld kunnen worden: “Doen we het?” en “Hoe doen we het?”.	
Toelichting: Er worden maatregelen getroffen voor detectie, preventie en herstel om te beschermen tegen virussen en er zijn geschikte procedures ingevoerd om het bewustzijn van de gebruikers te vergroten.	

Niveaus	**Beheersmaatregel (plus evidence)**	**Audit**
Volwassenheidsniveau 1 (Initieel / ad hoc)	Processen en werkwijzen worden op ad-hoc basis benaderd. Er is geen sprake van een vastomlijnd proces of beleid.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Detectie, herstel en verwijdering van virussen vindt plaats op basis van individuele voorzieningen en meldingen van gebruikers. Er kan sprake zijn van gelijksoortige voorzieningen bij groepen gebruikers met gezamenlijke IT-ondersteuning. Voor herstel is geen vaste procedure.)	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Het gebruik van virus- en malware detectie is voorgeschreven, gebruikers worden voorgelicht en er zijn vaste en gedocumenteerde herstelprocedures. **Evidence:** 1. Kopie beleid voor bescherming tegen malware m.b.t. kwaliteit van de gebruikte tools; 2. Kopie procedurebeschrijving voor maatregelen tegen virussen; 3. Schermprint uit systeem waaruit blijkt dat de anti-malware voorzieningen zijn ingericht 4. Kopie e-mails, flyers, nieuwsbrief waaruit blijkt dat de anti-malware voorziening is gecommuniceerd met de medewerkers; 5. Kopie monitoring op gebruik en incidenten en follow-up daarvan.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	De werking van virus- en malware detectie wordt gecontroleerd. Er zijn aanvullende detectie mechanismes in gebruik. De herstelprocedures zijn gebaseerd op interne best practice. **Evidence in aanvulling op 3:** 1. Overzicht van aanvullende detectie mechanismes; 2. Van het gebruik en van besmetting, detectie en correctie wordt statistiek bijgehouden.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	Er worden externe best practice en normen toegepast. Processen, beleid en procedures zijn gestandaardiseerd en geïntegreerd, ten behoeve van een effectief beheer en verbeteringen in alle stadia. De detectiemiddelen worden periodiek geëvalueerd op hun effectiviteit en zo nodig wordt een andere mix gekozen. **Evidence in aanvulling op 4:** 1. Rapportage periodieke evaluatie van de effectiviteit en hieruit voortvloeiende adviezen.	

Controledoelstelling 4.3

Cluster: Continuïteit	**ISO 27002 nummer: 12.2.1.1**
Controledoelstelling: Beheersmaatregelen tegen malware Ter bescherming tegen malware behoren beheersmaatregelen voor detectie, preventie en herstel te worden geïmplementeerd.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

4.4 Beheersmaatregelen tegen malware

Cluster: Continuïteit	**ISO 27002 nummer: 12.2.1.2**
Controledoelstelling: Beheersmaatregelen tegen malware Er zijn geschikte procedures ingevoerd om het bewustzijn van de gebruikers te vergroten ten aanzien van het gevaar van virussen en dergelijke.	
Tips: geen aanvullende opmerkingen.	
Toelichting: Er worden maatregelen getroffen voor detectie, preventie en herstel om te beschermen tegen virussen en er zijn geschikte procedures ingevoerd om het bewustzijn van de gebruikers te vergroten.	

Niveaus	**Beheersmaatregel (plus evidence)**	**Audit**
Volwassenheidsniveau 1 (Initieel / ad hoc)	Er wordt sporadisch naar aanleiding van specifieke incidenten gecommuniceerd over het gevaar van virussen en de noodzaak tot het gebruik van beschermende maatregelen.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Men realiseert zich dat er iets gedaan moet worden. Er is informatie beschikbaar over beschikbare hulpmiddelen voor bescherming tegen virussen en er zijn instructies over hoe deze gebruikt moeten worden.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Gebruikers worden specifiek ingelicht over het verplichte gebruik van detectiemiddelen en over preventie. **Evidence:** 1. Kopie e-mails, flyers, nieuwsbrief waaruit blijkt dat de anti-malware voorziening is gecommuniceerd met de gebruikers; 2. Kopie van informatie waaruit blijkt dat de gebruikers verplicht gebruik moeten maken van de beschikbare anti-malware voorziening: • schermprint uit systeem waaruit blijkt dat er blokkades zijn tegen bepaalde e-mails; • schermprint uit systeem waaruit blijkt dat de anti-virusscanner verplicht is ingesteld bij elke gebruiker.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	Gebruikers worden geregeld ingelicht over het verplichte gebruik van detectiemiddelen en actuele dreigingen. Er worden volwaardige communicatietechnieken en standaard communicatietools ingezet. Gebruikers worden geregeld gewezen op preventief gedrag. **Evidence in aanvulling op 3:** 1. Uit de documentatie moet blijken dat er herhaaldelijk aandacht aan voorlichting besteed wordt voor alle gebruikers.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	Men heeft diepgaand inzicht in zowel actuele als toekomstige behoeften. Er wordt proactief gecommuniceerd over kwesties op basis van trends. Volwaardige communicatietechnieken worden ingezet, alsmede geïntegreerde communicatietools. **Evidence in aanvulling op 4:** 1. Aantoonbaar inzet van meerdere technieken en middelen.	

Controledoelstelling 4.4

Cluster: Continuïteit	**ISO 27002 nummer: 12.2.1.2**
Controledoelstelling: Beheersmaatregelen tegen malware Er zijn geschikte procedures ingevoerd om het bewustzijn van de gebruikers te vergroten ten aanzien van het gevaar van virussen en dergelijke.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

4.5 Back-up van informatie

Cluster: Continuïteit	**ISO 27002 nummer: 12.3.1.1**
Controledoelstelling: Back-up van informatie Regelmatig behoren back-upkopieën van informatie, software en systeemafbeeldingen te worden gemaakt.	
Tips: controle van het back-up volume is gewenst (is van alle informatie een back-up gemaakt?). Controleer logboek back-up.	
Toelichting: Er worden back-up kopieën van informatie en programmatuur gemaakt en regelmatig getest overeenkomstig het vastgestelde back-upbeleid.	

Niveaus	**Beheersmaatregel (plus evidence)**	**Audit**
Volwassenheidsniveau 1 (Initieel / ad hoc)	Er is geen sprake van een vastomlijnd proces of beleid voor het maken van back ups.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Er zijn verschillende back-up procedures in gebruik op basis van individuele keuzes m.b.t. frequentie, omvang en type data. **Evidence:** 1. Overzicht van verschillende back-up activiteiten inclusief de scope (wat wordt er naar back-up weggeschreven).	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Voor in ieder geval alle concerninformatie zijn back-up-procedures ingericht met een vaste frequentie. Back-ups worden op een andere locatie dan de productieomgeving opgeslagen . **Evidence:** 1. Kopie beleid of procesbeschrijving van het proces back-up op concerninformatie; 2. Kopie van informatie dat het back-up wordt opgeslagen op een andere locatie (kopie overeenkomsten waarin het vermeld wordt bij gebruik van derde partij): • kopie back-up rapportages; 3. Waarneming ter plaatse (fysieke bescherming).	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	Voor alle informatie en programmatuur zijn back-up-procedures ingericht met een vaste frequentie. Back-ups worden op een andere locatie opgeslagen. back-ups worden gecontroleerd op compleetheid. **Evidence in aanvulling op 3:** 1. Kopie procesbeschrijving voor controle op compleetheid back-up; 2. Documentatie die aantoont dat alle informatiesystemen in back-up meegenomen worden.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	Er worden externe best practice en normen toegepast. De procesdocumentatie is geëvolueerd tot een stelsel van geautomatiseerde workflows. Processen, beleid en procedures zijn gestandaardiseerd en geïntegreerd, ten behoeve van een effectief beheer en verbeteringen in alle stadia. Er vindt periodiek een evaluatie plaats van de gebruikte technieken en controlemechanismes. **Evidence in aanvulling op 4:** 1. Kopie van een recent evaluatieverslag.	

Controledoelstelling 4.5

Cluster: Continuïteit	**ISO 27002 nummer: 12.3.1.1**
Controledoelstelling: Back-up van informatie Regelmatig behoren back-upkopieën van informatie, software en systeemafbeeldingen te worden gemaakt.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

4.6 Back-up van informatie 12.3.1.2

Cluster: Continuïteit	**ISO 27002 nummer: 12.3.1.2**
Controledoelstelling: Back-up van informatie Gemaakte back ups worden regelmatig getest conform het back-up beleid.	
Tips: terugzetten van bestanden (restore) middels een logboek controleren.	
Toelichting: Er worden back-up kopieën van informatie en programmatuur gemaakt en regelmatig getest overeenkomstig het vastgestelde back-upbeleid.	

Niveaus	**Beheersmaatregel (plus evidence)**	**Audit**
Volwassenheidsniveau 1 (Initieel / ad hoc)	Er zijn wellicht enkele standaard tools van het OS of open source. Er is geen sprake van een gecoördineerde aanpak van het gebruik van deze tools.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Er zijn verschillende test- en controleprocedures in gebruik op basis van individuele keuzes. Daar waar sprake is van een gemeenschappelijke benadering van de tools, is dat gebaseerd op oplossingen die op collegiale wijze worden gedeeld.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Voor in ieder geval alle concerninformatie worden gemeenschappelijke back-up- en restore tools gebruikt die beschikken over logfaciliteiten en integriteitscontroles. **Evidence:** 1. Kopie beleid of procesbeschrijving van het proces restore van back-up op concerninformatie; 2. Kopie van informatie waaruit blijkt dat de organisatie over logfaciliteiten beschikt en integriteitcontrole gebruikt voor back -up en restore. Te denken aan: • kopie van twee meest recente rapportages van de "test herstelprocedures" die uitgevoerd zijn; • kopie van informatie dat back-ups door middel van encryptie of signering/hashing plaats vinden; 3. Overzicht van back-up tools en wijze van gebruik.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	Voor alle informatie en programmatuur worden gemeenschappelijke back-up- en restore tools gebruikt die beschikken over logfaciliteiten en integriteitscontroles. Er vinden geregeld restores plaats om de feitelijke bruikbaarheid van back-ups te testen. **Evidence in aanvulling op 3:** 1. Informatie waar uit blijkt dat regelmatig restore tests gedaan worden en van de resultaten van de restore test; 2. Informatie waar uit blijkt dat de procedures aangepast worden wanneer blijkt dat de restore niet goed of niet volledig is of wanneer er anderszins fouten zijn ontdekt in de back-up procedure; 3. Informatie waaruit blijkt dat de kwaliteit van de back-up media periodiek geëvalueerd wordt.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	Op alle afdelingen worden gestandaardiseerde tool sets gebruikt. De tools zijn volledig geïntegreerd met verwante systemen, zodat processen van begin tot eind worden ondersteund. Er worden tools ingezet ter ondersteuning van procesverbeteringen en automatische detectie van afwijkingen. Er vindt periodiek een evaluatie plaats van de gebruikte technieken en controlemechanismes. **Evidence in aanvulling op 4:** 1. Kopie van een recent evaluatieverslag.	

Controledoelstelling 4.6

Cluster: Continuïteit	**ISO 27002 nummer: 12.3.1.2**
Controledoelstelling: Back-up van informatie Gemaakte back ups worden regelmatig getest conform het back-up beleid.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

4.7 Software installeren op operationele systemen

Cluster: Continuïteit	**ISO 27002 nummer: 12.5.1**
Controledoelstelling: Software installeren op operationele systemen Om het op operationele systemen installeren van software te beheersen behoren procedures te worden geïmplementeerd.	
Tips: toevoegen aan niveau 3: zowel de beheerder als de **gebruiker** moet de procedures kunnen vinden. De doelstelling is generiek, dus bijv. laptops vallen er ook onder.	
Toelichting: De integriteit van operationele systemen dient gewaarborgd te blijven. Alleen dan kan informatieverwerking betrouwbaar plaatsvinden.	

Niveaus	**Beheersmaatregel (plus evidence)**	**Audit**
Volwassenheidsniveau 1 (Initieel / ad hoc)	Vastgestelde procedures zijn niet beschikbaar. Updates op operationele systemen worden naar goedachten van degenen met beheerrechten op de systemen geïnstalleerd.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Beheerders hanteren een werkwijze die vaker wordt toegepast, een werkwijze die mogelijk een best practice binnen de organisatie is geworden. Ook is het nog mogelijk dat iedere beheerder een eigen best practice hanteert. Beschreven en gedeeld is de werkwijze echter niet. **Evidence:** 1. Gespreksverslagen met beheerders; 2. Kopie stappenplannen of basale checklists, mogelijk in de vorm van een Wiki.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Procedures voor het installeren van software op operationele systemen zijn beschreven, vastgesteld, gecommuniceerd en in gebruik. **Evidence in aanvulling op 2:** 1. Kopie formeel vastgestelde procedures; 2. Duidelijk locatie waar iedere beheerder de relevante (actuele) procedures kan vinden.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	De procedures voor het installeren van software op operationele systemen zijn aantoonbaar in gebruik en de kwaliteit van uitvoering is meetbaar. **Evidence in aanvulling op 3:** 1. Procedures worden periodiek gevalideerd; 2. Changes worden vooraf geaccordeerd; 3. Fallback plannen zijn aanwezig; 4. Uitvoering vindt plaats door getrainde beheerders; 5. Uit configuratiedetails blijkt dat alle programmatuur is geautoriseerd.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	De procedures voor het installeren van software op operationele systemen vinden procesmatig plaats en dit proces is, onder andere door automatisering, geoptimaliseerd. **Evidence in aanvulling op 4:** 1. Het proces Configuration Management is aantoonbaar operationeel; 2. Procedures rond installatie worden ondersteund met workflow; 3. Voorgaande versies van programmatuur zijn gearchiveerd.	

Controledoelstelling 4.7

Cluster: Continuïteit	**ISO 27002 nummer: 12.5.1**
Controledoelstelling: Software installeren op operationele systemen Om het op operationele systemen installeren van software te beheersen behoren procedures te worden geïmplementeerd.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

4.8 Beheer van technische kwetsbaarheden

Cluster: Continuïteit	**ISO 27002 nummer: 12.6.1**

Controledoelstelling: Beheer van technische kwetsbaarheden
Informatie over technische kwetsbaarheden van informatiesystemen die worden gebruikt behoort tijdig te worden verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden te worden geëvalueerd en passende maatregelen te worden genomen om het risico dat ermee samenhangt aan te pakken.

Tips: Worden de updates van (bijvoorbeeld) Microsoft (hot fixes) uitgevoerd. Wordt er periodiek een pentest uitgevoerd. Denk ook aan hardening van servers. Wordt er periodiek getest op kwetsbaarheden en worden ernstige kwetsbaarheden vervolgens opgelost.

Toelichting:
Er behoort tijdig informatie te worden verkregen over technische kwetsbaarheden van de gebruikte informatiesystemen. De mate waarin de organisatie blootstaat aan dergelijke kwetsbaarheden behoort te worden geëvalueerd en er behoren geschikte maatregelen te worden genomen voor behandeling van daarmee samenhangende risico's.

Niveaus	Beheersmaatregel (plus evidence)	Audit
Volwassenheidsniveau 1 (Initieel / ad hoc)	Informatie over technische kwetsbaarheden wordt ad hoc en individueel verkregen op basis van toevallig geraadpleegde websites of andere nieuwsbronnen, of op aangeven van een leverancier of relatie.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Er wordt structureel informatie bijgehouden over technische kwetsbaarheden, de wijze waarop verschilt per persoon. **Evidence:** 1. Informatie over recente kwetsbaarheden en de hiervoor gebruikte bronnen; 2. Overzicht van abonnementen op newsfeeds.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Er wordt tijdig en gestructureerd informatie verkregen over technische kwetsbaarheden. Dit is per informatiesysteem of groep van systemen Gedefinieerd en georganiseerd en wordt procesmatig aangepakt. Informatie over kwetsbaarheden wordt geanalyseerd en beoordeeld op urgentie en impact. Op beperkte schaal worden detectie middelen ingezet om kwetsbaarheden in de infrastructuur en de systemen op te sporen. **Evidence:** 1. Kopie procedurebeschrijving voor het beheren van technische kwetsbaarheden van de gebruikte informatiesystemen; 2. Kopie risicoanalyse met onderbouwing op technische kwetsbaarheden van de gebruikte informatiesystemen (versienummer + datum); 3. Kopie van informatie waaruit het blijkt dat de organisatie conform de procedure uitvoert. Te denken aan: • Kopie lijst met informatie over de leverancier van programmatuur, versienummer, huidige gebruiksstatus; • Kopie herstelprogramma waarin de beoordeling door de organisatie zichtbaar is; 4. Kopie overzicht van geconstateerde technische storingen en oplossing daarvan.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	Beheer van technische kwetsbaarheden is geïntegreerd in het beheer van de informatiesystemen. Hiervoor zijn processen ingericht en verantwoordelijkheden belegd. Periodiek wordt de werking van de processen geëvalueerd. **Evidence in aanvulling op 3:** 1. Procesbeschrijvingen en RACI-tabel.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	Voor het beheer van technische kwetsbaarheden wordt gebruik gemaakt van best practice. **Evidence in aanvulling op 4:** 1. Overzicht gebruikte best practice, samenwerkingsovereenkomsten of abonnementen.	

Controledoelstelling 4.8

Cluster: Continuïteit	**ISO 27002 nummer: 12.6.1**
Controledoelstelling: Beheer van technische kwetsbaarheden Informatie over technische kwetsbaarheden van informatiesystemen die worden gebruikt behoort tijdig te worden verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden te worden geëvalueerd en passende maatregelen te worden genomen om het risico dat ermee samenhangt aan te pakken.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

4.9 Beperkingen voor het installeren van software

Cluster: Continuïteit	**ISO 27002 nummer: 12.6.2**
Controledoelstelling: Beperkingen voor het installeren van software Voor het door gebruikers installeren van software behoren regels te worden vastgesteld en te worden geïmplementeerd.	
Tips: geen aanvullende opmerkingen.	
Toelichting: De organisatie behoort een strikt beleid te definiëren en ten uitvoer te brengen met betrekking tot de (soorten) software die gebruikers mogen installeren.	

Niveaus	**Beheersmaatregel (plus evidence)**	**Audit**
Volwassenheidsniveau 1 (Initieel / ad hoc)	Regels voor het door gebruikers installeren van software zijn niet aanwezig. Gebruikers hebben de rechten die zij ooit gekregen hebben en kunnen wel of juist geen software installeren.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Beheerders hanteren doorgaans dezelfde criteria voor het toekennen van bevoegdheden en beschikbaar stellen van software. Mogelijk zijn best practice hiervoor beschreven en in een Wiki opgenomen. Desondanks blijft de werkwijze afhankelijk van de individuele beheerder en gebruiker. **Evidence:** 1. Gespreksverslagen met beheerders; 2. Kopie best practice, mogelijk in een Wiki.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Regels met betrekking tot installeren van software door gebruikers zijn beschreven en vastgesteld. Beheerders en gebruikers zijn met de regels bekend gemaakt. **Evidence als 2 plus:** 1. Kopie vastgestelde regels; 2. Kopie communicatieregels; 3. Kopieën ingediende aanvragen en afhandeling daarvan.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	De regels met betrekking tot het door gebruikers installeren van software worden consequent uitgevoerd en gehandhaafd. **Evidence in aanvulling op 3:** 1. Operationeel IAM-proces waarin op basis van business rules installatierechten worden toegekend en eventueel ook weer ingetrokken; 2. Ingestelde policies waarmee installatierechten op uniforme wijze geautomatiseerd worden beheerd, zoals middels Active Directory policies; 3. Beveiligingsrapportages waaruit evaluatie van installatieregels blijkt; 4. Automatische installatie voor specifieke software (patches en updates) zodat gebruikers zich hier niet mee bezig hoeven houden.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	Door vergaande automatisering en snelle beslisprocessen beschikt iedere gebruiker continu over de goedgekeurde programmatuur die deze nodig heeft voor taakuitvoering. **Evidence in aanvulling op 4:** 1. Gebruikers kunnen via vooraf Gedefinieerde packages en business rules zelf die software installeren die de organisatie op de verschillende platformen voor de verschillende gebruikers en gebruikersgroepen geschikt acht; 2. Rapportages waaruit blijkt dat niet geautoriseerde programmatuur automatisch wordt herkend en geblokkeerd; 3. Licenties worden actief beheerd zodat software die gedurende lange tijd niet gebruikt is, gede-installeerd wordt.	

