Beleidslijn informatieveiligheid en privacy

Aankopen, ontwerpen, ontwikkelen en onderhouden van toepassingen

(BLD APPDEV)

INHOUDSOPGAVE

1. INLEIDING 3

2. VEILIGHEIDSVEREISTEN BIJ AANKOPEN, ONTWERPEN, ONTWIKKELEN EN ONDERHOUDEN VAN TOEPASSINGEN 3

2.1. CLASSIFICATIE VAN GEGEVENS 3
2.2. REGLEMENTAIRE VEREISTEN 3
2.2.1. EU GDPR en KSZ wet 3
2.2.2. Machtigingen van het Sectoraal Comité 3
2.2.3. Bewijskracht 4
2.2.4. Uniek dossier 4
2.2.5. Toelatingen KSZ 4
2.3. BELEIDSLIJNEN 4
2.3.1. Communicatie 4
2.3.2. Toegangsbeheer 4
2.3.3. Uitbesteding aan derden 5
2.3.4. Checklist 5
2.3.5. Controle voor in productiestelling 5
2.3.6. Gestructureerde aanpak 5
2.3.7. Logbeheer 5
2.3.8. Back-up/Restore 5
2.3.9. Continuïteitsbeheer 6
2.3.10. Incidentenbeheer 6
2.3.11. Documentatie 6
2.3.12. Inventaris 6
2.3.13. Audit 6

BIJLAGE A: DOCUMENTBEHEER 7

BIJLAGE B: REFERENTIES 7

BIJLAGE C: SECURE PROJECT LIFECYCLE 8

Initiatie 8
Planning 8
Realisatie 8
Afsluiting 10

BIJLAGE D: LINK MET DE ISO-NORM 27002:2013 10

1. Inleiding

Dit document maakt integraal deel uit van de methodologie informatieveiligheid en privacy binnen de sociale zekerheid. Dit document is bestemd voor de verantwoordelijken, voor de verwerkers van informatie, voor de informatieveiligheidsconsulent (CISO), voor de functionaris voor de gegevensbescherming (DPO) van de openbare instelling van de sociale zekerheid (OISZ), voor de projectverantwoordelijken en alle partijen die betrokken zijn bij de ICT projecten.

In het kader van een goede beveiligingsorganisatie is het nodig dat veiligheidsvereisten gedefinieerd worden vanaf de designfase van een project.

Dit document heeft betrekking op de informatieveiligheid- en privacy-aspecten van het aankopen, ontwerpen, het ontwikkelen en het onderhouden in het kader van ICT projecten.

2. Veiligheidsvereisten bij aankopen, ontwerpen, ontwikkelen en onderhouden van toepassingen

Elke organisatie onderschrijft de volgende beleidslijnen van informatieveiligheid en privacy voor alle informatie en informatiesystemen onder de verantwoordelijkheid van de organisatie:

2.1. Classificatie van gegevens

In elke fase van een project zal bijzondere aandacht besteed worden aan de informatieveiligheid- en privacy-maatregelen met betrekking tot de verwerking van gegevens, in overeenstemming met hun classificatie.

Vanaf het opstarten van elk project is het noodzakelijk een risico analyse uit te voeren in functie van de classificatie van de gegevens. Hierbij zal de nodige aandacht geschonken worden aan de veiligheids- en privacy-risico's[1]. Bijzondere aandacht moet besteed worden aan de bescherming van de cryptografische basisgegevens (sleutels, certificaten,…) die nooit in een onbeveiligde vorm in een systeem opgeslagen mogen worden (ISP).

Maatregelen worden genomen om te voorkomen dat informatie die wordt uitgewisseld met andere organisaties verloren gaat, gewijzigd of misbruikt wordt.

2.2. Reglementaire vereisten

2.2.1. EU GDPR en KSZ wet

Er moet over gewaakt worden dat de wettelijke en veiligheidsvereisten waaraan de gebruikte informatiesystemen onderworpen zijn, nageleefd worden.

2.2.2. Machtigingen van het Sectoraal Comité

Een machtiging van het bevoegd Sectoraal Comité is vereist om aan een organisatie toe te laten persoonsgegevens uit te baten indien de organisatie niet de eigenaar van deze gegevens is.

