C H E C K L I S T

# 3 Beveiligingsbeleid

## 3.1.1 Beleidsdocument voor informatiebeveiliging

| | | J | N | G | O |
|---|---|---|---|---|---|
| 1 | Is er een beleidsdocument voor informatiebeveiliging beschikbaar? | ❒ | ❒ | ❒ | ❒ |
| 2 | Wordt in dat document een definitie gegeven van het begrip informatiebeveiliging (doelstellingen, scope en reikwijdte)? | ❒ | ❒ | ❒ | ❒ |
| 3 | Is in het document aangegeven in hoeverre de (belangrijkste) bedrijfsprocessen afhankelijk zijn van informatiesystemen? | ❒ | ❒ | ❒ | ❒ |
| 4 | Toont het management zich zichtbaar betrokken met een verklaring die de doelstellingen en de principes van informatiebeveiliging ondersteunt? | ❒ | ❒ | ❒ | ❒ |
| 5 | Is er in het beleidsdocument aandacht besteed aan: | | | | |
| | • het voldoen aan wettelijke en contractuele verplichtingen; | ❒ | ❒ | ❒ | ❒ |
| | • de eisen voor scholing van beveiligingsfunctionarissen; | ❒ | ❒ | ❒ | ❒ |
| | • de eisen voor de continuïteit van de bedrijfsprocessen? | ❒ | ❒ | ❒ | ❒ |
| 6 | Geeft het document duidelijk aan welke algemene en specifieke taken en verantwoordelijkheden op het gebied van informatiebeveiliging zijn toebedeeld aan functionarissen en disciplines? | ❒ | ❒ | ❒ | ❒ |
| 7 | Is in het document opgenomen dat het belang van beveiliging bij herhaling duidelijk moet worden gemaakt aan alle managers en werknemers? | ❒ | ❒ | ❒ | ❒ |
| 8 | Bevat het document de verplichting voor de werknemers om beveiligingsincidenten te melden, waarna rapportage aan het management volgt? | ❒ | ❒ | ❒ | ❒ |
| 9 | Is het opstellen en onderhouden van het beleidsdocument opgedragen aan een specifieke functionaris? | ❒ | ❒ | ❒ | ❒ |
| 10 | Is in het document vastgelegd met welke regelmaat het beleid moet worden aangepast? | ❒ | ❒ | ❒ | ❒ |
| 11 | Is in het beleidsdocument de bepaling opgenomen dat bij nieuwe informatiesystemen of bij belangrijke wijzigingen opnieuw een risico-inventarisatie behoort te worden uitgevoerd? | ❒ | ❒ | ❒ | ❒ |
| 12 | Bevat het beleidsdocument een globale beschrijving hoe de risico-inventarisatie moet worden uitgevoerd? | ❒ | ❒ | ❒ | ❒ |
| 13 | Wordt er regelmatig een risico-inventarisatie uitgevoerd? | ❒ | ❒ | ❒ | ❒ |
| 14 | Wordt daarin vastgesteld wat de belangrijkste bedrijfsprocessen van de onderneming zijn en wat de belangrijkste bedreigingen zijn? | ❒ | ❒ | ❒ | ❒ |
| 15 | Wordt daarin ook vastgelegd wat de resterende risico's zijn die nog door de leiding van de onderneming aanvaardbaar worden geacht? | ❒ | ❒ | ❒ | ❒ |
| 16 | Wordt een afweging gemaakt van de kosten van beveiligingsmaatregelen en de effectiviteit van die maatregelen? | | | | |
| 17 | Wordt de uitkomst van de risico-inventarisatie schriftelijk vastgelegd? | ❒ | ❒ | ❒ | ❒ |
| 18 | Is de documentatie op een uniforme wijze opgezet, zodat de resultaten van een nieuwe inventarisatie kunnen worden vergeleken met die van een eerdere inventarisatie? | ❒ | ❒ | ❒ | ❒ |
| 19 | Wordt elk document formeel vastgesteld door de hoogste leiding? | ❒ | ❒ | ❒ | ❒ |
| 20 | Wordt periodiek een beschrijving gemaakt van de actuele situatie van de informatiebeveiligingsmaatregelen? | ❒ | ❒ | ❒ | ❒ |
| 21 | Worden aan de hand van wijzigingen in de organisatie, geconstateerde incidenten of nieuwe bedreigingen geïnventariseerd op welke onderdelen de informatiebeveiligingsmaatregelen moeten worden aangepast? | ❒ | ❒ | ❒ | ❒ |



Zo beantwoorden: ☑

**J**a
**N**ee
**G**edeeltelijk
**O**nbekend

| | | J | N | G | O |
|---|---|---|---|---|---|
| 22 | Is een plan opgesteld hoe men, uitgaand van de actuele situatie, de gewenste situatie kan bereiken? | ❒ | ❒ | ❒ | ❒ |
| 23 | Is een plan van aanpak voor de implementatie opgesteld, waarin de taken zijn verdeeld? | ❒ | ❒ | ❒ | ❒ |
| 24 | Is de prioriteit vastgesteld voor de implementatie van de verschillende informatiebeveiligingsmaatregelen? | ❒ | ❒ | ❒ | ❒ |
| 25 | Is een begroting opgesteld met een schatting van de benodigde kwalitatieve en kwantitatieve capaciteiten die nodig zijn voor een succesvolle implementatie? | ❒ | ❒ | ❒ | ❒ |
| | **3.1.2 Beoordeling en evaluatie** | | | | |
| 1 | Kent het beleid een eigenaar die verantwoordelijk is voor handhaving en evaluatie? | ❒ | ❒ | ❒ | ❒ |
| 2 | Is in het beleidsdocument beschreven, dat regelmatig de werking van de beveiliging wordt gecontroleerd, waarbij het management van de bevindingen op de hoogte wordt gesteld? | ❒ | ❒ | ❒ | ❒ |
| 3 | Is in het beleidsdocument aangegeven dat aanpassing van de informatiebeveiliging noodzakelijk is bij belangrijke wijzigingen in de | | | | |
| | • omgeving van de organisatie; | ❒ | ❒ | ❒ | ❒ |
| | • kritische bedrijfsprocessen; | ❒ | ❒ | ❒ | ❒ |
| | • informatiesystemen, waarmee die kritische bedrijfsprocessen worden ondersteund? | ❒ | ❒ | ❒ | ❒ |
| 4 | Wordt het beleidsdocument aangepast naar aanleiding van opgetreden incidenten? | ❒ | ❒ | ❒ | ❒ |
| 5 | Worden periodieke evaluaties uitgevoerd op: | ❒ | ❒ | ❒ | ❒ |
| | • de effectiviteit van het beleid aan de hand van het aantal, het type en de gevolgen van beveiligingsincidenten; | ❒ | ❒ | ❒ | ❒ |
| | • de kosten en het effect van de beveiligingsmaatregelen op de efficiency van de organisatie; | ❒ | ❒ | ❒ | ❒ |
| | • het effect van technologische veranderingen? | ❒ | ❒ | ❒ | ❒ |

## 4 Beveiligingsorganisatie

### 4.1.1 Managementforum voor informatiebeveiliging

| | | | | | |
|---|---|---|---|---|---|
| 1 | Bestaat binnen de onderneming een beleidsbepalend forum (bijvoorbeeld een stuurgroep informatiebeveiliging) op een zo hoog mogelijk niveau om richting en gezag aan beveiliging te geven? | ❒ | ❒ | ❒ | ❒ |
| 2 | Is een lid van het managementteam als voorzitter van de stuurgroep belast met de coördinatie van de werkzaamheden op het gebied van informatiebeveiliging? | ❒ | ❒ | ❒ | ❒ |
| 3 | Is aangegeven wie de verantwoordelijkheid draagt voor het implementeren van het beveiligingsbeleid in de diverse organisatorische eenheden? | ❒ | ❒ | ❒ | ❒ |
| 4 | Heeft de hoogste leiding van de onderneming een projectorganisatie ingesteld om het beveiligingsbeleid en beveiligingsplan te ontwerpen en te implementeren? | ❒ | ❒ | ❒ | ❒ |
| 5 | Bestaat er een formele procedure waarin het (herziene) beveiligingsbeleid formeel wordt goedgekeurd en de verantwoordelijkheden worden toegekend? | ❒ | ❒ | ❒ | ❒ |
| 6 | Krijgt het forum informatie over de belangrijkste bedreigingen waaraan de bedrijfsinformatie is blootgesteld? | ❒ | ❒ | ❒ | ❒ |
| 7 | Vindt aan het forum rapportage plaats van belangrijke beveiligingsincidenten en de naar aanleiding daarvan genomen maatregelen? | ❒ | ❒ | ❒ | ❒ |
| 8 | Worden initiatieven op het gebied van uitbreiding van informatiebeveiliging goedgekeurd in een formele procedure? | ❒ | ❒ | ❒ | ❒ |



Zo beantwoorden: ☑

**J**a
**N**ee
**G**edeeltelijk
**O**nbekend

| | | J | N | G | O |
|---|---|---|---|---|---|
| | **4.1.2 Coördinatie van informatiebeveiliging** | | | | |
| 1 | Is de onderneming zodanig groot dat de coördinatie van informatiebeveiliging gewenst is? | ❒ | ❒ | ❒ | ❒ |
| 2 | Indien coördinatie is gewenst, is daarvoor dan een commissie ingesteld van leden uit verschillende disciplines en specialisten voor informatiebeveiliging? | ❒ | ❒ | ❒ | ❒ |
| 3 | Zijn de taken en verantwoordelijkheden op het gebied van informatiebeveiliging van de leden van die commissie voldoende duidelijk en is het voorzitterschap van de commissie organisatorisch op voldoende hoog niveau binnen de onderneming belegd? | ❒ | ❒ | ❒ | ❒ |
| 4 | Over welke methoden en processen voor informatiebeveiliging heeft die commissie overeenstemming bereikt, bijvoorbeeld over een methode van risico-inventarisatie en classificatie van informatie? | ❒ | ❒ | ❒ | ❒ |
| 5 | Ondersteunt de commissie voldoende de initiatieven tot informatiebeveiliging die gelden voor de gehele onderneming (bijvoorbeeld het bevorderen van het beveiligingsbewustzijn bij het personeel)? | ❒ | ❒ | ❒ | ❒ |
| 6 | Bevordert de commissie het tot stand komen van een samenhangend geheel van maatregelen en procedures, gebaseerd op een geaccepteerd beveiligingsplan en afgeleid van een ondernemingsplan? | ❒ | ❒ | ❒ | ❒ |
| 7 | Bestaan er normen en richtlijnen uit de branche of van organisaties voor standaardisatie en, zo ja, zijn deze gebruikt bij het uitwerken van het beveiligingsbeleid? | ❒ | ❒ | ❒ | ❒ |
| 8 | Coördineert de commissie de implementatie van nieuwe beveiligingsmaatregelen voor nieuwe systemen of diensten? | ❒ | ❒ | ❒ | ❒ |
| 9 | Levert de commissie een zichtbare bijdrage aan informatiebeveiliging in de onderneming? | ❒ | ❒ | ❒ | ❒ |
| 10 | Wanneer geen commissie is ingesteld, is de coördinatie van de informatiebeveiliging dan opgedragen aan een eigen specialist, zoals bijvoorbeeld een ‘information security officer’? | ❒ | ❒ | ❒ | ❒ |
| 11 | Is bij de benoeming van zo’n functionaris rekening gehouden met de vertrouwenspositie die hij in de onderneming inneemt? | ❒ | ❒ | ❒ | ❒ |
| 12 | Zijn er zo weinig mogelijk operationele taken op het gebied van informatiebeveiliging aan die beveiligingsfunctionaris toebedeeld? | ❒ | ❒ | ❒ | ❒ |
| | **4.1.3 Toewijzing van verantwoordelijkheden voor informatiebeveiliging** | | | | |
| 1 | Zijn de verantwoordelijkheden voor de bescherming van gegevens en het uitvoeren van beveiligingsprocedures expliciet gedefinieerd? | ❒ | ❒ | ❒ | ❒ |
| 2 | Bestaan in het informatiebeveiligingsbeleid algemene richtlijnen voor het toewijzen van functies en verantwoordelijkheden voor beveiliging binnen de onderneming, zoals het verlenen van toegangsrechten voor informatiesystemen en het verlenen van toegang tot ruimten? | ❒ | ❒ | ❒ | ❒ |
| 3 | Zijn deze aangevuld met detailvoorschriften voor bepaalde lokaties, informatiesystemen en diensten? | ❒ | ❒ | ❒ | ❒ |
| 4 | Bevatten die detailvoorschriften ook aanbevelingen voor het expliciet toewijzen van lokale verantwoordelijkheid voor afzonderlijke gegevens (zowel gegevensdragers als informatie) en beveiligingsprocedures (bijvoorbeeld gericht op de continuïteit van de belangrijkste bedrijfsprocessen)? | ❒ | ❒ | ❒ | ❒ |
| 5 | Is een verantwoordelijk manager als ‘eigenaar’ aangewezen voor de beveiliging van een informatiesysteem? | ❒ | ❒ | ❒ | ❒ |
| 6 | Wanneer deze verantwoordelijk manager zijn werkzaamheden heeft overgedragen aan anderen, is dan duidelijk hoe de rechten en plichten op het gebied van de informatiebeveiliging zijn verdeeld (bijvoorbeeld vastgelegd in een dienstverleningsovereenkomst)? | ❒ | ❒ | ❒ | ❒ |



Zo beantwoorden: ☑

**J**a
**N**ee
**G**edeeltelijk
**O**nbekend

| | | J | N | G | O |
|---|---|---|---|---|---|
| 7 | Zijn de verschillende soorten gegevens en beveiligingsprocedures van elk afzonderlijk informatiesysteem geïdentificeerd en duidelijk gedefinieerd? | ❒ | ❒ | ❒ | ❒ |
| 8 | Heeft de verantwoordelijke manager de beveiligingsprocedures geaccordeerd en zijn verantwoordelijkheden gedocumenteerd? | ❒ | ❒ | ❒ | ❒ |
| 9 | Bestaat er een duidelijke definitie en documentatie van de autorisatieniveaus in alle informatiesystemen? | ❒ | ❒ | ❒ | ❒ |
| | **4.1.4 Autorisatieproces voor IT-voorzieningen** | | | | |
| 1 | Bestaat er een goedkeuringsprocedure voor de installatie van nieuwe voorzieningen of wijziging van bestaande voorzieningen voor informatietechnologie (apparatuur en programmatuur)? | ❒ | ❒ | ❒ | ❒ |
| 2 | Is daarin vastgelegd dat geen ongeautoriseerde voorzieningen mogen worden geïnstalleerd en gebruikt? | ❒ | ❒ | ❒ | ❒ |
| 3 | Moet volgens die procedure elke installatie formeel worden goedgekeurd, waarbij het doel en gebruik worden geautoriseerd, en bestaat er zowel een zakelijk als een technisch autorisatieniveau? | ❒ | ❒ | ❒ | ❒ |
| 4 | Zijn de managers aangewezen die zakelijke goedkeuring mogen verlenen? | ❒ | ❒ | ❒ | ❒ |
| 5 | Behoren daartoe ook managers die verantwoordelijk zijn voor het onderhoud van het systeem, zodat zekerheid bestaat over naleving van de relevante beveiligingseisen en -procedures? | ❒ | ❒ | ❒ | ❒ |
| 6 | Is bij de goedkeuring ook rekening gehouden met de effectiviteit en de efficiency van de informatiebeveiliging, zoals bijvoorbeeld beheerskosten, mate van controleerbaarheid en soort rapportage? | ❒ | ❒ | ❒ | ❒ |
| 7 | Is bekend welke managers technische goedkeuring mogen verlenen? | ❒ | ❒ | ❒ | ❒ |
| 8 | Mag slechts apparatuur of programmatuur in een netwerk worden geplaatst van een technisch goedgekeurd type? | ❒ | ❒ | ❒ | ❒ |
| 9 | Mag slechts apparatuur of programmatuur worden gebruikt van een technisch goedgekeurd type, zodat het dienstverlenend bedrijf dat het onderhoud verzorgt niet voor verrassingen komt te staan? | ❒ | ❒ | ❒ | ❒ |
| 10 | Wordt steeds gecontroleerd of de voorschriften uit de procedure worden nageleefd? | ❒ | ❒ | ❒ | ❒ |
| 11 | Is bekend wie die controle uitvoert en aan wie wordt gerapporteerd? | ❒ | ❒ | ❒ | ❒ |
| | **4.1.5 Specialistisch advies over informatiebeveiliging** | | | | |
| 1 | Wordt periodiek specialistisch advies ingewonnen op het gebied van informatiebeveiliging? | ❒ | ❒ | ❒ | ❒ |
| 2 | Wordt, als er geen interne beveiligingsadviseur aanwezig is, een externe beveiligingsadviseur aangetrokken van een gerenommeerd bedrijf? | ❒ | ❒ | ❒ | ❒ |
| 3 | Is dat bedrijf aangesloten bij een branche- of beroepsorganisatie, die eisen stelt aan de kwaliteit van de dienstverlening? | ❒ | ❒ | ❒ | ❒ |
| 4 | Wordt van de externe beveiligingsadviseur een geheimhoudingsverklaring gevraagd? | ❒ | ❒ | ❒ | ❒ |
| 5 | Indien er in de onderneming geen interne beveiligingsadviseur bestaat, is er dan wel een functionaris aangewezen als contactpersoon voor de externe beveiligingsadviseur? | ❒ | ❒ | ❒ | ❒ |
| 6 | Is vastgelegd dat interne of externe beveiligingsadviseurs bij incidenten rechtstreeks toegang krijgen tot managers op alle niveaus in de onderneming, waarbij zij kunnen beschikken over alle benodigde informatie? | ❒ | ❒ | ❒ | ❒ |
| 7 | Is vastgelegd dat bij een incident onmiddellijk een interne dan wel een externe beveiligingsadviseur gewaarschuwd wordt, zodat de onderneming direct de beschikking heeft over deskundig advies en hulp bij onderzoek? | ❒ | ❒ | ❒ | ❒ |



Zo beantwoorden: ☑

**J**a
**N**ee
**G**edeeltelijk
**O**nbekend

| | | J | N | G | O |
|---|---|---|---|---|---|
| | **4.1.6 Samenwerking tussen organisaties** | | | | |
| 1 | Hebben de interne beveiligingsspecialisten regelmatig contact met vakgenoten in de eigen branche of met externe beveiligingsadviseurs? | ❒ | ❒ | ❒ | ❒ |
| 2 | Wordt daarbij informatie uitgewisseld over nieuwe bedreigingen en nieuwe maatregelen daartegen? | ❒ | ❒ | ❒ | ❒ |
| 3 | Werken de beveiligingsspecialisten in een branche samen bij het uniformeren van het beveiligingsbeleid en het opstellen van normen en richtlijnen? | ❒ | ❒ | ❒ | ❒ |
| 4 | Onderhouden de beveiligingsspecialisten ook contact met wetgevende autoriteiten, dienstverlenende leveranciers en telecommunicatiebedrijven, om snel te reageren op nieuwe ontwikkelingen? | ❒ | ❒ | ❒ | ❒ |
| 5 | Is het uitwisselen van informatie zodanig beperkt dat vertrouwelijke bedrijfsinformatie niet in handen valt van ongeautoriseerde personen? | ❒ | ❒ | ❒ | ❒ |
| | **4.1.7 Onafhankelijke beoordeling van informatiebeveiliging** | | | | |
| 1 | Wordt het bestaan en de werking van het informatiebeveiligingsbeleid beoordeeld door een onafhankelijke functionaris? | ❒ | ❒ | ❒ | ❒ |
| 2 | Is bepaald wie er opdracht geeft tot die beoordeling en aan wie moet worden gerapporteerd? | ❒ | ❒ | ❒ | ❒ |
| 3 | Wordt opdracht verstrekt (door wie/aan wie) tot het aanpassen van maatregelen, wanneer uit de rapportage blijkt dat deze maatregelen geen effect sorteren of niet uitvoerbaar zijn? | ❒ | ❒ | ❒ | ❒ |
| 4 | Mag het resultaat van de beoordeling worden toegezonden aan externe toezichthoudende instanties? | ❒ | ❒ | ❒ | ❒ |
| | **4.2.1 Identificeren van risico's van toegang door derden** | | | | |
| 1 | Hebben derden, zoals leveranciers, klanten, onderhouds- of telecommunicatiebedrijven, via een netwerkaansluiting naar buiten geen toegang tot apparatuur of programmatuur van de onderneming? | ❒ | ❒ | ❒ | ❒ |
| 2 | Zijn de risico's van die toegang geanalyseerd? | ❒ | ❒ | ❒ | ❒ |
| 3 | Is bij de analyse van die risico's rekening gehouden met: | | | | |
| | • de wijze waarop toegang wordt verkregen; | ❒ | ❒ | ❒ | ❒ |
| | • de waarde van de informatie; | ❒ | ❒ | ❒ | ❒ |
| | • de beveiligingsmaatregelen bij de andere partij; | ❒ | ❒ | ❒ | ❒ |
| | • de gevolgen van de verbinding voor de IT-infrastructuur? | ❒ | ❒ | ❒ | ❒ |
| 4 | Zijn er voldoende beveiligingsmaatregelen genomen om die risico's tot een aanvaardbaar niveau terug te brengen? | ❒ | ❒ | ❒ | ❒ |
| 5 | Krijgen derden slechts dan toegang tot IT-voorzieningen, nadat zij een contract hebben ondertekend met daarin onder andere een geheimhoudingsverklaring? | ❒ | ❒ | ❒ | ❒ |
| | **4.2.2 Beveiligingseisen in contracten met derden** | | | | |
| 1 | Zijn de overeenkomsten die betrekking hebben op de toegang tot IT-voorzieningen van de onderneming door externe gebruikers, gebaseerd op een formeel contract? | ❒ | ❒ | ❒ | ❒ |
| 2 | Is bij het opstellen van dat contract gebruik gemaakt van de expertise van een juridische deskundige? | ❒ | ❒ | ❒ | ❒ |
| 3 | Zijn in dat contract alle noodzakelijke beveiligingsvoorwaarden opgenomen? | ❒ | ❒ | ❒ | ❒ |
| 4 | Wordt bijgehouden welke contracten zijn afgesloten? | ❒ | ❒ | ❒ | ❒ |



Zo beantwoorden: ☑

**J**a
**N**ee
**G**edeeltelijk
**O**nbekend

| | | J | N | G | O |
|---|---|---|---|---|---|
| 5 | Is de verantwoordelijkheid voor het beheer van contracten duidelijk belegd binnen de organisatie? | ❒ | ❒ | ❒ | ❒ |
| 6 | Wordt gecontroleerd of een contract is getekend, voordat toegang tot de IT-voorzieningen wordt verleend? | ❒ | ❒ | ❒ | ❒ |
| 7 | Wordt in het contract aandacht besteed aan het algemene beleid ten aanzien van informatiebeveiliging? | ❒ | ❒ | ❒ | ❒ |
| 8 | Is in het contract vastgelegd welke toegangsmethoden zijn toegestaan en hoe gebruikersidentificaties en wachtwoorden moeten worden beheerd en gebruikt? | ❒ | ❒ | ❒ | ❒ |
| 9 | Beschrijft het contract welke IT-dienst beschikbaar wordt gesteld? | ❒ | ❒ | ❒ | ❒ |
| 10 | Wanneer het gebruik bij een contractpartij wordt toegestaan aan meerdere personen, bestaat dan de verplichting om een lijst daarvan bij te houden? | ❒ | ❒ | ❒ | ❒ |
| 11 | Zijn de tijdstippen en dagen, waarop de dienst beschikbaar moet zijn, vastgelegd in het contract? | ❒ | ❒ | ❒ | ❒ |
| 12 | Indien de wens bestaat tot een hoge beschikbaarheid, is dan in het contract aandacht besteed aan continuïteitsvoorzieningen? | ❒ | ❒ | ❒ | ❒ |
| 13 | Bevat het contract de verplichtingen van alle partijen waarop de overeenkomst betrekking heeft? | ❒ | ❒ | ❒ | ❒ |
| 14 | Wordt in het contract verwezen naar procedures voor de bescherming van bedrijfsmiddelen, waaronder ook informatie? | ❒ | ❒ | ❒ | ❒ |
| 15 | Is in het contract rekening gehouden met verantwoordelijkheden op grond van wettelijke eisen, zoals die uit de Wet Bescherming Persoonsgegevens, het Burgerlijk Wetboek en de Algemene Wet Rijksbelastingen? | ❒ | ❒ | ❒ | ❒ |
| 16 | Is zonodig in het contract geregeld, dat toezicht mag worden gehouden op de gebruikers, waarbij het recht bestaat om de bevoegdheden te herroepen? | ❒ | ❒ | ❒ | ❒ |
| 17 | Is per contract de verantwoordelijkheid geregeld voor de installatie en het onderhoud van apparatuur en programmatuur? | ❒ | ❒ | ❒ | ❒ |
| 18 | Bestaat het recht om de contractuele verantwoordelijkheden te controleren? | ❒ | ❒ | ❒ | ❒ |
| 19 | Zijn er in het contract beperkende bepalingen opgenomen ten aanzien van het kopiëren en openbaar maken van informatie? | ❒ | ❒ | ❒ | ❒ |
| 20 | Heeft men maatregelen getroffen die er op gericht zijn bij het beëindigen van het contract de informatie en goederen terug te geven of te vernietigen? | ❒ | ❒ | ❒ | ❒ |
| 21 | Zijn eventuele vereiste fysieke beveiligingsmaatregelen in het contract beschreven? | ❒ | ❒ | ❒ | ❒ |
| 22 | Bevat het contract procedures die ervoor zorgen dat de beveiligingsmaatregelen worden opgevolgd? | ❒ | ❒ | ❒ | ❒ |
| 23 | Zijn in het contract maatregelen beschreven ter voorkoming van het verspreiden van virussen? | ❒ | ❒ | ❒ | ❒ |
| 24 | Is in het contract aandacht besteed aan de autorisatieprocedure voor de toegangsrechten van de gebruikers? | ❒ | ❒ | ❒ | ❒ |
| 25 | Zijn in het contract de afspraken vastgelegd over onderzoek en rapportage van beveiligingsincidenten? | ❒ | ❒ | ❒ | ❒ |
| 26 | Bevat het contract bepalingen met sancties of boetebedingen voor het geval dat een contractpartij de verplichtingen niet naleeft? | ❒ | ❒ | ❒ | ❒ |

### 4.3.1 Beveiligingseisen in uitbestedingscontracten

| | | | | | |
|---|---|---|---|---|---|
| 1 | Zijn de beveiligingseisen bij uitbesteding vastgelegd in een contract dat bekrachtigd is door alle betrokken partijen? | ❒ | ❒ | ❒ | ❒ |
| 2 | Bevat het contract ook een bepaling hoe wordt voldaan aan wettelijke vereisten, zoals bijvoorbeeld de wetgeving ter bescherming van de privacy? | ❒ | ❒ | ❒ | ❒ |



Zo beantwoorden: ☑

**J**a
**N**ee
**G**edeeltelijk
**O**nbekend

| | | J | N | G | O |
|---|---|---|---|---|---|
| 3 | Is het contract zodanig opgesteld dat alle partijen zich bewust zijn van hun verantwoordelijkheden op het gebied van informatiebeveiliging? | ❒ | ❒ | ❒ | ❒ |
| 4 | Beschrijft het contract hoe de gewenste beveiliging van de bedrijfsmiddelen wordt gehandhaafd en getest? | ❒ | ❒ | ❒ | ❒ |
| 5 | Zijn de maatregelen van fysieke en logische toegangsbeveiliging, waarmee de toegang tot en gebruik van gevoelige bedrijfsinformatie wordt beperkt tot geautoriseerde gebruikers, vastgelegd in het contract? | ❒ | ❒ | ❒ | ❒ |
| 6 | Is in het contract een paragraaf opgenomen waarin is beschreven hoe in het geval van een calamiteit de beschikbaarheid van de dienstverlening wordt gewaarborgd? | ❒ | ❒ | ❒ | ❒ |
| 7 | Bevat het contract een passage over de mate waarin fysiek maatregelen moeten worden genomen ter bescherming van de uitbestede apparatuur? | ❒ | ❒ | ❒ | ❒ |
| 8 | Is in het contract het recht op controle door derden, zoals EDP auditors of registeraccountants, geregeld? | ❒ | ❒ | ❒ | ❒ |
| 9 | Dwingt het contract af dat alle partijen meewerken om een beveiligingsprotocol op te stellen aan de hand van beveiligingseisen en procedurebeschrijvingen? | ❒ | ❒ | ❒ | ❒ |
| 10 | Is het opgestelde beveiligingsprotocol formeel vastgesteld door de partijen? | ❒ | ❒ | ❒ | ❒ |
| 11 | Zijn er werkafspraken gemaakt tussen de partijen om de voorwaarden uit het contract nader in te vullen? | ❒ | ❒ | ❒ | ❒ |
| 12 | Kan op grond van het contract een geheimhoudingsverklaring worden geëist? | ❒ | ❒ | ❒ | ❒ |
| 13 | Zijn in het contract bepalingen opgenomen wanneer een van beide partijen door overmacht of faillissement niet meer aan de verplichtingen kan voldoen (bijvoorbeeld deponering van de broncodes van programmatuur bij een onafhankelijke partij)? | ❒ | ❒ | ❒ | ❒ |
| 14 | Bevat het contract bepalingen met betrekking tot onvoorziene gebeurtenissen? | ❒ | ❒ | ❒ | ❒ |
| 15 | Wordt bij overname van de leverancier door derden het contract opengebroken? | ❒ | ❒ | ❒ | ❒ |
| 16 | Is voorzien in regelmatig onderhoud van de applicaties en de gebruikte apparatuur? | ❒ | ❒ | ❒ | ❒ |
| 17 | Zijn in het geval van uitbesteding de licenties of auteursrechten van de gebruikte programmatuur geregeld? | ❒ | ❒ | ❒ | ❒ |
| 18 | Bevat het contract een regeling bij geschillen? | ❒ | ❒ | ❒ | ❒ |
| 19 | Is in het contract vermeld welke kwaliteitsnormen worden gehanteerd? | ❒ | ❒ | ❒ | ❒ |

## 5 Classificatie en beheer van bedrijfsmiddelen

### 5.1.1 Overzicht van bedrijfsmiddelen

| | | | | | |
|---|---|---|---|---|---|
| 1 | Is in het informatiebeveiligingsbeleid (zie 3.1.1) voorgeschreven dat een overzicht moet worden gemaakt van de belangrijkste bedrijfsprocessen? | ❒ | ❒ | ❒ | ❒ |
| 2 | Wordt daarbij ook een overzicht vervaardigd van de bedrijfsmiddelen, met behulp waarvan informatie wordt verwerkt, getransporteerd of opgeslagen? | ❒ | ❒ | ❒ | ❒ |
| 3 | Wordt bij de inventarisatie van de bedrijfsmiddelen onderscheid gemaakt naar bijvoorbeeld informatie, programmatuur, apparatuur en dienstverlening? | ❒ | ❒ | ❒ | ❒ |
| 4 | Zijn die bedrijfsmiddelen en IT-bedrijfsmiddelen duidelijk geïdentificeerd? | ❒ | ❒ | ❒ | ❒ |
| 5 | Is voor alle bedrijfsmiddelen vastgelegd wie de eigenaar of de houder is, zodat duidelijk is wie verantwoordelijk is voor een beveiligingsmaatregel (zie ook 4.1.3)? | ❒ | ❒ | ❒ | ❒ |
| 6 | Is geïnventariseerd wat de belangrijkste risico's zijn voor die bedrijfsmiddelen? | ❒ | ❒ | ❒ | ❒ |



Zo beantwoorden: ☑

**J**a
**N**ee
**G**edeeltelijk
**O**nbekend

| | | J | N | G | O |
|---|---|---|---|---|---|
| 7 | Is er een risicoprofiel bepaald, dat wil zeggen de kans dat een bedreiging zich voordoet en de omvang van de gevolgen van het optreden van een bedreiging? | ❒ | ❒ | ❒ | ❒ |
| 8 | Worden bij de risico-inventarisatie tevens de gevolgen bepaald voor de bedrijfsprocessen wanneer bedrijfsmiddelen niet beschikbaar zijn, door onbevoegden zijn gewijzigd of door onbevoegden zijn geraadpleegd? | ❒ | ❒ | ❒ | ❒ |
| 9 | Wordt die risico-inventarisatie periodiek herhaald? | ❒ | ❒ | ❒ | ❒ |
| | **5.2.1 Richtlijnen voor het classificeren** | | | | |
| 1 | Zijn de bedrijfsmiddelen geclassificeerd conform de informatie die ermee wordt verwerkt of opgeslagen? | ❒ | ❒ | ❒ | ❒ |
| 2 | Bestaan er duidelijke en formeel vastgestelde richtlijnen voor het uitvoeren van de classificatie? | ❒ | ❒ | ❒ | ❒ |
| 3 | Is de verantwoordelijkheid voor het classificeren toegewezen aan de ‘eigenaar’ van de informatie? | ❒ | ❒ | ❒ | ❒ |
| 4 | Beoordeelt de eigenaar de classificatie van de informatie periodiek, bijvoorbeeld bij historische informatie? | ❒ | ❒ | ❒ | ❒ |
| 5 | Heeft de eigenaar vooraf aangegeven hoe lang de geclassificeerde informatie moet worden bewaard? | ❒ | ❒ | ❒ | ❒ |
| 6 | Converteert een met de bewaring belaste medewerker tijdig de opgeslagen informatie op een veilige wijze? | ❒ | ❒ | ❒ | ❒ |
| 7 | Is er een medewerker aangewezen die verantwoordelijk is voor het up-to-date houden van de richtlijnen en procedures inzake de classificatie? | ❒ | ❒ | ❒ | ❒ |
| 8 | Wordt bij de classificatie rekening gehouden met de vertrouwelijkheid van informatie, dat wil zeggen de noodzaak om enerzijds informatie te verspreiden en anderzijds de informatie te beperken? | ❒ | ❒ | ❒ | ❒ |
| 9 | Wordt bij de classificatie steeds rekening gehouden met alle kwaliteitsaspecten van de informatie? | ❒ | ❒ | ❒ | ❒ |
| | **5.2.2 Labelen en verwerken van informatie** | | | | |
| 1 | Zijn de informatiedragers zodanig gekenmerkt dat zowel voor de mens als voor de machine duidelijk is hoe deze verwerkt moeten worden? | ❒ | ❒ | ❒ | ❒ |
| 2 | Is de classificatie zodanig ingericht dat duidelijk is hoe met de informatie moet worden omgegaan (inclusief de wijze van distributie, archivering, et cetera)? | ❒ | ❒ | ❒ | ❒ |
| 3 | Wordt als vertrouwelijk geclassificeerde informatie zodanig behandeld dat deze pas dan over netwerken verzonden mag worden en op alle van toepassing zijnde media mag worden opgeslagen, wanneer er gebruik gemaakt wordt van een voldoende veilige encryptie (vercijfering)? | ❒ | ❒ | ❒ | ❒ |
| 4 | Is bij de classificatie geregeld welke bestanden op draagbare pc’s (laptops) vercijferd dienen te worden? | ❒ | ❒ | ❒ | ❒ |
| 5 | Wordt bij het aanbrengen van het kenmerk op een bedrijfsmiddel gebruik gemaakt van een methode waarbij dat kenmerk niet ongeschonden verwijderd of veranderd kan worden? | ❒ | ❒ | ❒ | ❒ |
| 6 | Wordt in contracten vermeld dat de onderneming een classificatiestelsel heeft waar leveranciers of afnemers rekening mee moeten houden? | ❒ | ❒ | ❒ | ❒ |