Controledoelstelling 4.9

Cluster: Continuïteit	**ISO 27002 nummer: 12.6.2**
Controledoelstelling: Beperkingen voor het installeren van software Voor het door gebruikers installeren van software behoren regels te worden vastgesteld en te worden geïmplementeerd.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

4.10 Beveiligde ontwikkelomgeving

Cluster: Continuïteit	**ISO 27002 nummer: 14.2.6**
Controledoelstelling: Beveiligde ontwikkelomgeving Organisaties behoren beveiligde ontwikkelomgevingen vast te stellen en passend te beveiligen voor verrichtingen op het gebied van systeemontwikkeling en integratie, die betrekking hebben op de gehele levenscyclus van de systeemontwikkeling.	
Tips: beoordeling SaaS omgeving is eenvoudiger. Bij SaaS focus op acceptatie omgeving. Deze leidt tot de beoordeling van de evidence, met name op basis van aangeleverde certificering van leverancier.	
Toelichting: Een beveiligde ontwikkelomgeving omvat personen, processen en technologie die in verband staan met systeemontwikkeling en integratie.	

Niveaus	**Beheersmaatregel (plus evidence)**	**Audit**
Volwassenheidsniveau 1 (Initieel / ad hoc)	Er zijn geen beveiligde ontwikkelomgevingen vastgesteld en passend beveiligd voor verrichtingen op het gebied van systeemontwikkeling en integratie.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	De ontwikkelomgevingen worden binnen afdelingen of voor gelijksoortige systemen of processen op een gemeenschappelijke wijze beveiligd, maar de criteria zijn gebaseerd op de expertise van de betrokkenen. Bepaalde aspecten van de beveiliging zijn reproduceerbaar vanwege die individuele expertise en er kan sprake zijn van enige documentatie en een zeker begrip van policies en procedures. Er is geen sprake van een vastomlijnd beleid of best practice. **Evidence:** 1. Gespreksverslagen met beheerders; 2. Kopie (informele) documentatie.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Overeenkomstig het vereiste beschermingsniveau heeft de organisatie beveiligde omgevingen en corresponderende processen in veilige ontwikkelprocedures gedocumenteerd en deze beschikbaar gesteld aan alle (in- en externe) personen die ze nodig hebben. **Evidence in aanvulling op 2:** 1. Kopie (architectuur)modellen systeemomgevingen; 2. Kopieën inrichtingsdocumentatie (best practice inrichtingen); 3. Kopieën procesbeschrijvingen.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	De organisatie richt omgevingen consequent op de vastgestelde wijze in en hanteert aantoonbaar de afgesproken veilige ontwikkelprocedures. **Evidence in aanvulling op 3:** 1. Kopieën risico-classificaties; 2. Rapportages uit tool(s) voor versiebeheer; 3. Kopieën van beheer- en change logs; 4. Kopieën uitbestedingsovereenkomsten; 5. Kopieën opleidingscertificaten betrokken ontwikkelaars en beheerders.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	De organisatie heeft technische en workflow tools voor inrichting en beheer van omgevingen in gebruik. Hierdoor worden omgevingen structureel conform vastgestelde best practice ingericht en is de integriteit van de ontwikkelomgevingen (inclusief ontwikkelde programmatuur) blijvend gewaarborgd. **Evidence in aanvulling op 4:** 1. Kopieën best practice inrichtingen; 2. Kopieën workflow beschrijvingen; 3. Kopieën inrichtingsdocumenten en handleidingen van gebruikte tools; 4. Kopieën evaluaties workflows en gebruikte best practice.	

Controledoelstelling 4.10

Cluster: Continuïteit	**ISO 27002 nummer: 14.2.6**
Controledoelstelling: Beveiligde ontwikkelomgeving Organisaties behoren beveiligde ontwikkelomgevingen vast te stellen en passend te beveiligen voor verrichtingen op het gebied van systeemontwikkeling en integratie, die betrekking hebben op de gehele levenscyclus van de systeemontwikkeling.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

4.11 Beheer van veranderingen in dienstverlening van leveranciers

Cluster: Continuïteit	**ISO 27002 nummer: 15.2.2**
Controledoelstelling: Beheer van veranderingen in dienstverlening van leveranciers Veranderingen in de dienstverlening van leveranciers, met inbegrip van handhaving en verbetering van bestaande beleidslijnen, procedures en beheersmaatregelen voor informatiebeveiliging, behoren te worden, beheerd, rekening houdend met de criticaliteit van bedrijfsinformatie, betrokken systemen en processen en herbeoordeling van risico's.	
Tips: basis zijn gesprekken met leveranciers betreffende SLA's en SLR's. Informatie van leverancier is daarbij leidend.	
Toelichting: Wijzigingen in de dienstverlening door derden, waaronder het bijhouden en verbeteren van bestaande beleidslijnen, procedures en maatregelen voor informatiebeveiliging, worden beheerd, waarbij rekening wordt gehouden met de onmisbaarheid van de betrokken bedrijfssystemen en -processen en met heroverweging van risico's.	

Niveaus	**Beheersmaatregel (plus evidence)**	**Audit**
Volwassenheidsniveau 1 (Initieel / ad hoc)	Dienstverlening van derden wordt afgenomen "as is". Wijzigingen gebeuren op initiatief van de dienstverlener, veelal zonder goede afstemming over inhoud van de wijzigingen en tijdstip van de wijzigingen.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Wijzigingen in de dienstverlening worden per geval afgestemd om de continuïteit van onmisbare bedrijfsprocessen te borgen. De inhoud van de wijzigingen zijn soms wel en soms niet doorgesproken en/of goedgekeurd. **Evidence:** 1. Correspondentie over planning van wijzigingen; 2. Correspondentie over gewijzigde functionaliteit.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Wijzigingen in de dienstverlening door derden, waaronder het bijhouden en verbeteren van bestaande beleidslijnen, procedures en maatregelen voor informatiebeveiliging, worden beheerd, gepland en afgestemd, waarbij rekening wordt gehouden met de onmisbaarheid van de betrokken bedrijfssystemen en -processen en met heroverweging van risico's. **Evidence in aanvulling op 2:** 1. Kopie beleid of procesbeschrijving voor het beheer van wijzigingen in dienstverlening (versie beheer van contracten) door een derde partij; 2. Kopie van informatie waaruit blijkt dat de organisatiewijzigingen conform de procesbeschrijving heeft uitgevoerd. Te denken aan: • Kopie aanvraagformulieren; • Kopie twee meest recente risicoanalyses.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	Wijzigingen worden procesmatig doorgevoerd waarbij vóór het uitvoeren van de wijziging afstemming plaats vindt en na de wijziging de wijziging geëvalueerd wordt. Wijzigingen worden afgestemd met en ingepast in de algemene wijzigingskalender. **Evidence in aanvulling op 3:** 1. Verslag (e-mail, brief) van de evaluatie van een wijziging; 2. Kopie wijzigingskalender van laatste jaar of kwartaal; 3. Correspondentie over de afstemming met betrekking tot planning en inhoud van een wijziging.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	Er worden externe best practice en normen toegepast. De procesdocumentatie is geëvolueerd tot een stelsel van geautomatiseerde workflows. Processen, beleid en procedures zijn gestandaardiseerd en geïntegreerd, ten behoeve van een effectief beheer en verbeteringen in alle stadia. Wijzigingen worden qua planning, inhoud en impact afgestemd met alle dienstverleners en met interne belanghebbenden. **Evidence in aanvulling op 4:** 1. Procesdocumentatie met workflow statistieken; 2. Overzicht van gebruikte "best practice" voor verbetering eigen processen.	

Controledoelstelling 4.11

Cluster: Continuïteit	**ISO 27002 nummer: 15.2.2**
Controledoelstelling: Beheer van veranderingen in dienstverlening van leveranciers Veranderingen in de dienstverlening van leveranciers, met inbegrip van handhaving en verbetering van bestaande beleidslijnen, procedures en beheersmaatregelen voor informatiebeveiliging, behoren te worden, beheerd, rekening houdend met de criticaliteit van bedrijfsinformatie, betrokken systemen en processen en herbeoordeling van risico's.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

4.12 Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen

Cluster: Continuïteit	**ISO 27002 nummer: 16.1.4**
Controledoelstelling: Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen Informatiebeveiligingsgebeurtenissen behoren te worden beoordeeld en er behoort te worden geoordeeld of zij moeten worden geclassificeerd als informatiebeveiliging incidenten.	
Tips: geen aanvullende opmerkingen. Een beveiligingsincident kan leiden tot een datalek, dit is niet altijd het geval (bijvoorbeeld, gestolen notebook is versleuteld). Classificatieflow datalekken.	
Toelichting: Het contactpunt beoordeelt gebeurtenissen volgens het classificatieschema en prioriteert deze indien het incidenten zijn. Classificatie en prioritering worden in detail in een verslag vastgelegd. Een responseteam (indien in de organisatie aanwezig) ontvangt deze rapportage en bevestigt of her-beoordeelt het besluit.	

Niveaus	**Beheersmaatregel (plus evidence)**	**Audit**
Volwassenheidsniveau 1 (Initieel / ad hoc)	Gebeurtenissen worden naar inzicht van een medewerker beoordeeld en afgehandeld.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Medewerkers voeren op eigen initiatief classificatie uit. Dit gebeurt grotendeels intuïtief vanwege het individuele karakter van de expertise. Bepaalde aspecten van het proces zijn reproduceerbaar vanwege die individuele expertise en er kan sprake zijn van enige documentatie en een zeker begrip van risico's. Er is geen formeel classificatie- en rapportagebeleid. **Evidence:** 1. Gespreksverslagen contactpunten; 2. Kopieën documentatie.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	De organisatie heeft een classificatieschema vastgesteld welk consequent toegepast wordt door kundige contactpersonen. Voor rapportage is een template beschikbaar en communicatielijnen zijn bepaald. De activiteiten zijn onderdeel van een incident managementproces. **Evidence in aanvulling op 2:** 1. Kopie classificatieschema; 2. Kopie procesbeschrijving; 3. Kopie rapportagetemplate; 4. Kopie lijst contactpersonen/beoordelaars.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	Beoordelingen van informatiebeveiligingsgebeurtenissen vinden consequent volgens het vastgestelde proces door kundige beoordelaars en vastgestelde classificatieschema plaats. Gedetailleerde rapportages worden opgesteld en geëvalueerd, evenals het classificatieschema en proces periodiek beoordeeld worden. **Evidence in aanvulling op 3:** 1. Kopieën rapportages; 2. Kopieën evaluaties; 3. Kopieën trainingsbijeenkomsten en/of opleidingscertificaten; 4. Kopieën overall rapportages.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	Classificaties, beoordelingen en evaluaties zijn veelvuldig uitgevoerd. Herzieningen hebben plaatsgevonden en kennis en ervaring van betrokkenen wordt frequent gedeeld. Van fouten is geleerd; een betrouwbare, efficiënte en effectieve werkwijze is bereikt. **Evidence in aanvulling op 4:** 1. Kopieën van verslagen met leerpunten; 2. Verschillende versies classificatieschema en procesbeschrijving.	

Controledoelstelling 4.12

Cluster: Continuïteit	**ISO 27002 nummer: 16.1.4**
Controledoelstelling: Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen Informatiebeveiligingsgebeurtenissen behoren te worden beoordeeld en er behoort te worden geoordeeld of zij moeten worden geclassificeerd als informatiebeveiliging incidenten.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

4.13 Respons op informatiebeveiligingsincidenten

Cluster: Continuïteit	**ISO 27002 nummer: 16.1.5**
Controledoelstelling: Respons op informatiebeveiligingsincidenten Op informatiebeveiligingsincidenten behoort te worden gereageerd in overeenstemming met de gedocumenteerde procedures.	
Tips: geen aanvullende opmerkingen.	
Toelichting: Op informatiebeveiligingsincidenten behoort te worden gereageerd door een aangewezen contactpunt en andere relevante personen van de organisatie of externe partijen.	

Niveaus	**Beheersmaatregel (plus evidence)**	**Audit**
Volwassenheidsniveau 1 (Initieel / ad hoc)	Op incidenten wordt soms, afhankelijk van de omstandigheden, gereageerd.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Er is geen formele procedure voor het behandelen van informatiebeveiligingsincidenten, Wel kunnen binnen afdelingen of bepaalde bedrijfsprocessen afspraken gemaakt zijn. Deze zijn gebaseerd op individuele kennis en expertise en soms op beschikbare hulpmiddelen. **Evidence:** 1. Kopie procedurebeschrijving voor het behandelen van incidenten op een afdeling of in een bepaald bedrijfsproces.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Er is een vaste procedure voor het behandelen van incidenten, betrokkenen zijn bekend gemaakt met hun rol. **Evidence in aanvulling op 2:** 1. Kopie beleid of procedurebeschrijving voor het behandelen van incidenten; 2. Kopie van informatie dat de organisatie conform het beleid of procedurebeschrijving hanteert. Te denken aan: • Kopie twee meest recente rapportages van een informatiebeveiligingsincident.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	Op reguliere momenten worden over de afgelopen beveiligingsincidenten gerapporteerd, inclusief kentallen over reacties en escalaties. De directie gebruikt de rapportage als instrument om het incidentenproces te verbeteren. Ook zal gebruik gemaakt worden van een workflow tool voor afhandeling van (informatiebeveiligings-) incidenten. Ervaringen uit de praktijk kunnen eveneens leiden tot aanpassing van de procedures. **Evidence in aanvulling op 3:** 1. Eigen waarneming dat de rapportage beveiligingsincidenten bestaat; 2. Inrichtingsdocumentatie waaruit blijkt dat tool(s) voor afhandeling van beveiligingsincidenten in gebruik zijn.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	De incidentprocedure is gebaseerd op best practices en breed in gebruik. De procedure wordt geregeld geëvalueerd en zo nodig bijgesteld. De rapportage maakt onderdeel uit van een gestandaardiseerd en geïntegreerd intern audit en compliance proces. **Evidence in aanvulling op 4:** 1. Kopie waaruit blijkt welke best practice gehanteerd wordt (bijv. ITIL); 2. Eigen waarneming van (communicatie) hulpmiddelen (stickers, pop-up-berichten etc.) die de brede bekendheid ondersteunen; 3. Kopie van het interne audit en compliance proces.	

Controledoelstelling 4.13

Cluster: Continuïteit	**ISO 27002 nummer: 16.1.5**
Controledoelstelling: Respons op informatiebeveiligingsincidenten Op informatiebeveiligingsincidenten behoort te worden gereageerd in overeenstemming met de gedocumenteerde procedures.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

4.14 Informatiebeveiligingscontinuïteit implementeren

Cluster: Continuïteit	**ISO 27002 nummer: 17.1.2**

Controledoelstelling: Informatiebeveiligingscontinuïteit implementeren
De organisatie behoort processen, procedures en beheersmaatregelen vast te stellen, te documenteren, te implementeren en te handhaven om het vereiste niveau van continuïteit voor informatiebeveiliging tijdens een ongunstige situatie te waarborgen.

Tips: Continuïteit van de beveiliging van informatievoorziening.

Toelichting:
Ook tijdens ongunstige situaties, zoals tijdens crises en rampen, dient de kwaliteit van de informatiebeveiliging overeenkomstig de gestelde eisen te blijven functioneren. Daartoe worden maatregelen (in de vorm van processen, procedures en beheersmaatregelen, mogelijk in calamiteits- of continuïteitsplan) getroffen om de kwaliteit van de beveiliging tijdens ongunstige situaties op het vastgestelde niveau te handhaven.

Niveaus	Beheersmaatregel (plus evidence)	Audit
Volwassenheidsniveau 1 (Initieel / ad hoc)	Tijdens ongunstige situaties wordt een niveau van informatiebeveiliging naar beste kunnen door betrokkenen gehandhaafd.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Er zijn geen formele afspraken over het handhaven van het niveau van informatiebeveiliging tijdens ongunstige situaties. Wel kunnen binnen afdelingen of bepaalde bedrijfsprocessen afspraken gemaakt zijn. Deze zijn gebaseerd op individuele kennis en expertise en/of op ervaringen tijdens eerdere situaties. **Evidence:** 1. Gespreksverslagen met betrokkenen; 2. Kopie voorgenomen maatregelen te treffen tijdens ongunstige situaties; 3. Kopie Calamiteiten- of continuïteitsplannen.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Ongunstige omstandigheden zijn Gedefinieerd en rondom de handhaving van informatiebeveiliging in die omstandigheden zijn processen, procedures en beheersmaatregelen vastgesteld. Deze zijn aan betrokkenen gecommuniceerd. **Evidence in aanvulling op 2:** 1. Kopie inventarisatie ongunstige omstandigheden; 2. Kopie processen, procedures en maatregelen; 3. Kopieën taakbeschrijvingen tijdens ongunstige omstandigheden; 4. Kopie communicatiemiddelen waaruit bekendmaking blijkt.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	Processen, procedures en beheersmaatregelen zijn aantoonbaar in gebruik. Betrokkenen uit alle verschillende benodigde disciplines zijn bekend met hun rol en hebben mogelijk enkele ongunstige omstandigheden tijdens een oefening of in werkelijkheid meegemaakt. De afhandeling van deze omstandigheden is geëvalueerd. **Evidence in aanvulling op 3:** 1. Kopie oefendraaiboeken; 2. Kopie oefenings- en/of calamiteitenverslagen en evaluaties.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	Alle geformuleerde bijzondere omstandigheden zijn meerdere malen tijdens oefeningen nagebootst. De oefeningen zijn geëvalueerd en hebben tot aanpassingen in processen, procedures en beheersmaatregelen geleid. Alle betrokkenen zijn aantoonbaar met hun rol bekend en hebben de verwachting optimaal op alle mogelijke ongunstige situaties voorbereid te zijn. Mogelijk hebben de vooraf vastgestelde processen, procedures en beheersmaatregelen zich tijdens een werkelijke situatie in de praktijk bewezen. **Evidence:** 1. De evidence van (CMM-level) 4 over langere (minstens 3 jaar) perioden; 2. Evaluaties opgesteld tezamen met crisisexperts; 3. Kopie contracten met externe crisismanagementspecialisten.	

