

In applicaties/systemen, waarin geautomatiseerd rekening wordt gehouden met deze functiescheiding, kan indien gewenst ruimer worden geautoriseerd. Hiermee wordt bedoeld dat als de applicatie/het systeem opeenvolgende handelingen in het proces door één functionaris op één en hetzelfde dossier niet toestaat, maar wel voor andere dossiers, waar nog geen conflicterende handeling door deze functionaris is uitgevoerd.

Per proces moet een beschrijving van de te gebruiken applicatie/systemen gemaakt worden, inclusief de mogelijkheden om te kunnen voldoen aan de functiescheiding.

Indien op het gebied van autorisaties niet kan worden voldaan aan de vereiste functiescheiding mag hiervan slechts worden afgeweken mits:

- de risico's in kaart zijn gebracht (op basis van een risicoanalyse);
- er voldoende compenserende maatregelen zijn ingeregeld;
- de beveiligingsadviseur positief heeft geadviseerd aan het verantwoordelijk management.

Muteerrechten in het ondersteunend proces, zoals het registreren van SAP-Tijd, worden in een bedrijfsonderdeel overstijgend profiel (Everyone) of in een bedrijfsvoerings- of managementprofiel opgenomen. Deze autorisaties zijn voor ieder bedrijfsonderdeel gelijk.

B.1.3.2.4 Bijzondere rechten

Onder bijzondere rechten worden toegangsrechten verstaan waaraan specifieke voorwaarden worden gesteld. Bevoegdheden kunnen bijzonder zijn omdat deze:

- Potentieel de functiescheiding kunnen doorbreken;
- Alleen beperkt functioneel mogen worden toegekend;
- Bijzondere informatie ontsluiten, zoals die van vips;
- Gepaard gaan met licentiekosten;
- Om performanceredenen slechts beperkt mogen worden gebruikt;
- De mogelijkheid bieden elektronisch gegevens uit te wisselen.

Privileges

Indien er binnen een proces functioneel behoefte is aan privileges, dan kunnen deze in het bestaande profiel of als sub-profiel worden opgenomen.

Indien een privilege niet functioneel wordt toegekend (het privilege is niet opgenomen in het procesprofiel), moet de geëigende aanvraagprocedure worden gevolgd.

Daar waar de classificatie van informatie hogere eisen stelt aan de afscherming, worden de rechten alleen op individuele wijze toegekend. Deze rechten worden binnen het bijbehorende proces in een apart profiel 'Bijzondere taken' opgenomen.

Live- en productiegegevens

Het gebruiken van live/productiegegevens buiten de doelbinding (Wbp) is niet toegestaan. Per geval dienen alternatieven te worden onderzocht, waaronder pseudonimisatie of anonimisatie. Als afdoende blijkt dat er geen andere mogelijkheden zijn (explain), dient voor een uitzondering een risicoafweging en -acceptatie te worden gedaan. De verantwoordelijkheid hiervoor ligt in de lijn.

Opleidingen

Voor het opleiden van medewerkers van de Belastingdienst is het vaak noodzakelijk dat zij kunnen leren of oefenen in de systemen en applicaties van de primaire processen. Daarom dient gebruik gemaakt te worden van testomgevingen of speciaal voor opleidingen ontwikkelde omgevingen die door de bedrijfsonderdelen zelf worden beheerd.

In de onder verantwoordelijkheid van de BelastingdienstAcademie ontwikkelde, beheerde en uitgevoerde opleidingen wordt geen gebruik gemaakt van het oefenen in live/productieomgevingen.

Wel kunnen praktijkopdrachten als onderdeel van de leertrajecten ingericht worden waarbij individuele medewerkers onder begeleiding van een ervaren collega werken in de systemen of applicaties. Dit gebeurt dan op de werkplek en onder verantwoordelijkheid van het bedrijfs onderdeel, in casu de ervaren collega.

B.1.3.2.5 Beleid op controle op gebruik van autorisaties

Autorisaties geven toegang tot (geautomatiseerde) bedrijfsmiddelen. Bedoeld of onbedoeld misbruik hiervan moet kunnen worden gesignaleerd zoals bij het onbevoegd raadplegen of onbevoegd muteren van gegevens. Dat geldt ook buiten de grenzen van de organisatie zoals op internet. Hiertoe zijn procedures vastgesteld, waarbij het resultaat ervan regelmatig wordt beoordeeld.

Beveiligingsfuncties

Identificatie, authenticatie en autorisatie zijn de functies die de handhaving van functiescheiding, de herleidbaarheid van handelingen en de beperking van de toegang tot gegevens ondersteunen. Het wijzigen of inzien van gegevens dient herleidbaar te zijn tot de natuurlijke persoon die de handeling verricht.

Autorisaties die hierbij bijzondere aandacht behoeven zijn de privileges, waarmee het mogelijk is interne elektronische informatie buiten het (beveiligings)domein van de Belastingdienst te brengen en vice versa.

B.1.4. Beleid op informatieuitwisseling

Vanuit informatie gezien

Informatieuitwisseling omvat zowel in- en uitgaande informatie, langs alle kanalen zoals post, telefoon of elektronisch, formeel of informeel.

Enerzijds geldt voor de Belastingdienst als organisatie dat hij gehouden is aan de relevante wet- en regelgeving over de bescherming van vertrouwelijke (persoons)gegevens en (elektronische) informatieuitwisseling. Anderzijds gelden er voorschriften voor de medewerkers, gericht op plichten als geheimhouding en gewenst gedrag. Met name in de contacten met burgers en bedrijven wordt hier aandacht aan besteed binnen de dienstverleningsstrategie. We hanteren de volgende uitgangspunten:

- Uitwisseling van informatie met een wettelijke grond, met ketenpartners, gebeurt op basis van de bestaande wet- en regelgeving. We voldoen hieraan en stellen geen aanvullende eisen. Massale gegevensuitwisseling met derden wordt namens de Belastingdienst uitsluitend door de Centrale Administratie uitgevoerd;
- Andere uitwisseling van formele of vertrouwelijke informatie gebeurt onder het treffen van adequate generieke maatregelen ten aanzien van vertrouwelijkheid of rechtsgeldigheid, om bijvoorbeeld de bescherming van persoonsgegevens, authenticiteit of onweerlegbaarheid te borgen;
- Voor alle andere uitwisseling van informatie gelden voorwaarden en gedragsregels.

Presentatie

We presenteren veel (persoons)gegevens aan burgers, bedrijven en overheden. Maar alleen de benodigde gegevens en alleen aan personen en organisaties waarvan we een bepaalde zekerheid hebben omtrent de identiteit en bevoegdheid. Ook letten we op welke gegevens fraudegevoelig kunnen zijn omdat we de drempel voor mis- en oneigenlijk gebruik van elektronisch berichtenverkeer niet willen verlagen. We sluiten aan op de overheidsbreed ontwikkelde voorzieningen als DigiD, eID en MijnOverheid.

Authenticatie	<p>We vertrouwen onze medewerkers bij het muteren en vastleggen van gegevens. Onze gegevens zijn altijd vertrouwelijk. Het is in ons eigen belang dat we de aan ons toevertrouwde gegevens beschermen tegen ongeautoriseerde inzage of mutatie en dat de in- en uitgaande gegevens betrouwbaar zijn. We kiezen hierbij voor algemene authenticatiemiddelen met een beperkt aantal niveaus. Afhankelijk van de doelgroep maken we ruimte voor extra maatregelen.</p> <p>Aanvullend gelden, voor alle uitwisseling, voorschriften als het ARAR en de PUB. Specifieke voorwaarden, bijvoorbeeld voor het gebruik van e-mail of informatie van internet, houden rekening met deze invalshoeken met aandacht voor samenhang en werkbaarheid (zie ook B.1.7).</p> <p>Deze aspecten dienen breed in de bedrijfsvoering te worden verankerd.</p>
Vanuit domein gezien	<p>Naast de bovenstaande inhoudelijke indeling, kan ook een logische indeling worden gemaakt. De invalshoek is er dan één vanuit het organisatiedomein, waarbij domein vertaald kan worden in <i>invloedssfeer</i> in de zin van fysieke bescherming en beheer:</p>
Binnen domein, buiten basis beveiligingsstelsel	<ul style="list-style-type: none"> - Uitwisseling van informatie met partijen <i>buiten</i> het domein van de Belastingdienst. Deze uitwisseling gebeurt met burgers, ondernemers en andere (overheids)partijen en betreft informatie uit het primaire proces. Zodra de informatie buiten het domein van de Belastingdienst is, hebben we minder invloed op risicomitigerende maatregelen. We hanteren afspraken voor beveiliging in transport, opslag en verwerking tot vernietiging. - Uitwisseling van informatie <i>binnen</i> het domein van de Belastingdienst. Hiervoor geldt het basisniveau beveiliging.
Encryptie bij transport en opslag	<p>Bij alle transport van gegevens zorgen we voor adequate beveiliging door middel van het principe van isolatie, bijvoorbeeld in de vorm van fysieke of logische paden of encryptie. Met name encryptie geldt niet alleen bij gestructureerde gegevensuitwisseling maar ook bij het interne netwerk, een laptop, tablet, CD/DVD, USB-stick of met externe e-mail.</p>
Bedrijfsmiddelen	<p>In principe wordt bedrijfsinformatie uitsluitend verwerkt op de door de (onder verantwoording van de) Belastingdienst beschikbaar gestelde middelen.</p> <p>Gegevens van burgers en bedrijven dienen te worden versleuteld, niet alleen tijdens transport maar ook bij opslag. Dit ligt in lijn met de maatschappelijke en marktontwikkelingen en volgt onder meer uit het kabinetsstandpunt rond encryptie¹⁵ en de risicorapportage van het Centraal Planbureau¹⁶, op basis van het Cybersecuritybeeld Nederland van het NCSC¹⁷.</p>
Fysieke gegevensdragers	<p>Bij fysieke gegevensdragers bedoeld voor gegevensuitwisseling met derden isoleren we bijvoorbeeld door middel van encryptie¹⁸, aanvullend beschreven in de <i>Procedure voor fysieke gegevensuitwisseling met externe partijen – voor alle dienstonderdelen</i>¹⁹.</p>
Gevonden gegevensdragers	<p>Bijzondere aandacht betreft de omgang met gevonden gegevensdragers. USB-sticks, CD's en dergelijke kunnen door kwaadwillenden gebruikt worden voor het introduceren van malware op computers. Een populaire werkwijze daarvoor is het "verliezen" van een gegevensdrager waarop de malware is geplaatst.</p>

¹⁵ Kamerbrief over kabinetsstandpunt encryptie, VenJ/EZ, 4 januari 2016

¹⁶ Risicorapportage cyberveiligheid economie, Centraal Planbureau, 6 juli 2016,

¹⁷ VenJ/Nationaal Cyber Security Centrum

¹⁸ Informatiebeveiliging gegevensdragers, DGBel/CSO en CIO, 29 april 2010

¹⁹ Versie 1.0, B/CIE, 28 april 2010

Gevonden USB-stick nooit bekijken	Vervolgens wordt vertrouwd op de nieuwsgierigheid en/of eerlijkheid van de vinder, die al dan niet in een poging om de rechtmatige eigenaar te achterhalen wil weten wat er op staat. Daarmee wordt de malware in werking gezet. Het is dan ook uitdrukkelijk verboden om een gevonden gegevensdrager in een PC te stoppen. Gevonden gegevensdragers dienen te worden onderzocht door het CIE/Security Operations Center. Daartoe wordt de gegevensdrager bij een receptiemedewerker ingeleverd, die de te volgen procedure ²⁰ kent.
Antivirus, intrusion detection	Bij alle elektronische informatieuitwisseling van <i>buiten</i> het belastingdienst domein wordt op schadelijke programmatuur gecontroleerd en gescand (virussen, malware etc, ook op versleutelde stromen) en wordt de grens van het domein beschermd en gecontroleerd tegen aanvallen van binnen en buiten. Hierbij worden de richtlijnen die binnen de rijksoverheid gelden (zoals vanuit het NCSC) gevolgd en worden adequate middelen ingezet.
Clouddiensten	We slaan zelf geen gegevens op buiten onze invloedssfeer. Ten aanzien van clouddiensten volgen we het rijksoverheidsbeleid zoals beschreven in de informatiseringsstrategie Rijk ²¹ en de daaraan voorafgaande cloudstrategie ²² . Wat informatiebeveiliging betreft blijkt dat het via een "open" cloud uitbesteden van ICT diensten, dan wel opslag van informatie buiten Nederland, risico's met zich meebrengt die nog niet voldoende kunnen worden afgedekt. (sic)
Sourcingstrategie	In de herijkte sourcingstrategie ²³ staat dat het afnemen van clouddiensten tot de mogelijkheden behoort maar dat er alleen geshopt mag worden in de private cloud van de Belastingdienst of de Rijksoverheid, en dan nog alleen onder strikte condities. Deze condities hebben met name betrekking op het waarborgen van de beschikbaarheid en betrouwbaarheid van data die gehost wordt in de cloud.
Mobiele apparatuur	Een bijzondere vorm informatieuitwisseling binnen het domein zie je bij draagbare apparatuur (PDA's, tablets, smartphones, USB-sticks of draagbare computers (PPC's)). Deze apparatuur kan fungeren als informatiedrager, die weliswaar binnen het domein van de Belastingdienst valt, maar buiten de beschermende invloedssfeer ervan kan verkeren. Hiervoor treffen we extra beveiligingsmaatregelen: We transporteren ook hier niet onnodig gegevens, verstrekken geen onnodige autorisaties en we bieden hard- en softwarematige voorzieningen aan zoals externe media encryptie. Daarbij zijn we kritisch op de noodzaak van het gebruik van een bedrijfsmiddel, koppelen dat bij voorkeur aan een functie en zien er op toe dat de extra maatregelen ook daadwerkelijk worden gebruikt.
Label, logo of merk	Voor al de <i>bedrijfsmiddelen</i> die in dit kader worden gebruikt, geldt dat de herkenbaarheid als belastingdienst eigendom minimaal moet zijn. Uitwisseling en verwerking van informatie in het primair proces zoals de massale gegevensverwerking, ook binnen de eigen organisatie, is gebonden aan de wet- en regelgeving omtrent de bescherming van persoonsgegevens. Koppeling van (data uit) geautomatiseerde systemen gebeurt met inachtneming hiervan.
Koppeling van systemen	Bij de koppeling van (data uit) kantoorautomatiseringssystemen ontstaan risico's voor bijvoorbeeld controlemedewerkers, rechercheurs, vertrouwenspersonen, bedrijfsartsen en OR-leden (toegankelijkheid tot e-mail, agenda). Deze worden opgevangen door huisregels, houding en gedrag. Dit

²⁰ Richtlijn voor de omgang met gevonden gegevensdragers, B/CIE, 19 januari 2015.

²¹ I-strategie Rijk, BZK/DGOBR, 15 november 2011

²² Cloud Strategie, BZK/DIR, 20 april 2011

²³ Actualisatie Sourcingbeleid IV Belastingdienst, IV-Overleg, versie 4 september 2013

	<p>hoort thuis in de decentrale risicoanalyse en valt onder het desbetreffende management van een bedrijfsonderdeel.</p>
Archiefbeheer	<p>De Belastingdienst heeft de verantwoordelijkheid te borgen dat de ontvangen, gecreëerde en verzonden informatie betrouwbaar en duurzaam toegankelijk is. Dit geldt tot het moment van verwijdering, waarbij de verwijdering conform vastgelegde procedures verloopt.</p> <p>De informatie moet daarom volledig en authentiek zijn, vindbaar en beschikbaar, blijvend leesbaar (in bepaalde formaten zijn vastgelegd), waar selectiebeleid op kan worden toegepast.</p>
Bewaartermijnen	<p>Dergelijk informatiebeheer stelt de Belastingdienst in staat om aantoonbaar te voldoen aan de wettelijk vastgestelde bewaartermijnen. Hiermee ondersteunen we het leidend beginsel "Ik weet dat de Belastingdienst mijn gegevens niet langer bewaart dan wettelijk is toegestaan"²⁴.</p>
Autorisaties	<p>De kwaliteit van het informatiebeheer is in sterke mate bepalend voor de kwaliteit van de informatievoorziening, waarbij informatie wordt verstrekt op basis van autorisaties.</p> <p>B/CFD stelt als archiefbeheerder kaders voor de archivering en stelt instrumenten ter beschikking voor archiefbeheer zodat kan worden voldaan aan gestelde eisen. De eisen aan archiefbeheer worden bij het ontwerp van processen en informatiesystemen meegenomen en geborgd in de concernarchitectuur.</p> <p>Vanuit de toezichthoudende taak van B/CFD²⁵ wordt de informatiehuishouding jaarlijks middels een monitor getoetst of deze voldoet aan de normen en of er aanleiding is tot verbetering.</p>
Afvoer en vernietiging	<p>Een onbedoelde vorm van informatieuitwisseling betreft afvoer en vernietiging van ICT materieel, waaronder we hier met name Pc's, laptops, tablets, verwijderbare of externe harde schijven en USB-sticks verstaan.</p> <p>Afvoer gebeurt door Domeinen Roerende Zaken (DRZ), volgens de regelgeving voor afvoer materieel²⁶ en de <i>Regeling materieelbeheer rijksoverheid 2006</i>²⁷, waarin onder meer de bepalingen voor registratie en beheer staan opgenomen. De verantwoordelijkheid en risico's blijven bij de Belastingdienst tot de formele overdracht aan DRZ (proces-verbaal van acceptatie).</p>
Meldplicht bij datalekken van persoonsgegevens	<p>Een andere onbedoelde vorm van informatieuitwisseling betreft datalekken. Deze moeten worden gemeld zoals de Wet bescherming persoonsgegevens voorschrijft met de meldplicht bij de doorbreking van maatregelen voor de beveiliging van persoonsgegevens.</p> <p>Een melding van een datalek gebeurt aan de Autoriteit Persoonsgegevens²⁸. De meldplicht geldt wanneer de nadelige gevolgen zich hebben voorgedaan en dat er ernstige nadelige gevolgen zijn voor de bescherming van de verwerkte persoonsgegevens. <i>Ernstig</i> wordt bepaald aan de hand van de aard en omvang van de inbreuk, de aard van de gelekte persoonsgegevens en de mate waarin technische beschermingsmaatregelen zijn getroffen. De ernst wordt ingeschat en hoeft niet te zijn gebleken, zodat dit van geval tot geval moet worden beoordeeld. Voorts geldt dat alleen gemeld moet worden als de gelekte</p>

²⁴ Leidend beginsel bij afspraak 9 uit het Toetsingskader Architectuurboard Belastingdienst.

²⁵ Regeling Archiefbeheer Belastingdienst 2011

²⁶ Vanaf 1 juli 2010 vernietigt DRZ alle af te voeren ICT middelen (shredder)

²⁷ Handboek Financiële Informatie en Administratie Rijksoverheid (Hafir), MvF, 18 april 2006

²⁸ Voorheen het College Bescherming Persoonsgegevens

persoonsgegevens niet op passende wijze zijn beschermd, bijvoorbeeld door versleuteling, anonimisering of *remote wipe*. Bovendien wordt er gemeld aan de betrokkenen als er waarschijnlijk ongunstige gevolgen zijn voor zijn of haar persoonlijke levenssfeer.

Sancties	De Autoriteit Persoonsgegevens heeft de bevoegdheid om aan verantwoordelijken en bewerkers bestuurlijke boetes op te leggen voor een groot aantal specifieke overtredingen van de Wbp, zoals het verwerken van persoonsgegevens zonder legitiem belang of zonder rechtvaardigingsgrond (bijv. toestemming), het gebruik van persoonsgegevens voor onverenigbare doeleinden, het te lang bewaren van persoonsgegevens, schending van de beroepsgeheimhoudingsplicht, het niet of onvoldoende nemen van beveiligingsmaatregelen, overtreding van het verbod op verwerken van bijzondere gegevens (zoals etniciteit, gezondheidsgegevens en strafrechtelijke veroordelingen) of het BSN nummer, het niet of onvoldoende informeren van de betrokkene over het privacybeleid van de organisatie, het niet melden van een datalek, niet voldoen aan inzage-, of correctieverzoeken of het negeren van het recht van verzet, en het overtreden van de regels rond data-export naar niet-Europese landen.
Specifieke overtredingen	
Geheimhoudingsplicht	De Autoriteit Persoonsgegevens heeft ook de mogelijkheid om aan individuele werknemers een boete op te leggen voor het niet naleven van hun geheimhoudingsplicht.

B.1.5. Beleid op gebruik van mobiele apparatuur

Mobile devices	De inzet van ICT-middelen wordt steeds meer geharmoniseerd met rijksbrede ontwikkelingen. De hoofdlijn hiervan is: functionaliteit komt los van het eronder liggende apparaat. Dit geldt voor alle applicaties. Naast bedrijfsapplicaties is er het interne en rijksbrede ICT-aanbod voor persoonlijke productiviteit. We spreken dan over digitaal, online samenwerken en aanvullende applicaties. Hierin vallen zaken als e-mail, agenda, contacten, kantoor- en applicaties voor specifieke taken.
Footprint	Voor alle functionaliteiten geldt: de afhankelijkheid met het apparaat wordt gereduceerd tot een minimale <i>footprint</i> . Dat betekent dat functionaliteit alleen nog via de browser en/of een mobiele app aangeboden wordt. Ook alle identiteits- en autorisatiefuncties worden op (of achter) dit concept gebouwd.
Appstores	Beveiliging van data en het netwerktransport er van zal op het niveau van de functionaliteit (browser of app) plaatsvinden. Tussen browser of app en de <i>rijkscloud</i> zal een veilige verbinding zorgen voor de exclusiviteit van gegevens in (met name) het primaire proces. In de Belastingdienst en rijksbrede 'appstores' zal het formeel toegekende aanbod aan apps beschikbaar komen.

B.1.5.1. Gebruik van mobiele apparatuur in het buitenland

Wanneer de noodzaak bestaat om mobiele apparatuur mee te nemen naar of te gebruiken in het buitenland, dient toestemming gevraagd te worden aan de direct leidinggevende. Impliciet in deze toestemming wordt het risico geaccepteerd dat bij een grenscontrole het wachtwoord moet worden afgegeven, zodat de medewerker geen integriteitsrisico loopt. Wel dient het wachtwoord zo snel mogelijk daarna te worden gewijzigd.

B.1.5.2. Beheer van mobiele apparatuur

Centraal beheerd	De Belastingdienst voert centraal beheer uit op mobiele apparatuur voor de ondersteuning en beveiliging er van. Het richt zich op alle mobiele apparaten die verbinding (willen) maken met de Belastingdienst-infrastructuur of diensten
------------------	--

Keuze bij medewerker	<p>en werkt daarmee in principe apparaatonafhankelijk. Het gaat uit van de te gebruiken functionaliteiten (apps, diensten) om op een apparaat bepaalde (beveiligings) instellingen af te dwingen. De eisen die achter deze instellingen zitten, worden ingegeven vanuit de exploitatie (CIE) samen met de business (bedrijfsonderdelen).</p> <p>Het logische gevolg hiervan is dat we niet alle apps of diensten op alle soorten apparaten ondersteunen en dat het niet-accepteren van onze instellingen inhoudt dat een bepaalde functionaliteit in dat geval niet kan worden gebruikt.</p> <p>Er wordt permanent toegezien op de technische integriteit en beschikbaarheid van de infrastructuur en diensten. Daarom wordt een algemeen basisniveau ingesteld aan de hand van <i>best practices</i>. Aanvullend maken we bepaalde keuzes die bij onze organisatie en cultuur passen, maar wel generiek zijn. Deze keuzes worden hieronder toegelicht.</p>
Vertrouwen en verantwoordelijkheid	<p>B.1.5.3. Instellingen op mobiele apparatuur</p> <p>Bij de bepaling van de verschillende instellingen gaan we uit van het vertrouwen in onze medewerkers, waarbij een grotere vrijheid past bij de eigen verantwoordelijkheid. De medewerkers blijven altijd wel gehouden aan het hiertoe opgestelde gebruiks- en privacybeleid. De generieke keuzes zijn als volgt:</p> <p>Wachtwoorden voor toegang</p> <ul style="list-style-type: none"> - We stellen eisen aan de minimale lengte en samenstelling van de toegangscode tot het apparaat. Afhankelijk van de ontwikkelingen en het gebruik van vertrouwelijke gegevens op het apparaat, stellen we aanvullende eisen aan de lengte en samenstelling van de code; - We vereisen een periodieke wijziging van de toegangscode; - Na een beperkt aantal mislukte pogingen tot toegang wordt het apparaat teruggezet naar fabrieksinstellingen (gewist). <p>Versleuteling van de gegevens</p> <ul style="list-style-type: none"> - Gegevens die op het apparaat worden opgeslagen moeten worden versleuteld; - Op iOS apparaten worden gegevens versleuteld zodra een wachtwoord is ingesteld. Op Android apparaten wordt versleuteling op applicatie/containerniveau afgedwongen; - De eisen die we aan versleuteling stellen zijn marktconform. <p>Blokkeren van toegang bij afwijkingen</p> <ul style="list-style-type: none"> - Wanneer een apparaat afwijkt van de af te dwingen instellingen (non-compliance), wordt de toegang tot de infrastructuur geblokkeerd en/of worden de zakelijke gegevens gewist en/of wordt een melding aan de beheeromgeving gedaan. Dit laatste gebeurt bijvoorbeeld wanneer het apparaat een bepaald aantal dagen niet met de infrastructuur verbonden is geweest; - Wanneer de noodzakelijke beheercomponenten of accounts van het apparaat worden verwijderd wordt de toegang geblokkeerd. Dit gebeurt ook bij jailbreaking of rooting van een apparaat of bij het uitzetten van de versleuteling; - We stellen eisen aan (versies van de) besturingssystemen op het apparaat. <p>Wissen van mobiele apparaten</p> <ul style="list-style-type: none"> - Een apparaat kan door de medewerker zelf of de servicedesk worden gewist, waarbij er onderscheid gemaakt kan worden tussen zakelijke en privégegevens.
Remote wipe	<ul style="list-style-type: none"> - Een apparaat kan door de medewerker zelf of de servicedesk worden gewist, waarbij er onderscheid gemaakt kan worden tussen zakelijke en privégegevens.

Privacy van medewerkers

- | | |
|------------------------|--|
| Geïnstalleerde apps | - De aanwezigheid (installatie) van de noodzakelijke beheercomponenten op een apparaat wordt bijgehouden (gesynchroniseerd). Deze synchronisatie omvat ook de andere op het apparaat geïnstalleerde apps en kan worden gebruikt voor licentiedoeleinden en het kunnen weren van ongewenste apps (blacklist); |
| Laatst bekende locatie | - De locatiegegevens worden alleen gebruikt voor het bijhouden van de laatst bekende locatie ten behoeve van het terugvinden van het apparaat of in het kader van strafrechtelijk onderzoek bij diefstal. |

Indien er sprake is van een redelijke verdenking of vermoeden van ongeoorloofd handelen kan in opdracht van het management en DGBel/JZ in het kader van een integriteitsonderzoek de locatiefunctionaliteit worden gebruikt.

B.1.6. Beleid op telewerken/thuiswerken

Telewerken in de zin van plaats- en tijdsafhankelijk werken zal in onze organisatie een prominenter rol krijgen. Hierin sluiten we aan bij de tendens in de rijksdienst, waarin actief wordt ingespeeld op de mogelijkheden die de ICT biedt. De Raamregeling Telewerken²⁹ is ook voor onze organisatie van toepassing.

Vrijwilligheid	Deze regeling staat echter los van de beleidsmatige wenselijkheid van telewerken, waarbij de medewerker werkzaamheden verricht in of vanuit zijn of haar woning. Zo gauw deze werkvorm niet is vereist vanuit de functie van een medewerker, wordt deze per definitie op basis van vrijwilligheid toegepast. De raamregeling geeft wel meer duidelijkheid over de rechtspositionele aspecten van telewerken zodat toepassing ervan op dat vlak zorgvuldig kan gebeuren.
----------------	---

Telewerken wordt in onze organisatie uitsluitend op basis van vrijwilligheid toegepast: het is geen recht. Maar het is ook geen plicht: er zijn bijvoorbeeld geen functies waarbij de plaats van tewerkstelling de woning van de medewerker is. De organisatie is niet verplicht om telewerkvoorzieningen te verschaffen.

Keuze aan bedrijfs onderdeel	Zoals de raamregeling ook voorstaat, worden afspraken over de invoering van telewerken het best op decentraal, dat wil zeggen op bedrijfs onderdeelniveau, gemaakt. Uiteindelijk wordt de afweging tot telewerken door leidinggevende en medewerker samen gedaan.
------------------------------	---

DWB en DWR	Telewerken sluit aan bij de mogelijkheden die de Digitale Werkomgeving Belastingdienst ³⁰ (DWB) biedt. DWB is gericht op plaats-, tijd- en apparaatafhankelijk werken en houdt eveneens rekening met de eisen die aan de mobiliteit van de medewerkers worden gesteld vanuit de organisatiegerichte huisvesting. DWB volgt in principe de Digitale Werkomgeving Rijk die eveneens in de I-strategie Rijk wordt benoemd.
------------	--

De functionaliteit van DWB wordt uiteindelijk gekoppeld aan *digitale profielen* van onze medewerkers, waarbij beheer en beheersing van risico's is ingeregeld. In principe is de functionaliteit ontkoppeld van het gebruikte soort apparaat.

TPAW	Steeds meer medewerkers zijn in staat de werkzaamheden tijd-, plaats- en apparaatafhankelijk (TPAW) uit te voeren voor de Belastingdienst. Dit maakt
------	--

²⁹ Raamregeling Telewerken, BZK, 1 juni 2001.

³⁰ De Digitale Werkomgeving Belastingdienst volgt de Rijkswerkomgeving.

ons flexibeler in waar en wanneer we ons werk doen maar vraagt een grote mate van zelfstandigheid, zorgvuldigheid en verantwoordelijkheid van ons. Privé en werk lopen vaker in elkaar over en ieder voor zich moet hierin een balans vinden. Er wordt van je verwacht dat je werk van goede kwaliteit is en volgens de gemaakte resultaatafspraken wordt opgeleverd.

Zaken als afspraken nakomen, frequent en helder communiceren over het werk en je beschikbaarheid worden nog belangrijker. Een verantwoorde omgang met gevoelige data en informatie is vereist als deze informatie op afstand wordt geraadpleegd.

HNW

De visie van de Belastingdienst op Het Nieuwe Werken (HNW) en TPAW is bepaald³¹. Ons eigen zakelijk social media platform ConnectPeople biedt een veilige en beveiligde manier van samenwerken en communiceren over het werk.

BYOD/CYOD/COPE

Er zijn rijksbrede beleidskaders³² voor het werken op eigen apparatuur. Hierin wordt onderscheid gemaakt tussen apparatuur "buiten beheer", "met enig beheer" en "met extra beheer". De eerste categorie is te associëren met *bring your own device*, de tweede met *company owned, personally enabled or choose your own device*, zoals dit in de Belastingdienst is ingevoerd. Er zijn nog witte vlekken op dit relatief nieuwe terrein, zoals de financiële en juridische consequenties, aansprakelijkheid, arbeidsvoorwaarden etc. die hierbij komen kijken. Bij de invoering van HNW wordt hier aandacht aan besteed en we volgen de (toekomstige) rijksbrede beleidskaders op dit vlak.

De Belastingdienst gebruikt Enterprise Mobility Management voor het beheer van mobiele devices. Hiermee worden (beveiligings)instellingen afgedwongen voor alle mobiele devices die verbinding hebben met onze infrastructuur.

Apps

In het verlengde van het bedoelde gebruik van mobiele apparatuur geldt als richtlijn dat wanneer applicaties (*apps*) op de mobiele devices worden gebruikt met vertrouwelijke gegevens ofwel ter ondersteuning van bedrijfsprocessen, dat deze door de Belastingdienst of Rijksoverheid moeten worden verstrekt. Apps die niet in eigendom of licentie zijn bij de Belastingdienst of Rijksoverheid dienen hiervoor niet gebruikt te worden. Zie hiervoor ook de cloudstrategie in paragraaf B.1.4.

Beveiliging van apps omvat niet alleen de technische maatregelen maar raakt vooral ook de bewustwording van de medewerker. Daarnaast vormt onvoldoende aandacht voor monitoring en beheer een groot afbreukrisico. De business dient een bewuste afweging te maken tussen beveiliging en functionaliteit.

Eigen apparatuur

Telewerken is in eerste instantie gericht op toegang tot de interne algemene informatiebronnen (intranetten), e-mail en agenda en is geschikt voor gebruik op apparatuur "buiten beheer", zij het met enige aanvullende maatregelen zoals versleuteling en twee-factor authenticatie (*bring your own device*), meestal in de vorm van de eigen thuis-PC van de medewerker.

Hier treffen we adequate aanvullende maatregelen voor bijvoorbeeld de verbinding en het desbetreffende apparaat (eisen aan de browserversie, versleuteling, wissen van elektronische sporen etc, gedragsvoorschriften).

³¹ Visiedocument Het Nieuwe Werken, MT BD, maart 2013

³² BZK/DGOBR en ICCIO *Rijksbrede beleidskaders voor ondersteuning apparaatonafhankelijk werken*, november 2012 Gebaseerd op de *I-strategie Rijk* en notitie *Rijksbrede ambities rondom Tijd-, Plaats- en Apparaatonafhankelijk Werken (TPAW)*, juli 2012

Bedrijfsmiddelen	Voorts kan telewerken worden ingericht met behulp van Belastingdienst apparaten "met enig beheer" waarbij toegang tot bedrijfsapplicaties tot de mogelijkheden behoort. Het betreft dan bedrijfsmiddelen (<i>choose your own device</i>) waarbij ook extra beveiligingsmaatregelen en gedragsregels horen.
Extra bescherming	Er dienen afdoende en zoveel mogelijk generiek aanvullende maatregelen te worden getroffen. Denk in de techniek aan <i>browsercache-cleaners</i> waarmee informatie die ongemerkt is achtergebleven wordt verwijderd en <i>host-checkers</i> die vooraf controleren of een platform op een afdoende onderhouden niveau zit of dat vereiste antivirusmaatregelen zijn getroffen.
Randvoorwaarden telewerken	Bedrijfsonderdelen kunnen bepaalde vormen van telewerken verbijzonderen en daarbij aanvullende maatregelen treffen. Telewerken stelt het vertrouwen in de medewerker centraal, zowel wat betreft integriteit, houding en gedrag, als op het gebied van beveiliging. Aanvullend vindt de toegang tot het bedrijfsnetwerk minimaal plaats op basis van twee-factor authenticatie en versleuteling en worden er minimumeisen gesteld aan de apparaten waarmee toegang wordt verkregen, waarbij verplichte installatie van Belastingdienst-controleprogrammatuur tot de mogelijkheden behoort. Daarnaast gelden er (gedrags)voorwaarden aan het gebruik van voorzieningen voor telewerken.
Taak- of kenniswerker, mobiel of op kantoor	De digitale profielen sluiten in de basis aan bij de vier typologieën die voor de medewerkers worden gehanteerd in de Meerjarenvisie Huisvesting: de taakwerker en kenniswerker op kantoor en de mobiele taakwerker en kenniswerker. Elke groep heeft specifieke eisen voor wat betreft functionaliteit en eisen die vanuit de organisatie worden gesteld. De invulling van de eisen moet met behulp van profielen en privileges worden beheerd. Overigens wordt door de invoering van HNW het onderscheid tussen de groepen minder zichtbaar.
B.1.7. Beleid op het gebruik van internet en e-mail	
Geheimhoudingsplicht	Het gebruik van internet is niet zonder risico's. E-mailberichten kunnen door veel partijen worden gelezen of gewijzigd. Hyperlinks in berichten kunnen worden misbruikt. Het vinden van informatie is eenvoudig, maar we weten vaak niet of die informatie ook betrouwbaar is. Als je informatie naar buiten brengt, kan dat leiden tot het niet nakomen van de geheimhoudingsplicht. Ook mag je geen standpunt innemen dat het goed functioneren van jezelf in je functie of de overheid belemmert. E-mail mag worden gebruikt voor de uitwisseling van vertrouwelijke informatie of formele berichten mits we vooraf aanvullende maatregelen hebben getroffen en afspraken hebben gemaakt ten aanzien van het borgen van vertrouwelijkheid en authenticiteit van een bericht. Deze kunnen anders niet voldoende gewaarborgd worden, waarmee de geheimhoudingsplicht in het geding komt. Als deze maatregelen niet getroffen zijn, dienen zulke berichten op de gebruikelijk manier, zoals per post, te worden verzonden.
Terughoudendheid	De BelastingTelefoon (Roadmap Digitale Dienstverlening) positioneert e-mail niet als massaal kanaal maar voor één op één contacten, met de nodige terughoudendheid.
Hyperlinks	E-mail wordt eventueel gebruikt voor berichten als notificaties en statusupdates. De Belastingdienst gebruikt nooit hyperlinks in e-mailberichten vanwege het risico op misbruik door cybercriminelen.
Goed ambtenaarschap	In het gebruik van internet, e-mail en online communicatie wordt van de medewerkers <i>goed ambtenaarschap</i> verwacht. Daarom stelt de Belastingdienst

voorwaarden aan het gebruik van internet. Ze zijn gebaseerd op de Personele Uitvoeringsbepalingen Belastingdienst (PUB) en geven een nadere invulling aan het begrip *goed ambtenaar* zoals bedoeld in artikel 50 van het Algemeen Rijksambtenarenreglement.

Overigens wordt er permanent toegezien op de technische integriteit en beschikbaarheid van de infrastructuur en diensten. Alle communicatiestromen (inclusief versleutelde) worden hiertoe gescand en gelogd. Verwerkingen van persoonsgegevens worden verricht met inachtneming van de Wet bescherming persoonsgegevens.

Ten behoeve van het gebruik van internet op de werkplek wordt toegang geboden volgens het principe van black- en whitelisting. Wijzigingen hierin dienen vooraf te worden beoordeeld onder meer op basis van risicoanalyse en -acceptatie door zowel het Security Operations Center (aanbodzijde) als het betrokken management (vraagzijde).

B.1.8. Beleid op het gebruik van sociale media

Sociale media zijn in deze tijd niet meer weg te denken. Privé gebruik je het om contacten te onderhouden, foto's met vrienden te delen, deel te nemen aan discussies, filmpjes te bekijken etc. Maar ook voor je werk wordt het gebruik van sociale media steeds belangrijker. Hoe ga je nu goed met dit platform om en waar ligt de grens tussen werk en privé?

Sociale media zijn media die voor jouw werk bij de Belastingdienst veel voordelen hebben. Zo kun je snel en makkelijk informatie opzoeken, met collega's van gedachten wisselen, op de hoogte blijven van nieuwe ontwikkelingen en inzicht krijgen in wat de buitenwereld over de Belastingdienst en dienstverlening denkt, zodat we deze constant kunnen verbeteren. De Belastingdienst moedigt het dan ook aan, dat je actief gebruik maakt van al deze mogelijkheden.

Het gebruik van sociale media is echter ook gebonden aan bepaalde regels. Net als bij andere soorten van communicatie, zijn de drie basiswaarden van de Belastingdienst leidend: geloofwaardigheid, verantwoordelijkheid en zorgvuldigheid. Daarbij is het van groot belang te bedenken dat wat je op internet plaatst lange tijd beschikbaar blijft en makkelijk door anderen kan worden gebruikt of misbruikt. Het is daarom extra belangrijk om goed na te denken of de teksten, foto's en/of filmpjes die je plaatst de reputatie van de Belastingdienst kunnen schaden of de organisatie in verlegenheid kunnen brengen. Blijf daarom zakelijk in je uitlatingen en bespreek en deel nooit gevoelige informatie online over de Belastingdienst, onze klanten, partners of over elkaar. Dit betekent ook dat je geen collega's of andere belanghebbenden van de Belastingdienst citeert.

Omdat je sociale media zowel voor je werk als voor privédoeleinden gebruikt is het belangrijk om duidelijk aan te geven wanneer je als medewerker van de Belastingdienst online actief bent en wanneer op persoonlijke titel.

Ook wanneer je op persoonlijke titel informatie online zet is het altijd belangrijk na te denken, of dat wat je zegt en/of laat zien de Belastingdienst geen schade kan berokkenen. Kortom: gedraag je online ook als goed ambtenaar net zoals je dat offline zou doen, respecteer elkaars privacy, wees vriendelijk en behandel de ander met respect.

Daarnaast moet je je ook bewust zijn van de mogelijk negatieve effecten voor jezelf. Internetten is werken in een glazen huis. Je bent persoonlijk zichtbaar. Realiseer je dat lezers snel achter je identiteit kunnen komen door profielen en andere informatiesporen aan elkaar te koppelen.

Als je via de pers een algemene vraag of interviewverzoek ontvangt, stuur dit dan door naar de persvoorlichter³³ van je bedrijfs onderdeel.

Aanvullend heeft het Ministerie van Algemene Zaken de *Uitgangspunten online communicatie rijksambtenaren* gepubliceerd. Deze uitgangspunten volgen we en zijn samen met het bovengenoemde opgenomen in de in mei 2011 vastgestelde *Voorwaarden aan het gebruik van e-mail, internet en online communicatie* die zijn opgenomen in de PUB.

B.1.9. Beleid op versterkte weerbaarheid

B.1.9.1. Computercriminaliteit

Cybercrime

Onder computercriminaliteit of cybercrime verstaan we alle vormen van criminaliteit die betrekking hebben op computersystemen of die met computersystemen (inclusief netwerken) worden gepleegd, zowel van binnen als van buiten de organisatie. Het gaat om (georganiseerde) criminele activiteiten waarbij gebruik wordt gemaakt van ICT.

Ze zijn gericht tegen personen, eigendommen of organisaties, of tegen elektronische communicatienetwerken en informatiesystemen.

We bestrijden computercriminaliteit door:

- Het versterken van detectie van interne en externe computercriminaliteit via monitoring van informatiesystemen, het alert maken van de medewerkers en de melding van mogelijk strafbare feiten;
- De afhandeling van meldingen, verstoringen en incidenten niet alleen gericht te laten zijn op continuïteit van de bedrijfsvoering, maar ook op het verzamelen van bewijsmateriaal en het veiligstellen van gegevens die kunnen helpen bij opsporing, vervolging en het eventueel verhalen van schade;
- Aansluiting te hebben met het NCSC en het in overleg met DGBel/JZ doen van aangifte van computercriminaliteit bij de politie.

Phishing

Voor de afhandeling van *phishingmails* is een proces ingeregeld zowel intern voor medewerkers als extern voor burgers, bedrijven en organisaties. De meldingsprocedure hiervoor dient helder en het loket goed vindbaar te zijn. In samenwerking met het NCSC worden vervolgcacties ondernomen.

B.1.9.2. Spionage

KWAS

Mede naar aanleiding van de kabinetsreactie op het rapport *Kwetsbaarheidsanalyse Spionage Nederland (KWAS)* van de Inspectie Openbare Orde en Veiligheid³⁴ zijn de *cruciale belangen* van de Belastingdienst in kaart gebracht en vastgesteld. Onder een cruciaal belang verstaan we een verzameling van gegevens waarvan onbevoegde kennisname onze bedrijfsbelangen aantast en waarvan redelijkerwijs aangenomen kan worden dat andere partijen er interesse in hebben³⁵.

Indien opportuun wordt in de rapportagecyclus rekening gehouden met dreigingen vanuit spionage.

³³ De Instructie Perscontacten is op Belastingnet te vinden

³⁴ Vanaf 16 april 2012 de Inspectie Veiligheid en Justitie

³⁵ Definitie uit de Handleiding KWAS, BZK/AIVD januari 2011

Backdoors	In dit kader dienen er ook garanties te zijn dat onze gegevens veilig zijn bij verwerking door (<i>closed source</i>) programmatuur en over in hoeverre leveranciers de vertrouwelijkheid van onze gegevens kunnen waarborgen.
Sourcecode	De door ons (of in opdracht) ontwikkelde programmatuur en met name broncode heeft daarbij conform de cruciale belangen passende bescherming, onverlet het intellectueel eigendom. Hier ligt ook een relatie met de meldplicht op datalekken. Deze onderwerpen hebben rijksoverheidsbreed verhoogde aandacht ³⁶

B.1.9.3. Responsible disclosure

Beveiligingsonderzoek	Beveiligingsonderzoekers en goedwillende (<i>white-hat</i>) hackers kunnen een belangrijke rol vervullen in het veelal via internet zichtbaar maken van kwetsbare systemen. Momenteel bestaat er bij beveiligingsonderzoekers angst om kwetsbaarheden rechtstreeks bij een bedrijf of organisatie te melden, onder andere door de kans op strafrechtelijke vervolging. Door met hen samen te werken kan de beveiligingsgemeenschap onze ICT-veiligheid verhogen. Daarbij geven we aan hoe we met de melding van een beveiligingsonderzoeker omgaan en leggen de afspraken over deze van waarborgen voorzien handswijze vast en dragen die uit. Een belangrijk voordeel hiervan is dat we de tijd krijgen om een lek te dichten, voordat het publiek gemaakt wordt.
SOC	Het CIE/Security Operations Center bewaakt deze handswijze. Eén en ander is eveneens invulling van de nadrukkelijke wens van de Minister van VenJ ³⁷ . De <i>Leidraad om te komen tot een praktijk van responsible disclosure</i> van het NCSC is hierbij gevolgd.

B.1.10. Beleid op personele veiligheid en integriteit

B.1.10.1. Veiligheid

Fysieke veiligheid	De individuele veiligheid van onze medewerkers, bezoekers en ingehuurd personeel (de personele veiligheid) is verankerd in het voldoen aan de (arbo)wet- en regelgeving op dit gebied en heeft verwantschap met de fysieke toegangsbeveiliging uit paragraaf B.1.3.1. Een bijzonder aspect is brandveiligheid, aanvullend gericht op de bescherming van personeel, bezoekers en de omgeving van gebouwen. Hier is ook de wet- en regelgeving leidend, waaraan we dienen te voldoen.
VPT	We sluiten aan bij het programma Veilige Publieke Taak ³⁸ dat als doel heeft agressie en geweld tegen werknemers met een publieke taak te voorkomen en de daders aan te pakken.

B.1.10.2. Integriteit

Basiswaarden	De <i>Gedragscode Belastingdienst – Een integere Belastingdienst</i> ³⁹ beschrijft hoe onze basiswaarden geloofwaardigheid, verantwoordelijkheid en zorgvuldigheid in de praktijk gebracht kunnen worden ten gunste van het imago van de Belastingdienst, met als doel de bereidheid van burgers en bedrijven te
--------------	---

³⁶ Notitie Tussentijds beeld 2013 aan SG-Overleg, ADR, september 2013.

³⁷ Kamerbrief Responsible Disclosure 335692, VenJ, 28 december 2012

³⁸ Programma Veilige Publieke Taak 2011-2015, BZK en VenJ, 8 juli 2011

³⁹ De Gedragscode is te vinden op Belastingnet

vergroten om aan hun verplichtingen te voldoen. Hiermee geeft deze code invulling aan het tactisch beleid op personeelsgedrag.

Het gaat in op de basiswaarden en integriteit, onze verantwoordelijkheden naar belastingplichtigen en externen, vertrouwelijke informatie, onze verantwoordelijkheden naar de eigen organisatie en naar elkaar.

Gedragscode
Integriteit Rijk

De code past binnen de Gedragscode Integriteit Rijk⁴⁰. Het integriteitsbeleid wordt periodiek door de Kennisgroep Integriteit geactualiseerd (zie B.4.4).

B.1.10.3. Geheimhoudingsplicht

Als medewerker van de Belastingdienst kun je toegang hebben tot vertrouwelijke en persoonlijke gegevens. Dat soort informatie mag je natuurlijk nooit voor je eigen voordeel gebruiken, aan derden ter beschikking stellen of bij nevenwerkzaamheden gebruiken. Iedere ambtenaar heeft de geheimhoudingsplicht. Uitgangspunt is dat informatie voor geen ander doel mag worden gebruikt dan waarvoor de informatie is verstrekt.

Vertrouwen in overheid

Belastingplichtigen moeten erop kunnen vertrouwen dat we hun gegevens alleen gebruiken voor het werk. Ze mogen ervan uitgaan dat al hun informatie bij ons veilig is en dat we deze alleen gebruiken als dat voor het werk noodzakelijk is. Daarom tilt de Belastingdienst zwaar⁴¹ aan de geheimhoudingsplicht van zijn medewerkers. Deze plicht blijft ook gelden als je de Belastingdienst verlaat.

B.1.10.4. Beleid op clear desk en clear screen

Behalve je geheimhoudingsplicht heb je ook de verantwoordelijkheid om te voorkomen dat gegevens bij derden (collega's of buitenstaanders) terechtkomen. Daarom voert de Belastingdienst een clear-desk beleid: vertrouwelijke gegevens mogen niet onbeschermd op de werkplek achterblijven. Je hoort alle dossiers en elektronische gegevensdragers op te ruimen in afsluitbare kasten. Verder hoor je ervoor te zorgen dat niemand bij de gegevens in jouw computer kan komen. Geef je wachtwoord aan niemand, ook niet aan je naaste collega's en schakel, als je je werkplek verlaat, meteen de schermbeveiliging in (clear screen). Realiseer je, dat deze spelregels overal gelden waar je werkt zoals op kantoor, thuis, in de trein en bij de klant.

B.1.10.5. Beleid op aanvaardbaar gebruik van bedrijfsmiddelen

De Belastingdienst stelt bedrijfsmiddelen ter beschikking om je werk te kunnen doen. Er wordt van je verwacht dat je hier zorgvuldig mee omgaat.

Privégebruik

Het uitgangspunt is dat privégebruik van deze bedrijfsmiddelen beperkt is toegestaan. We realiseren ons, dat in de huidige tijd werk en privé steeds meer met elkaar vermengd worden. Desondanks is het niet de bedoeling dat je bijvoorbeeld:

- vaak of lang privégesprekken voert met de telefoon van de werkgever;
- Privé- of illegale content downloadt op gegevensdragers van de Belastingdienst;
- vaak of veel kopieert voor privégebruik;
- allerlei materiaal meeneemt voor privégebruik;

⁴⁰ Gedragscode Integriteit Rijk, BZK/DGOO, oktober 2016,

⁴¹ De Autoriteit Persoonsgegevens heeft daarnaast de bevoegdheid sancties op te leggen aan individuele werknemers bij het niet naleven van de geheimhoudingsplicht

Voorwaarden en gedragsregels	<p>- dienstauto's en andere bedrijfsmiddelen anders dan bedoeld gebruikt.</p> <p>Sluitende regels zijn niet te geven. Wanneer je bedrijfsmiddelen voor privédoeleinden wilt gebruiken, moet je je dus afvragen of je hiervoor goede redenen hebt.⁴²</p> <p>Voor ter beschikking gestelde ICT bedrijfsmiddelen met een verhoogd beveiligingsrisico hanteren we stringente (ondertekende) voorwaarden en gedragsregels. Denk hierbij aan <i>tokens</i> voor 2-factor authenticatie of door de Belastingdienst verstrekte smartphones of tablets. Overtreding van dergelijke regels kunnen worden aangemerkt als plichtsverzuim.</p>
	<p>B.1.10.6. Arbeidsvoorwaarden</p>
	<p>Voor de medewerkers geldt het Algemeen Rijksambtenarenreglement (ARAR) en de Personele Uitvoeringsbepalingen Belastingdienst (PUB), waarin onder meer de wederzijdse verantwoordelijkheden ten aanzien van beveiliging staan beschreven.</p> <p>Hieronder vallen ook de verplichting om de eed of belofte af te leggen (artikel 51 ARAR) en de geheimhoudingsplicht (artikel 1.5 PUB, artikel 125a Ambtenarenwet)⁴³, de registratie van het identiteitsbewijs en het overleggen van een Verklaring Omtrent het Gedrag (VOG).</p> <p>Voor de VOG dient de handleiding <i>Werkwijze Verklaring omtrent het Gedrag (VOG)</i>⁴⁴ te worden gebruikt.</p> <p>Voor tijdelijk (ingehuurd) personeel en stagiaires gelden aanvullende maatregelen waaronder het expliciet tekenen van een geheimhoudingsverklaring en het overleggen van een VOG.</p>
	<p>B.2. Basis beveiligingsniveau en risicoafweging</p>
Subsidiariteit	<p>Voor het merendeel van de processen en ondersteunende informatiesystemen (volgens VIR 2007) kunnen maatregelen worden getroffen volgens het basis beveiligingsniveau. Specifieke maatregelen worden getroffen op basis van een risicoafweging. Deze zijn nodig als de kenmerken van de processen en ondersteunende informatiesystemen afwijken ten opzichte van het basisniveau. Afwijkende situaties hebben betrekking op een ander dan het hier geformuleerde dreigingsprofiel, maar kunnen ook betrekking hebben op hogere beschikbaarheidseisen, voor wat betreft de Belastingdienst ongeëigend gebruik van of nieuwe technologie, gegevens met een bijzonder belang etc.</p>
Proportionaliteit	<p>Er zijn meer factoren op grond waarvan er in specifieke situaties afgeweken kan worden van de basismaatregelen: te hoge kosten, onvoldoende haalbaarheid, de mate van effectiviteit in de specifieke situatie, de ouderdom van het gebouw of van het informatiesysteem, etc. Die factoren vormen de randvoorwaarden.</p>
Stelsel van maatregelen	<p>Bij het niet-implementeren van maatregelen op het basisniveau zal eveneens een risicoafweging moeten plaatsvinden: weegt de besparing van de maatregel op tegen de kans van het optreden van de dreiging, waartegen de maatregel</p>
	<p>.....</p> <p>⁴² Regels voor het gebruik van bedrijfsmiddelen staan beschreven in Rijksportaal/Personeel/ Dienstverband/Integriteit/Gebruik van bedrijfsmiddelen/mijn organisatie</p> <p>⁴³ Nadere informatie is te vinden op het Rijksportaal/ De fiscale geheimhoudingsplicht staat beschreven in artikel 67 AWR</p> <p>⁴⁴ B/CA Unit Concerncontrol & Analyse, juni 2015 (http://intranet.belastingdienst.nl/cso/)</p>

	<p>een bijdrage levert. Hierbij speelt mee dat er meestal ook andere maatregelen zijn, die een bijdrage leveren aan het beperken van het risico.</p> <p>Bij een risicoafweging worden de bedreigingen benoemd en in kaart gebracht. Per bedreiging wordt de kans van het optreden ervan bepaald. Vervolgens wordt nagegaan wat de schade is die zou kunnen optreden als een bedreiging zich daadwerkelijk voordoet. Daarna worden analyses gemaakt van de kosten van te treffen maatregelen versus de baten van de hiermee te vermijden schaden of wordt bezien of de risico's kunnen worden vermeden, bijvoorbeeld door een andere procesimplementatie of het gebruik van beter beveiligbare ICT-middelen.</p>
Risicoafweging	
Accepteren van restrisico's	Tenslotte worden de restrisico's door het management geaccepteerd. Op basis van de onderkende risico's worden compenserende maatregelen (bovenop het basisniveau en passend in het bestaande stelsel) getroffen.
Methoden en standaarden	Voor het maken van risicoafwegingen bestaan vele methoden, standaarden en praktische uitwerkingen daarvan. Vooralsnog is er geen standaard methode ontwikkeld, die zich richt op specifieke bedreigingen bovenop de "normale" waarop het basisniveau is gebaseerd. Het beoordelen welke extra maatregelen geschikt zijn om de extra bedreigingen af te dekken is een zaak van vakkundige beoordeling en het rekening houden met de randvoorwaarden. Er is geen methode die dat kan overnemen.
Vakkundigheid	
CRSA, IRAM	Voor de verplicht gestelde risicoanalyse bij nieuwe projecten of majeure wijzigingen worden in de IV-keten methoden als Control & Risk Self Assessment (CRSA) en Information Risk Analysis Methodology (IRAM) gebruikt.
PIA	Met ingang van 1 september 2013 is het rijksbrede Toetsmodel Privacy Impact Assessment (PIA) verplicht. De Belastingdienst heeft een eigen PIA-instrument ontwikkeld dat expliciet geschikt is voor zijn uitvoeringspraktijk.
Veranderde omgeving	Maar ook voor bestaande infrastructuur, programmatuur en diensten dient te worden gekeken naar nieuwe risico's in een veranderde omgeving, zeker als deze dicht bij internet komt of mobiel is. Met name komen dan in aanmerking DWB, apps, mobiele apparatuur, netwerkverbindingen, remote of draadloos werken tot <i>Voice over IP</i> .
APK voor veilige exploitatie	Dit verstaan we onder <i>veilige exploitatie</i> , waarbij bijvoorbeeld periodiek een verplichte aanvals- en penetratietest wordt uitgevoerd, vergelijkbaar met een Algemene Periodieke Keuring.
ISMS	Het strekt tot aanbeveling om de uitkomsten van de diverse analyses te aggregeren en centraal beschikbaar te maken zodat de opgedane kennis kan worden hergebruikt en de business verantwoordelijkheid kan nemen in de risicoacceptatie.
	Daartoe kunnen hulpmiddelen zoals een Information Security Management System op basis van NEN-ISO 27001 worden ingezet.

B.3. Pas toe of leg uit

Verplichte beheersmaatregelen en te volgen implementatierichtlijnen	In hoeverre zijn beheersmaatregelen en implementatierichtlijnen verplicht? Beheersmaatregelen zijn verplicht, tenzij aangetoond kan worden dat ze niet van toepassing zijn. Implementatierichtlijnen zijn niet verplicht, maar omdat ze als <i>best practice</i> zijn vastgesteld moet bij het afwijken ervan aangetoond worden dat een andere implementatie tot het voldoen aan de beheersmaatregel leidt. Hierbij hanteren we het principe van <i>comply or explain</i> : pas toe of leg uit.
Comply or explain	

PDCA cyclus

Er dient aandacht te worden besteed aan het inpassen van de maatregelen in de PDCA cyclus⁴⁵.

Hierbij zijn de volgende kanttekeningen te maken:

- Om te voldoen aan een beheersmaatregel zal op basis van de implementatierichtlijnen in- of externe controle moeten worden uitgeoefend. Indien van de *best practice* wordt afgeweken zal eerst (bij voorkeur in een operationeel beleidsdocument) gemotiveerd moeten worden en vastgelegd hoe de beheersmaatregel anders wordt geïmplementeerd om in- of externe controle mogelijk te maken.
- Als bij de gezamenlijke evaluatie van het normenkader door allen die het moeten toepassen, blijkt dat velen tot een andere implementatie komen, zal de *best practice* moeten worden aangepast.

.....
⁴⁵ De Autoriteit Persoonsgegevens legt in de richtsnoeren meer de nadruk op de PDCA cyclus

B.4. Opbouw van de beveiligingsorganisatie

B.4.1. Sturing van beveiliging

De sturing van beveiliging benaderen we vanuit verschillende gezichtspunten.

Maatregelsturing	- Sturing op de maatregelen: deze verloopt langs de primaire verantwoordelijkheidsverdeling van de Belastingdienst. Beveiliging is een integraal onderdeel van de bedrijfsvoering en alle soorten maatregelen, die een organisatie treft om haar doelen te bereiken. Beveiliging is één van de vele aspecten waarop in samenhang moet worden gestuurd;
Aspectsturing	- Lijnsturing op het aspect: deze verloopt langs de lijn van de CFO's. Hierbij gaat het om de managementverantwoordelijkheid voor het aspect beveiliging met een accent op naleving van beveiligingskaders en samenhang van de maatregelen binnen het competentiegebied;
Functionele sturing	- Functionele sturing: deze verloopt van de strategisch beveiligingsadviseur tot de beveiligingsmedewerker en draagt bij zowel aan de lijnsturing op het aspect als de sturing op maatregelen.

B.4.2. Strategische beveiliging in het MT Belastingdienst

De invulling van strategische beveiliging staat beschreven in Deel A, paragraaf A.4.1.

B.4.3. Tactisch Beveiligingsoverleg (TBO)

Deelnemers TBO	De deelnemers zijn vertegenwoordigers van alle bedrijfsonderdelen. <ul style="list-style-type: none"> - Voorzitter: DGBel/Cluster Bedrijf; - Secretaris: DGBel/Cluster IV. <p>Inhoud overleg:</p> <ul style="list-style-type: none"> - Besluitvorming over onderhoud HBB; - Evaluatie geaggregeerde en geanonimiseerde bedrijfsonderdeelrapportages inzake beveiliging; - Evaluatie uitkomsten beveiligingsaudits; - Voorbespreking stukken voor CFO-overleg; - Evaluatie jaarlijkse risicoanalyses per bedrijfsonderdeel; - Voorstellen beveiligingsaudits.
Frequentie overleg	Het TBO komt drie keer per jaar bijeen of vaker naar aanleiding van bijvoorbeeld thema's of actuele beleidsonderwerpen.

B.4.4. Clusters en kennisgroepen

De groepen zijn:

- Cluster Business Continuity Management;
- Cluster Informatiebeveiliging;
- Cluster Fysieke Beveiliging;
- Cluster Personele Veiligheid en Integriteit;
- Kennisgroep Integriteit;
- Kennisgroep Privacy.

