naar de nieuwe gegevens(bestanden);
e. continuïteit van de operationele werkzaamheden;
f. wijze waarop zo nodig kan terug worden gevallen op de oude situatie of op bijzondere hiervoor ontworpen handmatige procedures (fall-back procedure);
g. welke overgangsmaatregelen moeten worden genomen voor, tijdens en na de invoering van de vernieuwde situatie;
h. te ondernemen acties bij het uitlopen van de invoeringsplanning;
i. aanstellen van deskundige aanspreekpunten per betrokken organisatieonderdeel ten behoeve van de algehele voorbereiding, coördinatie, samenhang en afstemming.
2. De impact en complexiteit van de nieuwbouw en het onderhoud alsmede van conversie- of migratieactiviteiten is bepalend voor de geleidelijke invoering, de mogelijkheden om terug te keren naar vorige situaties en de mate waarin wordt schaduwgedraaid als daar de mogelijkheden voor bestaan.

C.15.3. Beveiligingsparagraaf fasedocumenten technisch infrastructuur

Beheersmaatregel
In de beveiligingsparagraaf van de fasedocumenten voor het ontwerp en de inrichting van IT-voorzieningen van de technische infrastructuur wordt de inrichting van de beveiliging gedocumenteerd in overeenstemming met externe en interne normen.

Toelichting
In een beveiligingsparagraaf van de fasedocumenten voor het ontwerp en de inrichting van IT-voorzieningen van de technische infrastructuur wordt de inrichting van de beveiliging gedocumenteerd in overeenstemming met externe en interne normen. In de beveiligingsparagraaf kan worden volstaan met het – per fase in toenemende mate van detail - verwijzen naar de desbetreffende in- en externe beveiligingsnormen als ze geen vertaalslag nodig hebben, aangevuld met eventuele gemotiveerde afwijkingen daarop.

Implementatierichtlijnen (Code 12.1.1)
1. In een zo vroeg mogelijk ontwerpstadium wordt vastgesteld:
a. in hoeverre er sprake is van afwijkingen van het basis beveiligingsniveau;
b. welke beleidsdocumenten en ontwerpcriteria van toepassing zijn;
c. of de bestaande beveiligingsuitgangspunten dan wel –maatregelen aanpassing behoeven door nieuwe ontwikkelingen op het gebied van technologie;
d. in hoeverre de leveranciersinstructies voor het inrichten van de aspecten van beveiliging gebaseerd zijn op de facto beveiligingsrichtlijnen van erkende norminstituten als NIST;
e. in hoeverre er sprake is van de invoerings- en conversieproblematiek en welke oplossingsrichting wordt voorgestaan.
2. Afhankelijk van de uitkomsten van punt 2 hiervoor worden in een risicoanalyse de specifieke eigenschappen van de IT-voorziening in beschouwing genomen en de beveiligingsinrichting vastgesteld voor zover die niet (voldoende) is geadresseerd in de productnormen van hoofdstuk 16 IT-voorzieningen en de facto beveiligingsrichtlijnen van erkende norminstituten als NIST;
3. Bij het uitvoeren van een risicoanalyse zijn ten minste de functioneel bedrijfsmiddelenbeheerder, materiedeskundigen en beveiligingsspecialisten betrokken.
4. Geaccepteerde (rest)risico's worden expliciet vastgelegd met een motivering waarom hiervoor geen beveiligingsmaatregelen worden getroffen.
5. In de opgeleverde systeemdocumentatie wordt de beveiligingsparametrisering vastgelegd in overeenstemming met de leveranciersinstructies, met hoofdstuk 16. IT-voorzieningen en de facto beveiligingsrichtlijnen van erkende norminstituten als NIST.
6. Voor IT-voorzieningen met een bijzonder belang voor de logische toegang tot de gegevens is in de beveiligingsparagraaf aangegeven:
a. met welke frequentie en welke geautomatiseerde hulpmiddelen beveiligingsinstellingen gecontroleerd worden;
b. welk type security violations gesignaleerd moeten worden met welke frequentie en welke tooling.
In de signaleringen wordt onderscheid gemaakt naar signalen, die in de gebruikersorganisatie moeten worden afgehandeld en signalen die betrekking hebben op Technisch beheer en exploitatie;
c. welke uitgangspunten er worden gehanteerd voor de groepering van autorisaties opdat de dynamiek in IT-dienstverlening, processen, functies en organisaties niet tot onaanvaardbare, extra onderhoudswerkzaamheden kunnen leiden.
7. De beveiligingsdocumentatie van IT-voorzieningen met een bijzonder belang voor de logische toegang tot productiegegevens wordt goedgekeurd door tactisch beveiligingsbeheer.

C.16. IT-voorzieningen

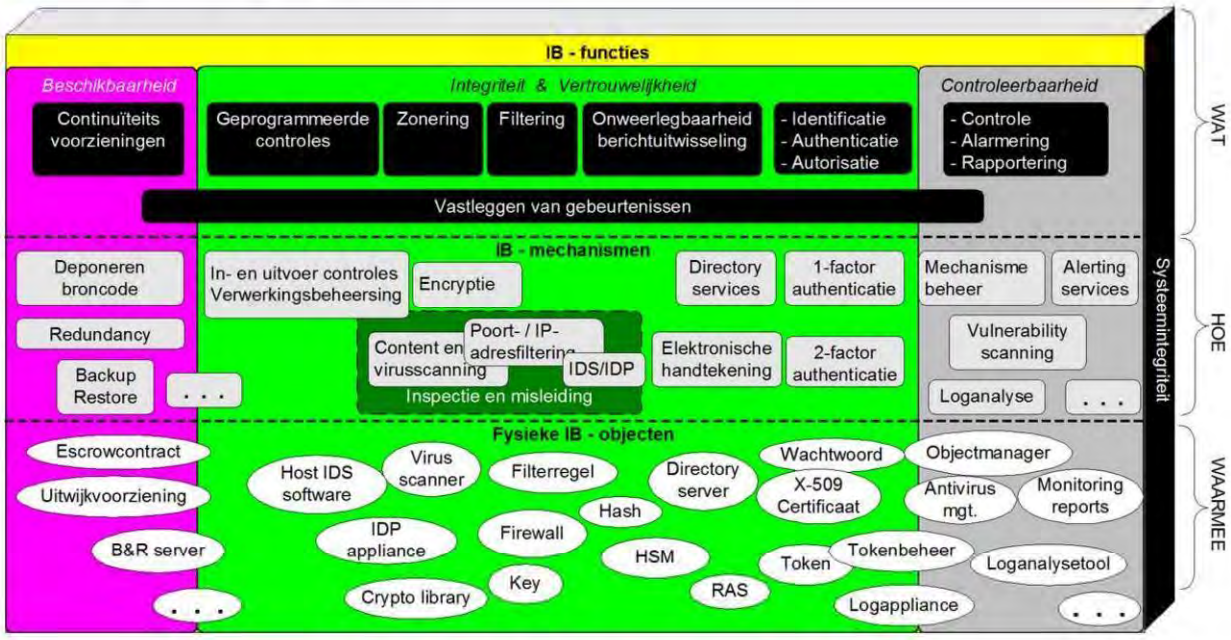
C.16.1. Inleiding

Doelstelling
IT-voorzieningen maken geautomatiseerde informatieverwerking mogelijk.

Afbakening
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.u.v. bedrijfstoepassingen, worden ook wel aangeduid als technische infrastructuur en betreft hardware, besturingsprogramma's en hulpprogramma's, datacommunicatievoorzieningen. De normen voor IT-voorzieningen gaan specifiek in op de instelmogelijkheden (parametrisering) van de voorzieningen en op de wijze waarop die 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 (zie figuur 5), 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-NEN 7498-2 Information processing systems – Open Systems Interconnection Basic Reference Model – Part 2: Security Architecture uit 1991.
Een IB-functie is een logische groepering van geautomatiseerde activiteiten die op een bepaald beveiligingsdoel is gericht. In samenhang worden de negen afgebeelde beveiligingsfuncties dekkend 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 Controleerbaarheid. In samenhang vormen ze de WAT-laag van het model.



Figuur 5 Model IB-functies

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 voor integriteit en vertrouwelijkheid dragen bijvoorbeeld ook bij aan beschikbaarheid.

De IB-mechanismen vormen de HOE-laag en zijn technische concepten (technieken) die het WAT van de IB-functies invullen. Omdat techniek zich steeds verder ontwikkelt, illustreert de figuur slechts een aantal bekende voorbeelden. De IB-mechanismen zijn de maatregelen waarmee IB-functies worden ingevuld. Elke maatregel kent één of meer implementatierichtlijnen; zie [3].
De fysieke IB-middelen vormen de WAARMEE-laag. Dit zijn IT-onderdelen, die de IB-mechanismen daadwerkelijk uitvoeren. Ze kunnen onderdeel zijn van een besturingsprogramma of applicatie, maar worden ook als afzonderlijke fysieke modules uitgevoerd. Ook hier zijn slechts enkele bekende voorbeelden getekend. Hoewel 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.

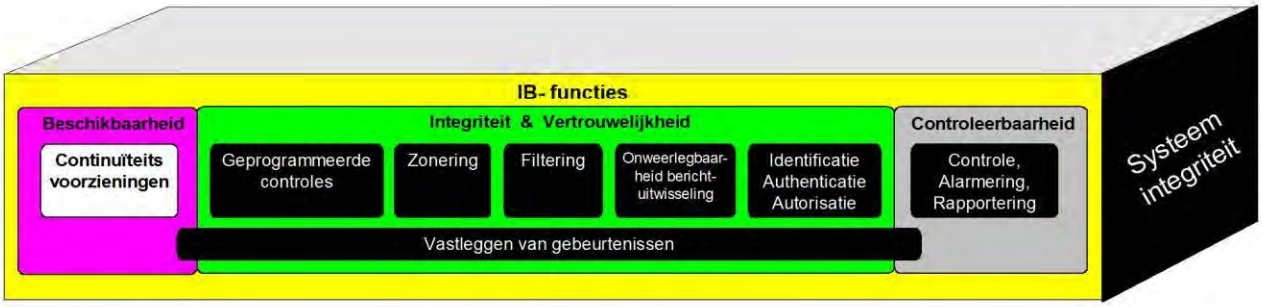
De drie niveaus in de normen corresponderen niet één-op-één met de drie lagen van het architectuurmodel. Het hoogste niveau van functies loopt wel gelijk met de normbeschrijving. De twee niveaus daaronder van de normbeschrijving hebben voornamelijk betrekking op laag 2, het HOE van het architectuurmodel.

De normen zijn voorts in “enge zin” 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 variabele instellingen, audit trail van mutaties (parameterwijzingen), functiescheidingen mogelijk maken, verwerkingsverslagen kunnen genereren. Deze algemene eisen maken onderdeel uit van de IB-functie Geprogrammeerde Controles. Deze IB-functie wordt uitgewerkt in onderdeel 9.6 Geprogrammeerde controles. Bij die uitwerking staan echter de bedrijfstoepassingen voor ogen, zoals die in maatwerk ontwikkeld kunnen worden of als standaard pakketten worden aangeschaft.

C.16.2. Continuïteitsvoorzieningen

Doelstelling
De IT-voorzieningen voldoen aan het voor de diensten 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 onaanvaardbaar lang stil komt te liggen. Een voorbeeld van een maatregel in dit kader is het dubbel uitvoeren van voorzieningen, waardoor de ene voorziening de functie van de ander kan overnemen bij uitval.
In de Code zijn onder het hoofd 'Fysieke beveiliging en beveiliging van de omgeving' veel preventieve maatregelen opgenomen, die van belang zijn voor de beschikbaarheid van de IT-voorzieningen. Denk aan maatregelen gericht op onderbrekingsvrije stroomvoorziening, klimaatbeheersing, brandpreventie, waterdetectie, toegangsbeperking e.d.. Onder deze IB-functie worden alleen IT-maatregelen opgesomd. In de Code ontbreken deze, terwijl ze in de praktijk inmiddels gangbaar zijn.

Motivering
Deze maatregelen voorkomen dat verstoringen en calamiteiten in de IT tot gevolg hebben dat de dienstverlening onaanvaardbaar lang niet ondersteund wordt.

C.16.2.1. Dubbele uitvoering en spreiding van IT-voorzieningen

Beheersmaatregel
Op basis van de eisen die voortvloeien uit 9.2.3 Plannen bedrijfscontinuïteit wordt bepaald in hoeverre delen van de technische infrastructuur dubbel worden uitgevoerd om single-points-of-failure te vermijden.

Implementatierichtlijnen (BS 7.5.2, 7.5.3)
1. Bij het vermijden van single-points-of-failure kunnen de volgende maatregelen worden getroffen:
a. dubbele uitvoering van voorzieningen: CPU's, de productieversie van de software, gegevensopslag zoals RAID op fileservers en databaseservers, hot of cold standby van beheervoorzieningen, clustering technologie van servers, fysieke verbindingen m.u.v. bekabeling binnen kantoorruimten;
b. zodanige plaatsing van dubbele IT-voorzieningen dat deze niet op één fysieke plaats zijn samengebracht (gescheiden kabels niet via één aansluitpunt) en dat er een veilige afstand tussen locaties bestaat;
c. IT-voorzieningen zo mogelijk geografische spreiden en op dezelfde technologie baseren;
d. snelle beschikbaarheid van reserve-voorzieningen;
e. uitwijkcontracten.

C.16.2.2. Herstelbaarheid van verwerking

Beheersmaatregel
Verwerkingen zijn herstelbaar.

Implementatierichtlijnen
1. De bediening van IT-voorzieningen is niet gebonden aan één fysieke locatie.
2. Datacommunicatievoorzieningen beschikken over automatisch werkende alternatieve routeringmechanismen om uitval van fysieke verbindingen op te vangen.
3. Systemen met hogere beschikbaarheidseisen dan het basisniveau beschikken over voorzieningen op het gebied van automatic failover en load balancing, waarbij de verwerking gespreid is over twee locaties.
4. Indien op grond van deze hogere beschikbaarheidseisen 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.
5. Er zijn routines voor back-up en recovery van databestanden en software, voor herstart en foutherstel van verwerkingen.
6. Berichten, die van derden zijn ontvangen en naar derden zijn verzonden, worden minimaal gebufferd totdat er voldoende zekerheid is over de integere verwerking.
7. Er is voldoende buffering van tussenbestanden bij langere verwerkingsketens.

C.16.2.3. Bewaking en alarmering IT

Beheersmaatregel
IT-voorzieningen proberen dreigende discontinuïteit van die voorzieningen zo mogelijk te voorspellen dan wel signaleren in een zo vroeg mogelijk stadium dat deze optreden.

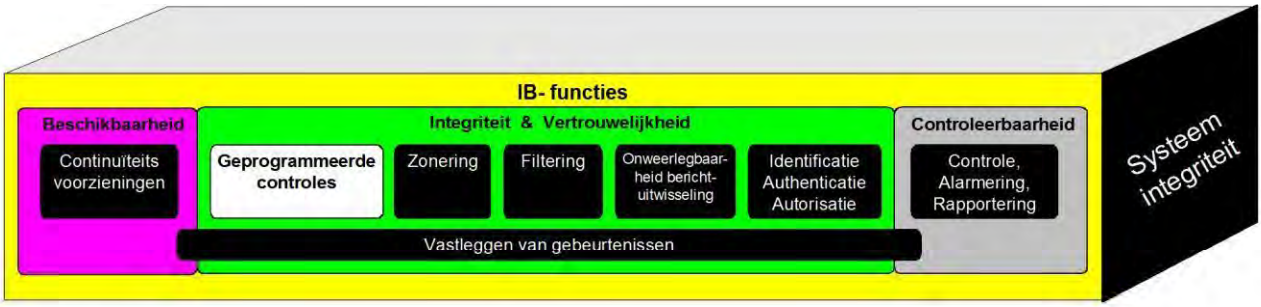
Toelichting
Denial of service attacks (het onbereikbaar maken van een dienst door een overvloed aan berichten te sturen) en controles op te grote omvang van berichten of bestanden zijn specifiek van betekenis voor de beschikbaarheid van de IT-voorzieningen, maar worden vanwege de samenhang van maatregelen gezien als onderdeel van de IB-functie 'Filtering'.

Implementatierichtlijnen
1. Er worden standaard voorzieningen geïmplementeerd om de beschikbaarheid van IT-voorzieningen te bewaken op basis van aanwezigheidssignalen en gebruiksmetingen. Overschrijdingen van drempelwaarden worden doorgegeven aan een Event Console. Deze drempelwaarden kunnen een voorspellende (zoals aantal schrijffouten bij diskunits, vrije diskruimte) of een signalerende werking (er is daadwerkelijk sprake van een dreiging voor de continuïteit: de disk is vol) hebben.
2. 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.16.3. Geprogrammeerde controles

Doelstelling
In toepassingsprogrammatuur worden geprogrammeerde controles opgenomen, gericht op invoer, verwerking en uitvoer.

Definitie
De functies die zorgen voor hetzij geautomatiseerde controles, hetzij de levering van informatie voor het uitvoeren van handmatige controles door gebruikers of beheerders.