Controledoelstelling 4.14

Cluster: Continuïteit	**ISO 27002 nummer: 17.1.2**
Controledoelstelling: Informatiebeveiligingscontinuïteit implementeren De organisatie behoort processen, procedures en beheersmaatregelen vast te stellen, te documenteren, te implementeren en te handhaven om het vereiste niveau van continuïteit voor informatiebeveiliging tijdens een ongunstige situatie te waarborgen.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

4.15 Beschikbaarheid van informatie verwerkende faciliteiten

Cluster: Continuïteit	**ISO 27002 nummer: 17.2.1**
Controledoelstelling: Beschikbaarheid van informatie verwerkende faciliteiten Informatie verwerkende faciliteiten behoren met voldoende redundantie te worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.	
Tips: betrek hier ook de keten bij.	
Toelichting: Organisaties behoren de bedrijfseisen voor de beschikbaarheid van informatiesystemen vast te stellen. Als de beschikbaarheid niet kan worden gegarandeerd door middel van de bestaande systeemarchitectuur, behoren redundante componenten of architecturen in overweging te worden genomen.	

Niveaus	**Beheersmaatregel (plus evidence)**	**Audit**
Volwassenheidsniveau 1 (Initieel / ad hoc)	De mate waarin huidige componenten of architecturen bij uitval voldoen aan beschikbaarheidseisen is niet structureel beoordeeld. Beschikbaarheid wordt naar beste kunnen gehandhaafd.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Bij nieuwe ontwikkelingen of herziening van bestaande componenten wordt door verschillende betrokkenen nagedacht over de noodzaak van redundante voorzieningen. Dit gebeurt echter niet structureel en de kwaliteit van het resultaat is afhankelijk van de individuele kennis en ervaring. **Evidence:** 1. Kopie gespreksverslagen betrokkenen; 2. Kopie architectuurschema's; 3. Kopie (informele) impact analyses; 4. Kopie lijst spare parts.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Tijdens ontwikkeling van architecturen en inrichting van voorzieningen is redundantie als maatregel voor continuïteit consequent een optie. Ook tijdens (jaarlijkse) beoordelingen van de informatievoorziening wordt beschikbaarheid geëvalueerd. Rollen van betrokkenen (zoals proceseigenaren, architecten en beheerders) zijn daarbij helder. **Evidence als 2 plus:** 1. Kopie ontwikkelprocessen; 2. Kopie goedgekeurde impact analyses; 3. Kopie architectuurbeoordeling; 4. Kopie audit- en/of reviewverslagen.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	Over de noodzaak van redundantie is aantoonbaar in de volle breedte nagedacht en besloten. Single Points of Failures zijn in kaart gebracht en door proceseigenaren geaccepteerd of overgezet naar dubbel uitgevoerde voorzieningen. De werking van dubbele uitvoering is getest. **Evidence in aanvulling op 3:** 1. Kopie inventarisatie Single Points of Failure; 2. Kopie besluitenlijsten; 3. Kopie testverslagen.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	De gevolgen van uitval van componenten is consequent en volledig doordacht en over de gevolgen van dubbel uitvoeren voor integriteit en vertrouwelijkheid is nagedacht. De eisen worden jaarlijks, of eerder bij belangrijke wijzigingen in de organisatie, herijkt en de impact daarvan op de componenten geanalyseerd. De test op juiste werking is periodiek herhaald. De organisatie weet in alle omstandigheden aan de beschikbaarheidseisen te voldoen. **Evidence:** 1. Kopie verslagen van vroegere tests; 2. Kopie eerdere impact analyses; 3. Actuele versies van documenten als bij (CMM-level) 4.	

Controledoelstelling 4.15

Cluster: Continuïteit	**ISO 27002 nummer: 17.2.1**
Controledoelstelling: Beschikbaarheid van informatie verwerkende faciliteiten Informatie verwerkende faciliteiten behoren met voldoende redundantie te worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

5. Toegangsbeveiliging en integriteit

Nr.	ISO27002	Controledoelstelling
5.1	9.1.1	**Beleid voor toegangsbeveiliging:** Een beleid voor toegangsbeveiliging behoort te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen.
5.2	9.1.2	**Toegang tot netwerken en netwerkdiensten:** Gebruikers behoren alleen toegang te krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.
5.3	9.2.1	**Registratie en afmelden van gebruikers:** Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.
5.4	9.2.2	**Gebruikers toegang verlenen:** Een formele gebruikerstoegangsverleningsprocedure behoort te worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.
5.5	9.2.3	**Beheren van speciale toegangsrechten:** Het toewijzen en gebruik van speciale toegangsrechten behoren te worden beperkt en beheerst.
5.6	9.2.4	**Beheer van geheime authenticatie-informatie van gebruikers:** Het toewijzen van geheime authenticatie-informatie behoort te worden beheerst via een formeel beheersproces.
5.7	9.3.1	**Geheime authenticatie-informatie gebruiken:** Van gebruikers behoort te worden verlangd dat zij zich bij het gebruiken van geheime authenticatie informatie houden aan de praktijk van de organisatie.
5.8	9.4.1	**Beperking toegang tot informatie:** Toegang tot informatie en systeemfuncties van toepassingen behoort te worden beperkt in overeenstemming met het beleid voor toegangsbeveiliging.
5.9	9.4.2	**Beveiligde inlogprocedures:** Indien het beleid voor toegangsbeveiliging dit vereist, behoort toegang tot systemen en toepassingen te worden beheerst door een beveiligde inlogprocedure.
5.10	10.1.2.1	**Sleutelbeheer:** Met betrekking tot het gebruik, de bescherming en de levensduur van cryptografische sleutels behoort tijdens hun gehele levenscyclus een beleid te worden ontwikkeld.
5.11	10.1.2.2	**Sleutelbeheer:** Er wordt gebruik gemaakt van tools om cryptografische sleutels tijdens hun gehele levenscyclus adequaat te beheren.
5.12	12.4.2	**Beschermen van informatie in logbestanden:** Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang.
5.13	13.1.1	**Beheersmaatregelen voor netwerken:** Netwerken behoren te worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen.
5.14	13.1.2	**Beveiliging van netwerkdiensten:** Beveiligingsmechanismen, dienstverleningsniveaus en beheereisen voor alle netwerkdiensten behoren te worden geïdentificeerd en opgenomen in overeenkomsten betreffende netwerkdiensten. Dit geldt zowel voor diensten die intern worden geleverd als voor uitbestede diensten.
5.15	13.1.3	**Scheiding in netwerken:** Groepen van informatiediensten, -gebruikers en -systemen behoren in netwerken te worden gescheiden.
5.16	13.2.3	**Elektronische berichten**: Informatie die is opgenomen in elektronische berichten behoort passend te zijn beschermd
5.17	14.1.3	**Transacties van toepassingen beschermen:** Informatie die deel uitmaakt van transacties van toepassingen behoort te worden beschermd ter voorkoming van onvolledige overdracht, foutieve routering, onbevoegd wijzigen van berichten, onbevoegd openbaar maken, onbevoegd vermenigvuldigen of afspelen.

Beperk voor de benchmark de scope tot SIS (inclusief studieresultaten), HR, Fin en ELO.

5.1 Beleid voor toegangsbeveiliging

Cluster: Toegangsbeveiliging en in3tegriteit	**ISO 27002 nummer: 9.1.1**	
Controledoelstelling: Beleid voor toegangsbeveiliging Een beleid voor toegangsbeveiliging behoort te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen.		
Tips: toegangsbeveiliging zowel voor het netwerk als voor applicaties. Zie “Leidraad toegangsbeveiliging”.		
Toelichting: Er behoort toegangsbeleid te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfseisen en beveiligingseisen voor toegang.		
Niveaus	**Beheersmaatregel (plus evidence)**	**Audit**
Volwassenheidsniveau 1 (Initieel / ad hoc)	Er is ad-hoc toegangsbeleid. Systeembeheer bepaalt vaak of iemand al dan niet toegang krijgt.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Er is toegangsbeleid, maar niet formeel vastgesteld en gedocumenteerd. **Evidence:** 1. Gespreksverslag hoofd systeembeheer.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Het toegangsbeleid is vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfseisen en beveiligingseisen voor toegang. **Evidence in aanvulling op 2:** 1. Kopie van toegangsbeleid; 2. Kopie van notulen waarin het toegangsbeleid is goedgekeurd door management; 3. Kopie flyers, nieuwsbrieven of e-mails waaruit blijkt dat de gebruikers op de hoogte zijn van de goedgekeurde toegangsbeleid. 4. Kopie van informatie waarin is beoordeeld dat de bedrijfseisen en beveiligingseisen voor toegang zijn meegenomen in het beleid. Te denken aan: • Kopie risicoanalyse; • Kopie de toegepaste normenkader of wetregelgeving voor het beleid.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	Het toegangsbeleid is vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfseisen en beveiligingseisen voor toegang. Er vindt logging plaats en controle op naleving. **Evidence in aanvulling op 3:** 1. Logs van toegang en verslagen van controle op deze logs (m.b.t. naleving beleid) .	
Volwassenheidsniveau 5 (Geoptimaliseerd)	Identity en Access management is geïmplementeerd en ondersteund door geautomatiseerde processen. De effectiviteit wordt regelmatig gecontroleerd. **Evidence in aanvulling op 4:** 1. Beschrijving geautomatiseerde processen; 2. Verslagen van periodieke controle op effectiviteit.	

Controledoelstelling 5.1

Cluster: Toegangsbeveiliging en in3tegriteit	**ISO 27002 nummer: 9.1.1**
Controledoelstelling: Beleid voor toegangsbeveiliging Een beleid voor toegangsbeveiliging behoort te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

5.2 Toegang tot netwerken en netwerkdiensten

Cluster: Toegangsbeveiliging en integriteit	**ISO 27002 nummer: 9.1.2**	
Controledoelstelling: Toegang tot netwerken en netwerkdiensten Gebruikers behoren alleen toegang te krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.		
Tips: het betreft hier technische netwerkdiensten, denk aan VPN en draadloos netwerk.		
Toelichting: Een beleid voor het gebruik van netwerken en netwerkdiensten behoort te worden geformuleerd.		
Niveaus	**Beheersmaatregel (plus evidence)**	**Audit**
Volwassenheidsniveau 1 (Initieel / ad hoc)	Er is geen beleid rond gebruikerstoegang tot netwerk(diensten) opgesteld. Toegang en toegangsmethoden worden ad hoc toegekend op het moment dat toegang aangevraagd worden.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Het netwerk is gesegmenteerd, meerdere toegangsmethoden zijn beschikbaar en er is een best practice ontstaan rond de toegang die gebruikers tot netwerk(diensten) krijgen toegewezen. De daadwerkelijk beschikbaar gestelde methode (VPN verplicht of niet, al dan niet token verstrekken, toegang vanaf openbaar netwerk toegestaan) blijft afhankelijk van de aanvrager en uitvoerend beheerder. **Evidence:** 1. Gespreksverslag beheerder; 2. Kopie beschrijving netwerksegmenten; 3. Technische voorzieningen (tokens, accesslists) aanwezig; 4. Inrichting firewall maakt onderscheid in toegang mogelijk.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Beleid rond netwerktoegang is aanwezig, voorzieningen zijn gestandaardiseerd. **Evidence in aanvulling op 2:** 1. Kopie vastgesteld toegangsbeleid met daarin de te onderscheiden toegangspaden en toegangsmethode(n) per type gebruiker; 2. Kopie materiaal waaruit blijkt dat beleid is gecommuniceerd; 3. Registratie van aanvragen en toekenningen is aanwezig.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	Proces wordt aantoonbaar uitgevoerd en bewaking op juist gebruik vindt plaats. **Evidence in aanvulling op 3:** 1. Registratie van uitgegeven certificaten en/of tokens; 2. Logs van toegang en verslagen van controle op deze logs (m.b.t. naleving en evaluatie van het beleid).	
Volwassenheidsniveau 5 (Geoptimaliseerd)	Beleid wordt aantoonbaar gedurende minstens 3 jaar gehanteerd, evaluatie heeft ten minste 2 keer plaatsgevonden. **Evidence in aanvulling op 3:** 1. Kopieën periodieke (halfjaarlijkse) gebruiksrapportages; 2. Kopieën incidentrapportage(s) maken blijk van beleidsevaluatie; 3. Verslagen van periodieke controle op effectiviteit.	

Controledoelstelling 5.2

Cluster: Toegangsbeveiliging en integriteit	**ISO 27002 nummer: 9.1.2**
Controledoelstelling: Toegang tot netwerken en netwerkdiensten Gebruikers behoren alleen toegang te krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

5.3 Registratie en afmelden van gebruikers

Cluster: Toegangsbeveiliging en integriteit	**ISO 27002 nummer: 9.2.1**	
Controledoelstelling: Registratie en afmelden van gebruikers Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.		
Tips: het betreft nieuwe gebruikers en het verwijderen van gebruikers.		
Toelichting: Er behoren formele procedures voor het registreren en afmelden van gebruikers te zijn vastgesteld om het verlenen en intrekken van toegangsrechten tot alle informatiesystemen en -diensten mogelijk te maken.		
Niveaus	**Beheersmaatregel (plus evidence)**	**Audit**
Volwassenheidsniveau 1 (Initieel / ad hoc)	Er zijn geen formele procedures voor het registreren en afmelden van gebruikers vastgesteld. Dit gebeurt op een ad hoc basis.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Er zijn gedeeltelijk formele procedures voor het registreren en afmelden van gebruikers vastgesteld. **Evidence:** 1. Procedurebeschrijvingen die beschikbaar zijn voor registreren en afmelden van gebruikers voor enkele informatiesystemen of -diensten.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Er zijn formele procedures voor het registreren en afmelden van gebruikers vastgesteld. **Evidence in aanvulling op 2:** 1. Kopie procedurebeschrijving voor de registratie van gebruikers en beheerders; 2. Kopie van informatie waaruit blijkt dat de organisatie gebruiker-ID's conform de procedures heeft toegekend. Te denken aan: • Kopie van aanvraagformulieren voor gebruikers-ID's; • Kopie uit systeem waaruit blijkt dat de gebruikers een unieke gebruikersidentificatie (ID) hebben; • Kopie twee meest recente rapportage waaruit blijkt dat de organisatie controle uitvoert op verwijderen of blokkeren van overtollige gebruiker-ID's en accounts.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	Er zijn formele procedures voor het registreren en afmelden van gebruikers vastgesteld. Deze worden in alle systemen toegepast en er vindt controle op naleving plaats. **Evidence in aanvulling op 3:** 1. Verslagen van periodieke controle op naleving.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	Identity en Access management is geïmplementeerd en ondersteund door geautomatiseerde processen. De effectiviteit wordt regelmatig gecontroleerd. **Evidence in aanvulling op 4:** 1. Beschrijving geautomatiseerd proces; 2. Verslagen van de effectiviteitscontroles.	

Controledoelstelling 5.3

Cluster: Toegangsbeveiliging en integriteit	**ISO 27002 nummer: 9.2.1**
Controledoelstelling: Registratie en afmelden van gebruikers Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

5.4 Gebruikers toegang verlenen

Cluster: Toegangsbeveiliging en integriteit	**ISO 27002 nummer: 9.2.2**	
Controledoelstelling: Gebruikers toegang verlenen Een formele gebruikerstoegangsverleningsprocedure behoort te worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.		
Tips: het verlenen van toegangsrechten tot applicaties op basis van functie en rollen (RBAC) van medewerkers.		
Toelichting: Een procedure voor het verlenen (toekennen, intrekken) van autorisaties aan gebruikers voor alle systemen en diensten is beschreven. Deze procedure is vastgesteld en aantoonbaar in gebruik.		
Niveaus	**Beheersmaatregel (plus evidence)**	**Audit**
Volwassenheidsniveau 1 (Initieel / ad hoc)	Er zijn geen formele procedures voor het toekennen en intrekken van toegangsrechten (autorisaties) vastgesteld. Registreren en intrekken gebeurt op een ad hoc basis.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Er zijn gedeeltelijk – zoals voor een deel van de systemen en diensten - formele procedures voor het toekennen en intrekken van toegangsrechten vastgesteld. **Evidence:** 1. Procedurebeschrijvingen die beschikbaar zijn voor het toekennen en intrekken van toegangsrechten aan gebruikers voor enkele informatiesystemen of -diensten.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Voor alle informatiesystemen of –diensten zijn formele procedures voor het toekennen en intrekken van toegangsrechten vastgesteld.) **Evidence in aanvulling op 2:** 1. Kopie procedurebeschrijving voor het toekennen van toegangsrechten; 2. Kopie van informatie waaruit blijkt dat de organisatie toegangsrechten conform de beleid en procedures heeft toegekend. Te denken aan: • Kopie van autorisatiematrix waarin relatie tussen functie en autorisatie blijkt; • Kopie vastgestelde toekenbare gebruikersprofielen; • Kopie goedkeuring systeemeigenaar voor toekenning autorisaties; • Kopie administratie uitgegeven, gemuteerde en ingetrokken autorisaties; • Kopie twee meest recente rapportage waaruit blijkt dat de organisatie controle uitvoert op verwijderen of blokkeren van toegangsrechten.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	Er zijn formele procedures voor het registreren en afmelden van gebruikers vastgesteld. Deze worden in alle systemen toegepast en er vindt controle op naleving plaats. **Evidence in aanvulling op 3:** 1. Geautomatiseerd autorisatiebeheer (zoals via IAM-tool met RBAC); 2. Verslagen van periodieke controle op naleving; 3. Gebruiksvoorwaarden beschrijven sancties bij constateren misbruik van autorisaties.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	Identity en Access management is geïmplementeerd en ondersteund door geautomatiseerde processen. De effectiviteit wordt regelmatig gecontroleerd. **Evidence in aanvulling op 4:** 1. Beschrijving geautomatiseerd proces; 2. Verslagen van de effectiviteitscontroles en mogelijk opgelegde sancties.	

Controledoelstelling 5.4

Cluster: Toegangsbeveiliging en integriteit	**ISO 27002 nummer: 9.2.2**
Controledoelstelling: Gebruikers toegang verlenen Een formele gebruikerstoegangsverleningsprocedure behoort te worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

5.5 Beheren van speciale toegangsrechten

Cluster: Toegangsbeveiliging en integriteit	**ISO 27002 nummer: 9.2.3**	
Controledoelstelling: Beheren van speciale toegangsrechten Het toewijzen en het gebruik van speciale toegangsrechten behoren te worden beperkt en beheerst.		
Tips: het betreft hier de super users / administrators rechten.		
Toelichting: De toewijzing en het gebruik van speciale bevoegdheden behoren te worden beperkt en beheerst.		
Niveaus	**Beheersmaatregel (plus evidence)**	**Audit**
Volwassenheidsniveau 1 (Initieel / ad hoc)	De toewijzing en het gebruik van speciale bevoegdheden is ad-hoc geregeld.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	De toewijzing en het gebruik van speciale bevoegdheden is beperkt. Hier zijn afspraken over gemaakt, maar die zijn niet vastgelegd of gecommuniceerd. **Evidence:** 1. Gespreksverslag hoofd systeembeheer.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	De toewijzing en het gebruik van speciale bevoegdheden is beperkt en beheerst volgens vaste procedures. Er is een integriteitscode voor technisch en functioneel beheerders. **Evidence in aanvulling op 2:** 1. Kopie van een integriteitscode die bestemd is voor technische en functioneel beheerders (indien opgenomen in functieomschrijving of contract, kopie functieomschrijving of contract); 2. Kopie beleid of procesbeschrijving voor het beheer van speciale bevoegdheden; 3. Kopie functie- of rolbeschrijvingen van de beheerders van speciale bevoegdheden; 4. Kopie vanuit systeem waaruit blijkt dat de technische of functioneel beheerders die speciale bevoegdheden hebben, ook een gewone gebruikers-ID hebben voor hun reguliere werkzaamheden.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	De toewijzing en het gebruik van speciale bevoegdheden is beperkt en beheerst. Beleid hiervoor is vastgelegd en er wordt toegezien op de naleving. **Evidence in aanvulling op 3:** 1. Kopie beleid; 2. Verslagen van nalevingscontrole.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	Identity en Access management is ook voor speciale bevoegdheden geïmplementeerd en wordt ondersteund door geautomatiseerde processen. De effectiviteit wordt regelmatig gecontroleerd. **Evidence in aanvulling op 4:** 1. Beschrijving geautomatiseerde processen (voor de speciale bevoegdheden); 2. Berslagen van de periodieke controle op effectiviteit.	