Deelnemers clusters	De deelnemers aan de clusters zijn vertegenwoordigers van de bedrijfsonderdelen. <p>De taken van de clusters/kennisgroepen zijn onder meer</p> <ul style="list-style-type: none"> - Uitwerken voorstellen tot onderhoud HBB;
---------------------	---

- Adviseren TBO over planning en uitvoering ICP's beveiliging;
- Adviseren over risico's;
- Adviseren bij veranderingen in de organisatie.

Kennisgroep
Integriteit

De Kennisgroep Integriteit is opgericht op grond van het besluit van het MT⁴⁶ met betrekking tot de uitkomsten van het project 'Revitalisering Integriteit'.

Integriteitsmanagement is een taak en verantwoordelijkheid van het management van de Belastingdienst op alle niveaus. De Kennisgroep treedt niet in die verantwoordelijkheid maar beoogt vanuit een concentratie van kennis en professionaliteit een waardevolle adviserende en ondersteunende bijdrage te leveren aan deze managementverantwoordelijkheid.

Het doel hierbij is om de snelheid, daadkracht en kwaliteit bij de ontwikkeling en evaluatie en bijstelling van het integriteitbeleid (en de bijbehorende regelgeving) te verhogen. Tevens is de Kennisgroep voor de bedrijfsonderdelen beschikbaar bij de uitvoering van het integriteitsbeleid. Dit alles vanuit een geïntegreerde bundeling van kennis en professionaliteit.

Deelnemers
kennisgroep

De Kennisgroep bestaat uit integriteitscoördinatoren van alle bedrijfsonderdelen, een communicatie-expert, een (arbeids)jurist, de compliance officer, de landelijk vertrouwenspersoon integriteit, een expert onderzoeker en de voorzitter.

De samenwerking tussen de beveiligingsadviseur of -medewerker en de integriteitscoördinator op elk bedrijfsonderdeel afzonderlijk is van groot belang. Vanuit de Kennisgroep worden planning en voortgang van initiatieven, activiteiten en producten binnen het TBO gemeld en zo nodig besproken. Het resultaat van het overleg binnen het TBO wordt vermeld op door te sturen documenten richting het MT.

Kennisgroep
Privacy

Als gevolg van de versterkte Europese en nationale wetgeving⁴⁷ voor gegevensbescherming en de daaraan verbonden verplichting tot *privacymangement* is de Kennisgroep Privacy ingesteld.

De Kennisgroep Privacy monitort, signaleert en adviseert met betrekking tot de (interne) naleving van wettelijke regels bij de veilige verwerking van persoonsgegevens. De Kennisgroep heeft de ambitie om het juridisch uitvoerings-, advies- en kenniscentrum te zijn voor de verwerking van (bijzondere) persoonsgegevens. De groep werkt samen langs de lijnen die er zijn op het gebied van informatiebeveiliging, in het bijzonder vanuit het oogpunt van *privacy by design* en *privacy by default*.

De Kennisgroep voorziet onder meer in:

- Advisering over implementatie en uitvoering van (nieuwe) wet- en regelgeving;
- Ontwikkeling en tot uitvoering brengen van beleid, onder andere in de vorm van kaders, normen, richtlijnen en (toetsings)producten;
- Actieve signalering ten aanzien van maatschappelijke en juridische ontwikkelingen en dilemma's in relatie tot gegevensverwerkingen;
- Juridische ondersteuning in de dagelijkse uitvoering van de gegevenspraktijk op het snijvlak van het mogen, willen en kunnen leveren van gegevensdiensten;
- Het geven van voorlichting, training en workshops ter bevordering van kennis en bewustzijn én zelfredzaamheid m.b.t. een zorgvuldige

⁴⁶ MT Belastingdienst d d 2 juli 2012. De Kennisgroep Integriteit is gestart per 1 januari 2013 op basis van het Startdocument Kennisgroep Integriteit v1 0 d d 13 november 2012

⁴⁷ Waar onder de Algemene Verordening Gegevensbescherming (AVG) en meldplicht datalekken/WBp

- gegevensverwerking door specialisten in het gegevensdomein;
- Het bevorderen van in- en externe samenwerking en relaties tussen specialisten, organisaties en bedrijfssonderdelen m.b.t. gegevensverwerking. Deelname aan in- en externe werkgroepen;

De Kennisgroep Privacy bestaat onder meer uit de Wbp-coördinatoren van de bedrijfssonderdelen, de Functionaris voor de Gegevensbescherming en experts uit het vakgebied.

B.4.5. Rollen en functies

Rol of functie

In de functies van beveiliging kan onderscheid worden gemaakt naar beveiligingsrollen en -functies. Met *beveiligingsrol* bedoelen we het uitvoeren van een deeltaak op het gebied van beveiliging, naast de primaire hoofdtaken van een functie.

Bij de *beveiligingsfuncties* gaan we alleen uit van de adviserende functies en niet op de uitvoerende beveiligingsfuncties die met een grote verscheidenheid overal in de organisatie van de Belastingdienst voorkomen. Denk hierbij aan: portiers- en bewakingsfuncties, security administrators, firewallbeheerders, IT-security ontwerpers etc.

BVA en FG

Naast de rollen en functies voor de (interne) beveiligingsorganisatie kennen we ook de departementale rollen van de Beveiligingsambtenaar (BVA, volgens VIR) en de Functionaris voor de gegevensbescherming (FG, volgens Wbp) die nauw betrokken zijn bij beveiliging in de Belastingdienst.

B.4.6. Beveiligingsrollen

In deze paragraaf staan de beelden van de beveiligingsrollen nader uitgewerkt.

B.4.6.1. Chief Security Officer (CSO)

Deze rol omvat de volgende taken:

- Opdrachtgever strategisch beveiligingsadviseurs;
- Vormt zich een visie op de betekenis van beveiliging voor de hele organisatie;
- Stelt doelen en beleid ter uitvoering vast;
- Draagt ervoor zorg dat er voldoende middelen voor uitvoering van het beleid aanwezig zijn;
- Draagt doelen en beleid uit in de hele organisatie;
- Draagt ertoe bij dat auditbevindingen en incidenten van ernstige aard worden opgelost.

B.4.6.2. Beleidsmedewerker voor een deelgebied van beveiliging

Deze rol omvat de volgende taken:

- Vormt zich een visie op de betekenis van het beleidsgebied binnen de hele organisatie;
- Draagt zorg voor het actueel houden van het tactisch beveiligingsbeleid voor het beleidsgebied;
- Bevordert dat er op strategisch niveau voldoende randvoorwaarden zijn voor het treffen van de beveiligingsmaatregelen op het beleidsgebied;
- Draagt doelen en beleid op het beleidsgebied uit in de hele organisatie;
- Draagt ertoe bij dat auditbevindingen en incidenten van ernstige aard binnen het beleidsgebied worden opgelost.

B.4.6.3. Integriteitscoördinator

Deze rol omvat de volgende taken:

- Draagt bij aan beleid, ontwikkeling en advies binnen het eigen bedrijfs onderdeel:
 - Inventariseert risico's;
 - Signaleert kansen en knelpunten;
 - Adviseert over bijstelling van beleid en/of uitvoering.
- Coördineert opleidingen, bewustwording en interventies op het gebied van integriteit binnen het eigen bedrijfs onderdeel:
 - Coördineert de integriteitsopleidingen;
 - Houdt zicht op het volgen van verplichte integriteitsopleidingen.
- Treedt op als aanspreekpunt binnen het eigen bedrijfs onderdeel en voor de Kennisgroep Integriteit:
 - Coördineert de aanpak van integriteitsincidenten binnen het eigen bedrijfs onderdeel;
 - Coördineert als Registratiepunt Integriteit de meldingen van vermoedens van misstanden en/of integriteitsschendingen binnen het eigen bedrijfs onderdeel.
- Neemt deel aan het integriteitscoördinatorenoverleg.

B.4.6.4. Wbp-coördinator/privacy officer

Deze rol omvat de volgende taken:

- Draagt bij aan alle privacygerelateerde onderwerpen:
 - Beleid binnen het eigen bedrijfs onderdeel;
 - Uitvoeringstoetsen, Privacy Impact Analyses (PIA), Compliance checks, convenanten;
 - Ontwikkeling van normen, kaders en sjablonen;
 - Inrichtingsproducten in de vorm van AO-IC en procesinrichting;
- Signaleert kansen en knelpunten, is kaderstellend en toetsend, adviseert gevraagd of ongevraagd over bijstelling van beleid en/of uitvoering.
- Coördineert workshops, trainingen en bewustwording op het gebied van gegevensbescherming binnen het eigen bedrijfs onderdeel.
- Is aanspreekpunt binnen het eigen bedrijfs onderdeel en voor de Kennisgroep Privacy en neemt deel aan het Wbp-coördinatorenoverleg.

B.4.6.5. Business Continuity Manager

De rol van Business Continuity Manager bestaat zowel op strategisch als op tactisch niveau (per bedrijfs onderdeel) en overbrugt (strategische) bedrijfsvoering en de (uitvoerende) lijn.

Deze rol omvat de volgende taken:

- Vormt zich een visie op de betekenis van het beleidsgebied BCM binnen de hele organisatie;
- Heeft kennis van de organisatorische inrichting van het BCM-proces;
- Stelt de BCM-visie en -beleid op op basis van de BCM-normatiek;
- Heeft kennis van bedreigingen- en kwetsbaarheidsanalyses;
- Heeft kennis van Business Impact Analyses (BIA);
- Stelt het calamiteitenplan op;

- Heeft kennis van bedrijfshulpverlening, crisismanagement, IT recovery, facilitair recovery, process recovery;
- Heeft kennis van het testen van calamiteitenplannen.

B.4.6.6. Crisismanager

Een crisismanager is tijdens een crisis onderdeel van een crisis-managementteam. Een crisis is een situatie waarbij de continuïteit van de bedrijfsvoering, de veiligheid van medewerkers (en bezoekers) en/of de reputatie van het bedrijf in gevaar is.

De rol van crisismanager omvat de volgende taken:

- Gemandateerd leidinggevende voor de gehele organisatie of bedrijfsonderdeel;
- Vastleggen besluiten en actiepunten (plotter);
- Verzorgen van de interne en externe communicatie (communicator);
- Actiehouder voor (deel)taken (portefeuillehouder);
- Draagt bij aan het besluitvormingsproces dat een crisis moet bezweren.

Een crisismanager wordt gekenmerkt door de volgende competenties:

- Persoonlijk gedrag: durf, initiatief, schakelvermogen, stressbestendigheid, optimisme en intrinsieke motivatie;
- Management en leidinggeven: taakgericht leiderschap, plannen & organiseren, voortgangsbewaking;
- Analyse en besluitvorming: besluitvaardigheid, probleemanalyse;
- Samenwerken en communicatie: teamwork, overzicht, overtuigingskracht.

B.4.7. Beveiligingsfuncties

Funcieweging

In deze paragraaf zijn de beelden van de beveiligingsfuncties nader uitgewerkt. Bij waardering van de beveiligingsfuncties wordt gebruik gemaakt van de vigerende methode van functiewaardering.

B.4.7.1. Strategisch beveiligingsadviseur

Doel van de functie

Het ontwikkelen van strategie en beleid gericht op beveiliging. Bevorderen en coördineren van de ontwikkeling van uitvoeringsrichtlijnen en toezien op de realisatie van het beleid.

Funciecontext

Functioneert als zelfstandig opererend intern beleidsadviseur, ressorterend onder het lid van het MT Belastingdienst dat verantwoordelijk is voor beveiliging. Geeft functioneel leiding aan beveiligingsmedewerkers in de gehele organisatie door het geven van richtlijnen en sturing op interne rapportages over de uitvoering van het beveiligingsbeleid en het naleven van uitvoeringsrichtlijnen.

Resultaatgebieden

Leidinggeven

- Geeft functioneel leiding aan beveiligingsmedewerkers in de gehele organisatie;
- Treedt op als projectleider of opdrachtgever voor organisatiebrede projecten op het gebied van beveiliging;
- Organiseert en faciliteert overleg voor sturing en coördinatie op het gebied van beveiliging.

Plan: Beveiligingseisen

- Vormt zich een visie op de betekenis van beveiliging voor de gehele organisatie door voortdurende beeldvorming over risico's en oplossingsrichtingen voor maatregelen passend bij het organisatiebeleid;
- Stelt doelen voor beveiliging voor;
- Ontwikkelt een strategie om die doelen te bereiken;
- Ontwikkelt beleid ter uitvoering van de strategie en stelt het centraal beleids- en jaarplan samen mede op basis van de deelplannen beveiliging.

Do: Treffen maatregelen

- Bevordert het ontwikkelen van uitvoeringsrichtlijnen en geeft hieraan richting;
- Initieert voorlichtings- en IB-bewustzijnsprogramma's;
- Adviseert bij en faciliteert risicoanalyses en PIA's op niveau van de hele organisatie;
- Toetst uitvoeringsrichtlijnen aan het beleid en adviseert zonodig over verbetering;
- Bereidt organisatiebrede beslissingen op het gebied van beveiliging voor;
- Adviseert de leiding van de organisatie, bedrijfsonderdelen en de IV-organisatie bij beleid(sbeslissingen) met consequenties voor beveiliging.

Check: Evaluatie en controle

- Beoordeelt rapportages van bedrijfsonderdelen over de naleving van uitvoeringsrichtlijnen;
- Beoordeelt rapportages van in- en externe auditinstanties op relevantie voor beveiliging;
- Geeft opdrachten tot het verrichten van interne onderzoeken en audits;
- Houdt een centrale registratie bij van beveiligingsincidenten en de afhandeling en evalueert de incidenten;
- Beoordeelt ontwikkelingen in de maatschappij, de overheid en het vakgebied.

Act: Aanpassen

- Stelt IB-visie, -strategie en -beleid bij en bevordert aanpassing van uitvoeringsrichtlijnen op basis van evaluaties.

Contacten

- Intern: CSO, leiding bedrijfsonderdelen, BVA van het ministerie, andere beveiligingsfunctionarissen;
- Extern: auditors, andere overheidsbeveiligingsfunctionarissen en beroepsgenoten.

Kennisgebieden

- IV en beveiliging (breed);
- Organisatie van informatievoorziening;
- Business processen (breed).

B.4.7.2. Beveiligingsadviseur

Doel van de functie

Het ontwikkelen van beleid gericht op het naleven van kaders voor beveiliging, ondersteunen van de CFO van het bedrijfsonderdeel hierbij en toezien op de realisatie van het beleid.

Resultaatgebieden

Plan: Beveiligingseisen

- Stelt jaarlijks het beveiligingsplan voor het bedrijfsonderdeel op;
- Draagt bij aan beleidsplannen voor beveiliging vanuit het perspectief van het bedrijfsonderdeel.

Do: Treffen maatregelen

- Adviseert over uitvoeringsrichtlijnen op het gebied van beveiliging, zowel centraal voor de Belastingdienst als bij het Bedrijfsonderdeel;
- vraagt uitvoeringsrichtlijnen op het gebied van beveiliging actief uit in de organisatie;
- Initieert voorlichtings- en bewustzijnsprogramma's en geeft hieraan richting;
- Voert risicoanalyses uit binnen zijn competentiegebied;
- Adviseert over het treffen van beveiligingsmaatregelen en bij besluitvorming binnen het bedrijfsonderdeel met gevolgen voor beveiliging.

Check: Evaluatie en controle

- Beoordeelt interne rapportages op beveiligingsaspecten;
- Stelt periodiek verantwoording rapportage op over beveiliging;
- Beoordeelt rapportages van in- en externe controle en auditinstanties;
- Adviseert de CFO inzake het verspreiden van interne onderzoeken en audits;
- Zorgt voor centrale melding van beveiligingsincidenten en beoordeelt afhandeling.

Act: Aanpassen

- Stelt het jaarplan beveiliging op en adviseert over uitvoeringsrichtlijnen op basis van zijn evaluatie.

Contacten

- Intern: management bedrijfsonderdeel op alle niveaus en andere beveiligingsfuncties;
 - Extern: afdelingen en beroepsfuncties.
- Resultaatbron
- Beveiliging
 - Belastingdienst processen;
 - Interne regelgeving.

Doel van de functie

B4.7.3. Beveiligingsmedewerker

Het ondersteunen en toezien op de realisatie van beleid gericht op het naleven van Belastingdienstkaders voor beveiliging en het management van het bedrijfsonderdeel hierbij ondersteunen.

Resultaatgebieden

Plan: Beveiligingsplan

- Vraagt bij aan de beleidsplannen voor beveiliging van het bedrijfsonderdeel.

Do: Treffen maatregelen

- Adviseert over uitvoeringsrichtlijnen op het gebied van beveiliging bij het bedrijfsonderdeel;
- vraagt uitvoeringsrichtlijnen op het gebied van beveiliging actief uit in de organisatie;
- Vraagt bij aan risicoanalyses binnen zijn competentiegebied;
- Adviseert over het treffen van beveiligingsmaatregelen en bij besluitvorming binnen het bedrijfsonderdeel met gevolgen voor beveiliging.

Check: Evaluatie en controle

- Beoordeelt interne rapportages op beveiligingsaspecten;
- Stelt de toedieke verantwoording rapportage op over beveiliging;
- Beoordeelt rapportages van interne controle.

Act: Aanpassen

- Stelt adviezen over uitvoeringsrichtlijnen bij op basis van zijn evaluatie.

Contacten

- Intern: management bedrijfsdeeldeel op alle niveaus en andere beveiligingsfuncties;
 - Extern: auditors en toezegagenota.
- Kenningsbladen**
- Beveiliging;
 - Belastingdienst processen;
 - Bescherming persoonsgegevens;
 - Interne regeling.

B.4.7.4. Procesarchitect Informatiebeveiliging

Doel van de functie	Hier artikelen en en actueel houden van een visie op de deelarchitectuur voor het aspect informatiebeveiliging in de bedrijfs- of procesarchitectuur als concretisering van een deel van het strategisch beveiligingsbeleid en de positionering van generieke beveiligingsfunctionaliteiten daartinnen.
Functiecontext	Procesarchitect met als specialisatie beveiliging. Vertaalt beleidskaders voor beveiliging naar bedrijfs- of procesarchitectuur en vult daarbij zowel een architecten- als adviseursrol. Treedt met name op als procesarchitect voor generieke beveiligingsfunctionaliteiten, bijvoorbeeld op het gebied van logische toegangsbeveiliging, encryptie, keyring en auditing. Ziet toe op naleving van architectuurprincipes voor beveiliging. Houdt voortdurend zicht op marktonwikkelingen op het gebied van beveiligingsproducten.
Resultaatgebieden	<p>Plan: Beveiligingsplan</p> <ul style="list-style-type: none"> - Vormt zich een visie op de betekenis van beveiliging in het kader van de bedrijfs- of procesarchitectuur en houdt daarbij rekening met de organisatiestrategie voor beveiliging; - Draagt bij aan de strategie van de organisatie voor beveiliging vanuit het perspectief van procesontwikkeling; - Draagt bij aan de beleidsvorming en jaarplannen ter uitvoering van deze strategie binnen zijn competentiegebied. <p>Do: Treffer maatregelen</p> <ul style="list-style-type: none"> - Ontwerpt zelfstandig de architectuur van de bedrijfs- of procesarchitectuur voor het domein van beveiliging of draagt bij aan het expliciet maken van het aspect beveiliging als integraal onderdeel van deze architectuur; - Voert risicoanalyse en PIR's uit binnen zijn competentiegebied; - Toont procesontwerpen aan architectuuruitgangspunten voor beveiliging en adviseert zonnodig over verbetering van die ontwerpen; - Toont ontwerpen voor generieke beveiligingsfunctionaliteiten aan architectuuruitgangspunten voor beveiliging en adviseert zonnodig over verbetering van die ontwerpen. <p>Check: Evaluatie en controle</p> <ul style="list-style-type: none"> - Bepoortst procesmatige ontwikkelingen in de bedrijfsvoering met mogelijke gevolgen voor de beveiliging; - Beoordeelt IT-audit rapportages, rapportages over beveiligingsincidenten en gebruikersevaluaties van generieke beveiligingsfunctionaliteiten. <p>Act: Aanpassen</p> <ul style="list-style-type: none"> - Drukt zorg voor het bijstellen van het aspect beveiliging in de bedrijfs- of procesarchitectuur of implementaties daarvan op basis van zijn evaluaties.

Contacten

- Intern: bedrijfsprocesarchitecten, procesontwepers, informatiemangers, projectleiders voor procesmatige vernieuwing, andere beveiligingsfuncties;
- Extern: IT-auditors en beroepsveren.

Kennisgebied

- IV en beveiliging;
- Organisatie van informatievoorziening;
- Bescherming persoonsgegevens;
- Architectuurprincipes;
- Felastingen streefwaarden (haal en draag)

Doel van de functie**B.4.7.5. Beveiligingsmanager ICT**

Het ontwikkelen van beleid gericht op informatiebeveiliging binnen de ICT-aanbiederorganisatie, anderszins van het management; zorgdragen voor de ontwikkeling van uitvoeringsrichtlijnen en toezien op de realisatie van het beleid.

Functiecontext

Functioneert namens het management van ICT-aanbieder als zelfstandig en breed opererend adviseur en toezichhouder op het gebied van beveiliging. Geeft functioneel leiding aan beveiligingsfuncties binnen de ICT-organisatie door het geven van richtlijnen en sturing op interne rapportages over de uitvoering van het beveiligingsbeleid en het naleven van uitvoeringsrichtlijnen. Overwint weerstand om het beleid en richtlijnen te laten naleven, die vaak als belemmerend worden ervaren in de uitvoering van het werk.

Resultaatgebieden**Wat: Beveiligingsseisen**

- Stelt jaarlijks het informatiebeveiligingsplan voor de ICT-aanbiederorganisatie op;
- Draagt bij aan de centrale strategie en beleidsplannen voor beveiliging vanuit het perspectief van de ICT-aanbiederorganisatie

Leidingsgeven

- Geeft eventueel functioneel of direct leiding aan andere beveiligingsfuncties binnen de ICT-aanbiederorganisatie;
- Organiseert en faciliteert overleg om maatregelen en evaluaties binnen de ICT-aanbiederorganisatie op het gebied van beveiliging op elkaar af te stemmen.

Do: Treffen maatregelen

- Adviseert over uitvoeringsrichtlijnen op het gebied van beveiliging, zowel centraal voor de aanbieder als bij de ICT-aanbiederorganisatie;
- Faciliteert voorlichtings- en bewustzijnsprogramma's en geeft hieraan richting;
- Voert initiatieven uit om binnen zijn competentiegebied en op centraal niveau als verlegeneroepder van de ICT-aanbiederorganisatie;
- Adviseert over het treffen van beveiligingsmaatregelen en bij besluitvorming binnen de ICT-aanbiederorganisatie met gevolgen voor beveiliging;
- Ziet toe op naleving adviseercontrolebevindingen bij certificeringsprocessen.

Check: Evaluatie en controle

- Beoordeelt afdelings- en procesrapportages binnen de ICT-aanbiederorganisatie;
- Beoordeelt rapportages van in- en externe controle en auditinstanties;

- Geeft opdrachten tot het verrichten van interne onderzoeken en audits;
- Beoordeelt of partijpoort in de afhandeling van beveiligingsincidenten;

Act: Aanpassen

- Stelt het beveiligingsjaarplan en adviezen over beveiligingsuitvoeringsrichtlijnen bij op basis van zijn evaluaties.

Contacten

- Intern: management bedrijfsinterne op alle niveaus en andere beveiligingsfuncties
 - Extern: auditors, branche- en beroepsverenigingen
- Kenmerken:
- ICT en informatiebeveiliging;
 - Organisatie van informatievoorziening
 - Bescherming persoonsgegevens;
 - ITIL.

B.4.7.6 Informatiebeveiligingsarchitect

Doel van de functie	Het ontwikkelen en actueel houden van het aspect beveiliging binnen de IV-architectuur dat zowel gericht is op het voldoen aan het beveiligingsbeleid en -voorschriften als op de generieke beveiligingsfunctionaliteiten binnen de technische infrastructuur. Daarbij wordt het toepasbaar maken van deze architectuur en handlijken (systemen) van het ontwerp en het onderhoud van de generieke beveiligingsfunctionaliteiten.
Functiegebied	IV-architect met als specialisatie beveiliging in relatie tot IV. Vertaalt beleidskaders voor beveiliging naar IV-architecturen en vervult daarbij zowel een architect- als adviseursrol. Treedt met name op als IV-architect voor generieke beveiligingsfunctionaliteiten, bijvoorbeeld op het gebied van logische toegangsbeveiliging, encryptie, logging- en auditing.
Resultaatgebieden	Ziet toe op de eaving van architectuurprincipes voor beveiliging. Houdt zich op marktontwikkelingen en op het gebied van beveiligingsproducten.
	<p>Plan: Beveiligingsplan</p> <ul style="list-style-type: none"> - Vormt zich een visie op de betekenis van beveiliging voor IV vanuit de centrale strategie door voortdurende helderving over risico's en oplossingsrichtingen voor maatregelen passend bij het centrale beleid; - Draagt bij aan de centrale strategie voor IV in relatie tot beveiliging; - Draagt bij aan de beleidsvorming en jaarplannen ter uitvoering van deze strategie binnen zijn competentiegebied. <p>Do: Interne maatregelen</p> <ul style="list-style-type: none"> - Ontwerpt zelfstandig de architectuur van het IV-complex voor het centrale beveiliging of draagt bij aan het ontwikkelen van het aspect beveiliging als integraal onderdeel van de IV-architecturen; - Treedt op als IV-architect voor generieke beveiligingsfunctionaliteiten; - Testt IV-ontwerpen aan architectuuruitgangspunten voor beveiliging volgens de Policy by Design en adviseert zonnig over verbetering van die ontwerpen. <p>Check: Evaluatie en controle</p> <ul style="list-style-type: none"> - Beoordeelt ontwikkelingen in de markt t.o.v. nieuwe informatiebeveiligingsrisico's en geeft die oplossingen van leveranciers; - Beoordeelt interne ontwikkelingen binnen de IV met mogelijke gevolgen voor IE-aspecten in de IV.

- Beoordeelt IT-audit rapportages, rapportages over beveiligingsincidenten en gebruiksevaluaties van gevoelige beveiligingsfuncties/activiteiten.

Act: Aanpassen

- Draagt zorg voor het bijstellen van het aspect beveiliging in IV-architecturen op basis van zijn evaluaties.

Contacten

- Intern: IV-architecten, IV-onderzoekers, projectleiders IV, andere beveiligingsfuncties;
- Extern: IT-auditors, IV-leveranciers en beroepsinstellingen
- IV en beveiliging;
- Architectuurprincipes;
- Bescherming persoonsgegevens;
- Standaards inzake beveiliging.

Kennisgebieden

B.5. Structuur van de implementatierichtlijnen

Voor het samenstellen en ordenen van de implementatierichtlijnen zijn een aantal uitgangspunten gekozen. Ze kunnen worden gebruikt als toetsinkader voor acceptatie van wijzigingen.

Deel C is gebaseerd op de NEN-ISO 27002:2013 die de invalshoek kent vanuit de informatietechnologie.

Deel D vindt zijn oorsprong in de NEN ISO 22313:2012 die een invalshoek heeft vanuit de bedrijfsprocessen, waarbij informatiebeveiliging een geïntegreerd onderdeel van BCM is.

B.5.1. Eigen implementatierichtlijnen

De richtlijnen en beheersmaatregelen zijn gebaseerd op de NFN-ISC 27000. Niet alle beheersmaatregelen en richtlijnen kunnen van toepassing te zijn en mogelijk zijn aanvullende beheersmaatregelen en richtlijnen, vermits die niet in deze norm zijn opgenomen. De richtlijnen kunnen daarom worden beschouwd als uitgangspunt voor het ontwikkelen van organisatie specifieke richtlijnen.

B.5.2. Ouderprestatie

Eén kader voor de hele Defensieinst

Doet als beveiligingsnormen in één handboek op te nemen is de onderlinge consistentie en volledigheid beter te borgen en het pas toe of af uit beginsel van de aan de overheid opgelegde standaarden beter te handhaven.

Conformiteitsnormen

Indien beveiligingsnormen te zeer op de organisatie van de Defensieinst en te zeer implementatieafhankelijk worden geformuleerd is niet meer duidelijk wat de oorspronkelijke uitgangspunten van de norm zijn. Er zal dan vaker onderhoud moeten worden gepleegd omdat organisaties steeds dynamischer worden. Bovendien kunnen de normen dan niet goed meer met derden worden afgestemd en kunnen ze niet meer dienen als eisen die aan jobbedings- of contractpartijen zijn te stellen.

Onderscheid tussen proces en product

Het maken van onderscheid naar normen voor processen en normen voor de uitvoeren van processen - dat zijn producten - dient steeds te worden.

Het onderscheid is van belang bij het stellen van eisen aan projecten en derden, omdat het daarbij vaak alleen maar gaat om het opleveren van een product, bijvoorbeeld een T-component of alleen het ontwerp ervan. Het zal niet altijd bij fysieke objecten, zoals een gebouw of computersysteem.

De kennis die nodig is om proces- of productnormen toe te passen bij advisering en controle is verschillend.

De processen zijn vaak dezelfde onderliggende principes van toepassing. De volgorde van gebeurtenissen of de PDCA-cyclus. Bij de aantelbaarheid van processen kan altijd dezelfde formele benadering worden gevolgd. Kennis omtrent de inhoud van de processen is niet primair vereist.

Bij producten is dit anders. Dat vraagt bijna altijd specialismatische kennis en een specifieke benadering bij het kiezen, aanpakken van de kwaliteit.

Dit onderscheid spreekt met het onderscheid tussen de procesgerichte en een algemeen algemene aanpak.

Samenhang

Afwijkend en
vrijsoortbaar

Processen

Producten

Verantwoordelijkheid, wederzijds	<p><i>Onderscheid tussen klant en leverancier (kwaliteitsrelatie)</i></p> <p>Organisaties (en zeker overheidsorganisaties) opereren steeds meer in kaders waarbij ze sterk van elkaar afhankelijk zijn. Uitbesteding van faciliteiten diensten, zoals IT, maar bijvoorbeeld ook huisvesting, is daarvan een prominent voorbeeld. Omdat verantwoordelijken niet kunnen worden uitbested, is het van belang zekerheid te krijgen over de juiste uitvoering van de uitbestede activiteiten. Hiervoor is het noodzakelijk de juiste mensen en namen aan de ander te kunnen toekennen en hiërarchische controle te kunnen laten uitoefenen. De huidige bevestigingsstandaarden zijn hierin niet ingedeeld.</p>
Duidelijk belegde verantwoordelijkheid	<p><i>Zo klein mogelijk voorafvoorspelbaarheid</i></p> <p>De indeling van de normen moet zorgen zijn dat naleving onderhandelbaar is toe te wijzen binnen een organisatie. Het moet niet de expertise van de controleur zijn die uiteindelijk bepaakt bij welke afdeling of als welk onderdeel van een proces normen op naleving moeten worden geroepen. Het onderscheid tussen beleid en uitvoering bijvoorbeeld is in grote organisaties vaak gecombineerd en dat betekent dat een dergelijk onderscheid ook moet doorwerken in de formulering van normen.</p>
Onderbouwde normen	<p><i>Controleerbaar met deugstukken</i></p> <p>Indien naleving van een norm niet rechtstreeks kan worden aangeleerd met bewijsstukken is de formulering van de norm niet concreet genoeg. Vaak leidt de omschrijving meer naar een doelstelling dan een norm. Een norm moet zo min mogelijk interpretatievrije schillen toelaten.</p>
Beheersmaatregelen en implementatie eisen	<p>Om die reden worden de normen ingedeeld naar beheersmaatregelen op een hoog abstractieniveau en verder ingevuld met zo concreet mogelijke implementatieeisen. Het is echter van belang dat de implementatieafhankelijkheid niet zijdt mogelijk interpretatievrije schillen geheel te voorkomen. In het HBB voorkomt de vage formulering.</p> <p>B.5.3. Beheers- en opbouw normen</p> <p>De normen zijn onderverdeeld in twee hiërarchische niveaus, de beheersmaatregelen met daaronder de implementatieeisen. De beheersmaatregelen dienen voor correctievorming in rapportage, de implementatieeisen zijn best practices, die aan de maatregelen invulling geven.</p> <p>De interne validatieprocedures zijn op deze implementatieeisen gericht om vervolgens per beheersmaatregel tot een oordeel te kunnen komen volgens het pas toe of stop uit principe.</p>

B.6. Verklaring van toepasselijkheid

B.6.1. Internationale normen

NEN-ISO

Volgens de NEN-ISO 27001:2013 dient een verklaring van toepasselijkheid (definitief of applicability) te worden opgesteld. Hierin staat beschreven welke beheersmaatregelen van toepassing zijn, hoe die zich verhouden tot de beheersmaatregelen uit NEN-ISO 27002:2013 en welke maatregelen om welke redenen zijn uitgesloten.

De Belastingdienst volgt de NEN-ISO 27002:2013 in zijn geheel, met waar van toepassing aanvullende maatregelen die specifiek voor de eigen organisatie gelden.

B.6.2. Nationale normen

NORA

De Nederlandse Overheid Referentie Architectuur Katern Beveiliging is als vastgestelde norm voor de Nederlandse overheid van toepassing voor de Belastingdienst. Dit katern van de NORA is online te raadplegen¹⁶.

RIK

De Rijksoverheid Informatiebeveiliging Rijkdienst – Technisch Normenkader (EIR-TKN) wordt overgenomen, inclusie¹⁷ de specifiek voor de Rijksoverheid geldende normen en de operationele handhaving.

¹⁶ <http://www.noronline.nl/wiki/Beveiliging>

Gebruikte afkortingen

ADR	Auditdienst Rijk
AVD	Algemene Inlichtingen- en Veiligheidsdienst (BZK)
ARAR	Algemeen Rijksarchiveringsreglement
BCM	Business continuity management, bedrijfscontinuïteitbeheer
DCMO	Business continuity management system
BHV	Bereijdschapverlening
BIA	Business Impact Analyse
BIH	Business Impact Informatiebeveiliging Rijksdienst
DVA	Deelvigingsambtenaar
RYOD	Rijng voor mijn device
BZK	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
CFD	Centrum voor Financiële Dienstverlening
CHJ	Chief Human Officer
CHRO	Chief Human Resource Officer
CIE	Centrum voor Infrastructuur en Exploitatie
CIO	Chief Information Officer
COPE	Company owned, personally enabled
CPB	Centraal Planbureau
CSO	Chief Security Officer
CYOD	Choose Your Own Device
DGBB	Directoriaal-generaal Beveiligingsdienst
DRZ	Domein Register Zaken
FG	Functieomschrijving van de Gegevensbescherming
FIOD	Fiscale Inlichtingen- en Opsporingsdienst
HBB	Harboerke beveiliging bevestiging dienst
IB	informatie beveiliging
IBR	Integraal Beveiligingsbeleid Rijksverheid
ICT	informatie- en communicatietechnologie
ICP	intern controleprogramma
IT	informatietechnologie
IV	informatievoorziening
MT	Managementplan
MvF	Ministerie van Financiën
NCSC	Nationaal Cyber Security Centrum
NORA	Nederlandse Overheid Reference Architecture
PDCA	Plan - do - check - act
PIA	Privacy Impact Assessment
PUB	Personale Uitbreidingbepalingen Balaastingdienst
SUC	Security Operations Center
TDO	Tactisch Beveiligingsoverleg
VenI	Ministerie van Veiligheid en Justitie
VIR	Voluetschrift Informatiebeveiliging Rijksdienst
VRBI	VIR - Bijzondere Informatie
VUG	Verdraging Overeen het Gedrag

bylage 32

1100034

00012



Ministerie van Financiën

Handboek Beveiliging Belastingdienst

2017

Deel C
Implementatierichtlijnen

1100034

00012

Inhoudsopgave	
Boekdels	6
Toelichting op Deel C	6
C.1 Strategisch beveiligingsbeleid en -organisaie	7
C.1.1 Strategisch beveiligingsbeleid	7
C.1.2 Beoordeling van het informatiebeveiligingsbeleid	8
C.1.3 Organisatie van beveiliging	8
C.2 Tactisch beveiligingsbeleid	11
C.2.1 Afreiking van wettelijke en contractuele eisen	11
C.2.2 Schieding van taken	12
C.2.3 Verkeersfuncties	13
C.2.4 Toegangsbeveiliging	13
C.2.5 Informatieuitwisseling en -transport	18
C.2.6 Mobile apparatuur	22
C.2.7 Toestellen en multimedial	24
C.2.8 Gebruik van cryptografische beheersmaatregelen	25
C.2.9 "Clear desk" en "clear screen"	27
C.2.10 "Stalen" van e-mailadressen	28
C.2.11 Geheimhouding	28
C.2.12 Bedrijfscontinuïteit	29
C.3 Tactisch beveiligingsbeheer	32
C.3.1 Kwiteit beveiligingsfunctiemensen	32
C.3.2 Stellen kader	33
C.3.3 Onderhouden beveiligingskaders	33
C.3.4 Advies en beveiliging	33
C.3.5 Evalueren beveiliging	34
C.3.6 Informatiebeveiligingsbeoordelingen	34
C.4 Personeel veiligheid	37
C.4.1 Voorafgaand aan het dienstverband	37
C.4.2 Tijdens het dienstverband	38
C.4.3 Beëindiging en wijziging van dienstverband	40
C.4.4 Kritische en risicovolle functies	40
C.5 Fysieke beveiliging en beveiliging van de omgeving	42
C.5.1 Beveiligde gebouwen	42
C.5.2 Apparatuur	44
C.6 Beheer van bedrijfsmiddelen	45
C.6.1 Inventariseren van bedrijfsmiddelen	49

C.5.2.	Eigendom van bedrijfsmiddelen	49
C.5.3.	Zaakbaar gebruik van bedrijfsmiddelen	49
C.5.4.	Tenuegeven van bedrijfsmiddelen	50
C.7.	Leveranciersrelaties	51
C.7.1.	Informatieveiligheid in leveranciersrelaties	51
C.7.2.	Eeher van dienstverlening van leveranciers	53
C.8.	Beveiliging bedrijfsvoering	56
C.8.1.	Eedehoeveelheidsprocedures en verantwoordelijkheden	56
C.8.2.	Eedehoeveelheidsprocedures	56
C.8.3.	Waken van back-ups	59
C.8.4.	Verlegging en migratie	60
C.8.5.	Eedehoeveelheidsprocedures van operationele software	62
C.8.6.	Eeher van technische fitbaarheid	63
C.8.7.	Eeher van netwerkbeveiliging	64
C.8.8.	Toegang tot netwerken en netwerkdiensten	66
C.8.9.	Toegangbeveiliging van systemen en toepassingen	66
C.9.	Beheer van informatieveiligheidsincidenten	70
C.9.1.	Eeher van informatieveiligheidsincidenten en -verbetereingen	70
C.10.	Informatiebeheer	74
C.10.1.	Staten kwadeveelheid van informatie	74
C.10.2.	Kwaliteitsbeheer	75
C.10.3.	Fase documenten ontwerp en invoering IT	75
C.11.	Algemeen beheer van handmatige processen	78
C.11.1.	Proceswandering	78
C.11.2.	Aanzetten operationele IT	79
C.11.3.	Vanmaken gegevens op basis van vragenlijsten	79
C.11.4.	Rapporteren over het proces	80
C.11.6.	Eedehoeveelheidsprocedures van het proces	80
C.12.	Ontwerpen van applicaties en informatiesystemen	81
C.12.1.	Eedehoeveelheidsprocedures voor informatiesystemen	81
C.12.2.	Eedehoeveelheidsprocedures in ontwikkelings- en ondersteunende processen	83
C.12.3.	Testgegevens	88
C.13.	Digitaal IT-voorzieningen	80
C.13.1.	Afleiding	89
C.13.2.	Consultatievoorzieningen	90
C.13.3.	Geprogrammeerde controles	92
C.13.4.	Zonering IT	100
C.13.5.	Activiteit	103

C.13.6. Onwettigbaarheidsberishtuizening	105
C.13.7. Identificatie, Authentificatie en Autorisatie	106
C.13.8. Vastleggen van oecurrisen	112
C.13.9. Controle, alarmering en rapportering	115
C.13.10. Systeemintegriteit	116

Bookdata

Titel Handboek Beroepsreg Belastingdienst 2017

Deel C : implementatierichtlijnen

Versie December 2016

Auteur Tactisch Bevoegdheidsverlof

Versie	Opmerkingen / revisies
Mei 2011	Eerste jaargang HBB Deel C
December 2012	Tweede jaargang HBB Deel C
December 2013	Derde jaargang HBB Deel C
December 2014	Vierde jaargang HBB Deel C
Februari 2016	Vijfde jaargang HBB Deel C
December 2016	Zesde jaargang HBB Deel C = Bookdata, 61st

Toelichting op Deel C

1. Beheersmaatregelen zijn verplicht, tenzij aangegeven kan worden dat ze niet van toepassing zijn. Implementatierichtlijnen zijn niet verplicht, maar omdat ze als best practice zijn vastgesteld moet bij het afwijken ervan aangegeven worden dat een andere implementatie tot het vo doen van de beheersmaatregel leidt. (9-BB 9.3.2.)
2. De normen zijn onderverdeeld in hiërarchische niveaus, de doelstellingen, de beheersmaatregelen en daaronder de implementatie-richtlijnen. De beheersmaatregelen dienen voor controleverifying en rapportage, de implementatie-richtlijnen zijn best practices die aan de maatregelen invulling geven.
3. De verwijzingen naar de NEN-ISO 27002:2013 staan opgenomen in de vorm [ISO...] en dienen ter referentie. Ze zijn niet bedoeld als nadere invulling van de richtlijn.

C.1. Strategisch beveiligingsbeleid en -organisatie

Doelstelling

Het verschaffen van directieaanduiding van en -aanpak voor informatiebeveiliging in overeenstemming met bedrijfsdoelen en relevante wet- en regelgeving. (ISO 5.1)

Het strategisch beveiligingsbeleid en -organisatie geeft voor de gehele organisatie richting aan het treffen van maatregelen voor beveiliging overeenkomstig de bedrijfsmatige eisen en van toepassing zijnde standaarden, wetten en voorschriften en het handhaven daarvan.

Toelichting

Het beveiligingsbeleid kan worden onderscheiden in een strategisch deel en beleidsdoelstellingen die te zien zijn als een nadere uitwerking van het strategisch beleidsdocument op het tactische niveau. Het strategisch deel is bedoeld voor managers en algemene voorlichtingsdoelinden en daarbij staat leesbaarheid en begrijpelijkheid voorop. Het tactisch deel is meer bedoeld voor specialisten, die verantwoordelijk zijn voor de inrichting van organisatie, processen en middelen.

Metvoering

Gezien de complexiteit van beveiliging als integraal aspect van de bedrijfsvoering is het van belang om op globaal niveau voor samenhang te zorgen en richting te geven aan het treffen van beveiligingsmaatregelen in de gehele organisatie. Daarvoor zijn eisen van omvang van over de verschillende verantwoordelijkheden heen op hoofdlijnen het strategisch beleid vertaald te werken, kan een organisatie sturing geven aan de invulling/implementatie van de normen.

C.1.1. Strategisch beveiligingsbeleid

Behoevenmaatregel

Ten behoeve van informatiebeveiliging behoeft een reeks beleidsregels te worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen. (ISO 5.1.1)

Toelichting

Organisaties behoeven op het hoogste niveau een 'informatiebeveiligingsbeleid' te definiëren dat is goedgekeurd door de directie en dat de aanpak van de organisatie beschrijft om haar doelstellingen inzake informatiebeveiliging te bereiken.

Het beleidsdocument voor beveiliging geeft de betrokkenheid van het hoogste management weer omtrent de benoeming van de organisatie ten aanzien van het beheer van beveiliging.

Implementatierichtlijn

Beleidsregels inzake informatiebeveiliging behoren eisen te behandelen die voortkomen uit:

- a) bedrijfsstrategie;
- b) wet- en regelgeving en contracten;
- c) huidige en verwachte bedreigingen inzake informatiebeveiliging.

Het informatiebeveiligingsbeleid behoort uitwerkingen te bevatten betreffende:

- a) de definitie van doelstellingen en principes van informatiebeveiliging om richting te geven aan alle activiteiten die verband houden met informatiebeveiliging;
 - b) toekenning van algemeen en specifieke verantwoordelijkheden voor informatiebeveiliging aan een gedefinieerde rolrol;
 - c) processen voor het behandelen van afwijkingen en uitwerkingen.
- Op een lager niveau behoort het informatiebeveiligingsbeleid te worden ondersteund door onderwerp-specifieke beleidsregels die de implementatie van beheersmaatregelen inzake informatiebeveiliging verplicht stellen en die specifiek gestructureerd zijn om de behoeften van bepaalde doelgroepen binnen een organisatie aan de orde te stellen of om bepaalde onderwerpen te behandelen.

Deze beleidsregels behoren te worden gecommuniceerd aan medewerkers en relevante externe partijen in een vorm die relevant, toegankelijk en begrijpelijk is voor de beoogde lezer, bijv. in de context van een bewustzijns-, opleidings- of trainingsprogramma voor informatiebeveiliging' (zie ISO 7.2.2).

C.1.2. Beoordeling van het informatiebeveiligingsbeleid

Beleidsmaatregel

Het beleid voor informatiebeveiliging behoort met geplande tussenpozen en als zich significante veranderingen voordoen, te worden beoordeeld om te waarborgen dat het voortdurend passend, adequaat en effectief is. (ISO 5.1.2)

Implementatie-richtlijn

Het toewijzen van de verantwoordelijkheden die bij informatiebeveiliging horen, behoort te worden gedaan in overeenstemming met de beleidsregels voor informatiebeveiliging (zie ISO 5.1.1). Verantwoordelijkheden voor het beschermen van individuele bedrijfsmiddelen en voor het uitvoeren van specifieke informatiebeveiligingsprocessen behoren te worden gedefinieerd. Verantwoordelijkheden behoren te worden gedefinieerd voor activiteiten met betrekking tot risicobeheer van informatiebeveiliging en in het bijzonder voor het accepteren van de overblijvende risico's. Deze verantwoordelijkheden behoren waar nodig te worden aangevuld met meer gedetailleerde richtlijnen voor specifieke locaties en informatieverwerkende faciliteiten. Lokale verantwoordelijkheden voor het beschermen van bedrijfsmiddelen en voor het uitvoeren van specifieke beveiligingsprocessen behoren te worden gedefinieerd.

Personen aan wie verantwoordelijkheden inzake informatiebeveiliging zijn toegekend mogen beveiligingstaken aan anderen delegeren. Niettemin blijven zij verantwoordelijk er behoren zij veel te stellen dat de afgelege taken correct zijn verricht.

Vermeldt behoort te worden welke personen voor welke gebieden verantwoordelijk zijn. Het volgende behoort in het bijzonder te gebeuren:

- de bedrijfsmiddelen en informatiebeveiligingsprocessen behoren te worden geïdentificeerd en gedefinieerd;
- de entiteit die verantwoordelijk is voor elk bedrijfsmiddel of informatiebeveiligingsproces behoort te worden bepaald en de details van deze verantwoordelijkheid behoren te worden gedocumenteerd (zie ISO 6.1.2);
- autorisatieniveaus behoren te worden gedefinieerd en gedocumenteerd;
- om in staat te zijn om de verantwoordelijkheden in het informatiebeveiligingsgebied te vervullen behoren de benoemde personen van het desbetreffende gebied kennis te hebben en bevoegd te zijn de mogelijkheden te worden geboden om de overdrachten bij te houden;
- coördinatie en overzicht van informatiebeveiligingsaspecten van leverancierrelaties behoren te worden geïdentificeerd en gedocumenteerd.

C.1.3. Organisatie van beveiliging

Doelstelling: Een beheerkader vaststellen om de implementatie en uitvoering van de informatiebeveiliging binnen de organisatie te faciliteren van te behuizen. (ISO 6.1)

C.1.3.1 Rollen en verantwoordelijkheden bij informatiebeveiliging

Beleidsmaatregel

Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen. (ISO 6.1.1)

Implementatie-richtlijn

Het toewijzen van de verantwoordelijkheden die bij informatiebeveiliging horen behoort te worden gedaan in overeenstemming met de beleidsregels voor informatiebeveiliging (zie ISO 5.1.1). Verantwoordelijkheden voor het beschermen van individuele bedrijfsmiddelen en voor het uitvoeren van specifieke informatiebeveiligingsprocessen behoren te worden geïdentificeerd.

Verantwoordelijkheden behoren te worden gedefinieerd voor activiteiten met betrekking tot de coördinatie van informatiebeveiliging en in het bijzonder voor het accepteren van de overblijvende risico's. Deze verantwoordelijkheden behoren waar nodig te worden aangewezen met meer gedetailleerde richtlijnen voor specifieke locaties en informatieverwerkende faciliteiten. Lokale verantwoordelijkheden voor het beschermen van bedrijfsmiddelen en voor het uitvoeren van specifieke beveiligingsprocessen behoren te worden gedefinieerd.

Persoon en wie verantwoordelijkheden inzake informatiebeveiliging zijn toegelaten mogen bevoegingen aan anderen delegeren. Niettemin blijven zij verantwoordelijk en behoren zij vast te stellen dat gedelegeerde taken correct zijn verricht.

Vastgelegd behoort te worden welke personen voor welke gebieden verantwoordelijk zijn. Het volgende behoort in het bijzonder te gebeuren:

- de bedrijfsmiddelen en informatiebeveiligingsprocessen behoren te worden geïdentificeerd en gedefinieerd;
 - de entiteit die verantwoordelijk is voor elk bedrijfsafdeling of informatiebeveiligingsproces behoort te worden bepaald en de details van deze verantwoordelijkheid behoren te worden gedocumenteerd (zie ISO 8.1.2);
 - autorisatievervals behoren te worden gedefinieerd en gedocumenteerd;
 - om te staan te zijn om de verantwoordelijkheden in het informatiebeveiligingsgebied te vervullen behoren de benoemde personen op het desbetreffende gebied zo ver mogelijk te zijn en behoort hun de nodige vaardigheden te worden geboden om de ontwikkelingen te behouden.
- a) de entiteit en de details van informatiebeveiligingsprocessen van leveringsorganisaties behoren te worden geïdentificeerd en gedocumenteerd.

C.1.2.2 Contact met overheidsinstellingen

Beheersmaatregel

Er behoren passende contacten met relevante overheidsinstellingen te worden onderhouden. (ISO 8.1.3)

Implementatierichtlijn

Organisaties behoren procedures te hebben die aangeven wanneer en door wie contact behoort te worden opgenomen met overheidsinstellingen (lijst, profiel, regulisatorische organismen, leiders (insuliniers) en hoe geïdentificeerde informatiebeveiligingsincidenten tijdig behoren te worden gerapporteerd (bijvoorbeeld het verspreiden bestaat dat mogelijk wetgeving is overtreft).

C.1.2.3 Contact met speciale belangengroepen

Beheersmaatregel

Er behoren passende contacten met speciale belangengroepen of andere gespecialiseerde beveiligingsorganisaties en professionele organisaties te worden onderhouden. (ISO 8.1.4)

Implementatierichtlijn

Lidmaatschap van speciale belangengroepen of fora behoort te worden overwogen als middel om:

- kennis te verbeteren over 'best practices' en op de hoogte te blijven van relevante beveiligingsinformatie;
- er voor te zorgen dat de kennis van informatiebeveiliging actueel en volledig is;
- vroegtijdige waarschuwingen te ontvangen inzake alerts, adviezen en patches die verband houden met beveiliging en kwetsbaarheden;
- toegang te krijgen tot gespecialiseerd advies over informatiebeveiliging;
- informatie over nieuwe technologieën, producten, bedrijven of kwetsbaarheden te delen om uit te wisselen;
- geschikte contactpunten te verkrijgen als er informatiebeveiligingsincidenten zijn. (ISO 16)

C.1.3.4 Informatiebeveiliging in projectbeheer

Beheersmaatregel

Informatiebeveiliging behoort aan de orde te komen in projectbeheer, ongeacht het soort project. (ISO 6.1.5)

Implementatierichtlijn

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

- a) informatiebeveiligingsdoelstellingen worden opgenomen in projectdoelstellingen;
- b) een risicobeoordeling van informatiebeveiliging in een vroeg stadium van het project wordt uitgevoerd om de nodige beheersmaatregelen te identificeren;
- c) informatiebeveiliging deel uitmaakt van alle fasen van de lifecycle projectmethode.

In alle projecten behoeven implicaties van informatiebeveiliging regelmatig te worden behandeld en beoordeeld. Verantwoordelijkheden voor informatiebeveiliging bijdragen te worden gedefinieerd en toegewezen aan specifieke rollen die zijn gedefinieerd in de projectbeheermethoden.

C.2. Tactisch beveiligingsbeleid

Doelstelling

Een beheerkader vaststellen om de implementatie en uitvoering van de informatiebeveiliging binnen de organisatie te initiëren en te beheren. (ISO 0.1)

Het tactisch uitvoeringsbeleid geeft beleidsangangspunten voor de inrichting van beveiliging overeenkomstig aan de onderscheiden processen en producten.

Toelichting

De beleidsverantwoordelijkheid wordt als gescheiden verantwoordelijkheid gezien t.o.v. de uitvoeringsverantwoordelijkheid.

De tactische beveiligingsacties hebben voor het merendeel betrekking op meerdere verantwoordelijke-richtlijnen waarbij de samenhang tussen de verschillende richtlijnen gehoord moet zijn of zo overtuigend het belang van de desbetreffende verantwoordelijke manager.

Uitvoering

Door een aantal mensen voor de inrichting op hoofdlijnen van beveiligingsaspecten afzonderlijk te definiëren kan de verantwoordelijkheid hiervoor nadrukkelijk door het hoogste management zelf – met ondersteuning van tactisch beveiligingsbeheer – worden gepositioneerd.

C.2.1. naleving van wettelijke en contractuele eisen

Doelstelling: Voorkomen van schendingen van wettelijke, statutaire, regelgevende of contractuele verplichtingen betreffende informatiebeveiliging en beveiligingsaspecten. (ISO 18.1)

C.2.1.1 Identificatie van toepasselijke kaders

Beheersmaatregel

Alle relevante wettelijke, statutaire, regelgevende, contractuele eisen en de wettelijke bepalingen van de organisatie zijn aan de organisatie bekend en worden voor elk informatiebeveiligingsaspect en de organisatie actief worden vastgesteld, gedocumenteerd en actueel gehouden. (ISO 18.1.1)

Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving. (ISO 18.1.4)

Implementatierichtlijn

Ook de specifieke beheersmaatregelen en individuele verantwoordelijkheden om aan deze eisen te voldoen behoren te worden gedefinieerd en gedocumenteerd.

Managers behoren alle wetgeving die toepasselijk is op hun organisatie vast te stellen om te voldoen aan de eisen voor hun soort bedrijfsmatigheid. Indien de organisatie zettelijke activiteiten in andere landen verricht, behoren managers te letten op naleving in alle relevante landen.

C.2.1.2 Privacy en bescherming van persoonsgegevens

Beheersmaatregel

Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving. (ISO 13.1.4)

Implementatierichtlijn

Organisaties behoren een beleid te ontwikkelen en te implementeren voor de privacy en bescherming van persoonsgegevens. Dit beleid betreft te worden gecommuniceerd aan alle personen die betrokken zijn bij het beheersen van persoonsgegevens.

Naleving van dit beleid en van alle relevant wet- en regelgeving betreffende het beschermen van de privacy van personen en de bescherming van persoonsgegevens varieert per organisatie, afhankelijk van de structuur en de werkwijze. Vaak kan dit het beste worden bereikt door een persoon te benoemen

die hiervoor verantwoordelijk is, zoals een privacyfunctionaris, die schikking behoort te geven aan managers, gebruikers en aanbieders van dienst en over hun individuele verantwoordelijkheden en de specifieke procedures die behoren te worden gevolgd. Het toewijzen van verantwoordelijkheid voor het handhaven van persoonsgegevens en het vastleggen dat medewerkers zich bewust zijn van de privacyprincipes behoort te worden uitgevoerd in overeenstemming met relevante wet- en regelgeving. Er behoren passende technische en organisatorische maatregelen te worden geïmplementeerd om persoonsgegevens te beschermen.

C.2.1.3 Beschermen van registraties

Beheersmaatregel

Registraties behoren in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfsvoorwaarden te worden beschermd tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave. (ISO 15.1.3)

Implementatieplichtig

Bij besluitvorming over bescherming van specifieke registraties van de organisatie behoort de classificatie daarvan gebaseerd op het classificatieschema van de organisatie in overweging te worden genomen. Registraties behoren te worden gecategoriseerd naar type, bijv. boekhoudkundige registraties, distributieprocedures, verspreidingsdocumenten, auditlogboeken en operationele procedures. Elk type behoort de beveiligingsmaatregelen te worden toegepast die worden vermeld, bijv. papier, microfilm, magnetische of optische opslag. Geavanceerde cryptografische sleutels en programma's die samenhangen met versleutelde archieven of digitale handtekening (zie hoofdstuk ISO 13), behoren ook te worden bewaard om decodering van de registraties mogelijk te maken gedurende de bewaarperiode van de registraties.

Er behoort rekening te worden gehouden met de mogelijkheid dat media die worden gebruikt om registraties te bewaren in kwelbare uitdruipingen. Procedures voor bewaren en beheren van deze media behoren te worden geïmplementeerd in overeenstemming met de aanbevelingen van de fabrikant.

Als elektronische opslagmedia worden gekozen behoren procedures te worden vastgesteld om te waarborgen dat de gegevens tijdens de bewaarperiode toegankelijk blijven (beschikbaar van zowel de media als van het gegevensformaat), om te voorkomen dat de informatie verloren gaat als gevolg van toekomstige technologische veranderingen.

Systemen voor gegevensopslag behoren zo te worden gekozen dat versteelde gegevens binnen een aanvaardbare tijdsperiode en in een aanvaardbaar formaat kunnen worden opgevoerd, afhankelijk van de aanpak waaraan moet worden voldaan.

Het systeem waarmee gegevens worden opgeslagen en behandeld, behoort de identificatie van registraties of hun bewaarperiode te waarborgen zoals gedefinieerd door, indien van toepassing, nationale of regionale wet- of regelgeving. Dit systeem behoort, los te staan dat registraties in afwijking van de norm op een passende manier worden vastgelegd als de organisatie ze niet langer nodig heeft.

Om te voldoen aan deze eisenstellingen met betrekking tot het vastleggen van registraties behoren binnen een organisatie de volgende stappen te worden genomen:

- a) er behoren richtlijnen te worden vastgesteld voor het bewaken, opslaan, behandelen en verwijderen van registraties en informatie;
- b) er behoort een bewaarschema te worden opgesteld waarin registratie en de periode dat ze moeten worden bewaard, zijn vastgelegd;
- c) er behoort een inventarisoverzicht van bronnen van belangrijke informatie te worden bijgehouden.

C.2.2. Scheiding van taken

Beheersmaatregel

Conflicterende taken en verantwoordelijkheden behoren te worden gescheiden om de kans op onbevoegd of onbehoorlijk wijzigen of misbruik van de bedrijfsmiddelen van de organisatie te verminderen. (ISO 6.1.2)

Toelichting

In de daarnoor in nummering komende paragrafen voor processen en producten zijn gedetailleerde normen uitgewerkt voor functieschelingen. Deze hebben betoetsen voor de afstemming en het toekennen van autorisaties. In het tactisch beleid wordt aangegeven welke functieschelingen er op het hoogste niveau van een organisatie worden gehanteerd.

Implementatierichtlijn

Er behoort op te worden gelet dat geen enkel persoon ongemerkt of zonder autorisatie toegang kan krijgen tot bedrijfsinformatie, zo kan wijzigen of gebruiken. Het initieel van een gebruikersnaam behoort te worden gecorrigeerd van de autorisatie ervan. Bij het ontwerpen van beheerstrategieën behoort rekening te worden gehouden met de mogelijke invloed van samenwerking.

Er is functiescheiding tussen

- a) beleidsvoorbereiding en uitvoering;
- b) gebruikers en ontwikkeling en beheer van faciliteiten voor zittingen (Huisvesting en ICT);
- c) tactische beheerprocessen en uitvoerende processen;
- d) beslissende, bewakende, registrerende, uitvoerende en controleerende functies.

C.2.3. Vertrouwenfuncties**Beheersmaatregel**

Er behoort te worden vastgesteld welke functies in de organisatie worden aangemerkt als vertrouwenfuncties conform de Leidraad aanwijzing vertrouwenfuncties van de AFVD.

C.2.4. Toegangsbeveiliging**C.2.4.1 Bedrijfsreizen voor toegangsbeveiliging**

Doelstelling: toegang tot informatie en informatieverwerkende faciliteiten beperken. (ISO 9.1)

C.2.4.1.1 Beleid voor toegangsbeveiliging**Beheersmaatregel**

Een beleid voor toegangsbeveiliging behoort te worden vastgesteld, gecoördineerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingsreizen. (ISO 9.1.1)

Implementatierichtlijn

Eigenaren van bedrijfsinformatie behoren passende regels voor toegangsbeveiliging, -rechten en -beperkingen voor specifieke gebruikersrollen ten aanzien van hun bedrijfsinformatie vast te stellen, waarbij de details en de striktheid van de beheersmaatregelen en afspiegeling zijn van de centrale informatiebeveiligingsrichtlijn.