[1] De risico-beoordeling zal bijvoorbeeld de nood aan cryptografische methodes bepalen voor de vrijwaring van de vertrouwelijkheid, de authenticiteit en de integriteit van de gegevens. Deze technieken kunnen ook bijdragen aan de niet-weerlegbaarheid van de transacties.

2.2.3. Bewijskracht

Wanneer de bewijskracht vereist is moet een dossier voorgelegd worden aan de bevoegde instanties. De context van de bewijskracht is gedefinieerd in Koninklijke Besluiten[2].

2.2.4. Uniek dossier

Binnen de sociale zekerheid is er een proces ingesteld om de wettelijke aspecten, de veiligheids- en privacy-aspecten te controleren bij de ingebruikname (in productiestelling) van een toepassing. Deze validatie wordt geformaliseerd in een 'Uniek Dossier (wettelijke aspecten bij het in productie brengen van een nieuwe toepassing)'. Dit dossier is verplicht voor toepassingen die gehost zijn op het portaal van de sociale zekerheid en het eHealth platform. Dit dossier centraliseert de noodzakelijke informatie om de systeembeheerders van de sociale zekerheid toe te laten om een toepassing in productie te stellen in overeenstemming met de regelgeving in verband met de informatieveiligheid en privacy van gegevens.

2.2.5. Toelatingen KSZ

Indien elektronische diensten (zoals web services) gebruikt worden van de KSZ, dan moet hiervoor tijdig de toelating gevraagd worden.

2.3. Beleidslijnen

De volgende punten worden opgelegd door de beleidslijnen informatieveiligheid en privacy zoals vastgelegd door het Sectoraal Comité van de Sociale Zekerheid en de Gezondheid. Indien er een specifieke beleidslijn is die aansluit bij het onderwerp dient deze gerespecteerd en toegepast te worden.

2.3.1. Communicatie

Een efficiënte en constructieve communicatie tussen de verschillende bij het project betrokken partijen (inclusief klanten en leveranciers) moet opgezet worden, in het bijzonder met de veiligheidsconsulent(en). Dit moet een adequaat niveau van informatieveiligheid en privacy garanderen gekend door iedereen.

De betrokkenen worden eveneens gewezen op hun persoonlijke verantwoordelijkheden zoals beschreven in de "Gedragscode voor de informatiebeheerders" of in een deontologische code inherent aan hun specifieke functie:

- de beperking van inzage van vertrouwelijke gegevens voor louter beroepsdoeleinden
- de geheimhouding van vertrouwelijke gegevens.

2.3.2. Toegangsbeheer

Alle medewerkers en in het bijzonder externe medewerkers (zoals consultants, contractors, interims, stagiairs, jobstudenten) die werken met ICT middelen die door de instelling ter beschikking worden gesteld, doen dit op basis van minimale autorisatie voor de uitvoering van hun taak.

Bij het ontwikkelen van de toegangsbeveiliging is het belangrijk rekening te houden met de reeds bestaande operationele systemen voor het toegangsbeheer (zoals UAM) en hun evolutie. Het gebruik van deze systemen garandeert de onafhankelijkheid tussen dit beheerssysteem en het ontwikkelde systeem.

Vereisten voor toegangsbeveiliging (identificatie, authenticatie, autorisatie) worden gedefinieerd, gedocumenteerd, gevalideerd en gecommuniceerd. Deze toegangsbeveiliging (zoals de aard van authenticatiemiddel) zal verschillen naargelang de toepassing (vb. graad van vertrouwelijkheid van behandelde gegevens) en van de bedreiging (vb. toegang via publieke netwerken) op basis van een risico analyse. Deze toegangen zullen gelogd worden.

[2] https://www.ksz-bcss.fgov.be/nl/bewijskracht-een-nieuwe-aanpak-voor-de-controle-van-de-dossiers-met-het-oog-op-het-verkrijgen-van

Er moet rekening gehouden worden met de granulariteit (fijnkorreligheid) van de toegang tot de gegevens. In het kader van een toepassing moeten verschillende gebruikersgroepen verschillende rechten (vb. lezen, schrijven, wijzigen) kunnen hebben met betrekking tot gegevens met verschillende vertrouwelijkheidsgraad.

Het beheer van de toegangen, intern in een applicatie, moet zo veel mogelijk vermeden worden. In uitzonderlijk voorkomend geval moeten formele procedures bestaan om alle fases in de levenscyclus van de toegangsbeveiliging te beheren (invoer, controle op basis van een inventaris, mutatie, schrapping) (ISP).