Zo beantwoorden: ☑

**J**a
**N**ee
**G**edeeltelijk
**O**nbekend

J N G O

## 6 Beveiligingseisen ten aanzien van personeel

### 6.1.1 Beveiligingseisen in de functieomschrijving

| | | |
|---|---|---|
| 1 | Is in het informatiebeveiligingsbeleid aandacht besteed aan de beveiligingseisen ten aanzien van het eigen vaste en tijdelijke personeel? | ❒ ❒ ❒ ❒ |
| 2 | Is geregeld dat personeelsleden met specifieke of unieke kennis of specialismen, deze kennis in het kader van informatiebeveiliging delen met anderen of voldoende documenteren, zodat geen kwetsbare functies kunnen ontstaan? | ❒ ❒ ❒ ❒ |
| 3 | Is gezorgd voor een tijdige vervanging van personeelsleden op een kwetsbare functie (bij vakantie, maar ook bij ziekte met een langere duur)? | ❒ ❒ ❒ ❒ |
| 4 | Zijn er maatregelen die er in voorzien dat bij vertrek of functieverandering van personeelsleden fysieke en logische toegangsregels direct gewijzigd worden? | ❒ ❒ ❒ ❒ |
| 5 | Zijn de voor de respectieve categorieën personeel (gebruikers en verwerkers) in het kader van informatiebeveiliging uit te voeren taken duidelijk omschreven en vastgelegd in functiebeschrijvingen? | ❒ ❒ ❒ ❒ |
| 6 | Zijn in de functiebeschrijvingen ook de verantwoordelijkheden en bevoegdheden in het kader van informatiebeveiliging vastgelegd, zodat daaruit de voor die functie noodzakelijke logische en fysieke autorisaties en authentificaties vallen af te leiden? | ❒ ❒ ❒ ❒ |
| 7 | Zijn er ook voor tijdelijke krachten functiebeschrijvingen, waarin voldaan wordt aan hetgeen onder de beide vorige items is gesteld? | ❒ ❒ ❒ ❒ |
| 8 | Gelden er voor ‘tijdelijke’ personeelsleden afwijkende maatregelen ten opzichte van ‘eigen’ personeelsleden (bijvoorbeeld een verbod om op de werkplek aanwezig te zijn na en voor een bepaalde tijd van de dag) en zijn deze in een functiebeschrijving vastgelegd? | ❒ ❒ ❒ ❒ |
| 9 | Zijn er bij een functiebeschrijving behorende werkomschrijvingen (administratieve organisatie) en zijn deze aan betrokkenen ter hand gesteld? | ❒ ❒ ❒ ❒ |
| 10 | Zijn er maatregelen genomen die er in voorzien dat bij het wijzigen van taakinhoud, verantwoordelijkheden of bevoegdheden ook de daaraan gekoppelde logische en fysieke bevoegdheden worden gewijzigd? | ❒ ❒ ❒ ❒ |
| 11 | Zijn er maatregelen getroffen, die er in voorzien dat niet alle bevoegdheden bij het uitvoeren van specifieke werkzaamheden in één hand terechtkomen (ook niet tijdens ziekte en vakantie van personeelsleden) en wordt deze functiescheiding formeel in functiebeschrijvingen vastgelegd (onverenigbaarheid van bepaalde taken)? | ❒ ❒ ❒ ❒ |
| 12 | Zijn er maatregelen die er op toezien dat er geen sterke vertrouwensfuncties of kwetsbare functies ontstaan, zonder dat daarvoor adequate informatiebeveiligingsmaatregelen zijn genomen en geïmplementeerd? | ❒ ❒ ❒ ❒ |
| 13 | Zijn er controlemaatregelen genomen, die erin voorzien dat wanneer vaste of tijdelijke personeelsleden van functie veranderen, er op hen een andere functiebeschrijving van toepassing is? | ❒ ❒ ❒ ❒ |

### 6.1.2 Screening en personeelsbeleid

| | | |
|---|---|---|
| 1 | Is er in het informatiebeveiligingsbeleid een passage opgenomen, die aangeeft in welke mate vaste en tijdelijke personeelsleden voor het aanvangen van de werkzaamheden zekere beveiligingsonderzoeken dienen te hebben ondergaan? | ❒ ❒ ❒ ❒ |



Zo beantwoorden: ☑

**J**a
**N**ee
**G**edeeltelijk
**O**nbekend

| | | J | N | G | O |
|---|---|---|---|---|---|
| 2 | Bevat de screening de volgende punten: | | | | |
| | • beschikbaarheid van positieve referenties; | ❒ | ❒ | ❒ | ❒ |
| | • controle van de volledigheid en de nauwkeurigheid van het curriculum vitae van de sollicitant; | ❒ | ❒ | ❒ | ❒ |
| | • verificatie van academische en professionele kwalificaties; | ❒ | ❒ | ❒ | ❒ |
| | • onafhankelijke identiteitscontrole (met behulp van paspoort)? | ❒ | ❒ | ❒ | ❒ |
| 3 | Wordt bij gevoelige functies ook een onderzoek ingesteld naar de kredietwaardigheid van de sollicitant? | ❒ | ❒ | ❒ | ❒ |
| 4 | Zijn maatregelen genomen om te voorkomen dat nieuw en onervaren personeel schade veroorzaakt aan gevoelige systemen? | ❒ | ❒ | ❒ | ❒ |
| 5 | Worden de werkzaamheden van het personeel regelmatig getoetst met behulp van beoordelings- en goedkeuringsprocedures? | ❒ | ❒ | ❒ | ❒ |
| 6 | Zijn er controlemaatregelen genomen om daadwerkelijk vast te stellen dat voor de aanvang van de werkzaamheden is voldaan aan de hiervoor genoemde beveiligingsmaatregelen ten aanzien van personeel? | ❒ | ❒ | ❒ | ❒ |
| 7 | Zijn managers er zich van bewust dat persoonlijke omstandigheden van hun personeel het werk kunnen beïnvloeden? | ❒ | ❒ | ❒ | ❒ |

**6.1.3 Geheimhoudingsverklaring**

| | | | | | |
|---|---|---|---|---|---|
| 1 | Is er in het informatiebeveiligingsbeleid voorzien dat personen een geheimhoudingsverklaring tekenen alvorens met de werkzaamheden aan te vangen (een rol die bij de overheid vervuld wordt door de eed of belofte)? | ❒ | ❒ | ❒ | ❒ |
| 2 | Zijn er controlemaatregelen genomen die er in voorzien dat daadwerkelijk wordt vastgesteld dat voor de aanvang van de werkzaamheden aan de hiervoor genoemde beveiligingsmaatregelen ten aanzien van personeel is voldaan? | ❒ | ❒ | ❒ | ❒ |

**6.1.4 Arbeidscontract**

| | | | | | |
|---|---|---|---|---|---|
| 1 | Zijn in het arbeidscontract passages opgenomen inzake de persoonlijke verantwoordelijkheden betreffende informatiebeveiliging? | ❒ | ❒ | ❒ | ❒ |
| 2 | Is in het arbeidscontract voorzien dat een personeelslid na het beëindigen van zijn/haar contract nog gedurende een bepaalde periode geheimhouding in acht dient te nemen? | ❒ | ❒ | ❒ | ❒ |
| 3 | Is in het arbeidscontract voorzien dat op het overtreden van voorschriften inzake informatiebeveiliging en geheimhouding sancties staan? | ❒ | ❒ | ❒ | ❒ |
| 4 | Is in het arbeidscontract voorzien dat wanneer thuis of elders buiten de formele werkplek gewerkt wordt, dezelfde verantwoordelijkheden bestaan als wanneer er op de formele werkplek gewerkt wordt? | ❒ | ❒ | ❒ | ❒ |
| 5 | Voorziet het arbeidscontract in een clausule die het intellectuele eigendom en het copyright regelt inzake de resultaten van de in dienstverband verrichte werkzaamheden? | ❒ | ❒ | ❒ | ❒ |

**6.2.1 Opleiding en training voor informatiebeveiliging**

| | | | | | |
|---|---|---|---|---|---|
| 1 | Zijn er maatregelen die erin voorzien dat nieuwe vaste en tijdelijke personeelsleden bij de eerste binnenkomst worden geïnformeerd over rechten en plichten in het kader van informatiebeveiliging (huisregels, cultuur, gewoonten, goede gebruiken, absolute verboden, enzovoort)? | ❒ | ❒ | ❒ | ❒ |



Zo beantwoorden: ☑

**J**a
**N**ee
**G**edeeltelijk
**O**nbekend

| | | J | N | G | O |
|---|---|---|---|---|---|
| 2 | Wordt bij het in het vorige punt bedoelde introductiegesprek materiaal uitgereikt waarin het informatiebeveiligingsregime uiteengezet wordt en laat men personeelsleden voor ontvangst en kennisname van dit documentatiemateriaal ook tekenen? | ❒ | ❒ | ❒ | ❒ |
| 3 | Zijn er maatregelen die erin voorzien dat de bekendheid met regels op het gebied van informatiebeveiliging op het gewenste niveau blijft? | ❒ | ❒ | ❒ | ❒ |
| 4 | Is in het informatiebeveiligingsbeleid voorzien dat vaste en vooral tijdelijke personeelsleden naar behoren zijn opgeleid en getraind in het kader van informatiebeveiliging, teneinde te voorkomen dat door proberen en experimenteren de betrouwbaarheid van de hen ter beschikking gestelde bedrijfsmiddelen wordt aangetast en daarmee de gewenste informatiebeveiliging geweld wordt aangedaan? | ❒ | ❒ | ❒ | ❒ |
| 5 | Zijn er maatregelen genomen om ervoor te zorgen dat geen situaties ontstaan waardoor personeelsleden in onmogelijke situaties worden geplaatst, die hen min of meer dwingen informatiebeveiligingsmaatregelen te doorbreken (overbelasting, onvoldoende middelen, functievermenging of cumulaties)? | ❒ | ❒ | ❒ | ❒ |
| 6 | Voorziet het informatiebeveiligingsbeleid in acties om het beveiligingsbewustzijn van vast en tijdelijke personeel op het gewenste niveau te brengen en te houden? | ❒ | ❒ | ❒ | ❒ |
| 7 | Zijn er maatregelen genomen om regelmatig het beveiligingsbewustzijn op bepaalde punten te toetsen? | ❒ | ❒ | ❒ | ❒ |
| 8 | Is er een personeelshandleiding waarin alle zaken betreffende informatiebeveiliging zijn bijeengebracht en is die handleiding aan ieder vast en tijdelijk personeelslid verstrekt, waarbij men voor ontvangst heeft getekend? | ❒ | ❒ | ❒ | ❒ |
| 9 | Zijn er helpdesks ingericht waar vast en tijdelijke personeel met vragen inzake het functioneren van bedrijfsmiddelen terecht kan en adequaat geholpen wordt? | ❒ | ❒ | ❒ | ❒ |
| 10 | Zijn er in het kader van informatiebeveiliging personeel relaties gelegd met wet- en regelgeving (ARBO-wet, Wet Bescherming Persoonsgegevens, Wet Computercriminaliteit)? | ❒ | ❒ | ❒ | ❒ |
| 11 | Is aan het personeel duidelijk gemaakt welke informatiebeveiligingsmaatregelen in bepaalde ruimten (bijvoorbeeld ruimten waarin een concentratie van risico's is bijeengebracht) getroffen zijn en hoe de werking daarvan is? | ❒ | ❒ | ❒ | ❒ |

### 6.3.1 Het rapporteren van beveiligingsincidenten

| | | | | | |
|---|---|---|---|---|---|
| 1 | Zijn er meldpunten ingericht waar personeelsleden beveiligingsincidenten inzake de ingezette bedrijfsmiddelen kenbaar kunnen maken (waarbij niet alleen gedacht moet worden aan een meldpunt inzake de informatietechnologie of datacommunicatie, maar ook inzake de werking van de infrastructurele voorzieningen en de beveiliging en bewaking van gebouwen en ruimten)? | ❒ | ❒ | ❒ | ❒ |
| 2 | Is het personeel duidelijk gemaakt wat onder een beveiligingsincident verstaan wordt (niet alleen beschadigingen of verlies van bedrijfsmiddelen, maar ook het verrichten van handelingen die in strijd zijn met de beveiligingsprocedures)? | ❒ | ❒ | ❒ | ❒ |
| 3 | Worden van alle informatiebeveiligingsincidenten rapportages samengesteld en uitgebracht aan het daartoe aangewezen management? | ❒ | ❒ | ❒ | ❒ |
| 4 | Zijn er maatregelen genomen die er op toezien dat het management reageert op de in dit kader uitgebracht rapportages en de daarin eventueel opgenomen aanbevelingen? | ❒ | ❒ | ❒ | ❒ |



Zo beantwoorden: ☑

**J**a
**N**ee
**G**edeeltelijk
**O**nbekend

J N G O

### 6.3.2 Het rapporteren van zwakke plekken in de beveiliging

1 Zijn er faciliteiten geschapen waar personeelsleden zwakke plekken in de beveiligingsorganisatie kunnen melden. Wordt daarop snel en adequaat gereageerd, zodat er een positief uitstralingseffect uitgaat van het beveiligingsregime? ❒ ❒ ❒ ❒

2 Wordt er gebruik gemaakt van logfiles voor het opsporen en analyseren van zwakke plekken in de beveiliging? ❒ ❒ ❒ ❒

3 Zijn er controleprogramma's en een controleplan, op grond waarvan periodieke controles worden uitgevoerd, en is daarin ook voorgeschreven dat naar zwakke plekken in de beveiliging gezocht moet worden? ❒ ❒ ❒ ❒

4 Is erin voorzien dat een review of audit wordt uitgevoerd op de blijvende werking van beveiligingsmaatregelen? ❒ ❒ ❒ ❒

### 6.3.3 Het rapporteren van onvolkomenheden in de software

1 Worden er van onvolkomenheden in software en van het niet correct werken van software rapportages samengesteld en uitgebracht aan het daartoe aangewezen management? ❒ ❒ ❒ ❒

2 Zijn er maatregelen genomen die waarborgen dat het management reageert op de in dit kader uitgebracht rapportages en de daarin eventueel opgenomen aanbevelingen? ❒ ❒ ❒ ❒

### 6.3.4 Lering trekken uit incidenten

1 Is er een registratie en analyse van alle incidenten en storingen? ❒ ❒ ❒ ❒

2 Wordt deze registratie ook gebruikt bij het leren van incidenten en storingen ten einde deze in de toekomst te kunnen voorkomen? ❒ ❒ ❒ ❒

### 6.3.5 Disciplinaire maatregelen

1 Is er in het informatiebeveiligingsbeleid ook een sanctiebeleid opgenomen dat gevolgd wordt bij het (herhaaldelijk) overtreden van de in het kader van informatiebeveiliging geldende stelsel van informatiebeveiligingsmaatregelen? ❒ ❒ ❒ ❒

2 Maakt het zich al of niet houden aan informatiebeveiligingsmaatregelen deel uit van personeelsbeoordelingen en heeft dat dan consequenties voor het betreffende personeelslid in carrière of beloning? ❒ ❒ ❒ ❒

## 7 Fysieke beveiliging en beveiliging van de omgeving

### 7.1.1 Fysieke beveiliging van de omgeving

1 Is de parkeerruimte op afstand van het gebouw gesitueerd? ❒ ❒ ❒ ❒

2 Zijn voorzieningen aangebracht waardoor slechts bevoegd gebruik mag worden gemaakt van de parkeerplaats? ❒ ❒ ❒ ❒

3 Wordt de parkeerruimte bewaakt door middel van tv-camera's? ❒ ❒ ❒ ❒

4 Zijn de fysiek te beveiligen ruimtes in het gebouw duidelijk gedefinieerd? ❒ ❒ ❒ ❒

5 Is de omvang van het beveiligde gebied in overeenstemming met de waarde van de bedrijfsmiddelen of de diensten die moeten worden beveiligd? ❒ ❒ ❒ ❒



Zo beantwoorden: ☑

**J**a
**N**ee
**G**edeeltelijk
**O**nbekend

| | | J | N | G | O |
|---|---|---|---|---|---|
| 6 | Worden in het gebouw verschillende zones onderscheiden, zoals: | | | | |
| | • publieksruimten, kantine; | ❒ | ❒ | ❒ | ❒ |
| | • algemene kantoorruimten; | ❒ | ❒ | ❒ | ❒ |
| | • ruimte voor verwerking van in- en uitvoer; | ❒ | ❒ | ❒ | ❒ |
| | • netwerkruimten, telefooncentrale; | ❒ | ❒ | ❒ | ❒ |
| | • technische ruimte voor energievoorziening; | ❒ | ❒ | ❒ | ❒ |
| | • centrale computerruimte; | ❒ | ❒ | ❒ | ❒ |
| | • kluisruimten? | ❒ | ❒ | ❒ | ❒ |
| 7 | Zijn er in het gebouw barrières aangebracht waardoor slechts bevoegden toegang krijgen tot zones waar zij uit hoofde van hun werkzaamheden mogen zijn? | ❒ | ❒ | ❒ | ❒ |
| 8 | Zijn de zones doelmatig van elkaar gescheiden? | ❒ | ❒ | ❒ | ❒ |
| 9 | Is het aantal verbindingen tussen die zones beperkt? | ❒ | ❒ | ❒ | ❒ |
| 10 | Wordt steeds gecontroleerd of de verbindingen tussen de zones beveiligd blijven? | ❒ | ❒ | ❒ | ❒ |
| 11 | Zijn de fysieke barrières van de vloer tot het plafond aangebracht om te voorkomen dat niet-bevoegden een gebied betreden of om verontreiniging vanuit aangrenzende ruimten tegen te gaan? | ❒ | ❒ | ❒ | ❒ |
| 12 | Kunnen maatregelen worden genomen waardoor ander personeel niet onnodig op de hoogte wordt gebracht van de activiteiten in het beveiligd gebied? | ❒ | ❒ | ❒ | ❒ |
| 13 | Is voor beveiliging van beveiligde ruimten gebruik gemaakt van voldoende deugdelijk hang- en sluitwerk? | ❒ | ❒ | ❒ | ❒ |
| 14 | Worden de beveiligde ruimten afgesloten, wanneer daarin geen werkzaamheden meer behoeven te worden verricht (denk aan kabelschachten)? | ❒ | ❒ | ❒ | ❒ |
| 15 | Zijn er maatregelen getroffen rond het beheer van sleutels, ook in het geval van een calamiteit? | ❒ | ❒ | ❒ | ❒ |
| 16 | Indien er gebruik wordt gemaakt van sleutels, die slechts door de leverancier worden bijgemaakt na het overleggen van een certificaat, is dan het beheer van de certificaten geregeld? | ❒ | ❒ | ❒ | ❒ |
| 17 | Wordt de technische staat van het hang- en sluitwerk regelmatig gecontroleerd? | ❒ | ❒ | ❒ | ❒ |
| 18 | Bevinden zich geen apparaten (kopieermachines, printers, faxapparatuur) in beveiligde gebieden, zodat niet geautoriseerde personen zo min mogelijk in dat gebied komen en gevoelige informatie zo min mogelijk in gevaar wordt gebracht? | ❒ | ❒ | ❒ | ❒ |
| 19 | Vindt ter voorkoming van brandgevaar de verwerking van papieren output buiten de computerruimte plaats? | ❒ | ❒ | ❒ | ❒ |
| 20 | Indien computer- of netwerkapparatuur door een externe onderneming wordt beheerd, is deze dan niet in dezelfde ruimte geplaatst als de eigen apparatuur? | ❒ | ❒ | ❒ | ❒ |
| 21 | Is het bij zeer gevoelige bedrijfsprocessen verboden dat iemand zonder toezicht in het beveiligde gebied werkzaamheden verricht? | ❒ | ❒ | ❒ | ❒ |
| 22 | Krijgt onderhouds- en schoonmaakpersoneel slechts toegang tot de beveiligde gebieden onder begeleiding, waarbij vooraf toestemming is verleend? | ❒ | ❒ | ❒ | ❒ |

### 7.1.2 Fysieke toegangsbeveiliging

| | | | | | |
|---|---|---|---|---|---|
| 1 | Is er bij de ingang een voorziening gebouwd die bezoekers verhindert om zonder meer door te lopen? | ❒ | ❒ | ❒ | ❒ |
| 2 | Zijn er regels gesteld voor het personeel onder welke voorwaarden bezoekers mogen worden toegelaten? | ❒ | ❒ | ❒ | ❒ |
| 3 | Vraagt men aan bezoekers om zich te legitimeren? | ❒ | ❒ | ❒ | ❒ |



Zo beantwoorden: ☑

**J**a
**N**ee
**G**edeeltelijk
**O**nbekend

| | | J | N | G | O |
|---|---|---|---|---|---|
| 4 | Wordt aan onderhoudspersoneel en de adviseurs van leveranciers van apparatuur, programmatuur en dergelijke gevraagd om een bedrijfslegitimatie te overleggen om vast te stellen of zij daar nog steeds in dienst zijn? | ❒ | ❒ | ❒ | ❒ |
| 5 | Worden bij bedrijfsrondleidingen niet de beveiligde zones getoond? | ❒ | ❒ | ❒ | ❒ |
| 6 | Zijn de medewerkers in de beveiligde zones verplicht om een zichtbare identificatie te dragen? | ❒ | ❒ | ❒ | ❒ |
| 7 | Worden die medewerkers aangemoedigd om onbekende personen aan te houden? | ❒ | ❒ | ❒ | ❒ |
| 8 | Wordt naleving van de beveiligingsprocedures steeds gecontroleerd en gerapporteerd aan het management? | ❒ | ❒ | ❒ | ❒ |
| 9 | Wordt aan medewerkers, aan wie ontslag is aangezegd en van wie geen verdere samenwerking verwacht kan worden, met onmiddellijke ingang de toegang tot de beveiligde zones ontzegd? | ❒ | ❒ | ❒ | ❒ |
| 10 | Indien het dienstverband met medewerkers is beëindigd, wordt dan toegezien op inlevering van sleutels, tokens en op het wijzigen van toegekende veiligheidscodes? | ❒ | ❒ | ❒ | ❒ |
| 11 | Wordt voor de toegangscontrole gebruik gemaakt van speciaal daarmee belaste beveiligingsmedewerkers? | ❒ | ❒ | ❒ | ❒ |
| 12 | Hebben deze medewerkers een diploma behaald aan één van de erkende opleidingen? | ❒ | ❒ | ❒ | ❒ |
| 13 | Bestaan er schriftelijke instructies voor de medewerkers? | ❒ | ❒ | ❒ | ❒ |
| 14 | Worden bezoekers bij binnenkomst en bij vertrek geregistreerd met vermelding van naam, firma, gastheer en bezoektijden? | ❒ | ❒ | ❒ | ❒ |
| 15 | Wordt dagelijks aan het einde van de dag gecontroleerd of alle binnengekomen bezoekers het pand hebben verlaten? | ❒ | ❒ | ❒ | ❒ |
| 16 | Hebben de beveiligingsmedewerkers instructies om personeel te verwijderen dat zich in zones bevindt waarvoor het niet is geautoriseerd? | ❒ | ❒ | ❒ | ❒ |
| 17 | Leggen de beveiligingsmedewerkers bijzonderheden vast in een beveiligingsrapport? | ❒ | ❒ | ❒ | ❒ |
| 18 | Bestaat toezicht op de beveiligingsmedewerkers en worden de in de rapportage vermelde gegevens onderzocht? | ❒ | ❒ | ❒ | ❒ |
| 19 | Is de ruimte met bewakingsapparatuur beschermd met een kogelvrije glaswand? | ❒ | ❒ | ❒ | ❒ |
| 20 | Zijn de kogelwerende constructies consequent uitgevoerd, dus ook boven de verlaagde plafonds? | ❒ | ❒ | ❒ | ❒ |
| 21 | Is direct contact onmogelijk met beveiligingspersoneel in de bewakings- en controleruimte? | ❒ | ❒ | ❒ | ❒ |
| 22 | Indien gebruik gemaakt van de diensten van een externe beveiligingsdienst, wordt dan een geheimhoudingsverklaring gevraagd? | ❒ | ❒ | ❒ | ❒ |
| 23 | Wordt gecontroleerd of die beveiligingsdienst in het bezit is van de vereiste vergunningen? | ❒ | ❒ | ❒ | ❒ |
| 24 | Is door een onafhankelijke instantie een certificaat verleend voor de te installeren technische voorzieningen voor toegangscontrole? | ❒ | ❒ | ❒ | ❒ |
| 25 | Wordt direct na het installeren van de technische voorzieningen getest of deze voldoen aan de vooraf opgesteld specificaties? | ❒ | ❒ | ❒ | ❒ |
| 26 | Is een onderhoudscontract afgesloten? | ❒ | ❒ | ❒ | ❒ |
| 27 | Zijn technische voorzieningen aangebracht waarmee misbruik van zones wordt gesignaleerd? | ❒ | ❒ | ❒ | ❒ |
| 28 | Worden bij een calamiteit (brandalarm, wateroverlast of stroomuitval) de deurvergrendelingen tussen de beveiligde ruimten opgeheven? | ❒ | ❒ | ❒ | ❒ |
| 29 | Kunnen alle deurvergrendelingen centraal vanuit de controle- en bewakingsruimte worden bediend? | ❒ | ❒ | ❒ | ❒ |
| 30 | Wordt de werking van de beveiligingsinstallatie regelmatig getest? | ❒ | ❒ | ❒ | ❒ |
| 31 | Zijn er voorzieningen ter vermijding van vals inbraakalarm? | ❒ | ❒ | ❒ | ❒ |
| 32 | Wordt de signalering van illegale toegang gemeld bij een eventuele centrale meldingspost? | ❒ | ❒ | ❒ | ❒ |



Zo beantwoorden: ☑

**J**a
**N**ee
**G**edeeltelijk
**O**nbekend

| | | J | N | G | O |
|---|---|---|---|---|---|
| 33 | Indien deze meldingspost niet bemand is, wordt dat signaal dan extern doorgeleid naar een aantal sleutelhouders? | ❒ | ❒ | ❒ | ❒ |
| 34 | Zijn richtlijnen verstrekt voor de aanwezigheid van sleutelhouders? | ❒ | ❒ | ❒ | ❒ |
| 35 | Vindt in bepaalde gevallen automatische doormelding van illegale betreding naar de beveiligingsdienst en/of politie plaats en zijn hierover afspraken gemaakt met de beveiligingsdienst en de politie? | ❒ | ❒ | ❒ | ❒ |
| 36 | Kan de situering van de melding van een illegale betreding worden waargenomen op een meldingstableau? | ❒ | ❒ | ❒ | ❒ |
| 37 | Worden door het systeem de bewegingen van de medewerkers vastgelegd? | ❒ | ❒ | ❒ | ❒ |
| 38 | Worden eventuele overtredingen (bijvoorbeeld het langdurig open laten staan van een deur naar een beveiligde zone) met behulp van die registratie opgespoord? | ❒ | ❒ | ❒ | ❒ |
| 39 | Is aan de medewerkers meegedeeld dat gegevens van hun bewegingen worden vastgelegd? | ❒ | ❒ | ❒ | ❒ |
| 40 | Zijn richtlijnen aanwezig voor het onderkennen en afhandelen van die overtredingen (inclusief het veiligstellen van de registratie als bewijsmateriaal)? | ❒ | ❒ | ❒ | ❒ |
| 41 | Wanneer de apparatuur voor toegangsbeveiliging het karakter heeft van een personeelsvolgsysteem (kenmerk waarvan is dat beoordeling van het personeel plaats vindt op grond van die registratie), is er dan overleg geweest binnen de ondernemingsraad? | ❒ | ❒ | ❒ | ❒ |
| 42 | Wordt de toegang tot de zones met behulp van tv-camera's bewaakt? | ❒ | ❒ | ❒ | ❒ |
| 43 | Welke keuze is gemaakt bij de plaatsing van de camera: zichtbaar met het accent op preventie of onzichtbaar met een repressief accent? | ❒ | ❒ | ❒ | ❒ |
| 44 | Is een onderhoudscontract afgesloten? | ❒ | ❒ | ❒ | ❒ |
| 45 | Hangen de camera's op een zodanige plaats dat niet-geautoriseerde personen achteraf goed kunnen worden herkend? | ❒ | ❒ | ❒ | ❒ |
| 46 | Is de camera op ooghoogte geplaatst? | ❒ | ❒ | ❒ | ❒ |
| 47 | Is rekening gehouden met tegenlicht en met de slechtste en de beste lichtsituatie? | ❒ | ❒ | ❒ | ❒ |
| 48 | Is de video-apparatuur opgesteld in een beveiligde ruimte? | ❒ | ❒ | ❒ | ❒ |
| 49 | Zijn er richtlijnen vastgesteld voor het bewaren van gemaakte video-opnamen (duur opslag, registratie media)? | ❒ | ❒ | ❒ | ❒ |
| 50 | Worden de gemaakte opnamen veilig bewaard? | ❒ | ❒ | ❒ | ❒ |
| 51 | Bezitten de opnameapparatuur en de media voldoende capaciteit om de gewenste beveiligingstijden te bestrijken? | ❒ | ❒ | ❒ | ❒ |
| 52 | Vindt regelmatig onderhoud plaats aan de camera's en de opnameapparatuur? | ❒ | ❒ | ❒ | ❒ |
| 53 | Wordt een dagelijkse test uitgevoerd? | ❒ | ❒ | ❒ | ❒ |
| 54 | Wordt het camerabeeld dagelijks op de monitor gecontroleerd? | ❒ | ❒ | ❒ | ❒ |
| 55 | Worden de juiste media gebruikt en worden deze steeds tijdig gewisseld? | ❒ | ❒ | ❒ | ❒ |
| 56 | Zijn richtlijnen aanwezig voor de behandeling van beeldmateriaal nadat een overtreding is geconstateerd? | ❒ | ❒ | ❒ | ❒ |
| 57 | Kan het beeldmateriaal worden afgedrukt op papier? | ❒ | ❒ | ❒ | ❒ |
| 58 | Wordt gebruik gemaakt van tokens, waarmee de toegang tot de zones wordt geregistreerd? | ❒ | ❒ | ❒ | ❒ |
| 59 | Worden de tokens gepersonaliseerd per medewerker? | ❒ | ❒ | ❒ | ❒ |
| 60 | Wordt de aanvraag tot verstrekking van een token pas in behandeling genomen, nadat de bevoegdheid van de aanvrager is gecontroleerd? | ❒ | ❒ | ❒ | ❒ |
| 61 | Is het beheer van de voorraad van niet gepersonaliseerde tokens geregeld? | ❒ | ❒ | ❒ | ❒ |
| 62 | Worden gepersonaliseerde tokens aan de medewerkers uitgereikt nadat de identiteit daarvan is vastgesteld? | ❒ | ❒ | ❒ | ❒ |



Zo beantwoorden: ☑

**J**a
**N**ee
**G**edeeltelijk
**O**nbekend

| | | J | N | G | O |
|---|---|---|---|---|---|
| 63 | Tekent die medewerker voor ontvangst van zijn persoonlijke token? | ❒ | ❒ | ❒ | ❒ |
| 64 | Bestaan er schriftelijke instructies voor het gebruik van het token (alleen persoonlijk gebruik, onmiddellijke melding van verlies of diefstal) door de medewerkers? | ❒ | ❒ | ❒ | ❒ |
| 65 | Worden die instructies bij herhaling aan de medewerkers duidelijk gemaakt? | ❒ | ❒ | ❒ | ❒ |
| 66 | Worden de tokens bij vertrek of ontslag onmiddellijk ingeleverd, dan wel wordt de toegangsmogelijkheid ingetrokken? | ❒ | ❒ | ❒ | ❒ |
| 67 | Wordt regelmatig gecontroleerd of medewerkers met wie het dienstverband is beëindigd ook inderdaad uit het systeem zijn verwijderd? | ❒ | ❒ | ❒ | ❒ |
| 68 | Wordt dan ook gecontroleerd of aan personen met een token de juiste autorisaties zijn verstrekt? | ❒ | ❒ | ❒ | ❒ |
| 69 | Wordt de toegang en vertrek met behulp van het token geregistreerd? | ❒ | ❒ | ❒ | ❒ |
| 70 | Is deze registratie vooraf bekend gemaakt aan de medewerkers (personeelsvolgsysteem)? | ❒ | ❒ | ❒ | ❒ |
| 71 | Heeft de beveiligingsmedewerker instructies voor het geval dat een onbekend token wordt aangeboden? | ❒ | ❒ | ❒ | ❒ |

**7.1.3 Beveiliging van kantoren, ruimten en voorzieningen**

| | | | | | |
|---|---|---|---|---|---|
| 1 | Zijn de belangrijkste voorzieningen niet geplaatst in gebieden die publiek toegankelijk zijn of waar openbare voertuigen komen? | ❒ | ❒ | ❒ | ❒ |
| 2 | Is voor ruimten voor computer- of netwerkactiviteiten zo weinig mogelijk aangegeven wat binnen gebeurt en zijn geen duidelijke tekenen zichtbaar die kunnen duiden op die activiteiten? | ❒ | ❒ | ❒ | ❒ |
| 3 | Zijn op verwijsborden of telefoongidsen van de onderneming geen nummers vermeld van lokaties met computervoorzieningen? | ❒ | ❒ | ❒ | ❒ |
| 4 | Worden gevaarlijke en brandbare materialen op veilige afstand van de computervoorzieningen opgeslagen? | ❒ | ❒ | ❒ | ❒ |
| 5 | Worden computertoebehoren zoals papier pas op het moment dat zij nodig zijn in de computerruimten geplaatst? | ❒ | ❒ | ❒ | ❒ |
| 6 | Wordt reserveapparatuur op veilige afstand bewaard? | ❒ | ❒ | ❒ | ❒ |
| 7 | Worden media met reservekopieën op veilige afstand bewaard? | ❒ | ❒ | ❒ | ❒ |
| 8 | Zijn de noodprocedures volledig gedocumenteerd? | ❒ | ❒ | ❒ | ❒ |
| 9 | Worden de noodprocedures regelmatig getest? | ❒ | ❒ | ❒ | ❒ |
| 10 | Worden de ruimten afgesloten als er geen medewerkers meer aanwezig zijn? | ❒ | ❒ | ❒ | ❒ |
| 11 | Is aan de buitenkant van de ramen en de deuren extra bescherming aangebracht? | ❒ | ❒ | ❒ | ❒ |
| 12 | Is een bliksemafleidingsinstallatie (noodzakelijkheid afhankelijk van vorm, constructie en plaats van het gebouw) aanwezig? | ❒ | ❒ | ❒ | ❒ |
| 13 | Voldoen de bij de bouw en inrichting van een computercentrum toegepaste materialen en constructies aan daaraan te stellen eisen inzake brandvoortplanting en rookontwikkeling (brandgedrag)? | ❒ | ❒ | ❒ | ❒ |
| 14 | Voldoen de brandwerende scheidingen in hun geheel aan deze eisen met inbegrip van aansluitingen, doorvoeringen en dergelijke? | ❒ | ❒ | ❒ | ❒ |
| 15 | Is aandacht besteed aan materiaal en doorvoer van luchtkanalen, elektriciteits- en andere leidingen, afsluiting van openingen enzovoorts? | ❒ | ❒ | ❒ | ❒ |
| 16 | Is in het interieur geen gemakkelijk ontvlambare stoffering gebruikt of daarmee gestoffeerd meubilair geplaatst? | ❒ | ❒ | ❒ | ❒ |
| 17 | Geven de gebruikte materialen alsmede de overige in het pand aanwezige goederen bij verhitting geen corroderende en/of giftige gassen af? | ❒ | ❒ | ❒ | ❒ |