Toegangsbeveiligingsmaatregelen zijn zowel logisch als fysiek van aard (zie hoofdstuk ISO 11) en behoren als een geheel te worden beschouwd. Gebruikers en dienstverleners behoren een duidelijke verklaring te ontvangen waarin is vastgelegd aan welke bedrijfsreizen en toegangsbeveiligingsmaatregelen zij moeten voldoen.

Het beleid behoort rekening te houden met het volgende:

- a) beveiligingsreizen van de bedrijfsreizenreizen;
- b) beleidsregels voor informatieverspreiding en -autorisatie, bijv. het 'need-to-know' of 'need-to-do'-principe, informatiebeveiligingsniveau en -classificatie (zie ISO 8.2);
- c) consistentie tussen de toegangsrechten en de beleidsregels inzake informatieclassificatie van systemen en netwerken;
- d) relevante werving en contractuele verplichting met betrekking tot toegang aan de toegang tot gegevens en informatie (zie ISO 13.1);
- e) het beheer van toegangsrechten in een desk/bulk- en netwerkgeving die alle beschiktare

soorten verbindingen herkent;

f) scheiding van toegangsbeveiligingsrollen (bijv. toegangsverzoek, -autorisatie, -administratie);

g) eisen voor formele autorisatie van toegangsverzoeken (zie ISO 9.2.1 en ISO 9.2.2);

h) eisen voor het periodiek beoordelen van toegangsrechten (zie ISO 9.2.5);

i) intrekken van toegangsrechten (zie ISO 9.2.6);

j) archiveren van verslaggeving van alle belangrijke gebeurtenissen betreffende het gebruik en het beheer van gebruikersidentificaties en geheime authenticatie-informatie;

k) rollen met speciale toegangsrechten (zie ISO 9.2.3).

Het gebruik van systeemupmiddelen die in staat zijn om beheersmaatregelen voor systemen en toegangslijnen te onttrekken behoort te worden beperkt en nauwkeurig te worden gecontroleerd. (ISO 9.4.4)

C.2.4.2 Beheer van toegangsrechten van gebruikers

Doelstelling: Toegang voor bevoegde gebruikers bewerkstelligen en onbevoegde toegang tot systemen en diensten voorkomen. (ISO 9.2)

C.2.4.2.1 Registratie en afmelden van gebruikers

Beheersmaatregel

Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken. (ISO 9.2.1)

Implementatierichtlijn

De procedure voor het behouden van gebruikersidentificaties behoort te omvatten:

a) het gebruik van unieke gebruikersidentificaties zodat gebruikers kunnen worden geïdentificeerd en verantwoordelijk kunnen worden gesteld voor hun acties; het gebruik van goedgedefinieerde identificaties behoort alleen te worden toegestaan als deze om bedrijf- of operationele redenen noodzakelijk zijn en beheer te worden goedgedocumenteerd;

b) het onmiddellijk ongeduid maken of verwijderen van de gebruikersidentificatie van gebruikers die de organisatie hebben verlaten (zie ISO 9.2.6);

c) het periodiek identificeren en verwijderen van overbodige gebruikersidentificaties;

d) het ervoor zorgen dat overbodige gebruikersidentificaties niet aan andere gebruikers worden afgegeven.

C.2.4.2.2 Gebruikers toegang verlenen

Beheersmaatregel

Een formele gebruikerstoeegangsverleningsprocedure behoort te worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken. (ISO 9.2.2)

Implementatierichtlijn

De procedure voor het toewijzen of intrekken van toegangsrechten aan gebruikersidentificaties behoort te omvatten:

a) automatische verificaties van de eigenaar van het informatie-systeem of de informatie-dienst voor het gebruik van het informatie-systeem of de informatie-dienst (zie beheersmaatregel ISO 9.1.2); afzondelijke goedkeuring voor toegangsrechten door de directie is mogelijk, eek relevant;

b) vaststellen dat het verdoende toegangsniveau in overeenstemming is met de beleidsregels voor toegang (zie ISO 9.1) en consistent is met andere eisen zoals een scheiding van taken (zie ISO 6.1.2);

c) waarborgen dat toegangsrechten niet worden geactiveerd (bijv. door dienstverleners) voordat de autorisatieprocedures zijn afgerond;

d) bijhouden van een centraal overzicht van toegangsrechten die aan een gebruiker/identificatie zijn toegekend om toegang te verkrijgen tot informatiesystemen en -diensten;

e) aanpassen van toegangsrechten van gebruikers van wie de rollen of functies zijn gewijzigd en toegangsrechten van gebruikers die de organisatie hebben verlaten onmiddellijk verwijderen of blokkeren;

f) met eigenaars van de informatiesystemen of -diensten periodiek de toegangsrechten beoordelen (zie ISO 9.2.6).

C.2.4.2.3 Beheeren van speciale toegangsrechten

Beheersmaatregel

Het toewijzen en gebruik van speciale toegangsrechten behoren te worden besproken en goedgekeurd. (ISO 9.2.3)

Implementatierichtlijn

Het toewijzen van speciale toegangsrechten behoort te worden beheerd door een formele autorisatieprocedure die in overeenstemming is met het relevante toegangsbeveiligingsbeleid (zie beheersmaatregel ISO 9.1.1). De volgende stappen behoren in overweging te worden genomen:

a) de speciale toegangsrechten behorend bij elk systeem of proces, bijv. bestuursprogramma, databeheersysteem en elke toepassing, en de gebruikers van wie ze moeten worden toegewezen, behoren te worden gedefinieerd;

b) speciale toegangsrechten behoren op basis van noodzaak tot gebruik en per gebeurtenis aan gebruikers te worden toegekend in overeenstemming met het toegangsbeveiligingsbeleid (zie ISO 9.1.1), d.w.z. gebaseerd op wat minimaal is vereist voor hun functionele rollen;

c) er behoort een autorisatieprocedure en een verslaggeving van alle toegekende speciale toegangsrechten te worden bijgehouden. Speciale toegangsrechten behoren niet te worden verleend voordat de autorisatieprocedure is afgerond;

d) voor het vervallen van speciale toegangsrechten behoren eisen te worden gedefinieerd;

e) speciale toegangsrechten behoren te worden toegekend aan een gebruiker/identificatie die vereist is voor de functies die voor reguliere bedrijfsactiviteiten worden gebruikt. Reguliere bedrijfsactiviteiten behoven niet met een speciale gebruikersidentificatie te worden verricht;

f) de competenties van gebruikers met speciale toegangsrechten behoven regelmatig te worden beoordeeld om te vaststellen of ze in overeenstemming zijn met hun taken;

g) specifieke procedures behoren te worden vastgesteld en erin te houden om onbevoegd gebruik van gebruikersidentificaties voor algemeen beheer te voorkomen, in overeenstemming met de configuratiecapaciteiten van het systeem;

h) voor gebruiker/identificaties voor algemeen beheer behoort de geheimhouding van geheime authenticatie-informatie in acht te worden genomen als deze wordt gecreëerd (bijv. wisselveranderingen van wachtwoord en zodra een speciale gebruiker verroopt of van functie verandert, dit onder speciale gebruiker/identificaties met de passende mechanismen).

C.2.4.2.4 Beheer van geheime authenticatie-informatie van gebruikers

Beheersmaatregel

Het toewijzen van geheime authenticatie-informatie behoort te worden beheerst via een formeel beheersproces. (ISO 9.2.4)

Implementatierichtlijn

Het proces behoort de volgende eisen te bevatten:

- gebruikers behoren te worden verplicht een verklaring te ondertekenen dat zij persoonlijke geheime authenticatie-informatie geheimhouden en gegevensinformatie, d.w.z. gecodeerde geheime authenticatie-informatie, binnen de groep houden; deze getekende verklaring kan worden opgenomen in de arbeidsovereenkomst (zie ISO 7.1.2);
- als gebruikers hun eigen geheime authenticatie-informatie moeten onderhouden behoort hun eerst tijdelijke geheime authenticatie-informatie te worden gegeven die zij bij het eerste gebruik moeten wijzigen;
- er behoren procedures te worden vastgesteld om de identiteit van een gebruiker vast te stellen voordat nieuwe, vervangende of tijdelijke geheime authenticatie-informatie wordt verstrekt;
- tijdelijke geheime authenticatie-informatie behoort op een veilige manier naar gebruikers te worden gegeven; gebruikmaken van externe partijen of onbeschermde e-mailberichten (niet-gecodeerde tekst) behoort te worden vermeden;
- tijdelijke geheime authenticatie-informatie behoort uniek voor een persoon te zijn en behoort niet te kunnen worden geademd;
- gebruikers behoren de ontvangst van geheime authenticatie-informatie te bevestigen;
- 'default' geheime authenticatie-informatie van een leverancier behoort te worden gewijzigd na de installatie van systemen of software.

C.2.4.2.5 Beoordeling van toegangsrechten van gebruikers

Beheersmaatregel

Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen. (ISO 9.2.5)

Implementatierichtlijn

Bij het beoordelen van toegangsrechten van gebruikers behoren de volgende aspecten in aanmerking te worden genomen:

- toegangsrechten van gebruikers behoren regelmatig en na wijzigingen, zoals promotie, degradatie of beëindiging van het dienstverband, te worden beoordeeld (zie hoofdstuk ISO 7);
- toegangsrechten van gebruikers behoren te worden beoordeeld en op een wijze te worden toegekend bij functieverandering binnen dezelfde organisatie;
- autorisaties voor speciale toegangsrechten behoren vaker te worden beoordeeld;
- toewijzingen van speciale toegangsrechten behoren regelmatig te worden gecontroleerd om te waarborgen dat speciale toegangsrechten niet onbeveegd zijn verkrijgen;
- van wijzigingen in speciale accounts behoren voor periodieke beoordeling logbestanden te worden bijgehouden.

C.2.4.2.6 Toegangsrechten inbreken of aanpassen

Beheersmaatregel

De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatieverwerkende faciliteiten behoren bij beëindiging van hun dienstverband, contract of overeenkomst te worden verwijderd en bij wijzigingen behoren ze te worden aangepast. (ISO 9.2.6)

Implementatierichtlijn

Bij beëindiging van het dienstverband behoren de toegangsrechten van een persoon voor informatie en bedrijfsmiddelen die samenhangen met informatieverwerkende faciliteiten en diensten te worden ingetrokken of opgeschort. Hierdoor kan worden vastgesteld of het noodzakelijk is om toegangsrechten in te trekken.

Wijzigingen in het dienstverband behoren te worden weerspiegeld in het intrekken van alle toegangsrechten die niet voor het nieuwe dienstverband zijn goedgekeurd. De toegangsoverrechten die behoren te worden ingetrokken of aangepast omvatten ook de fysieke en logische toegangsrechten. Intrekking of aanpassing kan plaatsvinden door verwijdering, intrekking of vervanging van sleutels, identificatiekaarten, informatieverwerkende faciliteiten of abonnementen. Elk document dat toegangsrechten van medewerkers en contactanten identificeert, behoort de intrekking of aanpassing van toegangsrechten weer te geven. Indien een medewerker die uit dienst gaat of een externe gebruiker wachtwoord kent van gebruikerscertificaten die actief blijven, dan behoren deze bij beëindiging of wijziging van dienstverband, contract of overeenkomst te worden gewijzigd.

Toegangsrechten voor informatie en bedrijfsmiddelen die samenhangen met informatieverwerkende faciliteiten behoren te worden vermindert of ingetrokken voordat het dienstverband eindigt of wijzigt, afhankelijk van de evaluatie van risicofactoren zoals:

- of de beëindiging of wijziging is geïnitieerd door de medewerker, de externe gebruiker of door de directie, en de reden voor de beëindiging;
- de huidige verantwoordelijkheden van de medewerker, externe gebruiker of overige gebruikers;
- de waarde van de bedrijfsmiddelen die op dat moment toegankelijk zijn.

C.2.4.2.7 Geheime authenticatie-informatie gebruiken

Beheersmaatregel

Van gebruikers behoort te worden verwacht dat zij zich bij het gebruiken van geheime authenticatie-informatie houden aan de praktijk van de organisatie. (ISO 1554)

Implementatierichtlijn

Alle gebruikers behoren het advies te krijgen om:

- vertrouwelijk om te gaan met geheime authenticatie-informatie, en ervoor te zorgen dat deze informatie niet openbaar wordt gemaakt aan andere partijen, met inbegrip van gezaghebbende personen;
- geen geheime authenticatie-informatie te registreren (bijv. op papier, in een computerv bestand of op een zakkapparaat), tenzij deze informatie veilig kan worden opgeslagen en de opslagmethode is goedgekeurd (bijv. "password vault");
- geheime authenticatie-informatie te wijzigen als er een aanwijzing is dat deze mogelijk is gecompromiteerd;
- als wachtwoorden als geheime authenticatie-informatie worden gebruikt, sterke wachtwoorden te kiezen van voldoende lengte, die:
 - gemakkelijk te onthouden zijn;
 - niet zijn gebaseerd op gegevens die iemand anders gemakkelijk kan raden of achterhalen (zoar persoonsgegevens, informatie te gebruiken, zoals namen, telefoonnummers en geboortedata);
 - niet kwetsbaar zijn voor woordenboekaanvallen (d.w.z. niet bestaan uit woorden die in woordenboeken zijn opgenomen);
 - geen opeenvolgende identieke tekens bevat, en niet alleen uit cijfers of letters bestaat;
 - bij het eerste inloggen worden gewijzigd als ze tijdelijk zijn;
- geen geheime authenticatie-informatie te delen;

- f) te zorgen voor passende bescherming van wachtwoorden wanneer wachtwoorden worden gebruikt als referentie authenticatie-informatie in geautomatiseerde logprocedures en worden opgeslagen;
- g) niet dezelfde gevoelige authenticatie-informatie voor zakelijke en particuliere toepassingen te gebruiken.

C.2.6. Informatieuitwisseling en –transport

C.2.6.1 Classificatie

Doelstelling: Bewerkstelligen dat informatie een passend beschermingsniveau krijgt dat in overeenstemming is met het belang ervan voor de organisatie. (ISO 8.2.)

C.2.6.1.1 Classificatie van informatie

Beheersmaatregel

Informatie behoort te worden geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging. (ISO 8.2.1.)

Implementatierichtlijn

Classificaties en de bijbehorende beschermende beheersmaatregel en voor informatie behoren rekening te houden met de zakelijke behoeften om informatie te delen en te beperken, en met wettelijke eisen. Al deze bedrijfsmiddelen van informatie kunnen ook worden geclassificeerd in overeenstemming met de classificatie van informatie die is opgeslagen in, verwerkt door of anderszins behandeld of beschermd door het bedrijfsmiddel.

Eigenschappen van informatiebedrijfsmiddelen behoren verantwoordelijk te zijn voor de classificatie ervan. Het classificatiesysteem behoort regels voor het classificeren te bevatten, en criteria voor het na verloop van tijd evalueren van de classificatie. Het beheersingsniveau dat in het schema wordt vastgelegd behoort te worden vastgesteld door de vertrouwelijkheid, integriteit en beschikbaarheid en eventuele andere eisen voor de desbetreffende informatie te analyseren. Het schema behoort in overeenstemming te worden gebracht met het beleid voor toegangsbeveiliging (zie ISO 9.1.1).

Elk niveau behoort ook naar te krijgen die betekenis heeft in de context van de toepassing van het classificatieschema.

Het schema behoort organisatiebreed consistent te zijn zodat iedereen informatie en gerelateerde bedrijfsmiddelen op dezelfde manier classificeert op basis van een gemeenschappelijk begrip van beschermingsniveau en de passende bescherming toepast.

Classificatie behoort te worden opgenomen in de procedures van de organisatie en organisatiebreed consistent en coherent te zijn. Resultaten van classificatie behoren de waarde van bedrijfsmiddelen aan te geven afhankelijk van hun gevoeligheid en belang voor de organisatie, bijv. in de zin van vertrouwelijkheid, integriteit en beschikbaarheid. Resultaten van classificatie behoren te worden geactualiseerd in overeenstemming met wijzigingen in hun waarde, gevoeligheid en belang in de loop van hun levenscyclus.

C.2.6.1.2 Informatie labelen

Beheersmaatregel

Om informatie te labelen behoort een passende reeks procedures te worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie. (ISO 8.2.2.)

Implementatierichtlijn

Procedures voor het labelen van informatie behoren te gaan over informatie en gerelateerde bedrijfsmiddelen in fysieke en elektronische formaten. De labeling behoort in overeenstemming te zijn

met het classificatieschema vastgesteld in ISO 8.2.1. De labels beken gemakkelijk herkenbaar te zijn. De procedures betreffen richtlijnen te geven over waar en hoe labels zijn bevestigd, rekening houdend met hoe de informatie wordt gecreëerd of hoe de bedrijfsdelen worden geïntegreerd afhankelijk van de soorten media. De procedures kunnen geven en definiëren waarin labels niet wordt toegepast, bijvoorbeeld op vertrouwelijke informatie, om de werklust te verminderen. Medewerkers en contractanten behoren op de hoogte te worden gebracht van de labelprocedures.

Output van systemen die informatie bevatten die is geclassificeerd als gevoelig of essentieel behoort een passend classificatie label te dragen.

C.2.5.4.3 Behandelen van bedrijfsmiddelen

Beheersmaatregel

Procedures voor het behandelen van bedrijfsmiddelen behoren te worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie. (ISO 8.2.5)

Implementatierichtlijn

Voor het hanteren, verspreken, opslaan en communiceren van informatie behoren procedures te worden opgesteld die consistent zijn met de classificatie van de informatie (zie ISO 8.2.1).

Met de volgende aspecten behoort rekening te worden gehouden:

- toegangsbeperkingen die de beschermingsniveau van elk classificatieniveau ondersteunen;
- onderhoud van een formele verslaggeving van de bevoegde ontvangers van bedrijfsmiddelen;
- bescherming van tijdelijke of permanente kopieën van de informatie tot een niveau dat consistent is met de bescherming van de originele informatie;
- opslag van IT-tekstbestanden in overeenstemming met de vereisten van de federatie;
- duidelijke markering van alle kopieën van media ter attentie van de bevoegde ontvanger.

Het binnen de organisatie gebruikte classificatieschema is mogelijk niet gelijk aan de schema's die door andere organisaties worden gebruikt, zelfs als de namen van de niveaus gelijk zijn; bovendien kan informatie die al tussen u gemeenlijk beweegt verschillen in classificatie afhankelijk van de context in elke organisatie, zelfs als de classificatienamen's identiek zijn.

Overeenkomsten met andere organisaties waar het delen van informatie in voorkomt, behoren procedures te bevatten voor het identificeren van de classificatie van de informatie en voor het interpreteren van de classificatie labels van andere organisaties.

C.2.6.2 Beleid en procedures voor informatieverspreiden

Beheersmaatregel

Ter bescherming van het informatieverspreiden, dat via alle soorten communicatiefaciliteiten verloopt, behoren formele beleidsregels, procedures en beheersmaatregelen voor verspreiden van kracht te zijn. (ISO 12.2.1)

Implementatierichtlijn

Bij procedures die moeten worden gevolgd en beheersmaatregelen die moeten worden uitgevoerd bij het gebruik van communicatiefaciliteiten voor informatieverspreiden behoren de volgende punten in overweging te worden genomen:

- procedures die zijn ontworpen ter beveiliging van overgedragen informatie tegen interceptie, kopiëren, wijziging, foutieve routing en vernietiging;
- procedures voor het opsporen van en beschermen tegen malware die kan worden overgebracht door het gebruik van elektronische communicatie (zie ISO 12.2.1);
- procedures ter bescherming van als bijlage geïmplementeerde gevoelige elektronische informatie;

c) beleid of richtlijnen die aantoonbaar gebruik van communicatiefaciliteiten omschrijven (zie ISO 6.1.3);

e) verantwoordelijkheden van personeel, van externe partijen en van andere gebruikers om de organisatie niet te compromitteren, b.v. door laster, pesten, aanvaringen van een valco hoedanigheid, leegstraven, onbeveegde inroepen enz.

f) gebruik van cryptografische codering, bijv. om de vertrouwelijkheid, integriteit en authenticiteit van informatie te beschermen (zie hoofdstuk ISO 10);

g) richtlijnen voor bewaren en vernietigen van alle bedrijfsgegevens, waaronder berichten, in overeenstemming met relevante nationale en lokale wet- en regelgeving;

h) beheersmaatregelen en beperkingen die samenhangen met het gebruik van communicatiefaciliteiten, bijv. het gebruik van afzenderinstellingen voor e-mail naar externe e-mailadressen;

i) personeel adviseren om passende voorzorgsmaatregelen te treffen om geen vertrouwelijke informatie bekend te maken;

j) geen berichten die vertrouwelijke informatie bevatten achterlaten op antwoordapparaten omdat deze kunnen worden afgeleest door onbevoegde personen, op gemeenschappelijke systemen kunnen worden opgeslagen of onjuist kunnen worden opgeslagen als gevolg van foutieve nummerkeuze;

k) personeel informeren over problemen in verband met het gebruiken van faxapparatuur of -diensten, zie bijl. 1.

1) onbeveegde toegang tot: ingebouwde berichtenboxen om berichten op te vragen;

2) opzettelijk of onbedoeld programmeren van machines waardoor berichten naar bepaalde nummers worden gestuurd;

3) documenten en berichten naar het verkeerde nummer sturen door onjuiste nummerkeuze of door het verkeerde opgeslagen nummer te gebruiken.

Overeenskomsten behoren te worden gesloten met de voorzitter van de werkgroep, met de voorzitter van de werkgroep of met de voorzitter van de werkgroep, met de voorzitter van de werkgroep of met de voorzitter van de werkgroep.

Uitsluitend op het gebied van informatietransport behoren te worden aan te relevantie te worden (zie ISO 13.1).

C.2.5.3 Overeenkomsten over informatietransport

Beheersmaatregel

Overeenkomsten behoren betrekking te hebben op het beveiligd transporteren van bedrijfsinformatie tussen de organisatie en externe partijen. (ISO 13.2.2)

Implementatierichtlijn

Overeenkomsten over informatietransport behoren het volgende te bevatten:

a) directieverantwoordelijkheden voor het beheersen en notificeren van overdracht, verzending en ontvangst;

b) procedures om de traceerbaarheid en onweerslegbaarheid te waarborgen;

c) technische minimumwaarden voor het verpakken en verstuuren;

d) bergovereenkomsten;

e) kenmerkend etiketteren;

f) versiebeheersing en aansprakelijkheden in geval van informatiebeveiligingsincidenten, zoals verlies van gegevens;

g) gebruik van een afzenderlabelsysteem voor gevoelige of essentiële informatie dat waarborgt dat de betekenis van de labels meteen duidelijk is en dat de informatie passend is beschermd (zie ISO 8.2).

h) technische normen voor het vastleggen en lezen van informatie en software;

i) speciale beheersaanpakke en die vereist zijn om gevoelige informatie te beschermen, zoals cryptografie (zie hoofdstuk ISO 19);

j) handhaven van en bewakingstaken voor informatie tijdens verzending;

k) acceptabele niveau voor toegangsbeveiliging.

Tu besluit overring van informatie en fysieke media bij het uitvoeren van het overnamebeleid, procedures en methoden te worden vastgesteld en gehandhaafd (zie ISO R 3.3), en hieraan behoort in overeenstemming met de vooraf te worden vermeld.

De informatiebeveiligingsinhoud van een overeenkomst behoort de beveiliging van de desbetreffende bedrijfsinformatie weer te geven.

C.2.5.4 Archiefbeheer

Beheersmaatregel

Er worden voldoende maatregelen genomen om op een efficiënte manier bij te dragen aan het behoud van het waardevolste verleden van de informatie uitstraling. Het archiefbeheer moet voldoen aan de gestelde eisen zoals opgenomen in de Baseline Informatiehuishouding Bijlageverhaal.

Implementatierichtlijn

De verbeteringen die voortvloeien uit de bevindingen van de jaarlijkse monitor (vanuit het bezicht) zijn ingebed in de werkprocessen van de bedrijfsonderdelen. Bij de bedrijfsonderdelen is een kwaliteitsysteem binnen de eigen plan- en verbetercyclus geïmplementeerd en in werking.

C.2.5.5 Beheer van verwijderbare media

Beheersmaatregel

Voor het beheeren van verwijderbare media behoren procedures te worden ontwikkeld en in overeenstemming met het classificatieschema dat door de organisatie vastgesteld (ISO E.3.1)

Implementatierichtlijn

Voor het beheeren van verwijderbare media behoren de volgende richtlijnen in acht te worden genomen:

- van herbruikbare media die de organisatie verlaten, behoort de inhoud, als die niet meer nodig is, onherstelbaar te worden verwijderd;
- indien nodig en haalbaar behoort goedkeuring te worden verkregen om media uit de organisatie te verwijderen en er behoort een vastlegging van dergelijke verwijderingen te worden bijgehouden voor het onterhouden van een audittrail;
- alle media behoren te worden opgeslagen in een veilige beveiligde omgeving, in overeenstemming met de voorschriften van de afzender;
- indien vertrouwelijkheid of integriteit van gegevens belangrijke overwegingen zijn, behoren specifieke maatregelen te worden getroffen om gegevens op verwijderbare media te beschermen;
- om het risico te verminderen dat media in kwalitatief achteruitgaan terwijl de opgeslagen gegevens nog nodig zijn, behoren te worden overgebracht naar nieuwe media voordat ze onleesbaar worden;
- van waardeloze gegevens behoren meerdere kopieën op verschillende media te worden opgeslagen om het risico verder te verminderen van toevallige beschadiging of verlies van gegevens;
- om de kans op verlies van gegevens te beperken behoort registratie van verwijderbare media te worden overwogen;
- instructies voor verwijderbare media behoren alleen te worden uitgegeven aan een bedrijfsunit die dit is vereist;
- als er behoefte is om verwijderbare media te gebruiken behoort de overdracht van informatie op dergelijke media te worden overwogen.

Procedures en activiteiten voor het beheer van documenten.

C.2.6.6 Verwijderen van media

Beheersmaatregel

Media behoren op een veilige en beveiligde manier te worden verwijderd als ze niet langer nodig zijn, eventueel na formele procedures. (ISO 8.3.2)

Implementatie-richtlijn

Voor het beveiligd verwijderen van media behoren formele procedures te worden vastgesteld om het risico zo klein mogelijk te houden dat vertrouwelijke informatie bij onbevoegde personen terechtkomt. De procedures voor het beveiligd verwijderen van media die vertrouwelijke informatie bevatten, behoren in verhouding te staan tot de gevoeligheid van die informatie. Met de volgende aspecten behoren rekening te worden gehouden:

- a) media die vertrouwelijke informatie bevatten behoren op een beveiligde manier te worden opgeslagen en verwijderd, bijv. door verbranding of versnippering, of de gegevens behoren te worden gewist voordat de media worden gebruikt door een andere toepassing in de organisatie;
- b) er behoren procedures te zijn om media te identificeren die mogelijk veilig moeten worden verwijderd;
- c) mogelijk is het eenvoudiger om ervoor te kiezen alle media in te zamelen en veilig te verwijderen in plaats van te proberen de gevoelige media te scheiden van de rest;
- d) veel organisaties bieden voor media inzamelings- en verwijderingsdiensten aan; de keuze voor een passende externe partij die beschikt over adequate beheersmaatregelen en ervaring behoort zorgvuldig te gebeuren;
- e) verwijdering van gevoelige media behoort te worden geregistreerd om een audit trail te onderhouden.

Bij het accumuleren van media voor verwijdering behoort rekening te worden gehouden met het aggregatie-effect, waardoor een grote hoeveelheid niet-gevoelige informatie gevoelig kan worden.

C.2.6.7 Media fysiek overdragen

Beheersmaatregel

Media die informatie bevatten, behoren te worden beschermd tegen onbevoegde toegang, misbruik of corruptie tijdens transport. (ISO 8.3.3)

Implementatie-richtlijn

De volgende richtlijnen behoren te worden overwogen om media die informatie bevatten te beschermen tijdens transport:

- a) er behoren betrouwbare transport- of koeriersdiensten te worden gebruikt;
- b) met de afzender kan worden afgesproken welke koeriersdiensten bevoegd zijn;
- c) er behoren procedures te worden ontwikkeld om de identificatie van koeriers te verifiëren;
- d) de verpakking behoort toereikend te zijn om de inhoud te beschermen tegen fysieke schade die tijdens transport kan ontstaan en behoren in overeenstemming te zijn met de voorschriften van de fabrikant. Bijv. bescherming tegen milieufactoren die het herstelvermogen van de media kunnen verminderen zoals blootstelling aan hitte, vocht of elektromagnetische velden;
- e) er behoren registraties te worden bijgehouden die de inhoud van de media en de toegepaste bescherming identificeren en waarin wordt vastgelegd hoe vaak de media zijn vervoerd naar de besteller en het in ontvangst nemen op de plaats van bestemming.

C.2.6.8 Elektronische berichten

Beheersmaatregel

Informatie die is opgenomen in elektronische berichten behoort passend te zijn beschermd. (ISO

13.2.3)

Implementatierichtlijn

Overnames betreffende informatiebeveiliging van elektronisch berichtenverkeer behoren de volgende aspecten te behelzen:

- a) berichten beschermen tegen onbevoegde toegang, wijziging of weigering van dienstverlening in overeenstemming met het classificatieschema dat de organisatie heeft aangenomen;
- b) correcte adressering en transport van het bericht waarborgen;
- c) betrouwbaarheid en beschikbaarheid van de dienst;
- d) veilige overdrachten, bijv. eisen voor elektronische handtekeningen;
- e) bescherming van het verkeer voordat aan het gebruiken van externe openbare diensten zoals instant messaging, sociale netwerken of delen van bestanden;
- f) lagere niveaus van authenticatie voor het controleren van de toegang vanuit openbaar toegankelijke netwerken.

C.2.6. Mobile apparatuur**Deheersmaatregel**

Beleid en ondersteunende beveiligingsmaatregelen behoren te worden vastgesteld om de fysieke die het gebruik van mobiele apparatuur met zich meebrengt te beheersen. (ISO 6.5.1)

Implementatierichtlijn

Bij het gebruikmaken van mobiele apparatuur behoort er speciaal op te worden gelet dat bedrijfsinformatie niet wordt gecompromiteerd. Het beleid voor mobiele apparatuur behoort rekening te houden met de status's van werker met mobiele apparatuur in onbestede omgevings.

Het beleid voor mobiele apparatuur behoort te evenwogen te nemen:

- a) registratie van mobiele apparatuur;
- b) eisen voor fysieke bescherming;
- c) beperking van installatie van software;
- d) eisen voor softwareversies voor mobiele apparatuur en voor het toepassen van patches;
- e) beperking van verbinding met informatiebronnen;
- f) toegangsbeveiligingsmaatregelen;
- g) cryptografische technieken;
- h) bescherming tegen malware;
- i) het op afstand onbruikbaar maken, wissen, uitsluiten;
- j) back-ups;
- k) gebruik van internetsdiensten en -apps.

Voorzichtigheid is geboden bij het gebruik van mobiele apparatuur in openbare ruimten, vergader ruimten en andere onbeschermde locaties. Er behoort beveiliging te zijn om onbevoegde toegang tot of openbaarmaking van de op deze apparaten opgeslagen of verwerkte informatie te voorkomen, bijv. door gebruik te maken van cryptografische technieken (zie hoofdstuk ISO 10) en het gebruik van geheime authenticatie-informatie afwijzingen (zie ISO 9.2.4).

Mobilele apparatuur behoort ook fysiek te zijn beveiligd tegen diefstal, in het bijzonder wanneer deze wordt achtergelaten in bijvoorbeeld andere vervoermiddelen, in hotelkamers, conferentie- en ontmoetingsruimten. Er behoort ook speciale procedures te worden vastgesteld voor diefstal, verlies van mobiele apparatuur e.o. waar rekening is gehouden met juridische, verzekering- en andere veiligheidszaken die in de organisatie gelden. Apparatuur die belangrijke, gevoelige of essentiële bedrijfsinformatie draagt, behoort niet onbewaakt te worden achtergelaten, en behoort, waar mogelijk fysiek achter slot en grendel te worden opgeborgen of er behoren speciale sloten te worden gebruikt om de apparatuur te beveiligen.

Medewerkers die mobiele apparatuur gebruiken, behoren te worden getraind zodat ze zich bewust worden van de juiste risico's die deze manier van werken met zich meebrengt en ze weten welke beheersmaatregelen behoren te worden geïmplementeerd.

Als het beleid voor mobiele apparatuur toelaat dat medewerkers gebruikmaken van mobiele apparatuur die hun eigendom is, behoren het beleid en gerelateerde veiligheidsmaatregelen ook de volgende aspecten te beschrijven:

- scheiding van privé- en zakelijk gebruik van de apparatuur, met inbegrip van het gebruik van software ter ondersteuning van een dergelijke scheiding en ter bescherming van bedrijfsgegevens op een privéapparaat;
- toegang verschermt tot bedrijfsinformatie alleen nadat gebruikers een eindgebruikersovereenkomst hebben ondertekend waarin zij hun verplichtingen betreffen fysieke beveiliging, updates van software enz.), als en/of doen van afspraken van bedrijfsgegevens, toestaan dat de organisatie op afstand gegevens mist in geval van diefstal of verlies van het apparaat of inzien zij niet langer geautoriseerd zijn. Dit beleid moet rekening houden met de privacywetgeving.

C.2.7. Telewerken en thuiswerken

Beleersmaatregel

Beleid en ondersteunende beveiligingsmaatregelen behoren te worden geïmplementeerd ter beveiliging van informatie die vanaf telewerklocaties wordt benaderd, verwerkt of opgeslagen. (ISO 6.2.7)

Dit ook Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein (ISO 6.2.6)

Implementatiecriteriën

Organisaties die telewerken toestaan, behoren een beleid uit te vaardigen dat de voorwaarden en beperkingen definiëert voor het telewerken. Waar van toepassing geldt en waarbij toegestaan, behoren rekening te worden gehouden met de volgende zaken:

- de bestaande fysieke beveiliging van de telewerklocatie, waarbij rekening wordt gehouden met de fysieke beveiliging van het gebouw en de lokale omgeving;
 - de voorgeslede fysieke telewerkomgeving;
 - de beveiligingsaanpak die voor communicatie geldt, waarbij rekening wordt gehouden met de informatie aan levering up a hand uit de interne systemen van de organisatie, de gevoeligheid van de informatie die wordt benaderd en via de communicatiekoppeling wordt doorgegeven en de gevoeligheid van het interne systeem;
 - het verlies van virtuele sessietoegang waardoor het verspreken en opslaan van informatie op privéapparatuur wordt voorkomen;
 - de beveiliging van onbeveiligde toegang tot informatie of middelen van andere gebruikers van de accommodatie, bijv. familie en vrienden;
 - het gebruik van thuisnetwerken en de eisen of beperkingen van de configuratie van draadloze netwerkdiensten;
 - beleidsregels en procedures ter voorkoming van geschillen over rechten van intellectuele eigendom die is ontwikkeld op privéapparatuur;
 - toegang tot privéapparatuur (om de veiligheid van het apparaat vast te stellen of tijdens een onderzoek), wat wetgeving mogelijk kan verhinderen;
 - softwarelicentieovereenkomsten waardoor de organisatie aansprakelijk kan worden gesteld voor de aanschaf van diensten of voor werkzaamheden die privaat zijn van medewerkers of van andere gebruikers;
 - beveiliging tegen malware en eisen aan de firewall.
- De rechten te nemen richtlijnen en afspraken behoren te omvatten:
- het beschikbaar stellen van passende apparatuur en opbergmethoden voor de telewerkactiviteiten, waar bij het gebruik van privéapparatuur die niet onder het beheer van de organisatie staat, niet is toegestaan;

b) een definitie van goedgekeurde werkzaamheden, de werkdien, de classificatie van informatie waarover men mag beschikken en de interne systemen en diensten waartoe de telewerker bevoegde toegang heeft;

c) het beschikbaar stellen van passende communicatievoorzieningen, met inbegrip van methoden voor het beveiligen van de toegang op afstand;

d) fysieke beveiliging;

e) regels en richtlijnen voor toegang voor familie en bezoekers tot apparatuur en informatie;

f) het beschikbaar stellen van ondersteuning en eenheidsheid van hardware en software;

g) het regelen van de verzekering;

h) de procedures voor de back-up en de bedrijfscontinuïteit;

i) audits en monitoren van de beveiliging;

j) inbrenging van bevoegdheid en toegangsrechten, en het leveren van apparatuur na beëindiging van de telewerkactiviteiten.

C.2.8. Gebruik van cryptografische beheersmaatregelen

Doelstelling: Zorgen voor correct en doeltreffend gebruik van cryptografie om de vertrouwelijkheid, authenticiteit en/of integriteit van informatie te beschermen.

C.2.8.1. Beleid voor het gebruik van cryptografische beheersmaatregelen

Beheersmaatregel

Ter bescherming van informatie behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd. (ISO 19.1.1)

Implementatierichtlijn

Bij het ontwikkelen van een cryptografiebeleid behoren de volgende aspecten in aanmerking te worden genomen:

a) de manier waarop de directie het gebruik van cryptografische beheersmaatregelen in de gehele organisatie behandelt, met inbegrip van de algemene principes die gelden voor de bescherming van de bedrijfsinformatie;

b) het vereiste beschermingsniveau behoort te worden gedefinieerd op basis van een risicobeoordeling, rekening houdend met type, strikte en kwaliteit van het vereiste versleutelingsalgoritme;

c) het gebruik van versleuteling ter bescherming van informatie die wordt vervoerd per draagbare of verwijderbare media-apparatuur of via communicatiekanalen;

d) de aanpak van sleutelbeheer, waaronder methoden ter bescherming van cryptografische sleutels en het herstel van versleutelde informatie in geval van verlies, gecompromitteerde of beschadigde sleutels;

e) rollen en verantwoordelijkheden, bijv. wie is verantwoordelijk voor:

1) het implementeren van het beleid;

2) het sleutelbeheer, waaronder het aanmaken van sleutels (zie ISO 10.1.2);

f) de normen die moeten worden toegepast voor een doeltreffende implementatie in de gehele organisatie (welke oplossing wordt gebruikt voor welk bedrijfsproces);

g) de impact van het gebruik van versleutelde informatie op beheersmaatregelen die zijn gebaseerd op controle van de inhoud (bijv. detectie van malware).

Rij het implementeren van het cryptografiebeleid behoort rekening te worden gehouden met de regelgeving en nationale beperkingen die kunnen gelden voor het gebruik van cryptografische technieken in verschillende delen van de wereld en met problemen met grensoverschrijdende stromen van versleutelde informatie (zie ISO 18.1.9).

Cryptografische beheersmaatregelen kunnen worden gebruikt voor verschillende informatiebeveiligingsdoelstellingen, bijv.:

- a) vertrouwelijkheid: codering van informatie gebruiken om gevoelige of essentiële informatie, tijdens opslag of verzending, te beschermen;
- b) integriteit/authenticiteit: digitale handtekeningen of authenticatiecodes voor berichten gebruiken om de nauwkeurigheid of integriteit van gegevens of essentiële informatie tijdens opslag of verzending te verifiëren;
- c) overdraagbaarheid: cryptografische technieken gebruiken om bewijs te verkrijgen van het al dan niet plaatsvinden van een gebeurtenis of actie;
- d) authenticatie: cryptografische technieken gebruiken ter authenticatie van gebruikers en andere systeemiteiten die toegang vragen tot of die verrichtingen doen met systeemgebruikers, -entiteiten of -bronnen.

C.2.8.2 Beheer van cryptografische sleutels

Beheersmaatregel

Met betrekking tot het gebruik, de bescherming en de levensduur van cryptografische sleutels behoort tijdens hun gehele levenscyclus een beleid te worden ontwikkeld en geïmplementeerd. (ISU 10.1.2)

Implementatierichtlijn

Het beleid behoort eisen te bevatten voor het beheren van cryptografische sleutels tijdens hun gehele levenscyclus met inbegrip van het aanmaken, bewaren, archiveren, terugvinden, distribueren, terugtrekken en vernietigen van sleutels.

Cryptografische algoritmen, sleutelsoorten en gebruikspraktijken behoren te worden geselecteerd in overeenstemming met de "best practices". Passend sleutelbeheer uitvoeren na wettelijke procedures voor het aanmaken, bewaren, archiveren, terugvinden, distribueren, terugtrekken en vernietigen van cryptografische sleutels.

Alle cryptografische sleutels moeten te worden beschouwd tegen aanval op en verlies. Bovendien hebben geheime en particuliere sleutels bescherming nodig tegen onbevoegd gebruik en leggen opzettaamaking. Apparatuur die wordt gebruikt om sleutels aan te maken, op te slaan en te archiveren behoort fysiek te worden beschermd.

Een sleutelbeheersysteem behoort te zijn gebaseerd op een overeengekomen pakket van normen, procedures en beveiligingsmethoden voor:

- a) het aanmaken van sleutels voor verschillende cryptografische systemen en verschillende toepassingen;
- b) het verstrekken en verkrijgen van openbare sleutelcertificaten;
- c) het verspreiden van sleutels onder de beoogde entiteiten en een instructie hoe de sleutels na ontvangst behoren te worden geactiveerd;
- d) het opslaan van sleutels en de wijze waarop bevoegde gebruikers toegang tot sleutels krijgen;
- e) het wijzigen of uitsluiten van sleutels, met inbegrip van regels over wanneer en hoe sleutels behoren te worden gewijzigd;
- f) het omgaan met gecompromitteerde sleutels;
- g) het inrukken van sleutels, met inbegrip van hoe sleutels behoren te worden teruggetrokken of gedeactiveerd, bijv. als sleutels zijn gecompromiteerd of als een gebruiker die organisatie verlaat (in welk geval sleutels ook behoren te worden gedeactiveerd);
- h) het herstellen van sleutels die verloren of gecorumpieerd zijn;
- i) het back-uppen of archiveren van sleutels;
- j) het vernietigen van sleutels;

k) het registreren en auditen van aan sleutelbeheer gerelateerde activiteiten.

Om de kans op onjuist gebruik te verminderen behoren de activerings- en deactiveringsdatum van sleutels te worden vastgesteld zodat de sleutels alleen kunnen worden gebruikt tijdens de periode die in het desbetreffende sleutelbeheerbeleid is vastgesteld.

Naast het zorgvuldig beheren van gemeenschappelijke en persoonlijke sleutels behoort ook aandacht te worden besteed aan de authenticiteit van openbare sleutels. Deze authenticatieprocedure kan worden uitgevoerd met gebruikmaking van openbaresleutelcertificaten, die gewoonlijk worden uitgegeven door een certificeerende instantie, die een erkende organisatie behoort te zijn die beschikt over passende beheersmaatregelen of procedures om de vereiste mate van betrouwbaarheid te kunnen leveren.

De inhoud van dienstverleningsovereenkomsten of contracten met externe leveranciers van cryptografische diensten, bijv. met een certificeerende instantie, behoort aansprakelijkheid, betrouwbaarheid van dienstverlening en aansprakelijkheid voor dienstverlening te omvatten (zie ISO 15.2).

C.2.8.3 Voorschriften voor het gebruik van cryptografische beheersmaatregelen

Beheersmaatregel

Cryptografische beheersmaatregelen behoren te worden toegepast in overeenstemming met alle relevantie overeenkomsten, wet- en regelgeving (ISO 18.1.3).

Implementatierichtlijn

Voor de naleving van relevante overeenkomsten, wet- en regelgeving behoort met de volgende punten rekening te worden gehouden:

- beperkingen op de import of export van computerhardware en -software voor het uitvoeren van cryptografische functies;
- beperkingen op de import of export van computerhardware en -software die de uitvoering van cryptografische functies aan kunnen worden toegevoegd;
- beperkingen op de toepassing van codering;
- verplichting of beperking tot toegang voor nationale autoriteiten tot informatie die door hardware of software is versleuteld om in de vertrouwelijkheid van de inhoud te voorzien.

Om naleving van de relevante wet- en regelgeving te waarborgen behoort juridisch advies te worden ingewonnen. Ook voordat verscheidene informatie of cryptografische beheersmaatregelen over grenzen van rechtsgebieden worden versleuteld, behoort juridisch advies te worden ingewonnen.

C.2.9. "Clear desk" en "clear screen"

Beheersmaatregel

Er behoort een "clear desk"-beleid voor papieren documenten en verwijderbare opslagmedia en een "clear screen"-beleid voor informatieverwerkende faciliteiten te worden ingesteld. (ISO 11.2.9)

Implementatierichtlijn

Bij het "clear desk"- en "clear screen"-beleid behoort rekening te worden gehouden met de informatieclassificatie (zie ISO 0.2), wettelijke en contractuele eisen (zie ISO 19.1) en de tijdsgebonden risico's en de risico's voor de organisatie.

Met de volgende richtlijn behoort rekening te worden gehouden:

- gevoelige of essentiële bedrijfsinformatie, bijv. op papier of op elektronische opslagmedia, behoort in een afgebeelde vorm te worden bewaard (bestaat in een kluis, een lijst of een andere vorm van beveiligd meubilair), wanneer deze informatie niet verslet is, vooral als het verrek verlaten is;
- onbeheerde computers en terminals behoren uitgelogd of beschermd te zijn met een scherm- en toetsenbordverdeling met wachtwoord, tokens of vergelijkbare gebruikersauthenticatie; wanneer ze niet worden gebruikt behoren computers en terminals te worden beschermd voor toetsverdeling, wachtwoorden of andere beheersmaatregelen;

- c) ontveegd gebruik van fotokopieerapparaten en andere reproductieapparatuur (kijf, scanners, digitale camera's) behoort te worden voorkomen;
- d) media die gevoelige of vertrouwelijke informatie bevatten, behoren niet te worden afgedrukt of middellijk van printers te worden verwijderd.

C.2.10. Intellectuele-eigendomsrechten

Eeheimaatregel

Om de eelouwing van wettelijke, regelgevende en contractuele eisen in verband met intellectuele-eigendomsrechten en het gebruik van eigenzomssoftwareproducten te waarborgen behoren passende procedures te worden geïmplementeerd. (ISO 16.1.2)

Implementatierichtlijn

De volgende richtlijnen behoren in overweging te worden genomen om materiaal dat kan worden beschouwd als intellectueel eigendom te beschermen:

- a) een beleid te ontwerpen voor de afreiking van intellectuele-eigendomsrechten publiceren dat het wettig gebruik van software en informatieproducten definieert;
- b) software eisen verkrijgen bij bekende bedrijven met een goede reputatie, om te waarborgen dat het auteursrecht niet wordt geschonden;
- c) het bewustzijn in stand houden van het beleid voor de bescherming van intellectuele-eigendomsrechten en bekendheid geven aan het voornemen om discipline maatregelen te nemen tegen personeel dat deze rechten schendt;
- d) geschikte registers van bedrijfsmiddelen bijhouden, en alle bedrijfsmiddelen waarbij bescherming van intellectuele-eigendomsrechten vereist is identificeren;
- e) bewijs en bewijsmateriaal bijhouden van de eigendom van licenties, missieschrijven, handteekeningen enz.
- f) beheersmaatregelen implementeren om te bewerkstelligen dat een maximaal aantal gebruikers dat over leedl van de licentie is ingesloten niet wordt overschreden;
- g) beoelungen uitvoeren om te controleren dat alleen goedgekeurde software en licentie gegeven producten zijn geïmplementeerd;
- h) een beleid vaststellen voor het handhaven van de juiste licentievoorwaarden;
- i) een beleid vaststellen voor het verwijderen van of aan anderen overdragen van software;
- j) voorwaarden voor software en informatie verkrijgen van openbare netwerken;
- k) niet dualiseren, maar een ander voor maal converteren of een wilt enkel maken van commerciële opties (film, audio, tenz.) auteursrechtelijk toegestaan;
- l) geen boeken, artikelen, rapporten of andere documenten geheel of ten dele kopiëren, tenzij autorisatieflijk toegestaan.

C.2.11. Geheimhouding

Eeheimaatregel

Eisen voor vertrouwelijkheids- of geheimhoudingsvereenkomsten die de behoeften van de organisatie betreffende het beschermen van informatie weerspiegelen, behoren te worden vastgesteld, regelmatig te worden beoordeeld en gedocumenteerd. (ISO 13.2.4)

Implementatierichtlijn

Vertrouwelijkheids- of geheimhoudingsvereenkomsten behoren te eisen van bescherming van vertrouwelijke informatie te behouden binnen juridische afsluitende voorwaarden; Vertrouwelijkheids- of geheimhoudingsvereenkomsten zijn van toepassing op externe partijen of medewerkers van de organisatie. Rekening houdend met de aard van de andere partij en de aard toegestane toegang, of toelating van vertrouwelijke informatie behoren eisen te worden vastgesteld met betrekking tot de vertrouwelijkheid of vertrouwelijkheid.

Bij het vaststellen van eisen voor vertrouwelijkheids- of geheimhoudingsvereenkomsten, behoren de

volgende elementen in overweging te worden genomen:

- a) een definitie van de te beschermen informatie (bijv. vertrouwelijke informatie);
 - b) verwachte looptijd van een overeenkomst, met inbegrip van gevallen waarin de vertrouwelijkheid mogelijk onafhankelijk moet worden gehandhaafd;
 - c) variabele acties als een overeenkomst is beëindigd;
 - d) verantwoordelijkheden en acties van de ondertekenaars betreffende het verwijderen van onbevoegd openbaar maken van informatie;
 - e) eigendom van informatie, handelsgeheimen en intellectueel eigendom, en hoe dit zich verhoudt tot de bescherming van vertrouwelijke informatie;
 - f) het toegelaten gebruik van vertrouwelijke informatie en de rechten van de ondertekenaar om informatie te gebruiken;
 - g) het recht om activiteiten waar vertrouwelijke informatie bij betrokken is te auditen en te monitoren;
 - h) procedure voor het notifiëren en melden van ongewenste openbaarmaking of lekken van vertrouwelijke informatie;
 - i) voorwaarden voor teruggeven of vernietigen van informatie na beëindiging van de overeenkomst;
 - j) aanvullende acties die moeten worden ondernomen in geval van schending van de overeenkomst.
- Afhankelijk van de scope van de organisatie betreffende informatiebeveiliging behoren mogelijk nog andere elementen te worden opgenomen in een vertrouwelijkheids- of geheimhoudingsovereenkomst.
- Vertrouwelijkheids- en geheimhoudingsovereenkomsten behoren te voldoen aan alle toepasselijke wetten en regelgeving voor het rechtsgebied waar zij voor gelden (zie ISO 10.1).

Eisen voor vertrouwelijkheids- en geheimhoudingsovereenkomsten behoren te worden beoordeeld, en als zich veranderende voorwaarden die van invloed zijn op deze eisen.

C.2.12. Bedrijfscontinuïteit

C.2.12.1 Beleid voor bedrijfscontinuïteit

Beheersmaatregel

Erik tactisch beleid voor bedrijfscontinuïteit vastgesteld, gedocumenteerd en beheerbaar op basis van inzichten in risico's, ethische bedrijfsprocessen en toewijzing van prioriteiten.

Implementatierichtlijn

De implementatierichtlijnen staan beschreven in Doel C.

C.2.12.2 Informatiebeveiligingscontinuïteit

Doelstelling: Informatiebeveiligingscontinuïteit behoort te worden ingebod in de systemen van het bedrijfscontinuïteitsbehoor van de organisatie.

C.2.12.2.1 Informatiebeveiligingscontinuïteit plannen

Beheersmaatregel

De organisatie behoort haar eisen voor informatiebeveiliging en voor de continuïteit van het informatiebeveiligingsbehoor in ongunstige situaties, bijv. een crisis of een ramp, vast te stellen. (ISO 17.1.1)

Implementatierichtlijn

Een organisatie behoort vast te stellen of de continuïteit van de informatiebeveiliging onder het beheerproces van de bedrijfscontinuïteit valt of onder het beheerproces van rampenherstel. Informatiebeveiligingsgedeelten behoren te worden vastgesteld als de planning voor bedrijfscontinuïteit of rampenherstel wordt gemaakt.

Bij afwezigheid van een formele planning voor bedrijfscontinuïteit en rampenherstel behoort het

informatiebeveiligingsbeheer ervan uit te gaan dat informatiebeveiligingsleiden in ongunstige situaties hetzelfde blijven als in normale uitvoer (gevoelensmatigheid). In het andere geval kan een organisatie een herijfimpactanalyse uitvoeren voor informatiebeveiligingsaspecten om de informatiebeveiligingsleiden vast te stellen die van toepassing zijn op ongunstige situaties.

C.2.12.2.2 Informatiebeveiligingscontinuïteit implementeren

Beheersmaatregel

De organisatie behooft processen, procedures en beheersmaatregelen vast te stellen, te documenteren, te implementeren en te handhaven om het vereiste niveau van continuïteit voor informatiebeveiliging tijdens een ongunstige situatie te waarborgen. (ISO 171.7)

Implementatierichtlijn

Een organisatie behooft ervoor te zorgen dat:

- a) er een adequate beheersstructuur is die is voorbereid op een verstorende gebeurtenis, deze verzocht om erop reageert met personeel dat beschikt over de nodige autoriteit, ervaring en competentie;
- b) personeel voor incidentrespons wordt aangesteld dat beschikt over de nodige verantwoordelijkheid, autoriteit en competentie om een incident te af te handelen en de informatiebeveiliging te handhaven;
- c) op basis van door de directie goedgekeurde doelstellingen voor informatiebeveiligingscontinuïteit, gedocumenteerde plannen, respons- en herstelprocedures worden ontwikkeld en goedgekeurd, waarin gedetailleerd wordt omschreven hoe de organisatie een verstorende gebeurtenis zal aanpakken en haar informatiebeveiliging op een voornamelijk vastgesteld niveau zal handhaven (zie 17.1.1).

In overeenstemming met de boven voor informatiebeveiligingscontinuïteit behoort de organisatie het volgende vast te stellen, te documenteren, te implementeren en te onderhouden:

- a) beheersmaatregelen voor informatiebeveiliging binnen processen, procedures en ondersteunende systemen en instrumenten voor bedrijfscontinuïteit of rampenherstel;
- b) processen, procedures en implementatieveranderingen om bestaande beheersmaatregelen voor informatiebeveiliging tijdens een ongunstige situatie te handhaven;
- c) competentie beheersmaatregelen voor beheersmaatregelen voor informatiebeveiliging die tijdens een ongunstige situatie niet kunnen worden gehandhaafd.

C.2.12.2.3 Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren

Beheersmaatregel

De organisatie behooft de ten behoeve van informatiebeveiligingscontinuïteit vastgestelde en geïmplementeerde beheersmaatregelen regelmatig te verifiëren en te waarborgen dat ze doeltreffend en doelbaar zijn tijdens ongunstige situaties. (ISO 171.7)

Implementatierichtlijn

Veranderingen betreffende de organisatie, procedures, processen of van technische aard, hetzij in een context van uitvoering, hetzij van continuïteit, kunnen leiden tot veranderingen in de eisen betreffende informatiebeveiligingscontinuïteit. In dergelijke gevallen behoort de continuïteit van processen, procedures en beheersmaatregelen voor informatiebeveiliging te worden beoordeeld tegen de achtergrond van deze veranderingen.

Organisaties behoven de continuïteit van hun informatiebeveiligingsbeheer te verifiëren door:

- a) de functionaliteit van processen, procedures en beheersmaatregelen voor informatiebeveiligingscontinuïteit te controleren en te testen om te waarborgen dat ze consistent zijn met de doelstellingen van de informatiebeveiligingscontinuïteit;
- b) de kennis en vaardigheden van functionarissen van processen, procedures en beheersmaatregelen voor informatiebeveiligingscontinuïteit te controleren en te testen om te waarborgen dat de prestaties consistent zijn met de doelstellingen van de informatiebeveiligingscontinuïteit;

c) de **doelmatigheid** en **doeltreffendheid** van maatregelen voor informatieveiligheidscontinuïteit te beoordelen als informatiesystemen, informatiebeveiligingsprocedures, -procedures en -beheersmaatregelen, of de procedures en oplossingen van bedrijfscontinuïteitsbeheer of rampenherstelbeheer vereisen;

C.2.11.1.4 Beschikbaarheid van informatieverwerkende faciliteiten

Doelstelling: Beschikbaarheid van informatieverwerkende faciliteiten bewerkstelligen. (ISO 17.2)

Beheersmaatregel

Informatieverwerkende faciliteiten behoren met voldoende redundantie te worden gimp amentoord om een beschikbaarheidsdoel te voldoen. (ISO 17.2.1)

Implementatierichtlijn

Organisaties behoren de bedrijfsdoelen voor de beschikbaarheid van informatiesystemen vast te stellen. Als de beschikbaarheid niet kan worden gegarandeerd door middel van de bestaande systeemarchitectuur, behoren redundante componenten of architecturen in overweging te worden genomen.

Indien van toepassing behoren redundante informatiesystemen te worden getest om te waarborgen dat de automatische omschakeling van de ene op de andere component bij storing werkt zoals voorzien.

C.3. Tactisch beveiligingsbeheer

Doelstelling

Tactisch beveiligingsbeheer borgt op tactisch niveau het in samenhang doen treden van beveiligingsmaatregelen in de organisatie of het organisatiedeel in overeenstemming met de normen en behoeften op operationeel niveau de toegangsverlening tot en de overige beveiligingseigenschappen van voorzieningen voor IT en Fuisvesting.

Toelichting

Het beheren van informatiebeveiliging omvat het uitvoeren van de maatregelenverantwoordelijkheden op dit gebied, het afstemmen van de beveiligingsmaatregelen binnen de verschillende verantwoordelijkheidsgebieden, het inzetten van deskundig beveiligingsadvies en het controleren van de naleving van de beveiligingskaders (beleid en normen).

De begrippen (beleid), kader, advies, keuzen en Leiden in dit proces worden in zijn laatste uitsluitend context; het gaat hierbij om het beheren van het andere rekruteren van het management in de verschillende lagen van een organisatie. De activiteiten in dit ondersteunende proces zijn op de verschillende niveaus van de organisatie in principe hetzelfde, de mate van abstractie van de activiteiten verschilt, evenals het hoofdoel van de uitvoering van de verschillende fasen in het proces.

Motivering

Beveiliging is een lijn- en soms projectverantwoordelijkheid. Beveiligingsmaatregelen worden overal getroffen in de verschillende verantwoordelijkheidsgebieden (organisatie, processen en producten). Om te borgen dat deze beveiligingsmaatregelen een evenwichtig op elkaar afstemd geheel vormen, wordt aan het lijn- en projectmanagement ondersteuning verleend door beveiligingsdeskundigen. Het beveiligingsbeheer op tactisch niveau is voorwaartse reikend voor het aanpakbare kennis bereiken en handhaven van het gewenste beveiligingsniveau in een organisatie. Dit proces in combinatie met de organisatie van en communicatie tussen de verschillende beveiligingsbeheerders op tactisch niveau moet de totale samenhang van de maatregelen in een organisatie borgen.

Zonder kaderstelling, advisering, toelichting en evaluatie van getroffen maatregelen en kaders wordt het risico gelopen dat het geheel van de beveiligingsmaatregelen in en/of goed zijn afgestemd op de risico's in een organisatie.

C.3.1 Kwaliteit beveiligingsfuncties

Beheersmaatregel

Beveiligingsfuncties moeten aan eisen passend bij de beroepsuitoefening.

Implementatiecriteria

- Beveiligingsfuncties moeten aan het profiel van de beroepsuitoefening, aan eisen van opleiding en permanente educatie.
- Er worden in voldoende mate contacten onderhouden binnen de organisatie om tijdig betrokken te zijn bij de totstandkoming van beleidsstukken, architecturen en organisatieveranderingen met betrekking tot beveiliging.
- Er worden geschikte contacten met speciale belangengroepen of andere specialiseerde platformen voor beveiliging en professionele organisaties onderhouden, als middel om:
 - kennis te vergroten van bepaalde werkwijzen (best practices) en op de hoogte te blijven van de laatste stand van zaken op het gebied van beveiliging;
 - te waarborgen dat kennis en begrip van het vakgebied beveiliging volledig actueel en compleet zijn;
 - toegang te verkrijgen tot deskundig beveiligingsadvies;
 - informatie over nieuwe technologieën, producten, bedreigingen of kwetsbaarheden te delen en uit te wisselen.

C.3.2. Stelton kadere

Beheersmaatregel

Er worden kadere gesteld op het gebied van beveiliging als advies aan het management terzake richting te geven naar het treffen van beveiligingsmaatregelen in overeenstemming met wet- en regelgeving en standaards van het vakgebied.