Toelichting
Geprogrammeerde controles in toepassingsprogrammatuur (ook wel aangeduid als Application Controls) zijn onmisbaar om de integriteit van de informatie(voorziening) te waarborgen. Het spreekt voor zich dat geprogrammeerde controles veel efficiënter én effectiever zijn dan handmatige controles.
Geprogrammeerde controles verdienen extra aandacht bij toepassingsprogrammatuur die via internet loopt, om het lagere beheersingsniveau van die omgeving te compenseren.

De implementatierichtlijnen van geprogrammeerde controles zijn minder integraal van toepassing dan bij de andere IB-functies. De impact van geprogrammeerde controles op de bedrijfsvoering kan aanzienlijk zijn, zodat er meer dan bij de andere IB-functies naar haalbaarheid en effectiviteit in de specifieke situatie moet worden gekeken. Bovendien zijn vele geprogrammeerde controles overlappend ten opzichte van elkaar, zodat keuzevraagstukken meer 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 implementatierichtlijnen aangegeven bij welke verwerkingstypologie ze horen. Daartoe 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 onderscheid niet relevant is, zijn kruisjes opgenomen in alle kolommen achter de implementatierichtlijn.

De onder dit hoofdstuk uitgewerkte normen kunnen ook als referentiekader worden gezien voor de algemene IB-eisen voor besturingsprogramma's en (systeem) beheerpakketten die deel uitmaken van de technische infrastructuur. De normen zijn echter bedoeld voor bedrijfstoepassingen, dus zullen vele implementatierichtlijnen niet echt van toepassing zijn.

Motivering
Geprogrammeerde controles bieden de beste waarborgen dat de integriteit van de informatie(voorziening) gehandhaafd kan worden.

C.16.3.1. (Controle-technische) functie- en processcheidingen

Beheersmaatregel
Niemand in een organisatie of proces mag in staat worden gesteld om een gehele procescyclus te beheersen.

Toelichting

Controle-technische functiescheiding berust op het principe van het creëren van tegengestelde belangen. Kenmerkend binnen IT-omgevingen is dat deze binnen informatiesystemen moet worden afgedwongen door in de toepassing taken te scheiden en vervolgens de maatregelen van logische toegangsbeveiliging: identificatie, authenticatie en autorisatie daarop te laten aansluiten.

Implementatierichtlijnen

1. ***Basisscheidingen ("klassieke" functiescheiding)*** (Batch, On-line, Bericht) Bewarende, registrerende, uitvoerende, controlerende en beschikkende taken zijn gescheiden.
2. ***Stamgegevens versus mutaties*** (Batch, On-line, Bericht) Applicatietaken voor het opvoeren van stamgegevens en het opvoeren van mutatiegegevens zijn gescheiden. Stamgegevens, ook wel vaste of referentie gegevens genoemd (geen enkel gegeven is echter helemaal vast) hebben een doorlopende betekenis in processen. Voorbeelden: rekeningen en omschrijvingen van grootboekrekeningen, klantgegevens met NAW en kredietlimiet, nummer, naam en prijs van artikelen, etc.
3. ***Scheiding bij massale invoer*** (Batch) Bij massale data-invoerprocessen worden eerste invoer, controle-invoer en het aanbrengen van correcties naar aanleiding van uitgevoerde applicatiecontroles of –signaleringen als afzonderlijke (applicatie)taken onderkend. Controle-invoer kan zich beperken tot kritische gegevens.
4. ***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 applicatietaak voor het goedkeuren gecreëerd om de beschikkende functie beter te ondersteunen. De verwerking van de ingevoerde gegevens vindt pas plaats, nadat goedkeuring (door een andere gebruiker) heeft plaatsgevonden.
5. ***Scheiding per zaak*** (On-line) Als applicaties bestemd zijn voor gebruikersorganisaties, waarin kort-cyclische taakroulatie aan de orde is, worden de historie van gebruiker-id's en uitgevoerde applicatietaken per "zaak" (dossier) vastgelegd en op onverenigbaarheid van taken gecontroleerd voordat een taak voor een bestaande "zaak" voor een gebruiker ter beschikking komt. Workflow Management Systemen zijn speciaal toegerust om deze richtlijn te realiseren.
6. ***Scheiding naar inhoud van gegevens*** (On-line) Indien verschillende behandelgroepen binnen een centrale gegevensverzameling zijn te onderscheiden, worden de applicatietaken afhankelijk gemaakt door de identificatie van deze groepen te controleren met de inhoud van de gegevens. Bijvoorbeeld: lettergroepen van klanten, regionaal onderscheid.
7. ***Beheer versus gebruik*** (Batch, On-line, Bericht) Systeem- en applicatiebeheertaken zijn gescheiden van de overige gebruikerstaken. Muteren van rekenregels en variabelen (algemene rentepercentages, selectiecriteria) zijn als beheertaken te zien.
8. ***Scheiden en afhankelijk maken van processtappen*** (Batch, On-line, Bericht) Voor de betrouwbaarheid van processen en de gegevensverwerking kan het noodzakelijk zijn dat bepaalde processtappen in een bepaalde volgorde plaatsvinden en niet anders. Voorbeelden kunnen dit principe verduidelijken: - voor het verkrijgen van vergunning moet eerst een betaling zijn ontvangen voordat de vergunning wordt verstuurd. - voor het verkrijgen van een gewaarmerkte authenticatie voor een gebruikerscode moet eerst een activeringscode worden ingegeven, die na aanvraag wordt toegestuurd naar het officieel bekende huisadres
9. ***Eenduidige mutatieverantwoordelijkheden*** (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 aanwezig, dat mutatiebevoegdheden eenduidig binnen één organisatiedeel van gebruikers toegewezen kunnen worden. Alleen een batchgewijze eerste opvoer vanuit een andere applicatie of een systeemvreemde omgeving mag hierop, in de audit trail herkenbaar, inbreuk 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.
10. ***Dezelfde gegevens in meerdere gegevensverzamelingen*** (Batch, On-line) Indien dezelfde gegevens in meer gegevensverzamelingen voorkomen (zodat in beginsel sprake is van redundantie), worden mutaties altijd vanuit één gebruikersorganisatie in één gegevensverzameling gemuteerd, waarbij die mutaties automatisch, batchgewijs en als zodanig herkenbaar in de audit trail, worden overgebracht (gekopieerd) naar de andere gegevensverzamelingen.

C.16.3.2. Invoercontroles

Beheersmaatregel
Alle ingevoerde gegevens vanuit een systeemvreemde 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 systeemvreemde, niet-vertrouwde omgeving wordt verstaan elke omgeving die niet volledig kan worden beheerst vanuit het perspectief en de samenhang van het eigen toepassingsgebied.

Implementatierichtlijnen

1. ***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 (Code 12.2.2.a)
2. ***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 (Code 12.2.1.a) - waarden die buiten het geldige bereik vallen; - ongeldige tekens in invoervelden; - ontbrekende of onvolledige kritische gegevens; - overschrijding van boven- en ondergrenzen voor gegevensvolumes (buffer overruns/overflows, Code 12.2.2.d); - inconsistentie ten opzichte van andere gegevens binnen invoer dan wel in andere gegevensbestanden. Foutieve invoer wordt geweigerd, onwaarschijnlijke invoer wordt gesignaleerd.
3. ***Weigeren invoer per batch (J)*** (Batch) Voor het retourneren van batchgewijze invoer in verband met niet te verwerken posten (uitval) worden vuistregels gehanteerd, die periodiek worden geëvalueerd (bijv. bij meer dan 10 geweigerde posten, hele bestand retour afzender).
4. ***Signaleren invoer (J)*** (Batch, On-line, Bericht) Afwijkende invoer op grond van relatie- en redelijkheidscontrole wordt aan de gebruiker gesignaleerd voordat de invoer in de applicatie wordt verwerkt. (Code 12.2.1.e)
5. ***Terugmelden omschrijving (J)*** (On-line) Indien van toepassing worden bij ingevoerde codes of sleutelgegevens de daarbij behorende omschrijving teruggemeld ter visuele controle met het invoerdocument (bijv. NAW-gegevens bij BurgerServiceNummers.)
6. ***Verplichte veldinvulling bij kritische gegevens (J)*** (On-line) Gegevenselementen die kritisch zijn voor de toepassing worden verplicht ingevuld.
7. ***Default waarden (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*** gegevenselementen (zie 4.2.7).
8. ***Controle getal (check digit) (J)*** (Batch, On-line, Bericht) Relevante code- aanduidingen of sleutelgegevens (BurgerServiceNummer, rekeningnummers, et cetera) van 4 of meer posities zijn van een check-digit voorzien aan de hand waarvan de bestaanbaarheid van de codeaanduiding door de applicatie kan worden vastgesteld.
9. ***Voorkomen dubbele invoer / controle op uniciteit (J)*** (Batch) Het opnemen van volgnummers in records of berichten en controle op uniciteit kan dubbele invoer voorkomen. Toepassing is mede afhankelijk van de mogelijkheden van de verwerkingscontroles (zie onderdeel 3.4) dan wel productiecontroles (zie onderdeel 10.3) dan wel de ernst van gevolgen van dubbele verwerking.
10. ***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: wijzigen is verwijderen en toevoegen. (Code 12.2.2.c)
11. ***Invoer aan de bron (J)*** (Batch, On-line, Bericht) In een keten van verwerkingen (door meerdere organisaties) worden invoercontroles zoveel mogelijk bij de eerste verwerking (bij de bron) uitgevoerd, omdat daar de meeste kennis over die gegevens bestaat.
12. ***Voorinvullen e-formulieren (J)*** (Batch, Bericht) De invoervelden van elektronische formulieren worden zoveel mogelijk tevoren ingevuld met reeds vastgestelde gegevens.
13. ***Terugmelden invoer klantgegevens (J)*** *(Batch, On-line, Bericht)* Ingevoerde klantgerelateerde gegevens worden aan de klant als apart proces bevestigd met het verzoek de gegevens te controleren en meteen te (laten) wijzigen bij fouten.
14. ***Klant inschakelen (J)*** (Batch, On-line, Bericht) Klanten hebben inzage in hun eigen gegevens en worden gestimuleerd hun gegevens op eigen initiatief te wijzigingen indien nodig. Hiervoor worden functionaliteiten aangeboden.
15. ***Volledigheid (en juistheid) inzending berichten (J en V)*** (Bericht) Bij onregelmatige inzending van berichten wordt aan de verzender duidelijk gemaakt dat er meteen een bevestiging van ontvangst moet worden verkregen, zo mogelijk gecombineerd met de resultaten van de (eerste) verwerking. Hierdoor kan de inzender worden ingeschakeld bij het constateren dat de post (juist) is aangekomen.
16. ***Vastleggen verwerkingsdatum (T)*** (Batch, On-line, Bericht) Ten behoeve van de controle op tijdigheid van ontvangst en verdere verwerking wordt per verwerking de datum vastgelegd op basis van de

systeemdatum.
17. ***Voortgangscontrole (T)*** (Batch, On-line, Bericht) Door vergelijking van de verschillende (verwerkings)datums wordt voortgangscontrole op de verwerking uitgeoefend.
18. ***Volledigheid invoer /volgorde controle (V)*** (Batch, Bericht) Door het opnemen van volgnummers in berichten of invoerrecords kan de volledige ontvangst worden vastgesteld, mits het aantal invoerbronnen beperkt is.
19. ***Batch- en hashtotals (V)*** (Batch, Bericht) Door middel van het inbrengen van voortellingen van batch- (aantallen/bedragen) en -/hashtotals van invoerdocumenten / geleidelijsten in de applicatie wordt de volledigheid van massale invoer gecontroleerd. (Code 12.2.2.e)

C.16.3.3. Uitvoercontroles

Beheersmaatregel
De uitvoerfuncties van programma's maken het mogelijk om de juistheid, tijdigheid en/of volledigheid van de gegevens te kunnen vaststellen.

Implementatierichtlijnen

1. ***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: client). Elektronische uitvoer wordt niet pas op de bestemming gefilterd.
2. ***Maken afdruk van gegevens van een post/zaak (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 schermafdrukken is een te beïnvloeden functie, die geen bewijs kan opleveren van een geautoriseerde processtap.
3. ***Wettelijke eisen (J)*** (Batch, On-line, Bericht) Automatisch gegenereerde bescheiden voor klanten voldoen aan de wettelijke vereiste vormvoorschriften.
4. ***Afdrukken selectiecriteria bij uitvoerlijsten (J)*** (Batch) Bij variabele instelmogelijkheden worden de selectiecriteria, die gebruikt zijn om de uitvoer te bepalen, op de desbetreffende uitvoerlijsten afgedrukt.
5. ***Geleidelijsten (J en V)*** (Batch) Uitvoerbestanden die op verplaatsbare media worden uitgewisseld, zijn voorzien van geleidelijsten met (hash) totalen van ***kritische*** gegevens en bedragen. Deze (hash)totalen komen ook voor in het bestand (voorloop- of sluitrecord) (Code 12.2.2.e).
6. ***Volledigheid verzending berichten (V)*** (Bericht) Bij verzending van berichten, waarbij risico's op juridische geschillen mogelijk zijn, worden voorzieningen getroffen die volledige verzending kunnen aantonen. Mogelijkheden: (automatische) terugmelding van ontvangst; – tijdige signalering van het niet-tijdig reageren op het verzonden bericht; toekennen volgnummers aan berichten, waarbij er zekerheid moet zijn dat er volgnummercontrole plaatsvindt bij de ontvangende partij.
7. ***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.
8. ***Volledigheid uitvoerlijsten zelf (V)*** (Batch) Om de volledigheid van uitvoerlijsten te kunnen constateren, wordt elk verslag afgesloten met een "einde-verslag" regel of per pagina een nummering bestaande uit het paginanummer en het totale aantal pagina's van het document.
9. ***Controletellingen batchverwerking (V)*** (Batch) Batchuitvoer bevat controletellingen die zijn gebaseerd op tijdens de computerverwerking opgebouwde tellingen. Indien tellingen worden overgenomen uit bestanden, is dat kenbaar gemaakt op de uitvoerlijsten (Code 12.2.2.e).
10. ***Voldoende mogelijkheden tot informatievoorziening (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 toetsen van de juistheid, tijdigheid en volledigheid van de informatieverwerking. De informatievoorziening maakt cijferbeoordeling, ouderdomsanalyse, voortgangsbewaking via meerdere invalshoeken e.d. mogelijk.

C.16.3.4. Verwerkingsbeheersing

Beheersmaatregel
Toepassingsprogrammatuur biedt mogelijkheden om te constateren dat alle ter verwerking aangeboden invoer juist, volledig en tijdig is verwerkt.