Zo beantwoorden: ☑

**J**a
**N**ee
**G**edeeltelijk
**O**nbekend

| | | J | N | G | O |
|---|---|---|---|---|---|
| 18 | Zijn ruimten waarin elektrische apparatuur is geplaatst, op de deuren voorzien van het pictogram: zwart met gele diagonale strepen (dit betekent: niet blussen met water)? | ❒ | ❒ | ❒ | ❒ |
| 19 | Is signalering aangebracht voor nood- en vluchtwegen? | ❒ | ❒ | ❒ | ❒ |
| 20 | Wanneer het computercentrum zodanig is gesitueerd dat het zich beneden de stand van het grondwater of omringende oppervlaktewater bevindt, zijn dan voorzieningen getroffen om het binnendringen van water bij hoge waterstanden te voorkomen? | ❒ | ❒ | ❒ | ❒ |
| 21 | Zijn in de computerruimte geen leidingen aanwezig voor de afvoer van hemelwater, de afvoer van vuil water en de aanvoer van koud en warm water? | ❒ | ❒ | ❒ | ❒ |
| 22 | Komen deze leidingen ook niet voor in begrenzende wanden, vloer en plafond? | ❒ | ❒ | ❒ | ❒ |
| 23 | Is er in de vloer van de computerruimte een afvoer of pompput met voldoende capaciteit aangebracht waardoor eventueel blus- of lekwater kan wegvloeien? | ❒ | ❒ | ❒ | ❒ |
| 24 | Zijn er zodanige inbraakwerende voorzieningen aangebracht, dat onbevoegden niet binnen de reactietijd het gebouw hebben kunnen betreden? | ❒ | ❒ | ❒ | ❒ |
| 25 | Is afdoende signalering aanwezig in de computerruimte of andere ruimten met hoge brandveiligheidseisen en worden deze voorzieningen periodiek getest? | ❒ | ❒ | ❒ | ❒ |
| 26 | Reageren de melders, afhankelijk van de ter plaatse te stellen eisen op rook, dan wel temperatuur? | ❒ | ❒ | ❒ | ❒ |
| 27 | Zijn melders op diverse plaatsen in de computerruimte aangebracht in de nabijheid van de computers, onder de verhoogde vloer en boven het verlaagde plafond? | ❒ | ❒ | ❒ | ❒ |
| 28 | Zijn voorts geschikte melders aanwezig in elektrakasten, in netwerk- of telefoonruimten, in of nabij aanzuigopeningen van de luchtafvoerkanalen, in het inlaatkanaal voor de inlaat van verse lucht en in aan de computerruimte grenzende ruimten? | ❒ | ❒ | ❒ | ❒ |
| 29 | Zijn er ook signaleringen aanwezig in omliggende en andere belangrijke ruimten (kluizen, magazijnen en dergelijke)? | ❒ | ❒ | ❒ | ❒ |
| | Zo ja, schakelt deze melding ook de airconditioning van de computerruimte uit? | ❒ | ❒ | ❒ | ❒ |
| 30 | Indien er een automatische blusinstallatie aanwezig is, zijn er dan voorzieningen om onnodige blussing tegen te gaan (bijvoorbeeld door de melder op te nemen in verschillende lussen)? | ❒ | ❒ | ❒ | ❒ |
| 31 | Zijn er voorzieningen ter vermijding van vals alarm? | ❒ | ❒ | ❒ | ❒ |
| 32 | Wordt de signalering gemeld bij een eventuele centrale meldpost? | ❒ | ❒ | ❒ | ❒ |
| 33 | Indien deze meldpost niet bemand is, wordt het signaal dan extern doorgeleid naar een aantal sleutelhouders? | ❒ | ❒ | ❒ | ❒ |
| 34 | Zijn richtlijnen verstrekt voor de aanwezigheid van sleutelhouders? | ❒ | ❒ | ❒ | ❒ |
| 35 | Vindt in bepaalde gevallen automatische doormelding naar de brandweer plaats en zijn hierover afspraken gemaakt met de brandweer? | ❒ | ❒ | ❒ | ❒ |
| 36 | Kan de situering van de brandmelding worden waargenomen op een meldingstableau? | ❒ | ❒ | ❒ | ❒ |
| 37 | Als het computercentrum een ruimte is binnen een complex, is dan buiten het computercentrum bekend welke procedure in geval van een melding gevolgd moet worden? | ❒ | ❒ | ❒ | ❒ |
| 38 | Werkt de signalerings- en meldingsapparatuur bij het uitvallen van de elektrische spanning op een alternatieve voeding (bijvoorbeeld een accu)? | ❒ | ❒ | ❒ | ❒ |
| 39 | Is het (additioneel) plaatsen en gebruik van handmelders overwogen? Met welk resultaat? | ❒ | ❒ | ❒ | ❒ |
| 40 | Is het juiste soort handblussers aanwezig in de daarvoor in aanmerking komende ruimten (in de computerruimte en ruimten met fijne technische apparatuur is blusgas vereist)? | ❒ | ❒ | ❒ | ❒ |
| 41 | Is de computerruimte voorzien van een (automatische) blusgasinstallatie? Is deze op drie niveaus geïnstalleerd: in de computerruimte, onder de verhoogde vloer en boven het verlaagde plafond? | ❒ | ❒ | ❒ | ❒ |



Zo beantwoorden: ☑

**J**a
**N**ee
**G**edeeltelijk
**O**nbekend

| | | J | N | G | O |
|---|---|---|---|---|---|
| 42 | Zijn overige vitale ruimten eveneens voorzien van een blusgasinstallatie (bijvoorbeeld tapekluis en netwerkruimten)? | ❒ | ❒ | ❒ | ❒ |
| 43 | Is er een goede afzuigmogelijkheid na eventuele blussing met blusgas? | ❒ | ❒ | ❒ | ❒ |
| 44 | Voldoet het blusgas aan de juiste specificaties, die door de overheid zijn gesteld (bijvoorbeeld: voldoende bescherming van de medewerkers, zo weinig mogelijke belasting van het milieu)? | ❒ | ❒ | ❒ | ❒ |
| 45 | Zijn er instructies die aangeven hoe te handelen in geval van brandmelding? | ❒ | ❒ | ❒ | ❒ |
| 46 | Is in deze instructies aandacht besteed aan de volgende onderwerpen: | | | | |
| | • wijze van alarmering (eerst alarmeren, dan blussen); | ❒ | ❒ | ❒ | ❒ |
| | • gebruik van handblussers; | ❒ | ❒ | ❒ | ❒ |
| | • uitschakelen van computerapparatuur; | ❒ | ❒ | ❒ | ❒ |
| | • regelen van de airconditioning-apparatuur tijdens de brand en gedurende de periode daarna; | ❒ | ❒ | ❒ | ❒ |
| | • ontruiming en plaats van samenkomst; | ❒ | ❒ | ❒ | ❒ |
| | • redden van in gebruik zijnde informatiedragers; | ❒ | ❒ | ❒ | ❒ |
| | • gedrag bij in werking zijn van de automatische blusinstallatie? | ❒ | ❒ | ❒ | ❒ |
| 47 | Vindt regelmatig oefening van de instructies plaats? | ❒ | ❒ | ❒ | ❒ |
| 48 | Wordt een verslag opgemaakt van die oefening met eventuele aanbevelingen ten behoeve van het management? | ❒ | ❒ | ❒ | ❒ |
| 49 | Worden de voorraden van de (licht) ontvlambare (vloei)stoffen die in het computercentrum noodzakelijk aanwezig zijn zo laag mogelijk gehouden? | ❒ | ❒ | ❒ | ❒ |
| 50 | Zijn deze (vloei)stoffen opgeborgen in brandveilige kasten? | ❒ | ❒ | ❒ | ❒ |
| 51 | Zijn de overige voorraden op de computerruimte beperkt tot bijvoorbeeld één dag productie? | ❒ | ❒ | ❒ | ❒ |
| 52 | Geldt een rookverbod voor de computerruimte en voor andere ruimten waaraan hoge brandveiligheidseisen zijn gesteld? | ❒ | ❒ | ❒ | ❒ |
| 53 | Zijn in de ruimten waar geen rookverbod geldt, maatregelen genomen om het brandgevaar te beperken (bijvoorbeeld asbakken waar een sigaret niet brandend af kan vallen; metalen, zelfsluitende prullenbakken en dergelijke)? | ❒ | ❒ | ❒ | ❒ |
| 54 | Zijn buiten het gebouw ten behoeve van de brandweer blusaansluitingen aanwezig? | ❒ | ❒ | ❒ | ❒ |
| 55 | Zijn voorzieningen en gebruik van vluchtwegen met de brandweer doorgesproken? | ❒ | ❒ | ❒ | ❒ |
| | Is hierbij aandacht besteed aan de toegangsbeveiliging, ook tijdens brand (waarbij soms sprake kan zijn van tegenstrijdige belangen)? | ❒ | ❒ | ❒ | ❒ |
| 56 | Beschikt de brandweer over een zogeheten aanvalsplan? | ❒ | ❒ | ❒ | ❒ |
| 57 | Is er een contactpersoon aangewezen voor het onderhouden van contacten met de brandweer? | ❒ | ❒ | ❒ | ❒ |
| 58 | Zijn in de datakluis voorzieningen aanwezig tegen condensvorming en tegen het binnendringen van (blus)water en stoom (een datakluis dient zodanig brandwerend geconstrueerd te zijn dat hij beveiligd is tegen temperaturen boven 65°c en een relatieve vochtigheid van maximaal tachtig procent garandeert)? | ❒ | ❒ | ❒ | ❒ |
| 59 | Wanneer er toch waterleidingen door het computercentrum lopen, bijvoorbeeld ten behoeve van koeling, zijn er dan onder de verhoogde vloer van de computerruimte vochtdetectoren aangebracht waarmee eventuele lekkage wordt geconstateerd en worden deze detectoren periodiek getest? | ❒ | ❒ | ❒ | ❒ |
| 60 | Vindt signalering van de vochtdetectoren plaats naar een eventuele centrale meldingspost? | ❒ | ❒ | ❒ | ❒ |
| 61 | Indien deze meldingspost niet bemand is, wordt het signaal dan extern doorgeleid naar een aantal sleutelhouders? | ❒ | ❒ | ❒ | ❒ |
| 62 | Zijn er watermelders geplaatst? | ❒ | ❒ | ❒ | ❒ |



Zo beantwoorden: ☑

**J**a
**N**ee
**G**edeeltelijk
**O**nbekend

| | | J | N | G | O |
|---|---|---|---|---|---|
| 63 | Is bij waterleidingbreuk of een defect aan de koelinstallaties bekend hoe en waar de leiding moet worden afgesloten? | ❒ | ❒ | ❒ | ❒ |
| 64 | Is er apparatuur geïnstalleerd die de juiste omgevingscondities waarborgt? | ❒ | ❒ | ❒ | ❒ |
| 65 | Is bekend wat de optimale omgevingscondities voor de geïnstalleerde (computer)apparatuur zijn? | ❒ | ❒ | ❒ | ❒ |
| 66 | Wordt de goede werking van de klimaatbeheersingsapparatuur periodiek gecontroleerd? | ❒ | ❒ | ❒ | ❒ |
| 67 | Is er een onderhoudscontract afgesloten met betrekking tot de klimaatbeheersingsapparatuur? | ❒ | ❒ | ❒ | ❒ |

**7.1.4 Werken in beveiligde ruimten**

| | | | | | |
|---|---|---|---|---|---|
| 1 | Gelden de extra maatregelen voor het werken in beveiligde zones voor zowel eigen personeel, als personeel dat is ingehuurd van derden? | ❒ | ❒ | ❒ | ❒ |
| 2 | Weet alleen personeel dat er moet werken af van het bestaan van de beveiligde zones of de werkzaamheden, die daarin worden verricht? | ❒ | ❒ | ❒ | ❒ |
| 3 | Wordt in die zones alleen onder toezicht gewerkt om veiligheidsredenen en om ongewenste activiteiten te voorkomen? | ❒ | ❒ | ❒ | ❒ |
| 4 | Worden lege beveiligde zones afgesloten en periodiek geïnspecteerd? | ❒ | ❒ | ❒ | ❒ |
| 5 | Krijgt het personeel van externe leveranciers slechts in het uiterste geval toestemming om de beveiligde zones te betreden? | ❒ | ❒ | ❒ | ❒ |
| 6 | Houdt men nauwlettend toezicht op dat personeel? | ❒ | ❒ | ❒ | ❒ |
| 7 | Wordt gebruik gemaakt van deuren of sluizen om fysieke toegang te beperken tot beveiligde zones met verschillende beveiligingseisen? | ❒ | ❒ | ❒ | ❒ |
| 8 | Mag slechts met uitdrukkelijke toestemming worden gefilmd, gefotografeerd of een bandopname worden gemaakt? | ❒ | ❒ | ❒ | ❒ |

**7.1.5 Afgescheiden ruimten voor laden en lossen van goederen**

| | | | | | |
|---|---|---|---|---|---|
| 1 | Heeft alleen personeel met geldige identificatie en autorisatie toegang tot deze ruimten? | ❒ | ❒ | ❒ | ❒ |
| 2 | Is de ruimte zodanig ontworpen dat voorraden binnengebracht kunnen worden zonder dat andere delen van het gebouw kunnen worden betreden? | ❒ | ❒ | ❒ | ❒ |
| 3 | Wordt de buitendeur afgesloten wanneer de binnendeur wordt geopend? | ❒ | ❒ | ❒ | ❒ |
| 4 | Worden de binnenkomende materialen eerst gecontroleerd op mogelijke gevaren, voordat zij worden getransporteerd naar de lokatie voor opslag of verwerking? | ❒ | ❒ | ❒ | ❒ |

**7.2.1 Het plaatsen en beveiligen van apparatuur**

| | | | | | |
|---|---|---|---|---|---|
| 1 | Is de apparatuur in de computerruimte zodanig opgesteld dat er zo weinig mogelijk over de werkvloer behoeft te worden gelopen? | ❒ | ❒ | ❒ | ❒ |
| 2 | Zijn werkstations met gevoelige gegevens zodanig opgesteld dat onbevoegden het scherm niet kunnen aflezen? | ❒ | ❒ | ❒ | ❒ |
| 3 | Is de apparatuur die geclassificeerde gegevens verwerkt zodanig opgesteld (bijvoorbeeld in een afgesloten kabinet) dat de beveiliging van de ruimte niet extra behoeft te worden versterkt? | ❒ | ❒ | ❒ | ❒ |
| 4 | Is de apparatuur beveiligd tegen brand of tegen oververhitting (bijvoorbeeld door middel van koelsystemen)? | ❒ | ❒ | ❒ | ❒ |
| 5 | Is de apparatuur beveiligd tegen rook, bijvoorbeeld door deze in een afgesloten kast op te stellen? | ❒ | ❒ | ❒ | ❒ |
| 6 | Indien de ruimte met een sprinklerinstallatie wordt beschermd, is dan een zeiltje aanwezig om de apparatuur af te dekken? | ❒ | ❒ | ❒ | ❒ |



Zo beantwoorden: ☑

**J**a
**N**ee
**G**edeeltelijk
**O**nbekend

| | | J | N | G | O |
|---|---|---|---|---|---|
| 7 | Is de apparatuur beschermd tegen trillingen door schokken van zwaar verkeer of door lichte aardbevingen? | ❒ | ❒ | ❒ | ❒ |
| 8 | Wordt de apparatuur zoveel mogelijk beschermd tegen de invloed van chemische reacties, bijvoorbeeld door stoffen uit de omgeving? | ❒ | ❒ | ❒ | ❒ |
| 9 | Is de apparatuur beveiligd tegen interferentie van de stroomvoorziening via de elektrische installatie? | ❒ | ❒ | ❒ | ❒ |
| 10 | Beschermt een speciale constructie de computerruimte tegen elektromagnetische straling uit de omgeving? | ❒ | ❒ | ❒ | ❒ |
| 11 | Zijn printers apart geplaatst van de overige apparatuur, waardoor wordt voorkomen dat gemorste toner tot gegevensverlies leidt? | ❒ | ❒ | ❒ | ❒ |
| 12 | Is de printer zodanig opgesteld dat onbevoegden geen uitvoer kunnen meenemen? | ❒ | ❒ | ❒ | ❒ |
| 13 | Geldt er een rookverbod en een verbod om te eten en te drinken in de nabijheid van de apparatuur? | ❒ | ❒ | ❒ | ❒ |
| 14 | Indien de apparatuur is geplaatst in een industriële omgeving, zijn er dan extra beschermende maatregelen genomen (bijvoorbeeld een hoes voor een toetsenbord)? | ❒ | ❒ | ❒ | ❒ |
| 15 | Is de apparatuur tegen diefstal beveiligd (bijvoorbeeld door het aanbrengen van een kenmerk aan de buitenkant, het met een slot verankeren aan de omgeving)? | ❒ | ❒ | ❒ | ❒ |
| 16 | Is er een configuratieschema aanwezig van de geplaatste apparatuur? | ❒ | ❒ | ❒ | ❒ |
| 17 | Wordt er een administratie bijgehouden van de activa (apparatuur en daarop eventueel geplaatste programmatuur) waaruit blijkt welke apparatuur waar aanwezig moet zijn om eventuele diefstal te kunnen vaststellen? | ❒ | ❒ | ❒ | ❒ |
| 18 | Zijn voorschriften verstrekt en bekend gemaakt voor het verplaatsen van apparatuur? | ❒ | ❒ | ❒ | ❒ |
| 19 | Zijn die activa verzekerd tegen verlies, diefstal of brand? | ❒ | ❒ | ❒ | ❒ |
| 20 | Inventariseert men periodiek die activa om de verzekerde waarde vast te stellen? | ❒ | ❒ | ❒ | ❒ |

### 7.2.2 Stroomvoorziening

| | | | | | |
|---|---|---|---|---|---|
| 1 | Is de apparatuur beveiligd tegen stroomstoring en andere elektrische storingen, zoals bijvoorbeeld blikseminslag of statische elektriciteit? | ❒ | ❒ | ❒ | ❒ |
| 2 | Is geïnventariseerd wat de gevolgen zijn van een dergelijke stroomstoring voor de meest kritische bedrijfsprocessen en is daarna de maximaal toegestane uitvalsduur bepaald? | ❒ | ❒ | ❒ | ❒ |
| 3 | Wordt de maximaal toegestane uitvalsduur jaarlijks opnieuw bezien? | ❒ | ❒ | ❒ | ❒ |
| 4 | Voldoet de elektrische installatie aan brandveiligheidseisen? | ❒ | ❒ | ❒ | ❒ |
| 5 | Voldoet de stroomvoorziening aan de specificaties van de leverancier van de apparatuur? | ❒ | ❒ | ❒ | ❒ |
| 6 | Worden kabels en groepen niet tot het maximaal belastbare belast? | ❒ | ❒ | ❒ | ❒ |
| 7 | Worden verdeel- en aansluitkasten regelmatig gecontroleerd op losgeraakte contacten, vooral de hoofdaansluitingen? | ❒ | ❒ | ❒ | ❒ |
| 8 | Wanneer is geconstateerd dat de meest kritische processen geen uitvaltijd mogen kennen, is dan een reservevoedingseenheid geplaatst? | ❒ | ❒ | ❒ | ❒ |
| 9 | Kent de reservevoedingseenheid voldoende vermogen om de aan te sluiten apparatuur gedurende een vooraf bepaalde tijdsduur te kunnen bedienen (is er genoeg diesel voor het aggregaat)? | ❒ | ❒ | ❒ | ❒ |
| 10 | Is bekend welke onderdelen van de configuratie (dus ook eventuele componenten voor datacommunicatie) op de reservevoedingseenheid zijn aangesloten? | ❒ | ❒ | ❒ | ❒ |
| 11 | Is een noodprocedure aanwezig voor het geval de reservevoedingseenheid niet meer werkt? | ❒ | ❒ | ❒ | ❒ |
| 12 | Wordt voor de ongestoorde verwerking gebruik gemaakt van een eigen of een van derden gehuurde generator? | ❒ | ❒ | ❒ | ❒ |



Zo beantwoorden: ☑

**J**a
**N**ee
**G**edeeltelijk
**O**nbekend

| | | J | N | G | O |
|---|---|---|---|---|---|
| 13 | Worden de reservevoedingseenheid en de generator regelmatig getest overeenkomstig de voorschriften van de fabrikant? | ❒ | ❒ | ❒ | ❒ |
| | **7.2.3 Beveiliging van kabels** | | | | |
| 1 | Zijn de kabels voor stroomvoorziening en telecommunicatie voldoende beschermd tegen stroomstoring of aftappen? | ❒ | ❒ | ❒ | ❒ |
| 2 | Lopen de netwerkkabels door bijvoorbeeld buizen of kabelgoten, zodat zij niet beklemd of beschadigd kunnen raken? | ❒ | ❒ | ❒ | ❒ |
| 3 | Lopen de netwerkkabels zo weinig mogelijk door ruimten waar publiek aanwezig is? | ❒ | ❒ | ❒ | ❒ |
| 4 | Wordt gebruik gemaakt van encryptie wanneer bijzonder gevoelige of kritieke gegevens over het netwerk worden verzonden? | ❒ | ❒ | ❒ | ❒ |
| 5 | Worden in dat geval ook de kabels in gesloten kabelgoten en in afgesloten ruimten geïnstalleerd? | ❒ | ❒ | ❒ | ❒ |
| 6 | Worden stroomkabels en kabels voor telecommunicatie van elkaar gescheiden gehouden om storingen te voorkomen? | ❒ | ❒ | ❒ | ❒ |
| | **7.2.4 Onderhoud van apparatuur** | | | | |
| 1 | Wordt de apparatuur op de juiste wijze onderhouden? | ❒ | ❒ | ❒ | ❒ |
| 2 | Is er een onderhoudsschema opgesteld, aan de hand waarvan het onderhoud wordt uitgevoerd? | ❒ | ❒ | ❒ | ❒ |
| 3 | Vindt het onderhoud op de door de leverancier aangegeven geregelde tijden plaats? | ❒ | ❒ | ❒ | ❒ |
| 4 | Neemt het onderhoudspersoneel de voorschriften van de leverancier in acht? | ❒ | ❒ | ❒ | ❒ |
| 5 | Mag slechts geautoriseerd onderhoudspersoneel de reparaties en het onderhoud van de apparatuur uitvoeren? | ❒ | ❒ | ❒ | ❒ |
| 6 | Worden ter voorkoming van brandgevaar de papierverwerkende machines regelmatig en grondig gereinigd? | ❒ | ❒ | ❒ | ❒ |
| 7 | Wanneer voor het onderhoud gebruik wordt gemaakt van diensten van derden, zijn er dan afspraken gemaakt over de kennis en kunde van het onderhoudspersoneel en is er een geheimhoudingsverklaring getekend? | ❒ | ❒ | ❒ | ❒ |
| 8 | Legt men alle storingen vast? | ❒ | ❒ | ❒ | ❒ |
| 9 | Wordt het overzicht van de storingen gebruikt om het onderhoudsschema aan te passen, dan wel om apparatuur te vervangen? | ❒ | ❒ | ❒ | ❒ |
| 10 | Sluit men voor de apparatuur, waarvoor de hoogste eisen van ongestoorde verwerking gelden, een onderhoudsabonnement af met de leverancier? | ❒ | ❒ | ❒ | ❒ |
| 11 | Kent het onderhoudsabonnement een clausule waarin is vastgelegd binnen welke termijn de reparatie namens de leverancier moet zijn verricht? | ❒ | ❒ | ❒ | ❒ |
| 12 | Is er een administratie aanwezig van alle onderhoudsabonnementen? | ❒ | ❒ | ❒ | ❒ |
| 13 | Wanneer er sprake is van een onderhoudsabonnement, wordt dan gecontroleerd of bij een storing aan de voorwaarden van tijdige reparatie is voldaan? | ❒ | ❒ | ❒ | ❒ |
| 14 | Wordt toezicht gehouden wanneer personeel van een extern bedrijf onderhoud verricht aan apparatuur waarmee geclassificeerde gegevens worden verwerkt? | ❒ | ❒ | ❒ | ❒ |
| | **7.2.5 Beveiliging van apparatuur buiten de onderneming** | | | | |
| 1 | Zijn de belangrijkste bedreigingen bepaald van het gebruik van apparatuur buiten de onderneming en zijn de gekozen beveiligingsmaatregelen daarop afgestemd? | ❒ | ❒ | ❒ | ❒ |
| 2 | Zijn voorschriften aanwezig voor gebruik van apparatuur buiten de onderneming? | ❒ | ❒ | ❒ | ❒ |
| 3 | Is het personeel op de hoogte van deze voorschriften? | ❒ | ❒ | ❒ | ❒ |



Zo beantwoorden: ☑

**J**a
**N**ee
**G**edeeltelijk
**O**nbekend

| | | J | N | G | O |
|---|---|---|---|---|---|
| 4 | Zijn voorschriften verstrekt voor vervoer van apparatuur en media (bijvoorbeeld: het vervoer melden bij het passeren van de eventuele toegangscontrole, de apparatuur nooit onbeheerd achterlaten, draagbare computers vervoeren als handbagage)? | ❒ | ❒ | ❒ | ❒ |
| 5 | Besteden de voorschriften ook aandacht aan de beveiliging van draagbare computers, zoals wachtwoorden en/of encryptie van de opgeslagen gegevens (kwetsbaar voor diefstal, verlies of ongeautoriseerde raadpleging)? | ❒ | ❒ | ❒ | ❒ |
| 6 | Nemen de medewerkers ook buiten de onderneming de voorschriften van de leverancier in acht, bijvoorbeeld bescherming van de apparatuur tegen sterke elektromagnetische velden? | ❒ | ❒ | ❒ | ❒ |
| 7 | Wordt altijd viruscontrole toegepast op apparatuur die thuis wordt gebruikt voor doeleinden van de onderneming? | ❒ | ❒ | ❒ | ❒ |

**7.2.6 Veilig afvoeren en hergebruiken van apparatuur**

| | | | | | |
|---|---|---|---|---|---|
| 1 | Bestaan er richtlijnen voor het veilig afvoeren van apparatuur? | ❒ | ❒ | ❒ | ❒ |
| 2 | Worden de opgeslagen gegevens verwijderd, voordat apparatuur inclusief opslagmedia (harde schijven, tapes, cartridges en diskettes) afgevoerd worden? | ❒ | ❒ | ❒ | ❒ |
| 3 | Worden opslagmedia die gevoelige informatie bevatten, fysiek vernietigd? | ❒ | ❒ | ❒ | ❒ |
| 4 | Wanneer apparatuur (inclusief een opslagmedium zoals bijvoorbeeld een harde schijf) met bijzonder gevoelige gegevens beschadigd is, wordt dan een risicoanalyse uitgevoerd om te bepalen of deze vernietigd dan wel tegen korting aan de leverancier ter reparatie teruggegeven moeten worden? | ❒ | ❒ | ❒ | ❒ |

**7.3.1 Clear desk en clear screen policy**

| | | | | | |
|---|---|---|---|---|---|
| 1 | Zijn algemene voorschriften opgesteld ter bescherming van informatie tegen onbevoegde kennisneming, verlies of beschadiging? | ❒ | ❒ | ❒ | ❒ |
| 2 | Zijn deze voorschriften bekend gemaakt aan de medewerkers? | ❒ | ❒ | ❒ | ❒ |
| 3 | Wordt regelmatig gecontroleerd of medewerkers de voorschriften naleven? | ❒ | ❒ | ❒ | ❒ |
| 4 | Moeten papieren en diskettes worden opgeborgen in een kast, wanneer deze niet worden gebruikt? | ❒ | ❒ | ❒ | ❒ |
| 5 | Wanneer de papieren of diskettes kritische gegevens bevatten, moeten zij dan in een afgesloten (liefst brandvrije) kast worden opgeborgen, zeker wanneer het kantoor verlaten is? | ❒ | ❒ | ❒ | ❒ |
| 6 | Zijn personal computers en terminals beveiligd door middel van sloten, wachtwoorden, screensavers met wachtwoordbeveiliging of andere maatregelen, wanneer zij niet hoeven te worden gebruikt? | ❒ | ❒ | ❒ | ❒ |
| 7 | Zijn maatregelen genomen om binnenkomende en uitgaande post te beschermen? | ❒ | ❒ | ❒ | ❒ |
| 8 | Wordt toezicht gehouden op het gebruik van faxapparatuur? | ❒ | ❒ | ❒ | ❒ |
| 9 | Worden fotokopieerapparaten buiten kantooruren afgesloten of anders beveiligd tegen ongeautoriseerd gebruik? | ❒ | ❒ | ❒ | ❒ |
| 10 | Behoort gevoelige of geheime informatie direct na het afdrukken van de printer te worden verwijderd? | ❒ | ❒ | ❒ | ❒ |

**7.3.2 Het verwijderen van bedrijfseigendommen**

| | | | | | |
|---|---|---|---|---|---|
| 1 | Is aan de medewerkers bekend gemaakt dat zij slechts apparatuur, gegevens en programmatuur uit het gebouw mogen verwijderen met formele toestemming van het management? | ❒ | ❒ | ❒ | ❒ |
| 2 | Wordt gecontroleerd of de medewerkers zich aan die richtlijnen houden? | ❒ | ❒ | ❒ | ❒ |
| 3 | Worden media met geclassificeerde gegevens slechts verwijderd nadat de informatie is gewist? | ❒ | ❒ | ❒ | ❒ |



Zo beantwoorden: ☑

**J**a
**N**ee
**G**edeeltelijk
**O**nbekend

| | | J | N | G | O |
|---|---|---|---|---|---|
| 4 | Zijn er voor bijvoorbeeld mislukte papieren output zelfdovende afvalbakken beschikbaar? | ❒ | ❒ | ❒ | ❒ |
| 5 | Indien de mislukte output geclassificeerde gegevens bevat, zijn er dan afsluitbare afvalbakken beschikbaar? | ❒ | ❒ | ❒ | ❒ |
| 6 | Is voor vernietiging van papier met geclassificeerde gegevens een contract afgesloten met een gerenommeerd bedrijf dat een geheimhoudingsverklaring heeft ondertekend? | ❒ | ❒ | ❒ | ❒ |

## 8 Beheer van communicatie- en bedieningsprocessen

### 8.1.1 Gedocumenteerde bedieningsprocedures

| | | | | | |
|---|---|---|---|---|---|
| 1 | Zijn er procedures met gedetailleerde instructies voor de uitvoering van alle taken, waaronder (voorzover van toepassing): | | | | |
| | • de juiste behandeling van gegevensbestanden; | ❒ | ❒ | ❒ | ❒ |
| | • het opstellen van de planning de begintijd van de eerste en de eindtijd van de laatste bedieningstaak; | ❒ | ❒ | ❒ | ❒ |
| | • het afhandelen van fouten en andere uitzonderlijke gebeurtenissen die tijdens de uitvoering van de taken kunnen optreden, inclusief beperkingen in het gebruik van systeemhulpmiddelen; | ❒ | ❒ | ❒ | ❒ |
| | • informatie over contactpersonen in geval van onverwachte bedieningsmoeilijkheden of technische storingen. Het gaat hier om contactpersonen, zowel in de automatiseringsorganisatie (helpdesk, werkvoorbereiding, beheerders, leidinggevenden), als in de gebruikersorganisatie (beheerders, leidinggevenden); | ❒ | ❒ | ❒ | ❒ |
| | • de behandeling van computeroutput, zoals het gebruik van speciaal papier of het beheer van vertrouwelijke output (inclusief procedures voor een veilige verwerking van uitvoer van mislukte printopdrachten); | ❒ | ❒ | ❒ | ❒ |
| | • het opnieuw starten en herstellen van het computersysteem en/of netwerk in geval van storingen; | ❒ | ❒ | ❒ | ❒ |
| | • het gebruik van elke applicatie (productiehandboeken)? | ❒ | ❒ | ❒ | ❒ |
| 2 | Zijn er gedocumenteerde procedures voor de huishoudelijke activiteiten met betrekking tot computer- en netwerkbeheer, zoals opstart- en afsluitprocedures, het maken van reservekopieën, onderhoud van apparatuur, beheer en beveiliging van computerruimten, enzovoort? | ❒ | ❒ | ❒ | ❒ |
| 3 | Worden bedieningsprocedures als formele documenten behandeld (operatorhandboek) en worden wijzigingen alleen aangebracht na goedkeuring door een geautoriseerde manager? | ❒ | ❒ | ❒ | ❒ |
| 4 | Worden bijzonderheden met betrekking tot de dagelijkse operaties vastgelegd (journaal, dagrapportage)? | ❒ | ❒ | ❒ | ❒ |

### 8.1.2 Het beheer van wijzigingen

| | | | | | |
|---|---|---|---|---|---|
| 1 | Is wijzigingenbeheer gescheiden van ontwikkelings- en productietaken? | ❒ | ❒ | ❒ | ❒ |
| 2 | Zijn de verantwoordelijkheden en procedures van het management rond het wijzigingenbeheer formeel vastgelegd, zodat er voldoende controle is op alle wijzigingen aan apparatuur, programmatuur en procedures? | ❒ | ❒ | ❒ | ❒ |
| 3 | Zijn de verantwoordelijkheden en procedures van de afdelingen (functionarissen) betrokken bij het wijzigingenbeheer formeel vastgelegd? | ❒ | ❒ | ❒ | ❒ |
| 4 | Is er voldoende capaciteit beschikbaar om wijzigingen tijdig te kunnen behandelen? | ❒ | ❒ | ❒ | ❒ |
| 5 | Is er sprake van een juiste functiescheiding binnen het proces wijzigingenbeheer? | ❒ | ❒ | ❒ | ❒ |



Zo beantwoorden: ☑

**J**a
**N**ee
**G**edeeltelijk
**O**nbekend

| | | J | N | G | O |
|---|---|---|---|---|---|
| 6 | Is bij de procedures met betrekking tot wijzigingen voldoende aandacht besteed aan: | | | | |
| | • autorisatie van het wijzigingsverzoek (inclusief onderbouwing van de wijziging); | ❒ | ❒ | ❒ | ❒ |
| | • het vaststellen en noteren van belangrijke wijzigingen; | ❒ | ❒ | ❒ | ❒ |
| | • het bepalen van de mogelijke gevolgen van dergelijke wijzigingen; | ❒ | ❒ | ❒ | ❒ |
| | • een goedkeuringsprocedure voor voorgestelde wijzigingen voor vertrouwelijkheid, integriteit en beschikbaarheid; | ❒ | ❒ | ❒ | ❒ |
| | • een gedetailleerde mededeling van de wijzigingen aan alle betrokken personen; | ❒ | ❒ | ❒ | ❒ |
| | • procedures en verantwoordelijkheden voor het afbreken en herstellen van niet geslaagde wijzigingen; | ❒ | ❒ | ❒ | ❒ |
| | • voortgangsbewaking; | ❒ | ❒ | ❒ | ❒ |
| | • het genereren van een audittrail; | ❒ | ❒ | ❒ | ❒ |
| | • detectie en interne controle van wijzigingen? | ❒ | ❒ | ❒ | ❒ |
| 7 | Worden alle wijzigingsaanvragen geclassificeerd ten aanzien van de volgende aspecten: | | | | |
| | • prioriteit (spoed van de wijziging); | ❒ | ❒ | ❒ | ❒ |
| | • complexiteit (impact op de organisatie); | ❒ | ❒ | ❒ | ❒ |
| | • doorlooptijd; | ❒ | ❒ | ❒ | ❒ |
| | • soort object (hardware, besturingsprogrammatuur, applicaties, procedures)? | ❒ | ❒ | ❒ | ❒ |
| 8 | Zijn voor alle aspecten criteria opgesteld aan de hand waarvan de classificatie kan plaatsvinden? | ❒ | ❒ | ❒ | ❒ |