Wanneer een programma ontwikkeld wordt waarin de sociale zekerheidsinstelling een programmanummer overneemt in een bericht dat ze aan de KSZ richt, maar een natuurlijk persoon aan de basis van dit bericht ligt, moet deze organisatie in staat zijn zelf de relatie te leggen tussen dit programmanummer en de identiteit van de natuurlijke persoon die het bericht verstuurt.

2.3.3. Uitbesteding aan derden

Bij uitbesteding van ICT activiteiten wordt extra aandacht besteed aan veiligheids- en privacy-risico's. Het is belangrijk deze aspecten contractueel vastgelegd zijn. Vertrouwelijkheids- en continuïteitsclausules moeten voorzien worden.

2.3.4. Checklist

De projectleider dient altijd een controlelijst te voorzien. Op deze basis kan hij zich vergewissen dat het geheel van de beleidslijnen informatieveiligheid en privacy correct geëvalueerd en indien noodzakelijk geïmplementeerd worden tijdens de ontwikkelingsfase van het project.

2.3.5. Controle voor in productiestelling

Bij de in productiestelling van het project, moet de verantwoordelijke van de opvolging, project leider, zich vergewissen dat de veiligheids- en privacy-vereisten die bij het begin van het project werden vastgelegd ook daadwerkelijk geïmplementeerd werden.

2.3.6. Gestructureerde aanpak

Voorzieningen voor ontwikkeling, test en/of acceptatie en productie worden gescheiden – inclusief de bijhorende scheiding der verantwoordelijkheden in het kader van het project. Dit alles gebeurt onder de supervisie van de projectleider.

2.3.7. Logbeheer

In de specificaties van een project dient opgenomen te worden hoe de toegang tot en het gebruik van systemen en applicaties gelogd moet worden om bij te dragen tot de detectie van afwijkingen van de beleidslijnen informatieveiligheid en privacy. De logs dienen geconcipieerd te worden conform de beleidslijn logging.

Er moet rekening gehouden worden met reeds bestaande logbeheersystemen bij de evaluatie van logbehoeften in het kader van het project. Dit om te vermijden dat er per project een specifiek logbeheersysteem ontwikkeld wordt. Zo wordt ook de onafhankelijkheid tussen het logbeheersysteem en het project gegarandeerd.

2.3.8. Back-up/Restore

De projectleider moet er zich van vergewissen dat het project geïntegreerd kan worden in het back-up beheersysteem van de organisatie zoals opgelegd in de beleidslijnen. Dit omvat niet alleen de gegevens die verwerkt worden maar ook de documentatie die hierop betrekking heeft (broncode, programma's, technische documenten, …). De back-up dient regelmatig getest te worden via een herstel ("restore") oefening om na te gaan of de informatie überhaupt wel recupereerbaar is en hoelang dergelijke herstel opdracht duurt.

2.3.9. Continuïteitsbeheer

In de loop van de ontwikkeling van het project moeten de behoeften met betrekking tot continuïteit van de dienstverlening geformaliseerd worden, conform met de verwachtingen van de organisatie.

De volgende punten moeten nageleefd worden :

- In de programma's moeten de te definiëren herstartpunten duidelijk geïntegreerd worden om het hoofd te bieden aan operationele problemen. Deze informatie maakt deel uit van het exploitatie dossier.
- Tijdens de ontwikkeling van een project moet bijzondere aandacht besteed worden aan back-up en herstel ("restore") van informatie
- In de productie omgeving moet rekening gehouden worden met de eisen van de instelling met betrekking tot probleemtolerantie en redundantie van de infrastructuur
- Het continuïteitsplan en de bijhorende procedures moeten geactualiseerd worden in functie van de projectevolutie, met inbegrip van continuïteitstesten

In functie van de risico analyse die in het begin van het project werd uitgevoerd moeten noodprocedures gedefinieerd worden. Deze bevatten onder andere :

- De werking bij verminderde beschikbaarheid van informatie systemen
- De beschrijving van alternatieve informatie systemen met inbegrip van de uitrol, de exploitatie modaliteiten en de eventuele ontwikkeling van noodsystemen
- De kerntaken en kernprocedures in geval van systeemonderbreking
- De taken, de sleutelrollen en de in te zetten middelen om tot een optimale beschikbaarheid te komen.