Implementatierichtlijnen

1. **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 opgevangen op applicatieniveau als verwerkingszekerheid vereist is. *Toelichting:* Het implementeren van zekerheidsstelling op systeemniveau dat berichten ook daadwerkelijk aan het eind van een keten zijn verwerkt, kost vooralsnog veel overhead en dus performance. Een methode bij raadpleging kan zijn de ketens korter te maken door kopieën van (basis)bestanden in deeltrajecten te gebruiken. Vooralsnog is het effectiever dergelijke zekerheden in het proces (de applicatie) in te bouwen. Hiervoor bestaan diverse methoden; van het zenden van een bevestigingsbericht tot het dagelijks afstemmen van verwerkingstotalen.
2. ***Informatieverstrekking aan derden (J)*** (Batch) In de verwerkingsverslagen worden bij batchgewijze informatieverstrekking aan derden naast de uitvoertellingen tevens de ontvangende instantie vermeld.
3. ***Inhoud audit trail (J)*** (Batch, On-line, Bericht) De audit trail bevat voldoende gegevens om achteraf te kunnen herleiden welke essentiële handelingen wanneer door wie of vanuit welk systeem met welk resultaat zijn uitgevoerd. Tot essentiële handelingen worden in ieder geval gerekend: opvoeren en afvoeren posten, statusveranderingen met wettelijke, financiële of voor de voortgang van het proces, de zaak of de klant beslissende gevolgen.
4. ***Raadpleegbaarheid audit trail (J)*** (Batch, On-line, Bericht) Alle ingevoerde, gemuteerde of vervallen posten die onderdeel uitmaken van de audit trail, zijn op doelmatige wijze naar verschillende gezichtspunten raadpleegbaar ten behoeve van het oplossen van vragen en problemen alsmede voor het uitoefenen van interne controle.
5. ***Schonen audit trail (J)*** (Batch, On-line, Bericht) Indien gegevens ten behoeve van de audit trail in databases (als occurences) raadpleegbaar blijven, zijn er aparte applicatietaken beschikbaar voor het verwijderen van oude gegevens.
6. ***Bewaartermijn audit trail (J)*** (Batch, On-line, Bericht) De audit trail wordt tenminste twee jaar bewaard of zoveel langer als de wet bepaalt indien van toepassing.
7. ***Handmatige bestandscorrecties (J)*** (Batch, On-line, Bericht) Indien handmatige invoer ter correctie van bestandsgegevens niet te vermijden is (want dan heeft de applicatie kennelijk geen sluitend stelsel van controle- en correctiemaatregelen), worden de resultaten van deze bewerkingen in "was-wordt" verslagen vastgelegd. Speciale aandacht is dan te besteden aan de volledigheid van deze uitvoerverslagen, zie de normen hieraan voorafgaand.
8. ***Controletellingen (Code 12.2.2) vervolg (Code 12.2.2.a, 12.2.2.b, 12.2.4.b) (V)*** (Batch, On-line) De applicatie geeft door middel van controletellingen inzicht in de verwerking van de invoerstroom tot de uitvoerstroom en/of mutaties op basisregistraties. Daartoe worden op de verwerkingsverslagen controletellingen afgedrukt, die gesplitst zijn naar soort invoer, soort uitvoer of verwerking. *Toelichting:* na een afgeronde cyclus van verwerkingen (meestal per dag) wordt aangegeven in hoeverre ingevoerde mutaties wel of niet verwerkt zijn. Voor zover er basisregistraties worden verwerkt, worden deze tellingen gepresenteerd in de vorm van een doorrekening (balanscontrole) in aantallen: beginstand + nieuw – vervallen = eindstand. in bedragen: beginstand + nieuw wijzigingen – vervallen = eindstand
Overwegingen bij een stelsel van controletellingen - Het ontwerpen van een stelsel van controletellingen, waarmee een doorrekening 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 opwegen tegen het belang van het verkrijgen van zekerheden over de volledigheid van de basisregistratie. Indien de individuele posten in een basisregistratie 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 mogelijk juistheid van de posten in de basisregistratie. - Een ander punt van overweging is opslag in het systeem van de tellingen (met risico van manipulatie) versus het opnieuw herberekenen en presenteren van de resultaten als afzonderlijke automatisch (maar complex) proces of het berekenen als handmatige proces. Het maken van handmatige berekeningen borgt de attentie voor het signaleren van verschillen.
9. **Toepassen logistiek model *(V)*** (Bericht) Bij berichtgeoriënteerde verwerkingen en/of meerdere batchuitwisselingen per dag met andere organisaties wordt de volledigheid en tijdigheid van de verwerking beheerst door **logistieke meetpunten** en **parkeerplaatsen** in het primair proces aan te brengen. (Code 12.2.4.b) *Toelichting 1:* Gedurende de productie wordt een waarneming weggeschreven als een geval / zaak dat meetpunt passeert. In het kader van de volledigheidsbewaking heeft elk werkproces aan het begin en eind een **logistiek meetpunt**. Hierdoor kan waargenomen worden of een gevalsbehandeling nog in uitvoering is of afgerond of geannuleerd. Verder zijn logistieke meetpunten nodig voor tijdigheid- en juistheidsbepaling en dienstverlening. Hiervoor moeten logistieke meetpunten geplaatst worden aan het begin en eind van een voorraadpunt en handmatige behandeling van een geval. Aangezien een planning op tactisch niveau gerelateerd is aan de producten en diensten van de organisatie en dus de bedrijfsprocessen, is het ook van belang om in de logistieke meetpunten binnen de werkprocessen identificerende kenmerken van de bedrijfsprocesinstantie en de gevalsbehandeling vast te leggen. Hierdoor

kan uiteindelijk de samenhang van de gevalsbehandeling op tactisch niveau zichtbaar gemaakt en bewaakt worden. **Parkeerplaatsen** zijn bewust aangebrachte punten in het proces waar werk tijdelijk vastgehouden kan worden. Vanuit deze punten kan het verloop van het proces en de capaciteitsuitnutting in het bijzonder beïnvloed worden. In het kader van volledigheid is de zendende partij verantwoordelijk voor de logistieke aflevering op de afgesproken locatie volgens de afgesproken kwaliteit tot en met het moment dat de ontvangende partij de ontvangst bevestigd heeft (functioneel, technisch of beiden). De ontvangende partij heeft hierbij ten alle tijden een afnameplicht. Hiermee is de verantwoordelijkheid rondom volledigheid bij één enkele regelkring belegd. Onder partijen verstaan we hier bedrijfsfuncties en/of uitvoerende organisatie onderdelen. Wanneer er een voorraadpunt gepositioneerd is tussen de overgang van de gevalsbehandeling, geldt dezelfde regel. De ontvangende partij is hierbij verantwoordelijk voor het voorraadpunt. *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 verwerkingspunt, waarover zekerheid bestaat dat de posten goed zijn verwerkt.

C.16.3.5. Bestandscontrole

Beheersmaatregel
Kritische gegevens (bijvoorbeeld identificerende 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 sleutelgegevens in gegevensverzamelingen die op verschillende platforms voorkomen of door verschillende organisaties worden geëxploiteerd.

Implementatierichtlijn
- Er zijn meerdere alternatieven om aan deze doelstelling te voldoen:
- vergelijk dezelfde kritische gegevens in verschillende gegevensverzamelingen, waarbij verschillen worden gesignaleerd. Wellicht kan hiervoor standaard programmatuur worden gebruikt;
- indien de bestanden dezelfde metadata bevatten kan de controle plaatsvinden met hashtotalen. Bij verschillen zal op record- of occurrence-niveau vergelijking moeten plaatsvinden. De periodiciteit hangt af van de hoeveelheid verschillen, die bij eerdere vergelijkingen zijn geconstateerd dan wel de inschatting van risico's op het kunnen voorkomen van inconsistenties;
- bij afgeleide gegevensverzamelingen, die frequent en integraal worden overschreven door kopieën vanuit een basisgegevensverzameling, is deze vergelijking niet noodzakelijk.

C.16.3.6. Geprogrammeerde controles af te stemmen met generieke IT-voorzieningen

Beheersmaatregel
In toepassingsprogrammatuur zijn geen functies werkzaam, waarvoor kwalitatief betere generieke voorzieningen beschikbaar zijn, zoals die voor identificatie, authenticatie, autorisatie, onweerlegbaarheid en encryptie.

Toelichting en afbakening
Deze doelstelling zal doorgaans alleen volledig haalbaar zijn bij maatwerkapplicaties. Bij standaard applicaties / programmapakketten worden dergelijke functies meestal meegeleverd en zijn niet uit te schakelen en te vervangen door eigen generieke functies, hooguit daarmee te synchroniseren. Bovendien kunnen dan tevens andere generieke IB-functies aan de orde zijn. Voor de beveiliging van de generieke IB-functies gelden de normen van hoofdstuk 16. IT-voorzieningen, m.u.v. 16.3 Geprogrammeerde controles.

Implementatierichtlijnen
(niet uitputtend)

1. Autorisatiebeheersysteem
Voor het beheer van autorisaties wordt zoveel mogelijk gebruik gemaakt van standaard autorisatievoorzieningen of –modules. Indien dit op onderdelen niet is te vermijden (bijv. bij gegevensafhankelijke autorisatiemechanismen) worden deze functies als aparte module uitgevoerd.

2. (Ver)sterkte authenticatie

Bij het elektronisch communiceren vanuit een niet vertrouwde omgeving (bijv. vanuit de externe zone) kan het noodzakelijk zijn extra zekerheden (boven het basisniveau beveiliging) te verkrijgen omtrent de identiteit van derden. De hiervoor te treffen maatregelen worden afgestemd met het in deze gevoerde beleid en de beschikbare generieke oplossingen.

3. Onweerlegbaarheid juiste 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 voorzieningen van een Public Key Infrastructuur.

4. Encryptie
Als encryptie ter borging van vertrouwelijkheid en/of integriteit van gegevens binnen of ten behoeve van een applicatie wordt toegepast, dan gelden hiervoor de normen van de subparagrafen 16.4.3 Encryptie ten behoeve van zonering, 16.4.4 Sterkte van de encryptie, 16.4.5 Vertrouwelijkheid en integriteit sleutels.

5. Dubbele of ontbrekende bestandsuitwisseling
Bij uitwisseling van bestanden tussen centrale en decentrale servers of met externe partijen wordt zeker gesteld dat uitwisseling niet of dubbel plaatsvindt. Een dergelijk filetransfermechanisme is bij voorkeur als generieke voorziening in te richten.

C.16.3.7. Aanvullende normen

Beheersmaatregel
Aanvullende maatregelen boven het basisniveau beveiliging kunnen noodzakelijk zijn om een hoger beveiligingsniveau te bereiken bij extra risicovolle bedrijfsprocessen.

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 suggestie bedoeld.

Implementatierichtlijnen
1. Aparte applicatietaken
Applicatietaken, die gegevens verwerken met extra (hoog) belang, kunnen van de overige transacties gescheiden worden om functiescheiding op basis van autorisatie mogelijk te maken. In dat geval worden de desbetreffende gegevens als aparte gegevensrubriek gezien, waarvan de rubricering doorwerkt bij alle transacties van de toepassing. Gegevens van te onderscheiden aard kunnen ook worden opgenomen in aparte bestanden, zodat de toegang en verwerking gedifferentieerd kunnen worden.

2. Extra audit trail
Bij applicatietaken met een verhoogd belang kan meer uitgebreide vastlegging van uitgevoerde activiteiten in de audit trail worden overwogen. Dit kan ook het geval zijn als de applicatie mogelijkheden biedt tot oneigenlijk gebruik van raadpleegbevoegdheden. (Code 12.2.1.g)

3. Controletellingen database
Bij het online verwerken van mutaties in een database kunnen controletellingen van aantallen en bedragen apart worden bijgehouden en gemuteerd. Frequent wordt dan gecontroleerd of deze controletellingen in overeenstemming zijn met de daadwerkelijke telling van de database. Voor deze controle wordt dan een aparte taak gedefinieerd.

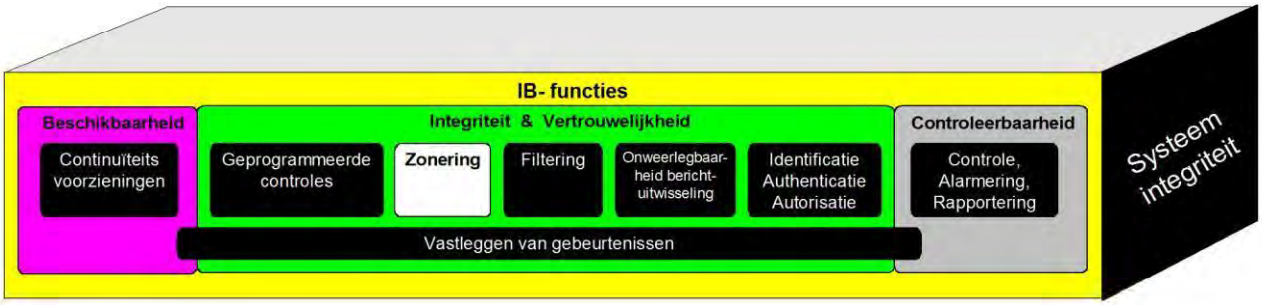
4. Gegevensencryptie
Gegevensencryptie op applicatieniveau (database niveau) is een extra middel om de vertrouwelijkheid en de integriteit van de gegevensuitwisseling of -opslag te waarborgen.

5. Gegevensrubricering tonen
Gegevensrubricering tonen op beeldscherm, output en verwisselbare gegevensdragers en meesturen met elektronische gegevensuitwisseling. De gebruikers en/of ontvangers dienen op de hoogte te zijn van wat de rubricering betekent voor de behandeling van de gegevens. Organisaties die gerubriceerde gegevens uitwisselen dienen op de hoogte te zijn van de betekenis van de rubricering; hanteren de organisaties een andere naamgeving, dan dienen zij onderlinge afspraken te maken hoe de verschillende naamgevingen op elkaar aansluiten.

C.16.4. 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 waarbinnen gegevens vrijelijk met hetzelfde niveau van beveiligingsmaatregelen kunnen worden uitgewisseld.



Toelichting
Het doel van zonering is:
1. het voorkomen of beperken van risico's door isolatie van onderdelen van de technische infrastructuur;
2. het scheiden van onderdelen waaraan verschillende betrouwbaarheidseisen worden gesteld.

Informatie-uitwisseling tussen zones verloopt via koppelvlakken, die de informatiestromen controleren. Hierdoor kunnen bepaalde dreigingen niet optreden dan wel niet doorwerken van de ene zone in de andere. Hierbij gaat het er niet alleen om de interne vertrouwde zone tegen de externe, onvertrouwde 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 informatiestromen en risicovolle beheercommando's te reguleren. Zonering als middel om toegang tot voorzieningen te beperken werkt op een hoger beheersingsniveau dan via logische toegangsbeveiliging. Zonering maakt het netwerk overzichtelijker voor beheer en dat is tevens van belang voor beveiliging.

Elke zone kent dus andere risico's, die samenhangen met de diensten of IT-voorzieningen die erin opgenomen zijn. Binnen zones kunnen met standaard maatregelen subzones (compartimentering) worden ingericht als het risicoprofiel dat vereist. Bijvoorbeeld om verschillende productieomgevingen uit elkaar te houden, die niet hetzelfde beveiligingsniveau hebben. Externe netwerken worden in dit zoneringsconcept ook als aparte zone gezien.

Aangezien het overgrote deel van de toepassingen van encryptie erop gericht zijn gegevensbeïnvloeding vanuit een andere IT-voorziening te voorkomen, worden dit type maatregelen onder zonering gepositioneerd.

Motivering
Door zonering kunnen risico's worden geïsoleerd, waardoor bedreigingen en incidenten die optreden in de ene zone niet doorwerken in een andere zone.

C.16.4.1. Zonering technische infrastructuur

Beheersmaatregel
De indeling van zones binnen de technische infrastructuur vindt plaats volgens een vastgesteld inrichtingsdocument (configuratiedossier) waarin is vastgelegd welke uitgangspunten gelden voor de toepassing van zonering.

Implementatierichtlijnen (Code 11.4.5)
1. Er zijn aparte zones voor Ontwikkeling, Test, Acceptatie en Productie (Code 10.1.4.b).

2. De experimenteer omgeving (laboratorium, sand box) is een fysiek gescheiden zone.
3. Beheer van zones vindt plaats vanuit een eigen zone.
4. 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 werkplek) gepositioneerd.
5. Dataservers waarvoor een hoger beveiligingsniveau geldt dan het basisniveau, kunnen in een eigen zone worden opgenomen (Code 11.6.2).
6. Van werkstations wordt bepaald welke onderdelen tot welke zone behoren, gelet op de risico's van het onbevoegd ontsluiten van data via de verschillende 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 geblokkeerd.
7. Interne systemen wisselen gegevens uit met ketenpartners en klanten via een centrale interne zone (DMZ) en een vertrouwde, externe zone.
8. Voor de uitwisseling van gegevens met derden (niet openbare gegevens) worden besloten externe zones (vertrouwde derden) gebruikt.
9. In een DMZ worden alleen openbare gegevens van een organisatie opgeslagen, die in het uiterste geval verloren mogen gaan. (Code 10.9.3.d)
10. Vitale bedrijfsgegevens worden in een aparte zone geplaatst.

C.16.4.2. Eisen te stellen aan zones

Beheersmaatregel
Zones zijn voor beveiliging en beheer als eenheid gedefinieerd.

Implementatierichtlijnen
1. Elke zone heeft een vastgesteld, uniek beveiligingsdoel.
2. Elke zone wordt slechts beheerd onder verantwoordelijkheid van één beheerinstantie (m.u.v. onvertrouwde derden).
3. Een zone heeft een gedefinieerd beveiligingsniveau, d.w.z. kent een gedefinieerd stelsel van samenhangende beveiligingsmaatregelen.
4. De maatregelen van logische toegangsbeperking zijn van toepassing op alle IT-voorzieningen in een zone.
5. Uitwisseling van gegevens tussen zones vindt uitsluitend plaats via een gedefinieerd koppelvlak.
6. Zones kunnen worden onderscheiden door gebruikmaking van routering van datastromen, verificatie van de bron- en de bestemmingsadressen (Code 11.4.7), door toepassing van verschillende protocollen, encryptietechnologie, partitionering of virtualisatie van servers, maar ook door fysieke scheiding.
7. Poorten, diensten en soortgelijke voorzieningen geïnstalleerd op een computer of netwerkvoorziening, die niet speciaal vereist zijn voor de bedrijfsvoering, worden uitgeschakeld of verwijderd. (Code 11.4.4)

C.16.4.3. Encryptie ten behoeve van zonering

Beheersmaatregel
De communicatie en de opslag van gegevens die buiten de invloedsfeer van de logische en fysieke toegangsbeveiliging maar wel binnen de eigen beheeromgeving vallen of waarvoor deze maatregelen onvoldoende zijn, zijn door encryptie beschermd.

Implementatierichtlijnen
1. Encryptie dient te worden toegepast in de volgende situaties:
a. bij verplaatsbare 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);
b. het extern geheugen van mobiele apparatuur (denk aan harde schijven van portable werkstations en geheugenkaarten in PDA's/smartphones);c. bij beheersessies over het eigen netwerk (met encryptievoorzieningen binnen de beheertools of gebruikte protocollen);
d. bij datatransport over onvertrouwde netwerkwerken (internet) of om een hoger beveiligingsniveau te bereiken (Code 10.6.1.c, 10.9.2.c, 12.2.3).
e. bij datatransport via mobiele datadragers buiten de reikwijdte van de fysieke toegangsbeveiliging van een organisatie;
f. bij draadloze datacommunicatie; (Code 10.6.1.c)
g. wachtwoorden, die worden opgeslagen of verzonden; (Code 11.5.3.i)
h. end-to-end encryptie als aanvullende beveiligingsmaatregel kan alleen binnen een zone gebruikt worden ter voorkoming van doorgeven van ongewenste soft- of malware van de ene zone naar de andere.