**8.1.3 Procedures voor het behandelen van incidenten**

| | | | | | |
|---|---|---|---|---|---|
| 1 | Is duidelijk gedefinieerd wat wordt verstaan onder (beveiligings)incidenten? | ❒ | ❒ | ❒ | ❒ |
| 2 | Zijn er procedures voor het afhandelen van storingen (noodzakelijk voor een snelle, effectieve en ordelijke afhandeling van (beveiligings)incidenten)? | ❒ | ❒ | ❒ | ❒ |
| 3 | Worden incidenten geregistreerd en wordt hierbij de impact, de urgentie en de verwachte inspanning aangegeven? | ❒ | ❒ | ❒ | ❒ |
| 4 | Is voor alle typen incidenten duidelijk welke functionaris/afdeling voor de afhandeling van het incident zorg draagt? | ❒ | ❒ | ❒ | ❒ |
| 5 | Is er voldoende aandacht van het management voor het proces van incidentenafhandeling wat zich onder meer uit door: | | | | |
| | • toekenning van taken en verantwoordelijkheden; | ❒ | ❒ | ❒ | ❒ |
| | • managementrapportages over het functioneren van incidentenafhandeling; | ❒ | ❒ | ❒ | ❒ |
| | • stroomlijning van de interactie tussen incidentenafhandeling, probleemafhandeling, wijzigingenbeheer en configuratiebeheer? | ❒ | ❒ | ❒ | ❒ |
| 6 | Is incidentenafhandeling gescheiden van andere functies die een conflicterend belang kunnen hebben (bijvoorbeeld wijzigingenbeheer, systeemontwikkeling, produktiebediening/-bewaking)? | ❒ | ❒ | ❒ | ❒ |
| 7 | Is er binnen het proces van incidentenafhandeling sprake van functiescheiding tussen beschikken, registreren, uitvoeren, bewaren en controleren? | ❒ | ❒ | ❒ | ❒ |
| 8 | Is er voldoende personeel met de juiste expertise om te zorgen voor een tijdige oplossing van de incidenten? | ❒ | ❒ | ❒ | ❒ |
| 9 | Zijn in de procedures alle mogelijk voorkomende beveiligingsincidenten gekwalificeerd, zoals: | | | | |
| | • systeemstoringen en niet beschikbaar zijn van diensten; | ❒ | ❒ | ❒ | ❒ |
| | • fouten die het resultaat zijn van incomplete of onnauwkeurige bedrijfsgegevens; | ❒ | ❒ | ❒ | ❒ |
| | • inbreuk op de vertrouwelijkheid van gegevens; | ❒ | ❒ | ❒ | ❒ |
| | • (pogingen tot)onbevoegde benadering van besturings- of applicatiebestanden; | ❒ | ❒ | ❒ | ❒ |



Zo beantwoorden: ☑

**J**a
**N**ee
**G**edeeltelijk
**O**nbekend

J N G O

- gedetecteerde beveiligings'lekken' (bijvoorbeeld ontdekt bij het testen van applicaties of besturingssystemen, dan wel ontdekt in de productieomgeving, omdat beveiligingsvoorzieningen verkeerd geïmplementeerd zijn of onder combinatie van omstandigheden anders werken); ❒ ❒ ❒ ❒
- virusaanvallen? ❒ ❒ ❒ ❒

10 Zijn in de procedures, naast de normale noodprocedures (die zijn ontworpen om systemen en (netwerk)diensten zo snel mogelijk te herstellen) maatregelen beschreven met betrekking tot:
- analyse en identificatie van de oorzaak van het probleem; ❒ ❒ ❒ ❒
- planning en implementatie van maatregelen om herhaling te voorkomen; ❒ ❒ ❒ ❒
- verzamelen van audittrails en gelijksoortig bewijsmateriaal; ❒ ❒ ❒ ❒
- communicatie met zakelijke gebruikers en anderen die getroffen zijn door (of betrokken zijn bij) het incident? ❒ ❒ ❒ ❒

11 Zijn de noodprocedures formeel vastgelegd en bevatten deze instructies ten aanzien van:
- wie de noodprocedures in werking mag stellen/autoriseren; ❒ ❒ ❒ ❒
- onder welke omstandigheden de noodprocedures in werking gesteld mogen worden; ❒ ❒ ❒ ❒
- het genereren en (laten) controleren van audittrails; ❒ ❒ ❒ ❒
- het beheren (tijdig verversen wachtwoord) en veilig opslaan van wachtwoorden van noodusers? ❒ ❒ ❒ ❒

12 Zijn de noodprocedures bij alle belanghebbenden bekend gesteld? ❒ ❒ ❒ ❒

13 Worden audittrails en soortgelijk bewijsmateriaal verzameld en veilig opgeslagen in verband met:
- interne probleemanalyse; ❒ ❒ ❒ ❒
- gebruik als bewijsmateriaal in geval van mogelijke contractbreuk of bij het overtreden van interne en/of wettelijke voorschriften; ❒ ❒ ❒ ❒
- onderhandelingen over compensatie door de leveranciers van apparatuur, programmatuur en diensten; ❒ ❒ ❒ ❒
- het aantonen van computermisbruik of overtreding van de Wet Bescherming Persoonsgegevens? ❒ ❒ ❒ ❒

14 Bevatten procedures dusdanige waarborgen dat de acties die dienen te worden ondernomen om beveiligingsincidenten en systeemstoringen te corrigeren en te herstellen zorgvuldig en formeel worden bestuurd? Wordt met name gewaarborgd dat:
- alleen duidelijk geïdentificeerde en geautoriseerde personen toegang krijgen tot operationele systemen en gegevens; ❒ ❒ ❒ ❒
- alle uitgevoerde herstelwerkzaamheden tot in detail zijn gedocumenteerd; ❒ ❒ ❒ ❒
- herstelwerkzaamheden zijn gerapporteerd aan het management en op een ordelijke manier zijn beoordeeld; ❒ ❒ ❒ ❒
- de integriteit van de systemen en hun beveiliging zo snel mogelijk wordt bevestigd; ❒ ❒ ❒ ❒
- incidenten tijdig worden afgehandeld en afgesloten; ❒ ❒ ❒ ❒
- inspanningen zich eveneens richten op alternatieve of tijdelijke oplossingen, als blijkt dat binnen de gewenste hersteltermijn geen permanente oplossing zal worden gevonden? ❒ ❒ ❒ ❒

15 Zijn er escalatieprocedures? Zo ja, is daarin opgenomen: ❒ ❒ ❒ ❒
- wanneer de gevolgen te groot zijn en het management moet worden gewaarschuwd (wie bij crisismanagement welke beslissingen neemt); ❒ ❒ ❒ ❒
- wie bij afwezigheid de leiding mag overnemen; ❒ ❒ ❒ ❒
- welke hulpmiddelen na het incident kunnen worden ingezet; ❒ ❒ ❒ ❒



Zo beantwoorden: ☑

**J**a
**N**ee
**G**edeeltelijk
**O**nbekend

J N G O

- wie belast is met de coördinatie indien externe partijen moeten worden geïnformeerd over het incident? ❒ ❒ ❒ ❒

**8.1.4 Functiescheiding**

1 Is er een lijst met organisatorische functies beschikbaar? ❒ ❒ ❒ ❒
2 Zijn van alle functies de taken, verantwoordelijkheden en bevoegdheden vastgelegd? ❒ ❒ ❒ ❒
3 Is bij het toekennen van taken en verantwoordelijkheden aan functies een scheiding aangebracht tussen beschikken, registreren, uitvoeren, controleren en bewaren? ❒ ❒ ❒ ❒
4 Is er vastgelegd welke functies gescheiden moeten worden? Is hierbij een scheiding gerealiseerd tussen, met name: ❒ ❒ ❒ ❒
- systeemontwikkeling (ontwikkelen/bouwen applicaties, programma- en systeemtesten, systeemonderhoud); ❒ ❒ ❒ ❒
- verwerking/exploitatie, dat wil zeggen management en staffuncties, beveiligingsfuncties, interne controle functie, bevoegdhedenbeheer, werkvoorbereiding, operating, technisch specialisten/beheerders (netwerkbeheer, systeemprogrammering), enzovoort; ❒ ❒ ❒ ❒
- gebruikersorganisatie (specificeren eisen, autoriseren wijzigingen, acceptatietesten, gebruik)? ❒ ❒ ❒ ❒

5 Wordt functiescheiding gehandhaafd bij de personele invulling van deze functies? ❒ ❒ ❒ ❒
6 Is er een actueel overzicht van personele bezetting van functies? ❒ ❒ ❒ ❒
7 Is functiescheiding adequaat geïmplementeerd binnen de software voor logische toegangsbeveiliging (betreft toegang tot netwerken, computer- en informatiesystemen)? ❒ ❒ ❒ ❒

**8.1.5 Scheiding van voorzieningen voor ontwikkeling en productie**

1 Wordt de programmatuur voor ontwikkeling en de programmatuur voor productie, voor zover mogelijk, door verschillende processoren of in verschillende domeinen of directory's uitgevoerd? ❒ ❒ ❒ ❒
2 Worden de werkzaamheden voor ontwikkelen en voor testen zoveel mogelijk gescheiden? ❒ ❒ ❒ ❒
3 Worden compilers, editors en andere systeemhulpmiddelen niet opgeslagen bij operationele systemen? ❒ ❒ ❒ ❒
4 Worden, om verwarring te voorkomen, verschillende aanlogprocedures gebruikt voor operationele systemen en testsystemen? ❒ ❒ ❒ ❒
5 Wordt het door ontwikkeling en productie gemeenschappelijk delen van computerresources tegengegaan (bijvoorbeeld geen shared DASD)? ❒ ❒ ❒ ❒
6 Wordt restrictief omgegaan met de toegang van ontwikkelaars en testers tot de productie omgeving? ❒ ❒ ❒ ❒
7 Wordt de scheiding tussen omgevingen voor productie en ontwikkeling adequaat ondersteund door formele overdrachtsprocedures? ❒ ❒ ❒ ❒

**8.1.6 Extern beheer van voorzieningen**

1 Is met de externe partij een contract afgesloten met daarin de noodzakelijke eisen op het gebied van beveiliging en is in het contract een geheimhoudingsclausule opgenomen? ❒ ❒ ❒ ❒
2 Is onderzocht of er gevoelige of kritieke toepassingen zijn die beter in eigen beheer kunnen worden uitgevoerd? ❒ ❒ ❒ ❒
3 Is er goedkeuring van de eigenaren van zakelijke toepassingen voor het uitvoeren van het beheer door derden? ❒ ❒ ❒ ❒
4 Zijn de gevolgen voor de beschikbaarheid, integriteit en vertrouwelijkheid van de bedrijfsvoering onderzocht? ❒ ❒ ❒ ❒



Zo beantwoorden: ☑

**J**a
**N**ee
**G**edeeltelijk
**O**nbekend

| | | J | N | G | O |
|---|---|---|---|---|---|
| 5 | Zijn er beveiligingsmaatregelen opgesteld en is er een procedure om te controleren of deze maatregelen worden nageleefd? | ❒ | ❒ | ❒ | ❒ |
| 6 | Zijn de verantwoordelijkheden en procedures voor het rapporteren en behandelen van beveiligingsincidenten vastgelegd (zie 8.1.3 ‘Procedures voor het behandelen van incidenten’)? | ❒ | ❒ | ❒ | ❒ |
| | **8.2.1 Capaciteitsplanning** | | | | |
| 1 | Wordt periodiek vastgesteld en vastgelegd welke toekomstige ontwikkelingen worden verwacht ten aanzien van het gebruik van de systeemresources? | ❒ | ❒ | ❒ | ❒ |
| 2 | Wordt het huidige beslag op de resources bewaakt? | ❒ | ❒ | ❒ | ❒ |
| 3 | Worden fout(storings)meldingen vastgelegd en geanalyseerd (met name waar het gaat om disk- en tape-errors, omdat dit aanleiding kan zijn tot preventief onderhoud)? | ❒ | ❒ | ❒ | ❒ |
| 4 | Wordt de hierboven genoemde informatie door managers van computers en netwerken gebruikt om potentiële knelpunten te signaleren en te voorkomen, zodat deze geen gevaar opleveren voor de beveiliging van het systeem of voor diensten aan gebruikers, en wordt de informatie gebruikt om de juiste tegenmaatregelen voor te bereiden? | ❒ | ❒ | ❒ | ❒ |
| 5 | Wordt er rekening mee gehouden dat vergroting van de operationele capaciteit tevens vergroting van de uitwijkcapaciteit kan inhouden? | ❒ | ❒ | ❒ | ❒ |
| | **8.2.2 Acceptatie van systemen** | | | | |
| 1 | Is er door (of namens) het management een projectorganisatie ingevoerd ten behoeve van selectie, acceptatie (inclusief testen) en implementatie (inclusief beveiliging) van nieuwe IT-componenten? | ❒ | ❒ | ❒ | ❒ |
| 2 | Zijn de eisen en de criteria ten aanzien van nieuwe IT-componenten vastgelegd en goedgekeurd door het management? | ❒ | ❒ | ❒ | ❒ |
| 3 | Is voor het testen een testplan opgesteld? | ❒ | ❒ | ❒ | ❒ |
| 4 | Zijn in het testplan de volgende onderwerpen opgenomen: | | | | |
| | • te testen items met verwacht resultaat; | ❒ | ❒ | ❒ | ❒ |
| | • acceptatiecriteria; | ❒ | ❒ | ❒ | ❒ |
| | • fout-, herstel- en herstartprocedures; | ❒ | ❒ | ❒ | ❒ |
| | • routinematige bedieningsprocedures? | ❒ | ❒ | ❒ | ❒ |
| 5 | Worden de testresultaten adequaat vastgelegd (trouble-reports) en geëvalueerd (evaluatie en/of eindrapport)? | ❒ | ❒ | ❒ | ❒ |
| 6 | Is bij het testen in toereikende mate aandacht gegeven aan het testen van beveiligings- en controlemaatregelen? | ❒ | ❒ | ❒ | ❒ |
| 7 | Heeft men de verzekering dat installatie van het nieuwe systeem (of systeemcomponenten) geen nadelige invloed heeft op bestaande systemen, in het bijzonder tijdens de drukste verwerkingstijden (zoals aan het einde van de maand)? | ❒ | ❒ | ❒ | ❒ |
| 8 | Is voorzien in cursussen voor bediening en gebruik van nieuwe systemen (of systeemcomponenten)? | ❒ | ❒ | ❒ | ❒ |
| | **8.3.1 Maatregelen tegen kwaadaardige software** | | | | |
| 1 | Is bij gebruikers het gevaar van virussen voldoende onder de aandacht gebracht (beveiligingsbewustzijn)? | ❒ | ❒ | ❒ | ❒ |



Zo beantwoorden: ☑

**J**a
**N**ee
**G**edeeltelijk
**O**nbekend

| | | J | N | G | O |
|---|---|---|---|---|---|
| 2 | Heeft de organisatie een formeel beleid met betrekking tot het naleven van programmatuurlicenties en verboden gebruik van niet-geautoriseerde programmatuur (zie 12.1.2 'Intellectuele eigendomsrechten')? | ❒ | ❒ | ❒ | ❒ |
| 3 | Is antivirusprogrammatuur geïnstalleerd op pc's, laptops, servers, gateways, firewalls, enzovoort? | ❒ | ❒ | ❒ | ❒ |
| 4 | Is de antivirusprogrammatuur afkomstig van een gerenommeerd bedrijf? | ❒ | ❒ | ❒ | ❒ |
| 5 | Wordt programmatuur die gericht is op het ontdekken van specifieke virussen voldoende frequent, op de wijze zoals door de leverancier aangegeven, gebruikt om op computers en opslagmedia te zoeken naar bekende virussen? | ❒ | ❒ | ❒ | ❒ |
| 6 | Worden voor deze programmatuur regelmatig updates aangeschaft en geïnstalleerd? | ❒ | ❒ | ❒ | ❒ |
| 7 | Is er op de computers eventueel programmatuur geïnstalleerd waarmee wijzigingen in uitvoeringscode zijn vast te stellen? | ❒ | ❒ | ❒ | ❒ |
| 8 | Wordt programmatuur voor het herstellen van door virussen veroorzaakte schade met zorgvuldigheid gebruikt, namelijk alleen in die gevallen waarin de kenmerken van het virus volledig worden begrepen en het zeker is dat de herstelwerkzaamheden correct kunnen worden uitgevoerd? | ❒ | ❒ | ❒ | ❒ |
| 9 | Vindt regelmatig controle plaats op de programmatuur en de inhoud van de gegevens van systemen waarop kritieke processen worden uitgevoerd? | ❒ | ❒ | ❒ | ❒ |
| 10 | Wordt de aanwezigheid van schijnbestanden of ongeautoriseerde toevoegingen aan bestanden formeel onderzocht? | ❒ | ❒ | ❒ | ❒ |
| 11 | Worden alle diskettes uit onzekere of ongeautoriseerde bron op virussen gecontroleerd voordat zij worden gebruikt? | ❒ | ❒ | ❒ | ❒ |
| 12 | Zijn er procedures en verantwoordelijkheden voor/door het management vastgelegd ten aanzien van het rapporteren en herstellen van virusaanvallen (zie 6.3 'Reageren op beveiligingsincidenten en storingen' en 8.1.3.'Procedures voor het behandelen van incidenten')? | ❒ | ❒ | ❒ | ❒ |
| 13 | Is er een continuïteitsplan opgesteld in verband met virusaanvallen, waarin onder andere de maatregelen worden beschreven die nodig zijn om reservekopieën te maken van alle noodzakelijke gegevens en programmatuur (zie 11.1 'Aspecten van continuïteitsmanagement')? | ❒ | ❒ | ❒ | ❒ |

**8.4.1 Reservekopieën maken (back-ups)**

| | | | | | |
|---|---|---|---|---|---|
| 1 | Wordt voldoende frequent een back-up (reservekopie) gemaakt van alle belangrijke gegevens, zoals: | | | | |
| | • (gewijzigde) databestanden en programmatuur; | ❒ | ❒ | ❒ | ❒ |
| | • autorisatie en logbestanden; | ❒ | ❒ | ❒ | ❒ |
| | • de volledige schijveninhoud? | ❒ | ❒ | ❒ | ❒ |
| 2 | Is het mogelijk om de sinds de vorige back-up verlorengegane gegevens te reconstrueren (bijvoorbeeld met behulp van roll-back/roll-forward principes)? | ❒ | ❒ | ❒ | ❒ |
| 3 | Is het systeem resistent tegen storingen van een individueel opslagmedium? | ❒ | ❒ | ❒ | ❒ |
| 4 | Worden de reservekopieën die minimaal nodig zijn om het systeem te herstellen, (samen met een nauwkeurig en volledig overzicht van de reservekopieën) opgeslagen op een locatie die zich op zodanige afstand bevindt dat geen schade kan worden aangericht als zich een calamiteit voordoet op de hoofdlocatie? | ❒ | ❒ | ❒ | ❒ |
| 5 | Worden van belangrijke zakelijke toepassingen meerdere generaties reservekopieën bewaard (bijvoorbeeld volgens het grootvader-, vader-, zoonprincipe)? | ❒ | ❒ | ❒ | ❒ |



Zo beantwoorden: ☑

**J**a
**N**ee
**G**edeeltelijk
**O**nbekend

| | | J | N | G | O |
|---|---|---|---|---|---|
| 6 | Worden voor de reservekopieën, conform de daaraan gestelde eisen, toereikende bewaartermijnen in acht genomen? | ❒ | ❒ | ❒ | ❒ |
| 7 | Worden reservekopieën en de ruimte waarin deze zijn opgeslagen, fysiek goed beveiligd volgens dezelfde normen die gelden voor de hoofdlocatie? | ❒ | ❒ | ❒ | ❒ |
| 8 | Gelden de maatregelen die getroffen zijn voor de media op de hoofdlocatie ook voor de uitwijklocatie? | ❒ | ❒ | ❒ | ❒ |
| 9 | Worden reservekopieën regelmatig getest, zodat het zeker is dat zij betrouwbaar zijn en in geval van nood kunnen worden gebruikt (testen back-up- en restore-procedures)? | ❒ | ❒ | ❒ | ❒ |
| 10 | Is duidelijk vastgelegd wie verantwoordelijk is voor het maken van back-ups (op servers, pc's, laptops en mainframe)? | ❒ | ❒ | ❒ | ❒ |
| 11 | Wordt gecontroleerd dat alle back-up-jobs zijn gedraaid en goed zijn geëindigd? | ❒ | ❒ | ❒ | ❒ |
| 12 | Zijn er voorschriften voor conversie van gegevens naar andere gegevensdragers, bijvoorbeeld in het kader van (wettelijke) bewaarplicht? | ❒ | ❒ | ❒ | ❒ |
| 13 | Wordt gecontroleerd of de gegevens na conversie nog leesbaar zijn? | ❒ | ❒ | ❒ | ❒ |
| 14 | Wordt na omzetting van de gegevens gecontroleerd of de gegevens juist en volledig zijn overgezet? | ❒ | ❒ | ❒ | ❒ |
| 15 | Is er een procedure opgesteld waarmee wordt gewaarborgd dat nieuwe media, indien vereist, worden opgenomen in het back-up proces? | ❒ | ❒ | ❒ | ❒ |

**8.4.2 Bijhouden van een logboek**

| | | | | | |
|---|---|---|---|---|---|
| 1 | Bevat het logboek registraties betreffende: | | | | |
| | • de tijdstippen waarop besturings(sub)systemen en applicaties zijn gestart en beëindigd; | ❒ | ❒ | ❒ | ❒ |
| | • fouten in de besturingssystemen, niet normaal beëindigde applicatiejobs, et cetera en de daarbij ondernomen correctieve acties; | ❒ | ❒ | ❒ | ❒ |
| | • de bevestiging dat gegevensbestanden en computeruitvoer correct zijn verwerkt, de bevestiging dat alle back-up-jobs zijn gestart en correct zijn beëindigd, et cetera; | ❒ | ❒ | ❒ | ❒ |
| | • de noodingrepen die zijn verricht (bijvoorbeeld met behulp van nood-users), de reden waarom deze ingrepen zijn verricht en wie daartoe autorisatie heeft verleend; | ❒ | ❒ | ❒ | ❒ |
| | • het tussentijds opnieuw starten van besturings(sub) systemen, de reden waarom opnieuw is gestart en wie daartoe autorisatie heeft verleend; | ❒ | ❒ | ❒ | ❒ |
| | • het einde van een computershift, inclusief vermelding van attentiepunten en/of nog openstaande acties die van belang zijn voor overdracht naar de volgende shift; | ❒ | ❒ | ❒ | ❒ |
| | • de naam van de persoon die de aantekening in het logboek heeft gemaakt? | ❒ | ❒ | ❒ | ❒ |
| 2 | Is de bewaartermijn van de logboeken vastgelegd? | ❒ | ❒ | ❒ | ❒ |
| 3 | Worden de logboeken tijdig op een veilige plaats opgeslagen? | ❒ | ❒ | ❒ | ❒ |
| 4 | Vinden regelmatig (statistische) analyses plaats van de in de logboeken geregistreerde informatie? | ❒ | ❒ | ❒ | ❒ |
| 5 | Worden de logboeken op periodieke basis gecontroleerd door een onafhankelijke controlediscipline? | ❒ | ❒ | ❒ | ❒ |

**8.4.3 Storingen opnemen in een logboek**

| | | | | | |
|---|---|---|---|---|---|
| 1 | Is aan gebruikers bekend gemaakt waar zij storingen en incidenten kunnen melden (bijvoorbeeld de helpdesk)? | ❒ | ❒ | ❒ | ❒ |
| 2 | Worden storingen en incidenten centraal vastgelegd (in een logboek en/of pakket voor incident- en probleemmanagement)? | ❒ | ❒ | ❒ | ❒ |



Zo beantwoorden: ☑

**J**a
**N**ee
**G**edeeltelijk
**O**nbekend

| | | J | N | G | O |
|---|---|---|---|---|---|
| 3 | Worden gebruikers geïnformeerd over het in behandeling nemen en de afdoening van de storing? | ❒ | ❒ | ❒ | ❒ |
| 4 | Worden op basis van vastleggingen systematische storingsanalyses uitgevoerd? | ❒ | ❒ | ❒ | ❒ |
| 5 | Wordt het proces van storingsanalyse en -behandeling gecontroleerd? | ❒ | ❒ | ❒ | ❒ |

**8.5.1 Maatregelen voor netwerken**

| | | | | | |
|---|---|---|---|---|---|
| 1 | Is de netwerkbeheerorganisatie beschreven, met daarin tenminste opgenomen: | | | | |
| | • de taken en verantwoordelijkheden; | ❒ | ❒ | ❒ | ❒ |
| | • de personele bezetting; | ❒ | ❒ | ❒ | ❒ |
| | • de benodigde externe krachten; | ❒ | ❒ | ❒ | ❒ |
| | • de relatie met interne en externe functionarissen? | ❒ | ❒ | ❒ | ❒ |
| 2 | Zijn alle netwerkcomponenten geregistreerd en beschreven, inclusief hun status en relatie met andere netwerkcomponenten en zijn in deze beschrijving opgenomen: | ❒ | ❒ | ❒ | ❒ |
| | • technische aspecten (zoals typenummer, serienummer, aanschafdatum, versienummer); | ❒ | ❒ | ❒ | ❒ |
| | • financiële aspecten (zoals onderhoudscontracten, verricht onderhoud, leverancier, serviceverlener); | ❒ | ❒ | ❒ | ❒ |
| | • organisatorische aspecten (zoals lokatie, beheerder, functioneel-, technisch- en budgethouder)? | ❒ | ❒ | ❒ | ❒ |
| 3 | Wordt periodiek gecontroleerd of de registratie een getrouwe afspiegeling is van de werkelijkheid (inventarisatie)? | ❒ | ❒ | ❒ | ❒ |
| 4 | Is de logische lay-out van het netwerk vastgelegd? | ❒ | ❒ | ❒ | ❒ |
| 5 | Zijn er procedures voor het wijzigen van netwerkcomponenten (hardware en software)? | ❒ | ❒ | ❒ | ❒ |
| 6 | Worden nieuwe componenten die in het netwerk worden opgenomen, vóór ingebruikname getest? | ❒ | ❒ | ❒ | ❒ |
| 7 | Is er toezicht op het gebruik van het netwerk? | ❒ | ❒ | ❒ | ❒ |
| 8 | Wordt het gebruik van netwerk(componenten) periodiek geanalyseerd (bezetting, routering) bijvoorbeeld door het inzetten van netwerk-analysers? | ❒ | ❒ | ❒ | ❒ |
| 9 | Is er een mechanisme/programmatuur om het gebruik van niet geautoriseerde programmatuur te signaleren? | ❒ | ❒ | ❒ | ❒ |
| 10 | Is de gebruikers duidelijk gemaakt wat het gevaar is van het gebruik van niet geautoriseerde programmatuur en welke sancties dit voor hen kan hebben? | ❒ | ❒ | ❒ | ❒ |
| 11 | Wordt gebruik gemaakt van de standaardbeveiliging in het gebruikte netwerkprotocol (pariteitscontrole, redundancy controle, frame sequency) ? | ❒ | ❒ | ❒ | ❒ |
| 12 | Bevat het netwerk ingebouwde redundantie (geen single point of failure)? | ❒ | ❒ | ❒ | ❒ |
| 13 | Wordt van alle componenten periodiek het functioneren getest? | ❒ | ❒ | ❒ | ❒ |
| 14 | Worden geslaagde en niet geslaagde pogingen tot ongeautoriseerde toegang tot het netwerk en de netwerkbeheerfuncties gesignaleerd, geregistreerd en gemeld en worden hierop acties genomen om herhaling te voorkomen? | ❒ | ❒ | ❒ | ❒ |
| 15 | Is duidelijk vastgesteld wat de gebruikerseisen zijn ten aanzien van de kwaliteitsaspecten van de te transporteren gegevens en daarmee ten aanzien van het netwerk? | ❒ | ❒ | ❒ | ❒ |
| 16 | Is duidelijk aangegeven welk serviceniveau wordt geboden voor transport via het netwerk? | ❒ | ❒ | ❒ | ❒ |
| 17 | Worden, indien het beheer van het netwerk (gedeeltelijk) is ondergebracht bij derden, de taken en verantwoordelijkheden hieromtrent schriftelijk vastgelegd (bijvoorbeeld in een Service Level Agreement)? | ❒ | ❒ | ❒ | |
| 18 | Zijn er procedures voor het onderhouden van tabellen in netwerkcomponenten, zoals routers en bridges, om te voorkomen dat computersystemen in bepaalde netwerkdelen en computersystemen uit andere netwerkdelen met elkaar communiceren? | ❒ | ❒ | ❒ | ❒ |



Zo beantwoorden: ☑

**J**a
**N**ee
**G**edeeltelijk
**O**nbekend

| | | J | N | G | O |
|---|---|---|---|---|---|
| 19 | Zijn er voorzieningen getroffen om te voorkomen dat onbevoegden van buiten het interne netwerk benaderen (bijvoorbeeld een firewall)? | ❒ | ❒ | ❒ | ❒ |
| 20 | Zijn er (technische) maatregelen getroffen ter voorkoming van het ongeautoriseerd aansluiten van computers/randapparatuur op het netwerk? | ❒ | ❒ | ❒ | ❒ |
| 21 | Wordt er, indien sprake is van het gebruik van netwerkbeheerinstrumenten voor het beheer van netwerkcomponenten op afstand (zowel binnen de onderneming, als ook extern door bijvoorbeeld leveranciers), aandacht besteed aan: | | | | |
| | • toevoegen of verwijderen van beheerders; | ❒ | ❒ | ❒ | ❒ |
| | • toekennen/wijzigen van autorisaties om bepaalde functies voor bepaalde componenten te kunnen uitvoeren; | ❒ | ❒ | ❒ | ❒ |
| | • het onderhouden van informatie om de authenticiteit van beheerders vast te stellen; | ❒ | ❒ | ❒ | ❒ |
| | • het onderhouden van informatie om de componenten in staat te stellen authenticiteit van beheerderoperaties te verifiëren? | ❒ | ❒ | ❒ | ❒ |
| 22 | Zijn technieken geïmplementeerd die non-repudiation (onweerlegbaarheid van informatie) ondersteunen? | ❒ | ❒ | ❒ | ❒ |
| 23 | Is de vertrouwelijkheid van de gegevens bij transport via het netwerk gewaarborgd, bijvoorbeeld door het toepassen van encryptie? | ❒ | ❒ | ❒ | ❒ |
| 24 | Zijn er procedures voor uitgeven en laden van encryptiesleutels? | ❒ | ❒ | ❒ | ❒ |
| 25 | Is het beheer van netwerken indien mogelijk gescheiden van het beheer van computers? | ❒ | ❒ | ❒ | ❒ |
| 26 | Zijn er speciale maatregelen genomen om, indien vereist, de vertrouwelijkheid en de integriteit te waarborgen van de gegevens die via openbare netwerken worden verzonden? | ❒ | ❒ | ❒ | ❒ |
| 27 | Vindt periodiek een review plaats van de kwaliteit van het netwerk (performance, beveiliging, flexibiliteit, beheer)? | ❒ | ❒ | ❒ | ❒ |

**8.6.1 Beheer van verwijderbare computermedia**

| | | | | | |
|---|---|---|---|---|---|
| 1 | Bestaan er procedures voor het beheer van verwijderbare computermedia (banden, schijven, cassettes, afgedrukte uitvoer)? | ❒ | ❒ | ❒ | ❒ |
| 2 | Zijn in de procedures de volgende maatregelen opgenomen: | | | | |
| | • het niet gebruiken van beschrijvende labels voor identificatie van computermedia (de opgeslagen gegevens mogen niet te identificeren zijn aan de hand van een extern label); | ❒ | ❒ | ❒ | ❒ |
| | • het wissen van de inhoud van een herbruikbaar medium voordat dit de onderneming verlaat; | ❒ | ❒ | ❒ | ❒ |
| | • een schriftelijke toestemming voor alle media die het bedrijf verlaten en het ter controle bijhouden van een overzicht van alle media die het bedrijf verlaten (zie 8.7.2. ‘Beveiliging van media tijdens transport’). | ❒ | ❒ | ❒ | ❒ |
| 3 | Is op de afgedrukte uitvoer de rubricering/merking duidelijk aangegeven (bijvoorbeeld personeelsvertrouwelijk, commercieel vertrouwelijk)? | ❒ | ❒ | ❒ | ❒ |
| 4 | Is het mogelijk de volledigheid van de afgedrukte uitvoer vast te stellen (bijvoorbeeld door doorlopende paginanummering of nul-rapportages)? | ❒ | ❒ | ❒ | ❒ |
| 5 | Is op elektronische media de classificatie van de informatie duidelijk aangegeven zodat hiernaar gehandeld kan worden (waarbij in bepaalde situaties, bijvoorbeeld waar sprake is van grote hoeveelheden niet geclassificeerde informatie of daar waar procedures altijd al erg gericht zijn op vertrouwelijkheid, kan worden overwogen de classificatie niet op de media aan te geven, daar dit juist de aandacht vraagt en aanvalsdoel wordt)? | ❒ | ❒ | ❒ | ❒ |
| 6 | Zijn er procedures die waarborgen dat alle media zijn voorzien van de juiste classificatie? | ❒ | ❒ | ❒ | ❒ |



Zo beantwoorden: ☑

**J**a
**N**ee
**G**edeeltelijk
**O**nbekend

| | | J | N | G | O |
|---|---|---|---|---|---|
| 7 | Zijn er duidelijke voorschriften met betrekking tot het bewaren van de verschillende media (bewaartermijnen, beveiligde opslag, geconditioneerde opslag, enzovoort)? | ❒ | ❒ | ❒ | ❒ |
| 8 | Is er controle op de conditie en de opslagplaatsen van de verschillende media? | ❒ | ❒ | ❒ | ❒ |
| 9 | Zijn er procedures voor het hergebruik van een bepaald medium (binnen de onderneming)? | ❒ | ❒ | ❒ | ❒ |
| 10 | Zijn er procedures voor het wissen en vernietigen van bepaalde media bij het uit roulatie nemen ervan? | ❒ | ❒ | ❒ | ❒ |
| 11 | Zijn alle procedures en autorisatieniveaus duidelijk gedocumenteerd? | ❒ | ❒ | ❒ | ❒ |

**8.6.2 Afvoer van media**

| | | | | | |
|---|---|---|---|---|---|
| 1 | Zijn media met gevoelige informatie die niet langer nodig zijn, als zodanig herkenbaar en worden deze gescheiden van het overige afval bewaard? | ❒ | ❒ | ❒ | ❒ |
| 2 | Hebben onbevoegden geen toegang tot de media met gevoelige informatie die moet worden vernietigd? | ❒ | ❒ | ❒ | ❒ |
| 3 | Worden media die gevoelige informatie bevatten op een veilige manier gewist, binnen het bedrijf of op een veilige wijze afgevoerd en verbrand of vernietigd (waarbij veilig wil zeggen dat de gegevens na wissen/vernietiging niet meer gereconstrueerd kunnen worden)? | ❒ | ❒ | ❒ | ❒ |
| 4 | Zijn er voorschriften voor het op een veilige manier afvoeren van: | | | | |
| | • invoerdocumenten (bijvoorbeeld telexen); | ❒ | ❒ | ❒ | ❒ |
| | • carbonpapier; | ❒ | ❒ | ❒ | ❒ |
| | • afgedrukte rapporten; | ❒ | ❒ | ❒ | ❒ |
| | • printerlinten voor éénmalig gebruik; | ❒ | ❒ | ❒ | ❒ |
| | • magneetbanden; | ❒ | ❒ | ❒ | ❒ |
| | • verwijderbare schijven of cassettes; | ❒ | ❒ | ❒ | ❒ |
| | • programma-listings; | ❒ | ❒ | ❒ | ❒ |
| | • testgegevens; | ❒ | ❒ | ❒ | ❒ |
| | • systeemdocumentatie? | ❒ | ❒ | ❒ | ❒ |
| 5 | Wordt voor het afvoeren van papier, apparatuur en media een geschikt bedrijf, dat hierin ervaring heeft, gekozen en wordt er, door een daartoe geautoriseerde functionaris, op toegezien dat dit bedrijf de nodige beveiligingsmaatregelen in acht neemt? | ❒ | ❒ | ❒ | ❒ |
| 6 | Wordt het afvoeren van gevoelige gegevens zoveel mogelijk genoteerd, zodat hierop in de toekomst een controle kan worden uitgevoerd? | ❒ | ❒ | ❒ | ❒ |

**8.6.3 Procedures voor de behandeling van informatie**

| | | | | | |
|---|---|---|---|---|---|
| 1 | Zijn er procedures voor een veilige behandeling van alle gevoelige in- en uitvoermedia (documenten, telexen, banden, schijven, rapporten) en andere gevoelige objecten (blanco cheques, facturen)? | ❒ | ❒ | ❒ | ❒ |
| 2 | Is bij de bovengenoemde procedures rekening gehouden met de volgende aspecten: | | | | |
| | • procedures voor de behandeling van in- en uitvoermedia en bijvoorbeeld het aanbrengen van labels op dit soort media; | ❒ | ❒ | ❒ | ❒ |
| | • het bijhouden van een formeel overzicht van personen die geautoriseerd zijn voor de ontvangst van bepaalde gegevens; | ❒ | ❒ | ❒ | ❒ |
| | • procedures om te controleren of de in te voeren gegevens compleet zijn; | ❒ | ❒ | ❒ | ❒ |
| | • procedures voor de ontvangstbevestiging van verzonden gegevens; | ❒ | ❒ | ❒ | ❒ |
| | • het beperken van de verspreiding van gegevens; | ❒ | ❒ | ❒ | ❒ |