2.3.10. Incidentenbeheer

In de loop van de ontwikkeling van het project moeten de procedures met betrekking tot het incidentbeheer geformaliseerd en gevalideerd worden. Dit moet toelaten het ontwikkelde systeem te integreren in het standaard incident beheerssysteem van de organisatie. De veiligheidsconsulent moet op de hoogte gesteld worden van de veiligheids- en privacy-incidenten.

2.3.11. Documentatie

Tijdens de levensloop van het project moet de documentatie (technisch, procedures, handleidingen, …) actueel gehouden worden.

2.3.12. Inventaris

Alle middelen inclusief aangekochte of ontwikkelde systemen zullen toegevoegd worden aan het beheerssysteem van de operationele middelen.

2.3.13. Audit

Voor interne en externe audit zal de gepaste medewerking verleend worden onder de vorm van het ter beschikking stellen van personeel, documentatie, logbeheer en andere informatie die redelijkerwijze beschikbaar is.

Bijlage A: Documentbeheer

Versiebeheer

Datum	Auteur	Versie	Beschrijving van de verandering	Datum goedkeuring	Datum in werking treden
2007	JC	V2007	Eerste versie	10/10/2007	01/11/2007
2011	PB	V2011	Tweede versie	29/03/2011	01/04/2011
2017	M. Vael	V2017	Integratie EU GDPR	07/03/2017	07/03/2017
2018	Policy werkgroep	V2018	Aanpassing naar aanleiding verandering in BLD LOG	06/02/2018	01/01/2019

Fouten en weglatingen

Wanneer bij het lezen van dit document fouten of problemen worden vastgesteld, dan wordt u als lezer verzocht om een korte beschrijving van de fout of het probleem en de locatie in het document samen uw contactinformatie door te geven aan de informatieveiligheidsconsulent (CISO) / functionaris van gegevensbescherming (DPO) van de organisatie.

Definities

Om consistentie te garanderen in gebruikte terminologie en begrippen doorheen alle beleidsdocumenten, worden alle definities met betrekking tot informatieveiligheid en privacy gecentraliseerd in één document genaamd “Definities informatieveiligheid en privacy”.

Bijlage B: Referenties

Hieronder staan documenten vermeld die hebben gediend als inspiratie voor dit document:

- ISO, “ISO/IEC 27001:2013 Information Security Management System Requirements”, september 2013, 23 blz.
- ISO, “ISO/IEC 27002:2013 Code of Practice for Information Security Management”, september 2013, 80 blz.
- ISO, “ISO/IEC 27034:2011 Security Techniques – Application Security”, November 2011, 67 blz.
- ISACA, “COBIT 5 for Information Security”, Mei 2012, 220 blz.

Hieronder staan referenties naar websites die hebben gediend als inspiratie voor dit document:

- https://www.iso.org/isoiec-27001-information-security.html
- http://www.iso.org/iso/catalogue_detail?csnumber=54534
- http://www.iso.org/iso/catalogue_detail?csnumber=54533
- https://www.iso.org/standard/44378.html
- http://www.isaca.org/cobit
- https://www.owasp.org
- http://www.webappsec.org/
- http://www.ccb.belgium.be/nl/work
- http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf
- https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design

Bijlage C: Secure project lifecycle

Initiatie

Zoals alle projectvereisten zullen ook de veiligheids- en privacy-vereisten met de opdrachtgever besproken en vastgelegd worden vanaf het begin van het project. De veiligheidsconsulent(en) en de DPO van de opdrachtgever(s) en de betrokken organisatie(s) moet(en) hierin betrokken worden.

Planning

In de planning van het project moet rekening gehouden worden met de nodige tijd en middelen om ook de veiligheids- en privacy-aspecten te verwezenlijken.

Het omzeilen van de veiligheids- en privacy-richtlijnen, om andere project-aspecten (bijvoorbeeld uit tijdsnood of budgetproblemen) te bevoordeligen, moet vermeden worden en moet geargumenteerd en formeel bevestigd worden op basis van een risico analyse. Alle afwijkingen moeten gevolgd worden door verbeteringsmaatregelen om de oorspronkelijke veiligheids- en privacy-doelstellingen te behalen.