Uitzondering hierop vormt de communicatie tussen werkstations en dataservers.
2. 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 computerapparatuur en -programmatuur die zo is ontworpen dat er cryptografische functies aan kunnen worden toegevoegd; (Code 15.1.6.b)
3. Er is in het kader van de naleving van de relevante overeenkomsten, wetten en voorschriften rekening gehouden met de beperkingen op het gebruik van versleutelingstechnieken; (Code 15.1.6.c)

C.16.4.4. Sterkte van de encryptie

Doelstelling
De sterkte van de encryptiemechanismen voldoet aan de eisen van de tijd.

Implementatierichtlijnen
1. De gebruikte cryptografische algoritmen zijn als open standaard per soort toepassing gedocumenteerd en staan als robuust bekend.
2. Hardware-oplossingen (bijv. smart card- en Hardware Security Module producten) zijn gecertificeerd volgens daartoe strekkende standaards.
3. De sleutellengte is instelbaar en voldoende groot om ook in de afzienbare toekomst bestand te zijn tegen succesvolle pogingen om de sleutels te laten achterhalen met inachtneming van het belang van de gegevens, die erdoor worden beschermd.

C.16.4.5. Vertrouwelijkheid en integriteit sleutels

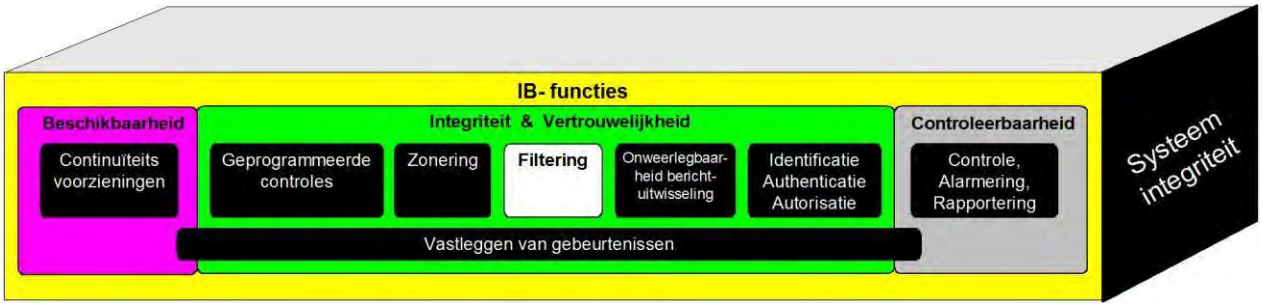
Beheersmaatregel
De vertrouwelijkheid en integriteit van geheime cryptografische sleutels is gewaarborgd tijdens het gehele proces van generatie, transport, opslag en vernietiging van de sleutels.

Implementatierichtlijnen
1. Cryptografische sleutels en certificaten kennen een geldigheidstermijn die is afgestemd op het kritische gehalte van de toepassing met een maximum van 1 jaar.
2. Sessie-encryptie met een unieke sessiesleutel heeft zo mogelijk de voorkeur boven encryptie met periodiek te wijzigen sleutels. Deze sessiesleutel wordt random gegeneerd, is bij voorkeur symmetrisch en wordt bij voorkeur uitgewisseld met een asymmetrisch algoritme.
3. Generatie en installatie van private keys, master keys en root certificates vinden plaats binnen een beschermende omgeving van cryptohardware.
4. Deze cryptohardware is tamper-resistant. Dit betekent dat er bijzondere voorzieningen zijn getroffen tegen onbevoegde kennisname van de opgeslagen cryptosleutels bij een fysieke inbreuk op de hardware.
5. Interactieve bediening van cryptohardware vindt plaats volgens het vier-ogen-principe (wachtwoorden van twee personen nodig voor één handeling). Denk hierbij aan installatie, wijzigingen in configuratie en generatie van master keys.

C.16.5. Filtering

Doelstelling
Op het koppelvlak tussen zones zijn filterfuncties gepositioneerd voor het gecontroleerd doorlaten van gegevens; niet-toegestane gegevens worden tegengehouden.

Definitie
Controle van informatiestromen op communicatiegedrag, vorm (protocol) en of inhoud van gegevens, afhankelijk van de aard van de informatiestromen en de zones of netwerkknooppunten waar ze vandaan komen of naar toe gaan.



Toelichting
Filtering beschermt zones tegen aanvallen, indringers, ongewenste inhoud en virussen, waardoor diensten onbereikbaar worden of onrechtmatige toegang tot gegevens of systemen wordt verkregen. Filtering controleert geen identiteiten van individuele gebruikers.
De communicatie tussen twee zones kan worden getoetst op ongewenste eigenschappen. Daarvoor wordt een elektronisch profiel vastgelegd van de zenders in de betrokken zones. Van het communicatiegedrag wordt elektronisch een 'reputatie score' vastgelegd, die enerzijds wordt vergeleken met het desbetreffend inrichtingsdocument (configuratiedossier) voor het doorlaten van communicatie en anderzijds met bekende patronen van ongewenste communicatie.
In de situatie dat end-to-end beveiliging wordt toegepast op berichten of documenten, zal minder filtering noodzakelijk zijn, maar dat tast het zonerings- en filteringsconcept niet aan; het kan wel tot een andere invulling 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-patronen aanleiding vormen de normering aan te passen.

Motivering
Filterfuncties zijn onlosmakelijk verbonden aan de IB-functie 'Zonering' en ontlenen daaraan ook hun motivering.

C.16.5.1. Controle op communicatiegedrag

Beheersmaatregel
Ongewenst communicatiegedrag wordt opgemerkt en geblokkeerd.

Implementatierichtlijnen
1. De filtering tussen zones is afgestemd op de doelstelling van de zones en het te overbruggen verschil in beveiligingsniveau. Hierbij vindt controle plaats op protocol en richting van de communicatie. Niet toegestane verbindingen worden geblokkeerd c.q. er wordt verhinderd dat deze tot stand komen.
2. 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 vollopen, dat onbereikbaarheid of uitval van computers het gevolg is (denial of service attacks).
3. Al het gegevensverkeer vanuit externe of onvertrouwde zones wordt real-time inhoudelijk geïnspecteerd op inbraakpogingen. Een update van aanvalspatronen vindt frequent plaats.

C.16.5.2. Controle op gegevensuitwisseling

Beheersmaatregel
De gegevensuitwisseling tussen zones wordt naar vorm en inhoud gecontroleerd, waarbij ongewenste gegevens worden geblokkeerd.

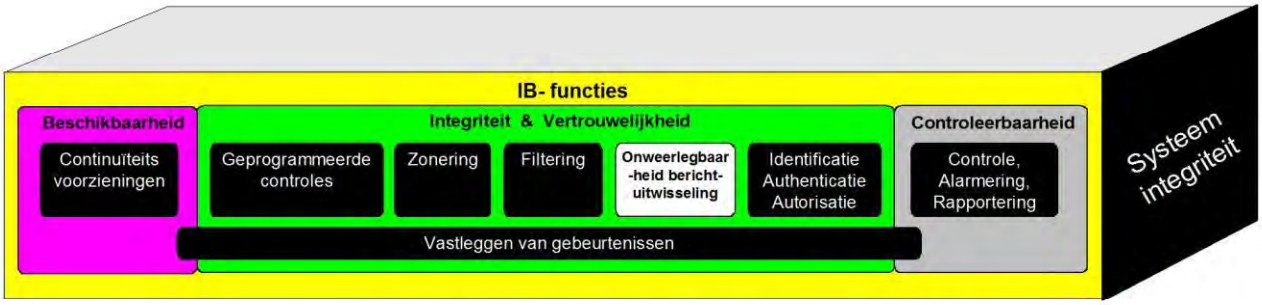
Implementatierichtlijnen
1. De uitvoer van toepassingssystemen waarmee gevoelige informatie wordt verwerkt, wordt alleen verzonden naar computerterminals en locaties met een autorisatie (Code 11.6.1.d)
2. Versleutelde gegevensstromen van en naar de externe zone worden ontsleuteld voor inhoudelijke controles.
3. E-mail berichten met bijlagen worden uitsluitend doorgelaten op basis van geformaliseerde afspraken over de coderingsvorm (extensie) van de bijlage. Gecontroleerd wordt of de aanduiding van de

coderingsvorm klopt met de werkelijke coderingsvorm van de bijlage.
4. Berichten en bestanden met een omvang boven een vastgestelde grenswaarde worden geblokkeerd om problemen wegens onbeschikbaarheid te voorkomen.
5. Er is antivirusprogrammatuur actief die e-mail berichten en webpagina's blokkeert met kwaadaardige code (virussen, wormen, trojans, spyware, etc.) in zowel ontvangen als verzonden e-mails. Een update van antivirusdefinities vindt frequent plaats (Code 10.4.1.d, 10.8.1.b)
6. Er is een (spam) filter geactiveerd voor zowel ontvangen als verzonden berichten. Een update van het spamfilter vindt frequent plaats.
7. Op alle werkstations en daarvoor in aanmerking komende servers is antivirusprogrammatuur resident actief. Een update van virusdefinities en/of antivirusprogrammatuur kan op ieder moment (handmatig) uitgevoerd worden en vindt periodiek of bij concrete dreigingen geautomatiseerd plaats. (Code 10.4.1.d)
8. In een keten van zones binnen een organisatie wordt antivirusprogrammatuur van verschillende leveranciers toegepast (Code 10.4.1)

C.16.6. 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 verstuurd 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 onvertrouwd 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 verstuurd. Dit wordt ook wel non-repudiation genoemd. Dit kan met behulp van een zogenoemde elektronische handtekening, die toepasbaar is als wettelijk bewijs mits voldaan wordt aan eisen in de Wet Elektronische Handtekening (WEH).
In het algemeen valt het 'zetten' van de digitale handtekening uiteen 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').
Verbinden van de unieke identiteit van de zender aan de hash.
Het zetten van een digitale handtekening kan plaatsvinden met verschillende methoden, waarvan de twee bekendste zijn:
- Symmetrische cryptografische sleutels = vooraf uitgedeeld door regiepartij.
- Asymmetrische cryptografie o.b.v. PKI = uitgedeeld door vertrouwde derde.

Bij een Public Key Infrastructure (PKI) worden twee encryptiesleutels toegepast: 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 én ontsleuteling. Deze sleutels hebben een unieke wiskundige relatie met elkaar. Hierdoor kunnen ze in combinatie met de betreffende certificaten

gebruikt worden voor authenticatie en het versturen van geheime (sleutel-) informatie over een onvertrouwd netwerk.

Motivering
Als er geen specifiek daarop afgestemde maatregelen zijn, wordt het risico gelopen dat een ontvanger van een bericht kan ontkennen ooit een bericht te hebben ontvangen of kan ontkennen een bericht te hebben ontvangen met de inhoud zoals deze door de verzender is verstuurd. In het elektronisch berichtenverkeer zijn aanmerkelijk meer risico's in deze te onderkennen dan in het fysieke postverkeer.

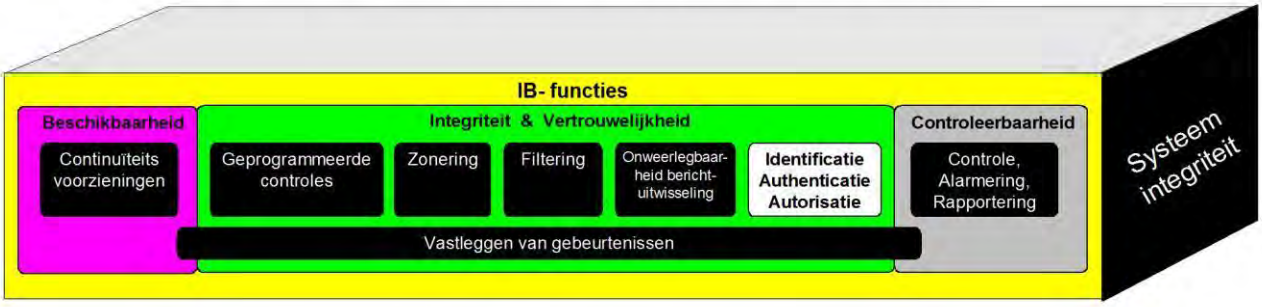
Beheersmaatregel
Bij berichtuitwisseling waaruit rechten en plichten ontstaan tussen partijen bestaat de zekerheid dat het ontvangen bericht afkomstig is van de verzender en dat de inhoud niet door derden is beïnvloed.

Implementatierichtlijnen
Onweerlegbaarheid kan worden verkregen op twee verschillende wijzen:
1. Een betrouwbare berichtendienst in het besloten netwerkverkeer, waarbij verzending en ontvangst van berichten bevestigd wordt door de berichtendienst dan wel hiervoor in de applicaties extra functies op te nemen. (Code 10.8.4.a, 10.8.4.b, 10.8.4.c)
Of bij een onvertrouwd netwerk:
2. Een PKI voldoet aan de daarvoor geldende standaarden, bij de overheid die van de PKI-Overheid (Code 10.9.2.a, 10.9.2.b, 10.9.2.d, 10.9.2.f, 10.8.4.a, 10.8.4.b, 10.8.4.c, 10.8.4.d, 12.2.3)
3. De elementen die het bewijs vormen van een elektronische handtekening, worden in de vorm van een juridisch logbestand zodanig samen met de originele data bewaard, dat datzelfde bewijs in de normale werkstroom van het bedrijfsproces altijd weer is te reproduceren.
4. De ontvangen berichten worden onmiddellijk na ontvangst in de juridische logging vastgelegd, voordat enige bewerking met toepassingssoftware aan de orde is.
5. De verzonden berichten worden in de laatste fase van verwerking onmiddellijk voordat verzending plaatsvindt in de juridische logging vastgelegd.
6. Voor de juridisch logging gelden dezelfde implementatierichtlijnen als voor logging, zie 16.8 Vastleggen van gebeurtenissen.

C.16.7. Identificatie, Authenticatie en Autorisatie

Doelstelling van de IB-functie
Logische toegangscontrole vindt plaats voordat IT-voorzieningen kunnen worden gebruikt.

Definities
Logische toegangscontrole 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 verkregen.



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 bekend maken 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 functies of gegevens wel benaderen en wat mag je ermee doen: uitvoeren, raadplegen of ook muteren?

Identificatie en Authenticatie wordt vrijwel altijd in combinatie met elkaar gebruikt. Autorisatie is een meer op zichzelf staande subfunctie, die qua implementatie in de IT geheel eigen consequenties heeft.

Motivering
Het kunnen handhaven 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.16.7.1. Identificatie

Beheersmaatregel
Alle toegangsvragers (gebruikers) tot een geheel van IT-voorzieningen zijn uniek herleidbaar tot één natuurlijk persoon, organisatie of IT-voorziening.

Implementatierichtlijnen
1. Natuurlijk personen, organisaties of IT-voorzieningen worden geïdentificeerd door een unieke identificatie. (Code 11.5.2, 11.5.3.a)
2. Vrijgesteld van identificatie zijn gebruikers met toegang tot systemen die alleen publieke of binnen een organisatie algemeen toegankelijke informatie ontsluiten.
3. Systeemprocessen draaien onder een eigen gebruikersnaam (een functioneel account), voor zover deze processen handelingen verrichten voor andere systemen of gebruikers.
4. IT-systemen bieden de mogelijkheid dat beheerders beheerwerkzaamheden uitvoeren onder hun eigen persoonsgebonden gebruikersnaam. In de operatie worden beheerwerkzaamheden en werkzaamheden als gewone gebruiker onder twee verschillende gebruikersnamen uitgevoerd.
5. Het gebruik van speciale beheer accounts (root, administrator) is uitgeschakeld, als gebruik onvermijdelijk is moet herleidbaarheid, doelbinding én onweerlegbare logging gecombineerd toegepast worden.

C.16.7.2. 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.

Implementatierichtlijnen
1. Bij het intern gebruik van IT-voorzieningen worden gebruikers minimaal geauthenticeerd op basis van wachtwoorden (Code 11.5.3.a).
2. In de volgende situaties vindt authenticatie van gebruikers plaats op basis van cryptografische techniek, ‘hardware tokens’ of een ‘challenge/response’-protocol:
a. Single Sign On;
b. toegang vanuit een onvertrouwde omgeving (Code 6.2.1.d, 10.8.4 f, 11.4.2);
c. bij beheer van kritische beveiligingsvoorzieningen (denk bijvoorbeeld aan Hardware Security Modules, firewalls, Intrusion Detection and Prevention Systems en routers).
3. Bij het niet-dagelijks beheer van kritische beveiligingsvoorzieningen vanuit een vertrouwde omgeving is het vier ogen principe een alternatief voor 2.b (dat wil zeggen dat er altijd twee functionarissen nodig zijn om een handeling uit te voeren).
4. Een mobiel apparaat (zoals een laptop, handheld computer, smartphone, PDA) vraagt om een pincode of wachtwoord bij het inschakelen.
5. Bij telewerken, beheer op afstand en mobiel werken (een mobiel apparaat dat draadloos verbonden is met IT-voorzieningen van de organisatie) wordt vastgesteld dat vanaf een voor dit doeleinde beschikbaar gestelde werkplek wordt gewerkt (Code 11.4.2, 11.4.3)
6. Wachtwoordbestanden worden gescheiden opgeslagen van gegevens van de toepassing. (Code 11.5.3.h)

C.16.7.3. Wachtwoordconventies

Beheersmaatregel
Bij authenticatie op basis van kennis dwingt het systeem het toepassen van sterke wachtwoordconventies af.