Zo beantwoorden: ☑

**J**a
**N**ee
**G**edeeltelijk
**O**nbekend

J N G O

- het aanbrengen van een duidelijke markering op alle kopieën van de gegevens waarmee wordt aangegeven wie toestemming heeft de gegevens te ontvangen; ❒ ❒ ❒ ❒
- procedures om verzendlijsten en lijsten van geautoriseerde ontvangers regelmatig te actualiseren? ❒ ❒ ❒ ❒

3 Wordt bij datatransport en zonodig bij dataopslag (laptops) van gevoelige gegevens encryptie toegepast? ❒ ❒ ❒ ❒

**8.6.4 Beveiliging van systeemdocumentatie**

1 Is de systeemdocumentatie opgeborgen in goed afgesloten kasten? ❒ ❒ ❒ ❒

2 Is de verzendlijst voor systeemdocumentatie zo kort mogelijk gehouden en is deze lijst geautoriseerd door de eigenaar van de applicatie? ❒ ❒ ❒ ❒

**8.7.1 Overeenkomsten over het uitwisselen van informatie en software**

1 Zijn er (schriftelijke) afspraken (bijvoorbeeld een geheimhoudingsverklaring) gemaakt voor het uitwisselen van gegevens en programmatuur tussen verschillende ondernemingen? ❒ ❒ ❒ ❒

2 Zijn in de overeenkomst de benodigde beveiligingsmaatregelen opgenomen, zoals:

- de verantwoordelijkheden van het management voor de rapportage van en het toezicht houden op het verzenden, het bewijs van verzending, en de ontvangst van gegevens; ❒ ❒ ❒ ❒
- de procedures voor verzending, bewijs van verzending en ontvangst van gegevens (onder andere een adequate registratie); ❒ ❒ ❒ ❒
- de eisen die minimaal worden gesteld aan verpakking en verzending; ❒ ❒ ❒ ❒
- kenmerken van de vervoerder; ❒ ❒ ❒ ❒
- de verantwoordelijkheden en verplichtingen in geval van verlies van gegevens; ❒ ❒ ❒ ❒
- het bepalen van de eigenaar van gegevens en programmatuur en het vastleggen van de verantwoordelijkheden voor gegevensbeveiliging, auteursrechten van programmatuur en meer van dergelijke overwegingen; ❒ ❒ ❒ ❒
- de technische normen voor het muteren en lezen van gegevens en programmatuur; ❒ ❒ ❒ ❒
- speciale maatregelen om bijzonder gevoelige gegevens te beschermen, bijvoorbeeld door encryptie? ❒ ❒ ❒ ❒

**8.7.2 Beveiliging van media tijdens transport**

1 Wordt er gebruik gemaakt van betrouwbare transport- of koeriersdiensten? ❒ ❒ ❒ ❒

2 Is er een procedure om de identificatie van vervoerders te controleren? ❒ ❒ ❒ ❒

3 Is de verpakking tijdens het transport in overeenstemming met de specificaties van de fabrikant en biedt deze afdoende bescherming tegen fysieke schade die tijdens het transport kan optreden? ❒ ❒ ❒ ❒

4 Zijn er, indien nodig, speciale maatregelen genomen zodat gevoelige informatie niet openbaar kan worden gemaakt of kan worden gewijzigd, zoals:

- het gebruik van afgesloten en zonodig verzegelde containers; ❒ ❒ ❒ ❒
- het achterwege laten van classificatie op de buitenzijde van de verpakking; ❒ ❒ ❒ ❒
- het persoonlijk afleveren van de goederen; ❒ ❒ ❒ ❒
- het gebruik van verpakkingsmateriaal waaraan direct te zien is of iemand geprobeerd heeft het pakket te manipuleren; ❒ ❒ ❒ ❒
- het in uitzonderlijke gevallen opsplitsen van de zending en de verschillende onderdelen apart of op verschillende manieren verzenden? ❒ ❒ ❒ ❒



Zo beantwoorden: ☑

**J**a
**N**ee
**G**edeeltelijk
**O**nbekend

| | | J | N | G | O |
|---|---|---|---|---|---|
| 5 | Worden door de verzender eisen gesteld aan het transport, bijvoorbeeld aan: | | | | |
| | • de verpakkingswijze; | ❒ | ❒ | ❒ | ❒ |
| | • de beveiliging; | ❒ | ❒ | ❒ | ❒ |
| | • de verzenddatum; | ❒ | ❒ | ❒ | ❒ |
| | • de adressering; | ❒ | ❒ | ❒ | ❒ |
| | • de toevoeging van vrachtbrieven, begeleidingsformulieren, overdrachtborderellen, formele overdrachten, enzovoort? | ❒ | ❒ | ❒ | ❒ |
| 6 | Vindt er registratie plaats van ontvangen en verzonden media, zoals: | | | | |
| | • tapes ontvangen van derden; | ❒ | ❒ | ❒ | ❒ |
| | • tapes verzonden naar derden? | ❒ | ❒ | ❒ | ❒ |

**8.7.3 Beveiliging van elektronische handel (e-commerce)**

| | | | | | |
|---|---|---|---|---|---|
| 1 | Is in het beveiligingsbeleid aandacht besteed aan elektronische handel? | ❒ | ❒ | ❒ | ❒ |
| 2 | Zijn in het beveiligingsbeleid overwegingen opgenomen zoals terzake van: | | | | |
| | • authenticatie (welke eisen moeten worden gesteld in de klant/leverancierrelatie over de wijze van verifieren van elkaars identiteit); | ❒ | ❒ | ❒ | ❒ |
| | • autorisatie (wie mag prijzen, handelsdocumenten et cetera autoriseren en hoe weet de handelspartner dat); | ❒ | ❒ | ❒ | ❒ |
| | • vertrouwelijkheid en integriteit (hoe zijn deze aspecten geregeld voor bijvoorbeeld prijsinformatie, kortingsregelingen, order-, betalings- en adresgegevens); | ❒ | ❒ | ❒ | ❒ |
| | • onweerlegbaarheid (zie paragraaf 10.3.4); | ❒ | ❒ | ❒ | ❒ |
| | • verevening (wat is de meest geschikte betalingsvorm teneinde fraude tegen te gaan); | ❒ | ❒ | ❒ | ❒ |
| | • aansprakelijkheid (wie draagt het risico voor frauduleuze transacties)? | ❒ | ❒ | ❒ | ❒ |
| 3 | Zijn er maatregelen getroffen om verminking van de inhoud van berichten tegen te gaan? Bijvoorbeeld: | | | | |
| | • Wordt in het bericht de gebruikte versie van (EDI-) standaards opgenomen? | ❒ | ❒ | ❒ | ❒ |
| | • Wordt gebruik gemaakt van zelfcorrigerende datacommunicatieapparatuur en netwerkprotocollen, controletotalen in het bericht en/of volgordenummers? | ❒ | ❒ | ❒ | ❒ |
| | • Worden er syntaxchecks of waarschijnlijkheidscontroles uitgevoerd? | ❒ | ❒ | ❒ | ❒ |
| | • Vindt encryptie van de berichten plaats? | ❒ | ❒ | ❒ | ❒ |
| 4 | Zijn er maatregelen getroffen om het verlies, het niet-verzenden of vertraging in de bezorging van berichten tegen te gaan? Bijvoorbeeld: | ❒ | ❒ | ❒ | ❒ |
| | • Zijn er procedures met betrekking tot het verzenden van berichten (nummering berichten, aankondiging verzending, verplichte ontvangstbevestiging)? | ❒ | ❒ | ❒ | ❒ |
| | • Zijn er standaards voor namen en adressen? | ❒ | ❒ | ❒ | ❒ |
| | • Vindt er periodiek afstemming plaats tussen de traffic-rapportages van de netwerkleverancier met eigen gegevens (aantallen berichten, bezorgadressen)? | ❒ | ❒ | ❒ | ❒ |
| | • Vindt er monitoring van het lijnverkeer plaats? | ❒ | ❒ | ❒ | ❒ |
| | • Worden er periodiek performance-tests uitgevoerd? | ❒ | ❒ | ❒ | ❒ |
| 5 | Zijn er maatregelen getroffen om de authenticatie van berichten te kunnen vaststellen (bijvoorbeeld een digitale handtekening)? | ❒ | ❒ | ❒ | ❒ |
| 6 | Zijn er maatregelen getroffen om inhoudelijke juistheid van de berichten te waarborgen? | ❒ | ❒ | ❒ | ❒ |



Zo beantwoorden: ☑

**J**a
**N**ee
**G**edeeltelijk
**O**nbekend

| | | J | N | G | O |
|---|---|---|---|---|---|
| 7 | Zijn er maatregelen getroffen om meervoudige verzending te voorkomen? Bijvoorbeeld: | ❒ | ❒ | ❒ | ❒ |
| | • Wordt verzending van een bericht vastgelegd in de statuscode van een bericht? | ❒ | ❒ | ❒ | ❒ |
| | • Vindt bij de ontvanger controle plaats op de meervoudige ontvangst van berichten? | ❒ | ❒ | ❒ | ❒ |
| | • Is er een tijdstempel in het bericht opgenomen? | ❒ | ❒ | ❒ | ❒ |
| | • Wordt re-transmission herkend? | ❒ | ❒ | ❒ | ❒ |
| 8 | Zijn er procecures voor selectie en periodieke evaluatie van netwerkleveranciers en wordt in deze procedures aandacht besteed aan: | | | | |
| | • Service Level Agreement; | ❒ | ❒ | ❒ | ❒ |
| | • onderhoudscontract/de kwaliteit van het technisch support; | ❒ | ❒ | ❒ | ❒ |
| | • beheerprocedures (problem-, change-, operations-, performance-management); | ❒ | ❒ | ❒ | ❒ |
| | • protocol-conversies; | ❒ | ❒ | ❒ | ❒ |
| | • lijnkwaliteit; | ❒ | ❒ | ❒ | ❒ |
| | • koppeling naar andere netwerken; | ❒ | ❒ | ❒ | ❒ |
| | • re-routingsmogelijkheden; | ❒ | ❒ | ❒ | ❒ |
| | • logging van berichten; | ❒ | ❒ | ❒ | ❒ |
| | • aansprakelijkheid; | ❒ | ❒ | ❒ | ❒ |
| | • materiedeskundigheid; | ❒ | ❒ | ❒ | ❒ |
| | • referenties? | ❒ | ❒ | ❒ | ❒ |
| 9 | Zijn er ten aanzien van elektronische handel (schriftelijke) afspraken gemaakt met de handelspartners? | ❒ | ❒ | ❒ | ❒ |
| 10 | Zijn er maatregelen getroffen ter voorkoming van het onbevoegd kennisnemen van berichten door derden, bijvoorbeeld: | ❒ | ❒ | ❒ | ❒ |
| | • afspraken over vertrouwelijkheid van het berichtenverkeer tussen handelspartners en met de netwerkleverancier; | ❒ | ❒ | ❒ | ❒ |
| | • Third Party Mededeling (TPM) over beveiliging bij handelspartners en netwerkleverancier; | ❒ | ❒ | ❒ | ❒ |
| | • encryptie van berichten; | ❒ | ❒ | ❒ | ❒ |
| | • variabele routering van berichten; | ❒ | ❒ | ❒ | ❒ |
| | • hoge transmissiesnelheden; | ❒ | ❒ | ❒ | ❒ |
| | • waarborgen voor het juist bezorgen van berichten; | ❒ | ❒ | ❒ | ❒ |
| | • fysieke beveiligingsmaatregelen? | ❒ | ❒ | ❒ | ❒ |

### 8.7.4 Beveiliging van elektronische post (e-mail)

| | | | | | |
|---|---|---|---|---|---|
| 1 | Bestaat er een beleid voor het gebruik van e-mail, waarin aandacht is besteed aan: | | | | |
| | • de voorwaarden waaronder e-mail mag worden gebruikt; | ❒ | ❒ | ❒ | ❒ |
| | • de attachments die bij een bericht worden meegestuurd; | ❒ | ❒ | ❒ | ❒ |
| | • de kwetsbaarheid van de berichten voor onbevoegde onderschepping of wijziging; | ❒ | ❒ | ❒ | ❒ |
| | • de gevoeligheid voor fouten (bijvoorbeeld foutieve adressering of verzending); | ❒ | ❒ | ❒ | ❒ |
| | • de gevolgen die een andere communicatiemethode kan hebben voor de onderneming (wat is bijvoorbeeld het effect van een snellere verwerking of van de wijziging van de benadering van onderneming-tot-onderneming in een benadering van persoon-tot-persoon); | ❒ | ❒ | ❒ | ❒ |
| | • wettelijke of contractuele voorschriften, de behoefte aan een bewijs van het oorspronkelijke bericht, een verzendbewijs, een bevestiging van aflevering, een ontvangstbewijs en uitsluiting van aansprakelijkheid (disclaimer); | ❒ | ❒ | ❒ | ❒ |
| | • de gevolgen voor de beveiliging als directory-gegevens bekend worden; | ❒ | ❒ | ❒ | ❒ |



Zo beantwoorden: ☑

**J**a
**N**ee
**G**edeeltelijk
**O**nbekend

| | | J | N | G | O |
|---|---|---|---|---|---|
| | • de behoefte aan beveiligingsmaatregelen in verband met de toegangscontrole voor gebruikers op afstand; | ❒ | ❒ | ❒ | ❒ |
| | • het ontbreken van garanties voor beschikbaarheid, integriteit en vertrouwelijkheid in geval van gegevenstransport op externe netwerken (internet)? | ❒ | ❒ | ❒ | ❒ |
| 2 | Is er een beleid vastgesteld met betrekking tot de technische inrichting van e-mail faciliteiten? | ❒ | ❒ | ❒ | ❒ |
| 3 | Omvat dit beleid richtlijnen ten aanzien van het beheer van de technische voorzieningen zoals: | | | | |
| | • toegang tot servers die worden gebruikt voor opslaan van berichten; | ❒ | ❒ | ❒ | ❒ |
| | • faciliteiten voor opmaak, verzending, ontvangst en verwerking van berichten; | ❒ | ❒ | ❒ | ❒ |
| | • beheer van het adresboek; | ❒ | ❒ | ❒ | ❒ |
| | • controle die voor het afleggen van verantwoording wordt uitgevoerd? | ❒ | ❒ | ❒ | ❒ |
| 4 | Is duidelijk welke gegevens via e-mail verstuurd en ontvangen mogen worden? | ❒ | ❒ | ❒ | ❒ |
| 5 | Is duidelijk welke attachments mogen worden geaccepteerd? | ❒ | ❒ | ❒ | ❒ |
| 6 | Zijn er er afspraken gemaakt tussen zender en ontvanger over authenticatie en wederzijdse acceptatie? | ❒ | ❒ | ❒ | ❒ |
| 7 | Is er een adresboek met ontvangers en zenders waarmee afspraken zijn gemaakt over het gebruik van e-mail? | ❒ | ❒ | ❒ | ❒ |
| 8 | Zijn er waarborgen om de gewenste integriteit te handhaven (bijvoorbeeld een hashwaarde opnemen in het bericht)? | ❒ | ❒ | ❒ | ❒ |
| 9 | Zijn er procedures die de beschikbaarheid van e-mail waarborgen (ingebouwde infrastructurele redundantie, storingsmeldingen, onderhoudsschema, enzovoort)? | ❒ | ❒ | ❒ | ❒ |
| 10 | Worden ontvangstbevestigingen gebruikt om de tijdigheid van de communicatie te controleren? | ❒ | ❒ | ❒ | ❒ |
| 11 | Worden (vertrouwelijke) berichten vercijferd? | ❒ | ❒ | ❒ | ❒ |
| 12 | Worden berichten voorzien van een digitale handtekening? | ❒ | ❒ | ❒ | ❒ |
| 13 | Zijn er maatregelen getroffen die het opnieuw/dubbel verzenden van berichten voorkomt (bijvoorbeeld statusindicatie van een bericht, bericht voorzien van een datum, berichten nummeren)? | ❒ | ❒ | ❒ | ❒ |
| 14 | Is er inzicht in de kosten van de verzending van e-mail? | ❒ | ❒ | ❒ | ❒ |
| 15 | Wordt bij externe e-mail gebruik gemaakt van de diensten van een Trusted Third Party (TTP) voor het verkrijgen van een bewijs voor verzenden en ontvangen van een bericht? | ❒ | ❒ | ❒ | ❒ |
| 16 | Zijn er maatregelen getroffen om de (externe) toegang tot het netwerk of computersysteem te beperken (bijvoorbeeld een firewall, terugbelmechanisme, afsluiten van de externe poorten wanneer deze niet worden gebruikt, enzovoort)? | ❒ | ❒ | ❒ | ❒ |
| 17 | Vindt registratie van verzonden en ontvangen berichten plaats? | ❒ | ❒ | ❒ | ❒ |
| 18 | Worden er viruschecks uitgevoerd op inkomende berichten? | ❒ | ❒ | ❒ | ❒ |
| 19 | Zijn afspraken met service providers vastgelegd in een schriftelijke overeenkomst (SLA)? | ❒ | ❒ | ❒ | ❒ |
| | **8.7.5 Beveiliging van elektronische kantoorsystemen** | | | | |
| 1 | Is er een duidelijk beleid voor het verwerken en verzenden van bepaalde gevoelige informatie (bijvoorbeeld geclassificeerde informatie, zie 5.2 'Classificatie van informatie')? | ❒ | ❒ | ❒ | ❒ |
| 2 | Is er een duidelijk beleid en bestaan er duidelijke maatregelen voor het beheer van gemeenschappelijke informatie, bijvoorbeeld het gebruik van elektronische bulletin boards in het bedrijf ? | ❒ | ❒ | ❒ | ❒ |
| 3 | Wordt de toegang tot informatie in elektronische agenda's beperkt tot bepaalde personen (bijvoorbeeld in geval personen die werken aan gevoelige projecten)? | ❒ | ❒ | ❒ | ❒ |



Zo beantwoorden: ☑

**J**a
**N**ee
**G**edeeltelijk
**O**nbekend

| | | J | N | G | O |
|---|---|---|---|---|---|
| 4 | Is voor alle gebruikers duidelijk in welke mate het systeem geschikt is en gebruikt mag worden voor zakelijke toepassingen, zoals orderverwerking of autorisatieprocedures? | ❒ | ❒ | ❒ | ❒ |
| 5 | Is duidelijk vastgelegd welke stafleden (en contractanten of handelspartners) het systeem mogen gebruiken en welke lokaties toegang tot het systeem geven? | ❒ | ❒ | ❒ | ❒ |
| 6 | Worden voorzieningen slechts beschikbaar gesteld aan gebruikers die deze in het kader van hun werkzaamheden nodig hebben? | ❒ | ❒ | ❒ | ❒ |
| 7 | Wordt, indien noodzakelijk, de status van gebruikers (bijvoorbeeld werknemer van het bedrijf of uitzendkracht) opgenomen in bedrijfsgidsen ten behoeve van andere gebruikers? | ❒ | ❒ | ❒ | ❒ |
| 8 | Is een beleid gedefinieerd ten aanzien van het bewaren van informatie in het systeem en het maken van reservekopieën? | ❒ | ❒ | ❒ | ❒ |
| 9 | Zijn er eisen en maatregelen voor uitwijkmogelijkheden? | ❒ | ❒ | ❒ | ❒ |
| 10 | Is er een duidelijk meldpunt voor (beveiligings)incidenten (bijvoorbeeld de helpdesk)? | ❒ | ❒ | ❒ | ❒ |
| 11 | Vindt registratie en beoordeling van problemen met cliënts, servers en de tussenliggende verbindingen plaats? | ❒ | ❒ | ❒ | ❒ |
| 12 | Zijn er voorschriften met betrekking tot de inrichting van een cliënt (werkstation)? | ❒ | ❒ | ❒ | ❒ |
| 13 | Zijn er procedures voor het aanbrengen van wijzigingen: | | | | |
| | • op servers; | ❒ | ❒ | ❒ | ❒ |
| | • op cliënts; | ❒ | ❒ | ❒ | ❒ |
| | • op netwerkcomponenten? | ❒ | ❒ | ❒ | ❒ |
| 14 | Is de gebruikers duidelijk gemaakt wat het risico is van het installeren van niet geautoriseerde programmatuur (zie 12.1.2 ‘Voorkomen van het onrechtmatig kopiëren van programmatuur’)? | ❒ | ❒ | ❒ | ❒ |
| 15 | Vindt registratie en inventarisatie plaats van alle netwerkcomponenten? | ❒ | ❒ | ❒ | ❒ |

**8.7.6 Publiek toegankelijke systemen (WEB-sites)**

| | | | | | |
|---|---|---|---|---|---|
| 1 | Is vastgesteld of de informatie op een voor het brede publiek toegankelijke systeem (met name website) in overeenstemming is met de wetgeving, gedragsregels en andere voorschriften in het rechtsgebied waar het systeem staat opgesteld en/of waar handel wordt gedreven? | ❒ | ❒ | ❒ | ❒ |
| 2 | Is er een formele procedure voor het autoriseren van de informatie voordat die aan het publiek beschikbaar wordt gesteld? | ❒ | ❒ | ❒ | ❒ |
| 3 | Worden programmatuur, gegevens en informatie, die aan het publiek beschikbaar worden gesteld en waarvoor hoge eisen zijn gesteld aan de juistheid (integriteit), afdoende beschermd met maatregelen als digitale handtekeningen? | ❒ | ❒ | ❒ | ❒ |
| 4 | Worden systemen voor elektronisch publiceren van informatie, vooral wanneer die een reactie vragen of een directe invoer van gegevens mogelijk maken, zo zorgvuldig beheerd dat: | | | | |
| | • informatie wordt verzameld volgens de wetgeving voor bescherming van persoonsgegevens; | ❒ | ❒ | ❒ | ❒ |
| | • invoer en verwerking door het publiek toegankelijke systeem juist, volledig en tijdig gebeurt; | ❒ | ❒ | ❒ | ❒ |
| | • gevoelige informatie wordt beschermd tijdens het verzamelen en tijdens opslag; | ❒ | ❒ | ❒ | ❒ |
| | • toegang tot het publiek toegankelijke systeem geen onopzettelijke toegang mogelijk maakt tot de netwerken die ermee zijn verbonden? | ❒ | ❒ | ❒ | ❒ |



Zo beantwoorden: ☑

**J**a
**N**ee
**G**edeeltelijk
**O**nbekend

J N G O

### 8.7.7 Overige vormen van informatieuitwisseling

1 Is het personeel gewezen op de risico's van informatie-overdracht via telefoon, fax of videocommunicatie, zoals:
- afluisteren van telefoongesprekken; ❒ ❒ ❒ ❒
- afluisteren van vertrouwelijke gesprekken in een openbare ruimte; ❒ ❒ ❒ ❒
- inspreken van berichten op een antwoordapparaat; ❒ ❒ ❒ ❒
- personen die zich voordoen als een ander; ❒ ❒ ❒ ❒
- manipulatie van handtekeningen op faxen (bewijskracht); het versturen van faxen naar verkeerd gekozen of verkeerd voorgeprogrammeerde nummers? ❒ ❒ ❒ ❒

## 9 Toegangsbeveiliging

### 9.1.1 Beleid ten aanzien van toegangscontrole

1 Is er op ondernemingsniveau een beleid geformuleerd waaruit blijkt:
- dat de eigenaar van een informatiesysteem verantwoordelijk is voor de toegangsbeveiliging van dat systeem en daarmee voor het toegangsbeleid en de autorisatie van de te verlenen toegangsrechten; ❒ ❒ ❒ ❒
- dat het autoriseren van de toegang tot de systeemsoftware (computers en netwerken) dient plaats te vinden door of namens het management van het computercentrum; ❒ ❒ ❒ ❒
- dat toegangsrechten uitsluitend mogen worden verleend op basis van het principe dat die rechten benodigd zijn voor het uitoefenen van de toegewezen taken; ❒ ❒ ❒ ❒
- welke soort aansluiting op externe netwerken zijn toegestaan; ❒ ❒ ❒ ❒
- welke beveiliging gerealiseerd moet worden bij aansluiting op een extern netwerk? ❒ ❒ ❒ ❒

2 Is in het toegangsbeleid vastgesteld bij welke discipline(s) de uitvoerende taken met betrekking tot het beheer van toegangsrechten (bevoegdhedenbeheer) is belegd? ❒ ❒ ❒ ❒

3 Is er een overzicht van informatiesystemen met hun respectieve eigenaren? ❒ ❒ ❒ ❒

4 Is per informatiesysteem een bevoegdhedenmatrix opgesteld, ofwel: welke toegangsrechten zijn voor welke (groep) subjecten toegestaan inzake welke (groep) objecten? ❒ ❒ ❒ ❒

5 Zijn bij het toewijzen van bevoegdheden de contractuele en wettelijke vereisten in acht genomen ter zake van de toegangsbeveiliging met betrekking tot gegevens en diensten? ❒ ❒ ❒ ❒

6 Wordt in het geval van IT-voorzieningen die algemeen toegankelijk moeten zijn, waar mogelijk gebruik gemaakt van toegangsprofielen? ❒ ❒ ❒ ❒

7 Is de toekenning van toegangsrechten gebaseerd op principes als:
- 'discretionary access control' (eigenaar bepaalt wie toegang heeft tot resources); ❒ ❒ ❒ ❒
- 'mandatory access control' (toegang op basis van classificatie); ❒ ❒ ❒ ❒
- 'niets mag, tenzij'; ❒ ❒ ❒ ❒
- 'protect all' (alle resources dienen beveiligd te zijn); ❒ ❒ ❒ ❒
- 'least privilege principle' (toegangsrechten overeenkomstig takenpakket); ❒ ❒ ❒ ❒
- 'always call' (bij benadering van een resource dient de toegangsbeveiligingssoftware te worden geactiveerd)? ❒ ❒ ❒ ❒

### 9.2.1 Registratie van gebruikers

1 Is er een formele procedure voor het toekennen/registreren van toegangsrechten ten aanzien van IT-voorzieningen? ❒ ❒ ❒ ❒



Zo beantwoorden: ☑

**J**a
**N**ee
**G**edeeltelijk
**O**nbekend

| | | J | N | G | O |
|---|---|---|---|---|---|
| 2 | Wordt in die procecure geregeld dat: | | | | |
| | • toegang pas wordt verleend als de machtigingsprocedure is afgerond; | ❒ | ❒ | ❒ | ❒ |
| | • er een overzicht bijgehouden wordt van functionarissen die opdrachten voor wijzigingen van toegangsrechten mogen autoriseren; | ❒ | ❒ | ❒ | ❒ |
| | • elke wijziging van toegangsrechten wordt teruggekoppeld naar de eigenaar van de betreffende IT-voorzieningen; | ❒ | ❒ | ❒ | ❒ |
| | • periodiek een overzicht wordt vervaardigd (bijvoorbeeld per informatiesysteem) van toegangsrechten van subjecten (voor controle doeleinden); | ❒ | ❒ | ❒ | ❒ |
| | • de eigenaren van IT-voorzieningen periodiek wordt gevraagd om de voor hun IT-voorzieningen geïmplementeerde toegangsrechten, te bekrachtigen; | ❒ | ❒ | ❒ | ❒ |
| | • de gebruikersidentificaties persoonlijk eigendom en uniek zijn? | ❒ | ❒ | ❒ | ❒ |
| 3 | Is er een procedure die voorziet in het verwijderen van toegangsrechten als een gebruiker van functie verandert of het bedrijf verlaat? | ❒ | ❒ | ❒ | ❒ |
| 4 | Is er een procedure die voorziet in het blokkeren van toegangsrechten als een gebruiker langdurig geen gebruik maakt van IT-voorzieningen? | ❒ | ❒ | ❒ | ❒ |
| | **9.2.2 Beheer van speciale bevoegdheden** | | | | |
| 1 | Wordt het gebruik van speciale bevoegdheden beperkt tot een minimum? | ❒ | ❒ | ❒ | ❒ |
| 2 | Worden speciale bevoegdheden uitsluitend toegewezen indien deze vereist zijn voor het uitoefenen van de functie? | ❒ | ❒ | ❒ | ❒ |
| 3 | Wordt het gebruik van bevoegdheden voor speciale werkzaamheden gescheiden van de andere reguliere werkzaamheden (dus een aparte user-ID gebruiken)? | ❒ | ❒ | ❒ | ❒ |
| 4 | Worden speciale bevoegdheden waar mogelijk toegewezen aan geautomatiseerde taken en/of nood-users? | ❒ | ❒ | ❒ | ❒ |
| 5 | Worden speciale bevoegdheden pas ingezet na voorafgaande autorisatie? | ❒ | ❒ | ❒ | ❒ |
| 6 | Wordt het gebruik van speciale bevoegdheden geregistreerd (audittrail) en gecontroleerd? | ❒ | ❒ | ❒ | ❒ |
| | **9.2.3 Beheer van gebruikerswachtwoorden** | | | | |
| 1 | Worden de gebruikers voldoende geïnformeerd over het persoonsgebonden en vertrouwelijke karakter van de aan hen toegewezen toegangsrechten en de daarbij benodigde combinatie van gebruikers-ID en wachtwoord? | ❒ | ❒ | ❒ | ❒ |
| 2 | Worden de gebruikers verplicht om hun persoonlijke wachtwoorden geheim te houden en wordt die verplichting: | | | | |
| | • ofwel opgenomen in de interne bedrijfsregels; | ❒ | ❒ | ❒ | ❒ |
| | • ofwel bevestigd door ondertekening van een schriftelijke verklaring dat zij de condities waaronder zij hun toegangsrechten verkrijgen, begrijpen? | ❒ | ❒ | ❒ | ❒ |
| 3 | Is er voor gezorgd dat een door de beheerder toegekend wachtwoord maar één keer gebruikt kan worden? | ❒ | ❒ | ❒ | ❒ |
| 4 | Is geregeld dat initiële wachtwoorden op een veilige manier aan de betrokken gebruikers worden doorgegeven? | ❒ | ❒ | ❒ | ❒ |
| 5 | Worden wachtwoorden van ‘noodgebruikers’ tijdig vernieuwd? | ❒ | ❒ | ❒ | ❒ |
| 6 | Is het voor het bedrijf op een veilige manier mogelijk om in geval van nood te beschikken over het wachtwoord van de systeembeheerder, ook als die niet aanwezig is? | ❒ | ❒ | ❒ | ❒ |
| 7 | Wordt eventueel gebruik gemaakt van biometrische kenmerken zoals een vingerafdruk of identificatie met behulp van een chipkaart? | ❒ | ❒ | ❒ | ❒ |



Zo beantwoorden: ☑

**J**a
**N**ee
**G**edeeltelijk
**O**nbekend

| | | J | N | G | O |
|---|---|---|---|---|---|
| 8 | Worden wachtwoorden op een veilige manier opgeslagen (bijvoorbeeld met behulp van een 'one-way' encryptiealgoritme)? | ❒ | ❒ | ❒ | ❒ |
| | **9.2.4 Verificatie van toegangsrechten** | | | | |
| 1 | Is er een regelmatige controle op juistheid van de aan gebruikers verleende toegangsrechten? | ❒ | ❒ | ❒ | ❒ |
| 2 | Is er een frequente controle op het beschikbaar stellen en gebruik van speciale bevoegdheden? | ❒ | ❒ | ❒ | ❒ |
| 3 | Zijn de bewaartermijnen voor bevoegdhedenmutaties, bevoegdhedenstanden, audittrails en dergelijke geregeld? | ❒ | ❒ | ❒ | ❒ |
| | **9.3.1 Gebruik van wachtwoorden** | | | | |
| 1 | Worden de gebruikers voldoende geïnformeerd over mogelijke consequenties van onjuist gebruik van toegangsrechten? | ❒ | ❒ | ❒ | ❒ |
| 2 | Worden de gebruikers bewust gemaakt van de gevaren die verbonden zijn aan: | | | | |
| | • het opschrijven van wachtwoorden; | ❒ | ❒ | ❒ | ❒ |
| | • het gebruik van eenvoudig te raden wachtwoorden? | ❒ | ❒ | ❒ | ❒ |
| 3 | Wordt afgedwongen dat een gebruiker zijn wachtwoord periodiek wijzigt en dat daarbij een oud wachtwoord niet opnieuw gebruikt kan worden? | ❒ | ❒ | ❒ | ❒ |
| 4 | Wordt afgedwongen dat een gebruiker zijn tijdelijke wachtwoord wijzigt bij de eerste aanlogprocedure? | ❒ | ❒ | ❒ | ❒ |
| 5 | Wordt de opslag van wachtwoorden in automatische aanlogprocedures verboden/uitgesloten? | ❒ | ❒ | ❒ | ❒ |
| 6 | Zijn er regels met betrekking tot de keuze van wachtwoorden (niet eenvoudig te raden zoals namen, automerken, minimaal zes karakters waaronder ook cijfers en bijzondere tekens)? | ❒ | ❒ | ❒ | ❒ |
| 7 | Worden gebruikers erop gewezen dat zij het wachtwoord moeten wijzigen wanneer er aanwijzingen zijn dat het wachtwoord bekend is bij anderen? | ❒ | ❒ | ❒ | ❒ |
| | **9.3.2 Onbeheerde gebruikersapparatuur** | | | | |
| 1 | Wordt het gebruik van screensavers met wachtwoordbeveiliging toegepast/gestimuleerd? | ❒ | ❒ | ❒ | ❒ |
| 2 | Worden sessies die langer dan een vooraf vastgelegde tijd niet actief zijn, automatisch afgebouwd en uitgelogd? | ❒ | ❒ | ❒ | ❒ |
| 3 | Worden gebruikers bewust gemaakt van de consequenties van het onbeheerd laten van openstaande sessies? | ❒ | ❒ | ❒ | ❒ |
| 4 | Zijn de direct leidinggevenden alert (in het bijzonder bij het gebruik van kritische informatiesystemen) op onbeheerd openstaande sessies? | ❒ | ❒ | ❒ | ❒ |
| 5 | Worden, bij constatering van onbeheerd openstaande sessies, sancties toegepast? | ❒ | ❒ | ❒ | ❒ |
| | **9.4.1 Beleid ten aanzien van het gebruik van netwerkdiensten** | | | | |
| 1 | Is in het beveiligingsbeleid aandacht geschonken aan risico's bij een toegangsbeveiliging van netwerken (bijvoorbeeld 'Beleid externe verbindingen' of 'internetbeleid') en de noodzaak van maatregelen ter bescherming tegen deze risico's? | ❒ | ❒ | ❒ | ❒ |
| 2 | Is de toegang tot netwerkdiensten beperkt tot alleen diegenen die daarvoor geautoriseerd zijn? | ❒ | ❒ | ❒ | ❒ |
| | **9.4.2 Verplichte route** | | | | |
| 1 | Is voorzien in een vaste routering van werkstation naar de computerservice? | ❒ | ❒ | ❒ | ❒ |
| 2 | Wordt gebruik gemaakt van vaste lijnen? | ❒ | ❒ | ❒ | ❒ |