Implementatierichtlijn

a) Afhankelijk van het niveau of verantwoordingsgebied waarvoor Toelichting Beveiligingsbehoefte functioneert, worden beveiligingsnormen, raaders, methoden, technieken, hulpmiddelen en voorschriften ontwikkeld, die

1. gebaseerd zijn op wet- en regelgeving en standaards in het vakgebied, rekeninghouding met het strategisch beveiligingsbeleid;
2. afgestemd zijn met relevante andere kadere binnen de organisatie en afspraken met klanten of ketenrelaties;
3. goedkeurd zijn door het management.

b) Voor gegevens die niet vallen onder het regiem van het VRI-BeI maar wel extra risico's met zich mee brengen, wordt op basis van een risicobehouds- en classificatie van (ex-ante) maatregelen opgesteld. Het kan om klantgegevens gaat anderszins gaan met een extra vertrouwelijk karakter.

c) Jaarlijk wordt er een draak het management goedkeurd beveiligingsplan opgesteld, waarin is vastgelegd welke verbeteracties er noodzakelijk zijn om aan de normen te voldoen. Dit plan is gebaseerd op wijzigingen in het draagrijger profiel, uitkomsten van de evaluatieproces, een analyse van verhoogde risico's en de te verwachten omkeeringen in de verschillende verantwoordelijkheidsgebieden (processen en producten).

C.3.3. Onderhouden beveiligings kadere

Beheersmaatregel

De beveiligingskadere worden bijgesteld op basis van controles, testen en evaluatie.

Implementatie richtlijn

a) Beveiligingskadere worden onderhouden op basis van

1. de uitkomsten van C.3.5. Evalueren beveiliging;
2. wijzigingen in organisatie, techniek en processen;
3. periodieke beoordeling van het beveiligingsbeleid;
4. het actuele draagrijger profiel

C.3.4. Advieseren beveiliging

Beheersmaatregel

Er worden deskundige adviezen gegeven om te bewerkstelligen dat het beveiligingsbeleid en de beveiligingsmaatregelen worden getroffen in overeenstemming met de kadere.

Implementatie richtlijn

a) Er worden afspraken gemaakt met het management of procesgeheeren op basis van welke criteria beveiligingscontroles moet worden ingevoerd, met name zijn wordt toegepast door het toetsing van beveiligingsmaatregelen plaatsvindt.

b) Er worden adviezen verstrekt aan toetsingen verricht aan de hand van beveiligingskadere na de belangrijke vernieuwingen en wijzigingen in processen en producten en er wordt toegezien op het daadwerkelijk treffen van beveiligingsmaatregelen.

c) De opleiding, training en bewustwording van beveiliging wordt bevorderd in alle lagen van de organisatie.

C.3.5. Evalueren beveiliging

Beheersmaatregel

De beveiligingsmaatregelen en normenkaders worden geëvalueerd.

Implementatierichtlijn

- De voortgang van het beveiligingsplan wordt geëvalueerd.
- Er wordt toezien op afspraken over de uitvoering van interne controles op de naleving van de kaders voor beveiliging.
- Er wordt toezien op het uitvoeren van controles op beveiligingsinstellingen van fysieke toegangsvoorzieningen en van IT-voorzieningen, die onderdeel uitmaken van de logische toegangsposities tot gegevens.
- De uitvoeren van interne en externe controlestudies met beveiligingsrelevante worden beoordeeld op hun effectiviteit voor de toepassing, het bestaan van de beveiligingsmaatregelen. Er wordt toezien op het tijdig, juist en volledig oplossen van bevindingen dan wel het verantwoord accepteren van risico's.
- Beveiligingsincidenten en actualiteiten geraden worden geëvalueerd.
- Er vindt regelmatig en gestructureerd overleg plaats tussen de verschillende beveiligingsdisciplines waarin kaderstelling, adviezen, evaluatie en onderhoud op het gebied van beveiliging aan de orde worden gesteld.

C.3.6. Informatiebeveiligingsbeoordelingen

Doelstelling: Verzeven dat informatiebeveiliging wordt geïmplementeerd en uitgevoerd in overeenstemming met de beleidsregels en procedures van de organisatie. (ISO 18.2)

C.3.6.1 Onafhankelijke beoordeling van informatiebeveiliging

Beheersmaatregel

De aanpak van de organisatie ten aanzien van het beheer van informatiebeveiliging en de implementatie ervan (bijv. beheersmaatregelen, beheersmaatregelen, beleidsregels, processen en procedures voor informatiebeveiliging), behoren onafhankelijk en met gezamenlijk tussenpozen of zodra zich belangrijke veranderingen voordoen te worden beoordeeld. (ISO 18.2.1)

Implementatierichtlijn

Deze onafhankelijke beoordeling behoort door de directie te worden geïnitieerd. Een dergelijke onafhankelijke beoordeling is nodig om te waarborgen dat de organisatie continue een geschikte, relevante en doeltreffende aanpak van het beheer van informatiebeveiliging hanteert. Deze beoordeling behoort (tevens het beoordelen van verbetermogelijkheid) er de noodzaak om wijzigingen aan te brengen in de beveiligingsaanpak te omvatten, met inbegrip van het beleid en de consensusstellingen.

Een dergelijke beoordeling behoort te worden uitgevoerd door personen met een onafhankelijke positie ten opzichte van het te beoordelen gebied, bijv. Jose de interne auditor, een onafhankelijke manager of een externe organisatie die gecertificeerd is in dergelijke beoordelingen. Personen die deze beoordelingen uitvoeren behoren te beschikken over passende vaardigheden en ervaring. De resultaten van de onafhankelijke beoordeling behoren te worden vastgelegd en te worden gerapporteerd aan de directie die de beoordeling heeft geïnitieerd. Deze verslagen behoren te worden leverbaar.

Indien in de onafhankelijke beoordeling wordt vastgesteld dat de aanpak en de implementatie van het beheer van informatiebeveiliging van de organisatie ontoereikend zijn, bijv. gedocumenteerde doelstellingen en essentie zijn niet gehaald of niet in overeenstemming met de keuzes voor informatiebeveiliging zoals opgenomen in de beleidsregels voor informatiebeveiliging (zie ISO 8.1.1), behoort de directie compenserende maatregelen te overwegen.

C.3.6.2 Naleving van beveiligingsbeleid en -normen

Beheersmaatregel

De directie behoort regelmatig de naleving van de informatieverwerking en -procedures binnen haar verantwoordelijkheidsgebied te beoordelen aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging. (ISO 18.2.2)

Implementatieplichtige

Managers behoren vast te stellen op welke manier wordt beoordeeld of is voldaan aan informatiebeveiligingseisen zoals gedefinieerd in beleidsregels, normen en andere toepasselijke regelgeving.

Voor een doeltreffende regelmatig beoordeeling behoort te worden overwogen om automatische meet- en rapportage-instrumenten in te zetten.

Indien de beoordeling een geval van niet-naleving oplevert, behoren managers:

- a) de oorzaken van de niet-naleving vast te stellen;
- b) de noodzaak te evalueeren tot het treffen van maatregelen om naleving te bewerkstelligen;
- c) passende corrigerende maatregelen te implementeren;
- d) de getroffen corrigerende maatregelen te beoordelen om de doeltreffendheid ervan te verifiëren en om gebreken of zwakke punten te identificeren.

Resultaten van door managers uitgevoerde beoordelingen en getroffen corrigerende maatregelen behoren te worden geregistreerd en deze resultaten behoren te worden bewaard. Managers behoren de resultaten te rapporteren aan de personen die operationele beveiligingen uitvoeren (zie ISO 18.2.1) wanneer een operationeel handreiking plaatsvindt binnen hun verantwoordelijkheidsgebied.

C.3.6.3 Beoordeling van technische naleving**Beheersmaatregel**

Informatiesystemen behoren regelmatig te worden beoordeeld op naleving van de beleidsregels en normen van de organisatie voor informatiebeveiliging. (ISO 18.2.3)

Implementatieplichtige

Technische naleving behoort bij voorkeur te worden beoordeeld met behulp van geautomatiseerde instrumenten die technische rapporten verzandigen, die vervolgens door een technisch specialist worden geïnterpreteerd. Als alternatief kunnen handmatige beoordelingen (indien nodig ondersteund door passende software-instrumenten) door een ervaren systeemtechnicus worden uitgevoerd.

Indien penetratietests of kwetsbaarheidsbeoordelingen worden toegepast is voorzichtigheid geboden omdat dergelijke activiteiten de beveiliging van het systeem kunnen compromitteren. Dergelijke tests behoren te worden gepland en gedocumenteerd en behoren herhaalbaar te zijn.

Beoordeling van technische naleving behoort uitsluitend te worden uitgevoerd door competente, bevoegde personen of onder toezicht van dergelijke personen.

C.3.6.4 Beheersmaatregelen voor audits op de technische infrastructuur**Beheersmaatregel**

Audits van en -activiteiten die verificatie van uitvoeringssystemen met zich meebringen, behoren regelmatig te worden gepland en afgeleid om bedrijfsprocessen zo min mogelijk te verstoren. (ISO 18.2.1)

Implementatieplichtige

De volgende richtlijnen behoren in acht te worden genomen:

- a) audits van voor toegang tot systemen en gegevens behoren met de juiste manager te worden overeengekomen;
- b) het toepassingsgebied van technische audits behoren te worden afgesproken en te worden gecontroleerd;
- c) audits behoren te worden beperkt tot alleen-lezen-toegang tot software en gegevens;

- c) toegang anders dan 'alleen lezen' behoort alleen te worden toegestaan voor gelijkeende kopieën van systeembestanden, die behoren te worden verwijderd als de audit is uitgevoerd, of ze behoren te worden beschermd indien het vereist is deze bestanden bij de vereiste auditdocumenten te bewaren;
- e) alleen voor speciale of extra verwerkingsactiviteiten behoren te worden vastgesteld en overeengekomen;
- f) audits die de beschikbaarheid van systemen kunnen beïnvloeden, behoren buiten weruren plaats te vinden;
- g) alle toegangshandelingen behoren te worden gemonitord en vastgelegd in een logbestand om een referentiebron te produceren.

C.4. Personele voligheid

C.4.1. Voorafgaand aan het dienstverband

Doelstelling: Waarborgen dat medewerkers en contractanten hun verantwoordelijkheden begrijpen en geschikt zijn voor de rollen waarvoor zij in aanmerking komen. (ISO 7.1)

C.4.1.1 Screening

Beheersmaatregel

Verificatie van de achtergrond van alle kandidaten voor een dienstverband behoort te worden uitgevoerd in overeenstemming met relevante wet- en regelgeving en ethische overwegingen en behoort in verhouding te staan tot de risico's, de classificatie van de informatie waartoe toegang wordt verleend en de vastgestelde risico's te zijn. (ISO 7.1.1)

Implementatierichtlijn

Verificatie behoort rekening te houden met alle relevante wetgeving op het gebied van privacy, beperking van persoonsgegevens en arbeidswetgeving, en behoort indien toegelaten, het volgende te omvatten:

- beschikbaarheid van positieve referenties, bijv. één zakelijk en één persoonlijk;
- een verificatie (op volledigheid en nauwkeurigheid) van het curriculum vitae van de sollicitant;
- bevestiging van de geclaimde academische en beroepskwalificaties;
- nuutbarelijke verificatie van de identiteit (rapport of gelijkwaardig document);
- meer gedetailleerde verificatie, zoals controle op kredietwaardigheid of strafblad.

Als een persoon wordt ingehuurd voor een specifieke informatiebeveiligingsrol, behoort de organisatie zich ervan te vergewissen dat:

- de kandidaat over de nodige competentie beschikt om de beveiligingsrol te vervullen;
- de kandidaat de rol kan worden toevertrouwd, in het bijzonder als de rol cruciaal is voor de organisatie.

Als een functie, hetzij bij een eerste aanstelling, hetzij bij promotie, met zich mee brengt dat de persoon toegang heeft tot faciliteiten die informatie verwerken, en, in het bijzonder, indien het hierbij gaat om vertrouwelijke informatie, bijv. financiële informatie of zeer vertrouwelijke informatie, behoort de organisatie ook verder, meer gedetailleerde verificaties te overwegen.

Procedures behoren criteria en beperkingen voor controleonderzoeken te definiëren, bijv. wie is competent om personen te screenen, en hoe, wanneer en waarom worden controlesonderzoeken uitgevoerd.

Ook voor contractanten behoort voor een screeningprocedure te worden gezorgd. In die gevallen behoort de overzaker kennis te geven de organisatie en de contractant de verantwoordelijkheden voor het uitvoeren van de screening te vermelden en de informatieprocedures die moeten worden gevolgd als de screening niet is afgevaardigd of als de resultaten aanleiding geven tot twijfel of bezorgdheid.

Informatie over alle kandidaten die in aanmerking komen voor posities binnen de organisatie behoort te worden verzameld en verwerkt in overeenstemming met de relevante wetgeving aanwezig in het minimum rechtsgebied. Afhankelijk van de toepasselijke wetgeving behoren kandidaten vooraf over de screeningsactiviteiten te worden geïnformeerd.

C.4.1.2 Arbeidsvoorwaarden

Beheersmaatregel

De contractuele overeenkomst met medewerkers en contractanten behoort hun verantwoordelijkheden voor informatiebeveiliging en die van de organisatie te vermelden. (ISO 7.1.2)

Implementatierichtlijn

De contractuele verplichtingen voor medewerkers of contractanten betreffen de beleidsregels van de organisatie voor informatiebeveiliging waar te gooien, en tevens duidelijk te maken en te vermelden:

- a) de alle medewerkers en contractanten aan wie toegang wordt verleend tot vertrouwelijke informatie een vertrouwelijke (de- of geheimhoudings)vereenkomst behoren te ondertekenen voordat hun toegang wordt verleend tot informatie overwerkende faciliteiten (zie ISO 13.2.4);
- b) de wettelijke verantwoordelijkheden en rechten van de medewerker of contractant, bijv. betreffende auteursrechtbeveiliging of wetgeving inzake gegevensbescherming (zie ISO 18.1.2 en ISO 18.1.4);
- c) verantwoordelijkheden voor de classificatie van informatie en het beheer van bedrijfsmiddelen van de organisatie die samenhangen met informatie, informatieverwerkende faciliteiten en informatiebronnen die door de medewerker of contractant worden gebruikt (zie hoofdstuk ISO 3);
- d) verantwoordelijkheden van de medewerker of contractant voor het verspreken van informatie die is ontvangen van andere bedrijven of externe partijen;
- e) actie die moet worden ondernomen indien de medewerker of contractant de beveiligingselen van de organisatie vernachzact (zie ISO 7.2.5).

De informatiebeveiligingsreken op de verantwoordelijkheden behoren zijden het voorbeot van het aanstellingsproces aan de kandidaat te worden gecommuniceerd.

De organisatie behoot ervoor te zorgen dat medewerkers en contractanten instamen met voorwaarden betreffende informatiebeveiliging die passen bij de aard en de maat van toegang die ze zullen krijgen tot de bedrijfsmiddelen van de organisatie die samenhangen met informatiesystemen en -diensten.

Vaar van toepassing behoren de verantwoordelijkheden die in de arbeidsvoorwaarden staan voor een vastgestelde periode na het einde van het dienstverband van kracht te blijven (zie ISO 7.5).

C.4.2. Tijdens het dienstverband

Doelstelling: Ervoor zorgen dat medewerkers en contractanten zich bewust zijn van hun verantwoordelijkheden op het gebied van informatiebeveiliging en deze nalemen. (SC 7.2)

C.4.2.1 Directie verantwoordelijkheden

Beheersmaatregel

De directie behoren van alle medewerkers en contractanten te eisen dat ze informatiebeveiliging toepassen in overeenstemming met de vastgestelde beleidsregels en procedures van de organisatie (ISO 7.2.1).

Implementatierichtlijn

De directie behoren ervoor te zorgen dat medewerkers en contractanten:

- a) op de juiste manier worden geïnsteueerd over hun informatiebeveiligingsrol en – verantwoordelijkheden voordat zij toegang krijgen tot vertrouwelijke informatie of informatiesystemen;
 - b) richtlijnen ontvangen die de verwachtingen met betrekking tot hun informatiebeveiligingsrol binnen de organisatie aangeven;
 - c) gemetveerd zijn om te voldoen aan de beleidsregels met betrekking tot informatiebeveiliging van de organisatie;
 - d) een niveau van bewustzijn over informatiebeveiliging bereiken dat relevant is voor hun rollen en verantwoordelijkheden binnen de organisatie (zie ISO 7.2.2);
 - e) zich conformeren aan de arbeidsvoorwaarden, die het informatiebeveiligingsbeleid en passende werkmethoden omvatten;
 - f) contentu beschikken over de juiste vaardigheden en kwalificaties en regelmatig worden bijgeschoold;
 - g) via een aanrnfom kannd behoudingen van de beleidsregels of procedures met betrekking tot informatiebeveiliging kunnen melden (klikknijder).
- De directie behoot te laten zien dat ze de beleidsregels, procedures en beheersmaatregelen met betrekking tot informatiebeveiliging ondersteunt, en als rolmodel te handelen.

C.4.2.2 Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging

Beheersmaatregel

Alle medewerkers van de organisatie en, voor zover relevant, contractanten behoren een passende bewustzijnsopleiding en -training te krijgen en regelmatig bijbehoudig van beleidregels en procedures van de organisatie, voor zover relevant voor hun functie. (ISO 7.2.2)

Implementatierichtlijn

Een bewustzijnsprogramma met betrekking tot informatiebeveiliging behoort erop gericht te zijn om medewerkers en, indien relevant contractanten, bewust te maken van hun verantwoordelijkheden voor informatiebeveiliging en de manieren waarop men zich aan deze verantwoordelijkheden kan kwijten.

Een bewustzijnsprogramma met betrekking tot informatiebeveiliging behoort te worden vastgesteld in overeenstemming met de beleidsregels en relevante procedures inzake informatiebeveiliging van de organisatie, rekening houdend met de informatie van de organisatie die moet worden beschermd en de beleidsregels die zijn geïmplementeerd om de informatie te beschermen. Het bewustzijnsprogramma behoort een aantal bewustwordingsactiviteiten te bevatten, zoals campagne(s) (bijv. een 'informatiebeveiligingsdag') en het verspreiden van boekjes of nieuwsbrieven.

Eig de oorzak van het bewustzijnsprogramma behoort rekening te worden gehouden met de rollen van de medewerkers in de organisatie en, indien relevant, de verwachtingen van de organisatie met betrekking tot de bewustwording van contractanten. De activiteiten in het bewustwordingsprogramma behoren op zijn minst te worden gespreid en bij voorkeur regelmatig te worden uitgevoerd. Het de activiteiten worden herhaald en nieuwe medewerkers en contractanten deze ook mee maken. Het bewustwordingsprogramma behoort ook regelmatig te worden geactualiseerd, zodat het in overeenstemming blijft met de beleidsregels en procedures van de organisatie, en er behoort te worden voortgebouwd op de lessen die zijn geleerd uit informatiebeveiligingsincidenten.

Beleidsregels en procedures met betrekking tot informatiebeveiliging worden verspreid door het bewustzijnsprogramma. Inzake informatiebeveiliging van de organisatie. Deze bewustzijnsopleiding kan op verschillende manieren worden gegeven, bijv. klassikaal, via afstandsonderwijs, via internet, in eigen tempo.

Opleiding en training met betrekking tot informatiebeveiliging behoren ook algemene aspecten te omvatten zoals:

- a) het aanroepen van de betrokkenheid van de directie bij informatiebeveiliging in de gehele organisatie;
- b) de noodzaak om bekend te worden met en te voldoen aan de van toepassing zijnde regels en verplichtingen met betrekking tot informatiebeveiliging zoals gedefinieerd in beleidsregels, normen, wetten, regelgeving, contracten en overeenkomsten;
- c) persoonlijke verantwoordelijkheid voor eigen doen en laten, en algemene verantwoordelijkheid ten opzichte van het beveiligen of beschermen van informatie die eigendom is van de organisatie (of externe partijen);
- d) basisprocedures inzake informatiebeveiliging (zoals het melden van informatiebeveiligingsincidenten) en basisbeheersmaatregelen (zoals wachtwoordbeveiliging, netwerkcontroles en opgeruimde bureaus);
- e) contactpunten en bronnen voor aanvullende informatie en advies over informatiebeveiligingsregels en procedures, met inbegrip van een vastgesteld 'wettelijk'- en trainingsmaterieel met betrekking tot informatiebeveiliging.

Opleiding en training voor informatiebeveiliging behoort periodiek plaats te vinden. De basisopleiding en -training geldt voor personen die worden overgeplaatst naar nieuwe functies of rollen met substantieel verschillende eisen ten aanzien van informatiebeveiliging. Het advies voor nieuwe starters, en behoort plaats te vinden voordat de rol actief wordt.

De organisatie behoort het opleidings- en trainingsprogramma te ontwikkelen om de opleiding en training doeltreffend uit te kunnen voeren. Het programma behoort in overeenstemming te zijn met de beleidsregels en relevante procedures inzake informatiebeveiliging van de organisatie, rekening houdend met de informatie van de organisatie die moet worden beschermd en de beleidsmaatregelen die zijn geïmplementeerd om de informatie te beschermen. Het programma behoort verschillende vormen van opleiding en training te bevatten, bijv. lezingen of zelfstudie.

C.1.2.3 Disciplinaire procedure

Beheersmaatregel

Er behoort een formele en gecommuniceerde disciplinaire procedure te zijn om actie te ondernemen tegen medewerkers die een inbreuk hebben gepleegd op de informatiebeveiliging. (ISO 7.2.3)

Implementatierichtlijn

De disciplinaire procedure behoort niet te worden gestart voordat is gevestigd dat een inbreuk op de informatiebeveiliging heeft plaatsgevonden. (zie ISO 16.1.7).

De formele disciplinaire procedure behoort te waarborgen dat medewerkers die worden verdacht van een inbreuk op de informatiebeveiliging terecht en eerlijk worden behandeld. De formele disciplinaire procedure behoort te voorzien in een geadviseerd antwoord dat rekening houdt met factoren zoals de aard en ernst van de inbreuk en de impact ervan op de bedrijfsvoering, of dit een eerste of herhaalde overtreding is, of de overtreding al dan niet juist getraind was, relevante wetgeving, zakelijke contracten en, indien vereist, andere factoren.

De disciplinaire procedure behoort ook te worden gebruikt als een afschrikmiddel om te voorkomen dat medewerkers de beleidsregels en procedures niet betrekking tot informatiebeveiliging overtreden en om eventuele andere inbreuken op de informatiebeveiliging te voorkomen. Bij epzezzelijke inbreuken van onmiddellijke actie vereist zijn.

C.4.3. Beëindiging en wijziging van dienstverband

Uitstelling: Het beschermen van de belangen van de organisatie als onderdeel van de wijzigings- of beëindigingsprocedures van het dienstverband. (ISO 7.3)

C.4.3.1 Beëindiging of wijziging van verantwoordelijkheden van het dienstverband

Beheersmaatregel

Verantwoordelijkheid, en taken met betrekking tot informatiebeveiliging die van kracht blijven na beëindiging of wijziging van het dienstverband behoren te worden gedefinieerd, gecommuniceerd aan de medewerker of contractant, en ten uitvoer gebracht. (ISO 7.3.1)

Implementatierichtlijn

Tot het communiceren van verantwoordelijkheden na beëindiging van het dienstverband behoren voortdurende eisen en wettelijke verantwoordelijkheden met betrekking tot informatiebeveiliging en, waar van toepassing, verantwoordelijkheden die zijn opgenomen in vertouwelijkheidsvoorwaarden (zie ISO 13.2.4) en de arbeidsvoorwaarden (zie ISO 7.1.2) die goederen en goederenloze perioden na beëindiging van het dienstverband van de medewerker of contractant van kracht blijven.

Verantwoordelijkheid en plichter die van kracht blijven na beëindiging van het dienstverband behoren te worden opgenomen in de arbeidsvoorwaarden van de medewerker of contractant. (zie ISO 7.1.2)

Wijziging in verantwoordelijkheid of dienstverband behoren te worden gemiddeld als het beëindigen van de desbetreffende verantwoordelijkheid of het desbetreffende dienstverband behoort te worden gecombineerd met het initiëren van de nieuwe verantwoordelijkheid of het nieuwe dienstverband.

C.4.4. Kritische en risicovolle functies

Beheersmaatregel

Er is een strategie ontwikkeld en geïmplementeerd om blijvend over specialistische kennis en vaardigheden van werknemers en ingehuud personeel te kunnen beschikken, die kritische bedrijfsactiviteiten uitvoeren en aanvullende maatregelen te treffen voor risicovolle functies.

Toelichting

Bij kritische en risicovolle functies gaat het er om te borgen dat er geen ongewenst of frauduleus gebruik van de bevoegdheden wordt gemaakt en tevens dat de bedrijfscontinuïteit gehandhaafd blijft.

Implementatierichtlijn

- a) Er is vastgesteld wel kritische en relatieve functies zijn.
- b) Aan medewerkers is verbaard gemaakt dat zij een kritische en/of risicovolle functie vervullen.
- c) Er is een strategie vastgesteld om bijeen over voldoende voldoende en huidige werkmensen en ingehuurd personeel te kunnen beschikken voor zover het kritische functies betreft. Deze strategie is gebaseerd op een analyse van de voorgede uitgangspunten/overwegingen:
1. documentatie van de wijze waarop kritische bedrijfsactiviteiten worden uitgevoerd;
 2. vaardigheidstraining en opleiding;
 3. schieding van basiskaarigheden om het risico te spreiden;
 4. mogelijkheden om derde partijen in te schakelen;
 5. planning van de opvolging;
 6. kennisbehoef en -behoor.
- d) Van medewerkers die kritische functies vervullen, worden opleiding, vaardigheden en ervaring geregistreerd.
- e) Er is een strategie vastgesteld om eenigzinnig gebruik van risicogevolge bevoegdheden te voorkomen. Deze strategie is gebaseerd op een analyse van de voorgede uitgangspunten en overwegingen:
1. functionariele of relatie van kantens/verantworsers/contacten;
 2. sociale controle, werkes in teams;
 3. wettelijke;
 4. extra interne controle.

C.5. Fysieke beveiliging en beveiliging van de omgeving

C.5.1 Beveiligde gebieden

Doelstelling: Ontbrekende fysieke toegang tot, schade aan en interferentie met informatie en informatieverwerkende faciliteiten van de organisatie voorkomen. (ISO 11.1)

C.5.1.1 Fysieke beveiligingszones

Beheersmaatregel

Beveiligingszones behoren te worden gedefinieerd en gebruikt om gebieden te beschermen die gevulde of essentiële informatie of informatieverwerkende faciliteiten bevatten. (ISO 11.1.1)

Implementatierichtlijn

Voor zover van toepassing behoren de volgende richtlijnen voor fysieke beveiligingszones te worden overwogen:

- Beveiligingszones behoren te worden gedefinieerd, en de locatie en strekking van elke zone behoren af te hängen van de beveiligingsdoelen van de bedrijfsmiddelen die zich binnen de zone bevinden en van de resultaten van een risicoevaluering;
- De begrenzing van een gebouw of locatie waarin zich informatieverwerkende faciliteiten bevinden, behoort fysiek te zijn (i.e.w.z. er behoren geen openingen in de begrenzing te zijn) en er behoren geen manieren te zijn waar potentiële kwaadwilligen (inbrekers) het dak, de muren en vloer van de locatie behoren aan te raken of alle buitendeuren behoren passende tegen onbevoegde toegang te zijn beschermd met controlemechanismen (d.w.z. afsluitbomen, alarmsystemen, sloten); deuren en ramen behoren afgesloten te zijn als er niemand aanwezig is, en voor ramen, is het bijvoorbeeld de of de tegengestelde behoor externe bescherming te worden overwogen;
- Er behoort een normale routine of andere werkwijze ter controle van de fysieke toegang tot de locatie of het gebouw aanwezig te zijn; toegang tot locaties en gebouwen behoort te worden beperkt tot bevoegd personeel;
- Er behoren, indien van toepassing, fysieke hindernissen te worden aangebracht om onbevoegde fysieke toegang en vernieling van de omgeving te voorkomen;
- Alle branddeuren in een beveiligde zone behoren te worden voor- en van slag, te worden gemonteerd en getest in conformiteit met de normen en het vereiste niveau van brandweerschiktheid in overeenstemming met passende regionale, nationale en internationale normen vast te stellen; de werking van de deuren behoort, in overeenstemming met de plaatselijke brandcode, faalveilig te zijn;
- Iegen indringers behoren op alle buitendeuren en toegankelijke ramen passende detectiesystemen in overeenstemming met nationale, regionale of internationale normen te worden geïnstalleerd en regelmatig getest; er moeten ramen behoren te allen tijde te zijn voorzien van een alarmsysteem, ook andere sensor, bijv. de computer- of communicatiesamen, behoren te worden beschermd door het alarmsysteem;
- Informatieverwerkende faciliteiten die worden behandeld door een organisatie behoren fysiek te zijn gescheiden van informatieverwerkende faciliteiten die door externe partijen worden behandeld.

C.5.1.2 Fysieke toegangsbeveiliging

Beheersmaatregel

Beveiligde gebieden behoren te worden beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt. (ISO 11.1.2)

Implementatierichtlijn

Met de volgende richtlijnen behoort rekening te worden gehouden:

- datum en tijdstip van binnenkomst en vertrek van bezoekers behoort te worden geregistreerd, en op alle bezoekers behoort toezicht te worden gehouden (and) hun toegang vooraf te goedkeuren; personen behoort afvoer toegang te worden verleend voor specifieke, goedgkeunde doelen, en zij

betonen instructies over de beveiligingsplan van het gebied en de noodprocedures te ontvangen. De identiteit van bezoekers behoort met passende middelen te worden vastgesteld;

b) toegang tot gebieden waar vertrouwelijke informatie wordt verwerkt of opgeslagen behoort te worden beperkt tot het noodzakelijke personeel door passende toegang/beveiligingsmaatregelen te implementeren, bijv. door het te implementeren van een dubbel authenticatiemechanisme zoals een toegangskaart en een globale pincode;

c) van elke toegang behoort een fysiek logboek of een elektronisch audittrail te worden onderhouden te gemonitord;

d) van alle medewerkers, contractanten en externe partijen behoort te worden verlangd dat zij een bepaalde vorm van zichtbare identificatie dragen en zij behoren onmiddellijk beveiligingspersoneel te informeren als zij bezoekers zonder begeleiding en personen die geen zichtbare identificatie dragen, tegenkomen;

e) personeel van externe partijen die ondersteunende diensten verlenen, behoort alleen indien noodzakelijk beperkte toegang tot beveiligde gebieden of faciliteiten die vertrouwelijke informatie verwerken te worden verleend; deze toegang behoort te worden goedgekeurd en gemonitord;

f) toegangsrechten voor beveiligde gebieden behoren regelmatig te worden beoordeeld, geactualiseerd en indien nodig te worden ingetrokken (zie 9.2.5 en 9.2.6).

C.5.1.3 Kantoren, ruimten en faciliteiten beveiligen

Beheersmaatregel

Voor kantoren, ruimten en faciliteiten behoort fysieke beveiliging te worden ontworpen en toegepast. (ISO 11.1.3)

Implementatierichtlijn

Bij het beveiligen van kantoren, ruimten en faciliteiten behoren de volgende richtlijnen in aanmerking te worden genomen:

a) belangrijke faciliteiten behoren zo te worden gesitueerd dat ze niet voor iedereen toegankelijk zijn;

b) indien van toepassing behoren gebouwen inbegrijpend te zijn en zo min mogelijk aanwijzingen te geven over het gebruikte adres, zonder daarbij tekenen, borden of tekenen het gebouw, die op de aanwezigheid van informatieverwerkende activiteiten duiden;

c) faciliteiten behoren zo te zijn geconfigureerd dat wordt voorkomen dat vertrouwelijke informatie of activiteiten van buitenaf zichtbaar of hoorbaar zijn. Voor zover van toepassing behoort elektromagnetische afscherming ook te worden overwogen;

d) adresborden en interne tekenborden waarin locaties worden aangegeven met faciliteiten die vertrouwelijke informatie verwerken, behoren niet vrij toegankelijk te zijn voor onbevoegden.

C.5.1.4 Bescherming tegen bedreigingen van buitenaf

Beheersmaatregel

Tegen natuurschommelingen, tweedevluggige aanvallen of ongelukken behoort fysieke bescherming te worden ontworpen en toegepast. (ISO 11.1.4)

Implementatierichtlijn

Over het vermijden van schade door brand, overstroming, aardbeving, explosie, opvoer en andere vormen van natuurschommelingen of door persoonlijke veroorzaken na open behoefte aan specifiek advies te worden ingewonnen.

C.5.1.5 Werken in beveiligde gebieden

Beheersmaatregel

Voor het werken in beveiligde gebieden behoren procedures te worden ontwikkeld en toegepast. (ISO 11.1.5)

Implementatierichtlijn

Met de volgende richtlijnen behoort rekening te worden gehouden:

- a) personeel behoort alleen op grond van 'lead-to-know' bekend te zijn met het bestaan van of de activiteit in een beveiligd gebied;
- b) zonder toezicht werken in beveiligde gebieden behoort te worden vermeden, zowel om veiligheidsredenen als om geen gelegenheid te bieden voor inwaaierdige activiteiten;
- c) toegankende beveiligde ruimten behoren fysiek te worden afgesloten en periodiek te worden geïnspecteerd
- d) foto-, video-, audio- of andere opnameapparatuur, zoals camera's, in mobiele apparatuur, behoort te zijn goedgekeurd, niet te worden toegestaan.

De afpakken voor het werken in beveiligde zones bevatten beheersmaatregelen voor de medewerkers en voor externe bezoekers die in de beveiligde zone werken en toegang alle activiteiten die in de beveiligde zone plaatsvinden.

C.5.1.6 Leed- en Isolatie

Beheersmaatregel

toegangspunten zoals leed- en isolaties en andere punten waar onbevoegde personen het terrein kunnen betreden, behoren te worden beheerd, en zo mogelijk te worden afgeschermd van informatieverwerkende faciliteiten om onbevoegde toegang te vermijden. (ISO 11.1.6)

Implementatierichtlijn

Met de volgende richtlijnen behoort rekening te worden gehouden:

- a) toegang tot een leed- en isolatie van buiten het gebouw behoort te worden beperkt tot geïdentificeerd en bevoegd personeel;
- b) de leed- en isolatie behoort zo te zijn ontworpen dat goederen kunnen worden geladen en gelost zonder dat de overgang toegang heeft tot andere delen van het gebouw;
- c) de buitenruimte van een leed- en isolatie behoort beveiligd te zijn als de binnenruimte open zijn;
- d) inkomende materialen behoren te worden gecontroleerd en onderzocht op explosieven, chemische of andere gevaarlijke materialen voordat ze vanaf een leed- en isolatie worden overgebracht;
- e) inkomende materialen behoren bij binnenkomst op de locatie te worden geïnspecteerd in overeenstemming met de procedures voor beoefening van de beveiliging (zie hoofdstuk ISO 8);
- f) inkomende en uitgaande zendingen behoren, voor zover mogelijk, fysiek te worden gescheiden;
- g) inkomende materialen behoren te worden gecontroleerd op mogelijke aanwijzingen van vervalsing tijdens het transport. Indien vervalsing wordt ontdekt behoort dit direct aan beveiligingspersoneel te worden gemeld.

C.5.2 Apparatuur

Doelstelling: Verlies, schade, diefstal of compromittering van beoefening van de beveiliging van de bedrijfsvoering van de organisatie voorkomen. (ISO 11.2)

C.5.2.1 Plaatsing en bescherming van apparatuur

Beheersmaatregel

Apparatuur behoort zo te worden geplaatst en beschermd dat risico's van bederflijgen en gevaren van brandst, alsook de kans op onbevoegde toegang worden verkleind. (ISO 11.2.1)

Implementatierichtlijn

Om apparatuur te beschermen behoren de volgende richtlijnen in overweging te worden genomen

- a) apparatuur behoort zo te worden geplaatst dat onnodige toegang tot de werkvloer zo veel mogelijk wordt beperkt.

- b) informatieverwerkende faciliteiten die gevoelige gegevens behandelen, moeten zorgvuldig te worden geplaatst om het risico te verminderen dat informatie tijdens verwerking door onbevoegde personen wordt ingezien;
- c) opstapelaars behoren te worden beveiligd om onbevoegde toegang te voorkomen;
- d) onderdelen die speciale bescherming nodig hebben, behoren te worden beveiligd zodat het algemene beschermingsniveau dat vereist is, kan worden verlaagd;
- e) beheersmaatregelen behoren te worden aangehouden om het risico van potentiële fysieke bedreigingen en bedreigingen van buitenaf, bijv. diefstal, brand, explosie, rijk, wateroverstoot of uitval van watervoorziening, stof, billig, ultraviolette straling, schaling, in de vorm van de aanwezigheid of in communicatievoorzieningen, elektromagnetische straling en vandalisme, zo laag mogelijk te houden;
- f) voor stek, draden en kabels in de nabijheid van informatieverwerkende faciliteiten behoren richtlijnen te worden vastgesteld;
- g) omgevingsomstandigheden zoals temperatuur en vochtigheid behoren te worden gecontroleerd en gecontroleerd op omstandigheden die de werking van informatieverwerkende faciliteiten negatief kunnen beïnvloeden;
- h) bij alle gebouwen behoort blikseminbeveiliging te worden toegepast en op alle inkomende stroom- en communicatielijnen behoren blikseminbeveiligingsfilters te worden geïnstalleerd;
- i) voor apparatuur in industriële omgevingen behoort de toepassing van speciale beschermingsmiddelen zoals teetschermfolie te worden overwogen;
- j) apparatuur die vertrouwelijke informatie verwerkt, behoort te worden beschermd om het risico van weglekken van informatie door elektromagnetische emissie zo laag mogelijk te houden.

C.5.2.2 Nutsvoorzieningen

Beheersmaatregel

Apparatuur behoort te worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door vertragingen in nutsvoorzieningen. (ISO 11.2.2)

Implementatieplichtige

Nutsvoorzieningen (bijv. elektriciteit, telecommunicatie, watervoorziening, gas, rooien, ventilatie en airconditioning) behoren:

- a) in overeenstemming te zijn met de technische beschrijving van de fabrikant en de lokale wetelijke eisen;
- b) regelmatig te worden onderzocht om te beoordelen of hun capaciteit overeenkomstig is voor de grootte van het bedrijf en de interactie met andere nutsvoorzieningen;
- c) regelmatig te worden geïnspecteerd en getest om te waarborgen dat ze correct functioneren;
- d) zo nodig, te worden voorzien van een alarmsysteem om disfuncties op te sporen;
- e) voor zover nodig, te beschikken over eenvoudige toegang tot een verschillenbare fysieke ruimte. noodverlichting en communicatiemiddelen behoren aanwezig te zijn. nabij nooduitgangen of ruimten waar apparatuur aanwezig is, behoren nooddekkalans en knoppen te zijn waarmee stroom, water, gas of andere voorzieningen kunnen worden uitgeschakeld.

C.5.2.3 Beveiliging van bekabeling

Beheersmaatregel

Voedings- en telecommunicatiekabels voor het versturen van gegevens of die informatiebronnen ondersteunen, behoren te worden beschermd tegen interceptie, verstoring of schade. (ISO 11.2.3)

Implementatieplichtige

Met de volgende richtlijnen voor beveiliging van bekabeling behoort rekening te worden gehouden:

a) voeding- en telecommunicatieleidingen naar informatieverwerkende faciliteiten behoren, zo mogelijk, ondergronds te lopen, of er behoort adequate alternatieven bescherming te zijn.

b) voedingkabels behoren gescheiden te zijn van communicatiekabels om interferentie te voorkomen:

c) voor gevoelige essentiële systemen kunnen de volgende aanvullende beheersmaatregelen worden vastgesteld:

- 1) het installeren van gewapende kabelgoten en afgesloten kokers of dozen bij inspectie- en afsluipruiten;
- 2) het gebruik van elektromagnetische afscherming ter bescherming van de kabels;
- 3) het installeren van technische scheurmaatbeurten en fysieke controles op aansluiting van niet-goedgekeurde apparaten op de kabels;
- 4) beveiligde toegang tot schakelpanden en kabelruimten.

C.5.2.4 Onderhoud van apparatuur

Beheersmaatregel

Apparatuur behoort correct te worden onderhouden om de continue beschikbaarheid en integriteit ervan te waarborgen. (ISO 11.2.4)

Implementatierichtlijn

Met de volgende richtlijnen voor onderhoud van apparatuur behoort rekening te worden gehouden:

- a) apparatuur behoort te worden onderhouden in overeenstemming met de door de leverancier aanbevolen intervalen voor servicebeurten en voorschriften;
- b) alleen bevoegd onderhoudspersoneel behoort reparaties en onderhoudsbeurten aan apparatuur uit te voeren;
- c) er behoren registraties te worden bijgehouden van alle vermeende en daadwerkelijke fouten, en van al het preventieve en correctieve onderhoud;
- d) als apparatuur is ingepand voor onderhoud behoren passende maatregelen te worden geïmplementeerd, waarbij in aanmerking wordt genomen of dit onderhoud wordt uitgevoerd door personeel op locatie of buiten de organisatie; voor zover nodig behoort vertrouwelijke informatie uit de apparatuur te worden verwijderd of het onderhoudspersoneel behoort voldoende betrouwbaar te worden verklaard;
- e) er behoort te worden voldaan aan alle onderhoudsplan en de verzekeringspolissen zijn up-to-date.

Tevens wordt verzocht de leverancier hiervan in kennis te stellen. Het is de taak van de leverancier te vinden om te waarborgen dat er niet is geknoeid met de apparatuur en dat deze niet is slecht functioneert.

C.5.2.5 Verwijdering van bedrijfsmiddelen

Beheersmaatregel

Apparatuur, informatie en software behoren niet van de locatie te worden meegenomen zonder voorafgaande goedkeuring. (ISO 11.2.5)

Implementatierichtlijn

Met de volgende richtlijnen behoort rekening te worden gehouden:

- a) medewerkers en gebuik¹ van (externe partijen¹) die bevoegd zijn om toe te staan dat bedrijfsmiddelen van de lokale worden meegenomen behoren te worden geïdentificeerd;
- b) aan de afwezigheid van bedrijfsmiddelen behoren tijdsgrenzen te worden gesteld en er behoort te worden geveerd of ze worden teruggebracht;
- c) voor zover nodig en gepast behoort het meenemen om de terugkeer van bedrijfsmiddelen te worden

geregistreerd;

- d) de identiteit en connectie van iedereen die bedrijfsmiddelen hanteert of gebruikt, behoort te worden gedocumenteerd en deze documenten behoren samen met de apparatuur, informatie of software te worden getoetst.

C.5.2.6 Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein**Beheersmaatregel:**

Bedrijfsmiddelen die zich buiten het terrein bevinden, behoren te worden beveiligd, waarbij rekening behoort te worden gehouden met de verschillende risico's van werken buiten het terrein van de organisatie. (ISO 11.2.6)

Implementatierichtlijn

Het buiten het terrein van de organisatie gebruiken van apparatuur waarop informatie is opgeslagen en die informatie verspreikt, behoort door de directie te worden goedgekeurd. Dit geldt voor apparatuur die algemeen is van de organisatie en voor apparatuur die persoonlijk eigendom is en ten behoeve van de organisatie wordt gebruikt.

De volgende richtlijnen behoren in overweging te worden genomen voor het beschermen van apparatuur buiten het terrein van de organisatie:

- a) apparatuur en media die buiten het terrein worden gebruikt behoren niet ongehoord te worden achtergelaten in openbare ruimtes;
- b) voorschriften van de fabrikant voor het beschermen van de apparatuur behoren te allen tijde in acht te worden genomen, bijv. bescherming tegen blootstelling aan sterke elektromagnetische velden;
- c) beheersmaatregelen voor locaties buiten het terrein, zoals locaties voor thuiswerken, telewerken en tijdelijke locaties, behoren op basis van een risico-evaluatie te worden vastgesteld, en passende beheersmaatregelen behoren voor zover relevant te worden toegepast, bijv. afsluitbare archiefkasten, 'steer clear'-beleid, toegangsbeveiligingsmaatregelen voor computers en beveiligde communicatie met het kantoor;

- d) alle apparatuur buiten het terrein tussen verschillende personen of externe partijen wordt overgedragen, behoort een overzicht te worden bijgehouden dat de bewakingsvelden voor de apparatuur vastlegt, met daarin opgenomen ten minste de namen en organisaties die voor de apparatuur verantwoordelijk zijn.

Hiernaast, bijv. op schade, diefstal of afwijkingen, kunnen sterk tussen locaties verspreid en behoren bij het vaststellen van de meest geschikte beheersmaatregel om in overweging te worden genomen.

¹ Zoals het risico wordt gedefinieerd.

C.5.2.7 Veilig verwijderen of hergebruiken van apparatuur

Beheersmaatregel

Alle onderdelen van de apparatuur die opslagmedia bevatten, behoren te worden geïdentificeerd en te waarborgen dat gevoelige gegevens en in licentie gegeven software voorafgaand aan verwijdering of hergebruik zijn verwijderd of betrouwbare veilig zijn overschreven. (ISO 11.2.7)

Implementatierichtlijn

Vorafgaand aan verwijdering of hergebruik behoort te worden gecontroleerd of apparatuur opslagmedia bevat.

Opslagmedia die vertrouwelijke of door auteursrecht beschermde informatie bevatten, behoren, in plaats van met de standaard 'cofete' functie te worden gewist of te worden gemaakt, fysiek te worden vernietigd of de informatie behoort te worden vernietigd, verwijderd of overschreven met gebruikmaking van technieken die het onmogelijk maken de oorspronkelijke informatie terug te halen.

C.5.2.8 Onbeheerde gebruikerapparatuur

Beheersmaatregel

Gebruikers moeten ervoor zorgen dat onbeheerde apparatuur voldoende beschermd is. (ISO 11.2.8)

Implementatierichtlijn

Alle gebruikers behoren op de hoogte te worden gebracht van de beveiligingsbeleid en de procedures voor het beschermen van onbeheerde apparatuur, en van hun verantwoordelijkheden voor het implementeren van die bescherming. Gebruikers behoren te worden geïnformeerd dat zij:

- gevoelige sessies na beëindiging afsluiten, tenzij de sessies kunnen worden beveiligd door een geschikte verspreiding, bijv. een schermvervalsing die door een wachtwoord wordt beschermd;
- afsluiten uit toepassingen of netwerkdiensten die niet langer nodig zijn;
- aanmaken of mobiele apparatuur beveiligen tegen onbevoegd gebruik door middel van toetsvoorziening of een wachtwoord, bijv. toegang via wachtwoord, als de apparatuur niet in gebruik is.

C.6. Beheer van bedrijfsmiddelen

C.6.1. Inventariseren van bedrijfsmiddelen

Beheersmaatregel

Bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten behoren te worden geclassificeerd, en van deze bedrijfsmiddelen behoort een inventaris te worden opgesteld en onderhouden. (SO 8.1.1)

Implementatierichtlijn

Een organisatie behoort bedrijfsmiddelen die relevant zijn in de levenscyclus van informatie te identificeren en hun belang te documenteren. De levenscyclus van informatie behoort aanmaak, verwerking, opslag, overdracht, verwijdering en vernietiging te omvatten. Documentatie behoort te worden onderhouden in speciale of bestaande inventarislijsten indien van toepassing.

De inventarislijst van de bedrijfsmiddelen behoort nauwkeurig, actueel, consistent en in overeenstemming met andere inventarisoverzichten te zijn.

Voor elk van de geïdentificeerde bedrijfsmiddelen behoort het eigendom te worden toegekend (zie C.6.2) en de classificatie te worden geïdentificeerd (zie ISO 8.2).

C.6.2. Eigendom van bedrijfsmiddelen

Beheersmaatregel

Bedrijfsmiddelen die in het inventarisoverzicht worden bijgehouden, behoren een eigenaar te hebben (ISO 8.1.2)

Implementatierichtlijn

Personeel evenals andere entiteiten die een deel van de directe geïdentificeerde verantwoordelijkheid hebben voor de levenscyclus van een bedrijfsmiddel, komen in aanmerking om te worden benoemd als eigenaar van een bedrijfsmiddel.

Gewoonlijk wordt een procedure geïmplementeerd die ervoor zorgt dat de benoeming van een eigenaar van bedrijfsmiddelen tijdig plaatsvindt. Het eigenaarschap behoort te worden toegekend als bedrijfsmiddelen worden aangekocht of als bedrijfsmiddelen naar de organisatie worden overgedragen. De eigenaar van het bedrijfsmiddel behoort verantwoordelijk te zijn voor het juiste beheer ervan voor de gehele levenscyclus van het bedrijfsmiddel.

De eigenaar van het bedrijfsmiddel betaamt:

- ervoor te zorgen dat bedrijfsmiddelen worden geïnventariseerd;
- ervoor te zorgen dat bedrijfsmiddelen passend worden geclassificeerd en beschermd;
- toegabeperkingen en classificatie van belangrijke bedrijfsmiddelen te definiëren en periodiek te beoordelen, rekening houdend met de van toepassing zijnde beleidsregels voor toegang/beveiliging;
- te zorgen voor een juiste gang van zaken als het bedrijfsmiddel wordt verwijderd of vernietigd.

C.6.3. Aanvaardbaar gebruik van bedrijfsmiddelen

Beheersmaatregel

Voor het aanvaardbaar gebruik van informatie en van bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten behoren regels te worden geïdentificeerd, gedocumenteerd en geïmplementeerd. (SO 8.1.3)

Implementatierichtlijn

Medewerkers en externe gebruikers die bedrijfsmiddelen van de organisatie gebruiken of er toegang toe hebben, behoren bewust te worden gemaakt van de informatiebeveiligingsaspecten van de bedrijfsmiddelen van de organisatie die samenhangen met informatie en informatieverwerkende

faciliteiten en bronnen. Zij behoven verantwoordelijk te zijn voor hun gebruik van informatievoorzieningen en voor gebruik onder hun verantwoordelijkheid.

C.5.4. Teruggeven van bedrijfsmiddelen

Beheersmaatregel

Alle medewerkers en externe gebruikers behoren alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben bij beëindiging van hun dienstverband, contract of overeenkomst terug te geven. (ISO 8.1.4)

Implementatierichtlijn

In de beëindigingsprocedures behoort formeel het teruggeven van alle eerder verstrekte fysieke en elektronische bedrijfsmiddelen die het eigendom zijn van of toebehoren zijn aan de organisatie te worden opgenomen.

Ingeval een medewerker of een gebruiker van een externe partij apparatuur van de organisatie koopt of eigen persoonlijke apparatuur gebruikt, behoren procedures te worden gevolgd om ervoor te zorgen dat alle relevante informatie aan de organisatie wordt overgedragen en nauwkeurig van de apparatuur wordt verwijderd (zie ISO 11.2.7).

Ingeval een medewerker of externe gebruiker beschikt over kennis die belangrijk is voor de lopende bedrijfsactiviteit, behoort die informatie te worden gedocumenteerd en aan de organisatie te worden overgedragen.

Tijdens de opzegtermijn behoort de organisatie controle uit te oefenen op u) bevoegd koptellen van relevante informatie (bijv. intellectueel eigendom) door medewerkers en contractanten van wie het dienstverband is opgezegd.

C.7. Leveranciersrelaties

Het begrip *leverancier* heeft, met name ook betrekking op interne leveranciers, meestal functionele diensten of organisatie-een. Daarnaast kan sprake zijn van een ketenpartner, die diensten in het primaire proces levert, waarbij overeenkomsten worden gesloten.

Bij het in- of extern uitbesteden van onderateenente diensten zullen de normen van dit handboek behorend bij die diensten gehandhaafd moeten blijven, mits de eigen verantwoordelijkheid niet anders wordt. Indien de eigen bedrijfsprocessen afhankelijk zijn van externe bedrijfsprocessen geldt, in principe hetzelfde, d.w.z. dat de eigen bedrijfsvoering afhankelijk wordt van de betrouwbaarheid van derden.

C.7.1. Informatiebeveiliging in leveranciersrelaties

Doelstelling: De bescherming waarborgen van bedrijfsdoelen van de organisatie die toegankelijk zijn voor leveranciers. (ISO 15.1)

C.7.1.1 Informatiebeveiligingsbeleid voor leveranciersrelaties

Beheersmaatregel

Met de leverancier behoren de informatiebeveiligingsnormen om risico's te verlagen die verband houden met de toegang van de leverancier tot de bedrijfsmiddelen van de organisatie, te worden overeengekomen en gedocumenteerd. (ISO 15.1.1)

Implementatierichtlijn

De organisatie beoordeelt beheersmaatregelen voor informatiebeveiliging vast te stellen en verplicht te stellen om specifiek de toegang van de leverancier tot de informatie van de organisatie beleidsmatig aan te pakken. Deze beheersmaatregelen betreffen betrekking te hebben op de door de organisatie te implementeren processen en procedures, en op de processen en procedures waarvan de organisatie behoort te eisen dat de leverancier deze implementeert, met inbegrip van:

- 1) vaststellen en documenteren van de soorten leveranciers, bijv. IT-diensten, logistieke voorzieningen, technische diensten, IT-infrastructuurcomponenten waarvan de organisatie de toegang tot de informatie wil toestaan;
- 2) een gezamenlijk vastgesteld proces en gestandaardiseerde levenscyclus voor het beheer van leveranciersrelaties;
- 3) definiëren van de soorten informatietoegang die verschillende soorten leveranciers wordt toegestaan, en de toegang monitoren en controleren;
- 4) een minimum aan informatiebeveiligingsnormen voor elk soort informatie en elk soort toegang dat dient als basis voor individuele leveranciersovereenkomsten, gebaseerd op de bedrijfsbehoeften en eisen van de organisatie en haar risico's;
- 5) processen en procedures voor het monitoren van de naleving van vastgestelde informatiebeveiligingsnormen voor elk soort leverancier en elk soort toegang, met inbegrip van toedeling van derden en productvalidatie;
- 6) beheersmaatregelen betreffende nauwkeurigheid en volledigheid ter waarborging van de integriteit van de informatie of informatieverwerking die elke partij kiest;
- 7) soorten verplichtingen die van toepassing zijn op leveranciers om de informatie van de organisatie te beschermen;
- 8) omgaan met incidenten en noodsituaties die verband houden met toegang van leveranciers met inbegrip van wanbetrouwbaarheden van zowel de organisatie als van de leveranciers;
- 9) regelgeving voor flexibiliteit en, zo nodig voor herstel en noodsituaties om de beschikbaarheid te herstellen van de informatie of de informatieverwerking die door elk van de partijen wordt gedeeld;
- 10) bewustzijns training voor het personeel van de organisatie dat betrokken is bij acquisitie met betrekking tot toepasselijke beleidsregels, processen en procedures;

k) bewustzijnstraining voor het personeel van de organisatie dat contacten onderhoudt met personeel van de overzieder betreffende passende regels van betrokkenheid en gedrag, gebaseerd op het type leverancier en het soort toegang dat de leverancier heeft tot systemen en informatie van de organisatie;

l) voorwaarden waarop informatiebeveiligingsplannen en beheersmaatregelen zullen worden gedocumenteerd in een overeenkomst die door beide partijen wordt ondertekend;

m) beheers van de nodige transitie van informatie, informat oververkende faciliteiten en al het andere dat moet overgaan, en waarborgen dat informatiebeveiliging tijdens de gehele transitieperiode wordt gehandhaafd.

C.7.1.2 Opnemen van beveiligingsaspecten in leveranciersovereenkomsten

Beheersmaatregel

Alle relevante informatiebeveiligingsaspecten behoren te worden vastgesteld en overeengekomen met elke leverancier die toegang heeft tot IT-infrastructuurcomponenten ten behoeve van de informatie van de organisatie, of daar verwerkt opstaat, onmiddellijk of later. (ISO 15.1.2)

Implementatieverplichting

Leveranciersovereenkomsten behoren te worden vastgesteld en gedocumenteerd om te waarborgen dat er geen misverstand tussen de organisatie en de leverancier bestaat ten aanzien van de verplichtingen van beide partijen om te voldoen aan relevante informatiebeveiligingsaspecten.

De volgende behoort te worden opgenomen in de overeenkomsten om te zorgen om te voldoen aan de vastgestelde informatiebeveiligingsaspecten:

- omschrijving van de informatie die moet worden verschaft of toegankelijk moet worden en methode om de informatie te verschaffen of toegankelijk te maken;
- classificatie van de informatie in overeenstemming met het classificatieschema van de organisatie (zie ISO 8.2); zo nodig ook mapping tussen het eigen schema van de organisatie en het schema van de leverancier;
- wettelijke en regelgevende eisen, met inbegrip van overheidsaanziening, rechten van intellectueel eigendom en auteursrecht, en een beschrijving van hoe wordt gewaarborgd dat ervan wordt voldaan;
- verplichting van elke contractuele partij om een overeengekomen aantal beheersmaatregelen te implementeren, waaronder toegangsbeveiliging, prestatiebeoordeling, monitoring, rapporteren en audit;
- de regels van aanvaardbaar gebruik van informatie, met inbegrip van aanvaardbaar gebruik indien noodzakelijk;

Tenzij een expliciete lijst van leverancierspersoneel dat geautoriseerde toegang heeft of bevoegd is informatie van de organisatie te ontvangen, hetzij procedures of voorwaarden voor autorisatie en het intrekken van de autorisatie, tot toegang tot of ontvangst van informatie van de organisatie voor leverancierspersoneel.

- beleidsregels betreffende informatiebeveiliging die relevant zijn voor het specifieke contract;
- eiser voor incidentbeheer en -procedures (in het bij zonder notificatie en samenwerking tijdens herstel van het incident);
- trainings- en bewustzijnselzen voor specifieke procedures om informatiebeveiligingsaspecten, bijv voor incidentresponsprocedures, autorisatieprocedures;
- relevante regelgeving voor schermscreemingen, met inbegrip van de beheersmaatregelen die moeten worden geïmplementeerd;
- relevante overeenkomstpartners, met inbegrip van een contactpersoon voor aangelegenheden betreffende informatiebeveiliging;
- indien relevant, screeningselzen voor leverancierspersoneel, met inbegrip van verantwoordelijkheidsveroor het uitvoeren van de screening en het fraudeprocedures indien de screening niet is voltooid of de resultaten aanmelding geven tot twijfel of bezorgdheid;

- m) het recht om de processen en beheersmaatregelen van de leverancier in verband met de overeenkomst te auditen;
- n) procedures voor het oplossen van defecten en conflicten;
- o) verplichting van de leverancier om periodiek een schriftelijk rapport te verstrekken over de beschikbaarheid van beheersmaatregelen, en overeenkomstig voor tijdige contractie van relevante kwesties die in het rapport aan de orde worden gesteld;
- p) verplichting van de leverancier om te voldoen aan de beveiligingsniveaus van de organisatie.

C.7.1.3 Toeleveringsketen van informatie- en communicatietechnologie

Beheersmaatregel

Over de leverancier moet overeenkomst behoren zamen te bevatten die betrekking hebben op de informatie- en communicatietechnologie in verband met de toeleveringsketen van de diensten en producten op het gebied van informatie- en communicatietechnologie. (ISO 15.1.3)

Implementatiecriteria

Overeenkomst behoort te worden de volgende onderwerpen op te nemen in leveranciersovereenkomsten betreffende beveiliging van de toeleveringsketen:

- a) informatiebeveiligingsbeleid, definities die gelden voor acquisitie van producten en diensten op het gebied van informatie- en communicatietechnologie naast de algemene informatiebeveiligingsbeleid voor leveranciersdata's;
- b) met betrekking tot diensten op het gebied van informatie- en communicatietechnologie, eisen dat leveranciers de beveiligingsniveaus van de organisatie in de gehele toeleveringsketen behoudend ten minste leveranciers die aan de organisatie overdragen, uitlokken;
- c) met betrekking tot producten op het gebied van informatie- en communicatietechnologie, eisen dat leveranciers passende beveiligingspraktijken in de gehele toeleveringsketen behoudend ten minste indien deze producten componenten bevatten die van andere leveranciers worden betrokken;
- d) een proces implementeren om aanvaardbare methoden implementeren om te valideren dat geleverde producten en diensten op het gebied van informatie- en communicatietechnologie in overeenstemming zijn met verklaarde beveiligingsniveaus;
- e) een proces implementeren voor het vaststellen van componenten van producten of diensten die essentieel zijn voor het handhaven van de functionaliteit en daarvoor verhoogde aandacht en toezicht vereisen als deze buiten de organisatie worden gebouwd, in het bijzonder indien de eindleverancier delen van componenten van producten of diensten aan andere leveranciers uitbesteedt;
- f) zekerheid verkrijgen dat essentiële componenten en de herkomst ervan in de toeleveringsketen kunnen worden nagekeurd;
- g) zekerheid verkrijgen dat de geleverde producten op het gebied van informatie- en communicatietechnologie functioneren zoals voorzien zonder ongewenste of ongewenste verschijnselen;
- h) regels definiëren voor het delen van informatie met betrekking tot de toeleveringsketen en potentiële leveranciers en compromissen tussen de organisatie en leveranciers;
- i) specifieke procedures implementeren voor het beheeren van de leveringscyclus en de beschikbaarheid van de componenten van de informatie- en communicatietechnologie en samenhangende beveiligingsdata's. Historie behoeft het beheeren van de risico's van componenten die niet langer beschikbaar zijn doordat leveranciers niet meer bestaan of doordat leveranciers deze componenten niet meer leveren in verband met veranderende technologie.