Implementatierichtlijnen
1. Wachtwoorden voldoen aan de volgende wachtwoordconventie (Code 11.2.3.d, 11.3.1.d, 11.5.3.c):
a. minimaal acht tekens;
b. minimaal één hoofdletter;
c. minimaal 4 kleine letters;
d. minimaal 1 cijfer en/of één vreemd teken;
e. nieuw wachtwoord moet in minimaal twee tekens verschillen met het vorig wachtwoord (Code 11.3.1.e, 11.5.3.f).
2. Wachtwoorden van gebruikersaccounts moeten minimaal elke 90 dagen gewijzigd worden (Code 11.3.1.e, 11.5.3.d).
3. Wachtwoorden van functionele accounts worden minder frequent gewijzigd, namelijk minimaal eens per jaar en ten 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.
4. De gebruikers hebben de mogelijkheid hun eigen wachtwoord te kiezen en te wijzigen. Hierbij geldt het volgende (Code 11.5.3.b):
a. Voordat een gebruiker zijn wachtwoord kan wijzigen, wordt de gebruiker opnieuw geauthenticeerd;
b. ter voorkoming van typefouten in het nieuw gekozen wachtwoord is er een bevestigingsprocedure;
c. alvorens een nieuw wachtwoord wordt gewijzigd, wordt geautomatiseerd gecontroleerd of het nieuwe wachtwoord aan de vereiste conventies voldoet.
5. De default en installatiewachtwoorden worden tijdens of direct na installatie verwijderd of gewijzigd. (Code 11.2.3.h)
6. Initiële wachtwoorden en wachtwoorden die gereset zijn, voldoen aan bovenstaande wachtwoordconventie en daarbij wordt door het systeem afgedwongen dat bij het eerste gebruik dit wachtwoord wordt gewijzigd (Code 11.2.3.b, 11.3.1.f, 11.5.3.e)

C.16.7.4. 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.

Implementatierichtlijnen
1. Er wordt zoveel mogelijk voorkomen dat gebruikers zich op de verschillende IT-voorzieningen in dezelfde keten opnieuw aan moeten melden. Als dit niet mogelijk is, dan wordt het aanmeldproces zo veel mogelijk enkelvoudig ingericht.
2. Expiratiedatums van accounts zijn afgestemd op de einddatum van de contracten van de medewerkers.
3. Op het eindgebruikers platform wordt gebruik gemaakt van schermbeveiligingsprogrammatuur (een screensaver) die na 30 minuten alle informatie op het beeldscherm onleesbaar maakt (Code 11.5.5). Het is toegestaan dat het systeem zo geconfigureerd wordt, dat binnen een toegestane periode van enkele seconden de gebruiker door een muisbeweging of toetsenbordaanslag kan verhinderen dat de schermbeveiliging wordt geactiveerd. Het systeem biedt de gebruiker ook zelf de mogelijkheid om de schermbeveiliging op eenvoudige wijze te activeren (Code 11.3.2.a). Het systeem is zo ingesteld dat na het activeren van de schermbeveiliging de gebruiker zich opnieuw moet authenticeren (de identificatie mag zichtbaar blijven).
4. Nadat voor een gebruikersnaam 5 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, totdat de gebruiker verzoekt deze lock-out op te heffen of het wachtwoord te resetten (Code 11.5.1.e)
5. Het wachtwoord wordt niet getoond op het scherm tijdens het ingeven van het wachtwoord. Het is wel gebruikelijk dat toetsaanslagen worden weergegeven door sterretjes of bullets (Code 11.5.1.h, 11.5.3.g).
6. Voorafgaand aan het aanmelden wordt aan de gebruiker een melding getoond dat alleen geautoriseerd gebruik is toegestaan voor expliciet door de organisatie vastgestelde doeleinden (Code 11.5.1.b).
7. Voor het inloggen vanuit een niet-vertrouwd netwerk wordt een maximumtijd van 10 minuten en een minimumtijd van 10 seconden vastgesteld; indien deze tijd wordt overschreden, beëindigt het systeem het

inlogproces (Code 11.5.1.f).
8. Netwerksessies worden na een vastgestelde periode van inactiviteit afgesloten. De duur van de periode tot de time-out is afgestemd op de vertrouwdheid van de zone (intern of extern), de gevoeligheid van de informatie die wordt verwerkt en de toepassingen die worden gebruikt. (Code 11.5.5)
9. Voordat een geslaagde 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 gebruikersnaam bestaat, maar slechts dat de combinatie gebruikersnaam en wachtwoord onjuist was, nadat alle gegevens voor het inloggen zijn ingevuld. Er wordt bovendien geen geheugensteun voor het wachtwoord getoond. (Code 11.5.1.a, 11.5.1.c, 11.5.1.d)
10. Zodra een inlogproces succesvol is voltooid, worden de datum en tijd van de voorgaande succesvolle login getoond (Code 11.5.1.g).
11. Automatisch aanmelden is niet toegestaan voor interactieve gebruikers. Hier wordt bedoeld dat automatisch wordt ingelogd zonder dat binnen de sessie door een gebruiker een wachtwoord wordt ingegeven (bijvoorbeeld het gebruik van Windows Auto Log-on mag dus niet, waarbij door het aanzetten van een PC een gebruiker automatisch wordt ingelogd onder een vooraf opgegeven gebruikersnaam met een vooraf opgegeven wachtwoord). Alleen systeemprocessen met functionele accounts mogen binnen een zone geautomatiseerd aanloggen (Code 11.3.1.g).

C.16.7.5. Autorisatie

Beheersmaatregel
Autorisaties zijn ingesteld op basis van ontwerp- of systeemdocumentatie, waarin aangegeven is welke rechten in welke gebruikersgroepen worden ondergebracht.

Toelichting en afbakening
De IB-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 procesontwerpers en functioneel beheerders, rollenbeheerders, ondersteunende functies bij het aanvragen van autorisaties door lijnmanagers.

Implementatierichtlijnen
1. De technische implementatie van autorisaties naar autorisatiegroepen is in overeenstemming met de ontwerp- of systeemdocumentatie.
2. Speciale (systeem)bevoegdheden zijn in aparte autorisatiegroepen opgenomen.
3. Bij het koppelen van gebruikers aan autorisatiegroepen kunnen aangegeven onverenigbaarheden worden gesignaleerd.

C.16.7.6. Minimaliseren rechten

Beheersmaatregel
IT-voorzieningen zijn met zo min mogelijk toegangsrechten ingesteld.

Implementatierichtlijnen
1. In de soort toegangsregels 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-voorziening en de daardoor veroorzaakte beheerslast. Zo kunnen bij schrijfrechten vaak rechten voor creëren (zoals create/insert/generate), wijzigen (zoals update/change/alter) en verwijderen (zoals delete/drop/purge) separaat worden toegekend. Standaard gebruikers krijgen geen execute-rechten. (Code 11.6.1.b).
2. De toekenning van rechten aan processen en bestanden is zo minimaal mogelijk. Bijvoorbeeld:
a. als het platform toestaat om gescheiden executie- en leesrechten toe te kennen, dan worden voor programmabestanden geen leesrechten toegekend;
b. tijdelijke (spool)bestanden (bijv. printgegevens) zijn alleen voor systeembeheer toegankelijk;
c. er worden geen, of anders zo weinig mogelijk rechten gegeven aan standaard groepen en accounts, zoals “guest”, “public” of “everyone”.
3. Toepassingen mogen niet onnodig en niet langer dan noodzakelijk onder een systeemaccount (een privileged user) draaien. Direct na het uitvoeren van handelingen waar 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 daarna terugschakelt naar userniveau. Een ander voorbeeld is het gebruik het 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.
4. De taken die met (tijdelijk) hogere rechten uitgevoerd worden, kunnen niet onderbroken of afgebroken worden met als gevolg dat deze hogere rechten voor andere doeleinden gebruikt kunnen worden (feitelijk misbruikt kunnen worden).

C.16.7.7. Tegengaan onbedoeld gebruik autorisaties

Beheersmaatregel
Er zijn maatregelen getroffen die onbedoeld gebruik van toegekende autorisaties voorkomen.

Implementatierichtlijnen
1. Gebruikers krijgen geen algemene commando-omgeving tot hun beschikking (bijvoorbeeld een Dos-prompt of Unix-shell) (Code 11.6.1.a).
2. Beheertaken verlopen zoveel mogelijk via een menusysteem en gestandaardiseerde werkwijzen (scripts) (Code 11.6.1.a).
3. Bij het overnemen van werkstations door beheerders om te kunnen meekijken op het werkstation wordt technisch afgedwongen dat hiervoor eerst toestemming aan de gebruiker wordt gevraagd. De gebruiker kan op elk moment de verleende toestemming intrekken.
4. Systeemdata, programmatuur en toepassingsgegevens zijn van elkaar gescheiden, dat wil zeggen dat de bestanden zoveel mogelijk in eigen directory's of partities geplaatst worden.
5. Er zijn in productiezones geen hulpmiddelen toegankelijk die het systeem van logische toegangsbeveiliging doorbreken of de integriteit van de productieverwerking kunnen aantasten, zoals: ODBC, bestandsviewers, editors, ontwikkelcode, compilers, tekstverwerkingsprogramma's en eventuele andere systeemhulpmiddelen (Code 10.1.4.c, 12.4.1.b).
6. Gebruikers hebben verschillende gebruiksprofielen voor operationele en proefsystemen, en de menu's tonen de juiste identificatieboodschappen om het risico van fouten te verminderen (Code 10.1.4 e).
7. Wachtwoorden worden versleuteld over een netwerk verzonden (Code 11.5.1.i, 11.5.3.i).
8. Opgeslagen wachtwoorden worden altijd met een one-way hashfunctie versleuteld. (Code 11.2.3.g, 11.5.3.i)
9. Besturingsprogrammatuur heeft de mogelijkheid zowel programma-, netwerk- als gebruikerssessies af te sluiten.
10. Er worden vooraf gedefinieerde perioden ('time slots') gebruikt, bijvoorbeeld voor overdracht van groepen bestanden ('batch file transfer') of met regelmatig tussenpozen terugkerende interactieve sessies van korte duur (Code 11.5.5, 11.5.6.a).
11. Authentificatieprocedures worden herhaald op basis van het hiervoor opgestelde beleid. (Code 11.5.6.c)
12. Werkstations die niet in gebruik zijn, worden tegen onbevoegd gebruik beveiligd met behulp van een toetsvergrendeling of vergelijkbare beveiliging, bijvoorbeeld een wachtwoord. (Code 11.3.2.c)

C.16.7.8. Beheersbaarheid autorisaties

Beheersmaatregel
Verleende toegangsrechten zijn inzichtelijk en beheersbaar.

Implementatierichtlijnen
1. De registratie van gebruikers en verleende toegangsrechten is zoveel mogelijk centraal geregeld (single-point-of-administration).
2. Toegangsrechten worden zoveel mogelijk via groeperingmechanismen (bijv. t.b.v. RBAC) toegekend (dus niet rechtstreeks aan individuele gebruikers). Uitzonderingen vergen extra aandacht bij het beheer.
3. Voor groeperingsmechanismen geldt een naamgevingconventie, die aansluit op zo stabiel mogelijke uitgangspunten (dus zo min mogelijk afdelingsgebonden als er regelmatig organisatiewijzigingen plaatsvinden).

C.16.7.9. Volledigheid toegangsbeveiliging

Beheersmaatregel
Op alle IT-voorzieningen is toegangsbeveiliging van toepassing.

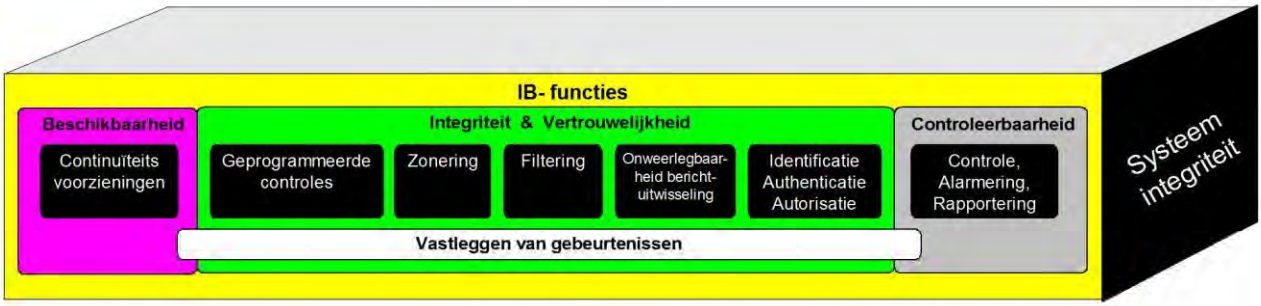
Implementatierichtlijnen
1. Toegangsbeveiliging is geïmplementeerd op alle middelen die gegevens bevatten of verwerken. Dit

betreft onder meer de volgende middelen:
a. platforms (vaste en mobiele werkplek, server, mainframe): bestanden, directory's, services en randapparatuur (denk aan USB-devices op de werkplek);
b. ondersteunende systemen: services;
c. primaire systemen: taken/functies in applicaties, stored procedures, gegevensbenadering in databases (views, tabellen, velden, records) (Code 11.6.1.c);
d. beheer: beheer van appliances en firmware van hardware voor zover dit kan. Mogelijk is er geen functionaliteit op de toegang tot firmware met een rechtenstructuur te beveiligen. Wel dient in ieder geval een wachtwoord te zijn ingesteld.

C.16.8. Vastleggen van gebeurtenissen

Doelstelling van de IB-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 voorziening van de technische infrastructuur is een voorbeeld van een gebeurtenis.
Het onweerlegbaar vastleggen van gebeurtenissen is noodzakelijk om achteraf controle te kunnen uitoefenen en/of foutsituaties te kunnen uitzoeken. Het vastleggen is tevens noodzakelijk als bewijsmiddel voor private of strafrechtelijke vordering.
Veel gebeurtenissen die voor het beheer van de technische infrastructuur van belang zijn, hebben tevens betekenis in het kader van informatiebeveiliging.
Logging moet niet verward worden met het begrip audit trail, dat betrekking heeft op het vastleggen van het verwerkingsproces door toepassingsprogrammatuur. Dit begrip wordt verder uitgewerkt bij de IB-functie 'Geprogrammeerde controles'.

Motivering
Het vastleggen van meldingen van besturingsprogramma's en andere systemen in de technische infrastructuur is noodzakelijk om achteraf controle te kunnen uitoefenen en/of foutsituaties te kunnen uitzoeken. Het vastleggen is tevens noodzakelijk als bewijsmiddel voor private- of strafrechtelijke vordering.

C.16.8.1. 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 grote 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 overwogen het juiste type berichten automatisch naar een tweede logbestand te kopiëren, en/of bepaalde systeemhulpprogramma's of audit-hulpmiddelen voor bestandsonderzoek en -rationalisatie te gebruiken.

Implementatierichtlijnen (Code 10.6.1.d, 10.10.1.a, 10.10.1.b, 10.10.1.c, 10.10.1.d, 10.10.1.e, 10.10.1.f, 10.10.1.g, 10.10.1.h, 10.10.1.i, 10.10.1.j, 10.10.1.k, 10.10.1.l)
1. De volgende uitgevoerde handelingen worden in ieder geval opgenomen in de logging:
a. gebruik van technische beheerfuncties en systeemhulpmiddelen (Code 11.5.4.f), zoals het wijzigingen van configuratie of instelling; uitvoeren van een systeemcommando, starten en stoppen, uitvoering van een back-up of restore, (tijdelijke) toekenning en uitoefening van hogere dan gebruikelijk rechten (incl. handelingen verricht met geprivilegieerde accounts, zoals root, superuser, proddba etc.);
b. gebruik van functionele beheerfuncties, zoals het wijzigingen van configuratie en instellingen, release van nieuwe functionaliteit, ingrepen in gegevenssets waaronder databases;
c. handelingen van beveiligingsbeheer, zoals het opvoeren en afvoeren gebruikers, toekennen en intrekken van rechten, wachtwoordreset, uitgifte en intrekken van cryptosleutels;
d. beveiligingsovertredingen (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);
e. verstoringen in het productieproces (zoals het vollopen van queues, systeemfouten, afbreken tijdens uitvoering van programmatuur, het niet beschikbaar zijn van aangeroepen programmaonderdelen of systemen);
f. handelingen van gebruikers, zoals verleende toegangsrechten, gebruik van on-line transacties en toegang tot bestanden door systeembeheerders.
2. In een te schrijven logregel wordt in ieder geval weggeschreven: (Code 10.10.4.a, 10.10.4.b, 10.10.4.c, 10.10.4.d)
a. de naar een natuurlijke persoon herleidbare gebruikersnaam die verzocht een handeling uit te voeren;
b. het soort handeling, het gegeven commando met de parameters;
c. waar mogelijk de identiteit van het werkstation of de locatie;
d. het middel waarop de handeling werd uitgevoerd of waar een event optrad;
e. het resultaat van de handeling indien dit niet uit het soort handeling is af te leiden;
f. de datum en het tijdstip van een handeling of event;
g. de severity-aanduiding: het beveiligingsbelang, waarop selectie t.b.v. de analyse kan plaatsvinden.
3. Systeemklokken worden tijdens openstelling gesynchroniseerd en worden gelijk gezet met een atoomklok op basis van het Network Time Protocol (NTP), zodat de juiste tijd in het logbestand vastgelegd kan worden. Een indicatie voor de synchronisatiefrequentie is 4 uur. De maximale afwijking ten opzichte van de standaardtijd is 100 milliseconden (Code 10.10.6).
4. In een te schrijven logregel worden in geen geval gegevens opgenomen waardoor de beveiliging doorbroken kan worden (zoals wachtwoorden, pincodes).