Zo beantwoorden: ☑

**J**a
**N**ee
**G**edeeltelijk
**O**nbekend

| | | J | N | G | O |
|---|---|---|---|---|---|
| 3 | Indien er gebruik wordt gemaakt van kieslijnen, wordt de beller dan teruggebeld voordat er een mogelijkheid ontstaat om in het systeem in te loggen? | ❒ | ❒ | ❒ | ❒ |
| 4 | Wordt gebruik gemaakt van het automatisch verbinden van poorten aan bepaalde toegangssystemen of beveiligings-gateways? | ❒ | ❒ | ❒ | ❒ |
| 5 | Worden menu's (menu-opties) beperkt tot de voor de gebruiker toegestane opties? | ❒ | ❒ | ❒ | ❒ |
| 6 | Wordt ronddwalen in het netwerk voorkomen? | ❒ | ❒ | ❒ | ❒ |
| | **9.4.3 Authenticatie van gebruikers bij externe verbindingen** | | | | |
| 1 | Worden verbindingen die door gebruikers op afstand tot stand worden gebracht via openbare netwerken, geverifieerd en bekrachtigd (inbelvoorzieningen, authenticatie van gebruikers met wachtwoorden, chipcards, enzovoort)? | ❒ | ❒ | ❒ | ❒ |
| 2 | Wordt voor elke soort verbinding het risico voor de organisatie van onterecht gebruik ingeschat en op basis daarvan het verificatieniveau bepaald? | ❒ | ❒ | ❒ | ❒ |
| | **9.4.4 Authenticatie van remote-computers** | | | | |
| 1 | Worden verbindingen die door computers op afstand tot stand worden gebracht via openbare netwerken, geverifieerd en bekrachtigd: | | | | |
| | • op sessie- en lijnniveau (encryptie); | ❒ | ❒ | ❒ | ❒ |
| | • op toepassingsniveau (wachtwoorden, chipcards, enzovoort)? | ❒ | ❒ | ❒ | ❒ |
| | **9.4.5 Beveiliging van op afstand benaderde diagnosepoorten** | | | | |
| 1 | Is in het contract met de externe partij opgenomen welke activiteiten wel/niet zijn toegestaan en welke sancties zijn verbonden aan het niet nakomen van het contract? | ❒ | ❒ | ❒ | ❒ |
| 2 | Is voor elke vorm van remote access vastgesteld welke functionaliteit wordt geboden en wat de daaraan verbonden risico's zijn? | ❒ | ❒ | ❒ | ❒ |
| 3 | Zijn adequate beveiligings- en controlemaatregelen genomen per type remote access (inbelvoorzieningen, authenticatie, logging, enzovoort)? | ❒ | ❒ | ❒ | ❒ |
| 4 | Is de inbelprocedure zodanig opgesteld, dat uitsluitend kan worden ingebeld op initiatief van / met medeweten van de eigenaar/beheerder van de IT-component waarop remote access zal plaatsvinden? | ❒ | ❒ | ❒ | ❒ |
| 5 | Worden de inbelprocedure en inbelvoorziening periodiek op werking getoetst? | ❒ | ❒ | ❒ | ❒ |
| 6 | Wordt het gebruik van diagnosepoorten per gebruikssituatie gecontroleerd door de beheerder van de computerdienst (kan slechts toegang worden verkregen op initiatief/met medeweten van de eigenaar/beheerder van de computerdienst)? | ❒ | ❒ | ❒ | ❒ |
| 7 | Wordt er aan de externe partij een schriftelijke geheimhoudingsverklaring gevraagd? | ❒ | ❒ | ❒ | ❒ |
| | **9.4.6 Scheiding in netwerken** | | | | |
| 1 | Is het interne netwerk zodanig omvangrijk dat het beter gesplitst kan worden in afzonderlijke logische netwerkdomeinen (segmentering), zonodig ondersteund met firewalls ter afscherming van de afzonderlijke domeinen? | ❒ | ❒ | ❒ | ❒ |
| 2 | Is het interne netwerk afdoende beveiligd tegen ongeautoriseerde toegang vanuit externe verbindingen/netwerken. (firewalls, secure gateways, enzovoort)? | ❒ | ❒ | ❒ | ❒ |
| 3 | Is bij de indeling in logische netwerkdomeinen rekening gehouden met het beveiligingsbeleid, het kostenaspect en de performance-eisen? | ❒ | ❒ | ❒ | ❒ |



Zo beantwoorden: ☑

**J**a
**N**ee
**G**edeeltelijk
**O**nbekend

J N G O

**9.4.7 Beheer van netwerkverbindingen**

1 Worden de verbindingsmogelijkheden voor gebruikers binnen het netwerk beperkt tot hetgeen noodzakelijk is voor de betreffende gebruiker? ❒ ❒ ❒ ❒
2 Worden niet toegestane netwerkdiensten adequaat geblokkeerd? ❒ ❒ ❒ ❒
3 Vindt detectie van overtredingen plaats en worden deze voldoende frequent beoordeeld? ❒ ❒ ❒ ❒

**9.4.8 Beheer van netwerkroutering**

1 Wordt netwerkroutering toegepast voor die delen van het netwerk die gemeenschappelijk met anderen gebruikt worden? ❒ ❒ ❒ ❒
2 Zijn de beveiligingsmaatregelen voor netwerkroutering gebaseerd op de controle van bron- en bestemmingsadressen? ❒ ❒ ❒ ❒
3 Is er voldoende kennis aanwezig met betrekking tot de kracht van de gebruikte hulpmiddelen voor adrescontrole (bron- en bestemmingsadres), netwerkadresvertaling en dergelijke? ❒ ❒ ❒ ❒

**9.4.9 Beveiliging van netwerkdiensten**

1 Is nagegaan welke gevolgen het gebruik van externe netwerk-services kan hebben voor de vertrouwelijkheid, integriteit en beschikbaarheid van de getransporteerde data en van de data die zich bevindt op de, aan het netwerk aangesloten, computers? ❒ ❒ ❒ ❒

**9.5.1 Automatische identificatie van werkstations**

1 Wordt automatische identificatie van werkstations toegepast voor toepassingen die alleen vanaf bepaalde werkstations gestart mogen worden? ❒ ❒ ❒ ❒
2 Zijn deze werkstations voorzien van (extra) beperkingen (fysiek of logisch) teneinde de beveiliging ervan te ondersteunen? ❒ ❒ ❒ ❒

**9.5.2 Aanlogprocedures voor werkstations**

1 Wordt in de aanlogprocedure voorkomen dat een onbevoegde gebruiker, via informatie op het aanlogscherm, hulp krijgt bij het aanloggen (ook foutboodschappen mogen potentiële onbevoegde gebruikers geen helpende hand bieden)? ❒ ❒ ❒ ❒
2 Wordt geen informatie verstrekt over de onderneming of het computersysteem voordat de procedure met succes is voltooid? ❒ ❒ ❒ ❒
3 Wordt de waarschuwing gegeven dat toegang uitsluitend is toegestaan voor bevoegde gebruikers? ❒ ❒ ❒ ❒
4 Wordt er bij een fout tijdens de aanlogprocedure geen hulp geboden (onbevoegd gebruik tegengaan)? ❒ ❒ ❒ ❒
5 Wordt de aanlog pas geverifieerd als alle benodigde aanloggegevens zijn ingevoerd? ❒ ❒ ❒ ❒
6 Wordt er geen informatie vertrekt over de juistheid van de afzonderlijke gegevens? ❒ ❒ ❒ ❒
7 Wordt het aantal mislukte aanlogpogingen beperkt (bijvoorbeeld maximaal drie) en wordt na het overschrijden van dit aantal in een extra beperking voorzien? ❒ ❒ ❒ ❒
8 Wordt de discipline, belast met het toegangsbeheer, direct geïnformeerd in geval van overschrijding van het aantal toegestane aanlogpogingen en wordt daar dan ook direct actie door ondernomen? ❒ ❒ ❒ ❒
9 Wordt de tijd om de aanlogprocedure met succes te doorlopen, beperkt? ❒ ❒ ❒ ❒
10 Wordt de gebruiker na een geslaagde aanlogprocedure geïnformeerd over de laatste succesvolle aanlogpoging en over alle mislukte aanlogpogingen sedert de laatste succesvolle poging? ❒ ❒ ❒ ❒



Zo beantwoorden: ☑

**J**a
**N**ee
**G**edeeltelijk
**O**nbekend

J N G O

### 9.5.3 Gebruikersidentificatie en authenticatie

1 Wordt er gebruik gemaakt van unieke gebruikersidentificaties per afzonderlijke gebruiker, zodat activiteiten herleid kunnen worden tot individuele personen? ❒ ❒ ❒ ❒
2 Wordt, indien in uitzonderlijke gevallen het gebruik van een groepsidentificatie noodzakelijk is, een formele goedkeuringsprocedure gevolgd? ❒ ❒ ❒ ❒
3 Geven de gebruikersidentificaties geen inzicht in de bevoegdheid van een persoon? ❒ ❒ ❒ ❒
4 Worden gebruikers geïdentificeerd aan de hand van biometrische kenmerken en/of het bezit van een specifieke fysieke sleutel (bijvoorbeeld een chipcard)? ❒ ❒ ❒ ❒
5 Is iedere gebruiker geattendeerd op de gevaren die verbonden zijn aan het gebruik van zijn gebruikersidentificatie door anderen? ❒ ❒ ❒ ❒
6 Is in de richtlijnen vastgelegd dat het ‘uitlenen’ van gebruikersidentificaties verboden is? ❒ ❒ ❒ ❒

### 9.5.4 Wachtwoordbeheersysteem

1 Is het voor de gebruiker mogelijk om zelf zijn wachtwoord te wijzigen? ❒ ❒ ❒ ❒
2 Is bij wijziging voorzien in een controlemogelijkheid (dubbel toetsen) om te controleren of het wachtwoord juist is ingetoetst? ❒ ❒ ❒ ❒
3 Wordt gebruik gemaakt van éénrichtingencryptie bij de vastlegging en transport van wachtwoorden? ❒ ❒ ❒ ❒
4 Wordt het gebruik van eenvoudig raadbare wachtwoorden voorkomen? ❒ ❒ ❒ ❒
5 Wordt regelmatige wijziging van het wachtwoord afgedwongen? ❒ ❒ ❒ ❒
6 Wordt hergebruik van wachtwoorden voorkomen? ❒ ❒ ❒ ❒
7 Wordt voorkomen dat een wachtwoord ooit leesbaar wordt gemaakt (ook niet tijdens transport over netwerken)? ❒ ❒ ❒ ❒
8 Is een minimale lengte en een bepaalde syntax voor wachtwoorden afgedwongen? ❒ ❒ ❒ ❒
9 Worden wachtwoorden gescheiden van de programmatuur opgeslagen? ❒ ❒ ❒ ❒

### 9.5.5 Gebruik van systeemhulpmiddelen

1 Is voor elk systeemhulpmiddel vastgesteld en vastgelegd wie wanneer welk hulpmiddel mag gebruiken en wie dit gebruik vooraf dient te autoriseren? ❒ ❒ ❒ ❒
2 Wordt de toegang tot systeemhulpmiddelen beperkt door specifieke wachtwoordbeveiliging? ❒ ❒ ❒ ❒
3 Worden systeemhulpmiddelen en toepassingsprogrammatuur van elkaar gescheiden gehouden? ❒ ❒ ❒ ❒
4 Wordt het gebruik van systeemhulpmiddelen beperkt tot een klein aantal vertrouwde en opgeleide gebruikers? ❒ ❒ ❒ ❒
5 Wordt de beschikbaarheid van systeemhulpmiddelen in de tijd beperkt? ❒ ❒ ❒ ❒
6 Wordt het gebruik van systeemhulpmiddelen gelogd? ❒ ❒ ❒ ❒
7 Worden de logs gecontroleerd en inhoudelijk aangesloten met de geautoriseerde aanvragen voor het gebruik van systeemhulpmiddelen? ❒ ❒ ❒ ❒
8 Worden software tools en systeemsoftware die niet strict nodig zijn, steeds verwijderd? ❒ ❒ ❒ ❒

### 9.5.6 Stil alarm ter bescherming van gebruikers

1 Wordt het gebruik van een stil alarm (om onder dwang verkregen toegang te signaleren) toegepast voor gebruikers die het risico lopen het doelwit te worden van dwang? ❒ ❒ ❒ ❒
2 Zijn de acties die als reactie op een stil alarm worden genomen bij zowel de gebruikers als de discipline die moet reageren op het alarm, duidelijk vastgelegd? ❒ ❒ ❒ ❒
3 Worden stil-alarm-procedures periodiek getest? ❒ ❒ ❒ ❒



Zo beantwoorden: ☑

**J**a
**N**ee
**G**edeeltelijk
**O**nbekend

J N G O

**9.5.7 Time-out voor werkstations**

1 Wordt gebruik gemaakt van een screensaver met wachtwoord beveiliging en/of een voorziening die de programma- en netwerksessies na een vooraf bepaalde tijd van inactiviteit afsluit? ❒ ❒ ❒ ❒

**9.5.8 Beperking van verbindingstijd**

1 Wordt gebruik gemaakt van bepaalde perioden waarin een verbinding mag bestaan? ❒ ❒ ❒ ❒

**9.6.1 Beperking van toegang tot informatie**

1 Is door/namens de eigenaar van de applicatie, inzake de toegang tot de gegevens, een bevoegdhedenmatrix opgesteld? ❒ ❒ ❒ ❒

2 Zijn er voorzieningen beschikbaar die het mogelijk maken voor de gegevensbeheerder om de toegang tot de gegevens in te voeren conform de opgestelde bevoegdhedenmatrices? ❒ ❒ ❒ ❒

3 Is het daarbij mogelijk om de toegangsrechten te differentiëren naar lezen, schrijven, wijzigen, uitvoeren, enzovoort? ❒ ❒ ❒ ❒

4 Is het in een multi-user-situatie onmogelijk om gegevens van twee gebruikers te vermengen bij nieuwe invoer en wijzigingen? ❒ ❒ ❒ ❒

5 Is toegang tot de gegevensbestanden alleen mogelijk door middel van de geautoriseerde programmatuur? ❒ ❒ ❒ ❒

6 Wordt gebruik gemaakt van menu's om de toegang tot functies te beperken? ❒ ❒ ❒ ❒

7 Wordt informatie over gegevens en/of functies waarvoor gebruikers geen toegang hebben, beperkt? ❒ ❒ ❒ ❒

8 Wordt restrictief omgegaan met het verstrekken van informatie over/uit een informatiesysteem aan gebruikers die geen toegang hebben tot dat systeem? ❒ ❒ ❒ ❒

9 Wordt de uitvoer van toepassingen waarin vertrouwelijke gegevens voorkomen, regelmatig beoordeeld op het voorkomen van overbodige vertrouwelijke gegevens? ❒ ❒ ❒ ❒

10 Worden vertrouwelijke gegevens tijdens transport beveiligd door middel van encryptie? ❒ ❒ ❒ ❒

11 Zijn in query-hulpmiddelen de functies update en delete uitgeschakeld? ❒ ❒ ❒ ❒

**9.6.2 Isolatie van gevoelige systemen**

1 Is de gevoeligheid van een informatiesysteem bepaald door de eigenaar daarvan? ❒ ❒ ❒ ❒

2 Wordt door de eigenaar van het gevoelige informatiesysteem, het gebruik in een gemeenschappelijke omgeving beoordeeld en goedgekeurd? ❒ ❒ ❒ ❒

3 Zijn kritische informatiesystemen zonodig geïmplementeerd in een separaat verwerkingsdomein? ❒ ❒ ❒ ❒

**9.7.1 Vastlegging van beveiligingsrelevante gebeurtenissen ("event-logging")**

1 Worden uitzonderingen en andere bijzondere gebeurtenissen vastgelegd en gedurende een overeengekomen periode bewaard ter ondersteuning van toekomstig onderzoek? ❒ ❒ ❒ ❒

2 Worden deze vastleggingen op een veilige manier bewaard? ❒ ❒ ❒ ❒

3 Bevatten de logs tenminste de volgende gegevens:

- user-identificatie; ❒ ❒ ❒ ❒
- datum en tijd van log in en log off; ❒ ❒ ❒ ❒
- identificatie van de gebruikte terminal of lokatie; ❒ ❒ ❒ ❒
- (geweigerde) toegangsbenaderingen van bestanden, jobs, transacties? ❒ ❒ ❒ ❒



Zo beantwoorden: ☑

**J**a
**N**ee
**G**edeeltelijk
**O**nbekend

J N G O

### 9.7.2 Monitoring van systeemgebruik

1 Zijn er procedures opgesteld voor het analyseren van het systeemgebruik ten einde vast te kunnen stellen dat gebruikers uitsluitend handelingen verrichten waarvoor zij zijn geautoriseerd? ❒ ❒ ❒ ❒

2 Is de mate van bewaking van het systeemgebruik vastgesteld door middel van een risico-inventarisatie? ❒ ❒ ❒ ❒

3 Zijn daarbij de volgende risicogebieden onderkend:

- toegestaan gebruik voorzover het wijzigingen in kritische bestanden betreft; waarbij geregistreerd wordt: de gebruikersnaam (user-ID), datum en tijd van de gebeurtenis, het soort gebeurtenis, de benaderde bestanden, de daarbij gebruikte programma's en/of hulpmiddelen; ❒ ❒ ❒ ❒
- gebruik van speciale bevoegdheden, zoals het gebruik van de account van de systeembeheerder ('Root', 'System', 'Special', en dergelijke) en het gebruik van nood-users, het opstarten en stoppen van het systeem, het koppelen van in- en uitvoerapparatuur; ❒ ❒ ❒ ❒
- registratie van pogingen tot het verkrijgen van onbevoegde toegang, zoals meldingen van gateways en firewalls, waarschuwingen van detectiesystemen enzovoort; ❒ ❒ ❒ ❒
- foutmeldingen/boodschappen en alarmen van het console, uitzonderingen in de systeemlog, alarm van het netwerkbesturingssysteem? ❒ ❒ ❒ ❒

4 Wordt het resultaat van de analyse van het systeemgebruik regelmatig beoordeeld? ❒ ❒ ❒ ❒

5 Is die regelmaat in overeenstemming met het onderkende risico? ❒ ❒ ❒ ❒

6 Wordt rekening gehouden met de volgende risico's:

- de afhankelijkheid van de applicatie; ❒ ❒ ❒ ❒
- de waarde, gevoeligheid en de afhankelijkheid van de betrokken informatie; ❒ ❒ ❒ ❒
- de recente ervaringen met misbruik of infiltratie in het systeem; ❒ ❒ ❒ ❒
- de mate waarin het systeem verbonden is met andere netwerken, vooral publiek toegankelijke netwerken? ❒ ❒ ❒ ❒

7 Bestaat bij de analyse van het systeemgebruik inzicht in de bedreigingen voor het systeem en in welke situaties deze zich kunnen voordoen? ❒ ❒ ❒ ❒

8 Is bekend wanneer een nader onderzoek nodig is naar gebeurtenissen in het geval van een beveiligingsincident? ❒ ❒ ❒ ❒

9 Wordt gebruik gemaakt van hulpmiddelen om bestanden te analyseren met gegevens over het systeemgebruik, waarbij alleen de relevante gegevens voor de beveiliging worden geselecteerd? ❒ ❒ ❒ ❒

10 Indien die hulpmiddelen worden gebruikt, wordt het onderzoek dan altijd verricht op een kopie van het oorspronkelijke bestand? ❒ ❒ ❒ ❒

11 Zijn voor die hulpmiddelen geen zware bevoegdheden nodig, waarmee onopzettelijk bestanden of programmatuur kan worden verminkt? ❒ ❒ ❒ ❒

12 Bestaat er een controletechnische functiescheiding tussen de medewerker die het systeemgebruik controleert en de medewerker van wie de activiteiten worden beoordeeld? ❒ ❒ ❒ ❒

13 Wordt bijzondere aandacht besteed aan de beveiliging van het bestand met de gegevens over het systeemgebruik (immers manipulatie van dit bestand leidt tot een onterecht gevoel van veiligheid)? ❒ ❒ ❒ ❒

14 Zijn de beheersmaatregelen er op gericht dat de vastgelegde gegevens worden beschermd tegen ongeautoriseerde wijzigingen en operationele problemen waaronder:

- het aan- en uitzetten van het vastleggingsmechanisme; ❒ ❒ ❒ ❒
- wijzigingen in de soorten boodschappen, die vastgelegd worden; ❒ ❒ ❒ ❒
- bestanden met gegevens over systeemgebruik die worden gewijzigd of weggegooid; ❒ ❒ ❒ ❒



Zo beantwoorden: ☑

**J**a
**N**ee
**G**edeeltelijk
**O**nbekend

| | | J | N | G | O |
|---|---|---|---|---|---|
| | • het vollopen van informatiedragers, waardoor gegevens niet meer worden vastgelegd of slechts worden vastgelegd over andere gegevens heen? | ❒ | ❒ | ❒ | ❒ |
| | **9.7.3 Synchronisatie van systeemklokken** | | | | |
| 1 | Worden systeemklokken regelmatig gesynchroniseerd teneinde de integriteit van logs te waarborgen? | ❒ | ❒ | ❒ | ❒ |
| 2 | Worden de systeemklokken tijdig correct ingesteld bij overgang van zomer- naar wintertijd en omgekeerd? | ❒ | ❒ | ❒ | ❒ |
| | **9.8.1 Mobiele computers** | | | | |
| 1 | Is er bij het gebruik van mobiele computers aandacht voor extra bewustwording bij de gebruikers van de risico's verbonden aan het gebruik en mogelijk verlies van een portable pc? | ❒ | ❒ | ❒ | ❒ |
| 2 | Vindt er een frequente inventarisatie plaats van de hard- en software? | ❒ | ❒ | ❒ | ❒ |
| 3 | Wordt er aandacht gegeven aan een goede en actuele virusbeveiliging? | ❒ | ❒ | ❒ | ❒ |
| 4 | Is er een procedure waarin de voorgaande punten worden beschreven en waaraan de gebruiker zich (schriftelijk) committeert? | ❒ | ❒ | ❒ | ❒ |
| 5 | Wordt de vaste schijf van mobiele computers volledig geëncrypt, en is er voor decryptie behalve een wachtwoord ook een fysiek of biometrisch token nodig? | ❒ | ❒ | ❒ | ❒ |
| 6 | Is voorzien in snelle en gemakkelijke back-up-hulpmiddelen voor de veiligstelling van de opgeslagen gegevens en zijn de veiliggestelde gegevens beschermd tegen bijvoorbeeld diefstal? | ❒ | ❒ | ❒ | ❒ |
| 7 | Zijn er voorschriften voor het gebruik van mobiele computers in het netwerk? | ❒ | ❒ | ❒ | ❒ |
| 8 | Worden gebruikers geattendeerd op de extra risico's van het gebruik van mobiele computers in openbare ruimten? | ❒ | ❒ | ❒ | ❒ |
| 9 | Worden 'thuiswerkers' bewust gemaakt van het risico van gevoelige gegevens op de vaste schijf van de thuis-pc? | ❒ | ❒ | ❒ | ❒ |
| 10 | Wordt er voorzien in toegangscontrole en adequate virusdetectie op thuis-pc's? | ❒ | ❒ | ❒ | ❒ |
| 11 | Wordt er aangedrongen op een veilige bewaarplaats (in de kantooromgeving) voor de (thuis)pc tijdens langdurige afwezigheid? | ❒ | ❒ | ❒ | ❒ |
| | **9.8.2 Telewerken** | | | | |
| 1 | Zijn op de thuiswerkplek passend meubilair en opbergmogelijkheden beschikbaar? | ❒ | ❒ | ❒ | ❒ |
| 2 | Zijn er richtlijnen voor het gebruik van informatie en apparatuur door familie/bezoekers? | ❒ | ❒ | ❒ | ❒ |
| 3 | Zijn er procedures met betrekking tot onderhoud van hard- en software en hulp bij het gebruik? | ❒ | ❒ | ❒ | ❒ |
| 4 | Zijn er richtlijnen met betrekking tot de fysieke beveiliging van de werkplek? | ❒ | ❒ | ❒ | ❒ |
| 5 | Zijn inbelvoorzieningen voorzien van terugbelconstructies, een firewall, authenticatiemechanisme en encryptie van de verbindingen? | ❒ | ❒ | ❒ | ❒ |
| 6 | Wordt een uitgeleende pc na terugbezorging expliciet geschoond en nagekeken op virussen? | ❒ | ❒ | ❒ | ❒ |
| 7 | Zijn er richtlijnen voor de telewerker met betrekking tot: | | | | |
| | • het soort werk dat gedaan mag worden; | ❒ | ❒ | ❒ | ❒ |
| | • de uren waarop gewerkt mag worden; | ❒ | ❒ | ❒ | ❒ |
| | • de classificatie van de informatie die op de pc bewaard mag worden? | ❒ | ❒ | ❒ | ❒ |



Zo beantwoorden: ☑

**J**a
**N**ee
**G**edeeltelijk
**O**nbekend

J N G O

## 10 Ontwikkeling en onderhoud van systemen

### 10.1.1 Analyse en specificatie van beveiligingseisen

1 Is er tijdens de definitiestudie/het ontwerpen van nieuwe systemen of releases van bestaande systemen een analyse gemaakt van de beveiligingseisen? ❒ ❒ ❒ ❒

2 Is bij de definitie van beveiligingseisen naast de geautomatiseerde (ingebouwde) maatregelen ook aandacht besteed aan 'handmatige' maatregelen (procedures)? ❒ ❒ ❒ ❒

3 Zijn er eisen geformuleerd ten aanzien van de waarborging van vertrouwelijkheid, integriteit en beschikbaarheid van de informatievoorziening? ❒ ❒ ❒ ❒

4 Zijn er eisen geformuleerd ten aanzien van het voorkomen, opsporen en herstellen van storingen en incidenten? ❒ ❒ ❒ ❒

5 Zijn de beveiligingseisen gedefinieerd in alle relevante documentatie? ❒ ❒ ❒ ❒

6 Is bij de analyse van de beveiligingseisen aandacht gegeven aan:

- logische toegangsbeveiliging; ❒ ❒ ❒ ❒
- gegevens encryptie; ❒ ❒ ❒ ❒
- het maken van reservekopieën; ❒ ❒ ❒ ❒
- interne en externe uitwijkvoorzieningen; ❒ ❒ ❒ ❒
- registratie van bijzondere gebeurtenissen (audittrails); ❒ ❒ ❒ ❒
- mogelijkheden om de integriteit van vitale gegevens te controleren en te beschermen; ❒ ❒ ❒ ❒
- het voldoen aan wettelijke/contractuele vereisten; ❒ ❒ ❒ ❒
- het voorkomen van ongeautoriseerde wijzigingen; ❒ ❒ ❒ ❒
- de (mogelijk negatieve) impact op de werking (van de beveiliging) van bestaande systemen? ❒ ❒ ❒ ❒

### 10.2.1 Validatie van invoergegevens

1 Worden invoercontroles toegepast met betrekking tot:

- de geldigheid van waarden, zowel ten aanzien van het waardenbereik als in relatie tot andere vastgelegde gegevens; ❒ ❒ ❒ ❒
- ontbrekende of onvolledige gegevens? ❒ ❒ ❒ ❒

2 Worden deze controles toegepast op zowel de normale invoergegevens als op tabellen en besturingsparameters? ❒ ❒ ❒ ❒

3 Worden invoerdocumenten gecontroleerd op de geldigheid ervan, zijn bijvoorbeeld geen ongeautoriseerde wijzigingen aangebacht? ❒ ❒ ❒ ❒

4 Zijn er procedures beschreven voor de correctie van fouten in de invoer? ❒ ❒ ❒ ❒

5 Is vastgesteld en vastgelegd wie welke gegevens mag invoeren? ❒ ❒ ❒ ❒

### 10.2.2 Validatie van de interne gegevensverwerking

1 Worden totalen van batches en/of sessies vastgelegd en vergeleken met vorige waarden? ❒ ❒ ❒ ❒

2 Wordt een mutatieoverzicht afgedrukt en worden de aantallen vergeleken met vooraf gemaakte tellingen? ❒ ❒ ❒ ❒

3 Is er een mogelijkheid om een vierkantstelling te maken? ❒ ❒ ❒ ❒

4 Wordt er, indien gegevens op een andere computer ingevoerd worden, nogmaals een controle uitgevoerd door de centrale verwerkingscomputer? ❒ ❒ ❒ ❒

5 Wordt er een geldigheidscontrole uitgevoerd op de door het systeem gegenereerde gegevens? ❒ ❒ ❒ ❒



Zo beantwoorden: ☑

**J**a
**N**ee
**G**edeeltelijk
**O**nbekend

| | | J | N | G | O |
|---|---|---|---|---|---|
| 6 | Wordt zonodig van kritieke gegevensvelden de stand aan het begin van de verwerkingscyclus vergeleken met de stand aan het einde van de vorige verwerkingscyclus? | ❒ | ❒ | ❒ | ❒ |
| 7 | Wordt er gebruik gemaakt van controle door middel van berekening en vergelijking van hash totals over de belangrijke bestanden/bestandsgegevens? | ❒ | ❒ | ❒ | ❒ |
| 8 | Zijn er controles op de juistheid van het verwerkingstijdstip? | ❒ | ❒ | ❒ | ❒ |
| 9 | Zijn er waarborgen voor een correcte volgorde voor het uitvoeren van programma's/jobs? | ❒ | ❒ | ❒ | ❒ |
| 10 | Zijn er procedures voor het adequaat afhandelen van niet normaal beëindigde programma's/jobs (signaleren, analyseren en herstellen van fouten; op juiste wijze herstarten programma/job)? | ❒ | ❒ | ❒ | ❒ |
| | **10.2.3 Authenticatie van berichten** | | | | |
| 1 | Is bekend van welke gegevens die op elektronische wijze worden verzonden, de integriteit vast moet staan? | ❒ | ❒ | ❒ | ❒ |
| 2 | Zo ja, wordt voor de verzending van berichten gebruik gemaakt van cryptografische technieken, zodat de authenticiteit ervan kan worden vastgesteld? | ❒ | ❒ | ❒ | ❒ |
| 3 | Is een risico-inventarisatie uitgevoerd om vast te stellen of controle op de authenticiteit van het bericht is vereist? | ❒ | ❒ | ❒ | ❒ |
| 4 | Is daarbij ook onderzocht welke methode het meest geschikt is voor de implementatie van die controle? | ❒ | ❒ | ❒ | ❒ |
| 5 | Wordt bij die methode gebruik gemaakt van erkende normen en standaarden (ISO) voor de vaststelling van de authenticiteit? | ❒ | ❒ | ❒ | ❒ |
| 6 | Zijn de gebruikte cryptografische algoritmes of technieken voldoende veilig voor de gewenste toepassing? | ❒ | ❒ | ❒ | ❒ |
| 7 | Is de apparatuur voor het gebruik van cryptografie in een beveiligde ruimte geplaatst, zodat deze niet kan worden bereikt door onbevoegden? | ❒ | ❒ | ❒ | ❒ |
| | **10.2.4 Validatie van uitvoergegevens** | | | | |
| 1 | Bevatten applicaties ingebouwde waarschijnlijkheidscontroles, waarmee de geldigheid van de waarden van de uitvoergegevens kan worden getest? | ❒ | ❒ | ❒ | ❒ |
| 2 | Zijn er vierkantstellingen in de applicaties ingebouwd om de volledigheid van de verwerking vast te kunnen stellen? | ❒ | ❒ | ❒ | ❒ |
| 3 | Biedt de uitvoer voldoende zekerheid voor de lezer (of de daaropvolgende applicatie) om de nauwkeurigheid, volledigheid, juistheid en classificatie van de informatie vast te kunnen stellen? | ❒ | ❒ | ❒ | ❒ |
| 4 | Bestaan er procedures, waarmee kan worden gereageerd op de resultaten van de controle van de uitvoergegevens? | ❒ | ❒ | ❒ | ❒ |
| 5 | Zijn de verantwoordelijkheden van alle betrokkenen bij de verwerking van de uitvoergegevens bekend? | ❒ | ❒ | ❒ | ❒ |
| | **10.3.1 Beleid ten aanzien van het gebruik van cryptografische beveiliging** | | | | |
| 1 | Is er een risico-inventarisatie uitgevoerd waarbij het gewenste niveau van de bescherming van de informatie is vastgesteld? | ❒ | ❒ | ❒ | ❒ |
| 2 | Wordt aan de hand van die risico-inventarisatie bepaald of cryptografie nuttig kan worden toegepast, op welke wijze en voor welk doel of voor welk bedrijfsproces? | ❒ | ❒ | ❒ | ❒ |
| 3 | Is in de onderneming een beleid vastgesteld voor het gebruik van cryptografie? | ❒ | ❒ | ❒ | ❒ |
| 4 | Weet men in de onderneming op alle niveaus van leidinggeven, dat met een beleid inzake cryptografie maximale voordelen kunnen worden behaald tegen minimale risico's? | ❒ | ❒ | ❒ | ❒ |



Zo beantwoorden: ☑

**J**a
**N**ee
**G**edeeltelijk
**O**nbekend

| | | J | N | G | O |
|---|---|---|---|---|---|
| 5 | Is bij het ontwikkelen van dat beleid rekening gehouden met de volgende elementen: | | | | |
| | • de aandacht van de leiding van de onderneming voor het gebruik van cryptografische hulpmiddelen, waarin begrepen de uitgangspunten voor de bescherming van bedrijfsinformatie; | ❒ | ❒ | ❒ | ❒ |
| | • de aandacht voor het beheer van de cryptografische sleutels, waarin begrepen het terug kunnen lezen van versleutelde informatie in geval van verloren, uitgelekte of beschadigde sleutels; | ❒ | ❒ | ❒ | ❒ |
| | • de taken en verantwoordelijkheden voor het beheer van de cryptografische sleutels, waarin begrepen de implementatie van het beleid inzake cryptografie; | ❒ | ❒ | ❒ | ❒ |
| | • de vaststelling van het gewenste niveau van cryptografische bescherming; | ❒ | ❒ | ❒ | ❒ |
| | • de standaarden die binnen de gehele onderneming toegepast moeten worden voor een effectieve implementatie per bedrijfsproces? | ❒ | ❒ | ❒ | ❒ |
| | **10.3.2 Versleuteling (encryptie)** | | | | |
| 1 | Wordt encryptie toegepast ter bescherming van vertrouwelijke of geheime informatie? | ❒ | ❒ | ❒ | ❒ |
| 2 | Wordt de mate van bescherming vastgesteld door middel van een risico-inventarisatie, waarbij type en kwaliteit van het cryptografische algoritme alsmede de lengte van de cryptografische sleutels worden meegewogen? | ❒ | ❒ | ❒ | ❒ |
| 3 | Wordt bij invoering van encryptie rekening gehouden met de nationale en internationale wet- en regelgeving, vooral bij grensoverschrijdend netwerkverkeer? | ❒ | ❒ | ❒ | ❒ |
| 4 | Is specialistisch advies ingewonnen voor het vaststellen van het gewenste niveau van bescherming, de selectie van daarvoor geschikte producten en de invoering van een veilig systeem voor sleutelbeheer? | ❒ | ❒ | ❒ | ❒ |
| 5 | Is zo nodig aanvullend juridisch advies ingewonnen, waarbij het gebruik van encryptie wordt getoetst aan wet- en regelgeving? | ❒ | ❒ | ❒ | ❒ |
| | **10.3.3 Digitale handtekeningen** | | | | |
| 1 | Vereist de bescherming van de authenticiteit en de integriteit van elektronische documenten het gebruik van digitale handtekeningen? | ❒ | ❒ | ❒ | ❒ |
| 2 | Is het nodig om de persoon vast te kunnen stellen die het elektronisch document heeft ondertekend en om vast te stellen of de inhoud van het ondertekende document is veranderd? | ❒ | ❒ | ❒ | ❒ |
| 3 | Wordt een asymmetrisch algoritme gebruikt, dat wil zeggen een methodiek waarbij de handtekening door de verzender wordt geplaatst met de private sleutel en de handtekening door de ontvanger wordt gecontroleerd met de publieke sleutel? | ❒ | ❒ | ❒ | ❒ |
| 4 | Zijn er afdoende maatregelen genomen om de private sleutel geheim te houden voor anderen dan de verzender? | ❒ | ❒ | ❒ | ❒ |
| 5 | Is de integriteit van de publieke sleutel voldoende beschermd door middel van een certificaat? | ❒ | ❒ | ❒ | ❒ |
| 6 | Is het gebruikte type algoritme voor de digitale handtekening voldoende sterk en is de sleutellengte voldoende sterk voor de duur van de archivering van de digitale handtekening? | ❒ | ❒ | ❒ | ❒ |
| 7 | Worden voor de digitale handtekening andere sleutels gebruikt dan die voor de encryptie? | ❒ | ❒ | ❒ | ❒ |
| 8 | Is de juridische bewijskracht van de digitale handtekening onderzocht? | ❒ | ❒ | ❒ | ❒ |
| 9 | Zijn er, voor het geval dat de wetgeving onvoldoende aanknopingspunten biedt, in het contract of aanvullende overeenkomst bepalingen opgenomen inzake de bewijskracht van de digitale handtekening? | ❒ | ❒ | ❒ | ❒ |
| 10 | Is voorafgaand aan het gebruik van digitale handtekeningen extern juridisch advies ingewonnen? | ❒ | ❒ | ❒ | ❒ |