Controledoelstelling 5.5

Cluster: Toegangsbeveiliging en integriteit	**ISO 27002 nummer: 9.2.3**
Controledoelstelling: Beheren van speciale toegangsrechten Het toewijzen en het gebruik van speciale toegangsrechten behoren te worden beperkt en beheerst.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

5.6 Beheer van geheime authenticatie-informatie van gebruikers

Cluster: Toegangsbeveiliging en integriteit	**ISO 27002 nummer: 9.2.4**	
Controledoelstelling: Beheer van geheime authenticatie-informatie van gebruikers Het toewijzen van geheime authenticatie-informatie behoort te worden beheerst via een formeel beheersproces.		
Tips: het betreft het wachtwoordenbeleid dat op basis van delegatie is goedgekeurd.		
Toelichting: De toewijzing van wachtwoorden behoort met een formeel beheerproces te worden beheerst.		
Niveaus	**Beheersmaatregel (plus evidence)**	**Audit**
Volwassenheidsniveau 1 (Initieel / ad hoc)	De toewijzing van wachtwoorden is niet formeel beheerst.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	De toewijzing van wachtwoorden voor sommige systemen is met een formeel proces beheerst. **Evidence:** 1. Procedurebeschrijving van de beheerste wachtwoord toewijzing.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	De toewijzing van wachtwoorden is met een formeel beheerproces beheerst. **Evidence in aanvulling op 2:** 1. Kopie beleid en procedurebeschrijving van het beheer van gebruikers-wachtwoorden; 2. Kopie notulen waaruit blijkt dat het beheer van gebruikerswachtwoorden is goedgekeurd; 3. Kopie van informatie waaruit blijkt dat de organisatie conform het beleid heeft uitgevoerd. Te denken aan: • Kopie verklaring waaruit blijkt dat de gebruikers een verklaring ondertekenen dat zij hun persoonlijke wachtwoorden geheimhouden; • Kopie uit systeem waaruit blijkt dat bepaalde minimale gestelde parameters zijn ingesteld.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	De toewijzing van wachtwoorden is met een formeel beheerproces beheerst. Effectiviteit wordt gecontroleerd. **Evidence in aanvulling op 3:** 1. Verslagen van periodieke controle op effectiviteit.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	De toewijzing van wachtwoorden is met een formeel beheerproces beheerst. Effectiviteit wordt gecontroleerd en efficiency geëvalueerd. **Evidence in aanvulling op 4:** 1. Verslagen van periodieke evaluatie.	

Controledoelstelling 5.6

Cluster: Toegangsbeveiliging en integriteit	**ISO 27002 nummer: 9.2.4**
Controledoelstelling: Beheer van geheime authenticatie-informatie van gebruikers Het toewijzen van geheime authenticatie-informatie behoort te worden beheerst via een formeel beheersproces.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

5.7 Geheime authenticatie-informatie gebruiken

Cluster: Toegangsbeveiliging en integriteit	**ISO 27002 nummer: 9.3.1**
Controledoelstelling: Geheime authenticatie-informatie gebruiken Van gebruikers behoort te worden verlangd dat zij zich bij het gebruiken van geheime authenticatie informatie houden aan de praktijk van de organisatie.	
Tips: geen aanvullende opmerkingen.	
Toelichting: Gebruikers dienen op juiste wijze gebruik van te maken van de aan hen toegekende wachtwoorden, pincodes, tokens of certificaten. Dit wordt bereikt door gebruikers te informeren over de wijze waarop zij met deze geheime authenticatie informatie dienen om te gaan.	

Niveaus	**Beheersmaatregel (plus evidence)**	**Audit**
Volwassenheidsniveau 1 (Initieel / ad hoc)	Authenticatiepraktijken van de organisatie worden niet gecommuniceerd, de wijze van gebruik van geheime authenticatie informatie wordt aan gebruikers overgelaten.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Bij het beschikbaar stellen van een authenticatiemiddel wordt verteld hoe met middel dient te worden omgegaan of, bij verstrekking via mail of brief, wordt in een herbruikbare tekst het gewenste gebruik toegelicht. **Evidence:** 1. Gespreksverslag beheerder; 2. Kopie brief of mail met uitleg gewenst gebruik.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Per authenticatiemiddel is een handleiding beschikbaar waarin het verwachte gebruik is uitgelegd dan wel voorgeschreven. Te denken valt aan uitleg over: • Verplichte geheimhouding; • Het niet noteren van toegangscodes; • Regels voor goede wachtwoorden (minimumlengte, speciale tekens, niet bestaande woorden); • Gebruik van verschillende wachtwoorden voor verschillende noodzakelijke beveiligingsniveaus. **Evidence als 2 plus:** 1. Kopie handleidingen; 2. Kopieën brieven en/of mails waarin handleidingen aan gebruikers zijn aangeboden.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	Verstrekking van authenticatie informatie vindt geüniformeerd of geautomatiseerd plaats, correct gebruik wordt ook na eerste uitgifte gecommuniceerd. **Evidence in aanvulling op 3:** 1. Authenticatiecodes worden geautomatiseerd gegenereerd en beveiligd (via separaat kanaal) gecommuniceerd; 2. Format van wachtwoorden wordt in systemen afgedwongen; 3. Juist gebruik van authenticatiemiddelen wordt periodiek aan gebruikers gecommuniceerd (mondeling in afdelingsoverleg of schriftelijk via flyers/mails).	
Volwassenheidsniveau 5 (Geoptimaliseerd)	Gebruik wordt periodiek geëvalueerd op kwaliteit en werkbaarheid, gebruikers hebben keuze uit authenticatiemethoden. **Evidence in aanvulling op 4:** 1. Bij incidenten wordt wachtwoordbeleid geëvalueerd; 2. Gebruikers kunnen kiezen uit de authenticatiemethode(n) zij prettig vinden in gebruik en de organisatie passend vinden voor het risiconiveau (regulier wachtwoord, passcode, picture password, TAN-code etc.); 3. Gebruikers worden periodiek (geautomatiseerd) gewezen op de sterkte van hun passcodes en wachtwoorden.	

Controledoelstelling 5.7

Cluster: Toegangsbeveiliging en integriteit	**ISO 27002 nummer: 9.3.1**
Controledoelstelling: Geheime authenticatie-informatie gebruiken Van gebruikers behoort te worden verlangd dat zij zich bij het gebruiken van geheime authenticatie informatie houden aan de praktijk van de organisatie.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

5.8 Beperking toegang tot informatie

Cluster: Toegangsbeveiliging en integriteit	**ISO 27002 nummer: 9.4.1**	
Controledoelstelling: Beperking toegang tot informatie Toegang tot informatie en systeemfuncties van toepassingen behoort te worden beperkt in overeenstemming met het beleid voor toegangsbeveiliging.		
Tips: de gebruiker ziet alleen die opties in het keuzemenu waartoe hij rechten heeft.		
Toelichting: Toegang tot informatie en functies van toepassingssystemen door gebruikers en ondersteunend personeel behoort te worden beperkt overeenkomstig het vastgestelde toegangsbeleid.		
Niveaus	**Beheersmaatregel (plus evidence)**	**Audit**
Volwassenheidsniveau 1 (Initieel / ad hoc)	Toegang tot informatie en functies van toepassingssystemen door gebruikers en ondersteunend personeel is soms beperkt. Er is geen beleid.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Toegang tot informatie en functies van toepassingssystemen door gebruikers en ondersteunend personeel is beperkt, er is geen samenhangend beleid. **Evidence:** 1. Uitdraai van gebruikers(groepen) en hun rechten op folders; 5. Uitdraai uit een informatiesysteem met groepen of individuele gebruikers en bijhorende rechten (autorisaties, menutoegang.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Toegang tot informatie en functies van toepassingssystemen door gebruikers en ondersteunend personeel is beperkt overeenkomstig het vastgestelde toegangsbeleid. **Evidence in aanvulling op 2:** 1. Kopie toegangsbeleid; 2. Kopie van informatie waaruit blijkt dat de toegang tot informatie en functies van toepassingssystemen is uitgevoerd conform vastgesteld toegangsbeleid. Te denken aan: • Kopie schermprint waarin het gebruik van menu's waarmee toegang tot functies van het informatiesysteem zijn beheerst; • Kopie aanvraagformulier; • Kopie UFO-profielen; • kopie overzicht waaruit blijkt dat er 1 inlognaam per medewerker is; • toegekende autorisatie is conform aanvraagformulier.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	Toegang tot informatie en functies van toepassingssystemen door gebruikers en beheerders is beperkt overeenkomstig het vastgestelde toegangsbeleid. Toegang wordt gelogd en gecontroleerd. Misbruik wordt automatisch gesignaleerd, bijvoorbeeld m.b.v. IDS- of IPS-systemen. **Evidence in aanvulling op 3:** 1. Overzicht logging, controleverslag; 2. Rapportage uit IDS- of IPS-systeem.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	Toegang tot informatie en functies van toepassingssystemen door gebruikers en ondersteunend personeel is beperkt overeenkomstig het vastgestelde toegangsbeleid. Toegang wordt gelogd en logging wordt gecontroleerd en er wordt over gerapporteerd. Regelmatig vindt evaluatie plaats van de toegepaste autorisatie technieken. **Evidence in aanvulling op 4:** 1. Verslaglegging van evaluaties van toegepaste autorisatietechnieken.	

Controledoelstelling 5.8

Cluster: Toegangsbeveiliging en integriteit	**ISO 27002 nummer: 9.4.1**
Controledoelstelling: Beperking toegang tot informatie Toegang tot informatie en systeemfuncties van toepassingen behoort te worden beperkt in overeenstemming met het beleid voor toegangsbeveiliging.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

5.9 Beveiligde inlogprocedures

Cluster: Toegangsbeveiliging en integriteit	**ISO 27002 nummer: 9.4.2**
Controledoelstelling: Beveiligde inlogprocedures Indien het beleid voor toegangsbeveiliging dit vereist, behoort toegang tot systemen en toepassingen te worden beheerst door een beveiligde inlogprocedure.	
Tips: een aantal aanbevelingen: • 2-way authenticatie; • Wachtwoord kan niet worden “afgeluisterd”; • Wachtwoord wordt niet weergegeven; • Wachtwoord en username komen niet overeen is de juiste foutmelding bij onjuist ingetypt wachtwoord.	
Toelichting: Toegang tot besturingssystemen behoort te worden beheerst met een beveiligde inlogprocedure.	

Niveaus	**Beheersmaatregel (plus evidence)**	**Audit**
Volwassenheidsniveau 1 (Initieel / ad hoc)	Toegang tot besturingssystemen wordt beheerst zonder een beveiligde inlogprocedure. Adminrechten worden niet beheerd. Accounts worden regelmatig met meerdere personen gedeeld en/of hebben standaard wachtwoorden.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Toegang tot besturingssystemen wordt incidenteel beheerst met een beveiligde inlogprocedure. Er is geen formeel beleid. Standaardwachtwoorden moeten verplicht gewijzigd worden, dit wordt technisch afgedwongen. **Evidence:** 1. Schermprint vanuit een besturingssysteem waaruit blijkt dat de toegang beheerst wordt door een beveiligde inlogprocedure.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Toegang tot besturingssystemen wordt beheerst met een beveiligde inlogprocedure volgens een vastgestelde policy. **Evidence in aanvulling op 2:** 1. Kopie beleid voor beveiligde inlogprocedures; 2. Kopie van notulen waaruit blijkt dat het beleid is goedgekeurd door het management; 3. Schermprint uit besturingssystemen waaruit blijkt dat het conform het beleid is ingericht; 4. Signalering van poging tot onterechte toegang (uit logbestand).	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	Toegang tot besturingssystemen wordt beheerst met een beveiligde inlogprocedure. Er is een beschreven policy en er vindt controle op naleving plaats. **Evidence in aanvulling op 3:** 1. Logging van toegang tot besturingssystemen; 2. Zichtbare review van deze logbestanden (Checklist aan de hand waarvan te zien is dat periodiek de logs van access-pogingen worden gereviewd, geautomatiseerde uitzonderingsrapportages).	
Volwassenheidsniveau 5 (Geoptimaliseerd)	Toegang tot besturingssystemen wordt beheerst met een beveiligde inlogprocedure. Er is een beschreven policy. Waar nodig wordt two-factor authenticatie toegepast. Er vindt controle plaats op de toegang, waar mogelijk worden maatregelen technisch afgedwongen. **Evidence in aanvulling op 4:** 1. Beschrijving technische inrichting afgedwongen controle; 2. Verslagen periodieke evaluatie van de effectiviteit van de inrichting van beveiligde toegang.	

Controledoelstelling 5.9

Cluster: Toegangsbeveiliging en integriteit	**ISO 27002 nummer: 9.4.2**
Controledoelstelling: Beveiligde inlogprocedures Indien het beleid voor toegangsbeveiliging dit vereist, behoort toegang tot systemen en toepassingen te worden beheerst door een beveiligde inlogprocedure.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

5.10 Sleutelbeheer (1)

Cluster: Toegangsbeveiliging en integriteit	**ISO 27002 nummer: 10.1.2**
Controledoelstelling: Sleutelbeheer Met betrekking tot het gebruik, de bescherming en de levensduur van cryptografische sleutels behoort tijdens hun gehele levenscyclus een beleid te worden ontwikkeld.	
Tips: beleid t.a.v. digitale sleutels. Bijvoorbeeld wanneer Bitlocker wordt toegepast is er een beleid waarin wordt omschreven hoe de sleutel wordt beheerd, hoe versleutelde bestanden teruggehaald kunnen worden bij verlies van de originele encryptiesleutel en hoe vervolgens een nieuwe encryptiesleutel wordt ingevoerd.	
Toelichting: Er is sleutelbeheer vastgesteld ter ondersteuning van het gebruik van cryptografische technieken binnen de organisatie.	

Niveaus	**Beheersmaatregel (plus evidence)**	**Audit**
Volwassenheidsniveau 1 (Initieel / ad hoc)	Er bestaan geen procedures die het sleutelbeheerproces weergeven en beschrijven.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Er bestaan niet-geformaliseerde procedures die het sleutelbeheerproces weergeven en beschrijven. **Evidence:** 1. Gespreksverslag hoofd systeembeheer.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Er bestaan vaste procedures die het sleutelbeheerproces weergeven en beschrijven. **Evidence in aanvulling op 2:** 1. Kopie procedurebeschrijving van sleutelbeheerproces; 2. Kopie notulen waarin blijkt dat het beleid is goedgekeurd door management; 3. Kopie van informatie waaruit blijkt dat de organisatie conform de procedure werkt. Te denken aan: • kopie systeemprint toepassing encryptie; • steekproef waarbij servicedesk of systeembeheer bijv. een versleutelde laptop leesbaar moeten krijgen of van nieuwe sleutel moet kunnen voorzien.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	Er bestaan procedures die het sleutelbeheerproces weergeven en beschrijven. Deze worden periodiek getoetst (technische audit). **Evidence in aanvulling op 3:** 1. Verslagen van een periodieke toetsing.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	Er bestaan procedures die het sleutelbeheerproces weergeven en beschrijven. Deze worden periodiek getoetst en de effectiviteit en efficiency van deze procedures wordt periodiek geëvalueerd. **Evidence in aanvulling op 4:** 1. Verslagen van een periodieke evaluatie.	

Controledoelstelling 5.10

Cluster: Toegangsbeveiliging en integriteit	**ISO 27002 nummer: 10.1.2**
Controledoelstelling: Sleutelbeheer Met betrekking tot het gebruik, de bescherming en de levensduur van cryptografische sleutels behoort tijdens hun gehele levenscyclus een beleid te worden ontwikkeld.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

5.11 Sleutelbeheer (2)

Cluster: Toegangsbeveiliging en integriteit	**ISO 27002 nummer: 10.1.2**	
Controledoelstelling: Sleutelbeheer Er wordt gebruik gemaakt van tools om cryptografische sleutels tijdens hun gehele levenscyclus adequaat te beheren.		
Tips: beheer van cryptografische sleutels (bijvoorbeeld Bitlocker maakt ook gebruik van een cryptografische sleutel).		
Toelichting: Er is sleutelbeheer vastgesteld ter ondersteuning van het gebruik van cryptografische technieken binnen de organisatie.		
Niveaus	**Beheersmaatregel (plus evidence)**	**Audit**
Volwassenheidsniveau 1 (Initieel / ad hoc)	Er wordt geen gebruik gemaakt van tools ten behoeve van sleutelbeheer.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Er wordt soms gebruik gemaakt van tools ten behoeve van sleutelbeheer. **Evidence:** 1. Lijst gehanteerde tools.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Er wordt structureel gebruik gemaakt van tools ten behoeve van sleutelbeheer. **Evidence in aanvulling op 2:** 1. Kopie van informatie waaruit het blijkt dat de organisatie tools ten behoeve van sleutelbeheer in gebruik heeft. Te denken aan: • beleidsstuk/werkinstructie waarin het structureel gebruik van tools voor sleutelbeheer wordt aangegeven; • kopie systeem rapportage; • kopie productomschrijvingen; • kopie systeemprint toepassing sleutelbeheer.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	Er wordt structureel gebruik gemaakt van tools ten behoeve van sleutelbeheer. De goede werking en het goede gebruik van deze tools wordt periodiek getoetst. **Evidence in aanvulling op 3:** 1. Toets verslagen werking en gebruik.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	Er wordt structureel gebruik gemaakt van tools ten behoeve van sleutelbeheer. De goede werking en het goede gebruik van deze tools wordt periodiek getoetst en de effectiviteit en efficiency geëvalueerd **Evidence in aanvulling op 4:** 1. Evaluatieverslagen werking en gebruik van deze tools.	