C.16.8.2. Integriteit logbestanden

Beheersmaatregel
De integriteit van opgeslagen logbestanden is gewaarborgd.

Implementatierichtlijnen (Code 10.10.3.a, 10.10.3.b)
1. Bij het schrijven en opslaan van logregels wordt zoveel mogelijk gebruik gemaakt van hiervoor ingerichte generieke beveiligingsvoorzieningen.
2. Bij het aanleggen van logbestanden wordt zo mogelijk gebruik gemaakt van “write once”-technologie.
3. De volledigheid van de logging kan worden vastgesteld, bijvoorbeeld met behulp van opeenvolgende nummers per log-event.
4. Uitsluitend geautoriseerde processen (operationeel onder een functioneel account) mogen logregels schrijven.
5. Het raadplegen van logbestanden is voorbehouden aan geautoriseerde gebruikers, waarbij de toegang is beperkt tot leesrechten.
6. 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 auditdoeleinden kent, dan wordt hiervan gebruik gemaakt bij het raadplegen.

C.16.8.3. Beschikbaarheid logbestanden

Beheersmaatregel
De beschikbaarheid van loginformatie is gewaarborgd binnen de termijn waarin loganalyse noodzakelijk

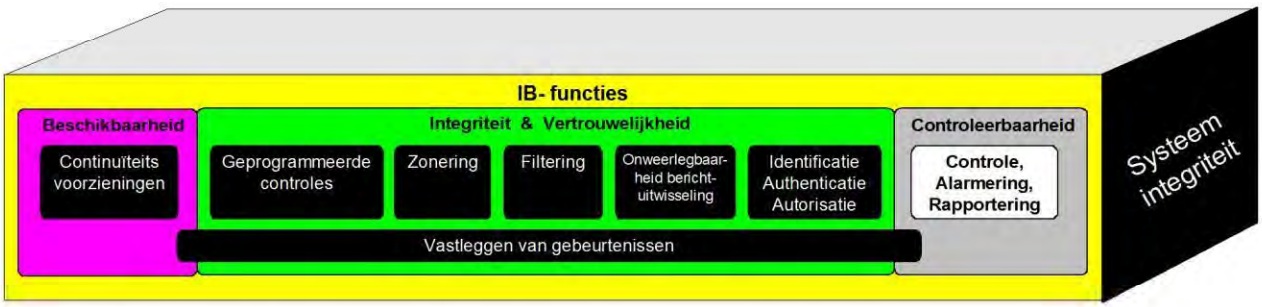
wordt geacht.

Implementatierichtlijnen
1. Loginformatie wordt bewaard totdat de bewaartermijnen verstreken zijn. Een indicatie voor de bewaartermijn is:
a. een transactie log wordt bewaard totdat is vastgesteld dat de juiste en volledige verwerking van de (batch) transactie(s) heeft plaats gevonden of totdat de mogelijkheid om een roll-back uit te voeren is verstreken, veelal maximaal één dag;
b. 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;
c. logging die van belang is voor auditing en onderzoek naar oneigenlijk gebruik wordt 2 jaar bewaard dan wel zolang als de gerechtelijke procedure duurt waarvoor de loggegevens als bewijsmateriaal dienen.
2. Er zijn query- en analysetools aanwezig voor het kunnen ontsluiten van loginformatie.
3. Het overschrijven of verwijderen van logbestanden wordt gelogd in de nieuw aangelegde log.
4. Het vollopen van het opslagmedium voor de logbestanden wordt gelogd en leidt tot automatische alarmering van de beheerorganisatie; bij kritische toepassingen 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 zekergesteld (op een ander medium). (Code 10.10.3.c)
5. Bij onderhoud op analyse- en raadpleegvoorzieningen voor een logbestand wordt achterwaartse compatibiliteit afgedwongen. Dit wil zeggen dat ook de eerder aangelegde logbestanden binnen de bewaartermijn van het logbestand met de nieuwe of gewijzigde voorziening ontsloten kunnen worden.

C.16.9. Controle, alarmering en rapportering

Doelstelling
In de technische infrastructuur zijn signaleringsfuncties werkzaam ter controle op vastgestelde inrichtingsdocument (configuratiedossier).

Definitie
Functies die erop gericht zijn te kunnen vaststellen dat de IT-voorzieningen overeenkomstig het vastgestelde inrichtingsdocument (configuratiedossier) functioneren en die signaleren wanneer dit niet het geval is of kan worden.



Toelichting
De tooling die in de markt verkrijgbaar is, maakt het mogelijk al deze functies geïntegreerd te behandelen. Zonder integratie 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 (configuratiedossier).
- Alarmering is een functie, die onmiddellijk signalen naar systeembeheerders kan afgeven als grenswaarden van het vastgestelde inrichtingsdocument (configuratiedossier) worden overschreden.
- Rapportering maakt het mogelijk beveiligingsincidenten, zoals hacking (ook van binnenuit) te onderkennen op basis van analyse en correlatie van vastleggingen.

Motivering
Op basis van de signaleringen kunnen beheerders acties ondernemen om verstoringen in de productieverwerking te voorkomen of om beveiligingsrisico's in de werking van een infrastructuur te kunnen

beheersen.

C.16.9.1. Controle op beveiligingsinstellingen

Beheersmaatregel
Instellingen van functies die voor de informatiebeveiliging van belang zijn en wijzigingen daarin worden automatisch gecontroleerd.

Implementatierichtlijnen
1. Bij automatische controle op beveiligingsinstellingen wordt het inbrengen van het Soll-bestand voor beveiligingsinstellingen gescheiden van andere systeemfuncties.
2. Instellingen van IB-functies, die betrokken zijn bij filtering kunnen automatisch op wijzigingen worden gecontroleerd en gealarmeerd .

C.16.9.2. Automatische signalering

Beheersmaatregel
Tevoren gespecificeerde, afwijkende gebeurtenissen volgens de loginformatie worden tijdig gesignaleerd en zo nodig gealarmeerd.

Implementatierichtlijnen
1. Er is gespecificeerd welke beveiligingsincidenten kunnen optreden. Deze beveiligingsincidenten zijn geclassificeerd naar ernst en urgentie.
2. 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.
3. Instelbaar is bij welke drempelwaarden de beheerorganisatie wordt gealarmeerd, zonodig ook buiten kantooruren.
4. De IB-functies voor Filtering en Logische Toegangsbeveiliging sluiten aan op de generieke beveiligingsvoorziening voor Security Incident en Event Management (SIEM) waarmee meldingen en alarmoproepen aan de beheerorganisatie gegeven kunnen worden

C.16.9.3. Analyse en rapportage

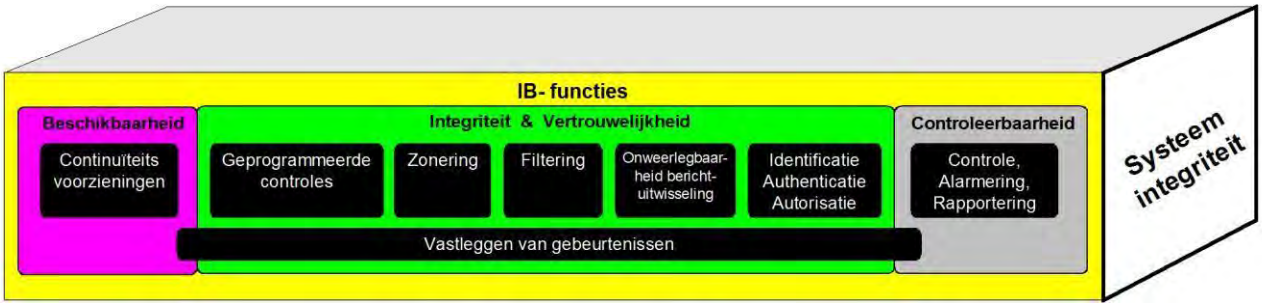
Beheersmaatregel
Logbestanden worden periodiek geanalyseerd en gecorreleerd ten einde beveiligingsincidenten dan wel de juiste werking van het systeem te detecteren.

Implementatierichtlijnen
1. Periodiek worden er automatisch correlaties en rapportages gemaakt over de verschillende vastgelegde gebeurtenissen.
2. Periodiek worden er trendanalyses vervaardigd en gerapporteerd over relevante gebeurtenissen in de logbestanden van een in te stellen periode.

C.16.10. Systeemintegriteit

Doelstelling
In de technische infrastructuur zijn functies werkzaam, die de systeemintegriteit ondersteunen.

Definitie
Het foutloos uitvoeren van de beoogde bewerkingen door de technische infrastructuur.



Toelichting
De factoren die in samenhang het foutloos uitvoeren van geautomatiseerde bewerkingen 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 infrastructurele functies, onjuiste of ontbrekende configuratie instellingen van programmatuurpakketten en voorzieningen van de technische infrastructuur, onjuiste deployment (functionele configuratie) van applicaties en/of infrastructuur.

Afbakening
De scope van de hieronder genoemde maatregelen is voor zover niet door andere functies bepaald, beperkt tot controlemechanismen op de actualiteit van de code, de integriteit van programmapakketten en infrastructurele programmatuur en mechanismen tot beheersing van mobiele code en tenslotte overige instellingen voor "hardening" van systemen. In de maatregelen is (nog) geen uitwerking gegeven aan normen voor webomgevingen.

Motivatie
In de huidige technologie resteert een aantal risico´s, die onder de noemer van systeemintegriteit als kapstokbegrip als IB-functie zijn aangemerkt. De maatregelen gericht op restrisico's zijn aan de praktijk ontleend.

C.16.10.1. Handhaven technische functionaliteit

Beheersmaatregel
De door de leverancier bepaalde technische functionaliteit van programmapakketten en infrastructurele programmatuur blijven gehandhaafd.

Toelichting en afbakening
In dit document worden voor de onderkende IB-functies normen geformuleerd, die deels bepalend zijn voor de instellingen van infrastructurele elementen van IT-voorzieningen. Het is echter niet mogelijk om voor alle beveiligingsrelevante instellingen productonafhankelijke normen te formuleren. Daarom blijft het noodzakelijk om alle overige instellingen op beveiligingsaspecten te beoordelen.

Implementatierichtlijnen
1. De technische integriteit van programmapakketten en infrastructurele programmatuur wordt gecontroleerd d.m.v. een hashingmechanisme en een controlegetal van de leverancier, dat via een vertrouwd kanaal is verkregen.
2. Behoudens de door de leverancier goedgekeurde updates worden er geen wijzigingen aangebracht in programmapakketten en infrastructurele programmatuur (Code 12.5.3.a, 12.5.3.b, 12.5.3.c, 12.5.3.d).
3. De instellingen (parametrisering) van programmapakketten en infrastructurele programmatuur zijn in overeenstemming met een vastgestelde inrichtingsdocument (configuratiedossier), dat is gebaseerd op aanwijzingen van de leveranciers, operationele productstandaards van bij voorkeur onafhankelijke instellingen, zoals die van NIST, voor zover de instellingen niet door de andere IB-functies van dit document zijn geadresseerd.
4. Instellingen van programmapakketten en infrastructurele programmatuur kunnen geautomatiseerd worden gecontroleerd op configuratieafwijkingen van het vastgestelde inrichtingsdocument.
5. Van programmapakketten en infrastructurele programmatuur kan bij voorkeur geautomatiseerd gecontroleerd worden of de laatste updates (patches) in zijn doorgevoerd.
6. Het automatisch doorvoeren van een update vindt alleen plaats als hierover speciale afspraken zijn gemaakt met de leverancier.
7. Van programmapakketten en infrastructurele programmatuur kan bij voorkeur geautomatiseerd

gecontroleerd worden of er bekende zwakheden in de configuratie voorkomen.

C.16.10.2. Systeemhulpmiddelen

Beheersmaatregel
Het gebruik van hulpprogrammatuur waarmee maatregelen in systeem- en toepassingssoftware zouden kunnen worden gepasseerd, wordt zoveel mogelijk beperkt.

Implementatierichtlijn
1. Identificatie-, authenticatie- en autorisatiemechanismen zijn ook voor systeemhulpmiddelen van toepassing. (Code 11.5.4.a)
2. Systeemhulpmiddelen en toepassingsprogrammatuur zijn gescheiden. (Code 11.5.4.b)
3. Onnodige hulpprogramma's en systeemprogrammatuur zijn verwijderd. (Code 11.5.4.h)

C.16.10.3. Hardening

Beheersmaatregel
Infrastructurele programmatuur, die vitale beveiligingsfuncties vervullen, bevatten geen onnodige en ongebruikte functies.

Toelichting
Vitale beveiligingsfuncties hebben hier betrekking op infrastructurele voorzieningen, die de zonering bepalen, deel uitmaken van de beheer en audit zone en van de zone waar de data van de bedrijfstoepassingen worden opgeslagen.

Afbakening
Voor het "hardenen" van infrastructurele IT-voorzieningen moet tevens worden voldaan aan de andere normen voor deze voorzieningen. Bij appliances wordt ervan uitgegaan die de onderliggende besturingssystemen reeds gehardend zijn.

Implementatierichtlijn
1. Onnodige en ongebruikte functies van infrastructurele programmatuur zijn uitgeschakeld.
2. Beheermogelijkheden zijn zoveel mogelijk afgesloten.
3. Er is zoveel mogelijk gebruik gemaakt van versleutelde beheermechanismen.
4. Beheer is alleen toegestaan vanaf vooraf gedefinieerde IP-adressen.
5. Voor toegang tot switches wordt gebruik gemaakt van Virtual LAN's (VLAN) en de toegang tot netwerkpoorten wordt beperkt op basis van MAC-adres (port security)

C.16.10.4. Mobiele code

Beheersmaatregel
Als gebruik van 'mobile code' wordt toegelaten, dan zorgt de configuratie ervoor dat de geautoriseerde 'mobile code' functioneert volgens een vastgesteld inrichtingsdocument (configuratiedossier) 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 en een specifieke functie verricht zonder of met weinig tussenkomst van de gebruiker. 'Mobile code' werkt samen met besturingsprogrammatuur (zgn. middleware) die de informatie-uitwisseling regelt tussen de cliëntsoftware en de software die de bedrijfsgegevens beheert. Vaak gaat het om gedistribueerde systemen en meerdere platforms.

Implementatierichtlijnen (Code 10.4.2)
1. De volgende handelingen worden overwogen om te verhinderen dat 'mobile code' ongeautoriseerde acties kan uitvoeren:
a. uitvoeren van toegestane 'mobile code' in een logisch geïsoleerde omgeving;
b. blokkeren van elk gebruik van 'mobile code';
c. blokkeren van ontvangen van 'mobile code';
d. activeren van technische maatregelen die beschikbaar zijn op een specifiek systeem om te waarborgen dat toegestane 'mobile code' wordt beheerd;

e. beheersen van de bronnen die beschikbaar zijn voor toegang tot toegestane ‘mobile code’;
f. cryptografische beveiligingsmaatregelen om toegestane ‘mobile code’ uniek te authenticeren.

C.16.10.5. Beheersing berichtenverwerking

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
1. Infrastructuur bevat logica die het beheer van foutbestanden mogelijk maakt.
2. Berichtverwerkende infrastructuur past foutloze berichtenverwerking toe (Persistence Messaging).
3. Foutbestanden worden niet gebruikt als opslagmechanisme (buffering). Voor tijdelijke opslag van berichten in verwerkingsketens worden aparte tussenbestanden gebruikt.
4. Stapelen van fouten wordt voorkomen door toepassing van ‘noodstop’ mechanismen. Juist verwerkte resultaten worden hierdoor niet noodgedwongen naar een foutief verwerkingsproces gestuurd.

C.16.10.6. Beheersing batchverwerking

Beheersmaatregel
Bij batchverwerking borgen productieplanning- en/of bewakingssystemen dat de risico’s van verwerkingsfouten die tot verlies van integriteit leiden geminimaliseerd worden.