C.7.2. Beheer van dienstverlening van leveranciers

Doelstelling: Een overeenkomstig niveau van informatiebeveiliging en dienstverlening in overeenstemming met de leveranciersovereenkomsten handhaven. (ISO 15.2)

C.7.2.1 Monitoring en beoordeling van dienstverlening van leveranciers

Beheersmaatregel

Organisaties behoren regelmatig de dienstverlening van leveranciers te monitoren, te beoordelen en te auditeren. (ISO 15 2.1)

Implementatierichtlijn

Het monitoren en beoordelen van dienstverlening van leveranciers behoort te waarborgen dat aan de voorwaarden van informatiebeveiliging wordt voldaan, en dat incidenten en problemen betreffende informatiebeveiliging op de juiste manier worden behandeld.

Mierne haktort een rimes over het beheer van de dienstverlening te herzien hettoende de relatie tussen de organisatie en de leverancier om:

- de prestatiehoeve van de dienstverlening te monitoren om naleving van de overeenkomsten te waarborgen;
- de rapporten over de dienstverlening die zijn opgesteld door de leverancier te beoordelen, en regelmatig voortgesprekken te regelen voor zover deze de overeenkomsten versien;
- audits van leveranciers uit te voeren indien beschikbaar tezamen met de beoordeling van rapporten van onafhankelijke auditors, en vastgestelde kwesties op te volgen;
- informatie te verstrekken over informatiebeveiligingsincidenten en deze informatie te beoordelen voor zover vereist door de overeenkomsten en ondersteunende richtlijnen en procedures;
- auditrapporten van leveranciers op verlagen van informatiebeveiligingsgecontroleerde operationele problemen, verbeteringen, opsporing van storingen, en onderbreuktoep in verband met de gevorderde dienst te beoordelen;
- vastgestelde problemen op te lossen en te beheeren;
- informatiebeveiligingsaspecten van de relaties van de leverancier met zijn eigen leveranciers te beoordelen;
- te overzichten op de leverancier voldoende capaciteit voor de diensten onderhoud samen met werkbaar plannen die zijn ontworpen om te waarborgen dat de overeenkomsten continue kunnen worden van de dienstverlening grote storingen of calamiteiten in de dienstverlening worden onderhouden (zie hoofdstuk ISO 17).

De verantwoordelijkheid voor het beheer van leveranciersrelaties behoort te worden toegevoegd aan een daartoe aangewezen persoon of dienstverrichtingbeheerzaam. De organisatie behoeft verder ervoor te zorgen dat leveranciers verantwoordelijkheden kwantificeren voor het beoordelen van de naleving en het dwingend uitvoeren van de eisen van de overeenkomsten. Om te monitoren dat de eisen van de overeenkomst, in het bijzonder de informatiebeveiligingsdelen, worden nagekomen, behoren voldoende technische mogelijkheden en middelen beschikbaar te worden gesteld. Als toezichtingen in de dienstverlening worden waargenomen behoort passende actie te worden ondernomen.

De organisatie behoort voldoende controle over en zicht te houden op alle beveiligingsaspecten betreffende gevoelige of essentiële informatie of informatieverwerkende activiteiten die toegankelijk zijn voor, worden verwerkt of behandeld door een leverancier. De organisatie behoort via een gedefinieerde rapportageprocedure zicht te houden op beveiligingsactiviteiten zoals wijzigingsbeheer, vaststellen van kwetsbaarheden en rapporteren van en respons op informatiebeveiligingsincidenten.

C.7.2.2 Beheer van veranderingen in dienstverlening van leveranciers**Beheersmaatregel**

Veranderingen in de dienstverlening van leveranciers, met inbegrip van herindividing van verdeling van bestaande behoeften, procedures en beheersmaatregelen voor informatiebeveiliging, behoren te worden beheerd rekening houdend met de kriticaliteit van bedrijfsinformatie, betrokken systemen en processen en herbeoordeling van risico's. (ISO 15 2.2)

Implementatierichtlijn

De volgende aspecten behoren in overweging te worden genomen:

- veranderingen in leveranciersovereenkomsten;

te veranderingen die door de organisatie zijn aangebracht ter implementatie van:

- 1) verbeteringen van de huidige aangeboden dienstverlening;
- 2) ontwikkelingen van nieuwe toepassingen en systemen;
- 3) wijzigingen in of updates van beleid en procedures van de organisatie;
- 4) nieuwe of gewijzigde beheersmaatregelen om informatiebeveiligingsincidenten op te lossen en om de veiligheid te verbeteren.

o) veranderingen in diensten van de leverancier ter implementatie van:

- 1) veranderingen en verbeteringen van netwerken;
- 2) gebruik van nieuwe technologieën;
- 3) samenvoering van nieuwe producten of nieuwe versies/uitvoeren;
- 4) nieuwe ontwikkelinstrumenten en omgevingen;
- 5) veranderingen in fysieke locatie van dienstverleningsfaciliteiten;
- 6) verandering van leveranciers;
- 7) enderaanname bij een andere leverancier.

C.8. Beveiliging bedrijfsvoering

C.8.1. Bedieningsprocedures en verantwoordelijkheden

Doelstelling: Correcte en veilige bediening van informatieverwerkende faciliteiten waarborgen. (ISO 12.1)

C.8.1.1. Gedocumenteerde bedieningsprocedures

Beheersmaatregel

Bedieningsprocedures moeten te worden gedocumenteerd en beschikbaar te worden gesteld aan alle gebruikers die ze nodig hebben. (ISO 12.1.1)

Implementatierichtlijn

Voor bedieningsprocedures die samenhangen met informatieverwerkende en communicatiefaciliteiten, zoals de procedures voor het starten en afsluiten van de computer, back-up, onderhoud van apparatuur, behandeling van media, beheer en veiligheid van computeruimte en postverwerking behoren gedocumenteerde procedures te worden opgesteld.

In de bedieningsprocedures behoren de bedieningsvoorschriften te zijn opgenomen, onder andere voor:

- de installatie en configuratie van systemen;
- verwerking en behandeling van informatie, zowel geautomiseerd als handmatig;
- back-up (zie ISO 12.3);
- eisen ten aanzien van de planning, met inbegrip van omlerige veronderheid met andere systemen, tijdstip waarop de eerste taak begint en tijdstip van afronding van de laatste taak;
- voorschriften voor de afhandeling van fouten of andere uitzonderlijke omstandigheden die tijdens de uitvoering van de taak kunnen optreden, waaronder beperkingen ten aanzien van het gebruik van systeemhulpmiddelen (zie ISO 9.4.4);
- ondersteunings- en escalatiecontacten, waaronder externe ondersteuningscontacten in geval van onverwachte bedienings- of technische moeilijkheden;
- voorschriften voor de behandeling van speciale uitvoer en media, zoals het gebruik van speciaal kantoorbenodigdheden of het creëren van vertrouwelijke uitvoer, waaronder procedures voor veilig verwijderen van uitvoer van verwijde taken (zie ISO 9.3 en ISO 11.2.7);
- procedures voor het opnieuw opstarten en herstellen van het systeem in geval van systeemoverstroomingen;
- het beheer van audit- en systeemlogbestandsformatie (zie 12.4);
- procedures voor het monitoren van activiteiten.

Bedieningsprocedures en de gedocumenteerde procedures voor systeemactiviteiten behoren te worden behandeld als formele documenten en wijzigingen behoren door de directie te worden goedgekeurd. Indien technisch haalbaar behoren informatiesystemen consistent te worden beheerd, met gebruikmaking van dezelfde procedures, instrumenten en hulpmiddelen.

C.8.1.2. Wijzigingsbeheer

Beheersmaatregel

Veranderingen in de organisatie, bedrijfsprocessen, informatieverwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging behoren te worden beheerd. (ISO 12.1.2)

Implementatierichtlijn

In het bijzonder met de volgende aspecten behoort rekening te worden gehouden:

- identificatie en registratie van significante veranderingen;
- plannen en toelien van veranderingen;
- de potentiële impact van dergelijke veranderingen beoordelen, waaronder de impact van de informatiebeveiliging;
- formele goedkeuringprocedure voor voorgestelde veranderingen;
- verificatie dat is voldaan aan de eisen van informatiebeveiliging;
- communicatie van veranderingen aan alle betrokken personen;
- uitvoeringsplan, wat onder procedures en verantwoordelijkheden voor het afbreken en herstellen van niet-geslaagde veranderingen en onvoorziene gebeurtenissen;
- voorzien in een noodveranderingsproces om veranderingen die nodig zijn om een incident op te lossen snel en behoorst te implementeren (zie ISO 16.1).

Verantwoordelijkheid en procedures voor beheer behoren formeel te worden vastgelegd om voldoende beheersing van alle veranderingen te waarborgen. Als de veranderingen hebben plaatsgevonden behoort een auditrapport te worden bewaard.

G.8.1.3 Capaciteitsbeheer

Beheersmaatregel

Het gebruik van middelen behoort te worden gemonitord en afgestemd, op de behorende verwachtingen te worden opgesteld voor toekomstige capaciteitsbehoeven om de vereiste systeemprestaties te waarborgen. (ISO 12.1.3)

Implementatierichtlijn

Capaciteitsbehoeven behoren te worden gedefinieerd, rekening houdend met de bedrijfskwaliteit van het betreffende systeem. Het systeem behoort te worden afgestemd en gemonitord om de beschikbaarheid en doelmattigheid van systemen te waarborgen en zo nodig te verbeteren. Om problemen vroegtijdig vast te stellen behoren detectiemaatregelen te worden genomen. Prognoses voor toekomstige capaciteitsbehoeven behoren rekening te houden met nieuwe bedrijfs- en systeemrisico's en de huidige en verwachte trends in de informatieovervloedige capaciteitsbehoeven van de organisatie. Speciale aandacht behoort te worden gegeven aan modellen met een lange levenscyclus of hoge kosten; behorende behoeven dienen het gebruik van belangrijke systemen/rollen te monitoren. Ze behoren trends in het gebruik te signaleren, vooral in relatie tot bedrijfsaanpassingen of beheersinstrumenten voor informatiesystemen.

Beheerders behoren deze informatie te gebruiken voor het signaleren en vermijden van potentiële knelpunten en afhankelijkheid van de aanrij personeel die een bedreiging kunnen vormen voor de systeembeveiliging en dienstverlening, en behoren passende actie te plannen.

Voldoende capaciteit kan worden verkregen door de capaciteit te verhogen of door de vraag te verlagen. De capaciteitsaanpak kan onder meer worden beheerst door:

- verouderde gegevens te verwijderen (schijfuitruiming);
- loopspansingen, systemen, databases of omgevings buiten gebruik te stellen;
- batchprocessen en -schemas te optimaliseren;
- loopspansingenlogica of databaseweggen te optimaliseren;
- de bandbreedte voor datastroom die veel energie verbruiken te weigeren of te beperken als deze niet van overwegend bedrijfsbelang zijn (bijv. videoconferencing).

Voor systemen die belangrijk zijn voor de missie behoort voor de capaciteit een gedocumenteerd beheersplan te worden overnemen.

C.8.1.4 Scheiding van ontwikkel-, test- en productieomgevingen

Beheersmaatregel

Ontwikkel-, test- en productieomgevingen behoven te worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te vermijden. (SC 12.1.4)

Implementatierichtlijn

Het scheiden van productie-, test- en ontwikkelomgevingen dat nodig is om operationele problemen te voorkomen behoort te worden geïdentificeerd en geïmplementeerd.

Met de volgende aspecten behoort rekening te worden gehouden:

- a) voor het maken van software van de ontwikkel- naar de operationele status behoren regels te worden gedefinieerd en gedocumenteerd;
- b) ontwikkelsoftware en operationele software behoren op verschillende systemen of computerprocessors te draaien en in verschillende combinaties van directory's;
- c) veranderingen aan productiesystemen en toepassingen behoren te worden getest in een test- of geïsoleerde omgeving voordat ze in productiesystemen worden toegepast;
- d) behoudens uitzonderlijke omstandigheden, behoren tests niet in productiesystemen te worden uitgevoerd (zie ook C.12.3. Toelagevoens);
- e) compilers, editors en andere ontwikkelinstrumenten of systemhulp-middelen behoren, indien ze niet nodig zijn, niet toegankelijk te zijn vanuit productiesystemen;
- f) gebruikers behoren voor operationele en testsystemen verschillende gebruikersprofielen te gebruiken, en monitoren behoren passende identificatiecodes toe te passen om historici op te kunnen te volgen;
- g) gevoelige gegevens behoren niet in de omgeving van het testsysteem te worden gekopieerd, te wij voor het testsysteem equivalente beheersmaatregelen zijn getroffen (zie ISO 14.3).

C.8.2 Bescherming tegen malware

Doelstelling: Waarborgen dat informatie en informatieverwerkende faciliteiten beschermd zijn tegen malware.

C.8.2.1 Beheersmaatregelen tegen malware

Beheersmaatregel

Ter bescherming tegen malware behoren beheersmaatregelen voor detectie, preventie en herstel te worden geïmplementeerd, in combinatie met een passend bewustzijn van gebruikers. (SC 12.2.1)

Implementatierichtlijn

Bescherming tegen malware behoort te zijn gebaseerd op software die malware opspoot en op herstelsoftware. Bewustzijn ten aanzien van informatie beveiliging en passende beheersmaatregelen met betrekking tot systeembewaking en wijzigingsplannen. De volgende richtlijnen behoren te worden genomen:

- a) een formeel beleid vaststellen dat het gebruik van ongeautoriseerde software verbodt (zie ISO 12.6.2 of ISO 14.2);
- b) controle en aanbevelen implementeren die het gebruik van ongeautoriseerde software voorkomen of opsporen (bijv. een witte lijst voor toepassingen opstellen);

- d) beheersmaatregelen implementeren die het gebruik van bekeerde of verdachte kwaadaardige websites voorkomen of opsporen (bijv. een zwarte lijst opstellen);
- e) een formeel beleid vaststellen ter bescherming tegen risico's die samenhangen met het verkrijgen van bestanden en software, hardzj van hardzj via externe netwerken of een ander medium, waarbij wordt aangegeven welke beschermende maatregelen behoren te worden genomen;
- f) kwetsbaarheden verminderen die kunnen worden geëxploiteerd door malware, bijv. via beheer van technische kwetsbaarheden (zie ISO 12.6);
- g) regelmatig beoordelingen uitvoeren van de software op governance van systemen die kritische bedrijfsprocessen ondersteunen; de aanwezigheid van niet-goedgekeurde bestanden of ongeautoriseerde wijzigingen behoort formeel te worden onderzocht;
- h) installeren en regelmatig updaten van software die malware opspoor: en van herstelssoftware, waarbij computers en media als voor-zorgmaatregel of routinematig worden gescand, de uitgevoerde scan behoort te omvatten:

- 1) alle bestanden die via netwerken of via elke vorm van opslagmedium zijn ontvangen, vóór gebruik op malware scannen;
- 2) bijlagen en downloads vóór gebruik op malware scannen; deze een behoorlijk en verscheidene plaatsen te worden uitgevoerd, bijv. op elektronische mailservers, op desktopcomputers en bij de toegang tot het netwerk van de organisatie;
- 3) internetpagina's op malware scannen;

- i) ter bescherming tegen malware op systemen procedures en verantwoordelijkheden definiëren, het gebruik ervan trainen, aanvallen van malware melden en herstellen;
- j) passende bedrijfscontinuïteitsplannen voorbereiden voor het herstellen na malwareaanvallen, met inbegrip van de nodige back-up van gegevens en software en hersteloplossingen (zie ISO 12.3);
- k) procedures implementeren om regelmatig informatie te verzamelen, zoals een abonnement op mailinglijsten of het raadplegen van websites die informatie over nieuwe malware geven;
- l) procedures implementeren om informatie in verband met malware te valideren en waarborgen dat waarschuwingsberichten nauwkeurig en informatief zijn; beheerders behoren ervoor te zorgen dat gekwalificeerde bronnen, bijv. goed aangeschreven атааде kranten, betrouwbare internetpagina's of leveranciers van anti-malware software, worden geconsulteerd om te differentiëren tussen een hoax en echte malware; alle gebruikers behoren te worden geïnformeerd over het probleem van hoaxes en wat te doen na ontvangst van een hoax;
- m) omgevingen isoleren als cybernetische impact dreigt.

C.3.3. Maken van back-ups

Doelstelling: Beschermen tegen het verliezen van gegevens. (ISO 12.5)

C.3.3.1 Disk-up van informatie

Beheersmaatregel

Regelmatig behoren back-upkopieën van informatie, software en systeemafbeeldingen te worden gemaakt; er gaten: in overeenstemming met een overeengekomen back-upbeleid. (ISO 12.3.1)

Implementatierichtlijn

Om de eisen van de organisatie voor het back-uppen van informatie, software en systemen te definiëren behoort een back-upbeleid te worden vastgesteld.

Het back-upbeleid behoort de eisen voor het bewaren en beschermen te definiëren.

Er behoort te worden voorzien in adequate back-upfaciliteiten om te waarborgen dat alle essentiële informatie en software na een calamiteit of na falen van media kan worden hersteld.

Bij het opstellen van een back-upplan, behoren de volgende punten in overweging te worden genomen:

- a) de behoren nauwkeurige en volledige registers van de back-upplannen en gedocumenteerde herstelprocedures aanwezig te zijn;
- b) de omvang (bijv. een volledige back-up of alleen van de wijzigingen) en de frequentie van de back-ups behoren in overeenstemming te zijn met de bedrijfsbehoefte van de organisatie, de beveiligingsbehoefte van de betrokken informatie en de kritiektheid van de informatie voor de voortzetting van de bedrijfsuitoefening van de organisatie;
- c) de back-ups behoren in een afgelegen locatie te worden bewaard, op een voldoende afstand om niet te worden beschadigd door een calamiteit op de hoofdlocatie;
- d) aan back-upinformatie behoort een passend niveau van fysieke en omgevingsbescherming te worden gegeven (zie hoofdstuk 11) overeenkomstig met de normen die op de hoofdlocatie worden toegepast;
- e) back-upmedia behoren regelmatig te worden getoetst om te waarborgen dat ze betrouwbaar zijn als ze in noodgevallen nodig zijn; dit behoort te worden gecoördineerd met een test van de herstelprocedures en van de tijd die voor herstel nodig is. Of de back-upgegevens kunnen worden hersteld, behoort te worden getoetst op speciaal daarvoor aangegeven testmedia, niet door de originele media te overnemen omdat het back-up- of herstelproces kan mislukken en onherstelbare schade aan of verlies van gegevens kan veroorzaken;
- f) in gevallen waarin vertrouwelijkheid belangrijk is, behoren back-ups te worden beschermd door ze te coderen.

Herstelprocedures behoren de uitvoering van back-ups te monitoren en fouten in geplande back-ups aan te pakken om de volledigheid van back-ups in overeenstemming met het back-upbeleid te waarborgen.

Herstelprocedures voor individuele systemen en diensten behoren regelmatig te worden getoetst om te waarborgen dat ze voldoen aan de eisen van de belangrijke (en/of) kritieke systemen. In geval van kritieke systemen en diensten behoren back-upprocedures betrokken te hebben op de informatie, toepassingen en gegevens van alle systemen die nodig zijn om het gehele systeem na een calamiteit te herstellen.

Voor belangrijke bedrijfsinformatie behoort de bewaartijd te worden vastgesteld, rekening houdend met eisen voor archiveringsplannen die permanent moeten worden bewaard.

C.8.4. Verslaggeving en monitoren

Doelstelling: Gebeurtenissen vastleggen en bewijzen verzamelen. (ISO 12.4)

C.8.4.1 Gebeurtenisregistreren

Beheersmaatregel

Logbestanden van gebeurtenissen die getruibersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld. (ISO 12.4.1)

Implementatierichtlijn

Logbestanden van gebeurtenissen behoren, voor zover relevant, te bevatten:

- a) gebruikersidentificatie;
- b) systeemactiviteiten;
- c) data, tijdstippen en details van belangrijke gebeurtenissen, bijv. in- en uitloggen;
- d) identiteit of indien mogelijk de locatie van de apparatuur en de systeemidentificatie;

- e) registratie van geslaagde en geweigerde pogingen om toegang tot het systeem;
- f) registratie van goedgekeurde en geweigerde gegevens en overige pogingen om toegang te verkrijgen tot bronnen van informatie;
- g) systeemconfiguratieveranderingen;
- h) gebruik van speciale bevoegdheden;
- i) gebruik van systemen/hulpmiddelen en toepassingen;
- j) bepalen die zijn gepend en het type toegang dat is verstrekt;
- k) netwerkadressen en protocollen;
- l) alarmen die worden afgegeven door het toegangsbeveiligingssysteem;
- m) activering en deactivering van beschermingsystemen, zoals antivirussystemen en inbraakdetectiesystemen;
- n) verslaglegging van irrasaties die door gebruikers in toepassingen zijn uitgevoerd.

C.8.4.2 Beschermen van informatie in logbestanden

Beheersmaatregel

Ingenieurs en informatie in logbestanden behoren te worden beschermd tegen vernieling en onbevoegde toegang. (ISO 12.4.2)

Implementatierichtlijn

Beheersmaatregelen behoren gericht te zijn op het beschermen van informatie in logbestanden tegen onbevoegde veranderingen en tegen operationele problemen met de logvoorziening, met inbegrip van:

- a) veranderingen aan de soorten berichten die worden vastgelegd;
- b) bewerken of verwijderen van logbestanden;
- c) overschrijven van de opslagcapaciteit van de media met de logbestanden, waardoor gebeurtenissen niet meer kunnen worden vastgelegd of eerder vastgelegde gebeurtenissen worden overschreven.

Als onderdeel van het beleid voor het bewaren van verslagen of in verband met eisen om bewijsmateriaal te verzamelen en bewaren kan het nodig zijn om bepaalde auditlogbestanden te archiveren (zie ISO 16.1.1).

C.8.4.3 Logbestanden van beheerders en operators

Beheersmaatregel

Aanmelden van systeembeheerders en -operators behoren te worden vastgelegd en de logbestanden behoren te worden beschermd op regelmatig te worden beoordeeld. (ISO 12.4.3)

Implementatierichtlijn

Houders van een speciaal account zijn mogelijk in staat om de logbestanden op informatieve werkende systemen die onder hun directe beheer staan te manipuleren. Daarom is het nodig de logbestanden te beschermen en te beoordelen om te handhaven dat specifieke gebruikers niet in staat zijn toegang te krijgen tot deze logbestanden.

C.8.4.4 Kloeksynchronisatie

Beheersmaatregel

De klokken van alle te evante informatieverwerkende systemen binnen een organisatie of beveiligingsdomein behoren te worden gesynchroniseerd met een referentiebron. (ISO 12.4.4)

Implementatierichtlijn

Externe en interne eiser voor waargave, synchronisatie en nauwkeurigheid van tijd behoren te worden gedocumenteerd. Dergelijke eisen kunnen welzijns, regelgevende of contractuele celen zijn, naleving van normen of eisen voor interne monitoring. Er behoort een standaard referentietijd voor gebruik binnen de organisatie te worden gedefinieerd.

De reikwijdte van de organisatie op een referentietijd op basis van externe bron(nen) te verkrijgen en hoe interne klokken betrouwbaar te synchroniseren behoort te worden gedocumenteerd en geïmplementeerd.

G.3.5. Beheersing van operationele software

Doelstelling: De integriteit van operationele systemen waarborgen. (ISO 12.5)

G.5.5.1 Software installeren op operationele systemen**Beheersmaatregel**

Om het op operationele systemen installeren van software te beheersen behoren procedures te worden geïmplementeerd. (ISO 12.5.1)

Implementatie richtlijn

De volgende richtlijnen behoren te worden genomen om de installatie van software op operationele systemen te beheersen:

- het opstellen van de productiesoftware, -toepassingen en -programma-bibliotheken behoort alleen te worden uitgevoerd door getrainde beheerders en na de juiste goedkeuring van de directie (zie ISO 9.4.6);
- productiesystemen behoren alleen goedgekeurde uitvoerbare codes te bevatten en geen ontwikkelcodes of compilers;
- toepassingen en bestuurssoftware behoren pas te worden geïmplementeerd na uitgebreide en succesvolle tests; de tests behoren betrekking te hebben op bruikbaarheid, beveiliging, efficiëntie op andere systemen en gebruikersvriendelijkheid, en behoren te worden uitgevoerd op getrainde systemen (zie ISO 12.1.4); gewaarborgd behoort te worden dat alle corresponderende broncodebibliotheken zijn geïnstalleerd;
- om alle geïnstalleerde software en systeemdocumentatie te beheersen behoort een configuratiebeheersysteem te worden toegepast;
- wanneer veranderingen worden doorgevoerd behoort een strategie voor het terugdraaien van de veranderingen te zijn vastgesteld;
- van alle updates van bestuursprogramma-bibliotheken behoort een auditlogboek te worden bijgehouden;
- wanneer verlies van bestuursprogramma-bibliotheken te worden hersteld voor noodzakelijk;
- oudere versies van software behoren te worden gerepliceerd samen met alle relevante informatie en parameters, procedures, configuratiebestanden en andere ondersteunende software, zolang zij gegevens in het archief worden bewaard.

Software en leveranciers die in productiesystemen wordt gebruikt behoort te worden onderhouden op een niveau dat door de licentienhouder wordt ondersteund. Na verloop van tijd zullen softwareleveranciers stappen met het ondersteunen van oudere softwareversies. De organisatie behoort te kijken naar het gebruik van niet-ondersteunde software te overwegen.

Bij beslissingen om te upgraden naar een nieuwe versie behoort rekening te worden gehouden met de beschikbaarheid van de versie, de veiligheid en de veiligheid van de versie, d.w.z. de introductie van nieuwe informatie-volligheidsfunctionaliteit of het aantal en de ernst van informatie-beveiligingsproblemen die zich bij deze versie voordoen. Softwarepatches behoren te

worden toegepast als ze kunnen bijdragen aan het verwijderen of verminderen van zwakke punten in de informatiebeveiliging (zie ISO 12.8).

Fysiek of logische toegang behoort alleen te worden verleend aan leveranciers wanneer dit noodzakelijk is voor ondersteuningsdoelstellingen en met toestemming van de directie. De activiteiten van de leverancier behoren te worden gemonteerd (zie ISO 15.2.1).

Computersoftware kan soms steunen op externe geleverde software en modules, die behoren te worden gemonteerd en beheerst om onbevoegde veranderingen te vermijden, die zwakke plekken in de beveiliging kunnen introduceren.

C.3.6. Beheer van technische kwetsbaarheden

Doelstelling: Benutten van technische kwetsbaarheden voorkomen. (ISO 12.6)

C.3.6.1 Beheer van technische kwetsbaarheden

Beheersmaatregel

Informatie over technische kwetsbaarheden van informatiesystemen die worden gebruikt behoort tijdig te worden verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden te worden geëvalueerd en passende maatregelen te worden genomen om het risico dat ermee samenhangt aan te pakken. (ISO 12.6.1)

Implementatiestapjes

Een actuele en volledige inventaris van bedrijfsmiddelen (zie hoofdstuk ISO 8) is een voorwaarde voor een doeltreffend beheer van technische kwetsbaarheden, lot de specifieke informatie die nodig is om beheer van technische kwetsbaarheden te ondersteunen behoren informatie over de softwareleveranciers, versiesnummers, huidige implementatie (bijv. welke software is geïnstalleerd op welke systemen) en de persoon of personen in de organisatie verantwoordelijk voor de software. Als reactie op de identificatie van potentiële technische kwetsbaarheden behoort passende en tijdige actie te worden ondernomen. Om een doeltreffend beheerproces voor technische kwetsbaarheden vast te stellen behoren de volgende richtlijnen te worden gevolgd:

- de organisatie behoort de rollen en verantwoordelijkheden in samenhang met het beheer van technische kwetsbaarheden te definiëren en vast te stellen, met inbegrip van het monitoren van de kwetsbaarheden, een risicobeoordeling van de kwetsbaarheden, het installeren van herstelprogramma's (patches), het traceren van bedrijfsmiddelen en de vereiste controlen/verantwoordelijkheden;
- informatiemiddelen die worden gebruikt om relevante technische kwetsbaarheden te bepalen en om het bevestigingsproces te leiden, behoren te worden vastgesteld voor software en andere technologie (op basis van de inventarislijst van bedrijfsmiddelen, zie ISO 8.1.1); deze informatiemiddelen behoren te worden geactualiseerd op basis van veranderingen in de inventarislijst of als andere nieuwe of nuttige methoden zijn gevonden;
- een tijdplan behoort te worden gedefinieerd waarbinnen moet worden gereageerd op aankondigingen van potentiële relevante technische kwetsbaarheden;
- als een potentiële technische kwetsbaarheid is geïdentificeerd, behoort de organisatie de samenhangende risico's en de te ondernemen acties vast te stellen; een dergelijke actie kan patching van kwetsbare systemen inhouden, of het toepassen van andere beheersmaatregelen;
- afhankelijk van hoe urgent een technische kwetsbaarheid moet worden aangepakt behoort de te ondernemen actie te worden uitgevoerd in overeenstemming met de beheersmaatregelen in verband met wijzigingsbeheer (zie ISO 12.1.2) of door responsovereenkomsten voor informatiebeveiligingsincidenten te volgen (zie ISO 16.1.5);
- indien een patch uit een legitieme bron beschikbaar is, behoren de risico's die verbonden zijn aan het installeren van de patch te worden beoordeeld (de risico's die worden gevormd door de kwetsbaarheid behoren te worden vergeleken met het risico van het installeren van de patch);

g) andere behoren te worden getoetst en geëvalueerd voordat ze worden geïmplementeerd om te waarborgen dat ze doeltreffend zijn en niet resulteren in bijverschijnselen die niet kunnen worden getoetst; indien geen patch beschikbaar is, behoren andere beheersmaatregelen te worden overwogen, zoals:

- 1) diensten of capaciteiten in verband met de kwetsbaarheid uitschakelen;
- 2) toegangsbeveiligingsmaatregelen aanpassen of toevoegen, bijv. firewalls, rond de grenzen van netwerken (zie ISO 13.1);
- 3) vaker monitoren om werkelijke ernstvallen op te sporen;
- 4) bewustzijn creëren; de kwetsbaarheid kwaker;

h) over alle procedures behoort een auditlogbestand te worden bijgehouden;

i) het beheerproces met betrekking tot de technische kwetsbaarheid behoort regelmatig te worden geïmplementeerd en geëvalueerd om de doeltreffendheid en doelmatachtigheid ervan te waarborgen;

j) systemen met een hoog risico behoren eerst te worden aangepakt;

k) een systeem met kwetsbaarheden te corrigeren kan aan de functie die moet worden opgevoerd, incidenteel om te voorzien in uit te voeren technische procedures in geval van een incident, behoort een doeltreffend beheerproces met betrekking tot de technische kwetsbaarheid te worden afgestemd op incidentbeheeractiviteiten;

l) een procedure definiëren om de situatie aan te pakken waar een kwetsbaarheid is geïdentificeerd maar waar geen passende beheersmaatregel voortvloeit. In deze situatie behoort de organisatie risico's in verband met de bekende kwetsbaarheid te evalueren en passende risicoregulerende en corrigerende maatregelen te definiëren.

C.8.2 Beperkingen voor het installeren van software

Beheersmaatregel

Voor het door gebruikers installeren van software behoren regels te worden vastgesteld en te worden geïmplementeerd. (ISO 12.8.2)

Implementatierichtlijn

De organisatie behoort een strikt beleid te definiëren en ten uitvoer te brengen met betrekking tot de soorten software die gebruikers mogen installeren.

Het principe van minimaal voorrecht behoort te worden toegepast. Indien aan gebruikers bepaalde voorrechten worden verleend, kunnen zij ook de mogelijkheid hebben om software te installeren. De organisatie behoort vast te leggen welke soorten software mogen worden geïnstalleerd (bijv. updates en beveiligingspatches voor bestaande software) en welke verboden zijn (bijv. software uitlopend voor persoonlijk gebruik of software waarvan de betrouwbaarheid met betrekking tot de potentiële kwaadaardigheid onbekend of verdacht is). Deze voorrechten behoren te worden verleend met oog voor de rollen van de betrokken gebruikers.

C.8.7 Beheer van netwerkbeveiliging

Doelstelling: De bescherming van informatie in netwerken en de ordersturende informatieverwerkende functies waarborgen. (ISO 13.1)

C.8.7.1 Beheersmaatregelen voor netwerken

Beheersmaatregel

Netwerken behoren te worden beheerd en beheerd om informatie in systemen en toepassingen te beschermen. (ISO 13.1.1)

Implementatierichtlijn

Er behoren beheersmaatregelen te worden geïmplementeerd om de veiligheid van informatie in netwerken te waarborgen en ongeautoriseerde toegang onbevoegde toegang te beschermen. Met de volgende aspecten behoort in het bijzonder rekening te worden gehouden:

- er behoren verantwoordelijkheden en procedures voor het beheer van netwerkapparatuur te worden vastgesteld;
- operationele verantwoordelijkheid voor netwerken behoort voor zover van toepassing te worden gescheiden van computerfuncties (zie ISO 6.1.2);
- om de betrouwbaarheid en integriteit van gegevens die via openbare netwerken of draadloze netwerken circuleren te waarborgen en van de aangesloten systemen en toepassingen te beschermen en behoren speciale beheersmaatregelen te worden vastgesteld (zie hoofdstuk ISO-10 en ISO 13.2); er kunnen ook speciale beheersmaatregelen vereist zijn om de beschikbaarheid van de netwerkfuncties en aangesloten computers te handhaven;
- om acties die van invloed kunnen zijn op of relevant zijn voor de informatiebeveiliging te kunnen vastleggen en opzorgen behoren passende maatregelen voor registreren en monitoren te worden toegestaan;
- beheeractiviteiten behoren na zij gezet te worden gecoördineerd, zowel om de dienstverlening voor de organisatie te optimaliseren als om te waarborgen dat beheersmaatregelen consistent is de hele informatieverwerkende infrastructuur worden toegepast;
- systemen in het netwerk behoren te worden geauthenticeerd;
- er behoort een beperking te gelden voor het aantal systemen dat met het netwerk verbonden is.

C.1.7.2 Beveiliging van netwerkdiensten

Beheersmaatregel

Beveiligingsmaatregelen, dienstverleningsniveau's en beheersniveaus voor alle netwerkdiensten behoren te worden gaderfiliseerd en opgenomen in overeenkomstig bestrijdende netwerkdiensten. Dit geldt zowel voor diensten die intern worden geleverd als voor uitbestede diensten. (ISO 13.1.2)

Implementatierichtlijn

De kundigheid van de aanbieder van de netwerkdienst om de overeengekomen diensten veilig te behalen behoeft te worden vastgesteld en regelmatig te worden gemonitord, en het recht om een audit uit te voeren behoort te worden overeengekomen.

De beveiligingsprocedures die nodig zijn voor bepaalde diensten, zoals beveiligingskenmerken, dienstverleningsniveau's en beheersniveaus, behoren te worden vastgesteld. De organisatie behoort ervoor te zorgen dat aanbieders van netwerkdiensten deze maatregelen implementeren.

C.1.7.3 Scheiding in netwerken

Beheersmaatregel

Groepen van informatiediensten, -gebruikers en -systemen behoren in netwerken te worden gescheiden. (ISO 13.1.3)

Implementatierichtlijn

Een van de methodes om de beveiliging van grote netwerken te beheren is ze te verdelen in geïsoleerde netwerkdomeinen. De domeinen kunnen worden gedefinieerd op basis van bijvoorbeeld aard van de dienst (bijv. openbaar toegankelijk domein, bureaubladdomein, serverdomein), naast organisatieafdelingen (bijv. personeelzaken, financien, marketing) of een combinatie (bijv. subdomeinen verbonden met meerdere afdelingen van de organisatie). Die scheiding kan tot stand worden gebracht door hetzij fysiek verschillende netwerken, hetzij verschillende logische netwerken te gebruiken (bijv. virtueel particulier netwerken).

De perimeter van elk domein behoort goed te worden gedefinieerd. Toegang tussen externe domeinen is toegelaten maar behoort bij de perimeter te worden beheerd door een gateway te gebruiken (bijv. een firewall, een filterende router). De criteria voor het scheiden van netwerken in domeinen, en de toegang die via de gateways wordt toegestaan, behoren te worden gebaseerd op een beoordeling van de beveiligingsrisico's voor elk domein. De beoordeling behoort in overeenstemming te zijn met het toegangsbeveiligingsbeleid (zie ISO 9.1.1), de toegangsrisico's, waar de een classificatie van verwachte informatie en behoort ook rekening te houden met de relatieve kosten en de gevolgen voor de prestaties van het integreren van gatewaytechnologie.

Draadloze netwerken vereisen een speciale behandeling in verband met de slecht gedefinieerde rekenprestaties. Voor gevoelige omgevingen behoort te worden overwogen om elke draadloze toegang te behandelen als externe verbinding en om deze toegang te scheiden van interne netwerken totdat de toegang een gateway is geïmplementeerd in overeenstemming met het netwerkbeveiligingsbeleid (zie ISO 13.1.1), waarop de toegang tot interne systemen wordt vasteld.

De authenticatie, oordeling en technologië van een netwerktoegang beveiliging voor het gebruikers niveau van netwerken, op netwerken gebaseerde draadloze netwerken zijn, kunnen correct geïmplementeerd, mogelijk voldoende voor directe verbinding met het interne netwerk van de organisatie.

C.3.8. Toegang tot netwerken en netwerkdiensten

Beheersmaatregel

Gebruikers behoren alleen toegang te krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn. (ISO 9.1.2)

Implementatierichtlijn

Een beleid voor het gebruik van netwerken en netwerkdiensten behoort te worden geformuleerd. Dit beleid behoort te omvatten:

- de netwerken en netwerkdiensten waartoe toegang wordt verleend;
- autorisatieprocedures om vast te stellen wie toegang krijgt tot welk netwerk en welke netwerkdiensten;
- beheersmaatregelen en -procedures om de toegang tot netwerkverbindingen en -diensten te beschermen;
- de middelen die worden gebruikt om toegang te krijgen tot netwerken en netwerkdiensten (bijv. VPN of draadloos netwerk);
- elven voor gebruikersauthenticatie voor de toegang tot de verschillende netwerkdiensten;
- monitors van het gebruik van netwerkdiensten.

Het beleid voor het gebruik van netwerkdiensten behoort aan te sluiten bij het toegangsbeveiligingsbeleid van de organisatie (zie ISO 9.1.1).

C.3.9. Toegangsbeveiliging van systemen en toepassingen

Doelstelling: Onbevoegde toegang tot systemen en toepassingen voorkomen. (ISO 9.4)

G.3.2.4 Beperking toegang tot informatie

Beheersmaatregel

Toegang tot informatie en systeemfuncties van toepassingen behoort te worden beperkt in overeenstemming met het beleid voor toegangsbeveiliging. (ISO 9.4.1)

Implementatierichtlijn

Toegangsheperkingen behoren te worden gebaseerd op eisen voor de afzonderlijke bedrijfsapplicaties en in overeenstemming met het beleid dat voor toegangsbeveiliging is gedefinieerd.

De volgende aspecten behoren in aanmerking te worden genomen om de eisen voor toegangsbeveiliging te ondersteunen.

- a) men's verschaften om de toegang tot systeemfuncties van toepassingen te beheersen;
- b) beheersen welke gegevens voor een bepaalde gebruiker toegankelijk zijn;
- c) toegangsrechten van gebruikers beheersen, bijv. lezen, schrijven, verwijderen en uitvoeren;
- d) toegangsrechten voor andere toepassingen beheersen;
- e) de informatie in output beperken;
- f) zorgen voor fysieke of logische toegangbeveiligingsmaatregelen voor het opslaan van gevoelige toepassingen, toepassingsgegevens of systemen.

C.8.9.2 Beveiligde inlogprocedures

Beheersmaatregel

Indien het beleid voor toegangsbeveiliging dit vereist, behoort toegang tot systemen en toepassingen te worden beheerd door een beveiligde inlogprocedure (ISO 9.4.2).

Implementatierichtlijn

Om de geïdentificeerde identiteit van een gebruiker te bewijzen behoort een passende authenticatietechniek te worden gekozen.

In geval van enige verificatie en authenticatie van de identiteit is vereist behoren andere authenticatiemethoden dan wachtwoorden te worden gebruikt, zoals cryptografische middelen, chipkaarten, tokens of biommetrische middelen.

De procedure om in een systeem in te loggen behoort zo te worden ontworpen dat de kans op onbevoegde toegang zo klein mogelijk wordt gemaakt. Om te voorkomen dat het een onbevoegde gebruiker gemakkelijk wordt gemaakt behoort de inlogprocedure zo min mogelijk informatie over het systeem of de toepassing openbaar te maken. Een goede inlogprocedure behoort:

- a) geen systeem- of toepassingscrashfuncties te maken voordat het inlogproces met succes is afgerond;
- b) een algemeen waarschuwing te tonen die de computer alleen toegankelijk is voor bevoegde gebruikers;
- c) tijdens de inlogprocedures geen helpboodschappen weer te geven waarmee onbevoegde gebruikers hun domeinnummer lossen;
- d) de informatie die pas na invoer van alle gegevens te valideren. Indien zich een fout voordoet, behoort het systeem niet aan te geven welke deel van de gegevens juist of onjuist is;
- e) bescherming te bieden tegen inlogpogingen die met grove middelen worden uitgevoerd;
- f) niet-succesvolle en succesvolle pogingen te registreren;
- g) een informatiebeveiligingsgebeurtenis te initiëren als een poging tot of een succesvolle scheidend van de inlogbeheersmaatregelen is vastgesteld;
- h) de volgende informatie te tonen nadat het inloggen met succes is voltooid.
 - 1) datum en tijdstip waarop de vorige keer met succes is ingelogd
 - 2) details van niet-succesvolle pogingen om in te loggen sinds de vorige succesvolle poging om in te loggen;
- i) een wachtwoord dat wordt ingevoerd niet weer te geven;

j) geen ongecodeerde wachtwoorden via een netwerk te versuren;

k) inactieve sessies na een bepaald tijd van inactiviteit te beëindigen, vooral op locaties met een hoog risico, zoals openbare of exams locaties die buiten het beveiligingsgebied van de organisatie vallen, of op mobiele apparaten;

l) de verblijfsduur te beperken om extra beveiliging te bieden voor toepassingen met een hoog risico en de mogelijkheden voor onbevoegde toegang te verminderen.

C.8.9.3 Systeem voor wachtwoordbeheer

Beheersmaatregel

Systemen voor wachtwoordbeheer behoren interactief te zijn en sterke wachtwoorden te waarborgen (ISO 9.4.3);

Implementatienotities

Een systeem voor wachtwoordbeheer beheert:

- het gebruik van individuele gebruikersidentificaties en wachtwoorden af te dwingen om de toerekenbaarheid te handhaven;
- gebruikers de mogelijkheid te bieden hun eigen wachtwoord te kiezen en te wijzigen, en een bevestigingsprocedure te bevatten die rekening houdt met foutieve invoer;
- de keuzes voor sterke wachtwoorden af te dwingen;
- gebruikers te dwingen hun wachtwoord bij het eerste inloggen te wijzigen;
- wijziging van het wachtwoord periodiek en telkens wanneer dat nodig is af te dwingen;
- een registratie van eerder gebruikte wachtwoorden bij te houden en te voorkomen dat deze opnieuw worden gebruikt;
- wachtwoorden niet op het scherm te tonen als ze worden ingevoerd;
- wachtwoordbestanden apart van systeemgegevens van toepassing op te slaan;

C.8.9.4 Speciale systeemhulpmiddelen gebruiken

Beheersmaatregel

Het gebruik van systeemhulpmiddelen die in staat zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen behoort te worden beperkt en nauwkeurig te worden gecontroleerd. (ISO 9.4.4)

Implementatienotities

Voor het gebruik van systeemhulpmiddelen die in staat zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen dienen de volgende notities te worden overwogen:

- gebruik van identificatie-, authenticatie- en autorisatieprocedures voor systeemhulpmiddelen;
- scheiding van systeemhulpmiddelen en toepassingssoftware;
- beperking van het gebruik van systeemhulpmiddelen tot het laagste aantal herbruikbare beveiligde gebruikers die praktisch haalbaar is (zie ISO 9.2.3);
- auditatie voor ad-hergebruik van systeemhulpmiddelen;
- beperking van de beschikbaarheid van systeemhulpmiddelen, bijv. voor de duur van een operationele wijziging;
- registreren van alle gebruik van systeemhulpmiddelen;
- definieren en documenteren van autorisatievraagstukken voor systeemhulpmiddelen;
- verwijderen of onbruikbaar maken van alle onnodige systeemhulpmiddelen.

i) niet beschikbaar stellen van systeembijstandsmiddelen aan gebruikers die toegang hebben tot vertrouwelijke systemen waarbij scheiding van taken vereist is.

C.3.9.5 Toegangsbeveiliging op programmacode

Beheersmaatregel

Toegang tot de programmacode behoort te worden beperkt. (ISC 9.4.5)

Implementatierichtlijn

Toegang tot programmacodes en samenhangende items (zoals ontwerpen, specificaties, verificatie- en validatieschema's) behoort strikt te worden beheerd om de introductie van onbevoegde functionaliteit en onbedoelde wijzigingen te voorkomen, alsmede om de vertrouwelijkheid van waardevolle intellectuele eigenschappen te handhaven. Het bereik van de programmacode kan dit worden bereikt door de code gecontroleerd centraal op te slaan, bijvoorbeeld in de broncodebibliotheek. De volgende richtlijnen behoren aan te worden overwogen om de toegang tot opeengepakte broncodebibliotheeken te beheersen en de kans op corruptie van computaprogramma's te verkleinen:

- waar mogelijk, behoren broncodebibliotheeken niet in operationele systemen te worden opgeslagen;
- de programmacode en de broncodebibliotheek beheert te worden beheerd in overeenstemming met vastgestelde procedures;
- ondersteund personeel behoort geen onbeperkte toegang tot broncodebibliotheeken te hebben;
- het updaten van broncodebibliotheeken en samenhangende items en het verstrekken van broncodes aan programmeurs behoort alleen plaats te vinden na ontvangst van een passende autorisatie;
- programma-licenties behoren in een beveiligde omgeving te worden bewaard;
- van elke toegang tot broncodebibliotheeken behoort een auditlogbestand te worden bijgehouden;
- ontdoeken en kopiëren van broncodebibliotheeken beheert aan strikte procedures voor wijzigingbeheer te worden onderworpen (zie ISO 14.2.2).

Indien het de bedoeling is dat de programmacode wordt gepubliceerd behoren aanvullende beheersmaatregelen die bijdragen aan het waarborgen van de integriteit ervan (bijv. een digitale handtekening) te worden overwogen.

C.9. Beheer van informatiebeveiligingsincidenten

C.9.1. Beheer van informatiebeveiligingsincidenten en -verrekeningen

Duidelijkheid: Een uitsluitend en doelgerichte aanpak bewerkstelligen van het beheer van informatiebeveiligingsincidenten, met inbegrip van communicatie over beveiligingsgebeurtenissen en zwakte punten in de beveiliging. (ISO 16.1)

C.9.1.1. Verantwoordelijkheden en procedures

Echeersmaatregel

Directieverantwoordelijkheden en -procedures behoren te worden vastgesteld om een snelle, doelgerichte en ordelijke respons op informatiebeveiligingsincidenten te bewerkstelligen. (ISO 16.1.1)

Implementatierichtlijn

Met betrekking tot het beheer van informatiebeveiligingsincidenten behoren de volgende richtlijnen voor directieverantwoordelijkheden en -procedures in overweging te worden genomen:

- a) er behoren directieverantwoordelijkheden te worden vastgesteld om te bewerkstelligen dat de volgende procedures adequaat bij de organisatie worden aangenomen en geïmplementeerd:
 - 1) procedures voor incidentresponsplanning en -voorbereiding;
 - 2) procedures voor het monitoren, opsporen, analyseren en rapporteren van informatiebeveiligingsgebeurtenissen en -incidenten;
 - 3) procedures voor de vastlegging van beheersactiviteiten betreffende incidenten;
 - 4) procedures voor het omgaan met forensisch bewijs;
 - 5) procedures voor het beoordelen van en besluitvorming over informatiebeveiligingsgebeurtenissen en beoordeling van schadeplekken in de informatiebeveiliging;
 - 6) responsprocedures met inbegrip van procedures voor escalatie, beheerd herstel van een nootdient en communicatie aan in- en extern personeel of organisaties.
- b) vastgestelde procedures behoren te bewerkstelligen dat:
 - 1) competent personeel de kwesties behandelt die verband houden met informatiebeveiligingsincidenten binnen de organisatie;
 - 2) een contactpunt voor het opsporen en rapporteren van beveiligingsincidenten wordt geïmplementeerd;
 - 3) passende contacten worden onderhouden met instanties, externe belangengroepen of fora die zangerepitheden behandelen die verband houden met informatiebeveiligingsincidenten.
- c) rapportageprocedures behoren de volgende aspecten te omvatten:
 - 1) formulieren voorbereiden voor het rapporteren van informatiebeveiligingsgebeurtenissen ter ondersteuning van de rapportage en om te beoordelen dat de rapportagepersoon aan alle nodige zaken streeft die in geval van een informatiebeveiligingsgebeurtenis moeten worden vermeld;
 - 2) de procedures die in geval van een informatiebeveiligingsgebeurtenis moeten worden uitgevoerd, bijv. onmiddellijk alle details noteren, zoals aard van niet-naleving of overtreding, optredende schade, toediening op het scherm, en onmiddellijk rapporteren aan het contactpunt om alleen gecoördineerde actie ondernemen;
 - 3) verwijzing naar een vastgestelde disciplinaire formele procedure voor het omgaan met medewerkers die beveiligingsovertredingen begaan;
 - 4) passende feedbackprocedures om te bewerkstelligen dat de personen die informatiebeveiligingsgebeurtenissen melden, worden geïnformeerd over de resulterende maatregelen die worden genomen en afgesloten.

De doelstellingen voor het beheer van informatiebeveiligingsincidenten, behoren met de directie te worden overeengekomen en er behoort te worden gewaarborgd dat de personen die verantwoordelijk zijn voor het beheer van informatiebeveiligingsincidenten op de hoogte zijn van de prioriteiten van de organisatie voor het behandelen van informatiebeveiligingsincidenten.

C.9.1.2 Rapportage van informatiebeveiligingsgebeurtenissen

Beheersmaatregel

Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende n verast te worden gerapporteerd. (ISO 16.1.2)

Implementatieplichtlijn

Alle medewerkers en contractanten behoren bewust te worden gemaakt van hun verantwoordelijkheid om informatiebeveiligingsgebeurtenissen zo snel mogelijk te rapporteren. Zij behoren ook te worden geïnformeerd over de procedure voor het rapporteren van informatiebeveiligingsgebeurtenissen en het contactpunt waaraan de gebeurtenissen behoren te worden gerapporteerd.

Met betrekking tot het rapporteren van informatiebeveiligingsgebeurtenissen behoort rekening te worden gehouden met de volgende situaties:

- a) niet-doelgerichte beveiligingsbeheersmaatregelen;
- b) schending van informatie-integriteit, vertrouwelijkheid of aanwezige verwachtingen;
- c) menselijke fouten;
- d) niet-naleving van beleidsregels of richtlijnen;
- e) schending van fysieke beveiligingsregelingen;
- f) onbeheerste systeemveranderingen;
- g) storingen in sort- of hardware;
- h) overtredingen van de toegangsregeling.

C.9.1.3 Rapportage van zwakke plekken in de informatiebeveiliging

Beheersmaatregel

Van medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten van de organisatie behoort te worden geëist dat zij die te systemen of diensten waargenomen of vermeende zwakke plekken in de informatiebeveiliging registreren en rapporteren. (ISO 16.1.3)

Implementatieplichtlijn

Alle medewerkers en contractanten behoren deze zaken zo snel mogelijk aan het contactpunt te rapporteren om informatiebeveiligingsincidenten te voorkomen. Het rapporteringsmechanisme behoort zo eenvoudig, toegankelijk en beschikbaar te zijn als mogelijk is.

C.9.1.4 Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen

Beheersmaatregel

Informatiebeveiligingsgebeurtenissen behoren te worden beoordeeld en er behoort te worden goedgekeurd of zij moeten worden geassocieerd als informatiebeveiligingsincidenten. (ISO 16.1.4)

Implementatieplichtlijn

Het contactpunt behoort elke informatiebeveiligingsgebeurtenis te beoordelen op basis van het overeengekomen classificatieschema voor gebeurtenissen en incidenten betreffende informatiebeveiliging, en te besluiten of de gebeurtenis behoort te worden geclassificeerd als informatiebeveiligingsincident. Classificeren en prioriteren van incidenten kan helpen de impact en omvang van een incident te bepalen.

In gevallen waarin de organisatie beschikt over een mechanisme voor informatiebeveiligingsincidenten (SIRT/SODC), kunnen de beoordeling en het besluit hier naar worden doorgevoerd voor bevestiging of herbeoordeling.

Resultaten van de beoordeling an het besluit behoren in detail te worden vastgelegd toe behoeve van toekomstige verwijzing en verificatie.

C.3.1.5 Respons op informatiebeveiligingsincidenten

Beheersmaatregel

Op informatiebeveiligings incidenten behoort te worden gereageerd in overeenstemming met de gedocumenteerde procedures. (ISO 18.1.9)

Implementatierichtlijn

Op informatiebeveiligings incidenten behoort te worden gereageerd door een aangewezen contactpunt en andere relevante personen van de organisatie of externe partijen (zie ISO 18.1.1).

De respons behoort de volgende aspecten te omvatten:

- zo snel mogelijk de gebeurtenis bewijs verzamelen;
- in de eerste plaats, een eerste analyse van de informatiebeveiliging uitvoeren (zie ISO 16.1.7);
- escaleren indien vereist;
- bewerkstelligen dat alle betrokken responsactiviteiten op de juiste manier worden vastgelegd voor latere analyse;
- het bestaan van het informatiebeveiligingsincident; of relevante details daarvan communiceren aan andere in- en externe personen of organisaties met een 'need-to-know';
- beheerders van de zwakke plekken in de informatiebeveiliging waarvan is vastgesteld dat deze het incident heeft/ hebben veroorzaakt; of eraan heeft/ hebben bijgedragen;
- het incident formeel afsluiten en vastlegging bijhouden zodra het incident met succes is behandeld.

Om de bron van het incident te identificeren behoort postincidentanalyse plaats te vinden.

C.3.1.6 Lering uit informatiebeveiligingsincidenten

Beheersmaatregel

Kennis die is verkregen door informatiebeveiligingsincidenten te analyseren en op te lossen behoort te worden gebruikt om de waarschijnlijkheid of impact van toekomstige incidenten te verkleinen. (ISO 18.1.6)

Implementatierichtlijn

Er behoren mechanismen te zijn ingesteld waarmee de aard, omvang en kosten van informatiebeveiligingsincidenten kunnen worden gekwantificeerd en gemiddeld. De informatie die is verkregen uit de evaluatie van informatiebeveiligingsincidenten behoort te worden gebruikt om terugkerende of ingrijpende incidenten te identificeren.

C.3.1.7 Verzamelen van bewijsmateriaal

Beheersmaatregel

De organisatie behoort procedures te definiëren en toe te passen voor het identificeren, verzamelen, verkrijgen en bewaren van informatie die als bewijs kan dienen. (ISO 18.1.7)

Implementatierichtlijn

Rij het omgaan met bewijs ten behoeve van rechtstreekse en wettelijke actie behoren interne procedures te worden ontwikkeld en gevolgd.

In het algemeen behoren deze bewijsprocedures processen in te houden voor het identificeren, verzamelen, verkrijgen en bewaren van bewijs in overeenstemming met de verschillende soorten media, apparaten en de status van de apparaten, bijv. in- of uitgeschakeld. De procedures behoren rekening te houden met de:

- bewakingsketen;

- b) volledigheid van bewijs;
- c) volledigheid van personeel;
- d) relatie en verantwoordelijkheid van het betrokken personeel;
- e) competentie van personeel;
- f) documentatie;
- g) interactie

Indien beschikbaar, behoren certificatie of andere relevante methoden om personeel en middelen te kwalificeren te worden gezocht om de waarde van het volkroon bewijs te verbeteren.

Forensisch bewijs kan grenzen van organisaties of rechtsgebieden overschrijden. In zulke gevallen behoort te worden gewaarschuwd dat de organisatie het recht heeft de wereld informatie als forensisch bewijs te verzamelen. De eisen van verschillende rechtsgebieden behoren ook in aanmerking te worden genomen om de kans zo groot mogelijk te maken dat het bewijs wordt toegelaten in de relevante rechtsgebieden.

C.10. Informatiebeheer

Deelstelling

Informatiebeheer omvat en beheert bedrijfsprocessen op functioneel niveau en verleent operationele ondersteuning aan gebruikers ten behoeve van een betrouwbare informatievoorziening.

Toelichting

Bedrijfsprocessen worden zodanig ontworpen dat de opgeleverde bedrijfsdiensten aan beveiligingsaspecten voldoen en dat voor belanghebbenden bij dit proces voldoende transparantie en bestuurbaarheid geboden wordt. Het voorontwerpingsproces van een product wordt ingezet in fase 1 in elke fase worden producten opgeleverd, zoals geactualiseerde opdrachtenportefolio, globaal en detail ontwerp.

Motivering

In het proces informatiebeheer worden vanuit de bedrijfsactiviteit (de "business") eisen voor beveiliging van de bedrijfsprocessen vastgesteld en bij de voorwaarden geschapen voor het opzetten van geprogrammeerde controles in applicaties (application controls) en daarop aansluitende analyseketen van ADRD (user controls) in de handvatte delen van de proceseisen. Voorts wordt in dit proces centraal voor de organisaie vastgesteld welke informatie onder welke beveiligingsvoorwaarden wordt uitgewisseld met andere organisaties.

Afbakening

De normer in deze paragraaf hebben betrekking op bedrijfsprocessen en de daarbij ondersteunende applicaties. De normen van de paragrafen C.10.1 tot en met C.10.2 betreffen functioneel ontwerp en implementatie. C.10.2 Kwaliteitsbeheer zijn zoveel mogelijk algemeen geformuleerd, zodat deze ook gebruikt kunnen worden voor het functioneel ontwerp en de implementatie van de technische infrastructuur.

C.10.1. Sturen functioneel ontwerp en implementatie

Beheersmaatregel

Het informatiebeheer kan voldoende sturing geven aan het functioneel ontwerp, onderhoud en implementatie van IT-voorzieningen.

Implementatiecriteria

- Er zijn criteria vastgesteld op grond waarvan voor de besturing van vernieuwing en onderhoud een aparte projectorganisatie wordt ingesteld. Deze criteria kunnen betrekking hebben op het middelenbestel, aantal betrokken organisatiedelen, gebruik nieuwe technologie e.d.
- Er zijn criteria vastgesteld op grond waarvan projecten niet te omvangrijk worden (daarmee slecht bestuurbaar) en op grond waarvan er met deelprojecten wordt gewerkt.
- In geval een aparte projectorganisatie noodzakelijk wordt geacht, wordt een stuurgroep ingesteld met vertegenwoordigers van alle belanghebbende (in- en externe) organisatiedelen met voldoende mandaat om over de inhoud en voortgang te beslissen.
- Er zijn criteria opgesteld op grond waarvan verplicht advies wordt ingewonnen van beveiligingsadviseurs, faseproducten daarvan worden gereviseerd en onafhankelijke beveiligingsbeoordeling plaatsvindt (bijv. door in- of externe IT-auditoren) bij de onderscheiden faseproducten.
- Het management van het ontwerpproces maakt afspraken naar het tijdstip en onafhankelijk toetsen van geplande faseproducten aan beveiligingsnormen en het rapporteren daarvan.
- De besluitvorming over acceptatie van faseproducten vindt op voldoende hoog managementniveau plaats.
- Het detailontwerp, op grond waarvan realisatie plaatsvindt wordt goedgekeurd door representatieve vertegenwoordigers van gebruikers, functioneel en technisch beheerders op basis van testrapporten en op basis van aspecten van kwaliteitsbeheer (zie C.10.2.)
- Er is functiescheiding tussen gebruikers, functionele ontwerpers, technische ontwerpers en bouwers en exploitatiedeskundigen.

C.10.2. Kwaliteitsbehoor

Beheersmaatregel

De kwaliteitseisen voor het ontwerpen en onderhouden van processen en IT-voorzieningen zijn vastgesteld en worden intern bewaakt op naleving.