Zo beantwoorden: ☑

**J**a
**N**ee
**G**edeeltelijk
**O**nbekend

J N G O

### 10.3.4 Onweerlegbaarheid

1 Is op grond van de risico-inventarisatie vastgesteld dat er geschillen kunnen ontstaan over gebeurtenissen of handelingen, zoals een geschil over een digitale handtekening onder een elektronisch contract of elektronische betalingsopdracht? ❒ ❒ ❒ ❒

2 Is het nodig om onomstotelijk vast te kunnen stellen dat een bericht door de verzender is verzonden en door de ontvanger is ontvangen? ❒ ❒ ❒ ❒

3 Wordt voor de vaststelling van de onweerlegbaarheid gebruik gemaakt van voldoende veilige cryptografische technieken, zoals de digitale handtekening of encryptie? ❒ ❒ ❒ ❒

### 10.3.5 Sleutelbeheer

1 Is het sleutelbeheer binnen de onderneming geregeld voor de volgende algemene cryptografische technieken:
- symmetrisch algoritme met een paar geheime sleutels; ❒ ❒ ❒ ❒
- asymmetrisch algoritme met een private sleutel en een publieke sleutel? ❒ ❒ ❒ ❒

2 Zijn de geheime en private sleutels beschermd tegen ongeautoriseerde inzage? ❒ ❒ ❒ ❒

3 Zijn alle sleutels beschermd tegen wijziging of vernietiging? ❒ ❒ ❒ ❒

4 Is de apparatuur waarmee sleutels worden aangemaakt, verwerkt, tijdelijk opgeslagen of gearchiveerd, fysiek beveiligd tegen ongeautoriseerde inzage? ❒ ❒ ❒ ❒

5 Is die apparatuur geplaatst in een extra beveiligde ruimte? ❒ ❒ ❒ ❒

6 Wordt bij de selectie van die apparatuur als voorwaarde gesteld dat deze moet voldoen aan internationale of nationale normen? ❒ ❒ ❒ ❒

7 Is de apparatuur gecertificeerd door onafhankelijke en deskundige instituten? ❒ ❒ ❒ ❒

8 Past de apparatuur in de architectuur van het netwerk en de computersystemen? ❒ ❒ ❒ ❒

9 Kan een persoon nooit inzage krijgen in cryptografische sleutels door deze:
- in klare taal slechts op te slaan in beveiligde apparatuur; ❒ ❒ ❒ ❒
- uitsluitend vercijferd op te slaan op electronische informatiedragers; ❒ ❒ ❒ ❒
- in klare tekst slechts in gedeelten op te slaan op sleutelbrieven? ❒ ❒ ❒ ❒

10 Is voor het sleutelbeheer gebruik gemaakt van internationaal overeengekomen standaarden, procedures en werkwijzen voor:
- aanmaak van sleutels voor verschillende cryptografische systemen en toepassingssystemen; ❒ ❒ ❒ ❒
- aanmaak en ontvangst van certificaten op basis van de publieke sleutel; ❒ ❒ ❒ ❒
- sleuteldistributie naar gebruikers, met beschrijving hoe de sleutels na ontvangst kunnen worden geactiveerd; ❒ ❒ ❒ ❒
- opslag van sleutels, met beschrijving hoe geautoriseerde gebruikers toegang kunnen krijgen tot hun sleutels; ❒ ❒ ❒ ❒
- verandering of vernieuwing van sleutels met richtlijnen, voor wanneer en hoe sleutels moeten worden gewijzigd; ❒ ❒ ❒ ❒
- hoe om te gaan met gekraakte sleutels; ❒ ❒ ❒ ❒
- inname van sleutels, met beschrijving hoe sleutels moeten worden ingetrokken of onbruikbaar gemaakt; ❒ ❒ ❒ ❒
- herstellen van sleutels die verloren zijn gegaan of zijn beschadigd (onderdeel van het continuïteitsplan); ❒ ❒ ❒ ❒
- archivering van sleutels; ❒ ❒ ❒ ❒
- vernietiging van sleutels; ❒ ❒ ❒ ❒
- vastleggen en controleren van activiteiten op het gebied van sleutelbeheer? ❒ ❒ ❒ ❒



Zo beantwoorden: ☑

**J**a
**N**ee
**G**edeeltelijk
**O**nbekend

| | | J | N | G | O |
|---|---|---|---|---|---|
| 11 | Is het sleutelbeheer beschreven in handboeken en procedurebeschrijvingen? | ❒ | ❒ | ❒ | ❒ |
| 12 | Zijn de taken op het gebied van sleutelbeheer expliciet toegewezen aan functionarissen met voldoende kennis en ervaring? | ❒ | ❒ | ❒ | ❒ |
| 13 | Houdt de onderneming regelmatig tests op het gebied van sleutelbeheer om kennis en ervaring op peil te houden? | ❒ | ❒ | ❒ | ❒ |
| 14 | Is een rooster voor het sleutelbeheer opgesteld met daarin aangegeven de verplichte aanwezigheid van de sleutelbeheerders, waarbij rekening is gehouden met verlof of ziekte en met de noodzakelijke functiescheidingen? | ❒ | ❒ | ❒ | ❒ |
| 15 | Worden sleutels ingenomen bij vertrek van een medewerker van de onderneming? | ❒ | ❒ | ❒ | ❒ |
| 16 | Hebben de sleutels een vastgestelde levensduur met een duidelijke begin- en eindtijd? | ❒ | ❒ | ❒ | ❒ |
| 17 | Wordt die levensduur vastgesteld aan de hand van de kans op schade, de sterkte van het algoritme en de omstandigheden waaronder de sleutels worden gebruikt? | ❒ | ❒ | ❒ | ❒ |
| 18 | Is de back-up en de opslag van sleutelgegevens duidelijk geregeld? | ❒ | ❒ | ❒ | ❒ |
| 19 | Zijn er procedures opgesteld voor het geval versleutelde informatie toegankelijk moet worden gemaakt om te dienen als bewijsmateriaal bij een juridische procedure? | ❒ | ❒ | ❒ | ❒ |
| 20 | Wordt een kopie van de cryptografische sleutels opgeslagen op een andere eveneens fysiek goed beveiligde locatie? | ❒ | ❒ | ❒ | ❒ |
| 21 | Worden publieke sleutels ook beschermd tegen misbruik door een certificaat? | ❒ | ❒ | ❒ | ❒ |
| 22 | Zorgt het certificaat voor een uniek verband tussen de informatie afkomstig van de eigenaar van de combinatie van publieke en private sleutel enerzijds en de publieke sleutel anderzijds? | ❒ | ❒ | ❒ | ❒ |
| 23 | Gebeurt die aanmaak van certificaten op een betrouwbare manier en door een betrouwbare certificerende instelling? | ❒ | ❒ | ❒ | ❒ |
| 24 | Bevat de dienstverleningsovereenkomst met leveranciers van cryptografische diensten passages over aansprakelijkheid, betrouwbaarheid van de dienstverlening en maximale uitvalsduur? | ❒ | ❒ | ❒ | ❒ |

**10.4.1 Beheer van operationele software**

| | | | | | |
|---|---|---|---|---|---|
| 1 | Is er een change-management procedure vastgesteld en omvat die tenminste regels voor het bijwerken van de operationele programmabibliotheken? | ❒ | ❒ | ❒ | ❒ |
| 2 | Wordt zoveel mogelijk voorkomen dat bronprogrammatuur aanwezig is in operationele systemen? | ❒ | ❒ | ❒ | ❒ |
| 3 | Wordt de programmatuur niet eerder in de productieomgeving opgenomen dan nadat die met succes is getest en geaccepteerd door of namens de eigenaar van de betreffende applicatie? | ❒ | ❒ | ❒ | ❒ |
| 4 | Wordt de programmatuur niet eerder in de productieomgeving opgenomen dan nadat de geaccepteerde bronprogramma's zijn gearchiveerd? | ❒ | ❒ | ❒ | ❒ |
| 5 | Wordt er een log bijgehouden van alle wijzigingen in de operationele programmabibliotheken? | ❒ | ❒ | ❒ | ❒ |
| 6 | Wordt van een aantal voorgaande versies van de programmatuur een reservekopie bewaard en wordt deze praktijk ondersteund door adequaat versiebeheer? | ❒ | ❒ | ❒ | ❒ |

**10.4.2 Beveiliging van testgegevens**

| | | | | | |
|---|---|---|---|---|---|
| 1 | Worden de procedures voor toegangsbeveiliging ook tijdens het testen gebruikt? | ❒ | ❒ | ❒ | ❒ |
| 2 | Worden productiegegevens alleen in een testomgeving gebruikt na autorisatie door of namens de eigenaar van deze gegevens? | ❒ | ❒ | ❒ | ❒ |
| 3 | Wordt het gebruik van productiegegevens voor testdoeleinden vastgelegd? | ❒ | ❒ | ❒ | ❒ |
| 4 | Is er een procedure om testgegevens te bewaren en productiegegevens in de testomgeving te wissen? | ❒ | ❒ | ❒ | ❒ |



Zo beantwoorden: ☑

**J**a
**N**ee
**G**edeeltelijk
**O**nbekend

| | | J | N | G | O |
|---|---|---|---|---|---|
| | **10.4.3 Toegangsbeveiliging voor softwarebibliotheken** | | | | |
| 1 | Zijn bronprogramma's opgeslagen in de daartoe specifiek gealloceerde programmabibliotheken? | ❒ | ❒ | ❒ | ❒ |
| 2 | Zijn deze bibliotheken niet opgeslagen in of niet benaderbaar vanuit de productieomgeving? | ❒ | ❒ | ❒ | ❒ |
| 3 | Is de toegang tot deze bibliotheken voorbehouden aan de daartoe aangestelde bibliotheekbeheerders? | ❒ | ❒ | ❒ | ❒ |
| 4 | Indien het programmabeheer is opgezet per applicatie, zijn dan de toegangsrechten van de respectieve beheerders verleend conform deze opzet? | ❒ | ❒ | ❒ | ❒ |
| 5 | Wordt een restrictief toegangsbeleid toegepast inzake de programmabibliotheken (geen onbeperkte toegang ten behoeve van programmaonderhoud; toegang uitsluitend conform taakuitoefening)? | ❒ | ❒ | ❒ | ❒ |
| 6 | Zijn de programma's die worden ontwikkeld of worden getest of in onderhoud zijn, opgeslagen in aparte bibliotheken (dus niet opslaan in de bibliotheken waarin de operationele bronprogramma's worden gearchiveerd)? | ❒ | ❒ | ❒ | ❒ |
| 7 | Worden bronprogramma's door de bibliotheekbeheerders pas gearchiveerd en gekopieerd voor onderhoud, nadat hiertoe formeel goedkeuring is verstrekt? | ❒ | ❒ | ❒ | ❒ |
| 8 | Worden wijzigingen in programma's gedetecteerd, gelogd en beoordeeld? | ❒ | ❒ | ❒ | ❒ |
| 9 | Worden toegangsbenaderingen van programmabibliotheken gedetecteerd, gelogd en beoordeeld (met name pogingen tot ongeautoriseerde toegang)? | ❒ | ❒ | ❒ | ❒ |
| 10 | Worden oude versies van bronprogramma's gearchiveerd met duidelijke vermelding van datum en tijd waarop deze operationeel waren en met bijbehorende ondersteunende software, taakbesturing, gegevensdefinities en procedures? | ❒ | ❒ | ❒ | ❒ |
| | **10.5.1 Procedures voor het beheer van wijzigingen** | | | | |
| 1 | Omvatten de procedures voor het beheer van wijzigingen tenminste de volgende onderwerpen: | | | | |
| | • een overzicht van autorisatieniveaus van contactpersonen in de IT-organisatie die wijzigingsaanvragen behandelen; | ❒ | ❒ | ❒ | ❒ |
| | • een overzicht van gebruikersautorisaties voor wijzigingsaanvragen; | ❒ | ❒ | ❒ | ❒ |
| | • een overzicht van gebruikersautorisaties voor het accepteren van voltooide of geteste wijzigingen; | ❒ | ❒ | ❒ | ❒ |
| | • een waarborg dat wijzigingen alleen geaccepteerd worden bij uitvoering door daartoe geautoriseerde gebruikers; | ❒ | ❒ | ❒ | ❒ |
| | • een overzicht van beveiligingsmaatregelen en integriteitsprocedures die gecontroleerd moeten worden om zeker te stellen dat deze niet in gevaar worden gebracht door de wijzigingen; | ❒ | ❒ | ❒ | ❒ |
| | • de eis van een schriftelijke specificatie vooraf van de aan te brengen wijzigingen; | ❒ | ❒ | ❒ | ❒ |
| | • de eis van goedkeuring vooraf op de wijzigingsvoorstellen; | ❒ | ❒ | ❒ | ❒ |
| | • de eis van acceptatie van wijzigingen voordat implementatie plaatsvindt; | ❒ | ❒ | ❒ | ❒ |
| | • de eis tot bijwerking van de systeemdocumentatie bij elke wijziging; | ❒ | ❒ | ❒ | ❒ |
| | • de eis van versiebeheer voor alle programmatuur-updates; | ❒ | ❒ | ❒ | ❒ |
| | • de eis tot het bijhouden van een administratie van wijzigingsaanvragen; | ❒ | ❒ | ❒ | ❒ |
| | • de eis tot bijhouden van een audit log van alle wijzigingen; | ❒ | ❒ | ❒ | ❒ |
| | • de eis dat wijzigingen zodanig gecoördineerd worden aangebracht dat geen productieverstoringen ontstaan (inclusief fallback-maatregelen)? | ❒ | ❒ | ❒ | ❒ |



Zo beantwoorden: ☑

**J**a
**N**ee
**G**edeeltelijk
**O**nbekend

| | | J | N | G | O |
|---|---|---|---|---|---|
| | **10.5.2 Technische controle op wijzigingen in het besturingssysteem** | | | | |
| 1 | Wordt bij wijzigingen in het besturingssysteem nagegaan welke consequenties die wijzigingen hebben voor de beveiliging van de applicaties? | ❒ | ❒ | ❒ | ❒ |
| 2 | Worden door systeemprogrammering releasenotes opgesteld en tijdig gedistribueerd? | ❒ | ❒ | ❒ | ❒ |
| 3 | Wordt in de releasenotes aandacht besteed aan de gevolgen voor beveiliging en controle (beveiligingsparagraaf)? | ❒ | ❒ | ❒ | ❒ |
| 4 | Zijn de beveiligings- en controleconsequenties afgestemd met de beveiligings- respectievelijk de controlediscipline? | ❒ | ❒ | ❒ | ❒ |
| 5 | Zijn er noodscenario's en/of fall back-scenario's opgesteld? | ❒ | ❒ | ❒ | ❒ |
| 6 | Omvat het jaarplan budgetten voor onderzoek en systeemtest naar aanleiding van wijzigingen in het besturingssysteem? | ❒ | ❒ | ❒ | ❒ |
| 7 | Worden wijzigingen in het besturingssysteem tijdig aangekondigd, zodat de benodigde controles/testen voorafgaand aan de implementatie van de wijzigingen kunnen plaatsvinden? | ❒ | ❒ | ❒ | ❒ |
| 8 | Bestaat een testprocedure voor de beoordeling van wijzigingen in het besturingssysteem? | ❒ | ❒ | ❒ | ❒ |
| 9 | Worden de continuïteitsplannen aangepast naar aanleiding van wijzigingen in het besturingssysteem? | ❒ | ❒ | ❒ | ❒ |
| | **10.5.3 Restricties op wijzigingen in softwarepakketten** | | | | |
| 1 | Is getest of de aangebrachte wijzigingen de beveiligingsmaatregelen en integriteitsprocessen niet in gevaar brengen? | ❒ | ❒ | ❒ | ❒ |
| 2 | Is toestemming verkregen van de leverancier? | ❒ | ❒ | ❒ | ❒ |
| 3 | Is het mogelijk om de wijzigingen door de leverancier te laten aanbrengen? | ❒ | ❒ | ❒ | ❒ |
| 4 | Is het mogelijk om na de aanpassing nog nieuwe versies van de leverancier te gebruiken? | ❒ | ❒ | ❒ | ❒ |
| 5 | Zijn de aangebrachte wijzigingen zodanig gedocumenteerd dat zij opnieuw aangebracht kunnen worden? | ❒ | ❒ | ❒ | ❒ |
| | **10.5.4 Geheime communicatiekanalen en Trojaanse paarden** | | | | |
| 1 | Wordt uitsluitend programmatuur aangeschaft bij betrouwbare leveranciers? | ❒ | ❒ | ❒ | ❒ |
| 2 | Wordt de programmatuur gekocht met de broncode, zodat die code gecontroleerd kan worden? | ❒ | ❒ | ❒ | ❒ |
| 3 | Wordt de programmatuur getest voordat deze in gebruik wordt genomen? | ❒ | ❒ | ❒ | ❒ |
| 4 | Is er continu aandacht voor virusdetectie (actuele virusdetectiesoftware, et cetera)? | ❒ | ❒ | ❒ | ❒ |
| 5 | Is ook na implementatie van programmatuur blijvende aandacht voor adequaat toegangs- en wijzigingsbeheer? | ❒ | ❒ | ❒ | ❒ |
| | **10.5.5 Uitbestede ontwikkeling van software** | | | | |
| 1 | Zijn licentierechten, eigendom van de software en het Intellectueel Eigendomsrecht contractueel vastgelegd? | ❒ | ❒ | ❒ | ❒ |
| 2 | Is door de leverancier een geheimhoudingsverklaring getekend? | ❒ | ❒ | ❒ | ❒ |
| 3 | Zijn de kwaliteitseisen inzake de op te leveren software contractueel vastgelegd? | ❒ | ❒ | ❒ | ❒ |
| 4 | Wordt de opgeleverde software op kwaliteit en nauwkeurigheid gecertificeerd? | ❒ | ❒ | ❒ | ❒ |
| 5 | Zijn afspraken voor het inspecteren van kwaliteit en nauwkeurigheid van het uitgevoerde werk contractueel vastgelegd? | ❒ | ❒ | ❒ | ❒ |
| 6 | Is een boetebeding opgenomen voor het geval de software niet voldoet aan de kwaliteitseisen of niet tijdig word opgeleverd? | ❒ | ❒ | ❒ | ❒ |



Zo beantwoorden: ☑

**J**a
**N**ee
**G**edeeltelijk
**O**nbekend

| | | J | N | G | O |
|---|---|---|---|---|---|
| 7 | Zijn escrow-regelingen getroffen voor het geval de externe partij in gebreke blijft, wordt overgenomen of failliet gaat? | ❒ | ❒ | ❒ | ❒ |
| 8 | Wordt voordat de software in gebruik wordt genomen nog getest op de veiligheid ervan (virussen, Trojaanse paarden, et cetera)? | ❒ | ❒ | ❒ | ❒ |
| | **10.6 Beveiliging tijdens het ontwikkel- en het onderhoudsproces** | | | | |
| 1 | Vindt het ontwikkelproces plaats volgens een standaardmethode vanaf de opdrachtgeving tot en met de oplevering? | ❒ | ❒ | ❒ | ❒ |
| 2 | Is in het ontwikkeltraject een aantal fasen onderkend, waarin terugkoppeling plaatsvindt naar de opdrachtgever en is daarbij ook diens goedkeuring vereist? | ❒ | ❒ | ❒ | ❒ |
| 3 | Is het testtraject in stappen afgebakend met tenminste een programmatest, systeemtest, integratietest en acceptatietest? | ❒ | ❒ | ❒ | ❒ |
| 4 | Zijn er voorschriften voor het documenteren van zowel ontwerpbeslissingen als programmatuur? | ❒ | ❒ | ❒ | ❒ |
| 5 | Vindt ontwikkeling plaats met standaard tools, waaronder een data dictionary? | ❒ | ❒ | ❒ | ❒ |
| 6 | Is er voldoende aandacht voor een schone, up-to-date ontwikkelomgeving, niet vervuild met allerlei tools en andere software die de werking van de ontwikkelde software nadelig kunnen beïnvloeden? | ❒ | ❒ | ❒ | ❒ |
| 7 | Is er voortdurend aandacht voor het virusvrij houden van de ontwikkelomgeving? | ❒ | ❒ | ❒ | ❒ |
| 8 | Is de ontwikkelomgeving afgesloten voor niet-ontwikkelaars (zoals testers)? | ❒ | ❒ | ❒ | ❒ |
| 9 | Worden applicaties die getest moeten worden daadwerkelijk gekopieerd naar de testomgeving (in plaats van het leggen van een link naar de ontwikkelomgeving)? | ❒ | ❒ | ❒ | ❒ |
| 10 | Wordt gebruik gemaakt van ‘proven technology’ of gebruikt men steeds de nieuwste versies van een product? | ❒ | ❒ | ❒ | ❒ |
| 11 | Zijn de ontwikkelaars voldoende opgeleid en ervaren met betrekking tot de tools die zij gebruiken? | ❒ | ❒ | ❒ | ❒ |
| 12 | Controleren de ontwikkelaars elkaars producten op toegepaste techniek, logica, opdrachtenrepertoire, documentatie, enzovoort? | ❒ | ❒ | ❒ | ❒ |
| 13 | Wordt gebruik gemaakt van ‘structured walk-throughs’? | ❒ | ❒ | ❒ | ❒ |
| **11** | **Continuïteitsmanagement** | | | | |
| | **11.1.1 Het proces van continuïteitsmanagement** | | | | |
| 1 | Is er een strategie vastgesteld en vastgelegd voor continuïteitsmanagement en sluit deze aan bij de ondernemingsdoelstellingen en bij de aan kritische bedrijfsprocessen toegekende prioriteiten? | ❒ | ❒ | ❒ | ❒ |
| 2 | Maken continuïteitsmanagement en de daarbij behorende ondersteunende processen integraal deel uit van processen en structuur van de onderneming als geheel? | ❒ | ❒ | ❒ | ❒ |
| 3 | Is de verantwoordelijkheid voor het coördineren van continuïteitsmanagement op voldoende hoog niveau belegd binnen de onderneming? | ❒ | ❒ | ❒ | ❒ |
| 4 | Zijn de risico’s die de onderneming loopt, geïdentificeerd en zijn de gevolgen van deze risico’s vastgesteld? | ❒ | ❒ | ❒ | ❒ |
| 5 | Zijn prioriteiten aan de kritische bedrijfsprocessen toegekend (met bekrachtiging door topmanagement)? | ❒ | ❒ | ❒ | ❒ |
| 6 | Is er een proces continuïteitsplanning ingericht in de onderneming? | ❒ | ❒ | ❒ | ❒ |
| 7 | Sluit deze continuïteitsplanning aan bij de strategie voor continuïteitsmanagement? | ❒ | ❒ | ❒ | ❒ |



Zo beantwoorden: ☑

**J**a
**N**ee
**G**edeeltelijk
**O**nbekend

J N G O

8 Als een proces van continuïteitsplanning is ingericht, omvat dat dan minimaal:
- specificatie van kritische bedrijfsprocessen, de daarbij behorende ondersteunende applicaties en de daartoe benodigde centrale en decentrale organisatorische en technische automatiseringsinfrastructuren; ❒ ❒ ❒ ❒
- toewijzing van continueringsprioriteiten aan bedrijfsprocessen/applicaties in termen van maximaal toegestane uitvalsduur (risicomanagement en gevolgschade onderzoek), waarbij processen/systemen als clusters beschouwd zijn in het geval zij van elkaar afhankelijk zijn; ❒ ❒ ❒ ❒
- inventarisatie van continuïteitsbedreigingen, de gevolgen hiervan voor de kritische bedrijfsprocessen/applicaties en de dan in te zetten interne dan wel externe continuïteitsvoorzieningen (bijvoorbeeld volledig gefaciliteerde interne/externe werkplekruimten); ❒ ❒ ❒ ❒
- vastlegging van verantwoordelijkheden met betrekking tot de in te zetten continuïteitsvoorzieningen, waarbij te denken valt aan escalatieprocedures, beslissingsstructuren (lijnmanagement bedrijfsprocessen tezamen met IT-management), crisismanagement, coördinatie bij het operationaliseren van de continuïteitsvoorzieningen; ❒ ❒ ❒ ❒
- documentatie terzake van de in te zetten continuïteitsvoorzieningen ten aanzien van onder meer centraal beheerde infrastructurele componenten (computers, netwerken, maar ook de daarbij behorende beheerprocessen en procedures) en de specifieke gebruikersgebonden decentrale hulpmiddelen, processen, procedures en dergelijke; ❒ ❒ ❒ ❒
- procedures voor het testen en bijwerken van continuïteitsplannen? ❒ ❒ ❒ ❒

9 Worden bij het ontwikkelen van nieuwe applicaties direct ook een continuïteitsplan ontwikkeld, continueringsprioriteiten vastgesteld en toegevoegd aan bestaande continuïteitsplannen? ❒ ❒ ❒ ❒

10 Zijn in overleg met de applicatie-eigenaren alternatieve werkwijzen of noodprocedures uitgewerkt voor tijdelijke overbrugging van uitgevallen delen van de geautomatiseerde gegevensverwerking (alternatieven zijn bijvoorbeeld: data-entry met pc's, tapeverwerking, handmatige verwerking)? ❒ ❒ ❒ ❒

11 Wordt het continuïteitsplan getriggerd vanuit het 'Incident Management (Helpdesk)' of 'Problem Management'-proces en heeft men daarvoor een escalatieprocedure beschikbaar? ❒ ❒ ❒ ❒

12 Bevat die escalatieprocedure ook oplossingen voor kleinere incidenten die de voortgang van de bedrijfsprocessen bedreigen? ❒ ❒ ❒ ❒

13 Zijn de coördinator en/of leden van het crisisteam met telefoonnummer (bij voorkeur mobiel) bekend in de organisatie? ❒ ❒ ❒ ❒

14 Zijn in het kader van het continuïteitsplan ook preventieve maatregelen genomen om de noodzaak van uitwijk te minimaliseren, zoals:
- het treffen van fysieke beveiligingsmaatregelen; ❒ ❒ ❒ ❒
- het maken van reservekopieën van schijfbestanden en de externe veiligstelling daarvan; ❒ ❒ ❒ ❒
- het tijdig aanpassen van de uitwijkconfiguratie conform de wijzigingen in de operationele configuratie (Change Management); ❒ ❒ ❒ ❒
- het treffen van goede en goed beveiligde, remote support-voorzieningen voor met name kritische hardware, systeem software en applicaties; ❒ ❒ ❒ ❒
- het vaststellen van een adequaat stelsel van nood-users en nood-user-procedures? ❒ ❒ ❒ ❒

15 Zijn er, als onderdeel van het continuïteitsplan, procedures opgesteld voor het opvangen van storingen waarvoor geen uitwijk noodzakelijk is (bijvoorbeeld storingen in randapparatuur)? ❒ ❒ ❒ ❒

16 Zijn in het kader van het continuïteitsplan ook maatregelen genomen om de kosten van eventuele uitwijk te minimaliseren door het afsluiten van daartoe strekkende verzekeringen? ❒ ❒ ❒ ❒



Zo beantwoorden: ☑

**J**a
**N**ee
**G**edeeltelijk
**O**nbekend

| | | J | N | G | O |
|---|---|---|---|---|---|
| 17 | Gaat een eventueel afgesloten verzekering niet ten koste van het treffen van de vereiste continuïteitsvoorzieningen? | ❒ | ❒ | ❒ | ❒ |
| | **11.1.2 Bedrijfscontinuïteit en analyse van mogelijke gevolgen** | | | | |
| 1 | Zijn de risico's gedefinieerd, die onderbreking van de bedrijfsprocessen kunnen veroorzaken (bijvoorbeeld: storing van apparatuur, wateroverlast en brand)? | ❒ | ❒ | ❒ | ❒ |
| 2 | Is er vervolgens een impact-analyse uitgevoerd om de gevolgen van dergelijke onderbrekingen vast te stellen (in de vorm van omvang van de schade en benodigde hersteltijd)? | ❒ | ❒ | ❒ | ❒ |
| 3 | Zijn deze activiteiten uitgevoerd met de volledige betrokkenheid van proceseigenaren, de IT-afdelingen en afdelingen zoals beveiliging, externe voorlichting, facilitaire diensten? | ❒ | ❒ | ❒ | ❒ |
| 4 | Is bij de continuïteitsanalyse een bredere scope gehanteerd dan alleen de IT-services? | ❒ | ❒ | ❒ | ❒ |
| 5 | Is er, gebaseerd op de resultaten van de continuïteitsanalyse, een (high-level) strategieplan ontwikkeld om vast te stellen wat de algemene aanpak moet zijn voor bedrijfscontinuïteit? | ❒ | ❒ | ❒ | ❒ |
| 6 | Is het eenmaal ontwikkelde (high-level) strategieplan door het top management bekrachtigd? | ❒ | ❒ | ❒ | ❒ |
| | **11.1.3 Het schrijven en invoeren van continuïteitsplannen** | | | | |
| 1 | Omvat het proces 'Continuïteitsmanagement' de volgende elementen: | | | | |
| | • identificatie en overeenstemming van alle verantwoordelijkheden met betrekking tot noodprocedures; | ❒ | ❒ | ❒ | ❒ |
| | • selectie en implementatie van alle noodprocedures om voortzetting en herstel mogelijk te maken binnen de maximaal toegestane uitvalsduur; | ❒ | ❒ | ❒ | ❒ |
| | • documentatie van overeengekomen procedures en processen; | ❒ | ❒ | ❒ | ❒ |
| | • afdoende opleiding van medewerkers in het uitvoeren van overeengekomen noodprocedures en processen, inclusief crisismanagement; | ❒ | ❒ | ❒ | ❒ |
| | • het testen en bijwerken van deze continuïteitsplannen? | ❒ | ❒ | ❒ | ❒ |
| 2 | Richt het planningsproces zich op de vereiste ondernemingsdoelstellingen (bijvoorbeeld het herstellen van diensten aan klanten binnen de maximaal toegestane uitvalsduur)? | ❒ | ❒ | ❒ | ❒ |
| 3 | Wordt er aandacht besteed aan alle diensten en middelen die dit mogelijk maken, inclusief de benodigde menskracht, niet IT-gerelateerde hulpmiddelen en uitwijkvoorzieningen voor IT-services? | ❒ | ❒ | ❒ | ❒ |
| | **11.1.4 Structuur van de continuïteitsplanning** | | | | |
| 1 | Wordt een modelstructuur voor continuïteitsplanning toegepast? | ❒ | ❒ | ❒ | ❒ |
| 2 | Zo ja, bevat deze minimaal de volgende onderdelen: | | | | |
| | • condities om het plan te activeren, waarin het proces wordt beschreven, dat moet worden gevolgd voordat het uitwijkplan wordt geactiveerd (zoals hoe elke situatie beoordeeld moet worden, wie daarbij betrokken moeten zijn, enzovoort); | ❒ | ❒ | ❒ | ❒ |
| | • procedures voor noodsituaties, waarin wordt beschreven welke acties onmiddellijk dienen te worden ondernomen na een incident, waarbij de bedrijfsvoering of mensenlevens in gevaar worden gebracht; | ❒ | ❒ | ❒ | ❒ |
| | • uitwijkprocedures waarin wordt beschreven welke acties dienen te worden ondernomen om belangrijke bedrijfsactiviteiten of diensten te verplaatsen naar alternatieve, tijdelijke lokaties en daar de processen weer binnen de vereiste tijdsduur operationeel te maken; | ❒ | ❒ | ❒ | ❒ |
| | • terugkeerprocedures waarin wordt beschreven welke acties dienen te worden ondernomen om de normale bedrijfsvoering te hervatten op de eigen lokatie; | ❒ | ❒ | ❒ | ❒ |



Zo beantwoorden: ☑

**J**a
**N**ee
**G**edeeltelijk
**O**nbekend

| | | J | N | G | O |
|---|---|---|---|---|---|
| | • een onderhoudsplanning waarin wordt beschreven hoe en wanneer het plan wordt getest en hoe het proces voor het onderhouden van het plan is ingericht; | ❒ | ❒ | ❒ | ❒ |
| | • bewustwordings- en opleidingsactiviteiten, die zijn opgezet om het besef van het belang van de bedrijfscontinuïteit te creëren en om zeker te stellen dat de procedures behorend bij continuïteitsmanagement ook permanent effectief blijven; | ❒ | ❒ | ❒ | ❒ |
| | • de verantwoordelijkheden van alle betrokkenen (en ook hun plaatsvervangers), waarin wordt beschreven wie verantwoordelijk is voor het uitvoeren van welke onderdelen van het continuïteitsplan/van de continuïteitsplannen? | ❒ | ❒ | ❒ | ❒ |
| 3 | Bevatten de procedures voor noodsituaties regels voor: | | | | |
| | • het behandelen van opslagmedia (om verlies van gegevens te voorkomen of te minimaliseren); | ❒ | ❒ | ❒ | ❒ |
| | • de wijze waarop externe voorlichting zal plaatsvinden; | ❒ | ❒ | ❒ | ❒ |
| | • een effectieve samenwerking met de juiste publieke organisaties (bijvoorbeeld politie, brandweer en lokale overheid); | ❒ | ❒ | ❒ | ❒ |
| 4 | Is elk continuïteitsplan aan een eigenaar toegewezen? | ❒ | ❒ | ❒ | ❒ |
| 5 | Is de verantwoordelijkheid voor noodprocedures, handmatige uitwijkhandelingen/ procedures en terugkeerprocedures toegewezen aan de betreffende proceseigenaren? | ❒ | ❒ | ❒ | ❒ |
| 6 | Is de verantwoordelijkheid voor uitwijkregelingen inzake technische voorzieningen, zoals computer- en netwerksystemen, toegewezen aan de manager die verantwoordelijk is voor het exploiteren en beheren van deze infrastructurele voorzieningen? | ❒ | ❒ | ❒ | ❒ |
| 7 | Is terzake van uitwijk gekozen voor één van de volgende mogelijkheden, of een combinatie daarvan: | | | | |
| | • dubbel computercentrum (intern of extern en volledig uitgerust); | ❒ | ❒ | ❒ | ❒ |
| | • uitwijk naar ‘collega’-computercentrum, met een identieke, dan wel nagenoeg identieke computerconfiguratie; | ❒ | ❒ | ❒ | ❒ |
| | • gebruikmaking van de diensten van een computerservicebureau; | ❒ | ❒ | ❒ | ❒ |
| | • aansluiting bij een commercieel uitwijkcentrum (vast of mobiel); | ❒ | ❒ | ❒ | ❒ |
| | • het in eigen beheer, dan wel in samenwerking met anderen operationeel hebben van een verplaatsbaar of mobiel computercentrum; | ❒ | ❒ | ❒ | ❒ |
| | • uitwijkafspraak met de hardwareleverancier(s)? | ❒ | ❒ | ❒ | ❒ |
| 8 | Is in het geval van algehele uitval van gegevensverwerkende systemen contractueel vastgelegd op welke alternatieve lokatie de gegevensverwerking kan worden voortgezet en zo ja: | | | | |
| | • Is door het hoogste management bepaald wanneer er sprake is van een zodanige calamiteit dat uitwijken noodzakelijk is? | ❒ | ❒ | ❒ | ❒ |
| | • Is in het uitwijkplan ook het crisisteam benoemd met namen, taak, functie en telefoonnummers? | ❒ | ❒ | ❒ | ❒ |
| | • Zijn de applicatie-eigenaren, die in nauw overleg met het IT-management moeten beslissen of er wel/niet wordt uitgeweken, ook lid van het crisisteam? | ❒ | ❒ | ❒ | ❒ |
| | • Vallen procedures voor noodsituaties, uitwijkvoorzieningen en terugkeerprocedures onder de verantwoordelijkheid van de ‘eigenaar’ van het desbetreffende bedrijfsproces? | ❒ | ❒ | ❒ | ❒ |
| | • Is er een specifieke uitwijkcoördinator benoemd door het management? | ❒ | ❒ | ❒ | ❒ |
| | • Heeft de uitwijkcoördinator voldoende resources en bevoegdheden? | ❒ | ❒ | ❒ | ❒ |
| | • Is de uitwijkcoördinator (met telefoonnummer) bekend in de organisatie? | ❒ | ❒ | ❒ | ❒ |
| | • Neemt de uitwijkcoördinator ook deel aan Problem en Change Management-vergaderingen? | ❒ | ❒ | ❒ | ❒ |