Implementatierichtlijn
1. De planning van reguliere batchprogramma’s is gebaseerd op de aangegeven tijdstippen en volgorde 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. (Code 10.1.1.c, 12.2.2.b, 12.2.2.f, 12.2.2.g)
2. Onderdelen voor verwerking van batches worden pas opgestart nadat voorafgaande verwerkingen succesvol zijn beëindigd. (Code 12.2.2.b, 12.2.2.g)
3. Generatievalidatie- en herstelmechanismen voorkomen dubbele of onvolledige verwerkingen en borgen onderlinge verwerkingsrelaties bij het oplossen van productiefouten.
4. Bij uitwisseling van bestanden tussen centrale en decentrale servers of met externe partijen wordt met een apart file-transfermechanisme zeker gesteld dat uitwisseling niet achterwege blijft of dubbel plaatsvindt, tenzij beheersing geheel kan plaatsvinden volgens punt 1 hiervoor.
5. Er wordt een logbestand aangemaakt van de activiteiten die tijdens de verwerking plaatsvinden. (Code 12.2.2.h)

C.17. Gebouwen en installaties

Doelstelling
Gebouwen en installaties zijn de voorzieningen voor huisvesting van het personeel en de IT-voorzieningen, die beveiligingsmaatregelen van fysieke aard bevatten.

Motivering
De inrichting van gebouwen en installaties zijn in belangrijke mate bepalend in combinatie met het proces Leveren huisvesting voor het voldoen aan de eisen voor fysieke beveiliging.

Afbakening
Computerruimten vormen een speciale categorie ruimten binnen een gebouw. In dit normenkader wordt de inrichting van computerruimten gezien als een aparte verantwoordelijkheid. Omdat deze inrichting niet altijd op alle onderdelen goed is af te bakenen van de algemene inrichting van gebouwen en de ruimten daarbinnen is onderlinge afstemming tussen de verschillende verantwoordelijkheden een absoluut vereiste.

C.17.1. Terreinen en buitenkant gebouwen

C.17.1.1. Terreinen

Beheersmaatregel
De inrichting van terreinen waarborgt voldoende zicht op de gebouwen.

Implementatierichtlijn
1. Eventuele begroeiing of beplanting mag het uitzicht op de locatie niet verslechteren.
2. Op risicovolle punten bij de gebouwen is aanvullende terreinverlichting aangebracht. Afhankelijk van de vorm, omvang en locatie van de afzonderlijke gebouwen wordt de optimaal mogelijke oplossing gekozen.
3. De terreinverlichting is vandalismebestendig en is op zodanige wijze aangebracht dat de kans op vernieling of ongeautoriseerd uitschakelen tot het minimum wordt beperkt.

C.17.1.2. Buitenkant gebouw

Beheersmaatregel
De buitenkant van gebouwen voorkomt blikseminslag en ongewenste binnendringing van personen.

Implementatierichtlijn
1. Gebouwen zijn voorzien van bliksembescherming en er zijn bliksembeschermingsfilters aangebracht op alle binnenkomende spannings- en communicatieleidingen. (Code 9.2.1.g)
2. Op regenwaterafvoeren is klimbeveiliging aangebracht. (Code 9.1.1.b)
3. Waar van toepassing zijn er zo min mogelijk aanwijzingen over het gebruiksdoel van gebouwen ten aanzien van de aanwezigheid van informatieverwerkingsactiviteiten. (Code 9.1.3.c)

C.17.1.3. Beglazing

Beheersmaatregel
De beglazing is bestand tegen schade en vandalisme.

Implementatierichtlijnen (Code 9.1.1.b)
1. Bij nieuwbouw worden alle ruiten van het souterrain op de begane grond en de eerste etage beschermd conform de doorgooibeperkende beglazingsklasse P4A (NEN 365).
2. Bij bestaande bouw worden gevelopeningen op de etages: souterrain, begane grond en eerste etage uitgevoerd met beglazing met een sterkte conform DIN 52290, klasse A3, doorgooibeperkende eigenschappen en doorbraakvertraging ca. 7 min.
3. Bij bestaande bouw geldt dat alleen kritische ruimten, welke zich in het souterrain, begane grond of eerste etage bevinden en/of in een gelijkwaardige situatie op een hogere etage worden beschermd met een vergelijkbaar resultaat als de doorgooibeperkende beglazingsklasse P4A (NEN 365).

C.17.1.4. Toegangsdeuren

Beheersmaatregel
De toegangsdeuren voorkomen ongewenste binnendringing door personen.

Implementatierichtlijnen (Code 9.1.1.b)
1. Alle toegangsdeuren zijn ingericht om sabotage te voorkomen;
2. De deur van de buitengevel die gebruikt wordt voor openen en sluiten van het gebouw is voorzien van een cilinder.

C.17.2. Toegangbeperking gebouwen en ruimten

C.17.2.1. Ruimtelijke zonering

Beheersmaatregel
Gebouwen en ruimten zijn ingedeeld volgens een risicoafweging in zones.

Implementatierichtlijnen (Code 9.1.1.a)
1. Alle ruimtes van het gebouw zijn op basis van de bestemming toegedeeld aan een risicozone waarmee het bijbehorende beveiligingsniveau is vastgelegd.
2. Bij een toegang tot zones worden fysieke toegangsbeperkende barrières ingericht.
3. De toegangen tot zones worden gecontroleerd door een toegangscontrolesysteem.
4. Er wordt een ‘audit trail’ (naspeurbare registratie) van de verleende toegang door het toegangscontrolesysteem bijgehouden. (Code 9.1.2.b)

C.17.2.2. Inrichting gebouw

Beheersmaatregel
De inrichting van gebouwen ondersteunt de zoneringsmaatregelen en de brandveiligheid.

Implementatierichtlijnen (Code 9.1.1.d)
1. Gebouwen voldoen aan de wet en regelgeving in het kader van de brandveiligheid zoals vastgelegd in bouw- en gebruiksbesluiten. (Code 9.1.1.e)
2. De laad- en losruimte is zo ontworpen dat voorraden kunnen worden afgeleverd zonder dat de leverancier andere delen van het gebouw hoeft te betreden. (Code 9.1.6.b)
3. Liften mogen geen open verbinding verzorgen tussen twee zones van verschillend beveiligingsniveau.
4. Op alle etages, waar inkijk vanuit de omgeving mogelijk is, zijn zichtbeperkende maatregelen getroffen.
5. Bij zonering op basis van risicogebieden wordt rekening gehouden met eisen van compartimentering als gevolg van brand.
6. Algemene en technisch kritieke ruimten zijn uitgerust met passende blusmiddelen. (Code 9.1.4.c)
7. In een gebouw zijn vluchtwegen aangegeven.
8. Waar van toepassing zijn er zo min mogelijk aanwijzingen over het gebruiksdoel ten aanzien van de aanwezigheid van informatieverwerkingsactiviteiten. (Code 9.1.3.c)

C.17.2.3. Deuren

Beheersmaatregel
De deuren zijn afgestemd op de zonering en bevorderen de veiligheid van het personeel.

Implementatierichtlijn
1. Toegangsdeuren aan de buitenkant van een gebouw en deuren tot de kritische ruimten zijn voorzien van schootstand detectie.
2. In een vluchtroute opgenomen (buiten)deuren slaan naar buiten toe open.
3. Nooduitgangen zijn uitgevoerd met paniekssluitingen. Hierbij worden additionele detectiemaatregelen toegepast, zodat het onjuist gebruik van deze (vlucht)deuren wordt voorkomen. Men kan daarbij denken aan het gebruik van deurstanddetectie, (brand)vluchtsloten of verbreekglas bij een ruimte, waarna de deur wordt vrijgegeven voor (calamiteiten)gebruik.

C.17.3. Apparatuur en bekabeling

Beheersmaatregel
Apparatuur en bekabeling voldoet aan dezelfde eisen zoals die worden gesteld aan computerruimten.

Implementatierichtlijn
1. Gebouwgebonden apparatuur en bekabeling voldoen aan de normen van:
a. 7.10.2 Plaatsing en bescherming apparatuur;
b. 7.10.3 Nutsvoorzieningen;
c. 7.10 4 Bekabeling.

C.17.4. Gebouwbeheer- en beveiligingsysteem

Beheersmaatregel
Er is een gebouwenbeheer- en beveiligingsysteem geïnstalleerd met automatisch werkende detectie van beveiligingsinbreuken en ontruiming kan ondersteunen.

Implementatierichtlijnen (Code 9.1.1.f)
1. Gebouwen zijn voorzien van een inbraakdetectiesysteem met luid- en stil-alarmfaciliteiten.
2. Op strategische punten in het gebouw zijn bewegingsmelders aangebracht.
3. Indien de brandweer (Code 6.1.6) dit eist, wordt een gecertificeerd brandmeldsysteem toegepast conform de NEN norm 2535.
4. Het brandmeldingsysteem wordt met een 24-uurs doormeldpost verbonden met de meldkamer.
5. Kritische ruimten worden volledig voor brand gedetecteerd alsmede de opslagruimte voor (vernietiging van) vertrouwelijke documenten en keukens.
6. Gebouwen zijn voorzien van een ontruimingsprotocol.

C.17.5. Toegangsvoorzieningen

Beheersmaatregel
De toegangsvoorzieningen verlenen alleen toegang tot ruimten aan daartoe geautoriseerde personen.

Implementatierichtlijn
1. Geautoriseerde toegangsverlening tot zones vindt plaats op basis van need to be there
2. De inrichting van de toegangscontrolevoorziening ondersteunt het voorkomen van ongeautoriseerde toegang van personen.
3. De laad- en losruimte is zo ontworpen dat voorraden kunnen worden afgeleverd zonder dat de leverancier andere delen van het gebouw hoeft te betreden. (Code 9.1.6.b, 9.1.6.c)

C.17.6. Inrichting verbijzonderde ruimten

Beheersmaatregel
Diverse ruimten voldoen aan aparte inrichtingseisen.

Implementatierichtlijnen
1. Voor verbijzonderde ruimten is een inrichtingsprotocol opgesteld.

C.18. Computerruimten

Doelstelling
Computerruimten zijn zodanig ingericht dat computerverwerking niet wordt verstoord door van buiten komende onheilen, brand, explosie, water, storingen in nutsvoorzieningen, gegevenstransport en dergelijke.

Motivering
De inrichting van computerruimten moet voldoen aan hoge eisen van beveiliging samenhangend met het belang van geautomatiseerde gegevensverwerking voor een organisatie.

Afbakening
Computerruimten vormen een speciale categorie ruimten binnen een gebouw. In dit normenkader wordt de inrichting van computerruimten gezien als een aparte verantwoordelijkheid. Omdat deze inrichting niet altijd op alle onderdelen goed is af te bakenen van de algemene inrichting van gebouwen en ruimten is onderlinge afstemming met deze laatste verantwoordelijkheid een absoluut vereiste.

C.18.1. Voorzieningen algemeen

Beheersmaatregel
Computerruimten voldoen aan beveiligingseisen.

Implementatierichtlijn
1. De apparatuur in de technische infrastructuur (m.u.v. clients) is aangesloten op meervoudige voeding, een onderbrekingsvrije noodstroomvoorziening voor gecontroleerde beëindiging van de verwerking en een spanningsstabilisator. Apparatuur in computerruimten met een vitale functie voor de gehele organisatie wordt aangesloten op een noodgenerator.
2. Bij computerruimten met een vitale functie voor de gehele organisatie zijn voorzieningen getroffen tegen de afhankelijkheid van (de ligging van) één datacommunicatiekabel naar de wijkcentrale. Meervoudige kabels komen vanuit verschillende richtingen en hebben verschillende aansluitpunten naar de computerruimte.
3. Op alle uitgaande communicatielijnen zijn bliksembeveiligingsfilters aangebracht.
4. Voor de computerruimte wordt gebruik gemaakt van passende blusmiddelen.
5. IT-voorzieningen die door de organisatie zelf worden beheerd, zijn fysiek gescheiden van systemen die door derden worden beheerd. (Code 9.1.1.g)
6. Reserveapparatuur worden op veilige afstand bewaard, om te voorkomen dat ze beschadigd raken door een calamiteit op de hoofdlocatie. (Code 9.1.4.b)

C.18.2. Plaatsing en bescherming apparatuur

Beheersmaatregel
De plaatsing en bescherming van apparatuur voldoet aan beveiligingseisen.

Implementatierichtlijn
1. Apparatuur wordt zodanig geplaatst dat onnodige toegang tot de werkvloer wordt geminimaliseerd. (Code 9.2.1.a)
2. IT-voorzieningen met gevoelige gegevens worden met een beperkte inkijkhoek geplaatst zodat de kans vermindert dat informatie door onbevoegden tijdens gebruik wordt gezien; de opslagvoorzieningen worden beveiligd tegen onbevoegde toegang. (Code 9.2.1.b)
3. Apparatuur die bijzondere bescherming nodig heeft wordt geïsoleerd, zodat het vereiste algemene beschermingsniveau kan worden verlaagd. (Code 9.2.1.c)
4. Er zijn maatregelen getroffen om het risico van mogelijke gevaren te minimaliseren, zoals diefstal, brand, explosie, rook, wateroverlast (of onderbreking van de watertoevoer), stof, trillingen, chemische reacties, verstoring van de elektriciteitsvoorziening en van de communicatie, elektromagnetische straling en vandalisme. (Code 9.2.1.d)
5. Omgevingsomstandigheden zoals temperatuur en luchtvochtigheid, worden gecontroleerd op omstandigheden die de werking van IT-voorzieningen negatief beïnvloeden. (Code 9.2.1.f)
6. Apparatuur waarmee gevoelige informatie wordt verwerkt is beschermd om het risico van lekken van informatie door uitstraling te minimaliseren. (Code 9.2.1.i)
7. Apparatuur wordt opgesteld en aangesloten conform de voorschriften van de leverancier.
8. Apparatuur die niet in de computerruimte is ondergebracht, is in afsluitbare kasten ondergebracht.

C.18.3. Nutsvoorzieningen

Beheersmaatregel
Apparatuur is beschermd tegen stroomuitval en andere storingen door onderbreking van nutsvoorzieningen.

Implementatierichtlijnen (Code 9.2.2)
1. Apparatuur die kritische bedrijfsactiviteiten ondersteunt, is voorzien van een onderbrekingsvrije stroomvoorziening (Uninterruptable Power Supply, UPS) om een goede afsluitprocedure te ondersteunen of de apparatuur ononderbroken te laten werken.
2. Er is een noodprocedure voor uitval van de UPS, bestaande uit een noodgenerator indien de gegevensverwerking ook tijdens een langdurige stroomuitval moet doorgaan. Er is een toereikende brandstoftoevoer beschikbaar zijn om te waarborgen dat de generator voor een lange tijd kan blijven werken.
3. Er wordt gebruik gemaakt van meer energiebronnen, of indien de locatie groot is, van een afzonderlijke hulpcentrale.
4. Noodschakelaars zijn aangebracht in de buurt van nooduitgangen van computerruimten, om in noodsituaties snel de stroom te kunnen uitschakelen. Er is noodverlichting aangebracht voor het geval zich een totale stroomstoring voordoet.
5. De watervoorziening is stabiel en voldoende voor de airconditioning, bevochtigingsapparatuur en brandbestrijdingssystemen (waar gebruikt).
6. Nutsvoorzieningen zijn aangesloten op een alarmsysteem om storingen in de nutsvoorzieningen te kunnen signaleren.
7. Telecommunicatieapparatuur is op ten minste twee verschillende manieren op de systemen van de telecomleverancier aangesloten om te voorkomen dat een storing in een verbindingsroute de spraakdienst verwijdert. De spraakdiensten voldoen aan de plaatselijke voorschriften voor noodcommunicatie.

C.18.4. Bekabeling

Beheersmaatregel
Voedings- en telecommunicatiekabels zijn tegen interceptie of beschadiging beschermd.

Toelichting
De specifieke kritieke ruimten van Rijksgebouwen moeten voldoen aan het Handboek IT-huisvesting en Bekabeling (HIB) van de Rijksgebouwendienst. Voorts moet de bekabeling worden aangelegd conform het voorschrift “Brandveilig bouwen” (NEN 2535). In deze baseline worden de normen van de Code aangehouden, zodat het overzicht bewaard blijft.

Implementatierichtlijnen
1. Elektriciteits- en telecommunicatiekabels voor IT-voorzieningen worden ondergronds aangelegd of op andere wijze afdoende beschermd. (Code 9.2.3.a)
2. Netwerkkabels zijn fysiek afgeschermd tegen ongeautoriseerd aftappen of beschadiging, bijvoorbeeld door ze in mantelbuizen of kabelgoten te leggen en zo min mogelijk door openbare ruimten te laten lopen. (Code 9.2.3.b)
3. Netsnoeren worden gescheiden gehouden van communicatiekabels, om interferentie te voorkomen. (Code 9.2.3.c)
4. Er worden duidelijk identificeerbare markeringen op kabels en apparatuur gebruikt om fouten bij bewerking te voorkomen. (Code 9.2.3.d)
5. Voor gevoelige of kritische systemen worden verder de volgende maatregelen getroffen: (Code 9.2.3.f)
a. het installeren van gewapende kabelgoten en afgesloten ruimten of dozen voor inspectie- en eindpunten;
b. het gebruik van alternatieve routes en/of transmissiemedia om de juiste mate van beveiliging te leveren;
c. het gebruik van glasvezelkabels;
d. het gebruik van elektromagnetische afscherming om de kabels te beschermen;
e. het gebruik van detectievoorzieningen om ongeautoriseerde apparatuur die op de bekabeling is aangesloten, op te sporen.