Implementatierichtlijn

- Hier: ontwerp en de realisatie wordt volgens standaard Method, Technieker, Hulpmiddelen en Voorschriften (MTHV's) uitgevoerd.
- De MTHV's bevatten een inventarisatie van risico's voor het slagen van het project, waarin aandacht wordt besteedt aan risico's (kwaliteit, risico's voorwaarden, beperkingen, ervaring met toe te passen procesmatige, organisatorische en technische vernieuwingen).
- De MTHV's geven aan wie welke mijlpastproducten oplevert en wie deze goedkeuren voordat en naar een volgende fase overgaat.
- De MTHV's bevatten acceptatiecriteria voor gangbare aspecten als COPAFIITH of P10FACH inclusief bepalingen i.c. de productnormen volgens de paragrafen **Fout! Verwijzingsbron niet gevonden.** asedocumenten en IT-voorzieningen, evenals de procesnormen C.11.1 Procesinrichting en C.11.4 rapporteren voor het proces als het gaat om het ontwerpen van processen.
- Afwijkingen van de opdracht, uitgangsdokumentatie, kaders en aanvullende afspraken worden gemeld in de opgeleverde fase-documenten.
- De fase-documenten worden bewaard eveneens volgens de vastgestelde bewaartermijnen.
- Er is een systeem van onafhankelijke kwaliteitsbeoordeling ter borging van de standaard MTHV's.
- Over de resultaten van de kwaliteitsbeoordeling wordt gerapporteerd aan het project- en informatie management.
- De standaard MTHV's worden periodiek geëvalueerd met alle betrokkenen en zo nodig bijgesteld.

C.10.3. Fase-documenten ontwerp en invoering IT

Deelstelling

Fase-documenten voor het ontwerp en invoeren van Tischeppet de voorwaarden voor een betrouwbare informatieverwerking, voor zover dat afhankelijk is van IT-voorzieningen.

C.10.3.1 Beveiligingsparagraaf procesontwerp

Beheersmaatregel

In de faseproducten van het ontwerp en ontzoud van processen en applicaties wordt in een beveiligingsparagraaf aangegeven op welke wijze de normen voor beveiliging zijn geïmplementeerd.

Implementatierichtlijn

- Er wordt een beveiligingsparagraaf in de fase-documenten opgenomen, waarbij de hierna volgende richtlijnen – per fase in toenemende mate van detail – worden uitgewerkt.
- In een zo vroeg mogelijk ontwerpfase wordt vastgesteld:
 - of er sprake is van afwijkingen van het basis beveiligingsniveau;
 - of er door of aan derden beveiligingsplekken worden gesteld i.v.m. externe insourcing of uitbesteding van primaire- en/of secundaire taken;
 - of de bestaande beveiligingsplekken en de –maatregelen aanpassing behoeven door nieuwe ontwikkelingen op het gebied van technologie dan wel ander gebruik daarvan;
 - of er sprake is van de specifieke beveiligings- of conversieproblematiek.
 Bij afwijkingen wordt advies gevraagd aan beveiligingsfunctionarissen.
- Er zijn criteria opgesteld op grond waarvan een risicoanalyse wordt toegepast, die mede richtinggevend is voor de implementatie van de beveiligingsmaatregelen. Criteria zijn onder meer:

geheel nieuwe processen van significante betekenis, tevens samenwerking bij primaire processen, gebruik nieuwe technologie of aan te schaffen, nieuwe T-voorzieningen al dan niet met bekende leverbaarheden

d) Wanneer applicaties met een hoger beveiligingsniveau naar gemeenschappelijke omgeving worden uitbevoord, worden de applicaties waartoe de zone in de technische infrastructuur wordt gedeeld, vastgesteld en geïdentificeerd door de procesbeheerder van die applicatie

e) Geaccepteerde (test)resultaten worden expliciet vastgelegd met een motivering waarom hiervoor (nog) geen beveiligingsmaatregelen worden getroffen

f) Er is vastgesteld of de uitgangspunten van de bedrijfscontinuïteitsplannen nog van toepassing zijn in de nieuwe of gewijzigde situatie. Het betreft:

1. de maximale toevallbare uitvoerder (MTU);
2. het maximale toegestaan digitaal gegevensverlies (MCSV);
3. aanvullende maatregelen die 1 en 2 niet geheel met de beschikbaarheid van Beteren en Flexibiliteit IT-voorzieningen worden ingewikkeld;
4. reconstructie naar digitale informatie.

g) Er wordt vastgesteld of voldaan moet worden aan het midden van de privacyaspecten aan de privacyfuncties.

h) Het verwerken van informatie aan andere informatiesystemen en derden voldoet aan het deeringbeginsel voor de privacybescherming.

i) De bewaartijden van informatiebronnen en registraties (papier, digitaal) zijn vastgesteld in een bewaarschema

j) Maatregelen van beveiliging worden getroffen op basis van de paragrafen 4.11.1 -roebesnoering, C.11.4 Rapporteren over het proces.

C.10.3.2 Implementatieplan processen en applicaties

Beheersmaatregel

Bij de invoering van nieuwe of gewijzigde processen en applicaties wordt een implementatieplan gemaakt.

Implementatierichtlijn

a) In het implementatieplan worden de volgende onderdelen uitsgewerkt:

1. benodigde mens- en middelen capaciteit voor de invoering bij alle betrokken partijen;
2. voorlichting en training in het gebruik van het informatiesysteem;
3. conversietraject;
4. interim controle bij conversie van gegevens op de juistheid en volledigheid van de overgang van de oude naar de nieuwe gegevensbestanden;
5. continuïteit van de operationele werkzaamheden;
6. wijze waarop zo nodig kan terug worden gevallen op de oude situatie of op bijzondere hiervoor ontworpen hardmatige procedures (fall-back procedure);
7. welke overgangsmaatregelen moeten worden genomen voor, tijdens en na de invoering van de vernieuwde situatie
8. te ondernemen acties bij het uitlopen van de invoeringsplanning;
9. aansluiten van deskundige aanspreekpunten per betrokken organisatie ter ziele in behoefte van de afzakele voorbereiding, coördinatie, samenwerking en afstemming.

b) De impact en complexiteit van de realisatie van het stabiliteit alsmede van conversie- of migratieactiviteiten is beperkt voor de operationele invoering. De impactheden om terug te keren naar vorige situaties en de mate waarin wordt schadevrijheid als daar te mogelijkheden voor bestaan.

C.10.3.3 Beveiligingsparagraaf fase-documenten technische infrastructuur

Beheersmaatregel

In de beveiligingsparagraaf van de fase-documenten voor het ontwerp en de inrichting van IT-voorzieningen van de technische infrastructuur wordt de inrichting van de beveiliging gedomineerd in overeenstemming met externe en interne normen.

Toelichting

In een beveiligingsparagraaf van de fase-documenten voor het ontwerp en de inrichting van IT-voorzieningen van de technische infrastructuur wordt de inrichting van de beveiliging gedomineerd in overeenstemming met externe en interne normen. In de beveiligingsparagraaf kan worden volstaan met het – per fase in overeenstemming met de detail – verwijzen naar de desbetreffende binnen- en externe beveiligingsnormen als ze geen vertaaling nodig hebben, aangevuld met eventuele gemiddelde afwijkingen daarop.

Implementatie-richtlijnen

- a) In een zo vroeg mogelijk ontwerp stadium wordt vastgesteld:
1. in hoeverre of sprake is van afwijkingen van het basis beveiligingsniveau
 2. welke beleidsdocumenten en ontwerpportefolio van toepassing zijn;
 3. of de bestaande beveiligingsuitgangspunten den wel –maatregelen aanpassing behoeven door nieuwe ontwikkelingen op het gebied van technologie;
 4. in hoeverre de leveranciersinstructies voor het leverbaar van de opgevoerde beveiliging gebaseerd zijn op de facto beveiligingsrichtlijnen van erkende norminstellingen als NIST;
 5. in hoeverre er sprake is van de inwerking- en uitvoeringsproblematiek en welke oplossingsrichting wordt voorgestaan.
- b) In een risicoanalyse worden de specifieke eisen van de IT-voorziening in beschouwing genomen en de beveiligingsinrichting vastgesteld voor zover die niet (voldoende) is geadresseerd in de productiespecificaties van IT-voorzieningen en de facto beveiligingsrichtlijnen van erkende norminstellingen als NIST.
- c) Bij het uitvoeren van een risicoanalyse zijn ten minste de functioneel bedrijfsmiddelenbeheerder, mededeskundigen en beveiligingspecialisten betrokken.
- d) Geaccpteerde (redelijke) worden expliciet vastgelegd met een novering waaraan hiervoor geen beveiligingsmaatregelen worden getroffen.
- e) In de opgeleverde systeemdocumentatie wordt de beveiligingsparameterisering vastgelegd in overeenstemming met de leveranciersinstructies en de facto beveiligingsrichtlijnen van erkende norminstellingen als NIST.
- f) Voor IT-voorzieningen met een bijzonder belang voor de logische toegang tot de gegevens in de beveiligingsparagraaf aangegeven:
1. met welke frequentie en welke geautomatiseerde hulpmiddelen beveiligingsaanpak wordt gecontroleerd worden;
 2. welke type security validatie geïmplementeerd moeten worden met welke frequentie en welke tooling.
- In de signaleringen wordt onderscheid gemaakt naar signalen, die in de gebruikerorganisatie moeten worden afgehandeld en signalen die betrekking hebben op Technisch beheer en exploitatie;
3. welke uitgangspunten er worden gehanteerd voor de grepering van autorisatie opdat de dynamiek in IT-diensten, processen, functies en organisaties niet tot onaanvaardbare, extra orderinvoeringskosten kunnen leiden.
- g) De beveiligingsdocumentatie van IT-voorzieningen met een bijzonder belang voor de logische toegang tot gevoelige gegevens wordt gecontroleerd door factisch beveiligingsbeheer.

C.11. Algemeen beheer van handmatige processen

Algemeen procesbeheer bevat de normen voor het beheersen van de handmatige verwerking (de A/D/C), die per proces uitgewerkt wordt als exemplaren en aluitdruk op de geautomatiseerde processen en daarin opgenomen controles van wel als uitdruk d handmatig proces.

Toelichting

Het algemeen procesbeheer is in hoofdzaak op de integriteit van informatie gericht. De andere aspecten betrouwbaarheid en vertrouwelijkheid worden veelal geborgd door andere (specifieke) processen in dit normenkader. Het werkinggebied is ruimer dan van informatiesystemen, omdat in een proces meerdere (soms zelfs vele) informatiesystemen kunnen worden gebruikt.

Matvering

Het beheersen van processen in het algemeen is met name het handmatige deel daarin, is een randvoorwaarde voor het borgen van de procesmatige beveiligingsnormen en kan niet los daarvan worden beschouwd.

Afwakening

Deze normen zijn als aanvulling te beschouwen op elk in dit normenkader voorkomend proces. Ier voorkoming van het toelagen van deze normen als soort proces hier éénmalig beschreven.

C.11.1. Procesinrichting

Beheersmaatregel

Handmatige handelingen voldoen aan eisen van beveiliging.

Implementatierichtlijn

- Taken, bevoegdheid en verantwoordelijkheden van functies/rollen zijn actueel en volledig vastgesteld.
- Per proces/application is aangegeven welke taken/profelen onverenigbaar zijn uit hoofde van functiescheiding.
- Bij onvoldoende functie- of rolvervulling (bijvoorbeeld onvoldoende functiescheiding) worden compenserende maatregelen getroffen.
- Bij de procesinrichting is vastgesteld of er sprake is van gegevens, waarvoor extra maatregelen van beveiliging van toepassing zijn: er is hiervoor de volgende overweging geldend:
 - de analyse van de aspecten van vertrouwelijkheid, integriteit en beschikbaarheid;
 - wie toegang heeft tot het gebruiken of bewerken van de informatie;
 - op welke wijze de informatie wordt: ontvangen, vastgelegd, bewaard, verzonden en vernietigd moet worden.
- Plagiëren in voerdocumenten worden gecontroleerd op geautomatiseerde wijzigingen (voor alle wijzigingen in voerdocumenten wordt toestemming gegeven)
- Bij de uitvoering van voelbare opslagmedia of basisbechouden, die betrekking hebben voor de integriteit en/of vertrouwelijkheid van de gegevens(verwerking) met of van andere organisaties of organisatiedelen wordt gebruik gemaakt van de de platen waarop in totalen (partities, bestanden) de zending is aangegeven. Het verspreiden en ontvangen van deze platen gebeurt via spaarbeveiliging en wordt vastgelegd. De taken op de geleidelijk worden z.s.m. na ontvangst afgehandeld met de daadwerkelijk aangeleverde media/beschouwen.
- Signalen en foutboodschappen op grond van interne- en externeaanvragen worden juist, volledig en tijdig afgehandeld. Uit de vastleggingen blijkt wie welke posten wanneer heeft afgehandeld.
- Bij hoge risico-posten worden de ingevoerde gegevens op juistheid gecontroleerd.
- Bij gegevens met een bijzondere betekenis voor het proces wordt een periodieke beoordeling gedaan van de inhoud van sleutelvelden of gegevensbestanden om hun geldigheid en integriteit te bevestigen.

j) Intern opstane bronndocumenten, die alleen voor intern gebruik zijn bedoeld, zoals werkopdrachten, verwerkingsverslagen, mutatie- en signaallijsten worden minimaal twee jaar na afloop van het jaar waarin de opdrachten zijn afgeleverd bewaard ten behoeve van controleactiviteiten. Dit taal criterium doet er andere criteria kaarsen zijn en interne documenten langer te bewaren.

k) De distributie van uitvoerlijsten wordt vastgelegd.

l) Bij vervangings- of functieschijfregelingen worden de functieschijfregelingen niet doorbroken.

m) Bij nood- of escalatiegevallen mogen de functieschijfregelingen alleen worden doorbroken door de hogere managementlaag, waarbij dit aanvankelijk schriftelijk wordt vastgelegd. Na afloop van de calamiteit wordt een haastgelek van de uitvoering vastgesteld of er de gegevensverwerking niet gecompromitteerd is en of de functionaliteit redelijk ten volle hersteld is.

n) Als problemen, calamiteiten e.d. alleen opgelost kunnen worden door het tijdelijk openeten af voorstellen van beveiligingsmaatregelen, wordt dit geëdigd en door het verantwoordelijke management en worden aanvullende maatregelen getroffen. Door het maatregelen wordt toegezien op naleving van deze maatregelen.

G.11.2. Aansluiten operationele IT

Beheersmaatregel

Vastgesteld wordt dat de geautomatiseerde delen van het proces integraal worden gecontroleerd.

Toelichting

De onderdeel is ook extra te beschouwen als een productieroom voor het proces van het leveren van processen. De productieverantwoordelijkheid voor de inrichting kan een andere zijn dan die voor de procesverantwoordelijkheid voor de naleving.

Implementatiecriteria

- Uitgevoerd wordt vastgesteld dat de batchverwerkingen hebben plaatsgevonden volgens het draaiboek.
- Door verwerkingslijsten getoonde controlebepalingen worden gebruikt om vast te stellen dat de geautomatiseerde verwerking juist en volledig heeft plaatsgevonden. In voorkomende gevallen wordt vastgesteld dat de beginstand aansluit op de eindstand van de voorgaande verwerking en periodek dat oeffingen van gegevensverzamelingen aansluiten op de vanuit de mutaties opgekourde eindstanden.
- Bij bestandsuitwisseling met systeemvreemde omgevingen worden de bestanden van ontvangen en verzonden bestanden met de bronndocumenten (gelede lijsten, verwerkingsverslagen) afgestemd.
- Ver schillen die geautomatiseerd worden bij periodieke bestandsvergelijkingen worden tijdig geïdentificeerd en opgelost, waarbij structurele problemen aan informatie management worden doorgegeven.
- Uitvoerlijsten worden gecontroleerd op volledigheid.
- Verabalenparameters in tabellen van applicaties worden periodiek gecontroleerd.
- Er is functieschijfregeling tussen bestelling, invoer en periodieke controle van (wijzigingen van) variabelenparameters in tabellen van applicaties.

G.11.3. Verwerken gegevens op basis van vraagstukken

Beheersmaatregel

De gegevensverwerking op basis van vraagstukken (queries, business intelligence systemen) worden aan sluiten van beveiliging.

Implementatiecriteria

- Bij het verstrekken van informatie uit vraagstukken worden de uitgangspunten voor de logische toegangsbeveiliging en doeltreffendheid van de controle van privacybescherming niet doorbroken.
- Bij het samenstellen van programma's op basis van vraagstukken wordt ervoor zorggedragen dat door middel van controlebepalingen kan worden vastgesteld dat de juiste en volledige

gegevensverzameling wordt gebruikt, terzij daarover andere zekerheden bestaan. Controletellingen kunnen bijvoorbeeld aansluiten op eerder te lokaliseren volgens werkefficiëntieslagen. Jan wel op tellingen of saldo vanuit andere gegevensverzamelingen met aanvullende gegevens, zoals het streefdoel.

- c) De bij rapportier gebruikte statistieken worden terzij worden op het veranderingstrendslag weergegeven, benoemde controle op de juistheid van de verwerking achteraf mogelijk te maken.
- c) De controle op volledigheid en juistheid van de selectie door middel van vragenlijst vindt plaats in functie geschieden van de ontwikkeling en productie van de output.

C.11.4. Rapporteren over het proces

Beheersmaatregel

Op basis van rapportage vindt sluiting van het proces plaats.

Doelstelling

Dit onderdeel is ook extra te beschouwen als een productnorm voor het proces van het inlichten van processen. De productverantwoordelijkheid voor de afsluiting kan een andere zijn Jan die voor de procesverantwoordelijkheid voor de afsluiting.

Implementatierichtlijn

- a) Het proces wordt periodiek gerapporteerd over Key Performance Indicatoren (KPI's), onder andere over de naleving van de bereikingsnormen de voortgang van de jaarplanning en procesbeheersing.
- b) Naast de rapportage-trends gedurende de rapportageperiode, wordt er bij voorkeur ook een trendmatig overzicht over de huidige en daarmee voorafgaande periodes weergegeven.
- c) Bij gebruik van vragenlijsten is vermeld hoe deze zijn berekend en zijn gekwalificeerde begrippen omschreven.
- d) Afwijkingen ten opzichte van de norm of/of trendbreuken worden geanalyseerd en in de rapportage toegelicht, waarbij tevens wordt vermeld welke acties in gang zijn gezet om de procesgang naar het gewenste niveau terug te brengen.
- e) De juistheid en volledigheid van de gerapporteerde cijfers zijn controleerbaar.

C.11.5. Beheersen en evalueren van het proces

Beheersmaatregel

De opzet en uitvoering van het proces wordt intern beheerd en geëvalueerd.

Implementatierichtlijn

- a) Het proces wordt door onafhankelijke interne controleurs volgens een Intern Controle Programma controle op naleving van de normen van C.11 Algemeen beheer van handmatige processen uitgevoerd.
- b) De frequentie van de uitvoering van de interne controle wordt mede bepaald door risicoanalyse.
- c) De uitvoering van de interne controles wordt gepland en geregistreerd.
- d) Van de uitvoering en conclusies van de interne controle is een audit trail met bewijsstukken beschikbaar.
- e) Over de resultaten van de controlewerkzaamheden i.e. geconstateerde afwijkingen van de normen, wordt periodiek gerapporteerd aan het verantwoordelijk lijn- of procesmanagement.
- f) Over het tijdig oplossen van negatieve bevindingen worden afspraken gemaakt, voortgangsbewaking ingesteld en verantwoordelijkheid afgelegd.
- g) In het verslag of daarop gebaseerde conclusies worden de risico's van de afwijking van het proces nog opgemerkt. Daarvan kan een risicoanalyse, risicoanalyse, proces- of interne controlemaatregelen een bijdrage leveren. Verslagen tot verbetering worden doorgegeven aan de procesbeheerder.

C.12. Ontwikkelen van applicaties en informatiesystemen

C.12.1. Beveiligingszaken voor informatiesystemen

Doelstelling: Waarborgen dat informatiebeveiliging integraal deel uitmaakt van informatiesystemen in de gehele levenscyclus. Hiertoe behoren ook de eisen voor informatiesystemen die diensten verlenen via openbare netwerken (ISO 14.1)

C.12.1.1 Analyse en specificatie van informatiebeveiligingszaken

Beheersmaatregel

De eisen die verband houden met informatiebeveiliging behoren te worden opgenomen in de eisen voor nieuwe informatiesystemen of voor uitbreiding van bestaande informatiesystemen. (ISO 14.1.1)

Implementatierichtlijn

Informatiebeveiligingszaken behoren te worden vastgesteld met gebruikmaking van verschillende methoden zoals het identificeren van risico's, de eisen van beleid, de eisen van de organisatie, de dreiging en de oorzaken, de beoordelingen van voorval en het gebruik van kwetsbaarheidsrapporten. Resultaten van de identificatie behoren te worden gedocumenteerd en beoordeeld door alle belanghebbenden.

Informatiebeveiligingszaken en beheersmaatregelen behoren een afspiegeling te zijn van de waarde van de betrokken informatie voor het bedrijf (zie 8.2) en de potentiële schade voor het bedrijf als gevolg van een gebrek aan adequate beveiliging.

Het vaststellen en behouden van informatiebeveiligingszaken en samenhangende processen behoort te worden gerealiseerd in een vroeg stadium van informatiesysteempogingen. Vroegtijdige overweging van informatiebeveiligingszaken, bijv. in het ontwerp stadium, kan leiden tot oplossingen die doeltreffender en goedkoper zijn.

Met betrekking tot informatiebeveiligingszaken behoren ook de volgende aspecten in overweging te worden genomen:

- de vereiste mate van betrouwbaarheid ten opzichte van de beweende identiteit van gebruikers om authenticatie-eisen voor gebruikers af te leiden
 - procedures voor het verlenen van toegang en authenticatie, voor zakelijke en voor bevoorrechte of technische gebruikers
 - gebruikers en operators informeren over hun plichten en verantwoordelijkheden;
 - de vereiste beschermingsniveaus van de betrokken bedrijfsmiddelen, in het bijzonder met betrekking tot de beschikbaarheid, vertrouwelijkheid en integriteit;
 - eisen die zijn afgeleid van bedrijfsprocessen, zoals registreren en monitoren van transacties, eisen voor omwettelijkheid;
 - eisen die verplicht zijn gesteld door andere beheersmaatregelen met betrekking tot beveiliging, bijv. interfaces voor het registreren en monitoren of systemen voor het opsporen van lekken van gegevens.
- Voor toepassingen die diensten verlenen via openbare netwerken of die transacties implementeren, behoren de beheersmaatregelen ISO 14.1.2 en ISO 14.1.3 in overweging te worden genomen.
- Bij het kiezen van producten behoort een formele test- en acceptatieprocedure te worden gevolgd. In de contracten met de leverancier behoren de vastgestelde beveiligingszaken te zijn opgenomen. Als de beveiligingsfunctionaliteit in een voorgoed product niet voldoet aan de voorgeschreven eis,

behoren het geïntroduceerde risico en de daarmee samenhangende beheersmaatregelen te worden herovervogen voordat het product wordt gekocht.

Beschikbare eisenlijnen voor de beveiligingsconfiguratie van het product die in overeenstemming zijn gebruikt met de afsluitende softwareinvalidering van het systeem behoren te worden gevalideerd en geïmplementeerd.

Criteria voor het accepteren van producten behoren te worden gedefinieerd, bijv. in de zin van hun functionaliteit, met behoud van aandacht voor de zelfstandige beveiligingsaanpak. Voordat producten worden gekocht behoren ze te worden geëvalueerd tegen deze criteria. Om te waarborgen dat de producten geen onacceptabele extra risico's introduceren, behoren extra functionaliteit te worden beoordeeld.

C.17.1.2 Toepassingen op openbare netwerken beveiligen

Beheersmaatregel

Informatie die deel uitmaakt van uitvoeringsplannen en die via openbare netwerken wordt uitgeruild, behoort te worden beschermd tegen fraudeuze activiteiten, geschillen over contracten en onbevoegde openbaarmaking en wijziging. (ISO 14.1.2)

Implementatierichtlijn

Overwegings betreffende informatie beveiliging voor toepassingen die zich over openbare netwerken bewegen, behoren de volgende aspecten te behelzen:

- a) de mate van betrouwbaarheid die beide partijen oeken van elkaar bewaarde identiteit, bijv. via authenticatie;
- b) autorisatieprocedures voor wie de inhoud van belangrijke transacties of documenten mag goedkeuren, belangrijke transactiedocumenten te circuleren mag krijgen of mag ondertekenen;
- c) beveiligingen die communicatiepartners volledig zijn geïnformeerd over hun beveiligingsaanpak om de dienst te verschaffen of te gebruiken;
- d) vaststellen van en voldoen aan eisen ten aanzien van vertrouwelijkheid, integriteit, bewijs van verzending en ontvangst van belangrijke documenten en de onweerlegbaarheid van contracten, bijv. in samenhang met elektronische en contractuele ooverzichten;
- e) de vereiste mate van vertrouwen in de integriteit van belangrijke documenten;
- f) de eisen ten aanzien van bescherming van vertrouwelijke informatie;
- g) de vertrouwelijkheid en integriteit van ordertransacties, betalingsinformatie, gegevens betreffende afrekeningsadressen en ontvangstbewijzen;
- h) de mate van verificatie die passend is voor controle van betalingsinformatie die door een klant is verzocht;
- i) de keuze van de meest geschikte betalingsvorm ter bescherming tegen fraude;
- j) het vereiste beveiligingsniveau om de vertrouwelijkheid en integriteit van orderinformatie te handhaven;
- k) vermijding van verliezen van of vernieuwingsvermindering van transactie informatie;
- l) aansprakelijkheid in verband met frauduleuze transacties;
- m) eisen met betrekking tot verzekering.

Veel van bovengenoemde aspecten kunnen worden aangepakt door toepassing van cryptografische beheersmaatregelen (zie hoofdstuk ISO 10), waarbij rekening wordt gehouden met naleving van wettelijke eisen (zie hoofdstuk ISO 18, zie in het bijzonder ISO 18.1.5 voor wetgeving betreffende cryptografie).

Regeringen tussen partners betreffende toepassingen beheers te worden ondersteund door een schriftelijke overeenkomst die beide partijen bindt aan de overeengekomen voorwaarden van de diensten, met inbegrip van afschrijven over subsidies (zie bijvoorbeeld punt b).

Eisen betreffende wetgeving tegen aanvallen behoren te worden overwogen; hierbij kan worden gedacht aan eisen ten aanzien van de betrokken toepassingen van vers of het waarborgen van de beschikbaarheid van onderlinge netwerkoördinatie die nodig zijn om de dienst te leveren.

C.12.1.3 Transacties van toepassingen beschermen

Beheersmaatregel

Informatie die deel uitmaakt van transacties van toepassingen behoort te worden beschermd ter voorkoming van onvolledige overdracht, foutieve routing, onbevoegd wijzigen van berichten, onbevoegd openbaar maken, onbevoegd vermenigvuldigen of afspelen. (ISO 14.1.3)

Implementatierichtlijn

Overvegingen betreffende informatiebeveiliging voor transacties van toepassingen behoren de volgende aspecten te behezen:

- het gebruik van elektronische handtekeningen door alle partijen die bij de transactie betrokken zijn;
- alle aspecten van de transactie, d.w.z. waarborgen dat:
 - geheime authenticatie-informatie van gebruikers van alle partijen gelijkelijk en geheimhoudend is;
 - de transactie vertrouwelijk blijft;
 - de privacy van alle betrokken partijen behouden blijft;
- verslechting van de communicatiekanalen tussen alle betrokken partijen;
- beveiliging van protocollen die worden gebruikt om te communiceren tussen alle betrokken partijen;
- bevestigen dat de oorsprong van transactiegegevens zich buiten een publiek toegankelijke omgeving bevindt, bijv. op een opslagplatform op het intranet van de organisatie, en niet wordt bewaard en getoond op een opslagmedium dat dienst vanuit internet toegankelijk is;
- als een vertrouwde instantie wordt gebruikt (bijv. voor het uitgeven en onderhouden van digitale handtekeningen of digitale certificaten), beveiliging integreren en inbedden in het gehele beheersproces van certificaathandelingen.

C.12.2. Beveiliging in ontwikkelings- en ondersteunende processen

Dit keuring: Bevestigen dat informatiebeveiliging wordt ontworpen en geïmplementeerd binnen de ontwikkelingscyclus van informatiesystemen. (ISO 14.2)

C.12.2.1 Beleid voor beveiligd ontwikkelen

Beheersmaatregel

Voor het ontwikkelen van software en systemen behoren regels te worden vastgesteld en op ontwikkelaarsvelden binnen de organisatie te worden toegepast. (ISO 14.2.1)

Implementatierichtlijn

Beveiligd ontwikkelen is een eis voor het opbouwen van een beveiligde dienstverlening, architectuur, software en een beveiligd systeem. In een beleid voor beveiligd ontwikkelen behoren de volgende aspecten in overweging te worden genomen:

- beveiliging van de ontwikkelomgeving;
- richtlijnen betreffende beveiliging in de levenscyclus van softwareontwikkeling;

- 1) beveiliging in de softwareontwikkelmethodologie;
 - 2) beveiligde coderingsrichtlijnen voor elke programmeertaal die wordt gebruikt;
 - c) beveiligingsvragen in de ontwikkelingsfase;
 - d) beveiligingsvoorwaarden in de afleveringen van het product;
 - e) beveiligde informatiecentra;
 - f) beveiliging van de versiecontrole;
 - g) versie-informatie over toezichtingsbeveiliging;
 - h) het vermogen van de ontwikkelaar om kwetsbaarheid te vermijden, te vinden en te repareren.
- Technieken voor beveiligd programmeren behoren zowel te worden gebruikt voor nieuwe ontwikkelingen als in scenario's voor hergebruik van codes waarvan de normen die voor de ontwikkeling zijn toegepast niet bekend zijn of niet consistent waren met de huidige 'best practices'. Toepassing van beveiligde ontwikkelingsnormen behoort te worden overwogen en indien relevant verplicht te worden gesteld. Ontwikkelingsbehoeften worden getraind in het toezien van codering, en het gebruik behoort te worden geverifieerd door de testen en de codes te beoordelen.
- Indien ontwikkelactiviteiten worden uitbesteed behoort de organisatie zich ervan te vergewissen dat de externe partij deze regels voor veilig ontwikkelen naleeft (zie ISO 14.2.7).

C.12.2.2 Proceduren voor wijzigingsbeheer met betrekking tot systemen

Beheersmaatregel

Wijzigingen aan systemen tijdens de levenscyclus van de ontwikkeling behoren te worden beheerd door het gebruik van formele procedures voor wijzigingsbeheer. (ISO 14.2.2)

Implementatierichtlijn

Formele procedures voor wijzigingsbeheer behoren te worden gedocumenteerd en afgedwongen om de integriteit van het systeem, de toepassingen en producten te waarborgen, vanaf de vroegste ontwerpfase tot en met de laatste onderhoudsactiviteiten. De introductie van nieuwe systemen en belangrijke wijzigingen aan bestaande systemen behoort een formeel proces te volgen van documentatie, specificatie, testen, kwaliteitscontrole en bevestigde implementatie.

Dit proces behooft een risicobebodding, een analyse van de gevolgen van wijzigingen en een specificatie van de nodige beveiligingsvrijheidsmaatregelen te omvatten. Dit proces beoogt ook te waarborgen dat bestaande beveiligings- en beheersprocedures niet worden geïmponeerd, dat programmeurs die ondersteunende werkzaamheden uitvoeren alleen toegang krijgen tot die delen van het systeem die zij voor hun werkzaamheden nodig hebben en dat voor elke wijziging formele instemming en goedkeuring is verkregen.

Waar mogelijk behoren procedures voor wijzigingsbeheer voor toepassingssoftware en voor de operationele omgeving te worden getelegeerd (zie ISO 14.2.2). De procedures voor wijzigingsbeheer behoren te omvatten, maar niet beperkt te zijn tot:

- a) verslaglegging bijhouden van overeengekomen autorisatievragen;
- b) waarborgen dat wijzigingen worden uitgevoerd door bevoegde gebruikers;
- c) beheersmaatregelen en integriteitsprocedures beoordeelbaar om te waarborgen dat deze niet worden geïmponeerd door de wijzigingen;
- d) alle software, informatie, database en hardware identificeren die wijziging behoeven;
- e) beveiligingskritische codes identificeren en controleren om de waarschijnlijkheid van bekende zwakke punten in de beveiliging zo gering mogelijk te houden;
- f) formele goedkeuring voor geadresseerde voorstellen verkrijgen voor aanname van de werkzaamheden;

- g) waarborgen dat bevoegde gebruikers de wijzigingen voorafgaand aan implementatie beoordelen;
- f) waarborgen dat de systeemovername na elke wijziging wordt geïnstalleerd en dat alle documentatie wordt geactualiseerd of verwijderd;
- i) beschikbaar voor alle software-updates (kernen);
- j) een audittraject voor alle wijzigingsverzoeken bijhouden;
- k) waarborgen dat alle relevante documentatie (zie ISO 12.1.1) en gebruikersprocedures indien nodig worden gewijzigd om ze toepasbaar te houden;
- l) waarborgen dat het implementatieplan van wijzigingen op het juiste moment plaatsvindt en de betrokken bedrijfsprocessen niet verstoort.

C.12.2.3 Technische beoordeling toepassingen na wijzigingen bestuursplatform

Behersmaatregel

Als bestuursplatforms zijn veranderd, behoren bedrijfskritische toepassingen te worden beoordeeld en getest om te waarborgen dat er geen nadelige impact is op de activiteiten of de beveiliging van de organisatie. (ISO 14.2.3)

Implementatieplichtige

In deze procedure behoort te zijn opgenomen:

- a) beoordelen van procedures voor toepassingscontrole en integratie om te waarborgen dat ze niet zijn gecompromiteerd door de veranderingen aan het bestuursplatform;
- b) waarborgen dat notificatie van veranderingen aan het bestuursplatform tijdig plaatsvindt zodat de aangewezen tests en beoordelingen voorafgaand aan implementatie plaats kunnen vinden;
- c) bewerkstelligen dat de laatste veranderingen plaatsvinden aan de bedrijfscontinuïteitsplan en (zie hoofdstuk ISO 17)

C.12.2.4 Beperkingen op wijzigingen aan softwarepakketten

Behersmaatregel

Wijzigingen aan softwarepakketten behoren te worden ontraden, beperkt tot noodzakelijke veranderingen en alle veranderingen behoren strikt te worden gecontroleerd. (ISO 14.2.4)

Implementatieplichtige

Voor zover mogelijk er haast behoren door aanbidders geleverde softwarepakketten ongewijzigd te worden gebruikt. Als het nodig is een softwarepakket te wijzigen, behoren de volgende punten als overweging te worden genomen:

- a) het risico dat ingebouwd beheersmaatregelen en integriteitsprocedures gecompromiteerd raken;
- b) of de helderheid van de verkoper behoren te worden verkregen;
- c) de mogelijkheid om de vereiste wijzigingen van de aanbieder als standaard programma-updates te verkrijgen;
- d) de impact als de organisatie verantwoordelijk wordt gehouden voor het toekomstig onderhoud van de software als gevolg van de veranderingen;
- e) compatibiliteit met andere software die in gebruik is.

Indien de veranderingen noodzakelijk zijn, moeten de originele software te worden bewaard en behoren de veranderingen een exacte back-up van de originele kopie te worden aangebracht. Er behoort een back-upprocedure voor het updaten van software te worden geïmplementeerd om te bewerkstelligen dat de meest recente goedgekeurde patches en toepassingsupdates bij alle goedgekeurde software zijn geïnstalleerd (zie ISO 12.8.1). Alle veranderingen behoren volledig te worden getest en geïmplementeerd zodat ze zo nodig opnieuw kunnen worden toegepast bij

toekomstige software-updates. Indien vereist behoren de wijzigingen door een onafhankelijke beoordelingsinstansie te worden geleest en gevalideerd.

C.12.2.6 Principes voor engineering van beveiligde systemen

Beheersmaatregel

Principes voor de engineering van beveiligde systemen behoren te worden vastgesteld, gedocumenteerd, vastberaden en toegepast voor alle verplichtingen betreffende het legale inspannen van informalsystemen. (ISO 14.2.6)

Implementatiecichtlijn

Procedures voor de engineering van beveiligde informalsystemen, gebaseerd op principes voor beveiligde engineering, behoren te worden vastgesteld, gedocumenteerd en toegepast op interne engineeringactiviteiten met betrekking tot informalsystemen. Beveiliging behoort te worden ontworpen in alle lagen van de architectuur (commercieel, gegevens, toepassingen en technologie), waarbij de behoefte aan informatiebeveiliging telkens te worden afgevoerd tegen de behoefte aan toegankelijkheid. Nieuwe technologie behoort te worden geanalyseerd op veiligheidsrisico's en het ontwerp behoort te worden beoordeeld aan de hand van zekere aanpakvoorwaarden.

Deze principes en de vastgestelde engineeringprocedures behoren regelmatig te worden beoordeeld om te waarborgen dat zij doelmatig bijdragen aan verbeterde normen voor beveiliging binnen het engineeringproces. Ze behoren ook regelmatig te worden beoordeeld om ervoor te zorgen dat ze actueel blijven in de zin dat ze nieuwe potentiële bedreigingen afwenden en toepasbaar blijven bij verbeteringen die worden toegepast in de technologieën en oplossingen.

De voor engineering vastgestelde beveiligingsprincipes behoren indien van toepassing te worden toegepast op zijkbestede informalsystemen via de contracten en andere bindende overeenkomsten tussen de organisatie en de leverancier van wie de organisatie afbesteedt. De organisatie behoort te bevestigen dat de strikte toepassing van de beveiligingsprincipes voor engineeringen vereikbaar is met het gebruik in de eigen organisatie.

C.12.2.8 Beveiligde ontwikkelomgeving

Beheersmaatregel

Organisaties behoren beveiligde ontwikkelomgevingen vast te stellen en passend te beveiligen voor verplichtingen op het gebied van systeemontwikkeling en integratie, die betrekking hebben op de gehele levenscyclus van de systeemontwikkeling. (ISO 14.2.8)

Implementatiecichtlijn

Een beveiligde ontwikkelomgeving omvat proceduren, processen en technologie die in verband staan met systeemontwikkeling en integratie.

Organisaties behoren risico's te beoordelen die samenhangen met individuele verrichtingen betreffende systeemontwikkeling en beveiligde ontwikkelomgevingen vast te stellen voor specifieke verrichtingen op het gebied van systeemontwikkeling, rekening houdend met:

- de gevoeligheid van de gegevens die door het systeem worden verwerkt, opgeslagen en verstuurd;
- toepasselijke externe en interne eisen, zij het van regelgeving of beleidsregels;
- beheersmaatregelen voor beveiliging die al voor de organisatie zijn geïmplementeerd ter ondersteuning van systeemontwikkeling;
- betrouwbaarheid van personeel dat in de omgeving werkt (zie ISO 7.1.1);
- de graad van uitbesteding met betrekking tot systeemontwikkeling;
- de behoefte aan synergie tussen verschillende ontwikkelomgevingen;
- toegangbeveiliging voor de ontwikkelomgeving.

- h) monitoren van veranderingen aan de omgeving en de daarin opgeslagen codes;
- i) de beheersmaatregel dat back-ups worden bewaard op veilige externe locaties;
- j) controles over bewegingen van gegevens van en naar de omgeving.

Als het beschermingsniveau voor een specifieke ontwikkelomgeving is vastgesteld, kunnen organisaties de respectievelijke processen in veilige ontwikkelprocedures te documenteren en deze beschikbaar te stellen aan alle personen die ze nodig hebben.

C.12.2.7 Uitbesteede softwareontwikkeling

Beheersmaatregel

Uitbesteede systeemontwikkeling behoort onder supervisie te staan van en te worden gemonteerd door de organisatie. (ISO 14.2.7)

Implementatierichtlijn

Als systeemontwikkeling wordt uitbesteed behoren de volgende punten in de gehele externe toeleveringsketen van de organisatie in overweging te worden genomen:

- a) licentievoorwaarden, eigendom van de broncode en intellectuele eigendomsrechten in verband met de uitbesteede inhoud (zie ISO 18.1.2);
- b) oorspronkelijke eisen voor bevestigde ontwikkel-, opleverings- en testpraktijken (zie 14.2.1);
- c) het goedgekeurde creëeringsmodel aan de externe ontwikkelaar beschikbaar stellen;
- d) acceptatietests voor de kwaliteit en nauwkeurigheid van de leveringen;
- e) bewijs leveren dat beveiligingsdrempels zijn gebruikt om minimumacceptatieniveaus voor de veiligheid en beschikbaarheid van privacy toe te passen;
- f) bewijs leveren dat voldoende tests zijn uitgevoerd om te waken voor de operationele of economische aanwezigheid van benodigde inhoud op het tijdstip van levering;
- g) bewijs leveren dat uitgevoerde tests zijn uitgevoerd om te waken voor de aanwezigheid van bekende kwetsbaarheden;
- h) regelingen voor het deponeren van de broncode, bijv. indien de broncode niet langer beschikbaar is;
- i) contractueel recht om ontwikkelprocessen en beheersmaatregelen te auditen;
- j) deo betreffende documentatie van de gebouwde omgeving die wordt gebruikt om af te leveren producten te creëren;
- k) de organisatie blijft verantwoordelijk voor naleving van toepasselijke wetten en verificatie van de correctheid van de controles.

C.12.2.8 Testen van systeembeveiliging

Beheersmaatregel

Tijdens ontwikkelactiviteiten behoort de beveiligingsfunctionaliteit te worden getest. (ISO 14.2.8)

Implementatierichtlijn

Tijdens de ontwikkelprocessen zijn voor nieuwe en geactualiseerde systemen uitvoerige tests en verificatie nodig, met inbegrip van het opstellen van een gedetailleerd schema van activiteiten en tests van inputs en verwachte outputs onder diverse omstandigheden. Voor interne ontwikkelactiviteiten behoren de volgende tests in eerste instantie te worden uitgevoerd door het ontwikkelteam. Verdelijgs benodigde operationele tests te worden uitgevoerd zowel voor interne als voor Linux-achtige ontwikkelactiviteiten om te bewerkstelligen dat het systeem uitsluitend werkt zoals voorzien (zie ISO 14.1.1 en ISO 14.1.9). De omvang van het testen behoort in verhouding te staan tot de belangrijkheid en de aard van het systeem.

C.12.2.9 Systemaacceptatietests

Beheersmaatregel

Voor nieuwe informatiesystemen, updates en nieuwe versies behoren programma's voor het uitvoeren van acceptatietests en gerelateerde activiteiten te worden vastgesteld. (ISO 14.2.9)

Implementatierichtlijn

Het uitvoeren van systemaacceptatietests behoort mede het testen van informatiebeveiligingsrisico's te omvatten (zie ISO 14.1.1 en ISO 14.1.2) en het volgen van een veilige werkwijze voor systeemontwikkeling (zie ISO 14.2.1). De tests behoren ook te worden uitgevoerd op ontvangen componenten en gebruiksgereide systemen. Organisaties kunnen geautomatiseerde instrumenten inzetten zoals instrumenten om codes te analyseren of om op kwetsbaarheden te scannen, en behoren het risico van beveiligingsgerelateerde tekortkomingen te verifiëren.

Tests behoren te worden uitgevoerd in een realistische testomgeving om te bewijzen dat het systeem geen kwetsbaarheden introduceert in de omgeving van de organisatie en dat de tests betrouwbaar zijn.

G.12.3. Testgegevens

Dezetting: Bescherming waarborgen van gegevens die voor het testen zijn gebruikt. (ISO 14.3)

G.12.3.1 Bescherming van testgegevens

Beheersmaatregel

Testgegevens behoren zorgvuldig te worden gekozen, beschermd en gecontroleerd. (ISO 14.3.1)

Implementatierichtlijn

Het voor testdoelstellingen gebruiken van operationele databases met persoonsgegevens of enige anderszins vertrouwelijke informatie behoort te worden vermijden. Indien persoonsgegevens of anderszins vertrouwelijke informatie wordt gebruikt voor testdoelstellingen, behoren alle gevoelige details en inhoud te worden beschermd door deze te verwijderen of te wijzigen.

De volgende richtlijnen behoren te worden toegepast om operationele gegevens te beschermen die voor testdoelinden worden gebruikt:

- a) de toegangbeveiligingsprocedures die gelden voor besturingssystemen behoren ook te gelden voor testsystemen;
- b) voor elke keer dat besturingsinformatie naar een testomgeving wordt gekopieerd, behoort een afzonderlijke autorisatie te worden vastgelegd;
- c) besturingsinformatie behoort, onmiddellijk na voltooiing van het testen uit een testomgeving te worden verwijderd;
- d) het kopiëren en gebruiken van besturingsinformatie behoort verslaglegging te worden bijgehouden om in een audit traject te voorzien.

C.13. Bijlage: IT-voorzieningen

C.13.1. Inhouding

Doelstelling

IT-voorzieningen maken geautomatiseerd informatieverwerking mogelijk.

Afbakening

De Betalingsdienst haartert de normen in dit hoofdstuk aanvullend op de NEN-ISO 27002:2013.

De normen voor IT-voorzieningen hebben geen betrekking op de inherente beveiligings- en kwaliteitsaspecten, zoals die door de leveranciers in hun producten zijn ontworpen en gebouwd. Voor dit type aspecten bestaan aparte beveiligingsnormen, de zogenaamde Common Criteria (ISO/IEC 15408). Deze normen zijn minder praktisch toepasbaar en niet echt vergelijkbaar met de normen in dit hoofdstuk.

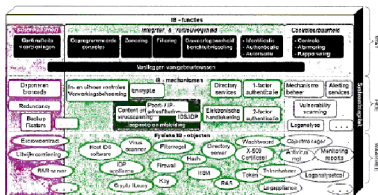
IT-voorzieningen m.n.v. bedrijfsvoorzieningen, worden ook wel aangeduid als technische infrastructuur en betreft hardware, besturingssystemen en hardwareprogramma's, die bestaan uit softwaretoelagen. De normen voor IT-voorzieningen gaan specifiek in op de installatie[methoden (parabeel)lagen] van de voorzieningen en op de wijze waarop de voorzieningen worden ingezet in het geheel van de technische infrastructuur, bijvoorbeeld in zones.

IB-functies

Het referentiekader voor de hier bedoelde normen wordt gevormd door het zogenaamde Model IB-functies, dat bedoeld is om te ordenen en te verbinden. Het model is in het kader van de NORA (Nederlandse Overheids Referentie Architectuur ontwikkeld op basis van ISO-NEK 7499-2: Information processing systems – Open Systems Interconnection Basic Reference Model – Part 2: Security Architecture uit 1991.

Een IB-functie is een logische groeping van geautomatiseerde activiteiten, die op een bepaald beveiligingsdoel is gericht. In samenhang worden de nagen afgebeelde beveiligingsfuncties gekend geacht voor de informatiebeveiliging van IT-voorzieningen (zwarte functieblokken).

In het architectuurmodel zijn deze IB-functies geprojecteerd op de kwaliteitscriteria voor informatiebeveiliging: Beschikbaarheid, Integriteit, Vertrouwelijkheid en Coördineerbaarheid. In samenhang vormen ze de WAT-laag van het model.



De IB-functies met bijbehorende mechanismen en fysieke middelen zijn voor de eenvoud van afbeelding op de criteria geprojecteerd, die ze primair ondersteunen, maar de functies weer integriteit en vertrouwelijkheid dragen bijvoelbeeld ook bij aan Lustikbaarheid.

De IB-mechanismen vormen de HOE-laag en zijn technische concepten (technieken) die het WAT van de IB-functies invullen. Omdat technisch zeld is steeds verder ontwikkeld, illustreert de figuur slechts een aantal bekende voorbeelden. De IB-mechanismen zijn de maatregelen waarmee IB-functies worden ingevuld. Elke maatregel kent een of meer implementatierichtlijnen.

De fysieke IB-middelen vormen de WAARMEE-laag. Dit zijn IT-architecturen, die de IB-mechanismen daadwerkelijk uitvoeren. Ze kunnen onderdeel zijn van een implementatieprogramma of applicatie, maar worden ook als afzonderlijke fysieke modules uitgevoerd. Ook hier zijn slechts enkele bekende voorbeelden getoond. Hoevel referentiearchitecturen de HOE- en WAARMEE-laag meestal niet beschrijven, is dat hier wel gedaan om duidelijk te maken hoe en waarmee beveiligingsfuncties uiteindelijk werkzaam zijn in de IT.

De drie niveaus in de normen corresponderen niet één-op-één met de drie lagen van het architectuurmodel. Het hogere niveau van functies loopt wel gelijk met de normbeschrijving. De twee andere niveaus onderscheiden de normbeschrijving hebben voornamelijk betrekking op laag 2, het HDE van het architectuurmodel.

De eerste zijn voort in 'lege ziele' beschreven, dat wil zeggen dat er per IB-functie geen algemene, functionele eisen beschreven worden die voor alle soorten geautomatiseerde functies gelden. Voorbeelden van die algemene, functionele eisen zijn: controleerbaarheid van variabelen, foutmeldingen, audit trail van mutaties (parameterwijzigingen), functiescheidingen mogelijk maken, vermogensverlagen kunnen genereren. Deze algemene eisen maken onderdeel uit van de IB-functie Geprogrammeerde Controls. Bij die uitwerking staan echter de bedrijfsprocessen voor ogen, zoals die in maatwerk ontwikkelde kunnen worden of als standaard pakketten worden aangeschaft.

C.13.2. Continuïteitsvoorzieningen

Doelstelling

De IT-voorzieningen voldoen aan het voor de dienst overeengekomen niveau van beschikbaarheid.

Definitie

De IB-functies die ervoor zorgen dat de juiste informatie op het juiste moment beschikbaar komt voor de dienstverlening.



Toelichting

Continuïteitsvoorzieningen voorkomen dat de dienstverlening door storingen en calamiteiten massaal onderbroken wordt. Een voorbeeld van een maatregel in dit kader is het dubbel uitvoeren van voorzieningen, waardoor de ene voorziening de functie van de ander overneemt bij uitval.

Motivering

Deze maatregelen voorkomen dat verstoringen en calamiteiten in de IT tot gevolg hebben dat de

ciensvoering onaanvaardbaar lang niet ondersteund wordt.

C.13.2.1 Dubbele uitvoering en spreiding van IT-voorzieningen

Beheersmaatregel

Op basis van de eisen die voortvloeien uit bedrijfscontinuïteit wordt bepaald in hoeverre de jaar van de technische infrastructuur dubbel worden uitgevoerd om single-points-of-failure te vermijden.

Implementatierichtlijnen

- a) Bij het vermijden van single-points-of-failure kunnen de volgende maatregelen worden getroffen:
1. dubbele uitvoering van voorzieningen: CPUs, de productieversie van de software, gegevensopslag zoals HNL op fileservers en databaseservers, hot of cold standby van beheervoorzieningen, clustering technologie van servers, fysieke verbindingen m.u.v. bekabeling binnen kantoorruimte;
 2. zodanige plaatsing van dubbele IT-voorzieningen dat deze niet op één fysieke plaats zijn samengebracht (gechieden kabels niet via één aansluitpunt), en dat er een veilige afstand tussen locaties bestaat;
 3. IT-voorzieningen zo mogelijk geografische spreiden en op dezelfde technologie baseren;
 4. single beschikbaarheid van reservevoorzieningen;
 5. slijpcontracten.

C.13.2.1.B Herstelbaarheid van verwerking

Beheersmaatregel

Verwerkingen zijn herstelbaar.

Implementatierichtlijnen

- a) De bediening van IT-voorzieningen is niet gebonden aan één fysieke locatie.
- b) Datacommunicatievoorzieningen beschikken over automatisch werkende alternatieve routingsmechanismen om uitval van fysieke verbindingen op te vangen.
- c) Systemen met hogere beschikbaarheidsniveaus dan het basiskraan beschikken over voorzieningen op het gebied van automatische failover en load balancing, waarbij de verwerking gesplitst is over twee locaties.
- d) Indien op grond van deze hogere beschikbaarheidsniveaus de verwerking is verspreid over twee locaties, is de afstand enerzijds zodanig groot dat de kans minimaal is dat beide locaties getroffen worden door dezelfde calamiteit, anderzijds zodanig klein dat herstel van communicatiefouten niet leidt tot nieuwe, onherstelbare fouten.
- e) Er zijn routines voor back-up en recovery van databestanden en software, voor herstart en foutherstel van verwerkingen.
- f) Berichten, die van derden zijn ontvangen en naar derden zijn verzonden, worden minimaal gebufferd zodat er voldoende zekerheid is over de integrale verwerking.
- g) Er is voldoende buffering van tussenbestanden bij langere verwerkingstijden.

C.13.2.2 Bewaking en alarmering IT

Beheersmaatregel

IT-voorzieningen proberen dreigende discontinuïteit van de verwerking zo mogelijk te voorspellen dan wel signaleren in een zo vroeg mogelijk stadium dat deze optreden.

Toelichting

Darid of service attacks (het onbereikbaar maken van een dienst door een overvloed aan berichten te sturen) en controles op te grote omvang van berichten of bestanden zijn specifiek van belang om de beschikbaarheid van de IT-voorzieningen, maar worden vanwege de same thing van maatregelen gezien als onderdeel van de IB-functie 'Filtering'.

Implementatierichtlijnen

- a) Er worden standaard voorkeuren geïmplementeerd om de beschikbaarheid van IT-voorzieningen te bewaken op basis van aanwezigheidslijsten en gebruiksaantallen. Voorvoorzieningen van slemprijwaarden worden doorgegeven aan een Event Console. Deze direct beschikbaar kunnen om voor spelende (zoals aantal schijffuncties bij diskunits, vrije diskruimte) of een tijdsperiode worden toe te schrijven (tijd) sprake van een dreiging voor de continuïteit, de d a k te van hebben.
- b) Er worden beperkingen opgelegd aan gebruikers en systemen ten aanzien van het gebruik van gemeenschappelijke resources (denk aan opslagcapaciteit, CPU-load, netwerkbandbreedte), zodat enkele gebruikers of een systeem niet een overmatig deel van resources kunnen opeisen en daarmee de beschikbaarheid van systemen in gevaar kunnen brengen.

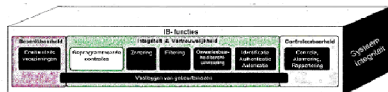
C.13.3. Geprogrammeerde controles

Doelstelling

In toepassingsprogrammatuur worden geprogrammeerde controles opgenomen, gericht op invoer, verwerking en uitvoer.

Definitie

De functies die zorgen voor hetzij geïntegreerde controles, hetzij de levering van informatie voor het uitvoeren van handmatig controles door gebruikers of beheerders.



Toelichting

Geprogrammeerde controles in toepassingsprogrammatuur (ook wel aangeduid als Application Controls) zijn onmisbaar om de integriteit van de informatievoorziening) te waarborgen. Het spreekt voor zich dat geprogrammeerde controles veel efficiënter en effectiever zijn dan handmatige controles. Geprogrammeerde controles verdienen extra aandacht: bij toepassingsprogrammatuur die via internet loopt, om het laagste beheersingsniveau van die omgeving te compenseren.

De implementatie richtlijn van geprogrammeerde controles zijn minder integraal van toepassing dan bij de andere IB-functies. De invloed van geprogrammeerde controles op de bedrijfsvoering kan aanzienlijk zijn, zodat er meer dan bij de andere IB-functies naar beschikbaarheid en effectiviteit in de specifieke situatie moet worden gekeken. Bovendien zijn vele geprogrammeerde controles overlappend ten opzichte van elkaar, zodat keuzes mogelijk niet aan de orde zijn dan bij de andere IB-functies.

Niet alle geprogrammeerde controles zijn altijd van toepassing. Om die reden is bij een aantal implementatie richtlijnen aangegeven bij welke verwerkingsstapen ze van toepassing zijn. Daarvoor wordt er onderscheid gemaakt naar:

- Batch, verwerking van een reeks posten in één keer;
- On-line, interactieve verwerking van een post via beeldscherm door een gebruiker (ook wel on-

line/real-time genoemd;

- Bericht: verwerking van een individuele post afkomstig vanuit het netwerk.

Indien het onderaand niet relevant is, zijn knipsjes opgenomen te alle kolommen achter de implementatierichtlijn.

De onder dit hoofdstuk uitgewerkte normen kunnen ook als referentiekader worden gezien voor de algemene (B-eisen voor bestuursprogramma's en (systeem) beheerspakketten) als doel uitmaken van de technische infrastructuur. De normen zijn echter bedoeld voor bedrijfsaanpassingen, dus zullen vele implementatielichtlijnen niet eoh: van toepassing zijn.

Motivering

Geprogrammeerde controles bieden de beste waarborgen dat de integriteit van de informatie(voorziening) gehandhaafd kan worden.

C.12.3.4 (Controle-technische) functie- en processcheidingen

Beheersmaatregel

Niemand in een organisatie of proces mag in staat worden gesteld om een gehele procescyclus te beheersen.

Toelichting

Centrale-technische functiescheiding beruist op het principe van het 'afreken' van tegengesteld belang. Kenmerkend shten IT-omgevingen is dat deze binnen informatie/systemen moet worden afgedwongen door in de toepassing taken te scheiden en vervolgens de maatregele van logische toegangbeveiliging: identificatie, authenticatie en autorisatie daarop te laten aansluiten.

Implementatierichtlijnen

- Basisscheidingen ("klassieke" functiescheiding)** (Batch, Un-line, Bericht) Herkende registrerende, uitvoerende, controlerende en beschikkende taken zijn gescheiden.
- Stamgegevens versus mutaties** (Batch, Un-line, Bericht) Applicatietaken voor het opvoeren van stamgegevens en het opvoeren van mutatiegegevens zijn gescheiden. Stamgegevens, ook wel vaste of referentie gegevens genoemd (geen aantal gegevens is achter haarsmaal vast) hebben een doorlopende bereikens in processen. Voorbeelden: rekeningen en omschrijvingen van grootboekrekeningen, klantgegevens met NAW en kredietlimiet, nummer, naam en prijs van artikelen, etc.
- Scheiding bij massale invoer** (Batch) Bij massale data-invoerprocessen worden eerste invoer, controle-invoer en het aanbrengen van correcties naar aanleiding van afgevoerde applicatiecontroles of -signa omlingen als afzo idelijken (applicatietaken) onderskend. Controle-invoer kan zich beperken tot kritische gegevens.
- Aparte taak voor goedkeuren** (On-line) Bij gegevens met een algemeen belang voor de integriteit van de gehele verwerking of bij het vaststellen van gegevens met een aanzienlijk financieel belang, wordt een aparte applicatietak voor het goedkeuren gecreeerd om de beschikkende functie beter te onderscheiden. De verwerking van de ingevoerde gegevens vindt pas plaats, nadat goedkeuring (door een andere gebruiker) heeft plaatsgevonden.
- Scheiding per zaak** (On-line) Als applicaties bestemd zijn voor gebruikersorganisaties, waarin kort-cyclische taakomlating van de orde is, worden de historie van gebruiker-id's en afgevoerde applicatietaken per 'zaak' (dossier) vastgelegd en op omvereenbaarheid van taken gecontroleerd voorzet een taak voor een bestaande 'zaak' voor een gebruiker ter beschikking wort. Workflow management systemen zijn speciaal ingericht om deze richtlijn te waarmaken.
- Scheiding naar inhoud van gegevens** (On-line) Indien verschillende behandelingsgroepen binnen een centrale gegevensverzameling zijn te onderscheiden, worden de applicatietaken afzonderlijk gemaakt door de identificatie van deze groepen te onderkennen met een label van de gegevens. Bijvoorbeeld, lichte groepen van klaman, regionaal onderscheid.

g) **Beheer versus gebruik** (Batch, On-line, Bericht) System- en applicatiebeheertaken zijn gescheiden van de overige gebruikerstaken. Muteren van rekenregels en variabelen (algemene rekenregels, selectiecriteria) zijn als beheer taken te zien.

h) **Scheiden en afhankelijk maken van processtappen** (Batch, On-line, Bericht) Voor de betrouwbaarheid van processen en de gegevensverwijzing kan het noodzakelijk zijn dat bepaalde processtappen in een bepaalde volgorde plaats vinden en niet anders. Voorbeelden kunnen dit principe verduidelijken - voor het verkrijgen van vergoeding moet eerst een betaling zijn ontvangen voordat de vergoeding wordt verstuurd - voor het verkrijgen van een gewaarmerkte authenticatie voor een gebruikssessie moet eerst een activatiecode werden ingevoerd, die na aanvraag wordt toegezonden naar het officieel bekende huisadres

i) **Eenduidige mutatieverantwoordelijkheid** (On-line) Om de verantwoordelijkheden voor gegevens eenduidig in een organisatie te kunnen toewijzen is voor het muteren van gegevens een zodanig consistente set applicatietaken aan te wijzen dat mutatiebevoegdheden eenduidig binnen één organisatie deel van gebruikers toegewezen kunnen worden. Alleen een batchgewijze eerste opvoer resulteert een andere applicatie of een systeemveranderde omgeving mag, liever, in de aard niet herkenbaar, in gebruik maken. Bijvoorbeeld: de personeelsadministratie is verantwoordelijk voor de gegevens die over de medewerkers in de Active Directory worden opgenomen. Is men niet daarin opgenomen dan krijgt men geen account.

j) **Dezelfde gegevens in meerdere gegevensverzamelingen** (Batch, On-line) Indien deze idee gegevens in meer gegevensverzamelingen voorkomen (zodanig in beginsel sprake is van redundantie), worden mutaties altijd vanuit één gegevensverzameling in één gegevensverzameling geplaatst, waarbij de mutaties automatisch, batchgewijze en als zodanig herkenbaar in de aard trail, worden overgebracht (gehoeloor) naar de andere gegevensverzamelingen.