Zo beantwoorden: ☑

**J**a
**N**ee
**G**edeeltelijk
**O**nbekend

J N G O

- Zijn in het uitwijkplan ook de namen en telefoonnummers van contactpersonen op de uitwijklokatie vastgelegd? ❒ ❒ ❒ ❒
- Is in het uitwijkplan ook bepaald welke hulpmiddelen, ook niet (direct) IT-gerelateerde middelen, mee moeten naar de uitwijklokatie? ❒ ❒ ❒ ❒
- Zijn in het uitwijkplan de aanvoerprocedures voor de benodigde informatiedragers en incheckprocedures vastgelegd? ❒ ❒ ❒ ❒
- Zijn op de uitwijklokatie ook kantoorruimten met de nodige infrastructuur gereserveerd? ❒ ❒ ❒ ❒
- Is er voor de uitwijk een gedetailleerd en getest uitwijkplan beschikbaar voor zowel de IT-organisatie als voor de gebruikersorganisatie? ❒ ❒ ❒ ❒
- Is in het uitwijkplan ook gedetailleerd beschreven hoe op de uitwijklokatie de uitwijkconfiguratie moet worden ingericht? ❒ ❒ ❒ ❒
- Zijn met de respectieve applicatie-eigenaren afspraken gemaakt over het tijdsbestek waarbinnen de productie weer uitgevoerd moet kunnen worden? ❒ ❒ ❒ ❒
- Zijn met de respectieve applicatie-eigenaren afspraken gemaakt over de service levels in geval van uitwijk (aantal gebruikers, performance, enzovoort)? ❒ ❒ ❒ ❒
- Wordt voor het maken en onderhouden van uitwijkplannen standaard software gebruikt? ❒ ❒ ❒ ❒
- Is in het uitwijkplan een schematisch overzicht van de gereserveerde computer- en netwerkvoorzieningen opgenomen? ❒ ❒ ❒ ❒
- Zijn voldoende continuïteitsvoorzieningen getroffen om de uitval van datacommunicatielijnen/netwerk doeltreffend op te vangen? ❒ ❒ ❒ ❒
- Is er in het geval van een client/server infrastructuur voorzien in een daarbij behorende infrastructuur in de uitwijkomgeving? ❒ ❒ ❒ ❒
- Is er in het kader van het uitwijkplan een zogenaamde ‘uitwijkkoffer’ beschikbaar in een externe kluis en bevat deze kopieën van de uitwijk- en terugkeerprocedures? ❒ ❒ ❒ ❒
- Bevinden zich in de externe kluis of op het uitwijkadres ook zaken als back-up-tapes met bijbehorende tapelijsten, nood-user-enveloppen, manuals (zo mogelijk op cd-rom), specifieke formulieren en voorbedrukt papier van bedrijfskritische applicaties, middelen om ook op de uitwijklokatie cryptografische functies te kunnen continueren (key-management, crypto-cards, reserve crypto-adapters, et cetera)? ❒ ❒ ❒ ❒
- zijn met de leverancier van de systeemsoftware en/of standaard applicatiesoftware afspraken gemaakt over licentierechten bij gebruik in het uitwijkcentrum? ❒ ❒ ❒ ❒

9 Omvat het uitwijkplan ook een terugkeerplan om na het opheffen van de verstoring de bedrijfsvoering weer te verplaatsen van de uitwijklokatie naar de primaire verwerkingslokatie? ❒ ❒ ❒ ❒

10 Is beoordeeld of de wijze waarop en de frequentie waarmee back-ups gemaakt worden doeltreffend genoeg is gezien de eisen die daaraan worden gesteld vanuit de respectieve applicaties? ❒ ❒ ❒ ❒

**11.1.5 Testen, onderhouden en evalueren van continuïteitsplannen**

1 Zijn de continuïteitsplannen intern onafhankelijk beoordeeld? ❒ ❒ ❒ ❒

2 Worden de continuïteitsplannen minimaal jaarlijks door de proceseigenaar geëvalueerd? ❒ ❒ ❒ ❒

3 Worden de continuïteitsplannen minimaal jaarlijks onafhankelijk beoordeeld (audit of review)? ❒ ❒ ❒ ❒

4 Wordt bij de beoordelingen (audits of reviews) ook de relatie tussen wijzigings- en continuïteitsbeheer beooordeeld? ❒ ❒ ❒ ❒

5 Wordt bij de beoordelingen (audits of reviews) ook dedoeltreffendheid van het continuïteitsbeheer beoordeeld? ❒ ❒ ❒ ❒



Zo beantwoorden: ☑

**J**a
**N**ee
**G**edeeltelijk
**O**nbekend

| | | J | N | G | O |
|---|---|---|---|---|---|
| 6 | Laat het management zich (op eigen initiatief) informeren over: | | | | |
| | • de opzet/status van de continuïteitsplannen (beschikbaarheid en actualiteit van de plannen); | ❒ | ❒ | ❒ | ❒ |
| | • de bevindingen van uitgevoerde evaluaties en audits of reviews (onafhankelijk oordeel over de plannen en de doeltreffendheid daarvan); | ❒ | ❒ | ❒ | ❒ |
| | • de resultaten van het testen van de continuïteitsvoorzieningen? | ❒ | ❒ | ❒ | ❒ |
| 7 | Is er een testschema opgesteld voor de continuïteitsplannen? | ❒ | ❒ | ❒ | ❒ |
| 8 | Is in dat schema aangegeven hoe, wat en door wie wordt getest? | ❒ | ❒ | ❒ | ❒ |
| 9 | Worden de tests gefaseerd uitgevoerd op basis van regelmatige tests van afzonderlijke onderdelen van de plannen? | ❒ | ❒ | ❒ | ❒ |
| 10 | Worden bij de tests alle continuïteitsvoorzieningen geraakt? | ❒ | ❒ | ❒ | ❒ |
| 11 | Worden de volgende testactiviteiten uitgevoerd: | | | | |
| | • testen van diverse scenario's vanachter het bureau (uitgaand van wie, wat, hoe, waarom en wanneer bij welke onderbrekingen herstel van bedrijfsactiviteiten moet uitvoeren); | ❒ | ❒ | ❒ | ❒ |
| | • simulaties (met name voor het trainen van personeel inzake hun taken/rollen in geval van incidenten en crisissituaties); | ❒ | ❒ | ❒ | ❒ |
| | • testen van technisch herstel (het adequaat opbrengen van de infrastructurele continuïteitsvoorzieningen, opdat de kritische applicaties operationeel zijn binnen de maximaal toegestane uitvalsduur); | ❒ | ❒ | ❒ | ❒ |
| | • testen van herstel op een uitwijklokatie (het uitvoeren van bedrijfsprocessen op een andere plaats dan normaal); | ❒ | ❒ | ❒ | ❒ |
| | • testen van voorzieningen en diensten die door toeleveranciers worden geleverd (om vast te stellen dat externe diensten en producten voldoen aan hetgeen daarover contractueel is vastgelegd); | ❒ | ❒ | ❒ | ❒ |
| | • volledige tests (testen dat organisatie, personeel, apparatuur, voorzieningen en processen bestand zijn tegen onderbrekingen)? | ❒ | ❒ | ❒ | ❒ |
| 12 | Worden per test met de beheerders van de continuïteitsvoorzieningen (intern dan wel extern) duidelijke afspraken gemaakt over de ter beschikking te stellen configuratie, ondersteuning, testduur, enzovoort (bij voorkeur schriftelijk)? | ❒ | ❒ | ❒ | ❒ |
| 13 | Wordt per test een testplan opgesteld, worden doelstellingen geformuleerd en wordt met alle, bij de test betrokken, disciplines afgestemd wat van hen wordt verwacht? | ❒ | ❒ | ❒ | ❒ |
| 14 | Als er sprake is van een uitwijkplan, wordt dat dan minimaal één keer per jaar getest? | ❒ | ❒ | ❒ | ❒ |
| 15 | Worden van alle uitgevoerde tests rapporten opgesteld met als doel de resultaten te evalueren? | ❒ | ❒ | ❒ | ❒ |
| 16 | Wordt naar aanleiding van deze evaluatie een actielijst opgesteld en afgewerkt, naar aanleiding van de problemen die zich tijdens een test hebben voorgedaan? | ❒ | ❒ | ❒ | ❒ |
| 17 | Wordt de afwerking van deze actielijst onafhankelijk beoordeeld (audit of review)? | ❒ | ❒ | ❒ | ❒ |
| 18 | Worden op basis van de volgende voorbeelden van wijzigingen de continuïteitsplannen bijgewerkt: | | | | |
| | • de aanschaf van nieuwe apparatuur of upgrades van de operationele besturingssystemen; | ❒ | ❒ | ❒ | ❒ |
| | • wijzigingen in datacommunicatiefaciliteiten; | ❒ | ❒ | ❒ | ❒ |
| | • het gebruik van nieuwe technieken voor het opsporen en oplossen van problemen; | ❒ | ❒ | ❒ | ❒ |
| | • het gebruik van nieuwe technieken voor klimaatbeheersing; | ❒ | ❒ | ❒ | ❒ |
| | • wijzigingen in het personeelsbestand of de organisatie; | ❒ | ❒ | ❒ | ❒ |
| | • verandering van tijdelijke werknemers of leveranciers; | ❒ | ❒ | ❒ | ❒ |
| | • wijzigingen bij belangrijke klanten; | ❒ | ❒ | ❒ | ❒ |
| | • wijzigingen in de bedrijfslocaties; | ❒ | ❒ | ❒ | ❒ |



Zo beantwoorden: ☑

**J**a
**N**ee
**G**edeeltelijk
**O**nbekend

| | | J | N | G | O |
|---|---|---|---|---|---|
| | • wijzigingen in adressen of telefoonnummers; | ❒ | ❒ | ❒ | ❒ |
| | • wijzigingen/vervallen van bestaande bedrijfsprocessen of uitbreiding met nieuwe processen; | ❒ | ❒ | ❒ | ❒ |
| | • wijziging in applicaties; | ❒ | ❒ | ❒ | ❒ |
| | • wijziging in risico's (operationeel en financieel); | ❒ | ❒ | ❒ | ❒ |
| | • wijziging in de bedrijfsstrategie; | ❒ | ❒ | ❒ | ❒ |
| | • wijziging in de bedrijfsvoering; | ❒ | ❒ | ❒ | ❒ |
| | • wijziging in de wetgeving? | ❒ | ❒ | ❒ | ❒ |
| 19 | Worden de continuïteitsplannen bijgewerkt naar aanleiding van reguliere audits of op basis van de volgende voorbeelden van controles die specifiek op het proces 'Continuïteitsplanning' zijn toegesneden: | | | | |
| | • onafhankelijke interne beoordelingen van continuïteitsplannen; | ❒ | ❒ | ❒ | ❒ |
| | • procesevaluaties; | ❒ | ❒ | ❒ | ❒ |
| | • tests, zowel vanachter het bureau, als in de praktijk en op de werkplekken; | ❒ | ❒ | ❒ | ❒ |
| | • periodiek uitgevoerde tests van de uitwijkplannen; | ❒ | ❒ | ❒ | ❒ |
| | • evaluaties van de resultaten van interne en externe uitwijktesten? | ❒ | ❒ | ❒ | ❒ |
| 20 | Is de verantwoordelijkheid voor het signaleren van wijzigingen en het (doen) wijzigen van continuïteitsplannen duidelijk belegd (separate functie 'coördinator continuïteitsplanning')? | ❒ | ❒ | ❒ | ❒ |
| 21 | Zijn personen aangewezen voor het signaleren en het aanbrengen van wijzigingen in de continuïteitsplannen? | ❒ | ❒ | ❒ | ❒ |
| 22 | Worden direct na alle relevante wijzigingen in de operationele IT-infrastructuur tevens de continuïteitsplannen aangepast (omdat de uitwijkconfiguratie een actuele representatie dient te zijn van de operationele configuratie)? | ❒ | ❒ | ❒ | ❒ |
| 23 | Is het wijzigen van continuïteitsplannen automatisch gekoppeld aan het 'Change Management'- en/of het 'Configuration Management'-proces? | ❒ | ❒ | ❒ | ❒ |
| 24 | Wordt na elke wijziging van het continuïteitsplan een kopie daarvan opgeborgen in de uitwijkkoffer in de externe kluis? | ❒ | ❒ | ❒ | ❒ |

## 12 Naleving

### 12.1.1 Specificatie van de van toepassing zijnde wetgeving

| | | | | | |
|---|---|---|---|---|---|
| 1 | Zijn voor elk informatiesysteem alle wettelijke en contractuele beveiligingseisen gedefinieerd en gedocumenteerd? | ❒ | ❒ | ❒ | ❒ |
| 2 | Zijn de maatregelen en individuele verantwoordelijkheden om aan deze eisen te voldoen eveneens gedefinieerd en gedocumenteerd? | ❒ | ❒ | ❒ | ❒ |

### 12.1.2 Intellectuele eigendomsrechten (Intellectual Property Rights, IPR)

| | | | | | |
|---|---|---|---|---|---|
| 1 | Worden de medewerkers er in de interne bedrijfsregels op gewezen dat de wettelijke verplichtingen ter zake van Intellectueel Eigendom (bijvoorbeeld auteursrecht) dienen te worden nageleefd? | ❒ | ❒ | ❒ | ❒ |
| 2 | Is er in de interne bedrijfsregels op gewezen dan niet naleving van deze wettelijke verplichtingen tot sancties zal leiden? | ❒ | ❒ | ❒ | ❒ |
| 3 | Is in de interne bedrijfsregels opgenomen dat: | | | | |
| | • programmatuur legaal via de standaard inkoopprocedure moet worden aangeschaft; | ❒ | ❒ | ❒ | ❒ |



Zo beantwoorden: ☑

**J**a
**N**ee
**G**edeeltelijk
**O**nbekend

| | | J | N | G | O |
|---|---|---|---|---|---|
| | • programmatuur uitsluitend met schriftelijke toestemming van de auteursrechthebbende naar andere computers mag worden gekopieerd (denk aan uitwijkconfiguraties, kantoor-pc's, laptops, en dergelijke); | ❒ | ❒ | ❒ | ❒ |
| | • kopiëren van auteursrechtelijk beschermde of bedrijfseigen programmatuur naar niet tot het bedrijf behorende computers niet zonder toestemming is toegestaan; | ❒ | ❒ | ❒ | ❒ |
| | • kopiëren van auteursrechtelijke beschermde of bedrijfseigen programmatuur voor niet zakelijke doeleinden niet is toegestaan? | ❒ | ❒ | ❒ | ❒ |
| 4 | Indien programmatuur dient te worden gebruikt door meerdere gebruikers, of op meerdere computers, wordt dan de licentie-overeenkomst aangepast (bij overschrijden van maximaal aantal gebruikers) of worden extra exemplaren van het product aangeschaft? | ❒ | ❒ | ❒ | ❒ |
| 5 | Wordt er een overzicht van de licentiegebonden programmatuur bijgehouden? | ❒ | ❒ | ❒ | ❒ |
| 6 | Wordt alle programmatuur met contracten en licenties beheerd (bijvoorbeeld met behulp van 'Configuration Management' of 'Beheer van Automatiseringsmiddelen')? | ❒ | ❒ | ❒ | ❒ |
| 7 | Wordt ter voorkoming van gebruik van illegale software gebruik gemaakt van een 'Software Control & Distribution' proces om legale software te distribueren over alle systemen? | ❒ | ❒ | ❒ | ❒ |
| 8 | Zijn maatregelen genomen om gebruik of distributie van illegale software te voorkomen? | ❒ | ❒ | ❒ | ❒ |
| 9 | Is door middel van awareness-programma's of folders bij de medewerkers aandacht gevraagd voor de risico's die het bedrijf loopt bij gebruik van illegale software (aantasting reputatie, financieel verlies, virusinfecties, en dergelijke)? | ❒ | ❒ | ❒ | ❒ |
| 10 | Worden regelmatig (geplande) audits uitgevoerd op programmatuur die aanwezig is op de computersystemen door deze te vergelijken met een overzicht van legale software? | ❒ | ❒ | ❒ | ❒ |
| 11 | Wordt, indien bij dergelijke audits illegale programmatuur wordt aangetroffen, gerapporteerd aan het management en door het management effectieve maatregelen genomen om de tekortkomingen weg te nemen? | ❒ | ❒ | ❒ | ❒ |
| 12 | Wordt bij het constateren van gebruik van illegale programmatuur de betreffende medewerker gewezen op de risico's die het bedrijf daardoor loopt? | ❒ | ❒ | ❒ | ❒ |
| 13 | Worden bij het constateren van gebruik van illegale programmatuur sancties getroffen tegen de betreffende medewerker? | ❒ | ❒ | ❒ | ❒ |
| | **12.1.3 Beveiliging van bedrijfsdocumenten** | | | | |
| 1 | Worden gegevens gecategoriseerd naar soort (accounting records, databaserecords, transactieverslagen, audit logging, operationele procedures en dergelijke)? | ❒ | ❒ | ❒ | ❒ |
| 2 | Wordt per soort gegeven vastgelegd wat de bewaartermijn is en welk type opslagmedium van toepassing is? | ❒ | ❒ | ❒ | ❒ |
| 3 | Worden, indien van toepassing, cryptografische sleutels van encrypte bestanden en digitale handtekeningen veilig bewaard? | ❒ | ❒ | ❒ | ❒ |
| 4 | Worden de bedrijfsvoorschriften ten aanzien van het bewaren, opslaan, verwerken en vernietigen van bedrijfsdocumenten en -gegevens gedistribueerd onder alle medewerkers? | ❒ | ❒ | ❒ | ❒ |
| 5 | Wordt in die voorschriften ook rekening gehouden met laptops waarop ook bedrijfskritische gegevens worden opgeslagen? | ❒ | ❒ | ❒ | ❒ |
| 6 | Is er een schema opgesteld waarin belangrijke documenttypen worden vermeld? | ❒ | ❒ | ❒ | ❒ |
| 7 | Is in dit schema vastgelegd hoe lang deze documenten dienen te worden bewaard? | ❒ | ❒ | ❒ | ❒ |
| 8 | Wordt een overzicht van belangrijke informatiebronnen bijgehouden? | ❒ | ❒ | ❒ | ❒ |
| 9 | Zijn maatregelen geïmplementeerd om belangrijke documenten en informatie te beveiligen tegen verlies, vernietiging en vervalsing? | ❒ | ❒ | ❒ | ❒ |



Zo beantwoorden: ☑

**J**a
**N**ee
**G**edeeltelijk
**O**nbekend

| | | J | N | G | O |
|---|---|---|---|---|---|
| 10 | Worden kopieën van belangrijke documenten ook buiten het gebouw in een beveiligde ruimte opgeslagen? | ❒ | ❒ | ❒ | ❒ |
| 11 | Worden bij wijziging van systemen of gegevensdragers ook de veilig gestelde bestanden met historische gegevens geconverteerd naar de nieuwe vorm? | ❒ | ❒ | ❒ | ❒ |
| 12 | Worden gegevensdragers waarop back-ups zijn opgeslagen na verloop van een bepaalde bewaartijd (of bij verandering van techniek) vernieuwd om achteruitgang van kwaliteit te voorkomen? | ❒ | ❒ | ❒ | ❒ |
| 13 | Zijn maatregelen getroffen om regelmatig te controleren of elektronisch opgeslagen kopieën van informatie verwerkbaar zijn? | ❒ | ❒ | ❒ | ❒ |
| 14 | Voldoen elektronisch opgeslagen kopieën van informatie aan de daaraan gestelde wettelijke eisen (zie: Bewbew)? | ❒ | ❒ | ❒ | ❒ |
| | **12.1.4 Bescherming van persoonsgegevens** | | | | |
| 1 | Worden persoonlijke gegevens op legitieme wijze verkregen en verwerkt? | ❒ | ❒ | ❒ | ❒ |
| 2 | Worden persoonlijke gegevens uitsluitend opgeslagen voor vastgestelde en legitieme doeleinden? | ❒ | ❒ | ❒ | ❒ |
| 3 | Zijn maatregelen getroffen om te bereiken dat persoonlijke gegevens niet worden gebruikt of bekend gemaakt voor andere redenen dan oorspronkelijk is bedoeld? | ❒ | ❒ | ❒ | ❒ |
| 4 | Zijn de persoonlijke gegevens relevant en adequaat? | ❒ | ❒ | ❒ | ❒ |
| 5 | Zijn de persoonlijke gegevens accuraat en worden ze up-to-date gehouden? | ❒ | ❒ | ❒ | ❒ |
| 6 | Worden persoonlijke gegevens niet langer bewaard dan nodig is? | ❒ | ❒ | ❒ | ❒ |
| 7 | Worden persoonlijke gegevens beschikbaar gesteld aan en kunnen deze zonodig worden gewijzigd door de betreffende persoon zelf? | ❒ | ❒ | ❒ | ❒ |
| 8 | Worden persoonlijke gegevens veilig opgeslagen en adequaat beveiligd tegen ongeautoriseerde toegang, wijzigingen, bekendmaking, verlies of vernietiging? | ❒ | ❒ | ❒ | ❒ |
| 9 | Wordt regelmatig getoetst of de bepalingen van de WBP worden nageleefd? | ❒ | ❒ | ❒ | ❒ |
| 10 | Is er een functionaris (‘Data protection officer’) binnen de organisatie aangewezen en voorzien van de nodige bevoegdheden voor uitvoering van de WBP? | ❒ | ❒ | ❒ | ❒ |
| 11 | Is een overzicht beschikbaar van alle (elektronische) bestanden waarop de WBP van toepassing is? | ❒ | ❒ | ❒ | ❒ |
| | **12.1.5 Voorkomen van misbruik van IT-voorzieningen** | | | | |
| 1 | Is aan de medewerkers bekend gemaakt dat IT-voorzieningen binnen een bedrijf uitsluitend mogen worden gebruikt voor bedrijfsdoeleinden? | ❒ | ❒ | ❒ | ❒ |
| 2 | Wordt misbruik van IT-voorzieningen onder de aandacht gebracht van het management, zodat zonodig disciplinaire maatregelen kunnen worden genomen? | ❒ | ❒ | ❒ | ❒ |
| 3 | Worden gebruikers bij het aanloggen erop gewezen dat toegang tot het netwerk en de daaraan gekoppelde computersystemen alleen toegestaan is, indien men daartoe geautoriseerd is? | ❒ | ❒ | ❒ | ❒ |
| 4 | Wordt jaarlijks door de externe accountant in de management letter aandacht gegeven aan het onderwerp informatiebeveiliging (zie naast de wetgeving ook: Norea, Wcc)? | ❒ | ❒ | ❒ | ❒ |
| | **12.1.6 Voorschriften ten aanzien van het gebruik van cryptografische middelen** | | | | |
| 1 | Is een inventarisatie aanwezig welke overeenkomsten, wetten, voorschriften of andere instrumenten van kracht zijn m.b.t. de toegang of het gebruik van cryptografie? | ❒ | ❒ | ❒ | ❒ |
| 2 | Is bekend of de gebruikte computerhardware/software import en/of export restricties kent? | ❒ | ❒ | ❒ | ❒ |



Zo beantwoorden: ☑

**J**a
**N**ee
**G**edeeltelijk
**O**nbekend

| | | J | N | G | O |
|---|---|---|---|---|---|
| 3 | Wordt de vertrouwelijkheid van gegevens in acht genomen indien nationaal bevoegde instanties toegang tot versleutelde informatie eisen? | ❒ | ❒ | ❒ | ❒ |
| 4 | Is juridisch advies ingewonnen om te bepalen welke wetgeving van toepassing is? | ❒ | ❒ | ❒ | ❒ |
| 5 | Is juridisch advies ingewonnen indien sleutels over landsgrenzen getransporteerd worden? | ❒ | ❒ | ❒ | ❒ |
| | **12.1.7 Verzamelen van bewijsmateriaal** | | | | |
| 1 | Wordt bij een incident tijdig overwogen of inschakeling van advocaat en/of politie noodzakelijk is? | ❒ | ❒ | ❒ | ❒ |
| 2 | Is, voor het geval zich een incident voordoet, het bewijsmateriaal toelaatbaar, oftewel kan het in een rechtszaak worden gebruikt? | ❒ | ❒ | ❒ | ❒ |
| | • Voldoen de computersystemen aan algemeen aanvaarde standaards en 'best practices' om toelaatbaar bewijsmateriaal te produceren? | ❒ | ❒ | ❒ | ❒ |
| | • Wordt het bewijsmateriaal adequaat beveiligd? | ❒ | ❒ | ❒ | ❒ |
| | • Worden mutatielogs, audittraces en operator logs aangemaakt en bewaard om later eventueel als bewijsmateriaal gebruikt te worden? | ❒ | ❒ | ❒ | ❒ |
| 3 | Wordt er in geval van een incident voor zorggedragen dat het bewijsmateriaal van voldoende kwaliteit en volledig is? | ❒ | ❒ | ❒ | ❒ |
| 4 | Zijn hiertoe voor gegevens op papieren documenten de volgende zaken geregeld: | | | | |
| | • Wordt inkomende post geregistreerd; | ❒ | ❒ | ❒ | ❒ |
| | • Wordt bij onduidelijke post (kan bijvoorbeeld geld of cheques bevatten), deze post in aanwezigheid van meer dan één persoon geopend; | ❒ | ❒ | ❒ | ❒ |
| | • Worden originele documenten veilig bewaard; | ❒ | ❒ | ❒ | ❒ |
| | • Wordt geregistreerd door wie, waar en wanneer de documenten zijn gecreëerd; | ❒ | ❒ | ❒ | ❒ |
| | • Wordt geregistreerd wie aanwezig was bij de ontdekking van de documenten; | ❒ | ❒ | ❒ | ❒ |
| | • Is vastgesteld dat niet geknoeid is met de originele documenten? | ❒ | ❒ | ❒ | ❒ |
| 5 | Zijn hiertoe voor gegevens op computermedia de volgende zaken geregeld: | ❒ | ❒ | ❒ | ❒ |
| | • Worden er kopieën gemaakt van gegevens op verwisselbare media (met name tapes); | ❒ | ❒ | ❒ | ❒ |
| | • Worden in- en uitgaande verwisselbare media geregistreerd? | ❒ | ❒ | ❒ | ❒ |
| | • Worden er kopieën van gegevens op harde schijven of geheugen gemaakt? | ❒ | ❒ | ❒ | ❒ |
| | • Worden alle acties tijdens het kopiëren van gegevens in logfiles opgeslagen? | ❒ | ❒ | ❒ | ❒ |
| | • Wordt het kopiëren van deze gegevens bijgewoond door een getuige? | ❒ | ❒ | ❒ | ❒ |
| | • Worden kopieën van media en logfiles veilig bewaard? | ❒ | ❒ | ❒ | ❒ |
| | **12.2.1 Naleving van het beveiligingsbeleid** | | | | |
| 1 | Is elke applicatie formeel toegewezen aan een eigenaar? | ❒ | ❒ | ❒ | ❒ |
| 2 | Zijn per applicatie de beveiligingseisen, die daaraan worden gesteld vanuit het beveiligingsbeleid, gedocumenteerd? | ❒ | ❒ | ❒ | ❒ |
| 3 | Wordt namens de eigenaar van een applicatie op voldoende frequente basis gecontroleerd of het beveiligingsbeleid en de beveiligingsnormen en procedures worden nageleefd? | ❒ | ❒ | ❒ | ❒ |
| 4 | Worden de bevindingen van deze controles rechtstreeks, eventueel op periodieke basis (wekelijks of maandelijks), gerapporteerd aan de desbetreffende eigenaar van een applicatie? | ❒ | ❒ | ❒ | ❒ |
| 5 | Worden ernstige inbreuken op de beveiliging van of mogelijke 'beveiligingslekken' direct onder de aandacht gebracht van de betreffende eigenaar van een applicatie of technische infrastructuur en wordt zonodig het management geïnformeerd? | ❒ | ❒ | ❒ | ❒ |



Zo beantwoorden: ☑

**J**a
**N**ee
**G**edeeltelijk
**O**nbekend

J N G O

6 Worden namens het management door een onafhankelijke discipline binnen de onderneming (bij grote bedrijven meestal verspreid over gebruikersafdelingen en computercentrum en gecontroleerd door de interne accountantsdienst, bij kleine bedrijven doorgaans geïntegreerd in één afdeling), op voldoende frequente basis en met behulp van daartoe opgezette controleprogramma's, gecontroleerd dat:
- de beveiliging voor applicaties zodanig werkt, dat de beveiligingsrisico's hiervoor binnen aanvaardbare grenzen zijn en blijven ingedamd; ❒ ❒ ❒ ❒
- de beveiliging voor computer- en netwerksystemen zodanig werkt, dat de beveiligingsrisico's voor de technische automatiseringsinfrastructuur en de daarop draaiende applicaties binnen aanvaardbare grenzen zijn en blijven ingedamd; ❒ ❒ ❒ ❒
- de beveiliging ook door leveranciers van computersystemen wordt gewaarborgd conform de geldende beveiligingsnormen; ❒ ❒ ❒ ❒
- de beveiliging ook door de gebruikers wordt gewaarborgd conform de geldende beveiligingsnormen? ❒ ❒ ❒ ❒

7 Worden de controlerapporten van deze controlediscipline afgestemd met de betreffende eigenaar van applicaties of technische infrastructuur? ❒ ❒ ❒ ❒

8 Wordt op periodieke basis door de onafhankelijke controlediscipline aan het management van de onderneming rapport uitgebracht over de belangrijkste controlebevindingen? ❒ ❒ ❒ ❒

9 Zijn de functies, taken en bevoegdheden van de controlediscipline schriftelijk vastgelegd en zijn deze binnen de onderneming bekend gemaakt? ❒ ❒ ❒ ❒

**12.2.2 Controle op naleving van technische normen**

1 Wordt regelmatig gecontroleerd of de beveiligingsmaatregelen voor apparatuur en programmatuur nog op de juiste wijze zijn geïmplementeerd? ❒ ❒ ❒ ❒

2 Worden deze controles uitgevoerd door (controle)functionarissen met voldoende ervaring en expertise? ❒ ❒ ❒ ❒

3 Wordt waar mogelijk gebruik gemaakt van logs (event-driven: operatorhandelingen, jobstatussen, violations, et cetera) en audittrails (registratie: wie, wanneer, wat heeft gedaan, met name bij financiële gegevensmutaties) om wijzigingen in applicatie- en besturingsprogrammatuur te detecteren en te beoordelen? ❒ ❒ ❒ ❒

4 Wordt waar mogelijk gebruik gemaakt van geautomatiseerde controleprogramma's (auditsoftware, audittools) om de beveiligingsinrichting van de computer- en netwerksystemen te beoordelen en eventuele wijzigingen hierin te detecteren en te beoordelen? ❒ ❒ ❒ ❒

5 Worden dikwijls controles uitgevoerd inzake onder meer:
- beveiligingsovertredingen (violations); ❒ ❒ ❒ ❒
- overdracht van applicatie- en systeemsoftware tussen verschillende computeromgevingen; ❒ ❒ ❒ ❒
- het inzetten van users met krachtige bevoegdheden (zoals nood-users) of het gebruik van krachtige commando's; ❒ ❒ ❒ ❒
- wijzigingen in de logische toegangsbeveiliging; ❒ ❒ ❒ ❒
- wijzigingen in beveiligings- en/of controlekritische besturingsparameters; ❒ ❒ ❒ ❒
- wijzigingen in kritische systeemsoftware-libraries; ❒ ❒ ❒ ❒
- het opstarten van de juiste versies van besturings(sub)systemen; ❒ ❒ ❒ ❒
- het tijdig verwijderen van user-ID's en/of toegangsrechten bij vertrek of functiewijziging van functionarissen? ❒ ❒ ❒ ❒



Zo beantwoorden: ☑

**J**a
**N**ee
**G**edeeltelijk
**O**nbekend

| | | J | N | G | O |
|---|---|---|---|---|---|
| 6 | Worden op periodieke basis penetratietesten uitgevoerd ten einde kwestbaarheden (mogelijke 'lekken') in de beveiliging te detecteren en wordt hierbij zonodig gebruik gemaakt van onafhankelijke experts? | ❒ | ❒ | ❒ | ❒ |
| 7 | Worden beveiligings- en controlefunctionarissen in voldoende mate betrokken bij het testen (bestaande beveiliging mag niet worden aangetast), bij de evaluatie van de testresultaten en bij de afdoening van eventuele aanvullende beveiligingsacties? | ❒ | ❒ | ❒ | ❒ |
| | **12.3.1 Beveiligingsmaatregelen bij systeem-audits** | | | | |
| 1 | Worden audits en andere controleactiviteiten op operationele informatiesystemen (of, op grond van performance-overwegingen, op kopieën hiervan) vooraf zorgvuldig gepland en afgestemd met de eigenaars van die systemen? | ❒ | ❒ | ❒ | ❒ |
| 2 | Zijn maatregelen getroffen om te voorkomen dat audits worden uitgevoerd zonder toestemming van de eigenaars van de operationele informatiesystemen? | ❒ | ❒ | ❒ | ❒ |
| 3 | Worden de audits/controles uitsluitend uitgevoerd door ervaren auditors/controleurs? | ❒ | ❒ | ❒ | ❒ |
| 4 | Wordt de bij de controles benodigde toegang beperkt tot alleen lezen (read-only) van programmatuur, gegevens, besturingsparameters, et cetera? | ❒ | ❒ | ❒ | ❒ |
| 5 | Zijn zodanige audittraces (systeeminstellingen, veelal binnen beveiligingssoftware, die specifiek worden geactiveerd om de handelingen van subjecten en/of de benaderingen van objecten in audit logs te kunnen registreren) geactiveerd op kritische applicatie- en/of besturingsbestanden, zodat kan worden gedetecteerd dat deze zijn benaderd voor audit-doeleinden? | ❒ | ❒ | ❒ | ❒ |
| 6 | Worden IT-hulpmiddelen voor het uitvoeren van de controles expliciet gedefinieerd en beschikbaar gesteld? | ❒ | ❒ | ❒ | ❒ |
| 7 | Vinden tests op mogelijke beveiligingslekken in applicatie- en/of besturingsprogrammatuur ('penetratietesten') uitsluitend plaats door beveiligingsspecialisten (hooguit op verzoek en in aanwezigheid van auditors, maar nooit door auditors)? | ❒ | ❒ | ❒ | ❒ |
| 8 | Wordt beveiligings- en controlerelevante informatie (dus zowel de input als de output van audits/controles) afgeschermd tegen onbevoegd gebruik? | ❒ | ❒ | ❒ | ❒ |
| | **12.3.2 Beveiliging van hulpmiddelen voor systeem-audits** | | | | |
| 1 | Zijn de hulpmiddelen voor audits afgeschermd tegen onbevoegd gebruik? | ❒ | ❒ | ❒ | ❒ |
| 2 | Zijn de met audittools gegenereerde gegevens afgeschermd tegen onbevoegd gebruik? | ❒ | ❒ | ❒ | ❒ |
| 3 | Zijn dusdanige audittraces geactiveerd op audittools en de daarmee gegenereerde output, dat kan worden gedetecteerd wie deze heeft gebruikt en/of benaderd? | ❒ | ❒ | ❒ | ❒ |
| 4 | Zijn zodanige maatregelen genomen, dat auditors zich geen krachtige privileges kunnen verschaffen met behulp van de audittools? | ❒ | ❒ | ❒ | ❒ |



Zo beantwoorden: ☑

**J**a
**N**ee
**G**edeeltelijk
**O**nbekend