Controledoelstelling 5.11

Cluster: Toegangsbeveiliging en integriteit	**ISO 27002 nummer: 10.1.2**
Controledoelstelling: Sleutelbeheer Er wordt gebruik gemaakt van tools om cryptografische sleutels tijdens hun gehele levenscyclus adequaat te beheren.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

5.12 Beschermen van informatie in logbestanden

Cluster: Toegangsbeveiliging en integriteit	**ISO 27002 nummer: 12.4.2**	
Controledoelstelling: Beschermen van informatie in logbestanden Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang.		
Tips: geen aanvullende opmerkingen.		
Toelichting: Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen inbreuk en onbevoegde toegang.		
Niveaus	**Beheersmaatregel (plus evidence)**	**Audit**
Volwassenheidsniveau 1 (Initieel / ad hoc)	Logfaciliteiten en informatie in logbestanden zijn niet of niet specifiek beschermd tegen inbreuk en onbevoegde toegang.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Sommige logfaciliteiten en informatie in sommige logbestanden zijn beschermd tegen inbreuk en onbevoegde toegang, de manier waarop is niet overal gelijk. **Evidence:** 1. (Procedure) beschrijving van de bescherming van een set van logbestanden.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Logfaciliteiten en informatie in logbestanden zijn op een samenhangende manier beschermd tegen inbreuk en onbevoegde toegang, met passende maatregelen. **Evidence in aanvulling op 2:** 1. Kopie beleid en procedurebeschrijving voor bescherming van informatie in logbestanden; 2. Kopie van informatie waaruit blijkt dat de organisatie conform het beleid of procedurebeschrijving heeft uitgevoerd. Te denken aan: • schermprint uit systeem waaruit blijkt dat bewerken of wissen van logbestanden niet mogelijk is; • kopie lijst van registratie van alle goedgekeurde wijzigingen in het soort berichten (change managementproces op de logbestanden).	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	Alle logfaciliteiten en informatie in logbestanden zijn beschermd tegen inbreuk en onbevoegde toegang. Dit wordt systematisch gecontroleerd. **Evidence in aanvulling op 3:** 1. Kopie beleid en procedurebeschrijving voor bescherming van informatie in logbestanden; 2. Overzicht van alle logfaciliteiten; 3. Verslagen systematische controle (bijvoorbeeld maandelijkse vergelijking acl's op folder en file niveau voor de logsystemen).	
Volwassenheidsniveau 5 (Geoptimaliseerd)	Alle logfaciliteiten en informatie in logbestanden zijn beschermd tegen inbreuk en onbevoegde toegang. Dit wordt systematisch gecontroleerd en periodiek geëvalueerd op efficiëntie en effectiviteit **Evidence in aanvulling op 4:** 1. Kopie beleid en procedurebeschrijving voor bescherming van informatie in logbestanden; 2. Overzicht van alle logfaciliteiten; 3. Verslagen systematische controle (bijvoorbeeld maandelijkse vergelijking acl's op folder en file niveau voor de logsystemen); 4. Verslagen periodieke evaluatie.	

Controledoelstelling 5.12

Cluster: Toegangsbeveiliging en integriteit	**ISO 27002 nummer: 12.4.2**
Controledoelstelling: Beschermen van informatie in logbestanden Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

5.13 Beheersmaatregelen voor netwerken

Cluster: Toegangsbeveiliging en integriteit	**ISO 27002 nummer: 13.1.1**	
Controledoelstelling: Beheersmaatregelen voor netwerken Netwerken behoren te worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen.		
Tips: beoordeling netwerk security. De volwassenheid van de documentatie van het netwerk wordt beoordeeld.		
Toelichting: Er behoren beheersmaatregelen te worden geïmplementeerd om de veiligheid van informatie in netwerken te waarborgen en aangesloten diensten tegen onbevoegde toegang te beschermen.		
Niveaus	**Beheersmaatregel (plus evidence)**	**Audit**
Volwassenheidsniveau 1 (Initieel / ad hoc)	Netwerkinrichting en beheeractiviteiten vinden ad hoc plaats, naar inzicht van individuele beheerders. Best practices zijn niet afgestemd, de verschillende netwerkcomponenten zijn niet in samenhang ingericht.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Beheerders richten apparatuur doorgaans op gelijke wijze in en voeren acties doorgaans op dezelfde wijze uit. Mogelijk zijn deze best practices beschreven en in een Wiki opgenomen. Desondanks blijft de werkwijze afhankelijk van de individuele beheerder. **Evidence:** 1. Gespreksverslagen met beheerders; 2. Kopie best practices, mogelijk in een Wiki.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Standaard configuraties zijn beschreven en bij beheerders bekend. Het beheerproces voor netwerken is geformaliseerd, o.a. middels standaard changes en staat los van applicatie- en systeembeheer. Beheerders hebben ook duidelijke functiebeschrijvingen en tools voor beheer. **Evidence in aanvulling op 2:** 1. Kopie configuratiebeschrijvingen of links naar referentiesite; 2. Kopie procesbeschrijving en procedures (standaard changes); 3. Kopie functiebeschrijvingen; 4. Kopie handleiding gebruikte tools.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	Alle componenten zijn volgens architectuur in samenhang ingericht, technische en workflow tools ondersteunen de uitvoering. Beheer van componenten vindt centraal plaats, correcte inrichting wordt periodiek (automatisch) gecontroleerd. Waar volgens risico-classificatie nodig wordt cryptografie toegepast. **Evidence in aanvulling op 3:** 1. Kopie netwerkarchitectuur; 2. Kopieën inrichtingsdocumenten; 3. Kopieën periodieke rapportage; 4. Kopieën beheer overleggen.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	Netwerken zijn volgens architectuur ingericht en worden proactief beheerd. Aan de hand van periodieke rapportages en real-time monitoring wordt zowel architectuur als beheerproces regelmatig geëvalueerd en verbeterd.) **Evidence in aanvulling op 4:** 1. Kopieën change evaluaties. 2. Kopieën voorgaande architecturen; 3. Kopieën voorgaande procesbeschrijvingen.	

Controledoelstelling 5.13

Cluster: Toegangsbeveiliging en integriteit	**ISO 27002 nummer: 13.1.1**
Controledoelstelling: Beheersmaatregelen voor netwerken Netwerken behoren te worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

5.14 Beveiliging van netwerkdiensten

Cluster: Toegangsbeveiliging en integriteit	**ISO 27002 nummer: 13.1.2**

Controledoelstelling: Beveiliging van netwerkdiensten
Beveiligingsmechanismen, dienstverleningsniveaus en beheer eisen voor alle netwerkdiensten behoren te worden geïdentificeerd en opgenomen in overeenkomsten betreffende netwerkdiensten. Dit geldt zowel voor diensten die intern worden geleverd als voor uitbestede diensten.

Tips: geen aanvullende opmerkingen.

Toelichting:
Tot netwerkdiensten behoren het leveren van aansluitingen, particuliere netwerkdiensten, netwerken met toegevoegde waarde en beheerde netwerkbeveiligingsoplossingen zoals firewalls en inbraakdetectiesystemen.

Niveaus	Beheersmaatregel (plus evidence)	Audit
Volwassenheidsniveau 1 (Initieel / ad hoc)	Beveiligingsmechanismen, dienstverleningsniveaus en beheereisen worden niet vooraf Gedefinieerd en overeengekomen. Dienstverlening vindt plaats naar beste kunnen en wordt niet door de opdrachtgever bewaakt.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Er zijn enige eisen Gedefinieerd en afspraken gemaakt, dienstverlener levert in enige vorm een periodieke rapportage. Audits op implementatie van beveiligingsmaatregelen vindt niet, of globaal, plaats De geformuleerde eisen worden, als dat zo uit komt, op andere momenten hergebruikt, de rapportage wordt incidenteel besproken. **Evidence:** 1. Kopie Programma's van Eisen; 2. Kopie rapportages; 3. Kopieën gespreksnotities of notulen; 4. In infrastructuur zichtbare maatregelen (zoals VPN-voorzieningen en VPN-verbindingen.)	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Beveiligingseisen en -niveaus zijn door vakkundige functionarissen vastgesteld en afgestemd met de in- of externe dienstverlener. De afspraken zijn vastgelegd in Service Level Agreements. Over de SLA's wordt gerapporteerd en bewaking van de SLA's vindt plaats. Daar waar het externe diensten betreft is de overeenkomst in samenwerking met Inkoop tot stand gekomen. **Evidence in aanvulling op 2:** 1. Kopie beschrijving Service Level Managementproces; 2. Kopie van ICT-inkoopprocedure.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	Organisatie voert het Gedefinieerde proces consequent uit en evalueert tevens of het proces tot het gewenste doel leidt.) **Evidence in aanvulling op 3:** 1. Notulen of verslagen waaruit blijkt dat eisen formeel vastgesteld zijn; 2. SLA of overeenkomst bevat clausule dat controles (audits) op kwaliteit van de beveiliging toegestaan zijn; 3. Notulen of verslagen waaruit blijkt dat rapportages periodiek besproken zijn; 4. Notulen, verslagen of rapportages waaruit blijkt dat controles of audit hebben plaatsgevonden.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	Proces en onderdelen daarvan is meerdere malen uitgevoerd, lering is getrokken uit evaluaties. **Evidence in aanvulling op 4:** 1. Evaluatieverslagen; 2. Bijgewerkte modellen (zoals voor risicoanalyse of bepaling risicoklassen) en procesbeschrijvingen.	

Controledoelstelling 5.14

Cluster: Toegangsbeveiliging en integriteit	**ISO 27002 nummer: 13.1.2**
Controledoelstelling: Beveiliging van netwerkdiensten Beveiligingsmechanismen, dienstverleningsniveaus en beheer eisen voor alle netwerkdiensten behoren te worden geïdentificeerd en opgenomen in overeenkomsten betreffende netwerkdiensten. Dit geldt zowel voor diensten die intern worden geleverd als voor uitbestede diensten.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

5.15 Scheiding in netwerken

Cluster: Toegangsbeveiliging en integriteit	**ISO 27002 nummer: 13.1.3**	
Controledoelstelling: Scheiding in netwerken Groepen van informatiediensten, -gebruikers en -systemen behoren in netwerken te worden gescheiden.		
Tips: zie "Leidraad toegangsbeveiliging" (cf. 3.5.1)		
Toelichting: Groepen informatiediensten, gebruikers en informatiesystemen behoren op netwerken te worden gescheiden.		
Niveaus	**Beheersmaatregel (plus evidence)**	**Audit**
Volwassenheidsniveau 1 (Initieel / ad hoc)	Groepen informatiediensten, gebruikers en informatiesystemen zijn op netwerken niet of niet volledig gescheiden.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Groepen informatiediensten, gebruikers en informatiesystemen zijn slechts gedeeltelijk, doch niet consequent, op netwerken gescheiden. **Evidence:** 1. Beschrijving scheidingsmaatregelen (uit technisch landschap dan wel gespreksverslag hoofd systeembeheer).	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Groepen informatiediensten, gebruikers en informatiesystemen zijn op netwerken gescheiden volgens formeel vastgestelde netwerk architectuur. **Evidence in aanvulling op 2:** 1. Kopie van beleid en procedurebeschrijving voor scheiding van netwerken; 2. Kopie van informatie waaruit blijkt dat de organisatie conform het beleid of procedure heeft gehanteerd. Te denken aan: • kopie uit systeem waaruit blijkt dat de productienetwerkdomeinen en administratienetwerkdomein gescheiden zijn; • kopie overzicht landscape en infrastructuur.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	Groepen informatiediensten, gebruikers en informatiesystemen zijn op netwerken gescheiden. De segmenten zijn m.b.v. technische middelen van elkaar afgeschermd. Er vindt logging en controle plaats. **Evidence in aanvulling op 3:** 1. Logs en verslagen van logreviews (bijvoorbeeld afgetekende checklists voor periodiek log review, geautomatiseerde uitzonderingsrapportages).	
Volwassenheidsniveau 5 (Geoptimaliseerd)	Groepen informatiediensten, gebruikers en informatiesystemen zijn op netwerken gescheiden. De segmenten zijn m.b.v. technische middelen van elkaar afgeschermd. Er vindt regelmatig een review van de toegepaste netwerkscheiding plaats. **Evidence in aanvulling op 4:** 1. Verslagen van periodieke evaluatie van de netwerkscheiding.	

Controledoelstelling 5.15

Cluster: Toegangsbeveiliging en integriteit	**ISO 27002 nummer: 13.1.3**
Controledoelstelling: Scheiding in netwerken Groepen van informatiediensten, -gebruikers en -systemen behoren in netwerken te worden gescheiden.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

5.16 Elektronische berichten

Cluster: Toegangsbeveiliging en integriteit	**ISO 27002 nummer: 13.2.3**	
Controledoelstelling: Elektronische berichten Informatie die is opgenomen in elektronische berichten behoort passend te zijn beschermd		
Tips: toetsen op certificering. Zie ook 3.1.12.		
Toelichting: Informatie die een rol speelt bij elektronische berichtuitwisseling op geschikte wijze beschermd.		
Niveaus	**Beheersmaatregel (plus evidence)**	**Audit**
Volwassenheidsniveau 1 (Initieel / ad hoc)	Informatie die een rol speelt bij elektronische berichtuitwisseling wordt niet systematisch beschermd.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Informatie die een rol speelt bij elektronische berichtuitwisseling wordt soms beschermd. Er is geen standaardvoorziening.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Informatie die een rol speelt bij elektronische berichtuitwisseling wordt op passende wijze beschermd. **Evidence:** 1. Kopie van beleid en procedurebeschrijving (maatregelen) m.b.t. elektronische berichtenuitwisseling; 2. Kopie testgegevens van de ingebouwde maatregelen; 3. Onderdeel van de maatregelen is het beveiligen van informatie rond herkomst en bestemming van berichten. Zichtbaar te maken via schermprint authenticatie en adresseringsprocedure.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	Informatie die een rol speelt bij elektronische berichtuitwisseling wordt op passende wijze beschermd. Er zijn standaard tools beschikbaar en er vindt controle op naleving plaats. **Evidence in aanvulling op 3:** 1. Kopie van beleid en procedurebeschrijving (maatregelen) m.b.t. elektronische berichtenuitwisseling; 2. Kopie testgegevens van de ingebouwde maatregelen 3. Onderdeel van de maatregelen is het beveiligen van informatie rond herkomst en bestemming van berichten. Zichtbaar te maken via schermprint authenticatie en adresseringsprocedure; 4. Overzicht gehanteerde tools; 5. Controle verslagen m.b.t. naleving beleid.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	Informatie die een rol speelt bij elektronische berichtuitwisseling wordt op passende wijze beschermd. Er zijn standaard tools beschikbaar en gedocumenteerd. Iedereen past deze toe waar dit nodig is. Er vindt regelmatig evaluatie plaats van gebruikte methode en technieken. **Evidence in aanvulling op 4:** 1. Kopie van beleid en procedurebeschrijving (maatregelen) m.b.t. elektronische berichtenuitwisseling; 2. Kopie testgegevens van de ingebouwde maatregelen; 3. Onderdeel van de maatregelen is het beveiligen van informatie rond herkomst en bestemming van berichten. Zichtbaar te maken via schermprint authenticatie en adresseringsprocedure; 4. Overzicht gehanteerde tools; 5. Controle verslagen m.b.t. naleving beleid; 6. Verslagen evaluatie van gebruikte methode en technieken.	

Controledoelstelling 5.16

Cluster: Toegangsbeveiliging en integriteit	**ISO 27002 nummer: 13.2.3**
Controledoelstelling: Elektronische berichten Informatie die is opgenomen in elektronische berichten behoort passend te zijn beschermd	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

5.17 Transacties van toepassingen beschermen

Cluster: Toegangsbeveiliging en integriteit	**ISO 27002 nummer: 14.1.3**

Controledoelstelling: Transacties van toepassingen beschermen
Informatie die deel uitmaakt van transacties van toepassingen behoort te worden beschermd ter voorkoming van onvolledige overdracht, foutieve routering, onbevoegd wijzigen van berichten, onbevoegd openbaar maken, onbevoegd vermenigvuldigen of afspelen.

Tips: Toetsen op vertrouwelijkheid, SSL-certificaat, officieel certificaat. Maar ook toetsen op integriteit. Bijvoorbeeld de koppeling naar DUO op basis van certificaten uitgegeven door een valide CA (bijv. SURFcertificaten-Digicert).

Toelichting:
De omvang van de aangenomen beheersmaatregelen behoort in overeenstemming te zijn met het niveau van het risico dat samenhangt met elke transactievorm van toepassingen. Transacties moeten mogelijk voldoen aan de eisen van wet- en regelgeving van het rechtsgebied waarin de transactie is gegenereerd, verwerkt, uitgevoerd of opgeslagen.

Niveaus	Beheersmaatregel (plus evidence)	Audit
Volwassenheidsniveau 1 (Initieel / ad hoc)	Informatie die een rol speelt bij transacties wordt op niet-standaard wijze beschermd om onvolledige overdracht, onjuiste routing, onbevoegde wijziging van berichten, onbevoegde openbaarmaking en onbevoegde vermenigvuldiging of afspelen van berichten te voorkomen.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Er zijn tools om informatie die een rol speelt bij transacties te beschermen om onvolledige overdracht, onjuiste routing, onbevoegde wijziging van berichten, onbevoegde openbaarmaking en onbevoegde vermenigvuldiging of afspelen van berichten te voorkomen. Deze zijn echter niet altijd geïntegreerd in de systemen en worden niet altijd toegepast. **Evidence:** 1. Kopie documentatie waaruit blijkt hoe voor een transactiesysteem de gegevens beschermd worden.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Informatie die een rol speelt bij transacties wordt beschermd om onvolledige overdracht, onjuiste routing, onbevoegde wijziging van berichten, onbevoegde openbaarmaking en onbevoegde vermenigvuldiging of afspelen van berichten te voorkomen. **Evidence in aanvulling op 2:** 1. Kopie beleid voor transacties; 2. Kopie van informatie waaruit blijkt dat de organisatie het beleid heeft uitgevoerd. Te denken aan: • Schermprint waaruit blijkt dat communicatie tussen alle partijen met protocollen zijn beveiligd; • Kopie documentatie met betrekking tot certificaat/handtekeningen beheerproces.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	Informatie die een rol speelt bij transacties wordt beschermd om onvolledige overdracht, onjuiste routing, onbevoegde wijziging van berichten, onbevoegde openbaarmaking en onbevoegde vermenigvuldiging of afspelen van berichten te voorkomen. Dit is vastgelegd in baselines. Controlemechanismen zijn geïmplementeerd. **Evidence in aanvulling op 3:** 1. Kopie relevante baselines; 2. Beschrijving controlemechanismen; 3. Rapportage vanuit controlemechanismen.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	Informatie die een rol speelt bij transacties wordt beschermd om onvolledige overdracht, onjuiste routing, onbevoegde wijziging van berichten, onbevoegde openbaarmaking en onbevoegde vermenigvuldiging of afspelen van berichten te voorkomen. Dit is vastgelegd in baselines gebaseerd op best practices. Systemen worden regelmatig ge-audit. **Evidence in aanvulling op 4:** 1. Kopie relevante baselines; 2. Beschrijving controlemechanismen; 3. Rapportage vanuit controlemechanismen; 4. Audit rapportages.	