Realisatie

- ***Ontwikkeling en test***

Bij de ontwikkeling en test dient rekening gehouden te worden met zwakke punten die kunnen uitgebaat worden om applicaties te compromitteren.

Een opleidingsprogramma, aangepast aan de verschillende verantwoordelijkheden, moet bestaan om de risico's in verband met toepassingen te verduidelijken en de tegenmaatregelen toe te lichten.

Het is dan ook van het grootste belang te verifiëren dat medewerkers de nodige opleiding krijgen om zich bewust te zijn van de bedreigingen voor en het belang van informatieveiligheid en privacy, en om de juiste middelen, kennis en vaardigheden tot hun beschikking te hebben om de systemen hiertegen te wapenen.

De toewijzing van speciale, kritieke rollen/rechten tijdens de ontwikkelingsfase (vb. voor het beheer van softwareversies) worden beperkt en het gebruik ervan gecontroleerd.

- Authenticatiemethodes (zoals wachtwoorden/wachtzinnen) en autorisatie-niveaus (zoals administrator) worden beheerd aan de hand van een formeel proces.
- Medewerkers worden gewezen op hun verantwoordelijkheid voor het handhaven van een effectieve toegangsbeveiliging.

Bij de ontwikkeling van systemen dient bijzondere aandacht besteed te worden aan de integriteit van de gegevens, bijvoorbeeld door de validatie van invoergegevens, de beveiliging van interne verwerking en de validatie van uitvoergegevens. Audit trails dienen ingebouwd te worden.

Bij de ontwikkeling van systemen wordt rekening gehouden met gekende zwakke punten op gebied van veiligheid (en privacy) eigen aan programmeertalen. Het nazicht van software door andere partijen dan de ontwikkelaars is een methode om deze risico's in te perken. Indien dit gebeurt door een externe partij dient de deontologie van deze partij nagegaan te worden.

Tijdens de ontwikkeling wordt de integriteit en consistentie van software gewaarborgd door een op procedures gebaseerd beheer van de softwareversies en de toegangsbeveiliging voor softwarebibliotheken.

Maximale maatregelen worden genomen om te vermijden dat geheime communicatiekanalen ("covert channels")[3] en Trojaanse Paarden[4] in ontwikkelde software verborgen worden.

[3] Deze geheime communicatiekanalen laten toe dat deze software achteraf, via deze kanalen, kan gebruikt worden voor oneigenlijke doeleinden.

Met het oog op het continuïteitsbeheer, worden de programma's opgebouwd met duidelijk afgebakende herstartpunten in het geval van operationele problemen.

Toegang tot en gebruik van systemen wordt gemonitord om afwijkingen van het toegangsbeleid of anomalieën te detecteren.

De uitwerking van documentatie bij de ontwikkeling van nieuwe en het onderhoud van bestaande systemen wordt formeel opgelegd om kostbare tijd te winnen voor de opvolgers van de initiële ontwikkelaars.

De uitwerking door de projectleider van een functionele en technische cartografie. Elk van deze cartografieën beschrijft tot op het gepaste niveau de verschillende gegevensstromen, de verschillende relevante elementen (servers, …) en hun rol in het project (applicatie-servers, databank,, ..),

Er dient zorgvuldig omgegaan te worden met test-gegevens om compromittering van professionele, vertrouwelijke en gevoelige gegevens te vermijden. Voor ontwikkelingsdoeleinden mag alleen toegang gegeven worden tot daartoe bestemde testgegevens. Er moet een expliciete goedkeuring verleend worden telkens de productiedata gekopieerd worden naar andere (test)omgevingen. Ofwel wordt hierbij anonimisering toegepast op de productiedata, ofwel erft de andere (test)omgeving dezelfde informatieveiligheids- en privacy vereisten van de productie-omgeving. Informatie uit de andere (test)omgevingen moet direct verwijderd worden zodra het testen voltooid is. Er moet een centraal overzicht zijn van alle informatiestromen tussen productie-, trainings-, pre-productie-, referentie-, integratie-, acceptatie-, test- en ontwikkelingsomgevingen. In het overzicht moet terug te vinden zijn welke data zich in elke omgeving bevindt en welke data op welke manier beschermd is. Procedures voor veilige data-overdracht tussen de productie-omgeving en andere omgevingen moeten opgesteld, gevalideerd, gecommuniceerd en toegepast worden.