C.13.3.2. Invoercontroles

Beheersmaatregel

Alle ingevoerde gegevens vanuit een systeemvermeende omgeving worden op juistheid (J), tijdigheid (T) en volledigheid (V) gecontroleerd voordat verdere verwerking plaatsvindt. Bij batchgewijze verwerking heeft de controle op de volledigheid ook betrekking op het aantal posten of mutaties dat deel uitmaakt van de batch.

Toelichting

Onder een systeemvermeende, niet-verticurede omgeving wordt verstaan elke omgeving die niet volledig kan worden beheerst vanuit het perspectief en de samenhang van het eigen toepassingsgebied.

Implementatierichtlijnen

a) **Onderscheid in invoeren, wijzigen en verwijderen** (J) (On-line) Er bestaan verschillende applicatietaken voor invoeren, wijzigen en verwijderen om de juiste invoercontroles (geautomatiseerd dan wel handmatig) mogelijk te maken.

b) **Validatie, bestaanbaarheid, relatie** (J) (Batch, On-line, Bericht) De ingevoerde gegevens vormen een complete en consistente gegevensset, in de context van de applicatie. De toegestane waarden van de ingevoerde gegevens worden op juistheid gecontroleerd om de volgende fouten te ontdekken - waarden die buiten het geldige bereik vallen; - ongelijke taken in invoervelden; - ontbrekende of onvolledige kritische gegevens; - overschrijding van boven- en ondergrenzen voor gegevensvolumes (buffer overflow/verflows); - inconsistentie ten opzichte van andere gegevens binnen invoer den net in andere gegevensbestanden. Plausible invoer wordt gewaagd, onwaarschijnlijke invoer wordt geïgnoreerd.

c) **Wijzigen invoer per batch** (J) (Batch) Voor het verbeteren van batchgewijze invoer is verband met niet te verwerken posten (bijval) worden vastregels opgesteld, die periodiek worden geëvalueerd (bijv. bij meer dan 10 geweelde posten, hele bestand retour afzender).

d) **Signaleren invoer** (J) (Batch, On-line, Bericht) Afwijkende invoer op grond van relatie- en

redelijkheidsoortloze wordt aan de gebruiker toegestaan voordat de invoer in de applicatie wordt verwerkt.

e) **Tussentijdse omschrijving (J)** (On-line) Indien van toepassing worden bij ingevoerde codes of sleutelgegevens de daarbij behorende omschrijving teruggeleverd ter visuele controle met het Invoerdocument (z.v. NAV-gegevens bij BurgerServiceNummers).

f) **Verplichte validatie/functie bij kritische gegevens (J)** (On-line) Gegevensbestand(en) die kritisch zijn voor de toepassing worden verplicht ingevuld.

g) **Default waarde (J)** (On-line) Vul de meest waarschijnlijke waarde van een veld al in, indien dit van toepassing is. Bijvoorbeeld: in een registratie voor tijdschrijven de code N voor normale uren versus O voor overwerk. Default waarden zijn niet toegestaan bij **kritische** gegevensbestand(en).

h) **Controle getui (check digit) (J)** (Batch, On-line, Bericht) Relevante eed- aanduidingen of sleutelgegevens (BurgerServiceNummer, rekeningnummers, etc.) etera) van 4 of meer posities zijn van een check-digit voorzien aan de hand waarvan de bestaansbaarheid van de eed/aanduiding door de applicatie kan worden vastgesteld.

i) **Voorkomen dubbele invoer / controle op uniciteit (J)** (Batch) Het voorkomen van duplicaten in records of berichten en controle op uniciteit kan dubbele invoer voorkomen. Toepassing is made afhankelijk van de mogelijkheden van de verwerkingscontroles en wel productiecontroles dan wel de afzet van gegevens van dubbele verwerking.

j) **Correctiemogelijkheden (J)** (Batch, On-line, Bericht) Er bestaan voldoende mogelijkheden om reeds ingevoerde gegevens te kunnen corrigeren door er gegevens aan te kunnen toevoegen en/of te verwijderen. NB: wijziging is verwijdering en toevoeging.

k) **Invoer aan de baan (J)** (Batch, On-line, Bericht) In een kriterium van verwerkingen (door meerdere gebruikers) worden invoerrecords zoveel mogelijk bij de eerste verwerking (bij de baan) afgevoerd, omdat daar de meeste kans is over die gegevens te beschikken.

l) **Voorkomen van foutmeldingen (J)** (Batch, Bericht) De invoer wordt niet enkel unieke bestanden worden zoveel mogelijk: overnemen ingevuld in het reeds vastgestelde gegevens.

m) **Tussentijdse invoer klantgegevens (J)** (Batch, On-line, Bericht) Ingevoerde klantgegevens worden na de klant te zijn opgevoerd met het vereiste de gegevens te controleren en meteen te (later) wijzigen bij fouten.

n) **Klant interacties (J)** (Batch, On-line, Bericht) Klanten hebben inzag in hun eigen gegevens en worden gestimuleerd hun gegevens op eigen initiatief te wijzigen indien nodig. Hiervoor werden functionaliteiten aangeboden.

o) **Verplichtheid (en juistheid) inzending berichten (I en V)** (Bericht) Bij regelmatigte inzending van berichten wordt aan de verzender duidelijk gemaakt dat er moeten een bevestiging van ontvangst moet worden ontvangen, zo mogelijk geautomatiseerd met de resultaten van de (eerste) verwerking. Hierdoor kan de zender worden geïnformeerd of het bericht(en) dat op gest (juist) is aangekomen.

p) **Vastleggen verwerkingsdatum (J)** (Batch, On-line, Bericht) Ten behoeve van de controle op juistheid van ontvangst en verdere verwerking wordt per verwerking de datum vastgelegd op basis van de systeemdatum.

q) **Voortaancontrole (I)** (Batch, On-line, Bericht) Een vergelijking van de verschillende (verwerkings)datums wordt voortaancontrole op de verwerking uitgevoerd.

r) **Volledigheid invoer/afgeleverde controle (V)** (Batch, Bericht) Door het opnemen van volkennummer in berichten of invoerrecords van de volledige ontvangst worden vastgesteld, mits het aantal invoerrecords bekend is.

s) **Batch-en hashproef (V)** (Batch, Bericht) Door middel van het inbrengen van voortellingen van batch-aantal en hashproef van invoerdocumenten / geleide lijsten in de applicatie wordt de volledigheid van massale invoer gecontroleerd.

C.13.3.3 Uitvoerecontroles

Beheersmaatregel

De uitvoerfuncties van programma's maken het mogelijk om de juistheid, tijdigheid en/of volledigheid van de gegevens te kunnen vaststellen.

Implementatierichtlijnen

a) **Uitvoer alleen van noodzakelijke gegevens (J)** (Batch, On-line, Bericht) De uitvoer (elektronisch of op papier) bevat alleen die gegevens die nodig zijn voor de doeleinden van de ontvanger (ook: cliënt). Elektronische uitvoer wordt niet pas op de bestemming geïnterd.

b) **Maken afdruk van gegevens van een postzaak (J)** (On-line) Het maken van een afdruk van gegevens mag alleen plaatsvinden via een applicatietaak en niet via een generieke hardcopy (print screen) functie van de werkstations. Toelichting: het maken van afdrukschriften is een te betrouwbare functie, die geen risico's kan opleveren van een geïntegreerde productie.

c) **Wettelijke eisen (J)** (Batch, On-line, Bericht) Automatisch gegenereerde bescheiden voor klanten uitbreiden aan de wettelijke vereisten van de documentatie.

d) **Afdrukken selectiecriteria bij uitvoerlijsten (J)** (Batch) Bij variabele inste mogelijkheden worden in selectiecriteria, die gebruikt zijn van de uitvoer te bepalen, op de desbetreffende uitvoerlijsten afgedrukt.

e) **Geleidelijken (J a b V)** (Batch) Uitvoerbesteden die op verschillende media's worden uitgewisseld, zijn voorzien van geleidelijke niet (naast) totalen van kritische gegevens en bedragen. Deze (naast)totaal komen ook voor in het bestand (woordoo- of skulrecode).

f) **Volledigheid verzending berichten (V)** (Bericht) Bij verzending van berichten, waarbij risicoloos op juridische geschillen mogelijk zijn, worden voorzieningen getroffen die volledige verzending kunnen zantonen. Mogelijkheden (automatische) terugkoming van ontvangst- en tijdige signaaling van het niet-tijdig reageren op het verzonden bericht, toekennen volgnummers aan berichten, waarbij zekerheid moet zijn dat er volgnummercontrole plaatsvindt bij de ontvangende partij.

g) **Volledigheid uitvoer (V)** (Batch) Als een batchproces geen uitvoer produceert, wordt een nihilverslag of nihilbestand aangemaakt. Hierdoor is het voor de volgende processen duidelijk dat er terecht geen uitvoer is. Kritische uitvoerlijsten, die niet met een vaste periodiciteit worden geproduceerd, bevatten volgnummers dan wel anderszins een verwijzing naar de laatste lijst.

h) **Volledigheid uitvoerlijsten zelf (V)** (Batch) Om de volledigheid van uitvoerlijsten te kunnen constateren, wordt elk verslag afgesloten met een "lei-de-verslag" regel of per pagina een nummering bestaande uit het paginummer en het totale aantal pagina's van het document.

i) **Controlelijnen batchverwerking (V)** (Batch) Batchuitvoer bevat controlelijnen die zijn gebaseerd op tijds- of computerverwerking opgevoerde lijnen. Indien de lijnen worden overgenomen uit bestanden, is dat kenbaar gemaakt op de uitvoerlijsten.

j) **Verdwane mogelijkheden tot informatieovereenkomst (J, T, V)** (Batch, On-line, Bericht) Het aanwezig zijn van voldoende mogelijkheden (gestructureerd, en ongestructureerd via bijv. queries) om over (geaggregeerde) informatie te beschikken, kan een bijdrage leveren aan het toekomen van de juistheid, tijdigheid en volledigheid van de informatieovereenkomst. De informatieovereenkomst maakt ditje beoordeling, onderzamenalyse, voortgangsbewaking via risicorendere invalshoeken e.d. mogelijk.

C.13.3.4 Verwerkingsbeheersing

Beheersmaatregel

Toepassingsprogramma's bieden mogelijkheden om te constateren dat alle ter verwerking aangeboden invoer juist, volledig en tijdig is verwerkt.

Implementatierichtlijnen

a) **Transactionele integriteit in lange ketens van verwerking (J)** (Bericht) De risico's van verlies

van transactionele integriteit bij het verwerken van gegevens in lange ketens wordt opgevoerd op applicatieniveau als **verwerkingszekerheid** wordt is.

Toelichting: Het impliceert een van zekerheidsniveaus op systeemniveau dat bereikt kan worden ook daadwerkelijk aan het eind van een keten zijn verwerkt, kost vooraf nog veel overhead en dus performance. Een methode bij raadpleging kan zijn de ketens korter te maken door koppelen van (basis)toestanden in deeltalocatie te gebruiken. Voorafnog is het effectiever dergelijke zekerheden in het proces (de applicatie) in te bouwen. Hiervoor bestaan diverse methoden; van het zenden van een beveiligingsbericht tot het dagelijks afstemmen van verwerkingstokken.

- b) **Informatieverstrekking aan derde(s) (-s)** (Batch, On-line, Bericht) In de verwerkingsverlagen worden bij belangrijke informatieverstrekking aan derden naast de uitvoerrelingen tevens de ontvangende instantie vermeld.
- c) **Inhoud audit trail (-s)** (Batch, On-line, Bericht) De audit trail bevat voldoende gegevens om achteraf te kunnen herleiden welke essentiële handelingen knaar door wie of vanuit welk systeem met welk resultaat zijn uitgevoerd. Tot essentiële handelingen worden in ieder geval gerekend: opvoeren en afvoeren posten, saluaveranderingen met wettelijke, financiële of voor de voortgang van het proces, de zaak of de klant beslissende gevolgen.
- d) **Raadpleegbaarheid audit trail (-s)** (Batch, On-line, Bericht) Alle ingevoerde, gemiddelde of verzamelde posten die onderdeel uitmaken van de audit trail, zijn op demandte wijze naar verschillende geïntegreerde raadgeelbaar ten behoeve van het oplossen van vragen en problemen alsmede voor het uitvoeren van interne controle.
- e) **Schone audit trail (-s)** (Batch, On-line, Bericht) Indien gegevens ten behoeve van de audit trail in databases (als occurrence) raadpleegbaar blijven, zijn de opeert applicatietokken beschikbaar voor het verwijderen van oude gegevens.
- f) **Bewaartijd audit trail (-s)** (Batch, On-line, Bericht) De audit trail wordt ten minste twee jaar bewaard of zoveel langer als de wet bepaalt indien van toepassing.

- g) **Handmatige bestandscorrecties (-s)** (Batch, On-line, Bericht) Indien handmatige invoer ter correctie van bestandsgegevens niet te vermijden is (want dan heeft de applicatie kenmerk geen sluitende status van controle- en correctieaangeregens, worden de resultaten van deze bewerkingen in twee wordt verslagen vastgelegd. Speciale aandacht is dan te besteden aan de volledigheid van deze uitvoerrelingen, zie de normen hieraan voorafgaand.
- h) **Controlestellingen vervolg (-s)** (Batch, On-line) De applicatie gaat door middel van controlestellingen inzicht in de verwerking van de invoer tot de uitvoerstromen en/of mutaties op bestregistraties. Daar toe worden op de verwerkingsverlagen controlestellingen afgedrukt, die geschikt zijn naar soot invoer, soot uitvoer of verwerking.

Toelichting: na een afgeronde cyclus van verwerking (meestal per dag) wordt aangegeven in hoeveel ingevoerde mutaties wel of niet verwerkt zijn. Voor zover er basisregistraties worden verwerkt, worden deze te lingen gepresenteerd in de vorm van een doormetingen (balansacties) in een reeks: beginstand - nieuw - verrijzen - eindstand. In bedragen: beginstand - nieuw (+) wijziging - verrijzen = eindstand

Overveglagen bij een stelsel van controlestellingen - Het ontwerpen van een stelsel van controlestellingen, waarvan een doormetingen kan worden gemaakt is bij complexe processen geen sinecure. Bovendien dienen de handmatige procedures hierop aan te sluiten, hetgeen een flink beslag op middelen kan betekenen. Dit moet opzorgen tegen het belang van het verkrijgen van zekerheden over de volledigheid van de bestregistratie. Indien de mutatieposten in een bestregistratie voldoende frequent worden gebruikt voor raadpleging en/of vergelijking met posten uit andere niet daarvan afgeleide gegevensverzamelingen, kan wellicht ook voldoende zekerheid worden verkregen over de volledigheid en mogelijke usheid van de posten in de bestregistratie. Een ander punt van overweging is opzeg in het systeem van de lidningen (met name van de (rijwaaie) versus het eenvoudiger herberekenen te presenteren van de resultaten die afzonderlijke automatisch (maar complex) proces of het berekenen als handmatige proces. Het maken van handmatige berekeningen borgt de aandacht voor het signaleren van verschillen.

ii) **Toepassen logistiek model (V) (Belech):** Bij bestelgegevensdata verwerkingen en/of meerdere batch uitvoeringen per dag met andere organisaties wordt de volledigheid en juistheid van de verwerking bevestigd door **logistieke meetpunten** en **parkeerplaatsen** in het primaire proces aan te brengen.

Toelichting 1: Gedurende de productie wordt een waarneming weggeschreven als een geval / zaak dat meetpunt passeert. In het kader van de volledigheidbewaking heeft elk werkproces aan het begin en eind een **logistiek meetpunt**. Hierdoor kan waargenomen worden of een geval/batchadeeling nog in uitvoering is of afgerond of geannuleerd. Verder zijn logistieke meetpunten nodig voor juistheid en prestatiebeoordeling en dienstverlening. Hiervoor moeten logistieke meetpunten geplaatst worden aan het begin en eind van een voortzetting of handmatige behandeling van een geval. Aangezien een planning op tactisch niveau gerelateerd is aan de producten en diensten van de organisaatie en dus de bedrijfsprocessen, is het ook van belang om in de logistieke meetpunten zijnen de werkprocessen identificeerbaar te maken van de bedrijfsorganisatie en de gevolgsbehandeling vast te leggen. Hierdoor kan uiteindelijk de samenhang van de gevolgsbehandeling op tactisch niveau zichtbaar gemaakt en bewaakt worden. **Parkeerplaatsen** zijn bovast aangebrachte punten in het proces waar werk fysiek vastgehouden kan worden. Vanuit deze punten kan het verloop van het proces na de geplaatste uitwerking in het kader bevestigd worden. In het kader van volledigheid is de zenderde partij verantwoordelijk voor de logistieke aflevering op de afgesproken locatie volgens de afgesproken kwaliteitsnorm en met het moment dat de ontvangende partij de overgang bevestigd heeft (functioneel, technisch of beiden). De ontvangende partij heeft hiërarchisch en alle tijden een afnameplicht. Hiermee is de verantwoordelijkheid rondom volledigheid bij één onkolor regeling te legd. Onder partijen waar aan we hier 'bedrijfsfunctioneel en/of' uitvoerende organisatie onderscheiden. Wanneer er een voortzetting geplaatst wordt tussen de overgang van de plaatsbehandeling, geldt dezelfde regel. De ontvangende partij is hiërarchisch verantwoordelijk voor het voortzetting.

Toelichting 2: Bij programmafouten en herstelverwerkingen bestaat het risico van onvolledige verwerking, zowel bij de eigen organisatie als bij de eventuele ketenpartner. Hierbij moet kunnen worden teruggegaan naar het laatste meetpunt waarvoor zekerheid bestaat dat de posten goed zijn verwerkt.

C.13.3.5 Bestaatscontrole

Beheersmaatregel

Kritische gegevens (bijvoorbeeld identificeer- en financiële gegevens), die in verschillende gegevensverzamelingen voorkomen, worden periodiek met elkaar vergeleken.

Toelichting:

Onder deze vergelijkingen vallen in ieder geval financiële gegevens in grootboek en subadministraties en financiële en statusgegevens in gegevensverzamelingen die op verschillende platformen voorkomen of door verschillende organisaties worden geexploiteerd.

Implementatierichtlijn

- Er zijn meerdere alternatieven om aan deze doelstelling te voldoen
- mogelijk dezelfde kritische gegevens in verschillende gegevensverzamelingen, waarbij verschillen worden geïdentificeerd. Wellicht kan hiervoor standaard programmering worden gebruikt.
- Indien de beranden dezelfde metadata bevatten kan de controle plaatsvinden met hashstaten. Bij verschillen zal de verzender of ontvanger niveau vergelijking moeten plaatsvinden. Dit gecompliceerd dan wel de beschrijving van risico's op het wettelijk vastmaken van manifestaties;
- bij afgeleide gegevensverzamelingen die frequent en integraal worden overgenomen door kopieën vanuit een basisgegevensverzameling is deze vergelijking niet noodzakelijk.

C.13.3.6 Geprogrammeerde controles t.r.t. generieke IT-voorzieningen

Beheersmaatregel

In toepassingsprogramma's zijn geen functies werkzaam, waarvoor kwalitatief betere generieke voorzeningen beschikbaar zijn, zoals die voor identificatie, authenticatie, autorisatie, versleuteling en encryptie.

Toelichting en afbakening

Deze doelstelling zal doorgaans alleen volledig haalbaar zijn bij maatwerkapplicaties. Bij standaard applicaties / programma'spakketten worden dergelijke functies meestal meegeleverd en zijn niet uit te schakelen of te vervangen door eigen generieke functies, hoewel daarmee te synchroniseren. Bovendien kunnen dan servers andere generieke IB-functies aan de orde zijn.

Implementatierichtlijnen niet uitputtend:

a) Autorisatiebeheersysteem

Voor het beheer van autorisaties wordt eenzelfde mogelijk systeem gemaakt van standaard autorisatievoorwaarden of -modulen. Indien dit op eerdere en niet te vernijden (bijv. bij gegevensafhankelijke autorisatiemechanismen) werden deze functies als scenario module uitgevoerd.

b) (Versterkte) authenticatie

Bij het elektronisch communiceren vanuit een niet vertrouwde omgeving (bijv. vanuit de externe zone) kan het noodzakelijk zijn extra zekerheden (boven het basisoniveau beveiliging) te verkrijgen omtrent de identiteit van de afzender. De hiervoor te treffen maatregelen worden afgeleerd met het in deze gevende beleid en de beschikbare generieke oplossingen.

c) Omkeerbaarheid jaista ontvanger/verzender

In situaties waar (juridische) geschillen kunnen ontstaan over het al dan niet ontvangen of verzenden van elektronische gegevens van of aan de juiste identiteit, wordt gebruik gemaakt van generieke voorzeningen van een Public Key Infrastructuur.

d) Encryptie

Als encryptie te bering van vertrouwelijkheid en/of integriteit van gegevens binnen of ten behoeve van een applicatie wordt toegepast, dan gelden hiervoor de normen van de subparagrafen C.13.4.3 Encryptie ten behoeve van verzending, C.13.4.4 Sleutel van de encryptie, C.13.4.5 Vertrouwelijkheid en integriteit afzender.

e) Duikende of uitbreken de bestandsbeveiliging

Bij uitwisseling van bestanden tussen centrale en decentrale servers of met externe partijen wordt zeker gesteld dat vertrouwelijk niet of gedeeltelijk vertrouwelijk. Een dergelijk theoretisch mechanisme is bij voorkeur als generieke voorziening in te richten.

C.13.1.7 Aanvullende normen

Beheersmaatregel

Aanvullende maatregelen boven het basisoniveau beveiliging kunnen noodzakelijk zijn om een hoger beveiligingsniveau te bereiken bij extra risicovolle zelfdynamische processen.

Toelichting

Afhankelijk van de specifieke risico's die kunnen samenhangen met het desbetreffende bedrijfsproces kan het aan de orde zijn extra maatregelen te treffen. De hieronder opgesomde maatregelen zijn als mogelijke indicatie.

Implementatierichtlijnen

a) Aparte applicatielake

Applicatielaken, die gegevens verwerken met extra (hoog) belang, kunnen van de overige transacties gescheiden worden om functionaliteit op basis van autorisatie mogelijk te maken. In de geval worden de desbetreffende gegevens als aparte gegevensruimte opgeslagen, waarvan de nabijheid doorwerkt bij alle transacties van de toepassing. Gegevens van te onderscheiden aard kunnen ook

worden opgesloten in aparte bestanden zodat de toegang en verwerking gedifferentieerd kunnen worden.

b) **Eén-a-zaak-buit**

Bij applicatiebasen met een unitaire link kan meer uitgebreide versiegeving van afgeleverde uitdruken in de audit trail worden ontvangen. Dit kan ook het geval zijn als de applicatie mogelijkheid biedt tot eigenlijk gebruik van raadgegbevoegdheden.

c) **Om-omstellingen database**

Bij het online verwerken van mutaties in een database kunnen controlstellingen van aanpak en bodagor zijn wat toe bijgehouden en gemiddeld. Hetzoudt wett dan gecontroleerd of deze controlelijnen in overeenstemming zijn met de daadwerkelijke link van de database. Voor deze controle wordt dan een aparte task gedefinieert.

d) **Gegevensencryptie**

Gegevensencryptie op applicatieniveau (database niveau) is een extra middel om de vertrouwelijkheid en de integriteit van de gegevensverzameling of -opslag te waarborgen.

e) **Gegevensrubricering tonen**

Gegevensrubricering tonen op beeldscherm, output en verspreidbare gegevensdragen en mechanismen met elektronische gegevensuitwisseling. De gebruikers en/of ontvangende dienen op de hoogte te zijn van wat de rubricering betekent voor de behandeling van de gegevens. Organisaties die gebruikmaken van gegevens uitwisselen dienen op de hoogte te zijn van de betekenis van de rubricering. Hetzoudt wett dan andere maatregelen, dan alleen zij onderlinge afspraken te maken met de verschillende samenlevingen op elkaar aansluitend.

C.13.4. Zonering IT

Doelstelling

De technische infrastructuur is in zones ingedeeld om isolatie van onderdelen hiervan mogelijk te maken.

Definitie

Afbakening van een logisch geheel van de technische infrastructuur waarin gegevens vrijelijk met hetzelfde niveau van beveiligingsmaatregelen kunnen worden uitgewisseld.



Toelichting

Het doel van zonering is:

- het voorkomen of beperken van risico's doordat delen van onderdelen van de technische infrastructuur;
- het scheiden van onderdelen waaraan verschillende betrouwbaarheidsniveaus worden gesteld. Informatie-uitwisseling tussen zones verloopt via koppelpunten, die de informatiestromen controleren. Hierdoor kunnen bepaalde dreigingen niet optreden die wel niet doorwerken van de ene zone in de andere. Hierbij gaat het er niet alleen om de interne vertrouwde zone tegen de externe,

omvouwde zone te beschermen, maar ook om interne zones (zoals ontwikkeling-, test-, acceptatie- en productie-omgevingen) van elkaar te scheiden.

Zonering maakt het voorts mogelijk om met verschillende beveiligingsniveaus binnen een infrastructuur te werken en informatiestructuren en risicovolle beheerscommando's te reguleren. Zurender als middel om toegang tot voorstellingen te beperken werkt op een hoger beveiligingsniveau dan via logische toegangsbeveiliging. Zonering maakt het netwerk overzichtelijker voor beheer en dat is levens van belang voor beveiliging.

Een zone komt dus andere risico's, die samenhangen met de diensten of IT-voorzieningen die om opgenomen zijn. Binnen zo'n risicosamenhang met standaard maatregelen voor zones (compartimentering) worden erge tijd alle het risicoprofiel dat verast. Bijvoorbeeld om verschillende productieomgevingen uit elkaar te houden, die niet hetzelfde beveiligingsniveau hebben. Externe netwerken worden in dit zoneringconcept ook als aparte zone gezien.

Zangezien het overgrote deel van de toepassingen van encryptie erop gericht zijn gegevensde invoering van een andere IT-voorziening te voorkomen, worden dit type maatregelen onder zonering gepositioneerd.

Metvoering

De zonering kan onrisico's worden gecreëerd, waardoor bedreigingen en incidenten die optreden in de ene zone niet doornemen in een andere zone.

C.12.4.4 Zonering technische infrastructuur

Beheersmaatregel

De indeling van zones binnen de technische infrastructuur vindt plaats volgens een vastgesteld richtingsdocument (configuratiedocumen waarin is vastgelegd welke uitgangspunten gelden voor de toepassing van zonering).

Implementatiechiffen

- Een aparte zones voor Ontwikkeling, Test, Acceptatie en Productie.
- De experimentele omgeving (laboratorium, sand box) is een fysiek gescheiden zone.
- Beheer van zones vindt plaats vanuit een eigen zone.
- IT-voorzieningen (zoals mobiele clients en werkstations) die buiten de fysieke toegangsbeveiliging van de gebouwen van de organisatie zijn opgesteld, worden in de externe zone (externe werkpak) gepositioneerd.
- Dataversen, waarvoor een hoger beveiligingsniveau geldt dan het basisniveau, kunnen in een eigen zone worden opgenomen.
- Van werkstations wordt bepaald welke onderdelen tot welke zone behoren, geel op de risico's van het onbevoegd ontkennen van data via de verschillend soorten poorten. Om deze reden kan lokale opslag van gegevens op de vaste schijven van werkstations (b.v. laptops) en opslag op verwijderbare opslagmedia worden geïmplementeerd.
- Interne systemen wisselen gegevens uit met partners en klanten via een centrale interne zone (DMZ) en een omvouwde, externe zone.
- Voor de uitvoering van overeenkomsten met derden (niet openbare gegevens) worden besloten externe zones (vertrouwde derden) gebruikt.
- In een DMZ worden alleen openbare gegevens van een organisatie opgeslagen, die in het uiterste geval verloren mogen gaan.
- Vitale bedrijfsgegevens worden in een aparte zone geplaatst.

C.11.4.2 Eisen te stellen aan zones

Beheersmaatregel

Zones zijn voor beveiliging en beheer als eenheid gedefinieerd.

Implementatierichtlijnen

- Elke zone heeft een vastgesteld, uniek beveiligingsdoel.
- Elke zone wordt slechts beheerd onder verantwoordelijkheid van één beheerinstantie (m.u.v. overtrovande derden)
- Elke zone heeft een gedefinieerd beveiligingsniveau, d.w.z. kent een gedefinieerd stelsel van samenhangende beveiligingsmaatregelen.
- De maatregelen van logische toegangsbeperking zijn van toepassing op alle IT-voorzieningen in een zone.
- Uitwisseling van gegevens tussen zones vindt uitsluitend plaats via een gedefinieerd koppelvlak.
- Zones kunnen worden onderscheiden door gebruikmaking van routing van datastromen, verticale van de bron- en de bestemmingadressen, door toepassing van verscheidende protocollen, encryptietechnologie, partitioering of virtualisatie van servers, maar ook door fysieke schieding.
- Poorten, die stromen en soortgelijke voorzieningen geïnstalleerd op een computer of routeringszetting, die niet speciaal vereist zijn voor de bedrijfsvoering, worden uitgeschakeld of beveiligd.

C.12.4.3 Encryptie ten behoeve van zonerig

Beheersmaatregel

De communicatie en de opslag van gegevens die buiten de invloedssfeer van de logische en fysieke toegangsbeveiliging maar wel binnen de eigen beheersomgeving vallen of waarvoor deze maatregelen onvoldoende zijn, zijn door encryptie beschermd.

Implementatierichtlijnen

- Encryptie dient te worden toegepast in de volgende situaties:
 - bij verzamelbare mediadragers indien deze buiten een beschermde zone worden bewaard (denk bijvoorbeeld aan extern opgeslagen back-up tapes, diskettes, DVD's, CD-ROM's en USB-sticks);
 - het extern geheugen van mobiele apparatuur (denk aan harde schijven van portable workstations en geheugenkaarten in PDA's/smartphones);
 - bij beheerszones over het eigen netwerk (met encryptievoorzieningen binnen de beveiligde of geïsoleerde protocollen);
 - bij datatransport over onbetrouwbare netwerken (internet) of om een hoger beveiligingsniveau te bereiken;
 - bij datatransport via mobiele data-dragers buiten de reikwijdte van de fysieke toegangsbeveiliging van een organisatie;
 - bij draadloze datacommunicatie;
 - wachwoorden, die worden opgeslagen of verzonden;
 - end-to-end encryptie als aanvullende beveiligingsmaatregel kan alleen binnen een zone gebruikt worden ter voorkoming van doorgang van gegevens en/of informatie van de ene zone naar de andere. Uitzondering hierop vormt de communicatie tussen werkstations en data servers.
- Er is in het kader van de naleving van de relevante overeenkomsten, wetten en voorschriften.

rekening gehouden met de beperkingen op de import en/of export van computersapparatuur en -programmatuur die zo is ontworpen dat er cryptografische functies aan kunnen worden toegevoegd;

c) Er is in het kader van de naleving van de relevante overeenkomsten, wetten en voorafschiet rekening gehouden met de beperkingen op het gebruik van versleutelingstechnieken.

C.13.4.4 Sterkte van de encryptie

Doelstelling

De sterkte van de encryptiemechanismen voldoet aan de eisen van de tijd.

Implementatierichtlijnen

- De gebruikte cryptografische algoritmen zijn als open standaard per soort toepassing gedocumenteerd en staan als robuust bekend.
- Hardware-observaties (bijv. smart card- en Hardware Security Module producten) zijn gecertificeerd volgens de relevante stekende standaards.
- De sleutellengte is instelbaar en voldoende groot om ook in de afzienbare toekomst bestand te zijn tegen succesvolle pogingen om de sleutels te laten achterblijven met inachtneming van het belang van de gegevens, die anderszins worden beschermd.

C.13.4.5 Vertrouwelijkheid en integriteit sleutels

Beheersmaatregel

De vertrouwelijkheid en integriteit van geheime cryptografische sleutels is gewaarborgd tijdens het gehele proces van generatie, transport, opslag en vernietiging van de sleutels.

Implementatierichtlijnen

- Cryptografische sleutels en certificaten kennen een geldigheidsdiermijn die is afgestemd op het kritische gehalte van de toepassing met een maximum van 1 jaar.
- Securiteit encryptie met een unieke sessiesleutel heeft zo mogelijk de voorkeur boven encryptie met periodiek te wijzigende sleutels. Deze sessiesleutel wordt random gegenereerd, is bij voorkeur symmetrisch en wordt bij voorkeur uitgewisseld met een asymmetrisch algoritme.
- Generatie en distributie van private keys, master keys en root certificaten vinden plaats binnen een beschermde omgeving van cryptohardware.
- Deze cryptohardware is temperatuurstabiel. Dit betekent dat ze bijzonder voorzichtig aan zijn getrokken tegen onbedoelde herinstallatie van de opgeslagen cryptosleutels bij een fysieke inbraak op de hardware.
- Interactieve besteding van cryptosleutels vindt plaats volgens het vier-ogen-principe (wachwoord van twee personen nodig voor één handeling). Deek hierbij aan installatie, wijzigingen in configuratie en generatie van master keys.

C.13.5. Filtering

Doelstelling

Op het knooppunt tussen zones zijn filterfuncties gepositioneerd voor het gecontroleerd doorlaten van gegevens; niet toegestane gegevens worden tegengehouden.

Definitie

Controle van informatiestromen op communicatievraag, vorm (protocol) en/of inhoud van gegevens, afhankelijk van de aard van de informatiestromen en de zones of netwerkknopen waar ze vandaan komen of naar toe gaan.



Teelichting

Filtering beschermt zones tegen aanvallen, indringers, ongewenste inhoud en virussen, waardoor dienovereenkomstig worden of onrechtmatige toegang tot gegevens of systemen wordt voorkomen. Filtering controleert geen identiteiten van individuele gebruikers.

De communicatie tussen twee zones kan worden getoetst op ongewenste eigenschappen. Daarvoor wordt een statistisch profiel vastgelegd van de zenders in de betrokken zones. Van het communicatiegedrag wordt elektronisch een 'repliceerbare' vastgelegd, die enerzijds wordt vergeleken met het doelbetreffend richtingsprofiel (configuratiebestand) voor het sociaal van communicatie en anderzijds met bekende patronen van ongewenste communicatie.

In de afsluiting die niet tot indringing wordt toegepast op blokken of deformaties, zal minder filtering noodzakelijk zijn, maar dat lost het zonering- en filteringsconcept niet op; het kan wel tot een andere indringing leiden.

In deze versie van document is nog niet gestreefd naar een echt uitgewerkte normering van de filterfunctie, gezien het complexe karakter daarvan. Wel zijn de elementen ervan benoemd. Naar verwachting zal het ontwikkelen van IB-zoneren aanleiding vormen de normering aan te passen.

Motivering

Fiterfuncties zijn onlosmakelijk verbonden aan de IB-functie 'Zonering' en onderaan daaraan ook hun motivering.

C.13.5.1 Controle op communicatiegedrag

Beheersmaatregel

Ongewenste communicatiegedrag wordt opgemerkt en geblokkeerd.

Implementatierichtlijnen

- De filtering tussen zones is afgestemd op de doelstelling van de zones en het te overdragen versie van de gegevens. Hierop wordt controle plaats op protocol en richting van de communicatie. Niet toegestane verbindingen worden geblokkeerd, o.a. wordt vasthouden dat deze tot stand komen.
- In koppelpunten met externe of onvertrouwde zones worden maatregelen getroffen om aanvallen te signaleren en te kunnen blokkeren die erop gericht zijn de verwerkingscapaciteit zodanig te laten vullen, dat onbereikbaarheid of alval van computers het gevolg is (denial of service attacks).
- Al het gegevensverkeer naar externe of onvertrouwde zones wordt real-time inhoudelijk geïnspiceerd op inbreukopzichten. Een update van aanvalsprofielen vindt frequent plaats.

C.13.5.2 Controle op gegevensuitwisseling

Beheersmaatregel

De gegevensuitwisseling tussen zones wordt naar vooraf bepaald gecontroleerd, waarbij ongewenste gegevens worden geblokkeerd.

Implementatierichtlijnen

- s) De uitvoer van leesapparaten systemen waarmee gevoelige informatie wordt verwerkt, wordt alleen verzonden naar computerterminals en locaties met een autorisatie.
- t) Versleutelde gegevensstromen van en naar de externe zone worden afgeleid voor inhoudelijke controle.
- c) E-mail berichten met bijlagen worden uitsluitend toegelaten op basis van formalisatie van afspraken over de oorsprong (extansie) van de bijlage. Gecontroleerd wordt of de aanduiding van de oorsprong klopt met de werkelijke oorsprong van de bijlage.
- d) Berichten en bestanden met een omtuig boven een vastgestelde grenswaarde worden geblokkeerd om problemen wegens onbetrouwbaarheid te voorkomen.
- e) Er is antivirusprogramma's actief die e-mail berichten en webpagina's blokkeert met kwaadaardige code (virussen, worms, trojans, spyware, etc.) in zowel ontvangens als verzendens e-mails. Een update van een virusdefinities vindt frequent plaats.
- f) Er is een (spam) filter geïmplementeerd voor zowel ontvangen als verzendens berichten. Een update van het spamfilter vindt frequent plaats.
- g) Op alle werkdagen en daarvoor is aanmerking komende servers is antivirusprogramma's resident actief. Een update van virusdefinities vindt antivirusprogramma's ten op ieder moment (hardnlog) uitgevoerd worden en vindt periodiek of bij concrete dreigingen geautomatiseerd plaats.
- h) In een keten van zones kunnen een organisatie wordt antivirusprogramma's van verschillende leveranciers toegevoegd.

G.12.6. Onweerlegbaarheid berichtuitwisseling

Doelstelling

Bij berichtuitwisseling wordt de onweerlegbaarheid van verzending en ontvangst geborgd.

Definitie

Onweerlegbaarheid van elektronische berichtuitwisseling houdt in dat:

- De zender van een bericht niet kan ontkennen een bepaald bericht verzonden te hebben;
- De ontvanger van een bericht niet kan ontkennen het bericht van de zender in de oorspronkelijke staat te hebben ontvangen.



Toelichting

De onweerlegbaarheid kan op twee wijzen verkregen worden:

- over een onbetrouwd netwerk, d.m.v. een Public Key Infrastructure (PKI);
- over een besloten netwerk via een betrouwbare berichtendienst.

De onweerlegbaarheid via PKI kan verkregen worden door middel van wederzijdse authenticatie van zender en ontvanger aangevuld met controle op de integriteit van het bericht. Hiermee wordt een bericht onweerlegbaar vastgesteld. Dit wordt ook wel non-regulair genoemd. Dit kan met behulp van een zogenoemde elektronische handtekening, die laagstbaar is als wettelijk bewijs mits voldaan

wordt aan eisen in de Wet Elektronische Handtekening (WEH).

In het algemeen valt het 'zenden' van de digitale handtekening uitsein in twee delen, die tot een unieke relatie leidt tussen het bericht in de handtekening:

Vastleggen van de unieke kenmerken van het bericht (in een 'hash').

Vorbiden van de unieke identiteit van de zender aan de haak.

Het zenden van een digitale handtekening kan plaatsvinden met verschillende methoden, waarvan de twee bekendste zijn:

- Symmetrische cryptografische sleutels = vooraf uitgedeeld door beide partijen.

- Asymmetrische cryptografie o.b.v. PKI = uitgedeeld door vertrouwde derde.

Eigen Public Key Infrastructure (PKI) worden samen met cryptografische ingespaard een publieke sleutel en een geheime, private sleutel. De publieke sleutel wordt opgenomen in het certificaat, uitgegeven door een (derde) vertrouwde partij. De private sleutel wordt bewaard en gebruikt door de persoon of instelling, van wie het certificaat is. Deze sleutels zijn nodig voor versleuteling en ontsleuteling. Deze sleutels hebben een unieke wettelijke relatie met elkaar. Hierdoor kunnen ze in combinatie met de betreffende certificaat gebruikt worden voor authenticatie en het versturen van geheime (sleutel-) informatie over een onvertrouwd netwerk.

Beveiliging

Als er geen specifiek dekstop afgestemde maatregelen zijn, wordt het risico gelopen dat een ontvanger zijn bericht kan ontvankelijk ook een bericht te hebben ontvangen of kan ontvangen een bericht te hebben ontvangen met de inhoud zoals deze door de verzender is verstuurd. In het elektronisch berichtenverkeer zijn namelijk meer risico's in deze te ontdekken dan in het fysieke postverkeer.

Beveiligingsmaatregel

Eig berichtuitwisseling waart rechten en plichten ontstaan tussen partijen bestaat de zekerheid dat het ontvangen bericht afkomstig is van de verzender en de inhoud niet is beïnvloed.

Implementatieberichten

Onverlegbaarheid kan worden verkregen op twee verschillende wijzen:

a) Een betrouwbare berichtendienst in het basistienetwerk, waarbij verzending en ontvangst van berichten bevestigd wordt door de berichtendienst dan wel hiervoor in de applicatie extra facilites op te nemen.

Of bij een onvertrouwd netwerk:

b) Een PKI voldoet aan de daarvoor geldende standaarden, bij de overheid die van de PKI-Overheid.

c) De elementen die het bewijs vormen van een elektronische handtekening, worden in de vorm van een juridisch bestand zodanig samen met de oorspronkelijke data bewaard, dat hetzelfde bereik in de normale werkdroom van het bedrijfsproces altijd weer te reproduceren.

d) De ontvangen berichten worden onmiddellijk na ontvangst in de juridische logging vastgelegd, voordat enige bewerking met toepassingssoftware aan de orde is.

e) De verzonden berichten worden in de laatste fase van verwerking onmiddellijk worden verzending plaatsvindt in de juridische logging vastgelegd.

f) Voor de juridische logging gelden dezelfde systemeneisenrichtlijnen als voor applicaties.

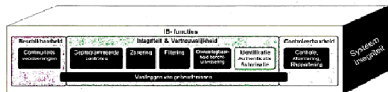
C.13.7. Identificatie, Authenticatie en Autorisatie

Doelstelling van de ID-functie

Logische toezichtaanpak vindt plaats voordat IT-voorzieningen kunnen worden gebruikt.

Definities

Logische toegangscriteria door middel van identificatie, authenticatie, autorisatie draagt ervoor zorg dat een persoon, organisatie of IT-voorziening uitsluitend gebruik kan maken van geautomatiseerde functies, waarvoor deze door middel van een aanvraagproces toegangsrechten heeft verkrijgen.



Toelichting

Deze functie bestaat uit drie afzonderlijke subfuncties en wordt in samenhang met de hier niet-beschouwde Beheersmaatregelen ook wel aangeduid met Identity and Access Management (IAM).

De begrippen voor de drie subfuncties zijn als volgt toe te lichten:

- Identificatie is het bepalen van de identiteit van personen, organisaties of IT-voorzieningen: wie ben je?
- Authenticatie is het aantonen dat degene die zich identificeert ook daadwerkelijk degene is die zich als zodanig voorgeeft: ben je het ook echt? Authenticatie noemt men ook wel verificatie van de identiteit.
- Autorisatie is het controleren van rechten voor de toegang tot geautomatiseerde functies en/of gegevens in IT-voorzieningen: mag je de gevraagde functie of gegevens wel benutten en wat mag je ermee doen: uitvoeren, raadplegen of ook wijzigen?

Identificatie en authenticatie wordt vrijwel altijd in combinatie met elkaar gebruikt. Autorisatie is een meer op zichzelf staande subfunctie, die nu implementatie in een IT-gebeel eigen consequenties heeft.

Motivering

Het kurium van de afwezigheid van functiescheiding, de herleidbaarheid van handelingen en het beperken van de toegang tot gegevens behoren tot de belangrijkste maatregelen van informatiebeveiliging. Identificatie, authenticatie en autorisatie zijn de functies waarmee aan deze doeleinden invulling kan worden gegeven.

C.13.7.1 Identificatie

Beheersmaatregel

Alle toegangsvragers (gebruikers) tot een geheel van IT-voorzieningen zijn uniek herleidbaar tot één natuurlijk persoon, organisatie of IT-voorziening.

Implementatierichtlijnen

- Natuurlijk personen, organisaties of IT-voorzieningen werden geïdentificeerd door een unieke identificatie.
- Wijstgesteld van identificeerbare gebruikers met toegang tot systemen die alleen publieke of binnen een organisatie algemeen toegankelijke informatie omvatten.
- Systeemprocessen draaien onder een eigen gebruikersnaam (een functionele account), voor zover deze processen handelingen verrichten voor andere systemen of gebruikers.
- IT-systemen bieden de mogelijkheid dat beheerders beheerwerkzaamheden uitvoeren onder hun eigen persoonlijke gebruikersnaam. In de operatie worden beheerwerkzaamheden en werkzaamheden als gewone gebruiker onder twee verschillende gebruikersnamen uitgevoerd.

e) Het gebruik van speciale beheer accounts (root, administrator) is uitgesloten, als gebruik overern mogelijk is met her eikbaarheid, doelbinding en onwenselijke logging gecombineerd toegepast worden.

C.12.7.2 Authenticatie

Beheersmaatregel

Alvorens een systeem toegang verleent, wordt de identiteit van de gebruiker of ander subject dat om toegang vraagt, vastgesteld door middel van authenticatie.

Implementatiedichtlijnen

a) Bij het intern gebruik van IT-voorzieningen worden gebruikers minimaal geauthenticeerd op basis van wachtwoorden.

b) In de volgende situaties vindt authenticatie van gebruikers plaats op basis van cryptografische techniek, 'hardware tokens' of een 'challenge/response'-protocol:

1. Single Sign-On;
2. Toegang vanuit een vertrouwde omgeving;
3. Bij beheer van kritische beveiligingsvoorzieningen (denk bijvoorbeeld aan Hardware Security Modules, firewalls, intrusion detection and prevention systems of routers).

c) Bij het niet-dagelijkse beheer van kritische beveiligingsvoorzieningen vanuit een vertrouwde omgeving is het voor ogen principe een a tomatief voor 2.b (dat wil zeggen dat er altijd twee functionarissen nodig zijn om een handeling uit te voeren).

d) Een mobiel apparaat (zoals een laptop, handheld computer, smartphone, PDA) vraagt om een pincode of wachtwoord bij het inschakelen.

e) Bij externe beheer op afstand en mobiel werken (een mobiel apparaat dat draadloos verbonden is met IT-voorzieningen van de organisatie) wordt vastgesteld wat van af een voor dit doelinstake beschikbaar gestelde werktoel wordt gewent.

f) Wachtwoordbestanden worden gescheiden opgeslagen van gegevens van de toepassing.

C.12.7.3 Wachtwoordconventies

Beheersmaatregel

Bij authenticatie op basis van kenmerk svingt het systeem het toepassen van sterke wachtwoordconventies af.

Implementatiedichtlijnen

a) Wachtwoorden voldoen aan de volgende wachtwoordconventie:

1. minimaal acht tekens;
2. minimaal één hoofdletter;
3. minimaal 4 kleine letters;
4. minimaal 1 cijfer en/of één versmd teken;
5. nieuw wachtwoord moet in minimaal twee tekens verschillen met het vorig wachtwoord.

b) Wachtwoorden van gebruikersaccounts moeten minimaal elke 90 dagen gewijzigd worden.

c) Wachtwoorden van functionale accounts worden minder frequent gewijzigd, namelijk minimaal eens per jaar er. Een minste elke nieuwe release van de IT service, maar daarentegen zijn de wachtwoorden langer, namelijk minimaal 20 posities, met willekeurig gekozen cijfers, tekens en speciale tekens.

d) De gebruikers hebben de mogelijkheid hun eigen wachtwoord te kiezen en te wijzigen. Hierbij geldt

het volgende:

1. Voordat een gebruiker zijn wachtwoord kan wijzigen, wordt de gebruiker opnieuw geïdentificeerd.
2. Iar voorkoming van typerfouten in het nieuw gekozen wachtwoord is er een bevestigingsprocedure.
3. Alvorens een nieuw wachtwoord wordt gewijzigd, wordt geautomatiseerd gecontroleerd of het nieuwe wachtwoord aan de vereiste eisen voldoet.

e) De default en installatiewachtwoorden worden tijdens of direct na installatie verwijderd of gewijzigd.

f) Initiale wachtwoorden en wachtwoorden die gerest zijn, worden aan bovenstaande wachtwoordcriteria en daarbij wordt door het systeem afgehandeld dat bij het eerste gebruik dit wachtwoord wordt gewijzigd.

C.13.7.4 Instellingen aanmelden op een IT-voorziening

Beheersmaatregel

Instellingen met betrekking tot het aanmelden op een IT-voorziening zijn er op gericht te voorkomen dat iemand werkt onder een andere dan de eigen gebruikersnaam.

Implementatie-eisen

- a) Er wordt zoveel mogelijk voorkomen dat gebruikers zich op de verschillende IT-voorzieningen in dezelfde letter opname aan moeten melden. Als dit niet mogelijk is, dan wordt het aanmeldproces zo snel mogelijk enkelvoudig ingericht.
- b) Expiratiestatus van accounts zijn afgestemd op de expiratie van de contracten van de medewerkers.
- c) Op het aangebruikers platform wordt gebruik gemaakt van schermbeveiligingsprogramma's (een screensaver) die na 30 minuten alle informatie op het beeldscherm onleesbaar maakt. Het is toegestaan dat het systeem zo wordt geconfigureerd, dat binnen een toegestane periode van enkele seconden de gebruiker door een muisbeweging of toetsaanslag kan verhinderen dat de schermbeveiliging wordt geactiveerd. Het systeem biedt de gebruiker ook zelf de mogelijkheid om de schermbeveiliging op eenvoudige wijze te activeren. Het systeem is zo ingesteld dat na het activeren van de schermbeveiliging de gebruiker zich opnieuw moet authenticeren (de identificatie mag zichtbaar blijven).
- d) Nadat voor een gebruikersnaam 6 keer een foutief wachtwoord gegeven is, wordt het account minimaal 10 minuten geblokkeerd. Indien er geen lock-out periode ingesteld kan worden, dan wordt het account geblokkeerd. In dat geval wordt de gebruiker verzocht deze lock-out op te heffen of het wachtwoord te veranderen.
- e) Het wachtwoord wordt niet getoond op het scherm tijdens het ingeven van het wachtwoord. Het is wel gebruikelijk dat toelichtingen worden meegegeven door sterretjes of tuitjes.
- f) Voorgaand aan het aanmelden wordt aan de gebruiker een melding getoond dat alleen goetdurend gebruik is toegestaan voor sessies die door de organisatie vastgesteld worden.
- g) Voor het inloggen vanaf een niet-vertrouwd netwerk wordt een maximumtijd van 10 minuten en een minimumtijd van 10 seconden vastgesteld. Indien deze tijd wordt overschreden, wordt het systeem het inlogproces.
- h) Netwerksesies worden na een vastgestelde periode van inactiviteit afgesloten. De duur van de periode tot de time-out is afgestemd op de vertrouwelijkheid van de zone (intern of extern), de gevoeligheid van de informatie die wordt verwerkt en de toepassingen die worden gebruikt.
- i) Voordat een gezagde aanmelding op een systeem heeft plaatsgevonden toont het systeem uitsluitend informatie die noodzakelijk is voor de aanmelding. Bij een foutieve aanmelding wordt niet vermeld of de gebruiker naam bestaat, maar slechts dat de combinatie gebruikersnaam en

wachtwoord juist was, nadat alle gegevens voor het leggen zijn ingevuld. Er wordt bovendien geen geheugensteun voor het wachtwoord getoond.

g) Zedre een inlogproces succesvol is voltooid, worden de datum en tijd van de voorgaande succesvolle login getoond.

h) Automatisch aanmelden is niet toegestaan voor inactieve gebruikers. Hier wordt bedoeld dat automatisch wordt ingeloopt zonder dat binnen de sessie door een gebruiker een wachtwoord wordt ingegeven (bijvoorbeeld het gebruik van Windows Auto Log-on mag dus niet, waartoe door het aanmelden van een PC een gebruik of automatisch wordt ingeloopt onder een vooraf opgegeven gebruikersnaam met een vooraf opgegeven wachtwoord). Alleen systeemprocessen met functionele accounts mogen blijven een zure geautomatiseerd aanloggen.

C.13.7.5 Autorisatie

Beheersmaatregel

Autorisaties zijn ingesteld op basis van oorsprong- of systeembdocumentatie, waarin aangegeven is welke rechten in welke gebruikersgroepen worden oedegebracht.

Toelichting en afbakening

De IT-subfunctie autorisatie wordt hier beschouwd vanuit het perspectief van de verantwoordelijkheid van de technisch beheerder. De feitelijke inhoud van de autorisaties is een verantwoordelijkheid van proceseigenaars en functionele beheerders, rollenbeheerders, onderstaande functies bij het aanvragen van autorisaties door lijnmanagers.

Implementatierichtlijnen

a) De technische implementatie van autorisaties naar autorisatiegroepen is in overeenstemming met de oorsprong- of systeembdocumentatie.

b) Speciale systeembevoegdheden zijn in aparte autorisatiegroepen opgenomen.

c) Bij het koppelen van gebruikers aan autorisatiegroepen kunnen aangegeven onverenigbaarheden worden gesignaleerd.

C.13.7.6 Minimaliseren rechten

Beheersmaatregel

IT-voorzieningen zijn met de min mogelijk toegangsrechten ingesteld.

Implementatierichtlijnen

a) In de oorsprongtoegangsregels wordt ten minste onderscheid gemaakt tussen lees- en schrijfbevoegdheden. De toegangsregels worden zo fijnmazig als mogelijk ter beschikking gesteld, afhankelijk van de mogelijkheden van de IT-voorzieningen en de daardoor veroorzaakte beheerslast. Zo kunnen bij schrijfrechten vaak rechten voor oraken (zoals create/read/generalize), wijzigen (zoals update/change/delete) en verwijderen (zoals delete/drop/purge) separaat worden toegekend. Standaard gebruikers krijgen geen execute-rechten.

b) De toekenning van rechten aan processen en bestanden is zo minimaal mogelijk. Bijvoorbeeld:

1. als het platform bestaat om geschieden sessies te beheren, dan worden voor systeembestanden geen sessierechten toegekend;
2. tijdelijke (spoel)bestanden (bijv. printgegevens) zijn alleen voor systeembeheer toegankelijk;
3. er worden geen of anderszels mogelijk rechten gegeven aan standaard groepen en accounts, zoals 'guest', 'public' of 'everyone'.

c) Toepassingen mogen niet omhoog en niet langer dan noodzakelijk onder een systeemaccount (een privilegeless account) draaien. Direct na het uitvoeren van handelingen naar hogere rechten voor nodig zijn wordt weer teruggeschakeld naar het niveau van een gewone gebruiker (een unprivileged user). Denk

bijvoorbeeld aan een daemon die onder root een poort opent en daar na terugschakelt naar `userless`. Een ander voorbeeld is het gebruik te `Substitute User` commando. Dit wordt alleen gebruikt voor die delen van een proces die tijdelijk onder hogere rechten draaien of om te voorkomen dat beheerders voortdurend met de hoogste systeemrechten moeten werken.

c) De taken die niet (tijdelijk) lagere rechten afgevoerd worden, kunnen niet onderbroken of afgebroken worden met o.a. gevolg dat deze hogere rechten voor andere de oindan gebruik kunnen worden (tijdelijk misbruikt kunnen worden).

C.13.7.7 Toegestaan embeddeerd gebruik autorisaties

Beheersmaatregel

Er zijn maatregelen getroffen die embeddeerd gebruik van toegesecce autorisaties voortkomen.

Implementatierichtlijnen

- Gebruikers krijgen geen algemene common-co-omgeving tot hun beschikking (bijvoorbeeld een `Dev` prompt of `Univshel`).
- Beheertaken verlopen zoveel mogelijk via een manussysteem en gestandaardiseerde werkwijzen (`script`).
- Bij het overnemen van werkstations door beheerders om te kunnen me kijken op het werkstation wordt technisch afgevoerd dat hiervoor eerst toestemming aan de gebruiker wordt gevraagd. De gebruiker kan op elk moment de verleende toestemming intrekken.
- Systeemdata, programmatuur en toepassinggegevens zijn van elkaar gescheiden, dat wil zeggen dat de bestanden zoveel mogelijk in eigen `directory's` of `partities` geplaatst worden.
- Er zijn in productiezone geen hulpmiddelen toegankelijk die het systeem van logische toegangsbeveiliging doorbreken of de integriteit van de productieverwerking kunnen aantasten, zoals `ODBC`, bestandsvierers, editors, ontwikkelcode, compilers, tekstverwerkingsprogramma's en overige andere systeemhulpmiddelen.
- Gebruikers hebben verschillende gebruikprofielen voor operationele en proefsystemen, en de menu's tonen de juiste identificeerbodschapper om het risico van fouten te verminderen.
- Wachtwoorden worden versleuteld over een netwerk verzonden.
- Opgegeven wachtwoorden worden altijd met een `one-way hash` functie versleuteld.
- Beveiligingsprogrammatuur heeft de mogelijkheid zowel programma's, netwer- als gebruikerssessies af te sluiten.
- Er worden vooraf gedefinieerde perioden (`time slots`) gebruikt, bijvoorbeeld voor overdracht van groepen bestanden (`batch file transfer`) of met regelmatig tussertijden terugkerende interactieve sessies van korte duur.
- Authenticatieprocedures worden herhaald op basis van hier hiervoor opgesleide beleid.
- Werkstations die niet in gebruik zijn, worden tegen onbevoegd gebruik beveiligd met behulp van een toetsvergroening of vergelijkbare beveiliging, bijvoorbeeld een wachtwoord.

C.13.7.8 Beheersbaarheid autorisaties

Beheersmaatregel

Verleende toegangsrechten zijn inzichtelijk en beheersbaar.

Implementatierichtlijnen

- De registratie van gebruikers en verleende toegangsrechten is zoveel mogelijk centraal geregeld (`single-point-of-administration`).
- Toegangsrechten worden zoveel mogelijk via groeperingsmechanismen (bijv. t.b.v. `RBAC`)

toegankelijk (dus niet rechtstreeks aan individuele gebruikers). Uitzonderingen vergen extra aandacht bij het beheer.

c) Voor groeperingsmechanismen geldt een naamgevingconventie, die aansluit op zo stabiel mogelijke uitgaanspunten (dus zo min mogelijk afhangingsgebonden als er regelmatig gebruikerswijzigingen plaatsvinden).

C.12.7.9 Volledigheid toegangsbeveiliging

Beleidsmaatregel

Op alle IT-voorzieningen is toegangsbeveiliging van toepassing.

Implementatierichtlijnen

a) Toegangsbeveiliging is geïmplementeerd op alle middelen die gegevens bevatten of verwerken. Dit betreft onder meer de volgende middelen:

1. platform (vast of mobiel werkplek, server, mainframe); bestanden, directory's, services en randapparatuur (zoek naar USB-afzetten op de werkplek);
2. ondersteunende systemen: services;
3. primaire systemen: toelichtingen in applicaties, stored procedures, gegevensbeheerders en databases (views, tabellen, velden, records);
4. beheer: beheer van applicaties en firmware van hardware voorzover dit kan. Mogelijk is er geen functioneelheid op de toegang tot firmware met een rechtenstructuur te beveiligen. Wel dient in ieder geval een wachtwoord te zijn ingesteld.

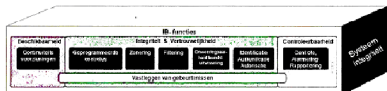
C.12.8. Vastleggen van gebeurtenissen

Doelstelling van de IS-functie

Handelingen in en meldingen van IT-voorzieningen in de technische infrastructuur worden vastgelegd in logging.

Definitie

Vastlegging van handelingen van personen en meldingen met betrekking tot de technische infrastructuur.



Toelichting

Een andere term voor het vastleggen van gebeurtenissen van de technische infrastructuur is logging. Voorbeelden van handelingen door natuurlijke personen zijn het wijzigen van parameters. Een foutmelding door een monitoring van de technische infrastructuur is een voorbeeld van een gebeurtenis.

Het onweerlegbaar vastleggen van gebeurtenissen is noodzakelijk om achteraf controle te kunnen uitvoeren en/of foutsituaties te kunnen onderzoeken. Het vastleggen is eveneens noodzakelijk als bewijsmiddel voor private of strafrechtelijke verdediging.

Veel gebeurtenissen die voor het beheer van de technische infrastructuur van belang zijn, hebben tevens betekenis in het kader van informatiebeveiliging.

Logging meet niet vervaard worden met het begrip audit trail, dat betrekking heeft op het vastleggen van het verwerkingsproces door toepassingprogrammeurs. Dit begrip wordt verder uitgewerkt bij de IO-functie 'Deprogrammeerde controles'.