Controledoelstelling 5.17

Cluster: Toegangsbeveiliging en integriteit	**ISO 27002 nummer: 14.1.3**
Controledoelstelling: Transacties van toepassingen beschermen Informatie die deel uitmaakt van transacties van toepassingen behoort te worden beschermd ter voorkoming van onvolledige overdracht, foutieve routering, onbevoegd wijzigen van berichten, onbevoegd openbaar maken, onbevoegd vermenigvuldigen of afspelen.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

6. Controle en logging

Nr.	ISO27002	Controledoelstelling
6.1	9.2.5	**Beoordeling van toegangsrechten van gebruikers:** Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen.
6.2	12.4.1	**Gebeurtenissen registreren:** Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.
6.3	12.4.3	**Logbestanden van beheerders en operators:** Activiteiten van systeembeheerders en -operators behoren te worden vastgelegd en de logbestanden behoren te worden beschermd en regelmatig te worden beoordeeld.
6.4	14.2.7	**Uitbestede softwareontwikkeling:** Uitbestede systeemontwikkeling behoort onder supervisie te staan van en te worden gemonitord door de organisatie.
6.5	14.2.8	**Testen van systeembeveiliging:** Tijdens ontwikkelactiviteiten behoort de beveiligingsfunctionaliteit te worden getest.
6.6	14.2.9	**Systeemacceptatietests:** Voor nieuwe informatiesystemen, upgrades en nieuwe versies behoren programma's voor het uitvoeren van acceptatietests en gerelateerde criteria te worden vastgesteld.
6.7	15.2.1	**Monitoring en beoordeling van dienstverlening van leveranciers:** Organisaties behoren regelmatig de dienstverlening van leveranciers te monitoren, te beoordelen en te auditen.
6.8	16.1.7	**Verzamelen van bewijsmateriaal:** De organisatie behoort procedures te definiëren en toe te passen voor het identificeren, verzamelen, verkrijgen en bewaren van informatie die als bewijs kan dienen.
6.9	18.2.2	**Naleving van beveiligingsbeleid en –normen:** Het management behoort regelmatig de naleving van de informatieverwerking en -procedures binnen haar verantwoordelijkheidsgebied te beoordelen aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.
6.10	18.2.3	**Beoordeling van technische naleving:** Informatiesystemen behoren regelmatig te worden beoordeeld op naleving van de beleidsregels en normen van de organisatie voor informatiebeveiliging.

6.1 Beoordeling van toegangsrechten van gebruikers

Cluster: Controle en logging	**ISO 27002 nummer: 9.2.5**

Controledoelstelling: Beoordeling van toegangsrechten van gebruikers
Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen.

Tips: een van de belangrijkste statements. De proceseigenaar moet samen met hoofd systeembeheer controleren of de toegangsrechten juist zijn. De accountant controleert dit statement regelmatig.
Zie ook “Leidraad toegangsbeveiliging” (cf. 3.5.1).

Toelichting:
De directie behoort de toegangsrechten van gebruikers regelmatig te beoordelen in een formeel proces. (Het gaat om periodieke toetsing van toegekende toegangsrechten om de toegang tot gegevens en diensten te kunnen beheersen; niet alleen uitgeven maar ook intrekken, gelet op verhuizingen, speciale bevoegdheden (kortere periodes en inhoudelijk), speciale bevoegdheden.

Niveaus	Beheersmaatregel (plus evidence)	Audit
Volwassenheidsniveau 1 (Initieel / ad hoc)	De toegangsrechten van gebruikers worden initieel en/of ad hoc, op basis van een incident of een melding beoordeeld. Er is geen sprake van een vastomlijnd proces of beleid.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Op basis van individuele expertise of individuele inschatting van grote(re) risico's worden de toegangsrechten van gebruikers beoordeeld. Dat kan in gelijksoortige systemen conform gemeenschappelijke processen plaatsvinden. Sommige controles zijn reproduceerbaar en gedocumenteerd. Op basis van individuele expertises is er sprake van begrip van policies en procedures. Er is geen sprake van een vastomlijnd proces of beleid vanuit het management. **Evidence:** 1. Kopie van overzicht van gebruikersrechten (deze kunnen de basis vormen voor verbeterstappen).	
Volwassenheidsniveau 3 (Gedefinieerd proces)	De (business)management beoordeelt regelmatig de toegangsrechten van gebruikers van ten minste de concernsystemen in een formeel proces. **Evidence in aanvulling op 2:** 1. Kopie van informatie waaruit blijkt de management periodiek de toegangsrechten beoordeelt. Te denken aan: • Aantonen hoe vaak de analyse wordt uitgevoerd; • Twee meest recente beoordelingsanalyses op gebruikers.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	Er is een gedegen en volledig beleid en het proces rondom de beoordeling van de toegangsrechten van alle systemen, afgestemd op het karakter van die rechten (risicoanalyse). Bijzondere accounts of bijzondere toegangsrechten worden frequenter beoordeeld en ook op hun inhoud. Er worden interne best practices toegepast. Alle aspecten van het proces zijn gedocumenteerd en reproduceerbaar. Er zijn werkafspraken gemaakt o.a. met waarborgen dat overzichten en beoordelingen van toegangsrechten niet door de betrokkenen zelf worden afgehandeld en deze afspraken worden overgenomen en nageleefd. Beleidsvoorschriften zijn goedgekeurd en bekrachtigd door het management. **Evidence in aanvulling op 3:** 1. Overzicht van differentiaties uit uitgevoerde analyses; 2. Twee meest recente beoordelingsanalyses op gebruikers met paraaf van behandelaar en beoordelaar.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	Er worden externe best practices en normen toegepast. De procesdocumentatie is geëvolueerd tot een stelsel van (geautomatiseerde) workflows, waarin voorzien is in integratie van verschillende businessprocessen en beoordeling door interne of externe auditors. Daarmee biedt het proces mogelijkheden tot beoordeling op adequate functiescheiding en op inefficiënties en daarmee mogelijkheden tot verbeteringen. **Evidence in aanvulling op 4:** 1. Overzicht workflows; 2. Recent bevindingenrapport van interne of externe auditor.	

Controledoelstelling 6.1

Cluster: Controle en logging	**ISO 27002 nummer: 9.2.5**
Controledoelstelling: Beoordeling van toegangsrechten van gebruikers Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

6.2 Gebeurtenissen registreren

Cluster: Controle en logging	**ISO 27002 nummer: 12.4.1**
Controledoelstelling: Gebeurtenissen registreren Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld**.**	
Tips: geen aanvullende opmerkingen.	
Toelichting: Activiteiten van gebruikers, uitzonderingen en informatiebeveiligingsgebeurtenissen behoren te worden vastgelegd in audit-logbestanden. Deze logbestanden behoren gedurende een overeengekomen periode te worden bewaard, ten behoeve van toekomstig onderzoek en toegangscontrole. (Audit logbestanden van o.m. de volgende gegevens: gebruikers-ID's, data, tijdstippen en details van in- en uitloggen, identiteit device/locatie, geslaagde/geweigerde pogingen om toegang te krijgen, gebruik van speciale bevoegdheden en dergelijke. Waar mogelijk behoren systeembeheerders geen toestemming te hebben om logbestanden van hun eigen activiteiten te wissen of deactiveren.)	

Niveaus	**Beheersmaatregel (plus evidence)**	**Audit**
Volwassenheidsniveau 1 (Initieel / ad hoc)	Er zijn wellicht logbestanden beschikbaar op diverse systemen. Deze zullen doorgaans ontstaan zijn vanuit een default instelling tijdens installatie. Er zijn geen afspraken over de inhoud van de logging of over bewaartermijnen.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Er zijn logbestanden beschikbaar op de relevante systemen. De log-levels zullen op soortgelijke systemen ook vergelijkbaar zijn ingesteld op basis van individuele expertises en er zijn mogelijk extra tools zoals een centrale syslog-server. Er is echter geen vastgesteld beleid over bewaartermijnen, inhoud van de logging of centrale opslag. **Evidence:** 1. Kopie van systeemconfiguratie voor zover beschikbaar (deze kunnen de basis vormen voor verbeterstappen); 2. Kopie van (een deel van) een logbestand .	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Activiteiten van gebruikers, uitzonderingen en informatiebeveiligingsgebeurtenissen zijn vastgelegd in audit-logbestanden. Deze logbestanden worden gedurende een overeengekomen periode bewaard, ten behoeve van toekomstig onderzoek en toegangscontrole. **Evidence in aanvulling op 2:** 1. Kopie beleid en procedurebeschrijving voor het aanmaken van audit-logbestanden; 2. Kopie van informatie waaruit blijkt dat de organisatie conform het beleid of procedure heeft uitgevoerd. Te denken aan: • Kopie uit systeem waaruit blijkt dat alle gebruikers een unieke gebruikers-ID hebben; • Kopie uit systeem waaruit blijkt dat registratie plaats vindt bij geslaagde en geweigerde pogingen om toegang te krijgen tot het systeem; • Kopie uit systeem waaruit blijkt dat men gebruik maakt van speciale bevoegdheden (redflag envelop).)	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	Activiteiten van gebruikers, uitzonderingen en informatiebeveiligingsgebeurtenissen worden op een gestandaardiseerde methode vastgelegd in audit-logbestanden. In ieder geval de logbestanden van de concernsystemen worden, zoveel mogelijk real-time, op een separate (SYSLOG) server opgeslagen, waarbij de bronbestanden niet gemuteerd kunnen worden door de systeembeheerders. Deze logbestanden worden gedurende een overeengekomen periode bewaard, ten behoeve van toekomstig onderzoek en toegangscontrole. Privacygevoelige informatie wordt adequaat afgeschermd en wordt na een afgesproken periode vernietigd, dan wel geanonimiseerd of geaggregeerd opgeslagen. Er zijn tools beschikbaar om logbestanden te analyseren, het procesbeheer te automatiseren en kritieke activiteiten en controlemechanismen te bewaken. **Evidence in aanvulling op 3:** 1. Kopie van de inrichtingsdocumenten van de centrale logserver(s); 2. Beschrijving van de beschikbare tooling en het beoogd en toegestane gebruik; 3. Kopie (bewakings-) rapportage over events (kritieke activiteiten, werking controlemechanismen).	

Volwassenheidsniveau 5 (Geoptimaliseerd)	Alle logbestanden van alle systemen worden op een gestandaardiseerde wijze verzameld en opgeslagen en er is een standaard toolset beschikbaar voor beheer en analyse. De datasets zijn uniform ingericht en de tools zijn volledig geïntegreerd, zodat processen van begin tot eind worden ondersteund en analyses over de datasets heen mogelijk zijn. Er worden analyse en rapportage tools ingezet ter ondersteuning van procesverbeteringen en automatische detectie van afwijkingen. **Evidence in aanvulling op 4:** 1. Kopie van de (trend)rapportage.	

Controledoelstelling 6.2

Cluster: Controle en logging	**ISO 27002 nummer: 12.4.1**
Controledoelstelling: Gebeurtenissen registreren Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld**.**	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

6.3 Logbestanden van beheerders en operators

Cluster: Controle en logging	**ISO 27002 nummer: 12.4.3**
Controledoelstelling: Logbestanden van beheerders en operators Activiteiten van systeembeheerders en -operators behoren te worden vastgelegd en de logbestanden behoren te worden beschermd en regelmatig te worden beoordeeld.	
Tips: geen aanvullende opmerkingen.	
Toelichting: Activiteiten van systeemadministrators en systeemoperators behoren in logbestanden te worden vastgelegd. (In logbestanden wordt onder meer vastgelegd: tijdstip succes/storing gebeurtenis, welke beheerder of operator, welke processen.)	

Niveaus	Beheersmaatregel (plus evidence)	Audit
Volwassenheidsniveau 1 (Initieel / ad hoc)	Er zijn wellicht logbestanden beschikbaar op diverse systemen. Deze zullen doorgaans ontstaan zijn vanuit een default instelling tijdens installatie. Er zijn geen afspraken over de inhoud van de logging, controle en bewaartermijnen.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Er zijn logbestanden beschikbaar op de relevante systemen. De logging-niveaus zullen op soortgelijke systemen ook vergelijkbaar zijn ingesteld op basis van individuele expertises en er zijn mogelijk extra tools zoals een centrale syslog-server of een logboek. Er is echter geen vastgesteld beleid over bewaartermijnen, controle, inhoud van de logging of centrale opslag. **Evidence:** 1. Kopie van systeemconfiguratie voor zover beschikbaar (deze kunnen de basis vormen voor verbeterstappen); 2. Kopie van (een deel van) een log-bestand.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Activiteiten van systeemadministrators en systeemoperators zijn in logbestanden (-boeken) vastgelegd. **Evidence in aanvulling op 2:** 1. Kopie beleid en procedurebeschrijving voor logbestanden (-boeken) van administrators en operators; 2. Kopie van informatie waaruit blijkt dat de activiteiten van systeemadministrators en systeemoperators zijn vastgelegd in de logbestanden. Te denken aan: • Kopie logbestand; • Kopie twee meest recente rapportages waaruit blijkt dat de logbestanden zijn beoordeeld door de organisatie.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	Activiteiten van systeemadministrators en systeemoperators zijn op een gestandaardiseerde methode vastgelegd in logbestanden (-boeken). In ieder geval de logbestanden van de concernsystemen worden, zoveel mogelijk real-time, op een separate (SYSLOG) server opgeslagen, waarbij de bronbestanden niet gemuteerd kunnen worden door de systeembeheerders en -operators. Deze logbestanden worden gedurende een overeengekomen periode bewaard, ten behoeve van toekomstig onderzoek en controle op werkinstructies. Op de belangrijkste concernsystemen worden tools ingezet om kritieke activiteiten en controlemechanismen te bewaken. **Evidence in aanvulling op 3:** 1. Kopie van de inrichtingsdocumenten van de centrale logserver(s); 2. Beschrijving van de beschikbare tooling en het beoogd en toegestane gebruik; 3. Rapportage uit bewakingstools over kritieke activiteiten.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	Op alle afdelingen worden gestandaardiseerde toolsets en werkinstructies gebruikt voor het registreren van activiteiten. Er worden tools ingezet om automatisch afwijkingen te detecteren, bijvoorbeeld een inbraakdetectiesysteem, zo mogelijk buiten het beheer van de betrokken systeemadministrators en systeemoperators om. Bij de beoordeling van de logbestanden wordt ook over de systemen of afdelingen heen gekeken en worden zo nodig verbetervoorstellen ingediend. **Evidence in aanvulling op 4:** 1. Inrichtingsdocument van detectiesysteem; 2. Kopie van de (evaluatie)rapportage.	

Controledoelstelling 6.3

Cluster: Controle en logging	**ISO 27002 nummer: 12.4.3**
Controledoelstelling: Logbestanden van beheerders en operators Activiteiten van systeembeheerders en -operators behoren te worden vastgelegd en de logbestanden behoren te worden beschermd en regelmatig te worden beoordeeld.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

6.4 Uitbestede softwareontwikkeling

Cluster: Controle en logging	**ISO 27002 nummer: 14.2.7**
Controledoelstelling: Uitbestede softwareontwikkeling Uitbestede systeemontwikkeling behoort onder supervisie te staan van en te worden gemonitord door de organisatie.	
Tips: geen aanvullende opmerkingen.	
Toelichting: Uitbestede ontwikkeling van programmatuur behoort onder supervisie te staan van en te worden gecontroleerd door de organisatie. (Aandachtspunten: licentieovereenkomsten, intellectueel eigendom (broncode), certificatie, kwaliteits- en continuïteitsborging, recht op audit, contractuele eisen voor de kwaliteit en beveiligingsfunctionaliteit van de broncode, testen.)	

Niveaus	**Beheersmaatregel (plus evidence)**	**Audit**
Volwassenheidsniveau 1 (Initieel / ad hoc)	De ontwikkeling van programmatuur wordt op ad hoc basis uitbesteed op voorwaarden die afhankelijk zijn van de expertise van de betrokkenen. Er is geen sprake van een vastomlijnd proces of beleid.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	De ontwikkeling van programmatuur wordt binnen afdelingen of voor gelijksoortige systemen of processen op een gemeenschappelijke wijze uitbesteed, maar de voorwaarden zijn gebaseerd op de expertise van de betrokkenen. Bepaalde aspecten van het proces zijn reproduceerbaar vanwege die individuele expertise en er kan sprake zijn van enige documentatie en een zeker begrip van policies en procedures. Er is geen sprake van een vastomlijnd proces of beleid. **Evidence:** 1. Kopie van vaker gebruikt uitbestedingscontract (deze kunnen de basis vormen voor verbeterstappen).	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Uitbestede ontwikkeling van programmatuur staat onder supervisie van en wordt gecontroleerd door de organisatie, ten minste voor de concernsystemen. **Evidence in aanvulling op 2:** 1. Kopie contract en bijlage (SLA en beveiligingsnormen) - kopie van licentieovereenkomsten, eigendom van de broncode en intellectuele eigendomsrechten waaruit blijkt dat de organisatie controle uitvoert. 2. Kopie procedurebeschrijving voor het uitbestede ontwikkeling van programmatuur; 3. Kopie van informatie waaruit blijkt dat de organisatie conform de procedure uitvoert. Te denken aan: • Kopie van certificatie van de kwaliteit en nauwkeurigheid van het uitgevoerde werk; • Kopie van een testrapport; 4. Kopie ISAE 3402 rapport van uitbestede ontwikkelingen/diensten.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	Er is een gedegen en volledig instelling breed uitbestedingsproces, gebaseerd op centrale ICT-inkoopvoorwaarden en conform het centrale inkoopproces. Alle aspecten van het proces zijn gedocumenteerd en reproduceerbaar. ICT-inkoopvoorwaarden en kwaliteitsnormen zijn goedgekeurd en bekrachtigd door het management. De werkafspraken worden overgenomen en nageleefd. **Evidence in aanvulling op 3:** 1. Kopie van ICT-inkoopprocedure; 2. Kopie van ICT-inkoopvoorwaarden en notulen of besluitenlijst/managementbesluit waaruit management goedkeuring blijkt. 3. Kopie contract voor uitbesteding waaruit blijkt dat de inkoopvoorwaarden gehanteerd worden.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	Er worden externe best practices en normen toegepast op het uitbesteden van softwareontwikkeling, bijv. sourcing-leidraden die in SURF-verband zijn ontwikkeld. De procesdocumentatie is geëvolueerd tot een stelsel van (geautomatiseerde) workflows waarbij het beleid en de gestandaardiseerde processen en procedures zijn geïntegreerd met die van de afdeling Inkoop. Er vinden periodiek evaluatiegesprekken plaats over het proces met het doel verbeteringen door te kunnen voeren in alle deelprocessen. **Evidence in aanvulling op 4:** 1. Kopie van de workflows; 2. Kopie verslag van een recent evaluatiegesprek.	

Controledoelstelling 6.4

Cluster: Controle en logging	**ISO 27002 nummer: 14.2.7**
Controledoelstelling: Uitbestede softwareontwikkeling Uitbestede systeemontwikkeling behoort onder supervisie te staan van en te worden gemonitord door de organisatie.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

6.5 Testen van systeembeveiliging

Cluster: Controle en logging	**ISO 27002 nummer: 14.2.8**
Controledoelstelling: Testen van systeembeveiliging Tijdens ontwikkelactiviteiten behoort de beveiligingsfunctionaliteit te worden getest.	
Tips: geen aanvullende opmerkingen.	
Toelichting: Tijdens de ontwikkelprocessen zijn voor nieuwe en geactualiseerde systemen uitvoerige tests en verificatie nodig, met inbegrip van het opstellen van een gedetailleerd schema van activiteiten en tests van inputs en verwachte outputs onder diverse omstandigheden. De omvang van het testen behoort in verhouding te staan tot de belangrijkheid en de aard van het systeem.	