- ***In productiestelling***

In dit stadium, zouden volgende aspecten met de personen verantwoordelijk voor in productiestelling en exploitatie moeten behandeld, geanalyseerd en gevalideerd zijn, in overeenstemming met de vereisten van de gebruikers.

- Het aanduiden van een medewerker met de rol van "Applicatie eigenaar" die verantwoordelijk is voor het ontwikkelde systeem (evolutie, documentatie, aanspreekpunt, …).
- De levering door de projectleider van een definitieve versie van de functionele en technische cartografie (as built). Deze documenten laten de systeembeheerders (netwerkbeheerders, databank beheerder, …) toe hun eigen cartografie actueel te houden.
- Overeenstemming van het project en de bijhorende gegevensstromen met de machtigingen afgeleverd door het Sectoraal Comité.
- Overeenstemming van het project met de continuïteitseisen zoals gespecifieerd
- Beschikbaarheid van documentatie en handboeken (o.a. het productiedossier).
- Definitie van te archiveren gegevens, het opslagmedium, de bewaartermijnen, eventuele encryptie
- Het respecteren van de veiligheids- en privacy-vereisten in productie (confidentialiteit, integriteit, beschikbaarheid, bewijskracht)
    - Vereisten voor confidentialiteit:
        - Identificatie
        - Sterke authenticatie
        - Autorisatie
        - Encryptie
        - Toegangscontrole
        - Loggen en monitoring van toegang
    - Vereisten voor integriteit (authenticiteit):
        - Verwerking van data in applicaties

[4] Trojaanse Paarden is de algemene term die gebruikt wordt voor een ongeoorloofde deelsoftware die de geoorloofde software (waarin deze deelsoftware verborgen wordt) andere functies laat uitoefenen dan deze waarvoor deze geoorloofde software oorspronkelijk bedoeld is.

- Integriteitscontroles
- Loggen en monitoring van activiteiten

- Vereisten voor beschikbaarheid:
  - Systeemredundantie
  - Back-up en herstel ("restore") plannen

- De middelen om bepaalde archivering uit te voeren dienen voorbereid te worden. Bijzondere aandacht dient gewijd aan de definitie welke gegevens moeten gearchiveerd worden, het opslagmedium, de bewaartermijnen, eventuele encryptie …
  Opmerking : met het oog op de naleving van de wettelijke bepalingen op de bewaring en het gebruik van gearchiveerde gegevens, moet bij elke evolutie van de informatica infrastructuur en het informatiesysteem die een weerslag kan hebben op de archivering, nagegaan worden of de gearchiveerde gegevens, de opslagmedia en de noodzakelijke applicaties nodig voor hun exploitatie, op elkaar afgestemd blijven.
- Daarenboven moeten, in voorkomend geval, de methodes zoals beschreven in het bewijskracht dossier strikt en blijvend gerespecteerd worden.
- Voor de goedkeuring tot het in productie stellen van een toepassing op het portaal van de Sociale Zekerheid dient een specifieke procedure van de KSZ gevolgd te worden (uniek dossier).
- De nodige middelen en competenties moeten ter beschikking staan om dringend in te grijpen in geval van moeilijkheden in de productiefase.

Afsluiting

De projectverantwoordelijke, de verantwoordelijke voor de behandeling van de gegevens en de verantwoordelijke voor de gegevensverwerking moeten er samen over waken dat het opgeleverde systeem in overeenkomst is met de toegekende machtiging (o.a. de te openen fluxen).

Bijlage D: Link met de ISO-norm 27002:2013

Hier wijzen we op de voornaamste clausule(s) van de ISO-norm 27002:2013 die verband houden met het onderwerp van het huidige document.

ISO-norm 27002:2013	
Veiligheidsbeleid	
Organisatie van de informatieveiligheid.	
Veilig personeel	
Beheer van bedrijfsmiddelen	
Toegangsbeveiliging	
Cryptografie	**Ja**
Fysieke beveiliging en beveiliging van de omgeving	
Beveiliging processen	
Communicatieveiligheid	
Aankopen, onderhouden en ontwikkelen van informatiesystemen	**Ja**
Leveranciersrelaties	
Beheer van veiligheidsincidenten	
Informatieveiligheidsaspecten van continuïteitsbeheer	
Naleving	

***** EINDE VAN DIT DOCUMENT *****