Met vering

Het vastleggen van meldingen van beschadigingsprogramma's en andere systemen in de technische infrastructuur is noodzakelijk om achteraf controle te kunnen uitoefenen en/of foutsignalisatie te kunnen uitlokken. Het vastleggen is tevens noodzakelijk als bewijsmiddel voor private- of strafrechtelijke verdediging.

C.13.8.1 Aanmaken logbestanden

Beheersmaatregel

In de logging wordt informatie vastgelegd waarmee reproduceerbaar is wie waar en wanneer welke handelingen heeft verricht.

Toelichting

Logbestanden bevatten vaak een groot hoeveelheid informatie, waarvan een groot deel irrelevant is voor de controle van de beveiliging. Om gebeurtenissen te identificeren die significant zijn voor de controle van beveiliging, wordt overvoerd het juiste type berichten automatisch naar een tweede logbestand te kopiëren, en/of bepaalde systeemprogramma's of audit-hulpmiddelen voor bestandsindexering en -vernieuwing te gebruiken.

Implementatierichtlijnen

a) De volgende uitgevoerde handelingen worden in ieder geval opgenomen in de logging:

1. gebruik van technische beheerfuncties en systeemhulpdiensten, zoals het wijzigingen van configuratie of instelling, uitvoeren van een systeemcommando, starten en stoppen, uitvoering van een back-up of restore, (tijdelijke) toekennng en uitsluiting van hogere dan gebruikelijk rechten (incl. het collages versiert met geprivilegieerde accounts, zoals root, superuser, proddca etc.);
2. gebruik van functionele beheerfuncties, zoals het wijzigen van configuratie en instellingen, release van nieuwe functionaliteit, ingrepen in gegevenssets waaronder databases;
3. handelingen van beveiligingsbeheer, zoals het opvoeren of afvoeren gebruikers, toekennen en intrekken van rechten, wachtwoordreset, uitgifte en intrekken van cryptosleutels;
4. beveiligingsovertradingen (zoals de constatering van een virus, worm, Trojaans paard of andere malware, een poort scan of testen op zwakheden, foutieve inlogpogingen, overschrijding van autorisatiebevoegdheden, geweigerde pogingen om toegang te krijgen, het gebruik van niet operationele systeemservices, het starten en stoppen van security services);
5. veranderingen in het productieproces (zoals het vollopen van queues, systeemfouten, afbreken tijdens uitvoering van programma's, het niet beschikbaar zijn van aangeroepen procedurebestanden of systeembestanden);
6. handelingen van gebruikers, zoals veranderende toegangsrechten, gebruik van on-line transacties en sessies tot buiten de door systeembeheerders.

b) In een te schrijven logregel wordt in ieder geval aangegeven:

1. de naam van natuurlijke persoon herleidbare gebruikersnaam die verzocht een handeling uit te voeren;
2. het soort handeling, het gegeven commando met de parameters;
3. waar mogelijk de identiteit van het werkstation of de lokale;

4. het middel waarop de handeling werd uitgevoerd of waar een event optrad;
5. het resultaat van de handeling indien dit niet uit het soort handeling is af te leiden;
6. de datum en het tijdstip van een handeling of event;
7. de severity-aanduiding, het beveiligingsbeleg, waarop selectie t.b.v. de analyse kan plaatsvinden.

c) Systemklokken worden tijdens opstelling gesynchroniseerd en worden gelijk gezet met een vloerlok op de basis van het Network Time Protocol (NTP), zodat de julete tijd in het logbestand vastgelegd kan worden. Een indicatie voor de synchronisatie/frequentie is 4 uur. De maximale schrijfsnelheid van de standaard tijd is 100 miliseconden.

c) In een te schrijven logregel worden in geen geval gegevens opgenomen waardoor de beveiliging controleketen kan worden (zoals wachtwoorden, pinnummers).

C.13.8.2 Integriteit logbestanden

Beheersmaatregel

De integriteit van opgeslagen logbestanden is gewaarborgd.

Implementatierichtlijnen

- a) Bij het ontvroe en opslaan van logregels wordt zoveel mogelijk gebruik gemaakt van hiervoor ingerichte generieke beveiligingsvoorzieningen.
- b) Bij het aanleggen van logbestanden wordt zo mogelijk gebruik gemaakt van 'write once'-technologie.
- c) De volledigheid van de logging kan worden vastgesteld, bijvoorbeeld met behulp van opeenvolgende nummers per log-event.
- d) Uitsluitend geautoriseerde processen (specifiek onder een functioneel account) mogen logregels schrijven.
- e) Het raadplegen van logbestanden is voorbehouden aan geautoriseerde gebruikers, waarbij de toegang is beperkt tot leesrechten.
- f) Beheerders zijn niet in staat de instellingen van de logging te wijzigen of logbestanden te verwijderen, tenzij het specifiek hiervoor bevoegde beheerders zijn. Wanneer een systeem een specifieke rol voor audittoetsing krijgt, dan wordt hiervan gebruik gemaakt bij het raadplegen.

C.13.8.3 Beschikbaarheid logbestanden

Beheersmaatregel

De beschikbaarheid van loginformatie is gewaarborgd binnen de termijn waarin loganalyse noodzakelijk wordt geacht.

Implementatierichtlijnen

- a) Loginformatie wordt bewaard totdat de bewaartermijn is verstreken zijn. Een indicatie voor de bewaartermijn is:
 1. een transactie log wordt bewaard totdat is vastgesteld dat de juiste en volledige verwerking van de (betaal) transactie(s) heeft plaats gevonden of totdat de mogelijkheid van een rol-back uit te voeren is verstrekt, veelal maximaal één dag;
 2. een technische log wordt bewaard totdat is vastgesteld dat er zich geen verstoring in het systeem heeft voorgedaan, veelal maximaal enkele dagen tot een week;
 3. logging die van belang is voor auditing en onderzoek maar originairlijk gebruik wordt 2 jaar bewaard dan wel zodanig als de gerechtelijke procedure duurt waarvoor de loggegevens als bewijsmateriaal dienen.

- b) Er zijn query- en analysetools aanwezig voor het kunnen ontlasten van loginformatie.
- c) Het overschrijven of verwijderen van logbestanden wordt gelokt in de nieuw aangelegde log.
- d) Het vollopen van het opslagmedium voor de logbestanden wordt gelokt en leidt tot automatische alarmering van de beheerorganisatie; bij kritische toevalligheden leidt het vollopen van het logbestand tot het stilzetten van de verwerking totdat nieuwe ruimte voor loggegevens beschikbaar is. Het volgelopen opslagmedium wordt pas weer vrijgegeven nadat de logbestanden zijn zakergesteld (op een ander medium).
- e) Bij verdere op analyse- en reactieproceduresingen voor een logbestand wordt de nieuwste compatibiliteit afdrukt. Dit wil zeggen dat ook de eerder aangelegde logbestanden binnen de bewaartijd van het logbestand met de nieuwe of gewijzigde voorziening ontlasten kunnen worden.

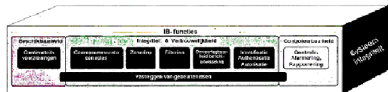
C.13.8. Controle, alarmering en rapportering

Doelstelling

In de technische infrastructuur zijn signaleringsfuncties werkzaam ter controle op vastgestelde inrichtingsdocumenten (configuratie-dossier).

Definitie

Functies die erop gericht zijn te kunnen vaststellen dat de IT-voorzieningen overeenkomstig het vastgestelde inrichtingsdocument (configuratie-dossier) functioneren en die signaleren wanneer dit niet het geval is of kan worden.



Toelichting

De toelichting die in de markt verkrijgbaar is, maakt het mogelijk al deze functies geïntegreerd te behandelen. Zonde: integrale zijn deze functies niet effectief te beheersen. Om die reden worden de hier bedoelde signaleringsfuncties als één geheel behandeld.

De signaleringsfuncties zijn als volgt afzonderlijk toe te lichten:

- Controle is de toets of een IT-voorziening is ingesteld conform een vastgesteld inrichtingsdocument (configuratie-dossier).
- Alarmering is een functie, die onmiddellijk signaleert naar systeembeheerders kan afgeven als er afwijkingen van het vastgestelde inrichtingsdocument (configuratie-dossier) worden overschreden.
- Rapportering maakt het mogelijk beveiligingsincidenten, zoals hacking (ook van binnen uit) te onderzoeken op basis van analyses en correlatie van vastleggingen.

Motivering

Op basis van de signaleringen kunnen beheerders acties ondernemen om veranderingen in de productieverwerking te voorkomen of om beveiligingsrisico's in de werking van een infrastructuur te kunnen beheersen.

C.13.8.1 Controle op beveiligingsinstellingen

Beheersmaatregel

instellingen van functies die voor de informatiebeveiliging van belang zijn en wijzigingen daarin worden automatisch gecontroleerd.

Implementatierichtlijnen

- Rijautomatische controle op beveiligingsinstellingen wordt niet inhervagen van het 'Sail-twistend van' beveiligingsinstellingen geschieden van andere systeemfuncties.
- Instellingen van IS-functies, die betrokken zijn bij filtering kunnen automatisch op wijzigingen worden gecontroleerd en gealarmeerd.

C.13.9.2 Automatische signalering

Beheersmaatregel

Tevoren gespecificeerde, a'wijkende gebeurtenissen volgens de loginformatie worden tijdig gesigaleerd en zo nodig gealarmeerd.

Implementatierichtlijnen

- Er is gespecificeerd welke beveiligingsincidenten kunnen optreden. Deze beveiligingsincidenten zijn geclassificeerd naar ernst en urgentie.
- Instelbaar is bij welke drempelwaarden (gebaseerd op de ernst en urgentie van een gebeurtenis daarbij rekening houdend met hoe vaak een gebeurtenis voorkomt) een melding wordt gegeven die direct zichtbaar is voor de beheerorganisatie.
- Instelbaar is de welke drempelwaarden de beheerorganisatie wordt gealarmeerd, zonodig ook buiten kantooruren.
- De IS-functies voor Filtering en Logische Toegangbeveiliging sluiten aan op de generieke beveiligingsvoorziening voor Security Incident and Event Management (SIEM) waarmee meldingen en alarmoproepen naar de beheerorganisatie gegeven kunnen worden.

C.13.9.3 Analyse en rapportage

Beheersmaatregel

Logbestanden worden periodiek geanalyseerd en gecontroleerd ten einde beveiligingsnodigheden dan wel de juiste werking van het systeem te detecteren.

Implementatierichtlijnen

- Periodiek worden er automatisch correlaties en rapportages gemaakt over de verschillende vastgelegde gebeurtenissen.
- Periodiek worden er manaralyas vervaardigd en gerapporteerd over relevante gebeurtenissen in de logbestanden van een in te stellen periode.

C.13.10 Systeemintegriteit

Doelstelling

In de technische infrastructuur zijn functies werkzaam, die de systeemintegriteit ondersteunen.

Definitie

Het focus is uitvoeren van de beoogde bewerkingen door de technische infrastructuur.



Toelichting

De factoren die in de mededinging het functioneren van geautomatiseerde bewakingsfuncties bepalen zijn legio en als geheel niet logisch onder te brengen onder één van de andere IB-functies. Factoren zijn o.a. 'bugs' in programmatuur, het bestaan van ongewenste applicatieve- en infrastructuurfuncties, onjuiste of onbetrekkende configuratie-instellingen van programmatuur, pakketten en voorwerpen van de technische infrastructuur, bijzondere deployment (functionele configuratie) van applicaties en/of infrastructuur.

Afbakening

De scope van de hieronder genoemde maatregelen is voor zover het door andere functies bepaald, beperkt tot controlemechanismen op de actualiteit van de code, de integriteit van programmapakketten en infrastructuurle programmatuur en mechanismen tot beheersing van mobiele code en testcode overgang instellingen voor "handhaving" van systemen. In de maatregelen is (nog) geen uitwerking gegeven aan normen voor wetgevingen.

Motivatie

In de huidige technologie bestaat een aantal risico's, die onder de noemer van systeeminzichtigheid als toepastbaar op IB-functies zijn aangemerkt. De maatregelen gericht op de risico's zijn aan de praktijk ontleend.

C.13.10.1 Handhaven technische functionaliteit

Deheersmaatregel

De door de leverancier bepaalde technische functionaliteit van programmapakketten en infrastructuurle programmatuur blijven gehandhaafd.

Toelichting op afbakening

In dit document worden voor de onderkende IB-functies normen gedefinieerd, die daals bedoeld zijn voor de instellingen van infrastructuurle elementen van II-voorwerpen. Het is echter niet mogelijk om voor alle beschikbare relevante instellingen productafhankelijke normen te formuleren. Daarom blijft het noodzakelijk om alle overige instellingen op beveiligingsniveau te bevoorwaarden.

Implementatieplichtlijnen

- De technische integriteit van programmapakketten en infrastructuurle programmatuur wordt gecontroleerd d.m.v. een heftingsmechanisme en een controegetal van de leverancier, dat via een vertrouwd kanaal is verkregen.
- Behoudens de door de leverancier goedgekeurde updates worden er geen wijzigingen aangebracht in programmapakketten en infrastructuurle programmatuur.
- De instellingen (parameterregels) van programmapakketten en infrastructuurle programmatuur zijn in overeenstemming met een vastgestelde heftingsgegevenslijst (configuratiebestand), dat is gebaseerd op de vereisten van de leveranciers, operationele productstandaards van de voorkeur onafhankelijke instellingen, zoals die van NIST, voor zover de instellingen niet door de andere IB-functies van dit document zijn gedefinieerd.

- d) Instellingen van programmapakketten en infrastructurele programmatuur kunnen geautomatiseerd worden gecontroleerd op configuratieafwijkingen van het vastgestelde inrichtingsdocument.
- e) Van programmapakketten en infrastructurele programmatuur kan bij voorkeur geautomatiseerd gecontroleerd worden of de laatste updates (patches) in zijn voorgevoerd.
- f) Het automatisch doorvoeren van een update vindt alleen plaats als hierover specifieke afspraken zijn gemaakt met de leverancier.
- g) Van programmapakketten en infrastructurele programmatuur kan bij voorkeur geautomatiseerd gecontroleerd worden of er bekende zwakheden in de configuratie voorkomen.

C.13.10.2 **Systeemhulpmiddelen**

Beheersmaatregel

Het gebruik van hulpprogrammatuur waarmee maatregelen in systeem- en toepassingssoftware zouden kunnen worden gepast, wordt zoveel mogelijk beperkt.

Implementatierichtlijn

- a) Identificatie-, authenticatie- en autorisatiemechanismen zijn ook voor systeemhulpmiddelen van toepassing.
- b) Systeemhulpmiddelen en toepassingsprogrammatuur zijn gescheiden.
- c) Onnodige hulpprogramma's en systeemprogrammatuur zijn verwijderd.

C.13.10.3 **Hardering**

Beheersmaatregel

Infrastructurele programmatuur, die vitale beveiligingsfuncties vervullen, bevat geen eronvulge en ongebruikte functies.

Toelichting

Witale beveiligingsfuncties hebben hier betrekking op infrastructurele voorzieningen, die de zoneering bepalen, deel uitmaken van de beheer en audit zone en van de zone waar de data van de bedrijfsapplicaties worden opgeslagen.

Afbakening

Waar het "harderen" van infrastructurele IT-voorzieningen moet plaatsvinden aan de andere normen voor deze voorzieningen. Bij afwijkingen wordt er van uitgegaan die op onderliggende besturingssystemen reeds gehardend zijn.

Implementatierichtlijn

- a) Onnodige en ongebruikte functies van infrastructurele programmatuur zijn uitgeschakeld.
- b) Beheerregels (hardening) zijn zoveel mogelijk afgesloten.
- c) Er is zoveel mogelijk gebruik gemaakt van vaststaande beheermechanismen.
- d) Beheer is alleen toegestaan vanaf vooraf gedefinieerde IP-adressen.
- e) Voor toegang tot switches wordt gebruik gemaakt van Virtual LAN's (VLAN) en de toegang tot netwerken wordt beperkt op basis van MAC-adres (port security).

C.13.10.4 **Mobile code**

Beheersmaatregel

Als gebruik van 'mobile code' wordt toegelaten, dan zorgt de configuratie ervoor dat de geautoriseerde 'mobile code' functioneert volgens een vastgesteld inrichtingsdocument (configuratieset) en voorkomt de configuratie dat niet-toegelaten 'mobile code' wordt uitgevoerd.

Toelichting

'Mobile code' is programmatuur die kan worden overgedragen van de ene naar de andere computer, automatisch wordt uitgevoerd op een specifieke functie verricht zonder of met weinig tussenkomst van de gebruiker. 'Mobile code' werkt samen met bestuursprogrammatuur (zo'n 'middleware'), die de informatie-uitwisseling regelt tussen de clientsoftware en de software die de bedrijfsgegevens beheert. Vaak gaat het om gedistribueerde systemen en meerdere platformen.

Implementatierichtlijnen

- a) De volgende handelingen worden overwogen om te verhindern dat 'mobile code' ongeautoriseerde acties kan uitvoeren:
1. uitvoeren van toegestane 'mobile code' in een logisch geïsoleerde omgeving;
 2. blokkeren van elk gebruik van 'mobile code';
 3. blokkeren van ontvangen van 'mobile code';
 4. activeren van technische maatregelen die beschikbaar zijn op een specifiek systeem om te verhinderen dat toegestane 'mobile code' wordt beheerd;
 5. beheersen van de bronnen die beschikbaar zijn voor toegang tot toegestane 'mobile code';
 6. cryptografische beveiligingsmaatregelen om toegestane 'mobile code' uniek te authenticeren.

C.12.16.5 Beheersing berichtverwerking**Beheersmaatregel**

De technische infrastructuur voor berichtverwerking is zodanig ontworpen en ingericht, dat foutsituaties worden voorkomen of herkend en dat functioneel beheer over foutbestanden mogelijk is.

Implementatierichtlijnen

- a) Infrastructuur bevat logica die het beheer van foutbestanden mogelijk maakt.
- b) Berichtverwerkende infrastructuur past foutloze berichtverwerking toe (Persistence Messaging).
- c) Foutbestanden worden niet gehandeld als opslagmechanisme (buffering). Voor tijdelijke opslag van berichten in verwerkingketens worden aparte tussenbestanden gebruikt.
- d) Stapelen van fouten wordt voorkomen door toepassing van 'noocloop' mechanismen. Juist verzonden resultaten worden hierdoor niet noodgedwongen naar een foutloze verwerkingscycclus gestuurd.

C.12.10.6 Beheersing batchverwerking**Beheersmaatregel**

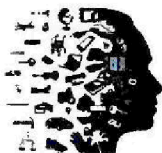
Bij batchverwerking worden productieplanning en/of bewakingscycli zodanig ingesteld dat de risico's van verwerkingfouten die tot verlies van inligtelijke zaken kunnen leiden gemitigeerd worden.

Implementatierichtlijnen

- a) De planning van reguliere batchprogramma's is gebaseerd op de aangegeven tijdslijnen en voldoende volgens de systeemdocumentatie en houdt rekening met de afhankelijkheden die er tussen verwerkingen en met andere applicaties kan bestaan, start van de eerste taak en beëindiging van de laatste taak.
- b) Onderdelen voor verwerking van batches worden pas opgestart, nadat voorgaande verwerkingen succesvol zijn beëindigd.
- c) Generatievalidatie- en herstelmechanismen voorkomen dubbele of onvolledige verwerkingen en worden gedurende verwerkingen (of bij het oplossen van productiefouten).
- d) Bij uitwisseling van bestanden tussen centrale en decentrale servers of met externe partijen wordt

met een apertie-transformatiemechanisme zeker gesteld dat uitwisseling niet achterwege blijft of dubbel plaatsvindt, tenzij benadering geheel kan plaatsvinden volgens punt f hierboven.

e) Er wordt een logbestand aangemaakt van de activiteiten die tijdens de verwerking plaatsvinden.



**AUTORITEIT
PERSOONSGEGEVENS**

Autoriteit Persoonsgegevens
Postbus 93374, 2509 AJ Den Haag
Bezuidenhoutseweg 30, 2594 AV Den Haag
T 070 8888 500 - F 070 8888 501
autoriteitpersoonsgegevens.nl

Vertrouwelijk/Aangetekend

Ministerie van Financiën
Directoraat-Generaal Belastingdienst
Concerndirectie Informatievoorziening en databeheersing
Ter attentie van:
Mevrouw drs. A.C. van Huffelen

Persoonsgegevens

Korte Voorhout 7
2500 EE Den Haag

3SRRC15346681

3SRRC15346682

Datum
12 november 2021

Ons kenmerk
z2021-16923

Contactpersoon

Persoonsgegevens

Onderwerp
Kopie voornemen handhaving en gelegenheid tot geven zienswijze

Geachte mevrouw Van Huffelen,

De Autoriteit Persoonsgegevens (AP) heeft het verwerken van persoonsgegevens in de Fraude Signaleringsvoorziening (FSV) en het gebruik van deze applicatie door de Belastingdienst onderzocht.

Hierbij treft u ter informatie een afschrift aan van de brief die de AP in het kader van deze zaak heeft verzonden aan de heer W.B. Hoekstra, minister van Financiën. Het betreft een voornemen tot handhaven en een gelegenheid tot het geven van een zienswijze op zowel de inhoud van het rapport als de mogelijke oplegging van een sanctie. Korthedshalve verwijs ik u naar de inhoud van deze brief.

Ik vertrouw er op u hiermee naar behoren te hebben geïnformeerd.

Hoogachtend,
de Autoriteit Persoonsgegevens,

Persoonsgegevens



AUTORITEIT
PERSOONSGEGEVENS

Autoriteit Persoonsgegevens
Postbus 90338
2500 LE Den Haag
T: 070 378 0600
E: autoriteit.persoonsgegevens.nl

De heer mr. W.B. Hoekstra, MBA
De minister van Financiën
Ter attentie van:
De heer mr. W.B. Hoekstra, MBA

Persoonsgegevens

Korte Voorhout 7
2500 EE Den Haag

Datum

10 oktober 2021

Ons kenmerk

11000056

Contactpersoon

W.B. Hoekstra

Onderwerp

Voornemen handhaving en gelegenheid tot geven zienswijze

Geachte heer Hoekstra,

De Autoriteit Persoonsgegevens (AP) heeft onderzoek gedaan naar het verwerken van persoonsgegevens in de Fraude Signalering Voorziening (FSV) van de Belastingdienst. De AP heeft op 29 oktober 2021 het definitief rapport met de bevindingen over dit onderzoek aan mevrouw Van Huffelen verstrekt.

Samengevat concludeert de AP in het rapport dat de minister van Financiën, als verwerkingsverantwoordelijke voor de verwerkingen van de Belastingdienst, van 4 november 2013 tot en met 27 februari 2020 door het verwerken van persoonsgegevens in FSV in strijd heeft gehandeld met de beginselen van rechtmatigheid, doelspecificatie, juistheid en opslagbeperking.¹

Naast het overtreden van de vier hiervoor benoemde beginselen concludeert de AP dat de Belastingdienst onvoldoende passende technische en organisatorische maatregelen heeft genomen ten aanzien van de toegangsbeveiliging, logging en controle op de logging om een passend beveiligingsniveau voor de persoonsgegevens in FSV te waarborgen.² Tot slot heeft de AP geconcludeerd dat de Belastingdienst de Functionaris gegevensbescherming niet naar behoren en tijdig heeft betrokken bij de uitvoering van de gegevensbeschermingseffectbeoordeling van FSV.³

¹ Zie artikel 5, eerste lid, aanhef en onder a, van de AVG en artikel 6 van de Wbp (rechtmatigheid), artikel 5, eerste lid, aanhef en onder b, van de AVG en artikel 7 van de Wbp (doelspecificatie), artikel 5, eerste lid, aanhef en onder d, van de AVG en artikel 11, tweede lid, van de Wbp (juistheid) en artikel 5, eerste lid, aanhef en onder e, van de AVG en artikel 10, eerste lid, van de Wbp (opslagbeperking)

² Zie artikel 32, eerste lid, aanhef van de AVG en artikel 13 van de Wbp.

³ Zie artikel 38, eerste lid, van de AVG jo. artikel 35, tweede lid, van de AVG.



Datum

2 november 2021

Ons kenmerk

Z100-19908

De AP is voornemens om, gelet op de bovenstaande geconstateerde overtredingen, de haar toekomende bevoegdheid tot het opleggen van een sanctie aan te wenden. U dient ermee rekening te houden dat dit kan resulteren in het opleggen van een bestuurlijke boete en/of een corrigerende maatregel.

Ingeval de AP overgaat tot boeteoplegging bepaalt zij de hoogte van de boete aan de hand van de door haar vastgestelde Boetebeleidsregels.⁴ Deze kunt u vinden op de website van de AP. De basisboetes kunnen worden verhoogd of verlaagd afhankelijk van de mate waarin de factoren die zijn genoemd in artikel 7 van de Boetebeleidsregels daartoe aanleiding geven.

Voordat de AP hierover beslist, stel ik u in de gelegenheid om een zienswijze te geven op zowel de inhoud van het rapport als de mogelijke oplegging van een sanctie. Een schriftelijke zienswijze ontvangt de AP graag uiterlijk **13 december 2021**. Als u uw reactie mondeling wenst te geven, verneemt de AP dat graag uiterlijk **22 november 2021**. U kunt hiervoor contact opnemen met bovengenoemd contactpersoon.

Een afschrift van deze brieven en de onderliggende op de zaak betrekking hebbende stukken zullen verstuurd worden naar de Belastingdienst.

Ik vertrouw er op u hiermee naar behoren te hebben geïnformeerd.

Indien u vragen heeft over deze brief, dan wel informatie wilt doorgeven of versturen, verzoek ik u contact op te nemen met bovengenoemd contactpersoon.

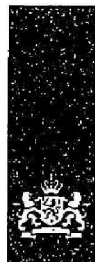
Hoogachtend,
Autoriteit Persoonsgegevens,
Namens deze,

Persoonsgegevens

⁴ Beleidsregels van de Autoriteit Persoonsgegevens van 19 februari 2019 met betrekking tot het bepalen van de hoogte van bestuurlijke boetes., *Stcrt.* 2019, 14586.

FSV

Deel 3/5



Ministerie van Financiën

Handboek Beveiliging Belastingdienst

2017

Deel D
Implementatierichtlijnen
BCM

Boekdata

Titel Handboek Beveiliging Belastingdienst 2017
Deel D : Implementatierichtlijnen BCM

Versie December 2016

Versie	Opmerkingen - revisies
December 2014	Eerste jaargang HBB Deel D
Februari 2016	Tweede jaargang HBB Deel D
December 2016	Derde jaargang HBB Deel D – Dit document bevat de vertaling in het Nederlands van de Europese norm EN ISO 22313:2014. – Bron: Rijksoverheid NEN Connect 2016-2020

Nederlandse norm

NEN-EN-ISO 22313

(nl)

Maatschappelijke veiligheid -
Managementsystemen voor bedrijfscontinuïteit
(business continuity management systems) -
Richtlijnen (ISO 22313:2012, IDT)

Societal security -
Business continuity management systems -
Guidance (ISO 22313:2012, IDT)

ICS 03.100.01
november 2014

ICS 03.100.01

Nederlandstalige versie

Maatschappelijke veiligheid – Managementsystemen voor bedrijfscontinuïteit (business continuity management systems) – Richtlijnen (ISO 22313:2012)

Sicherheit und Schutz des
Gemeinwesens –
Aufrechterhaltung der
Betriebsfähigkeit – Leitlinie
(ISO 22313:2012)

Societal security – Business
continuity management systems –
Guidance (ISO 22313:2012)

Sécurité sociétale – Systèmes de
management de la continuité
d'activité – Lignes directrices
(ISO 22313:2012)

Deze norm is de Nederlandstalige versie van de Europese norm EN ISO 22313:2014. Hij is vertaald door NEN. Hij heeft dezelfde status als de officiële versies.

Deze Europese norm is door CEN aangenomen op 18 oktober 2014.

CEN-leden zijn verplicht zich te houden aan het huishoudelijk reglement van CEN-CENELEC, waarin is vastgelegd onder welke voorwaarden aan deze Europese norm, zonder veranderingen, de status van nationale norm moet worden gegeven. Bijgewerkte lijsten van en bibliografische gegevens betreffende zulke nationale normen kunnen op aanvraag worden verkregen bij het managementcentrum van CEN-CENELEC en bij elk CEN-lid.

Deze Europese norm bestaat in drie officiële versies (Duits, Engels en Frans). Een versie in een andere taal die onder verantwoordelijkheid van een CEN-lid in zijn landstaal is gemaakt en die is aangemeld bij het managementcentrum van CEN-CENELEC, heeft dezelfde status als de officiële versies.

Leden van CEN zijn de nationale normalisatieorganisaties van België, Bulgarije, Cyprus, Denemarken, Duitsland, Estland, Finland, Frankrijk, Griekenland, Hongarije, Ierland, IJsland, Italië, Kroatië, Letland, Litouwen, Luxemburg, Macedonië, Malta, Nederland, Noorwegen, Oostenrijk, Polen, Portugal, Roemenië, Slovenië, Slowakije, Spanje, Tsjechië, Turkije, het Verenigd Koninkrijk, Zweden en Zwitserland.

CEN

Europees Comité voor Normalisatie
Europäisches Komitee für Normung
European Committee for Standardization
Comité Européen de Normalisation

Managementcentrum CEN-CENELEC: Marnixlaan 17, B-1000 Brussel

© 2014 CEN

Alle rechten van gebruik, in welke vorm en op welke wijze dan ook, zijn voorbehouden aan CEN-leden.

Ref. nr. EN ISO 22313:2014 nl

Inhoud

ISO-voorwoord	6
Inleiding	7
1 Onderwerp en toepassingsgebied	13
2 Normatieve verwijzingen	13
3 Termen en definities	13
4 Context van de organisatie	14
4.1 Inzicht in de organisatie en haar context	14
4.2 Inzicht in de behoeften en verwachtingen van belanghebbenden	15
4.3 Het toepassingsgebied van het BCMS vaststellen	16
4.4 Managementsysteem voor bedrijfscontinuïteit	17
5 Leiderschap	17
5.1 Leiderschap en betrokkenheid	17
5.2 Betrokkenheid van de directie	17
5.3 Beleid	18
5.4 Rollen, verantwoordelijkheden en bevoegdheden binnen de organisatie	19
6 Planning	20
6.1 Acties om risico's en kansen op te pakken	20
6.2 Doelstellingen voor bedrijfscontinuïteit en de planning om ze te bereiken	20
7 Ondersteuning	20
7.1 Middelen	20
7.2 Competentie	22
7.3 Bewustzijn	24
7.4 Communicatie	25
7.5 Gedocumenteerde informatie	26
8 Uitvoering	28
8.1 Operationele planning en beheersing	28
8.2 Bedrijfsimpactanalyse en risicobeoordeling	31
8.3 Strategie voor bedrijfscontinuïteit	35
8.4 Vaststellen en implementeren van procedures voor bedrijfscontinuïteit	43
8.5 Oefening en testen	55
9 Evaluatie van de prestaties	57
9.1 Monitoren, meten, analyseren en evalueren	57
9.2 Interne audit	60
9.3 Directiebeoordeling	60
10 Verbetering	62
10.1 Afwijkingen en corrigerende maatregelen	62
10.2 Continue verbetering	62
Bibliografie	64

ISO-voorwoord

ISO (International Organization for Standardization) is een wereldwijde federatie van nationale normalisatie-instituten (de ISO-leden). Het voorbereidingswerk voor internationale normen wordt doorgaans uitgevoerd door de technische commissies van ISO. Elk lid dat interesse heeft in een onderwerp waarvoor een technische commissie is samengesteld, heeft recht op vertegenwoordiging in deze commissie. Ook internationale organisaties, zowel overheidsinstanties als niet-gouvernementele organisaties, nemen in samenwerking met ISO deel aan deze werkzaamheden. ISO werkt nauw samen met de International Electrotechnical Commission (IEC) inzake alle elektrotechnische normalisatie.

Internationale normen worden opgesteld overeenkomstig de voorschriften die in de ISO/IEC-richtlijnen deel 2 zijn opgenomen.

De voornaamste taak van de technische commissies is de voorbereiding van internationale normen. Ontwerpversies van internationale normen die zijn aangenomen door de technische commissies, worden ter stemming voorgelegd aan de leden. Publicatie als internationale norm vereist goedkeuring van ten minste 75 % van de stemmen die zijn uitgebracht door deelnemende leden.

Er wordt gewezen op de mogelijkheid dat sommige elementen van dit document onderwerp kunnen zijn van patentrechten. ISO is niet verantwoordelijk voor identificatie van dergelijke patentrechten.

ISO 22313 werd opgesteld door Technische Commissie ISO/TC 223, *Societal security*.

Inleiding

Algemeen

Deze internationale norm geeft, indien van toepassing, richtlijnen voor de eisen die zijn beschreven in ISO 22301:2012 en in relatie hiermee aanbevelingen ('behoort te') en goedkeuring ('kunnen/mogen'). Het is niet de bedoeling van deze internationale norm om algemene richtlijnen voor alle aspecten van bedrijfscontinuïteit te geven.

Deze internationale norm heeft dezelfde hoofdstuktitels als ISO 22301 maar herhaalt niet de eisen voor managementsystemen voor bedrijfscontinuïteit en de termen en definities die ermee samenhangen. Organisaties die geïnformeerd willen worden over deze eisen, termen en definities moeten daarom ISO 22301 en ISO 22300 raadplegen.

Om nadere opheldering en uitleg over belangrijke punten te geven, bevat deze internationale norm een aantal figuren. Die figuren dienen alleen voor illustratieve doeleinden en de gerelateerde tekst in deze internationale norm heeft voorrang boven de figuren.

Een BCMS benadrukt het belang van:

- het onderkennen van de behoeften van de organisatie en de noodzaak om beleid en doelstellingen voor bedrijfscontinuïteitsmanagement vast te stellen;
- het implementeren en uitvoeren van beheersmaatregelen die ervoor zorgen dat een organisatie het vermogen heeft om versturende incidenten te managen;
- monitoren en beoordelen van de prestaties en de doeltreffendheid van het BCMS; en
- continue verbetering gebaseerd op objectieve meting.

Net als elk ander managementsysteem bestaat een BCMS uit de volgende hoofdcomponenten:

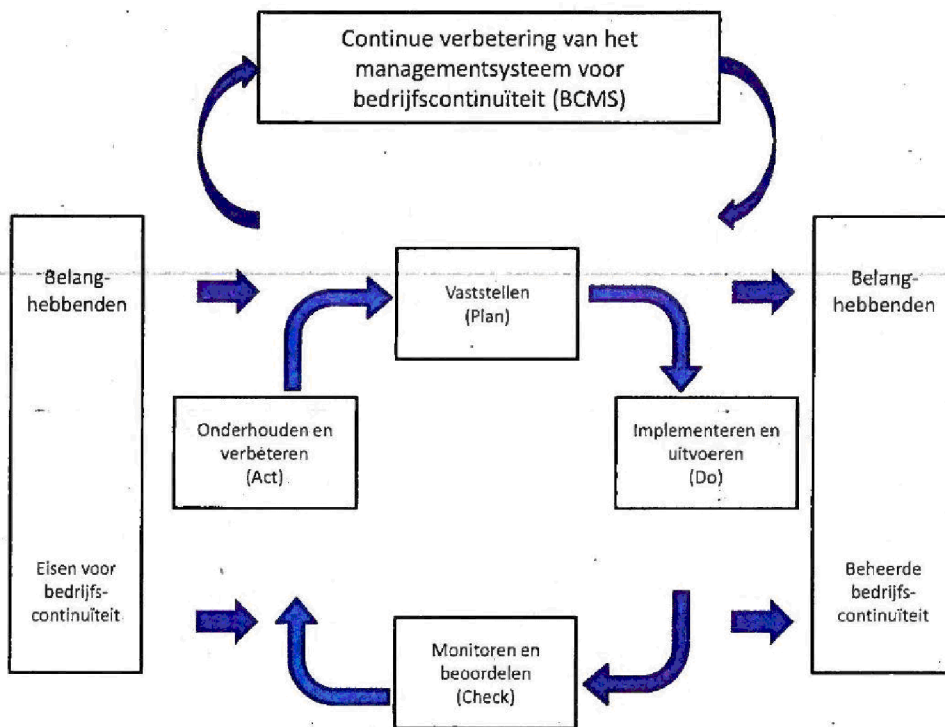
- a) beleid;
- b) mensen met gedefinieerde verantwoordelijkheden;
- c) managementprocessen met betrekking tot:
 - 1) beleid;
 - 2) planning;
 - 3) implementatie en uitvoering;
 - 4) prestatiebeoordeling;
 - 5) directiebeoordeling; en
 - 6) verbetering.
- d) documentatie waarmee auditeerbaar bewijsmateriaal wordt geleverd; en
- e) de BCMS-processen die relevant zijn voor de organisatie.

Bedrijfscontinuïteit is in het algemeen bedrijfsspecifiek, maar de implementatie ervan kan verstrekkende implicaties hebben voor de maatschappij en andere derden. Een organisatie heeft waarschijnlijk externe organisaties waar zij afhankelijk van is, en andere organisaties zijn afhankelijk van haar. Doeltreffende bedrijfscontinuïteit draagt daarom bij aan een veerkrachtiger maatschappij.

De Plan-Do-Check-Act-cyclus

Deze internationale norm past de Plan-Do-Check-Act (PDCA)-cyclus toe voor het plannen, inrichten, implementeren, uitvoeren, monitoren, beoordelen, onderhouden en continu verbeteren van de doeltreffendheid van het BCMS van de organisatie.

Figuur 1 laat zien hoe het BCMS de eisen van de belanghebbenden neemt als input voor bedrijfscontinuïteitsmanagement (BCM) en, door middel van de vereiste handelingen en processen, als uitkomsten continuïteit levert (d.w.z. beheerde bedrijfscontinuïteit) die aan deze eisen voldoet.



Figuur 1 — PDCA-model toegepast op BCMS-processen

Tabel 1 — Verklaring van het PDCA-model

Plan (Vaststellen)	Beleid, doelstellingen, taakstellingen, beheersmaatregelen, processen en procedures voor bedrijfscontinuïteit vaststellen die relevant zijn om de bedrijfscontinuïteit te verbeteren, teneinde resultaten te leveren die overeenstemmen met het algehele beleid en de doelstellingen van de organisatie.
Do (Implementeren en uitvoeren)	Beleid, beheersmaatregelen, processen en procedures voor bedrijfscontinuïteit implementeren en uitvoeren.
Check (Monitoren en beoordelen)	De prestaties ten opzichte van doelstellingen en beleid voor bedrijfscontinuïteit monitoren en beoordelen, de resultaten ter beoordeling aan het management rapporteren, en geaccordeerde maatregelen voor herstel en verbetering vaststellen.
Act (Onderhouden en verbeteren)	Het BCMS onderhouden en verbeteren door corrigerende maatregelen te nemen, op basis van de resultaten van de directiebeoordeling en herbeoordeling van het toepassingsgebied van het BCMS en tevens van het beleid en de doelstellingen voor bedrijfscontinuïteit

Componenten van PDCA in deze internationale norm

Er bestaat een directe relatie tussen de inhoud van figuur 1 en de hoofdstukken van deze internationale norm:

Tabel 2 — Relatie tussen het PDCA-model en de hoofdstukken 4 t/m 10

PDCA-component	Hoofdstuk dat een PDCA-component behandelt
Plan (Vaststellen)	Hoofdstuk 4 (Context van de organisatie) beschrijft wat de organisatie moet doen om zeker te stellen dat het BCMS voldoet aan de eisen, rekening houdend met alle relevante externe en interne factoren, met inbegrip van: <ul style="list-style-type: none"> — de behoeften en verwachtingen van belanghebbenden, — de verplichtingen voortkomend uit wet- en regelgeving, — het vereiste toepassingsgebied van het BCMS.
	Hoofdstuk 5 (Leiderschap) beschrijft de belangrijke rol van management in de zin van betrokkenheid tonen, beleid definiëren en rollen, verantwoordelijkheden en bevoegdheden vaststellen.
	Hoofdstuk 6 (Planning) beschrijft de maatregelen die nodig zijn om strategische doelstellingen en beginselen voor het BCMS als geheel vast te stellen. Deze geven de context voor de bedrijfsimpactanalyse en risicobeoordeling (8.2) en de bedrijfscontinuïteitsstrategie (8.3).
	Hoofdstuk 7 (Ondersteuning) identificeert de belangrijke elementen die aanwezig moeten zijn om het BCMS te ondersteunen, namelijk: middelen, competentie, bewustzijn, communicatie en gedocumenteerde informatie.
	Do (Implementeren en uitvoeren)

Check (Monitoren en beoordelen)	Hoofdstuk 9 (Evaluatie van de prestaties) biedt de basis voor het verbeteren van het BCMS door de prestatie te meten en te evalueren.
Act (Onderhouden en verbeteren)	Hoofdstuk 10 (Verbetering) behandelt de corrigerende maatregelen die nodig zijn om afwijkingen die door evaluatie van de prestatie zijn geïdentificeerd aan te pakken.

Bedrijfscontinuïteit

Bedrijfscontinuïteit is het vermogen van de organisatie om na een verstorend incident producten of diensten te blijven leveren op acceptabele, vooraf vastgestelde niveaus. Bedrijfscontinuïteitsmanagement (BCM) is het proces waarmee bedrijfscontinuïteit bereikt wordt en gaat over het voorbereiden van een organisatie op het afhandelen van versturende incidenten die anders zouden kunnen verhinderen haar doelstellingen te bereiken.

Door BCM te plaatsen binnen het kader en de disciplines van een managementsysteem wordt een bedrijfscontinuïteitsmanagementsysteem (BCMS) gecreëerd waardoor het BCM kan worden beheerst, geëvalueerd en continu verbeterd.

In deze internationale norm wordt het woord bedrijf gebruikt als een allesomvattende term voor de activiteiten en diensten die een organisatie verricht bij het nastreven van haar doelstellingen, doelen of missie. Als zodanig is het gelijkelijk van toepassing op grote, middelgrote en kleine organisaties die actief zijn in industriële, commerciële, publieke en non-profitsectoren.

Elk incident, groot of klein, natuurlijk, per ongeluk of opzettelijk, heeft de potentie om een grote verstoring te veroorzaken in de bedrijfsactiviteiten van een organisatie en haar vermogen om producten en diensten te leveren. Door echter bedrijfscontinuïteit te implementeren voordat zich een verstorend incident voordoet, in plaats van te wachten totdat het gebeurt, is de organisatie in staat haar bedrijfsactiviteiten voort te zetten voordat dit leidt tot onacceptabele impactniveaus.

BCM houdt in:

- a) duidelijk zijn over de belangrijkste producten en diensten van de organisatie en de activiteiten waar zij uit voortkomen;
- b) de prioriteiten kennen voor het voortzetten van activiteiten en de middelen die hiervoor vereist zijn;
- c) duidelijk inzicht hebben in de bedreigingen voor deze activiteiten, met inbegrip van hun afhankelijkheden, en weten wat de gevolgen zijn als de activiteiten niet hervat worden;
- d) beschikken over beproefde en vertrouwde voorzieningen om deze activiteiten te hervatten na een verstorend incident; en
- e) bewerkstelligen dat deze voorzieningen volgens vaste regels worden beoordeeld en geactualiseerd, zodat ze in alle omstandigheden doeltreffend zijn.

Bedrijfscontinuïteit kan doeltreffend zijn bij het behandelen van zowel plotselinge versturende incidenten (bijv. explosies) als incidenten die zich geleidelijk voltrekken (bijv. griepandemieën).

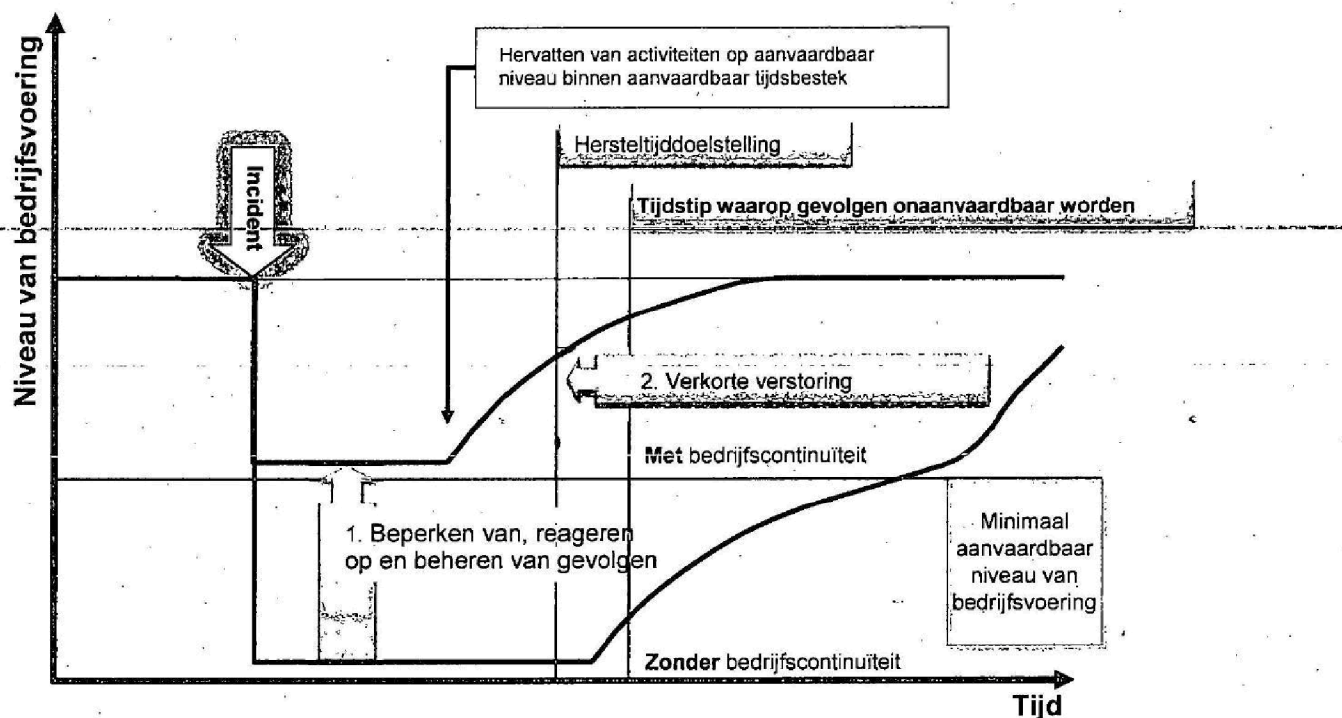
Activiteiten kunnen worden verstoord door veel verschillende incidenten die vaak moeilijk te voorspellen of te analyseren zijn. Door de aandacht te richten op het gevolg van de verstoring in plaats van op de oorzaak identificeert bedrijfscontinuïteit de activiteiten waar de organisatie van afhankelijk is om te overleven, en stelt het de organisatie in staat om vast te stellen wat nodig is om aan haar verplichtingen te blijven voldoen. Door middel van bedrijfscontinuïteit kan een organisatie herkennen wat gedaan moet worden om haar middelen (bijv. personen, gebouwen, technologie en informatie), toeleveringsketen, belanghebbenden en reputatie te beschermen, voordat zich een verstorend incident voordoet. Op basis van die herkenning is de organisatie in

staat de reactie die waarschijnlijk nodig is ingeval zich een verstoring voordoet realistisch te bezien, zodat zij het vertrouwen kan hebben dat ze de gevolgen kan managen en onaanvaardbare gevolgen kan vermijden.

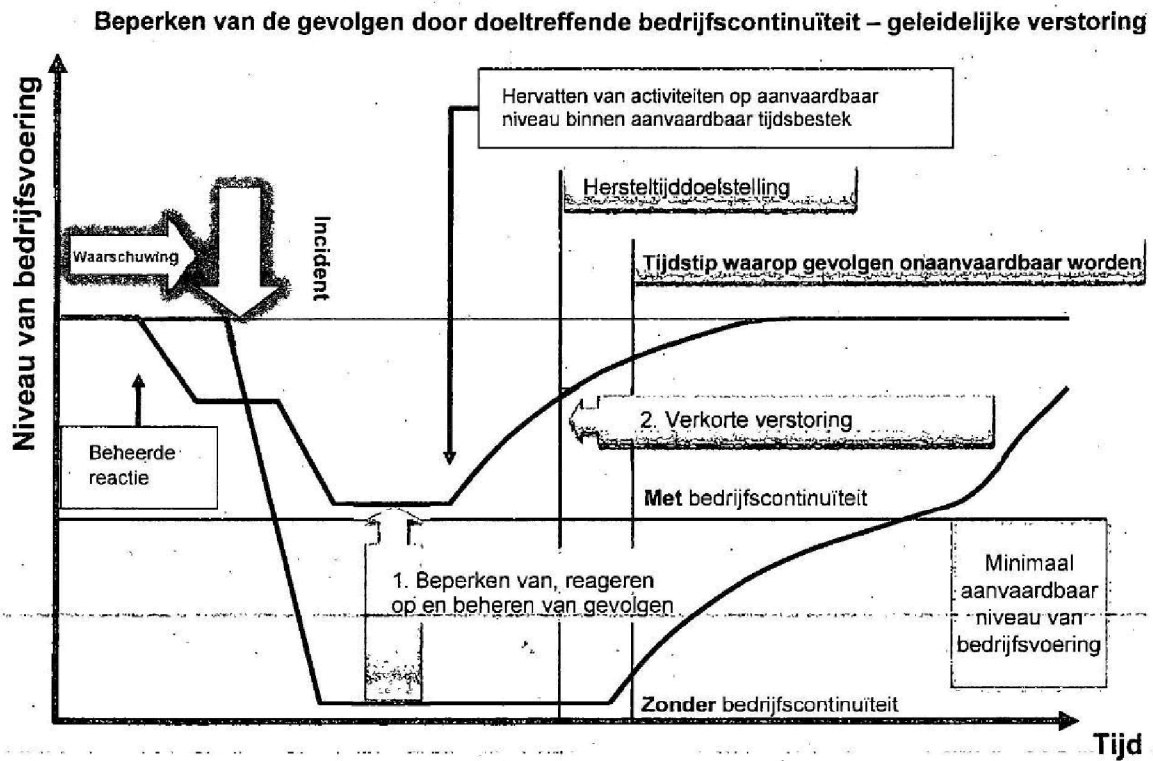
Een organisatie met de juiste bedrijfscontinuïteit kan ook profijt hebben van mogelijkheden die anders als te risicovol worden beoordeeld.

De volgende diagrammen (figuren 2 en 3) zijn bedoeld om conceptueel te illustreren hoe bedrijfscontinuïteit doeltreffend kan zijn om gevolgen in bepaalde situaties te beperken. Er zijn geen bepaalde tijdschalen geïmpliceerd door de relatieve afstand tussen de stadia die in beide diagrammen worden weergegeven.

Beperken van de gevolgen door doeltreffende bedrijfscontinuïteit – plotselinge verstoring



Figuur 2 — Illustratie van bedrijfscontinuïteit die doeltreffend is in geval van plotselinge verstoring



Figuur 3 — Illustratie van bedrijfscontinuïteit die doeltreffend is in geval van geleidelijke verstoring (bijv. een naderende pandemie)

Maatschappelijke veiligheid – Managementsystemen voor bedrijfscontinuïteit (business continuity management systems) – Richtlijnen

1 Onderwerp en toepassingsgebied

Deze internationale norm voor BCM geeft richtlijnen die zijn gebaseerd op een goede internationale werkwijze voor het plannen, inrichten, implementeren, uitvoeren, monitoren, beoordelen, onderhouden en continu verbeteren van een gedocumenteerd managementsysteem; ter bescherming tegen, verkleining van de kans op, voorbereiding op, reactie op en herstel van versturende incidenten wanneer deze zich voordoen.

Deze internationale norm heeft niet tot doel een uniforme structuur op te leggen voor een managementsysteem voor bedrijfscontinuïteit (BCMS), maar om een organisatie in staat te stellen een BCMS te ontwerpen dat op haar behoeften is afgestemd en dat voldoet aan de eisen van haar belanghebbenden. Deze behoeften worden gevormd door wettelijke, regelgevende, organisatie- en branchespecifieke eisen, de producten en diensten, de toegepaste processen, de omgeving waarin zij actief is, de omvang en structuur van de organisatie en de eisen van haar belanghebbenden.

Deze internationale norm is generiek en van toepassing op organisaties van elke omvang en van elk type, met inbegrip van grote, middelgrote en kleine organisaties die actief zijn in industriële, commerciële, publieke en non-profitsectoren, die:

- a) een BCMS willen inrichten, implementeren, onderhouden en verbeteren;
- b) naleving van het vastgestelde beleid voor bedrijfscontinuïteit willen bewerkstelligen; of
- c) zelf de naleving van deze internationale norm vast willen stellen en daarvan een eigen verklaring willen opstellen.

Deze internationale norm kan niet worden gebruikt ter beoordeling van het vermogen van een organisatie om te voldoen aan haar eigen bedrijfscontinuïteitseisen, noch aan die van een klant, of aan eisen van wet- of regelgeving. Organisaties die dit willen, kunnen de eisen van ISO 22301 gebruiken om aan andere partijen conformiteit aan te tonen of kunnen een geaccrediteerde certificatie-instelling vragen hun BCMS te certificeren.

2 Normatieve verwijzingen

De volgende documenten waarnaar is verwezen zijn onmisbaar voor de toepassing van dit document. Bij gedateerde verwijzingen is alleen de aangehaalde versie van toepassing. Bij ongedateerde verwijzingen is de laatste versie van het document (met inbegrip van wijzigings- en correctiebladen) waarnaar is verwezen van toepassing.

ISO 22300	<i>Societal security – Terminology</i>
ISO 22301	<i>Societal security – Business continuity management systems – Requirements</i>

3 Termen en definities

Met betrekking tot dit document gelden de termen en definities zoals beschreven in ISO 22300 en ISO 22301.

4 Context van de organisatie

4.1 Inzicht in de organisatie en haar context

Deze paragraaf gaat over inzicht krijgen in de context van de organisatie in verband met het inrichten en beheren van het BCMS. Het inrichten en beheren van BCM wordt behandeld in 8.1.

De organisatie behoort inzicht te hebben in de interne en externe factoren die relevant zijn voor haar doel en bedrijfsvoering en deze te evalueren. Deze informatie behoort in aanmerking genomen te worden bij het inrichten, implementeren, onderhouden en verbeteren van het BCMS van de organisatie en bij het toekennen van prioriteiten.

Een evaluatie van de externe context van de organisatie behoort, indien relevant, de volgende factoren te omvatten:

- het politieke, wettelijke en regelgevende kader, hetzij internationaal, nationaal, regionaal of lokaal;
- het sociale en culturele, financiële, technologische, economische, natuurlijke en concurrentiekader, hetzij internationaal, nationaal, regionaal of lokaal;

~~— verplichtingen voortkomend uit toeleveringsketens en relaties;~~

- overweging van interne studies over de risico's, rekening houdend met andere relevante informatiemanagementsystemen en meer in het algemeen informatie van kennismanagement;
- belangrijke sturende factoren en trends die invloed hebben op de doelstellingen en de bedrijfsvoering van de organisatie; en
- relaties met, en percepties en waarden van belanghebbenden buiten de organisatie.

Een evaluatie van de interne context van de organisatie behoort, indien relevant, de volgende factoren te omvatten:

- producten en diensten, activiteiten, middelen, toeleveringsketens, en relaties met belanghebbenden;
- het vermogen in termen van middelen en kennis (bijv. kapitaal, tijd, mensen, processen, systemen en technologieën);
- informatiesystemen, informatiestromen en besluitvormingsprocessen (zowel formeel als informeel);
- belanghebbenden binnen de organisatie;
- beleid, doelstellingen, en de aanwezige strategieën om deze te halen;
- toekomstige kansen en bedrijfsprioriteiten;
- percepties, waarden en cultuur;
- normen en referentiemodellen die binnen de organisatie worden gehanteerd; en
- structuren (bijv. bestuur, rollen en verantwoordelijkheden).

4.2 Inzicht in de behoeften en verwachtingen van belanghebbenden

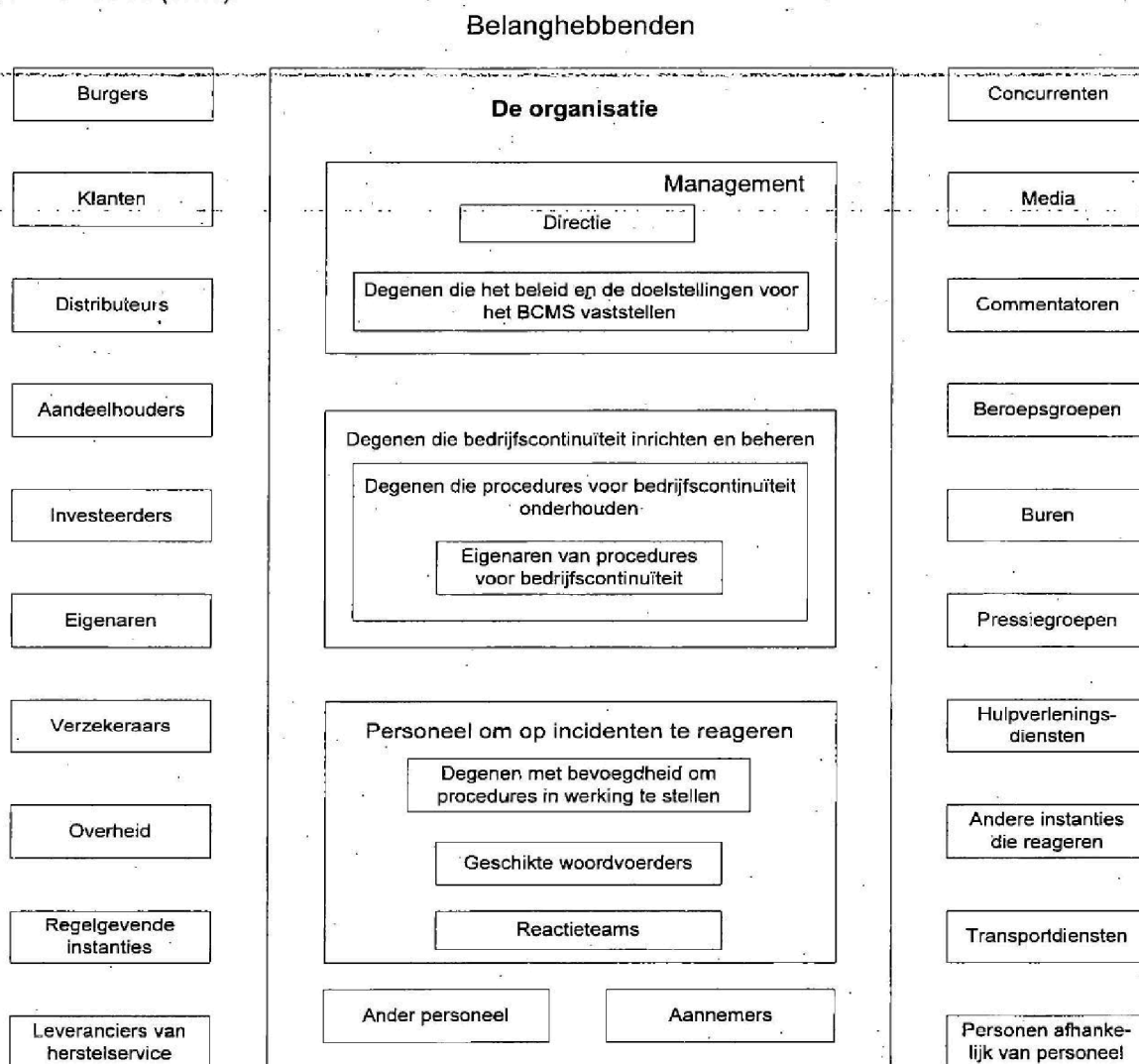
4.2.1 Algemeen

Bij het inrichten van haar BCMS behoort de organisatie te bewerkstelligen dat de behoeften en eisen van belanghebbenden in aanmerking worden genomen.

De organisatie behoort alle belanghebbenden die relevant zijn voor haar BCMS te identificeren, en gebaseerd op hun behoeften en verwachtingen, hun eisen vast te stellen. Het is belangrijk niet alleen verplichte en vastgelegde eisen te identificeren maar ook impliciete eisen.

OPMERKING De organisatie behoort zich bewust te zijn van iedereen die een belang heeft in de organisatie zoals de media, het publiek, concurrenten enz.

Bij het plannen en implementeren van het BCMS is het belangrijk activiteiten te identificeren die passend zijn in verband met belanghebbenden, maar te differentiëren tussen de verschillende categorieën. Het kan bijvoorbeeld passend zijn om na een verstoring incident te communiceren met alle belanghebbenden, maar het is mogelijk niet passend om bij het inrichten en beheren van BCM met alle belanghebbenden te communiceren (8.1.1).



Figuur 4 — Voorbeelden van belanghebbenden met wie in openbare en particuliere sectoren rekening gehouden moet worden