Niveaus	Beheersmaatregel (plus evidence)	Audit
Volwassenheidsniveau 1 (Initieel / ad hoc)	Ontwikkeling worden op ad hoc basis getest op voorwaarden die afhankelijk zijn van de expertise van de betrokkenen. Er is geen sprake van een vastomlijnd testproces.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Ontwikkelingen worden binnen afdelingen of voor gelijksoortige systemen of processen op een gemeenschappelijke wijze getest, maar de voorwaarden zijn gebaseerd op de expertise van de betrokkenen. Bepaalde aspecten van het testproces zijn reproduceerbaar vanwege die individuele expertise en er kan sprake zijn van enige documentatie en een zeker begrip van testmethodiek of -aanpakken. Er is geen sprake van een vastomlijnd testproces. **Evidence:** 1. Gespreksverslagen met ontwikkelaars en/of testers; 2. Kopieën beveiligingseisen waaraan ontwikkelingen moeten voldoen; 3. Kopieën bevindingenlijsten; 4. Kopieën testverslagen.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	De organisatie - of de externe partner, indien ontwikkeling is uitbesteed - beschikt over een vastgestelde testmethodiek inclusief voorgeschreven testproces. **Evidence in aanvulling op 2:** 1. Kopie testmethodiek; 2. Kopie templates voor testuitvoering; 3. Kopie dienstverleningsovereenkomst(en) waaruit afgesproken beveiligingstestactiviteiten blijken.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	De organisatie – of externe partner – voert het vastgestelde testproces aantoonbaar consequent uit, ondersteund met tools voor beheersing van het testproces als ook voor de uitvoering van het testen. **Evidence in aanvulling op 3:** 1. Kopieën testplannen met daarin risicoanalyse en selectie testtechnieken; 2. Kopieën testbevindingen en oplossingen; 3. Kopieën vrijgaveadviezen; 4. Kopieën handleidingen ingezette tools zoals voor codeanalyse en bevindingenbeheer; 5. Kopieën opleidingscertificaten ontwikkelaars en testers.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	Het testen van beveiligingsfunctionaliteiten is volledig geïntegreerd in het ontwikkelproces waardoor structureel op optimale wijze getest wordt. De best passende tools zijn beschikbaar, deze worden optimaal ingezet en effectiviteit van tools en proces worden periodiek geëvalueerd. **Evidence in aanvulling op 4:** 1. Meerdere testtools zijn beschikbaar en aantoonbaar in gebruik; 2. Kopieën evaluatierapportages; 3. Beoordelingen effectiviteit testproces aanwezig.	

Controledoelstelling 6.5

Cluster: Controle en logging	**ISO 27002 nummer: 14.2.8**
Controledoelstelling: Testen van systeembeveiliging Tijdens ontwikkelactiviteiten behoort de beveiligingsfunctionaliteit te worden getest.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

6.6 Systeemacceptatietests

Cluster: Controle en logging	**ISO 27002 nummer: 14.2.9**
Controledoelstelling: Systeemacceptatietests Voor nieuwe informatiesystemen, upgrades en nieuwe versies behoren programma's voor het uitvoeren van acceptatietests en gerelateerde criteria te worden vastgesteld..	
Tips: geen aanvullende opmerkingen.	
Toelichting: Er zijn aanvaardingscriteria vastgesteld voor nieuwe informatiesystemen, upgrades en nieuwe versies en er wordt een geschikte acceptatietest van het systeem of de systemen uitgevoerd alvorens deze worden overgezet naar de productieomgeving.	

Niveaus	Beheersmaatregel (plus evidence)	Audit
Volwassenheidsniveau 1 (Initieel / ad hoc)	Nieuwe informatiesystemen, updates en nieuwe versies worden in productie genomen zonder duidelijk te zijn Gedefinieerd, goedgekeurd, gedocumenteerd en getest. Aparte test en ontwikkelomgevingen zijn er alleen als deze toevallig voor handen zijn.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	De systemen worden niet gezien als onderdeel van een keten en worden meestal door dezelfde personen als eilandjes beheerd. Aanpassingen of testen worden vaak direct in de productieomgeving in de stille uurtjes gedaan. Bij uitzondering is er een aparte ontwikkel en of testomgeving aanwezig. Er verschijnen gelijksoortige en gemeenschappelijke change- en testprocessen, maar deze zijn grotendeels intuïtief vanwege het individuele karakter van de expertise. Bepaalde aspecten van het proces zijn reproduceerbaar vanwege die individuele expertise, en er kan sprake zijn van enige documentatie en een zeker begrip van beleid en procedures. **Evidence:** 1. Kopie change- en testverslagen van individuele medewerkers.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Nieuwe informatiesystemen, upgrades en nieuwe versies worden pas na formele acceptatie overgebracht naar de productieomgeving **Evidence in aanvulling op 2:** 1. Kopie van informatie waarbij de organisatie aan kan tonen dat nieuwe informatiesystemen, upgrades en nieuwe versies pas na formele acceptatie worden overgebracht naar de productie omgeving. Te denken aan: • Kopie beschrijving "overzettingsproces"; • Kopie checklist ; • Kopie geautoriseerde acceptatieformulieren.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	Er is een gedegen en volledig proces, en er worden interne best practices toegepast. Alle aspecten van het proces zijn gedocumenteerd en reproduceerbaar. Beleidsvoorschriften zijn goedgekeurd en bekrachtigd door het management. Wijzigingen worden via een OTAP ingevoerd. Er vindt formele overdracht plaats bij overgang tussen de diverse systemen in de OTAP-omgeving. Openstaande punten worden ofwel voor de overgang tot productie alsnog opgelost, ofwel formeel geaccepteerd door verantwoordelijk systeemeigenaar ofwel meteen omgezet in een change request op de operationele omgeving. De normen voor de procedures met betrekking tot de OTAP-omgeving worden overgenomen en nageleefd. **Evidence in aanvulling op 3:** 1. Kopie van overdrachtsdocument met restpunten en inzage in de afhandeling van Requests for Change.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	OTAP wordt gebruikt voor het releasematig in productie brengen van alle wijzigingen en nieuwbouw. Deze zijn proactief vanuit de processen verzameld tot een release en ingepland gedurende het jaar. Niets gaat meer buiten OTAP om en de meeste procedures zijn geautomatiseerd. **Evidence in aanvulling op 4:** 1. Kopie van change- en releasemanagement procedures; 2. Kopie release planning.	

Controledoelstelling 6.6

Cluster: Controle en logging	**ISO 27002 nummer: 14.2.9**
Controledoelstelling: Systeemacceptatietests Voor nieuwe informatiesystemen, upgrades en nieuwe versies behoren programma's voor het uitvoeren van acceptatietests en gerelateerde criteria te worden vastgesteld..	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

6.7 Monitoring en beoordeling van dienstverlening van leveranciers

Cluster: Controle en logging	**ISO 27002 nummer: 15.2.1**
Controledoelstelling: Monitoring en beoordeling van dienstverlening van leveranciers Organisaties behoren regelmatig de dienstverlening van leveranciers te monitoren, te beoordelen en te auditen.	
Tips: geen aanvullende opmerkingen.	
Toelichting: De diensten, rapporten en registraties die door de derde partij worden geleverd, worden regelmatig gecontroleerd en beoordeeld en er worden regelmatig audits uitgevoerd. (Controle en beoordeling van dienstverlening door derden behoort te waarborgen dat de voorwaarden van de overeenkomsten voor de informatiebeveiliging worden nageleefd, dat incidenten en problemen goed worden afgehandeld. Er is een proces voor het beheer van de dienstverlening (prestatieniveaus, DVO's, audit trails, change- en problemmanagement))	

Niveaus	**Beheersmaatregel (plus evidence)**	**Audit**
Volwassenheidsniveau 1 (Initieel / ad hoc)	De diensten, rapporten en registraties die door een derde partij worden geleverd, worden niet gecontroleerd of beoordeeld en er worden geen audits uitgevoerd.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	De diensten, rapporten en registraties die door een derde partij worden geleverd, worden opgeslagen in een registratiesysteem en gebruikt om achteraf bij te kunnen sturen. Ze worden niet regelmatig gecontroleerd en beoordeeld. Er worden alleen ad hoc audits uitgevoerd, bijvoorbeeld tijdens een algehele audit van het door de dienst van de derde partij ondersteunde business proces. **Evidence:** 1. Kopie of rapportage uit het registratiesysteem.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	De diensten, rapporten en registraties die door een derde partij worden geleverd, worden regelmatig gecontroleerd en beoordeeld en er worden regelmatig audits uitgevoerd. Het management realiseert zich dat de eindverantwoordelijkheid voor de informatie bij de eigen organisatie berust. **Evidence in aanvulling op 2:** 1. Kopie proces "contractmanagement" van de organisatie; 2. Kopie procesbeschrijving van het controleren en beoordelen van dienstverlening door een derde partij; 3. Kopie van informatie waaruit blijkt dat de organisatie het heeft gecontroleerd en beoordeeld. Te denken aan: • Kopie rapportage (evaluatie?) van het prestatieniveau van de dienstverlening, • Kopie dienstverleningsrapport die opgesteld is door derde partij, • Kopie auditbevindingen.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	De diensten, rapporten en registratie worden regelmatig gecontroleerd en beoordeeld en er worden regelmatig audits uitgevoerd. De dienstverleningsrapporten en auditbevindingen worden verwerkt in verbeterplannen. **Evidence in aanvulling op 3:** 1. Kopie verbeterplannen die door de derde partij worden geleverd.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	De diensten, rapporten en registraties die door de derde partij worden geleverd, worden regelmatig gecontroleerd en beoordeeld en er worden regelmatig audits uitgevoerd. De dienstverleningsrapporten en auditbevindingen worden verwerkt in verbeterplannen. De dienstverlening wordt periodiek geëvalueerd ten opzichte van het ondersteunde business proces en de dienstverleningscontracten worden zo nodig geoptimaliseerd. **Evidence in aanvulling op 4:** 1. Evaluatierapport.	

Controledoelstelling 6.7

Cluster: Controle en logging	**ISO 27002 nummer: 15.2.1**
Controledoelstelling: Monitoring en beoordeling van dienstverlening van leveranciers Organisaties behoren regelmatig de dienstverlening van leveranciers te monitoren, te beoordelen en te auditen.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

6.8 Verzamelen van bewijsmateriaal

Cluster: Controle en logging	**ISO 27002 nummer: 16.1.7**

Controledoelstelling: Verzamelen van bewijsmateriaal
De organisatie behoort procedures te definiëren en toe te passen voor het identificeren, verzamelen, verkrijgen en bewaren van informatie die als bewijs kan dienen.

Tips: bewijs dat gebruikt kan worden in een rechtszitting. Zodra een juridische procedure dreigt is het verstandig externe expertise in te huren om het maken van procedurefouten te voorkomen.

Toelichting:
Waar een vervolgprocedure tegen een persoon of organisatie na een informatiebeveiligingsincident juridische maatregelen omvat (civiel of strafrechtelijk), behoort bewijsmateriaal te worden verzameld, bewaard en gepresenteerd overeenkomstig de voorschriften voor bewijs die voor het relevante rechtsgebied zijn vastgelegd. (Implementatierichtlijnen uit ISO 27002 norm: Houdt rekening met: de toelaatbaarheid van het bewijs in een rechtszaak, de kwaliteit en volledigheid van het bewijsmateriaal, waarborgen dat informatiesystemen in overeenstemming zijn met gepubliceerde normen of praktijkcodes voor het genereren van toelaatbaar bewijsmateriaal, de kwaliteit en volledigheid van de beheersmaatregelen die zijn genomen om het verkregen bewijsmateriaal correct en consequent te beschermen.)

Niveaus	**Beheersmaatregel (plus evidence)**	**Audit**
Volwassenheidsniveau 1 (Initieel / ad hoc)	Ingeval van een informatiebeveiligingsincident met mogelijk juridische consequenties wordt bewijsmateriaal verzameld, bewaard en gepresenteerd op ad hoc basis, gebaseerd op de expertise en beschikbare tools van de betrokken beheerder(s). Er is geen sprake van een vastomlijnd proces of beleid of (het gebruik van) gestandaardiseerde tooling.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Ingeval van een informatiebeveiligingsincident met mogelijke juridische consequenties wordt bewijsmateriaal verzameld, bewaard en gepresenteerd op ad hoc basis, gebaseerd op de expertise en beschikbare tools van de betrokken beheerder(s). Er is sprake van aanvullende kennis en tooling en begrip van procedures bij beheerders die ervaring hebben met gelijksoortige incidenten of betrokken zijn bij processen met verhoogde risico's, maar de processtappen en tools zijn grotendeels intuïtief vanwege het individuele karakter van de expertise. Er is geen sprake van een vastomlijnd proces of beleid of (het gebruik van) gestandaardiseerde tooling. De kans is groot dat niet van het begin af de juiste zorgvuldigheid in het proces in acht wordt genomen. **Evidence:** 1. Verslag met overzicht van doorlopen proces en gebruikte tools.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Voor de belangrijkste business-processen is ingeregeld dat waar een vervolgprocedure tegen een persoon of organisatie na een informatiebeveiligingsincident juridische maatregelen omvat (civiel of strafrechtelijk), bewijsmateriaal wordt verzameld, bewaard en gepresenteerd overeenkomstig de voorschriften voor bewijs die voor het relevante rechtsgebied zijn vastgelegd. **Evidence in aanvulling op 2:** 1. Kopie beleid of procedurebeschrijving voor het verzamelen van bewijsmateriaal; 2. Kopie bewijsstukken dat de informatiesystemen in overeenstemming zijn met gepubliceerde normen of praktijkcodes voor het genereren van toelaatbaar bewijsmateriaal; 3. Kopie registerboek waarin alle papieren documenten zijn geregistreerd (wie, wat, waar, wanneer); 4. Waarneming ter plaatse (aantonen dat originele stukken zorgvuldig wordt bewaard).	

Volwassenheidsniveau 4 (Beheerd en meetbaar)	Er is een gedegen en volledig proces, en er worden interne best practices toegepast over de hele organisatie. In voorkomende gevallen wordt van het begin af aan de hulp ingeroepen van medewerkers of externen met voldoende expertise (bijv. getrainde leden van een CERT-team of ingehuurd personeel van een gecertificeerd bedrijf). Het hele proces wordt uitgevoerd door of wordt gecoördineerd door een medewerker met voldoende mandaten. Alle aspecten van het proces zijn gedocumenteerd en reproduceerbaar. De (CERT-)procedure en de mandaten zijn goedgekeurd en bekrachtigd door het management. De werkinstructies m.b.t. incidenten zijn gecommuniceerd en worden overgenomen en nageleefd. **Evidence in aanvulling op 3:** 1. Kopie procedurebeschrijving en mandatenregeling forensische deskundigen (CERT-team); 2. Kopie certificering forensische deskundigen; 3. Kopie recente werkinstructie naar (de)centrale IT-beheerders en managers; 4. Kopie contract extern bedrijf.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	Er worden externe best practices en normen toegepast. De procesdocumentatie en afgesloten casussen worden regelmatig geëvalueerd om verbeteringen door te kunnen voeren. Indien er geen recente casussen zijn wordt een oefening georganiseerd om doelmatigheid en technische werking van de procedures en de tooling te kunnen testen en waarborgen. **Evidence in aanvulling op 4:** 1. Kopie oefenscenario; 2. Kopie evaluatierapport recente casus of oefening.	

Controledoelstelling 6.8

Cluster: Controle en logging	**ISO 27002 nummer: 16.1.7**
Controledoelstelling: Verzamelen van bewijsmateriaal De organisatie behoort procedures te definiëren en toe te passen voor het identificeren, verzamelen, verkrijgen en bewaren van informatie die als bewijs kan dienen.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

6.9 Naleving van beveiligingsbeleid en -normen

Cluster: Controle en logging	**ISO 27002 nummer: 18.2.2**
Controledoelstelling: Naleving van beveiligingsbeleid en -normen Het management behoort regelmatig de naleving van de informatieverwerking en -procedures binnen haar verantwoordelijkheidsgebied te beoordelen aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging..	
Tips: proceseigenaren controleren of afspraken gerealiseerd zijn. Vragen zijn in de trant van: "Waar liggen de verantwoordelijkheden?" zijn beantwoord en gedocumenteerd.	
Toelichting: Managers behoren te bewerkstelligen dat alle beveiligingsprocedures die binnen hun verantwoordelijkheid vallen correct worden uitgevoerd om naleving te bereiken van beveiligingsbeleid en -normen. (Implementatierichtlijnen uit ISO 27002 norm: Managers behoren regelmatig te beoordelen of de informatieverwerking binnen hun verantwoordelijkheidsgebied voldoet aan het geldende beveiligingsbeleid, normen en andere beveiligingseisen.)	

Niveaus	**Beheersmaatregel (plus evidence)**	**Audit**
Volwassenheidsniveau 1 (Initieel / ad hoc)	Er is geen periodieke controle op naleving van beveiligingsbeleid en -normen. In voorkomende gevallen (bijvoorbeeld bij incidenten of specifieke vragen) wordt ad hoc op naleving getoetst en nemen medewerkers op eigen initiatief en op reactieve wijze verantwoordelijkheid voor kwesties.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Men neemt verantwoordelijkheid voor kwesties en wordt ook ter verantwoording geroepen, zelfs als dit niet formeel is geregeld. Bij problemen is echter vaak onduidelijk wie er verantwoordelijk is en men is geneigd de schuld door te schuiven. (Een risico is dat informatiebeveiliging daarmee ook wel wordt gebruikt als reden om zaken niet te doen ("is niet toegestaan vanwege security") zonder dat op het juiste niveau deze beslissing genomen/getoetst is.	
Volwassenheidsniveau 3 (Gedefinieerd proces)	Tenminste alle managers van de concernsystemen en de belangrijkste business processen stellen periodiek vast dat alle beveiligingsprocedures die binnen hun verantwoordelijkheid vallen correct worden uitgevoerd om naleving te bereiken van beveiligingsbeleid en -normen. **Evidence:** 1. Kopie beveiligingsbeleid en normen; 2. Overzicht systemen, processen, eigenaren, gebruikers en rollen (RACI); 3. Kopie twee meest recente rapportages waaruit blijkt dat managers periodiek beoordelen of de informatieverwerking binnen hun verantwoordelijkheidsgebied voldoet aan het geldende beveiligingsbeleid, normen en andere beveiligingseisen (versienummer + datum), dat kan bijvoorbeeld zijn: • Compliance verklaring; • Periodieke (her)classificatie van data of systemen en checklist bijbehorende maatregelen (baseline en aanvullend).	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	Er is een binnen de hele instelling aanvaarde structuur voor verantwoordelijkheid en verantwoording en de betreffende personen kunnen zich van hun verantwoordelijkheden kwijten. Deze verantwoordelijkheden zijn ingebed in functiebeschrijvingen, evaluatiegesprekken, overdrachtsdocumenten etc. Positieve actie wordt stelselmatig beloond om de betrokkenen te motiveren. **Evidence in aanvulling op 3:** 1. Kopie (beveiligings-)organisatiestructuur (kan ingebed zijn in beveiligingsbeleid document); 2. Kopie agenda jaargesprek; 3. Kopie standaard overdrachtsdocument.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	De verantwoordelijken hebben de vrijheid om besluiten en maatregelen te nemen. De verantwoordelijkheidsstructuur is tot op het laagste niveau ingebed in de organisatie. Deze verantwoordlijkheden zijn opgenomen in een mandatenregeling c.q. expliciet benoemd in procesbeschrijvingen of werkinstructies. **Evidence in aanvulling op 4:** 1. Kopie mandatenregeling; 2. Voorbeeld van procesbeschrijving of werkinstructie.	