Begrippen

Account	Een IT-voorziening waarmee een gebruiker zich identificeert in een doelsysteem.
Apparatuur	Die bedrijfsmiddelen, die ondersteunend zijn voor de fysieke beveiliging en computerverwerking, zoals nutsvoorzieningen, klimaatregelingen, powersupplies.
Appliances	Hardware module, die zelfstandig beveiligingsfuncties kan uitvoeren. De code voor de intelligentie van een appliance is meestal aangebracht in firmware die naar behoefte kan worden aangepast en geactualiseerd.
Audit trail	Vastlegging van de complete keten van opeenvolgende wijzigingen op een object in een bepaalde periode.
Basis beveiligingsniveau	Het geheel van maatregelen van beveiliging dat wordt bereikt door het implementeren en toepassen van de normen zoals geformuleerd in de Code voor Informatiebeveiliging, Business Continuity Management en WBP-classificatie II Verhoogd risico en waaraan de NORA een nadere uitwerking geeft, onder meer door normen voor IT-voorzieningen.
Bedrijfsmiddel	Elk middel waarin of waarmee bedrijfsgegevens kunnen worden opgeslagen en/of verwerkt en waarmee toegang tot gebouwen, ruimten en IT-voorzieningen kan worden verkregen: een bedrijfsproces, een gedefinieerde groep activiteiten, een gebouw, een apparaat, een IT-voorziening of een gedefinieerde groep gegevens.
Beschikbaarheid	De waarborg dat vanuit hun functie geautoriseerde gebruikers op de juiste momenten tijdig toegang hebben tot informatie en aanverwante bedrijfsmiddelen (informatiesystemen).
Beveiliging	Het brede begrip van Informatiebeveiliging, d.w.z. inclusief fysieke beveiliging, Business Continuity Management (BCM) ofwel beschikbaarheid van bedrijfsprocessen en persoonlijke veiligheid en integriteit.
Beveiligingsincident	Het manifest worden van een beveiligingsrisico (dreiging, oorzaak) als gevolg van een overtreding van beveiligingsregel, bijv. onbevoegde toegang tot IT-voorzieningen.
Beveiligingsinstellingen	In IT-voorzieningen kunnen in veel gevallen functionaliteiten, die invloed hebben op beveiliging geactiveerd, gewijzigd of uitgeschakeld worden door het opgeven van parameterwaarden.
Calamiteitenplan	Verzamelbegrip voor alle plannen voor het opvangen en beheersen van calamiteiten tot het terugkeren tot de normale situatie.
Certificaat	Een computerbestand dat fungeert als een digitaal paspoort voor de eigenaar van dat bestand. Een certificaat wordt gebruikt binnen de Public Key Infrastructure. Het wordt uitgereikt en beheerd door een Certificate Authority (CA). Het bevat: de geregistreerde naam van de eigenaar, de publieke sleutel van de eigenaar, de geldigheidsduur van het certificaat, de locatie van de 'Certificate Revocation List' (bij de uitgever van het certificaat), een samenvatting van het certificaat, versleuteld met de privé-sleutel van een vertrouwde partij.
Certificate Authority (CA)	Een vertrouwde derde partij (trusted third party) die digitale certificaten verleent aan andere partijen t.b.v. een PKI.
Check-digit	Toegevoegd controlegetal om op het geheel een berekening te kunnen uitvoeren met een voorspelbaar resultaat, bijvoorbeeld de optelsom van de getallen is deelbaar door elf.
Clustering technologie	Het verdelen van taken over een netwerk van servers.
Compilers	Standaard programmatuur die een computerprogramma in broncode (source) kan omzetten in uitvoerbare machinecode (load of object).
Continuïteitsplan	Een plan dat de organisatie in staat stelt haar bedrijfsactiviteiten te vervolgen bij calamiteiten tot een voorgedefinieerd niveau.
Controleerbaarheid	De mate waarin de werkelijkheid of representaties daarvan toetsbaar zijn, dat wil zeggen te vergelijken met andere “werkelijkheden of representaties daarvan” zodat objectieve oordeelsvorming mogelijk wordt.
CPU	Centrale Processing Unit, rekenmodule, ofwel de processor van computer.
Create/insert/generate	Maak nieuw/voeg in/maak nieuw op basis van bestaande input.

Crisismanagement plan	Plan gericht op het beheersen van de eerste fase van een geëscaleerd incident.
Cryptohardware	Hardware voor het berekenen en opbergen van geheime codes of encryptiesleutels, die zodanig is geconstrueerd dat bij een fysieke of logische inbraak de bewaarde gegevens automatisch worden vernietigd.
Daemon	Een proces In de Unix-omgeving die wacht tot er verzoek komt om een dienst uit te voeren. Hierbij kan de identiteit van de verzoeker (client) onbekend blijven.
Default waarde	Voorgedefinieerde waarde die wordt gebruikt als er geen andere waarde aan het veld wordt toegekend.
Delete/drop/purge	Verwijder.
Denial of Service (dos) attacks	Aanval, die ertoe leidt dat een computersysteem niet in staat is te functioneren. Hiervoor bestaan diverse methoden.
Device	Apparaat.
Doelsysteem	Een identificatie-, authentificatie- en/of autorisatie-voorziening behorend bij één of meerdere IT-voorzieningen. Deze kunnen zowel generiek in de technische infrastructuur als specifiek in een applicatie of programmapakket voorkomen.
Editors	Programma dat teksten kan maken.
Elektronische handtekening	Een elektronische handtekening is een methode voor het bevestigen van de juistheid van digitale informatie door middel van technieken van de asymmetrische cryptografie. De elektronische handtekening bestaat uit twee algoritmen: een om te bevestigen dat de informatie niet door derden veranderd is, de ander om de identiteit te bevestigen van degene die de informatie "ondertekent". De technieken worden toegepast met behulp van een PKI.
End-to-end encryptie	Versleuteling over alle verwerkingslagen heen van eindgebruiker tot eindgebruiker of van applicatie tot applicatie.
Event console	Beeldscherm waarop gebeurtenissen worden afgebeeld die om attentie of afhandeling vragen.
Executierechten	Bevoegdheden om programma's te kunnen uitvoeren.
Filtering	Het gecontroleerd doorlaten van gegevens op het grensvlak tussen zones in een netwerk.
Firewall	Het geheel van software- en eventueel ook hardwarevoorzieningen die voorkomen dat ongewenst verkeer van de ene netwerkzone terechtkomt in een andere, teneinde de veiligheid in de laatstgenoemde te verhogen.
Firmware	In hardware opgenomen software die zorgt voor het functioneren van die hardware.
Functioneel account	Niet-persoonsgebonden toegangsmogelijkheid tot programmatuur.
Generatievalidatie-mechanisme	Software die ervoor zorgt dat sequentiële bestanden altijd volgens het grootvader-vader-zoon principe worden verwerkt om herstelbaarheid van batchverwerkingen te borgen.
Hardening	Overbodige functies in besturingssystemen uitschakelen en/of van het systeem verwijderen en zodanige waarden toekennen aan beveiligingsinstellingen dat een maximale beveiliging ontstaat.
Hardware security module	Hardware voor het opbergen van geheime codes of encryptiesleutels, die zodanig is geconstrueerd dat bij een fysieke of logische inbraak de bewaarde gegevens automatisch worden vernietigd.
Hot of cold standby	Apparatuur, die functies automatisch kan overnemen, onmiddellijk of dynamisch (hot) of nadat ze als zodanig worden ingeschakeld (cold).
IB-functie	Een geheel van automatische informatiebeveiligingsverwerkingen die logisch met elkaar samenhangen.
IT-voorzieningen	Applicaties en technische infrastructuur, of wel het geheel van IT-voorzieningen.
Informatiebeveiliging	Het proces van vaststellen van de vereiste betrouwbaarheid van informatieverwerking in termen van vertrouwelijkheid, beschikbaarheid en integriteit alsmede het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen.
Informatiesysteem	Een samenhangend geheel van gegevensverzamelingen en de daarbij behorende personen, procedures, processen en programmatuur alsmede de voor het informatiesysteem getroffen voorzieningen voor opslag, verwerking

	en communicatie.
Insiderregeling	Besluit van 12 oktober 2006, houdende regels tot uitvoering van diverse bepalingen van hoofdstuk 5.4 van de Wet op het financieel toezicht (Besluit marktmisbruik Wft) ter voorkoming van misbruik van voorkennis bij privébeleggingen.
Integriteit	Het waarborgen van de juistheid, tijdigheid en volledigheid van informatie en de verwerking ervan.
Intrusion Detection and Prevention (IDS)	Logische inspectie van netwerkpakketten naar specifieke communicatiepatronen, die bedoeld zijn voor inbraakpogingen en blokkering van normaal netwerkverkeer. De IDP blokkeert ongewenste pakketten, legt informatie over het gedrag van netwerkverkeer (patronen) vast en alarmeert vervolgens netwerkbeheerders over mogelijke inbraakpogingen.
Juridische logging	Vastlegging van elektronische berichten onmiddellijk na ontvangst voordat enige bewerking met toepassingssoftware aan de orde is .
Klokkenluidersregeling	Regeling waarbij een werknemer al dan niet anoniem illegaal handelen, misstanden of onrecht binnen de organisatie aan de kaak kan stellen
Logging	Vastlegging van systeemhandelingen.
Malware	Illegale software met niet-gewenste functies.
Master key	Hoofdsleutel nodig om andere sleutelparen te kunnen genereren.
Middleware	Middleware omvat de besturingsprogramma's die de informatie-uitwisseling regelt tussen de cliëntsoftware en de software die de bedrijfsgegevens beheert. Vaak gaat het om gedistribueerde systemen en meer platforms.
NIST	National Institute of Standards and Technology, een gezaghebbend Amerikaans onderzoeksinstituut dat ook normen en 'best practices' op het gebied van informatiebeveiliging publiceert, o.a. gericht op alle veelgebruikte platforms.
Non-repudiation	Zie onweerlegbaarheid.
ODBC	Open DataBase Connectivity is een standaard database toegankelijkheidsmethode, om elk programma met een database te kunnen laten spreken, onafhankelijk van het type database.
Onafhankelijk	Onbevooroordeeld, geen belang hebbend bij de uitkomsten van het onderzoek, niet door derden beïnvloed
One Time Password token	Kleine, draagbare hardwarevoorziening die op basis van een algoritme per tijdseenheid of bij gebruik een code of wachtwoord genereert, die door de tijd of door het vorige wachtwoord gesynchroniseerd kan worden met eenzelfde berekening op een server. Hierdoor ontstaat een sterke authenticatie.
Ontwikkelcode	Programma in brontaal.
Onvertrouwd	Geen zekerheid over het beveiligingsniveau of zekerheid over het lager dan vereiste beveiligingsniveau
Onweerlegbaarheid	Het niet kunnen ontkennen, bijvoorbeeld, een bericht te hebben ontvangen dan wel te hebben verstuurd.
Partities , partitionering	Logische partitionering is een techniek die IBM toepast in verschillende servertypes om op een fysieke machine meerdere onafhankelijke servers te implementeren. Dit levert een sterkere scheiding op dan met behulp van logische toegangsbeveiliging.
Patch	Klein onderdeel van software dat de leverancier van software uitgeeft om fouten/updates aan door hem vervaardigde software.
Poort	Een hardwarepoort is de in- en/of uitgang van een computer, waar een randapparaat op kan worden aangesloten. Een netwerkpoort is een nummer dat aan gegevens in het TCP/IP-protocol wordt gehangen, naast het IP-adres. Het poortnummer wordt door het ontvangende systeem gebruikt om te bepalen voor welk programma de gegevens zijn bestemd.
Port scan	Een methode om te achterhalen over welke poorten een verbinding te maken is met een bepaalde computerhost.
Private key	Geheime sleutel, die in combinatie met de openbare sleutel deel uitmaakt van een PKI.
Privileged user	Gebruiker met bevoegdheden op systeemniveau.
Public key infrastructure (PKI)	Een systeem waarmee uitgifte en beheer van sleutels binnen asymmetrische versleuteling. Dit gebeurt doorgaans via digitale certificaten. Een certificaatautoriteit (CA) waarborgt de integriteit en authenticiteit van het certificaat en staat dus in voor de identiteit van de certificaatbezitter. De

	Registratie Autoriteit (RA) is een instelling waar gebruikers aanvragen kunnen indienen voor het verkrijgen van een certificaat.
Query	Bevraging in een vraagtaal, die op basis van gebruikersvriendelijke en krachtige commando's selecties en berekeningen op bestanden kan uitvoeren, in eerste instantie alleen voor raadpleegdoeleinden.
Query Language	Vraagtaal, die op basis van gebruikersvriendelijke en krachtige commando's selecties en berekeningen op bestanden kan uitvoeren.
Querytool	Gereedschap om een query te maken.
Queue	Wachtrij, bijvoorbeeld van printopdrachten.
Raid	Redundant Arrays of Independent Disks, de benaming voor een set methodieken voor fysieke dataopslag op harde schijven waarbij de gegevens over meer schijven verdeeld worden voor snelheidswinst en/of beveiliging tegen gegevensverlies.
Restore	Terugzetten van bestanden, bijv. vanuit een back-up.
Root	De directory in een bestandssysteem waaronder alle andere directory's zich bevinden (in UNIX/Linux terminologie).
Root certificate	Certificaat, waarmee op het hoogste niveau toegang kan worden verkregen.
Router	Een apparaat (dat kan een computer zijn) dat twee of meer verschillende computer(sub)netwerken aan elkaar verbindt.
Rules	Toegangsbeperkende maatregelen opgenomen in programmatuur, meestal afhankelijk van de soort gegevens en relaties daartussen.
Security services	Diensten op het gebied van de informatiebeveiligingsfuncties.
Sessie-encryptie	Vorm van encryptie waarbij de encryptie plaatsvindt per sessie en alle bij die sessie behorende gegevensuitwisselingen.
Single Party Control	Bij sleutelbeheer: handeling door één persoon
Single Party Control-Audited	Bij sleutelbeheer: handeling door één persoon plus controle door een andere persoon
Multi Party Control - Audited	Bij sleutelbeheer: handeling door twee personen plus controle door een derde persoon
Single-point-of-failure	Elke IT-voorziening, waarvan de functie niet door een andere voorziening kan worden overgenomen bij storing of vernietiging.
Single sign on (sso)	Éénmalig aanloggen, waarna bij positieve verificatie toegang tot meer platforms of toepassingen wordt verkregen zonder dat opnieuw authenticatie nodig is.
Spam	Ongewenste elektronische post.
Spyware	Computerprogramma's (of delen daarvan) die informatie vergaren over een computergebruiker en deze doorsturen naar een externe partij.
Stored procedures	Programma dat bewaard wordt binnen een databank. Het voordeel van een opgeslagen procedure is dat deze direct toegang heeft tot de gegevens die ze moet manipuleren en het over en weer sturen van grote hoeveelheden gegevens vermijdt. Tevens beveiligingstechniek.
Systeemaccount	Toegang met bevoegdheden op systeemniveau.
Systeemvreemde omgeving	Elke omgeving die niet volledig kan worden beheerst vanuit het perspectief en de samenhang van het eigen toepassingsgebied.
Technische infrastructuur	Het geheel van IT-voorzieningen voor generiek gebruik, zoals servers, firewalls, netwerkapparatuur, besturingssystemen voor netwerken en servers, database management systemen, beheer- en beveiligingstools, inclusief bijbehorende systeembestanden.
Transactionele integriteit	Een transactie bestaat uit een aantal samenhangende wijzigingen in een database. Transactionele integriteit voldoet aan de eisen: * Atomair: een transactie wordt altijd volledig uitgevoerd. Ook al bestaat een transactie uit meer onderdelen, na afloop van een transactie zijn of alle onderdelen uitgevoerd of geen van de onderdelen. * Consistent: na uitvoering van een transactie is de database consistent, dat wil zeggen dat alle regels die zijn vastgelegd voor de gegevens gelden. * Duurzaam: na de uitvoering van een transactie zijn de gegevens duurzaam vastgelegd. * Geïsoleerd: transacties worden geïsoleerd van elkaar uitgevoerd, dat wil zeggen. dat transacties die tegelijkertijd worden uitgevoerd geen inzicht hebben in elkaars tussenresultaten en elkaar niet beïnvloeden.
Trojan	Een functie die verborgen zit in een programma dat door de gebruiker wordt

	geïnstalleerd en die toegang tot de geïnfecteerde computer kan verschaffen aan kwaadwillenden.
Update/change/alter	Bevoegdheid om te wijzigen.
Vertrouwd	In overeenstemming met een vastgesteld beveiligingsniveau
Vertrouwelijkheid	Het waarborgen dat informatie alleen toegankelijk is voor degenen die hiertoe zijn geautoriseerd.
View	Gedefinieerd geheel van gegevenselementen dat wordt gebruikt om een database te benaderen en/of het resultaat in de termen van conform de view gepresenteerde gegevens.
Worm	Een replicerend computerprogramma, dat via een netwerk kopieën doorstuurt zonder tussenkomst van een gebruiker. Een worm kan bestanden verwijderen, achterdeurtjes van andere programma's openzetten of het netwerk vertragen.
Write once-(read many) technologie	Technologie, waarbij een medium eenmalig beschreven en vervolgens niet meer veranderd kan worden, bijvoorbeeld een CD-R.
Zone	De logische verzameling van IT-voorzieningen met hetzelfde beveiligingsniveau, die via beveiligde koppelvlakken gegevens kunnen uitwisselen.