Controledoelstelling 6.9

Cluster: Controle en logging	**ISO 27002 nummer: 18.2.2**
Controledoelstelling: Naleving van beveiligingsbeleid en -normen Het management behoort regelmatig de naleving van de informatieverwerking en -procedures binnen haar verantwoordelijkheidsgebied te beoordelen aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging..	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

6.10 Beoordeling van technische naleving 18.2.3

Cluster: Controle en logging	**ISO 27002 nummer: 18.2.3**
Controledoelstelling: Beoordeling van technische naleving Informatiesystemen behoren regelmatig te worden beoordeeld op naleving van de beleidsregels en normen van de organisatie voor informatiebeveiliging.	
Tips: beoordeling op technisch inhoudelijk gebied.	
Toelichting: Informatiesystemen behoren regelmatig te worden gecontroleerd op naleving van implementatie van beveiligingsnormen. (Implementatierichtlijnen uit 27002 norm: Controle automatisch of handmatig; ervaren systeemtechnicus; technische rapportage; Eventueel penetratieproeven of kwetsbaarheidsbeoordelingen (gepland, gedocumenteerd en Herhaalbaar).	

Niveaus	**Beheersmaatregel (plus evidence)**	**Audit**
Volwassenheidsniveau 1 (Initieel / ad hoc)	Er is geen periodieke controle op naleving van de implementatie van beveiligingsnormen. In voorkomende gevallen (bijvoorbeeld bij incidenten of n.a.v. specifieke berichtgeving) wordt door medewerkers ad hoc op eigen initiatief en op reactieve wijze de naleving getoetst. Daarbij is de kwaliteit van deze toetsing afhankelijk van de expertise van de medewerker en de beschikbare tooling.	
Volwassenheidsniveau 2 (Herhaalbaar maar intuïtief)	Medewerkers voeren op eigen initiatief controles uit op bekende risicogebieden en voor gelijksoortige systemen wordt dat ook wel gemeenschappelijke ingericht. Dit gebeurt grotendeels intuïtief vanwege het individuele karakter van de expertise. Bepaalde aspecten van het proces zijn reproduceerbaar vanwege die individuele expertise en er kan sprake zijn van enige documentatie en een zeker begrip van beleid en procedures. Zo kan er sprake zijn van geautomatiseerde processen om systemen te controleren op hun beveiligingsstatus zoals bij centraal beheerde werkstations (controle op virusscanner, updates etc.) Er is geen formeel (rapportage)proces of beleid. **Evidence.** 1. Rapportages van geautomatiseerde controles (indien van toepassing).	
Volwassenheidsniveau 3 (Gedefinieerd proces)	(Concern-)Informatiesystemen worden regelmatig gecontroleerd op naleving van implementatie van beveiligingsnormen. **Evidence in aanvulling op 2:** 1. Kopie beleid met opgenomen de controle op naleving van technische normen; 2. Kopie onderhoudscontract met de leveranciers; 3. Kopie factuur of rapportage waaruit blijkt dat op de informatiesystemen (software en hardware) controles worden uitgevoerd door een ervaren systeemtechnicus; 4. Kopie productbeschrijvingen; 5. Kopie checklisten die worden gebruikt bij de controle.	
Volwassenheidsniveau 4 (Beheerd en meetbaar)	Er is een gedegen en volledig proces met duidelijke werkinstructies en er worden interne best practices toegepast. De wijze en frequentie van controleren is gebaseerd op risicoanalyses. Alle aspecten van het proces zijn gedocumenteerd en reproduceerbaar. Werkinstructies en met name controles op operationele systemen zijn goedgekeurd en bekrachtigd door het management. De werkinstructies en procedures worden overgenomen en nageleefd. **Evidence in aanvulling op 3:** 1. Kopie vastgesteld controleschema; 2. Kopie notulen of besluitenlijst m.b.t. goedkeuring controles op operationele systemen.	
Volwassenheidsniveau 5 (Geoptimaliseerd)	Er worden externe best practices en normen toegepast. Processen, beleid en procedures zijn gestandaardiseerd en geïntegreerd, er wordt op een standaardwijze gerapporteerd. Rapportages worden geëvalueerd en er vindt regelmatig een onafhankelijke toetsing plaats zodat mogelijke verbeteringen in de processen ontdekt kunnen worden. **Evidence in aanvulling op 4:** 1. Kopie rapportages; 2. Kopie evaluatieverslag.	

Controledoelstelling 6.10

Cluster: Controle en logging	**ISO 27002 nummer: 18.2.3**
Controledoelstelling: Beoordeling van technische naleving Informatiesystemen behoren regelmatig te worden beoordeeld op naleving van de beleidsregels en normen van de organisatie voor informatiebeveiliging.	
Beoordeling (aanwezigen, datum en locatie)**:**	
Bevindingen: • **Documenten:** • **Interviews:** • **Waarneming ter plaatse:**	
Aanbevelingen:	

Bijlage 1 Beleid en procedures voor informatietransport

Deze leidraad heeft als doel handvatten te bieden voor het opstellen van een beleid met betrekking tot de uitwisseling van informatie met derde partijen.

De maatregelen kunnen worden opgenomen in een “Acceptable Use Policy” of in een aparte richtlijn.

Er behoren formeel beleid, formele procedures en formele beheersmaatregelen te zijn vastgesteld om de uitwisseling van informatie via het gebruik van alle typen communicatiefaciliteiten te beschermen. (De uitwisseling tussen organisaties is gebaseerd op formeel uitwisselingsbeleid, in lijn met uitwisselingsovereenkomsten en in overeenstemming met relevante wetgeving. Er zijn procedures en normen vastgesteld ter bescherming van informatie die wordt uitgewisseld.)

N.B. informatie opgenomen in elektronische berichten valt ook onder maatregel 5.16 van het Normenkader IBHO.

Informatieoverdracht kan plaatsvinden tussen collega's, over netwerken, tussen afdelingen binnen een instelling, over de grenzen of naar derde-partijen – of een combinatie hiervan.
Informatie wordt te allen tijde op grond van een risicobeoordeling geclassificeerd om verlies, diefstal of corruptie te voorkomen.
Gegevensoverdracht kan onderworpen zijn aan wettelijke eisen (GDPR).
Maatregelen beschrijven hoe wordt omgegaan met het automatisch doorsturen van berichten naar externe adressen en met het beheer van vertrouwelijke informatie.

Referenties

Normenkader Informatiebeveiliging HO v1.4 (2015).
ISO 27002:2013, hoofdstuk 13.2 “Informatietransport” (2013)
SCIPR Leidraad Classificatie (2015

Uitgangspunten

Om te bepalen op welke manier informatie uitgewisseld kan worden met derde partijen is dataclassificatie vereist (ref. maatregel 1.7 & 1.8). Dat betekent onder meer dat:

- alle gegevens, applicaties, processen en systemen een eigenaar hebben;
- die eigenaar heeft vastgesteld wat het vereiste beschermingsniveau is en welke restrisico’s aanvaardbaar zijn;
- de CISO, in afstemming met de gebruikersorganisatie en ICT, heeft bepaald wat passende beveiligingsmaatregelen zijn bij het beschermingsniveau;
- het classificatieniveau verantwoord maar zo 'laag' mogelijk is, zodat geen onnodige kosten worden gemaakt;
- de eigenaar periodiek een review uitvoert.

In de SCIPR “Leidraad Classificatie” worden voor ieder beveiligingsaspect drie classificatieniveau’s onderscheiden:

Classificatie-niveau	Schade	Beschikbaarheid	Integriteit	Vertrouwelijkheid
Laag	Enige (in)directe schade mogelijk.	Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende langer dan 1 week brengt geen merkbare (meetbare) schade toe aan de belangen van de instelling, haar medewerkers of haar studenten of klanten.	Het bedrijfsproces staat enkele integriteitsfouten toe.	Informatie die toegankelijk mag of moet zijn voor alle of grote groepen medewerkers of studenten. Vertrouwelijkheid is gering. Daar waar informatie openbaar is, is inzage geen issue, beheer (ten behoeve van de integriteit) wel.
Midden	Serieuze schade mogelijk.	Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende langer	Het bedrijfsproces staat zeer weinig integriteits-	Informatie die alleen toegankelijk mag zijn voor een beperkte

Classificatie-niveau	Schade	Beschikbaarheid	Integriteit	Vertrouwelijkheid
		dan 1 dag brengt merkbare schade toe aan de belangen van de instelling, haar medewerkers of haar studenten of klanten.	fouten toe. Bescherming van integriteit is absoluut noodzakelijk.	groep gebruikers. De informatie is vertrouwelijk.
Hoog	Zeer grote schade mogelijk.	Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende langer dan 1 uur brengt merkbare schade toe aan de belangen van de instelling, haar medewerkers of haar studenten of klanten.	Het bedrijfsproces staat geen integriteitsfouten toe.	Dit betreft zeer vertrouwelijke informatie, alleen bedoeld voor specifiek benoemde personen, waarbij onbedoeld bekend worden buiten deze groep grote schade kan toe brengen.

Maatregelen

Maatregelen worden genomen op basis van de classificatie van de informatie. Voor informatietransport zijn integriteit en vertrouwelijkheid de belangrijkste security aspecten waarmee rekening wordt gehouden. Zekerheid omtrent integriteit (en authenticiteit) en vertrouwelijkheid (exclusiviteit) van informatie tijdens transport kan worden bereikt door het gebruik van cryptografische middelen en, indirect, door het invoeren van beschermingsmaatregelen tegen malware infecties en inbraakpogingen. Verder speelt bewustzijn bij de medewerkers een belangrijke rol: je kunt nog zo veel technische maatregelen invoeren, als medewerkers nut en noodzaak ervan niet inzien is de kans groot dat dat die maatregelen niet toegepast worden of ineffectief zijn.

In het beleid is opgenomen dat:

- bij transport van vertrouwelijke informatie over niet vertrouwde netwerken, zoals het internet, altijd geschikte encryptie dient te worden toegepast;
- er procedures zijn opgesteld en geïmplementeerd voor opslag van vertrouwelijke informatie op verwijderbare media;
- verwijderbare media met vertrouwelijke informatie niet onbeheerd mogen worden achtergelaten op plaatsen die toegankelijk zijn zonder toegangscontrole;
- het meenemen van instellingsvertrouwelijke informatie buiten gecontroleerd gebied uitsluitend plaatsvindt indien dit voor de uitoefening van de functie noodzakelijk is;
- digitale documenten waar derden rechten aan kunnen ontlenen worden verzonden met gebruikmaking van een certificaat uitgegeven door een erkende root CA (Certificate Authority) en CSP (Certificate Service Provider);
- er een (spam-)filter is geactiveerd voor e-mail berichten;
- er standaard communicatieprotocollen worden gebruikt die geen afbreuk doen aan het gewenste beveiligingsniveau;
- fysieke verzending van bijzondere informatie dient te geschieden met goedgekeurde middelen, waardoor de inhoud niet zichtbaar, niet kenbaar en inbreuk detecteerbaar is.

In onderstaande tabel worden mogelijke maatregelen gegeven. We hanteren hierbij twee niveaus: laag en midden/hoog.

Classificatie	Maatregelen
laag	Geen bijzondere maatregelen nodig.
midden/hoog	• Bij het transport van informatie in elektronische berichten worden cryptografische methoden gebruikt om de vertrouwelijkheid en integriteit van informatie te borgen. Bijvoorbeeld bij e-mail wordt gebruik gemaakt van elektronische versleuteling en ondertekening van berichten; dit geldt ook voor eventuele bijlagen. Implementatie voorbeelden zijn S/MIME en PGP/GPG die worden ondersteund in de meeste e-mail cliënts. • Voor het transport van elektronische bestanden die niet via e-mail kunnen worden verstuurd (in verband met limieten op de grootte van bijlages) wordt een veilige dienst als SURFfilesender gebruikt (met de optie “Encrypt this file” actief – dan wordt het bestand versleuteld met AES-256; het wachtwoord wordt via een ander kanaal aan de geadresseerde gestuurd, bijv. SMS of telefonisch). • Voor het transport van informatie via niet-elektronische weg, is beschreven hoe deze informatie verpakt wordt en welke verzendmethode moet worden gehanteerd. Er is bijvoorbeeld een standaard envelop/doos die wordt gebruikt om de informatiedrager te verpakken en de geselecteerde koeriersdienst hanteert een procedure voor het volgen en afleveren van de zending, zodat te allen tijde kan worden vastgesteld waar de zending zich bevindt en of die in ongeschonden staat is afgeleverd.

Bijlage 2: Toelichting

Kenmerkend voor het vakgebied auditing is dat een onderzoek plaatsvindt ten opzichte van een eerder opgesteld en afgestemd normenkader. Zonder normenkader is een onderzoek feitelijk geen audit.
MBOaudit hanteert het generieke internationale normenkader voor informatiebeveiliging ISO27001 en de daarvan afgeleide set van best practices ISO 27002. In de literatuur is dit normenkader bekend onder de titel "Code voor Informatiebeveiliging". Het operationele toetsingskader van de **MBOaudit** is afgeleid van ISO 27002. Het normenkader wordt verrijkt tot een toetsingskader door er bewijslast aan toe te voegen. Allereerst is het normenkader ingedeeld in clusters.

Clustering naar zes thema's

Dit normenkader (27002 versie 2013) bevat 83 statements verdeelt over 6 clusters:

Cluster 1: Beleid en organisatie	20 statements
Cluster 2: Personeel, studenten en gasten	6 statements
Cluster 3: Ruimten en apparatuur	15 statements
Cluster 4: Continuïteit	15 statements
Cluster 5: Toegangsbeveiliging	17 statements
Cluster 6: Controle en logging	10 statements

De clustering is gebaseerd op een logische indeling die goed bruikbaar is voor het mbo- onderwijs. Per cluster zijn ook kwaliteitsaspecten af te leiden.

Schematische samenvatting:

Cluster	Onderwerpen (o.a.)	Kwaliteitsaspecten	Betrokkenen
1. Beleid en Organisatie	Informatiebeveiligingsbeleid Classificatie Inrichten beheer	• Beschikbaarheid • Integriteit • Vertrouwelijkheid • Controleerbaarheid	College van Bestuur Directeuren
2. Personeel, studenten en gasten	Informatiebeveiligingsbeleid Aanvullingen arbeidsovereenkomst Scholing en bewustwording	• Integriteit • Vertrouwelijkheid	College van Bestuur Dienst HR Ondernemingsraad
3. Ruimte en Apparatuur	Beveiligen van hardware, devices en bekabeling	• Beschikbaarheid • Integriteit	College van Bestuur ict dienst of afdeling
4. Continuïteit	Anti virussen, back up, bedrijf continuïteit planning	• Beschikbaarheid	College van Bestuur ict dienst of afdeling Functioneel beheer
5. Toegangsbeveiliging en Integriteit	Gebruikersbeheer, wachtwoorden, online transacties, sleutelbeheer, validatie	• Integriteit • Vertrouwelijkheid	College van Bestuur Functioneel beheer ict dienst of afdeling
6. Controle en logging	Systeemacceptatie, loggen van gegevens, registreren van storingen, toetsen beleid	• Controleerbaarheid	College van Bestuur Stafmedewerker informatiebeveiliging Kwaliteitszorg

Kwaliteitsaspecten nader uitgewerkt

Het toetsingskader hanteert dus de kwaliteitsaspecten: Beschikbaarheid, Integriteit, Vertrouwelijkheid en Controleerbaarheid. Deze kwaliteitsaspecten zijn niet vrij te interpreteren maar zijn strikt gedefinieerd en dus niet op verschillende manieren uit te leggen.

Beschikbaarheid: de mate waarin beheersmaatregelen de beschikbaarheid en ongestoorde voortgang van de ict-dienstverlening waarborgen.
Deelaspecten hiervan zijn:

- Continuïteit: de mate waarin de beschikbaarheid van de ict-dienstverlening gewaarborgd is;

- Portabiliteit: de mate waarin de overdraagbaarheid van het informatiesysteem naar andere gelijksoortige technische infrastructuren gewaarborgd is;
- Herstelbaarheid: de mate waarin de informatievoorziening tijdig en volledig hersteld kan worden.

Integriteit: de mate waarin de beheersmaatregelen (organisatie, processen en technologie) de juistheid, volledigheid en tijdigheid van de IT-dienstverlening waarborgen.
Deelaspecten hiervan zijn:

- Juistheid: de mate waarin overeenstemming van de presentatie van gegevens/informatie in IT-systemen ten opzichte van de werkelijkheid is gewaarborgd;
- Volledigheid: de mate van zekerheid dat de volledigheid van gegevens/informatie in het object gewaarborgd is;
- Waarborging: de mate waarin de correcte werking van de IT-processen is gewaarborgd.

Vertrouwelijkheid: de mate waarin uitsluitend geautoriseerde personen, programmatuur of apparatuur gebruik kunnen maken van de gegevens of programmatuur, al dan niet gereguleerd door (geautomatiseerde) procedures en/of technische maatregelen.
Deelaspecten hiervan zijn:

- Autorisatie: de mate waarin de adequate inrichting van bevoegdheden gewaarborgd is;
- Authenticiteit: de mate waarin de adequate verificatie van geïdentificeerde personen of apparatuur gewaarborgd is;
- Identificatie: de mate waarin de mechanismen ter herkenning van personen of apparatuur gewaarborgd zijn;
- Periodieke controle op de bestaande bevoegdheden. Het (geautomatiseerd) vaststellen of geïdentificeerde personen of apparatuur de gewenste handelingen mogen uitvoeren.

Controleerbaarheid: de mogelijkheid om kennis te verkrijgen over de structurering (documentatie) en werking van de IT-dienstverlening.
Deelaspecten hiervan zijn:

- Testbaarheid: De mate waarin de integere werking van de IT-dienstverlening te testen is;
- Meetbaarheid: Zijn er voldoende meet- en controlepunten aanwezig;
- Verifieerbaarheid: De mate waarin de integere werking van een IT-dienstverlening te verifiëren is.

De kwaliteitsaspecten effectiviteit en efficiëntie worden verder niet besproken. In een financiële ict-benchmark worden deze onderzocht, maar niet in de MBOaudit.

Bewijsvoering wordt ingedeeld op een 5 volwassenheidsniveaus

Het **Capability Maturity Model** is een model dat aangeeft op welk volwassenheidsniveau de informatiebeveiliging van een organisatie zit. Door ervaring in het gebruik is gebleken dat dit model op diverse processen in de organisatie toepasbaar is, ook op informatiebeveiligingsbeleid.
:

Volwassenheidsniveau 1 (Adhoc / initieel)	Initial: op dit niveau is de aanpak chaotisch en ad hoc. Problemen worden pas opgelost als ze zich voordoen. Dit is het niveau dat iedere organisatie aankan.
Volwassenheidsniveau 2 (haalbaar maar intuïtief)	Repeatable: is het niveau waarbij de organisatie zover geprofessionaliseerd is (bijvoorbeeld door het invoeren van projectmanagement) dat bij het ontwikkelproces gebruik wordt gemaakt van de kennis die eerder is opgedaan. Beslissingen worden dus genomen op basis van ervaring.
Volwassenheidsniveau 3 (gedefinieerd proces)	Defined: is het niveau waarbij de belangrijkste processen zijn gestandaardiseerd. *Een en ander is vastgelegd en daardoor controleerbaar (HO toevoeging).*
Volwassenheidsniveau 4 (Beheerst en meetbaar)	Managed: is het niveau waarbij de kwaliteit van het ontwikkelproces wordt gemeten zodat het kan worden bijgestuurd. *Een PDCA cyclus wordt aantoonbaar doorlopen (toevoeging HO).*
Volwassenheidsniveau 5 (Geoptimaliseerd)	Optimised: is het niveau waarbij het ontwikkelproces als een geoliede machine loopt en er alleen maar sprake is van fijn afstemming (de puntjes op de i).

Bijlage 3: Framework informatiebeveiliging en privacy in het mbo