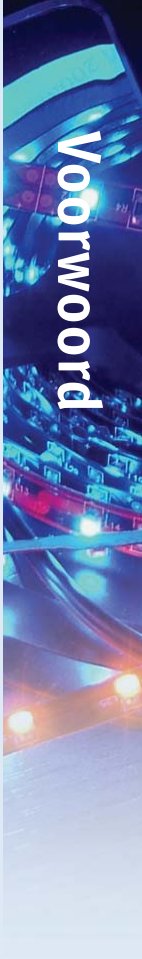
Functies in de informatiebeveiliging

Inhoudsopgave



Voorwoord

Er is veel onduidelijkheid over functies in de informatiebeveiliging (in het navolgende als IB-functies aangeduid). Er wordt een grote verscheidenheid aan functiebenamingen en titels aangetroffen in de internationale literatuur, in regelgeving en in de praktijk bij organisaties. Daarbij kan vaak de vraag worden gesteld in hoeverre het om dezelfde soort functies gaat. Wanneer betreft het een technische functie en wanneer een functie waar meer nadruk wordt gelegd op organisatorische en managementaspecten? En als functies dan naar aard en niveau verschillen, hoe hangen ze dan samen? Ook is het van belang te weten hoe ze zich verhouden ten opzichte van verwante functies op het gebied van beveiligings-, risico- en continuïteitsbeheer. Andere vragen betreffen de eisen die er aan functies kunnen worden gesteld en hoe een carrièrepad in de informatiebeveiliging eruit zou kunnen zien.

Al deze vragen zijn de aanleiding geweest om ordening en profilering aan te brengen. Ook al omdat er steeds meer soorten opleidingen, zowel in het regulier onderwijs, als bij commerciële instellingen ontstaan die beogen professionals op het gebied van informatiebeveiliging af te leveren of bij te scholen. Daarbij hoort dan weer de vraag: welke soort opleiding is passend voor welke functie?

Organisaties en onderwijsinstellingen willen duidelijkheid en dat geldt evenzeer voor professionals die in dit vakgebied opereren. Daarom heeft een werkgroep bestaande uit leden van het Genootschap van Informatiebeveiligers (GvIB) en het Platform Informatiebeveiliging (PI) zich ten doel gesteld om deze functieprofilering uit te werken in een visiedocument. Begin 2005 is er een Expertbrief aan deze problematiek gewijd, waarna een evaluatie van functiebeschrijvingen uit de praktijk heeft plaatsgevonden in een Security Café. Dit visiedocument is het vervolgproduct daarvan. Het concept van deze visie is aan bestuur en leden van GvIB en PI voorgelegd, evenals aan vertegenwoordigers van verwante beroepsgroepen, opleidingsinstituten en andere belanghebbenden. Uit de vele reacties zijn discussiepunten geformuleerd en in een workshop met werkgroepleden en vakgenoten besproken. Op basis daarvan is deze definitieve versie opgesteld. Het resultaat is een door vakgenoten gedragen document geworden, dat als handreiking door organisaties en opleidingsinstellingen kan worden gebruikt. Dit visiedocument richt zich niet alleen op vakgenoten en verwante functies, maar ook op het management en de Human Resource Management (HRM)-functies die verantwoordelijk zijn voor de inrichting, werving en selectie van IB-functies.

De leden van de werkgroep die dit visiedocument hebben samengesteld, zijn:

Bart Bokhorst RE RA, Belastingdienst
Drs. Fred van Noord, Verdonck, Klooster & Associates
Drs. Gerda van den Brink-Heikamp RE, 3A - Audit en Advies op Afstand
Drs. Leo van Koppen, Academie voor ICT Zoetermeer
Ing. Renato Kuiper, LogicaCMG
Ing. Sebastiaan de Looper, Ernst & Young
Dr. ir. Paul Overbeek RE, KPMG
Lex Pels, Capgemini
Ir. Jeroen de Waal van Zuidema Personeelsmanagement heeft de werkgroep als adviseur voor functieprofilering ter zijde gestaan.

Leeswijzer

Allereerst wordt de historische ontwikkeling geschetst, waarbij de groeifasen van informatiebeveiliging aan de orde komen. In de hoofdstukken 2 en 3 worden algemene begrippen en uitgangspunten gedefinieerd die bepalend zijn voor de context waarin de IB-functies opereren en de wijze waarop tegen deze functies wordt aangekeken. In hoofdstuk 4 wordt ingegaan op de managementverantwoordelijkheden voor informatiebeveiliging aan de hand van de Code voor Informatiebeveiliging. Vervolgens geeft hoofdstuk 5 een toelichting op de onderkende IB-functies, hun positionering in grote en kleinere organisaties en hun relatie tot verwante functies. Daarbij wordt ook ingegaan op de betekenis van teamvorming voor de IB-functies. In hoofdstuk 6 worden de resultaatgebieden afgeleid uit de Plan-Do-Check-Act methodologie en worden de functieprofielen uitgewerkt. Hoofdstuk 7 gaat kort in op groeipaden en legt de link naar de opleidingen.

Uitsluitend ter wille van de leesbaarheid zijn de IB-functies in de mannelijke vorm geschreven. Vrouwelijke collegae mogen zich uiteraard eveneens aangesproken voelen.

Managementsamenvatting

Het vakgebied informatiebeveiliging heeft de afgelopen decennia een grote vlucht genomen. Dat hangt nauw samen met het voortdurend toenemende belang van geautomatiseerde gegevensverwerking en de daarmee gepaard gaande risico's voor een integere, vertrouwelijke en ongestoorde informatievoorziening. Die risico's hebben een extra dimensie gekregen door de explosieve en de mondiale groei van elektronische gegevensuitwisseling tussen mensen en organisaties. Voor veel organisaties is ICT een fors deel van het primaire proces geworden. Het beheersen van informatiebeveiligingsrisico's heeft onder meer geleid tot een scala aan specialismen binnen het vakgebied. Door de breedte van het vakgebied en de raakvlakken met vele andere vakgebieden zoals IT-audit, risicomanagement, beveiliging en continuïteitshandhaving is er een grote diversiteit ontstaan bij de invulling van functies en functiebenamingen. De hierdoor gegroeide begripsverwarring en de overlappingen van functiegebieden doen afbreuk aan de professionaliteit waarmee invulling aan de informatiebeveiliging moet worden gegeven. Deze professionele invulling is niet alleen van betekenis om risico's te beheersen, maar biedt juist ook kansen om nieuwe mogelijkheden voor elektronische dienstverlening te benutten met behulp van de expertise van informatiebeveiligingsfuncties.

De in dit document uitgewerkte functieprofilering is bedoeld om professionals in de informatiebeveiliging evenals het management van de organisaties waarin zij werken, te ondersteunen bij het bereiken van een volgende fase in de volwassenwording van het vakgebied.

Bij het onderscheiden van functies in de informatiebeveiliging staat een aantal criteria centraal:

- Business versus ICT
- Strategisch, tactisch en operationeel
- Generalist versus specialist

Op basis hiervan zijn zes hoofdfuncties benoemd, die in samenhang een evenwichtige verdeling van taken in een organisatie geven. Omdat organisaties verschillen in omvang, complexiteit en het belang dat aan informatiebeveiliging wordt gehecht, is in dit visiedocument veel aandacht besteed aan positioneringsmogelijkheden van functies in organisaties en aan samenhang met andere functies in aanpalende vakgebieden.

Voor het succesvol implementeren van informatiebeveiliging in een organisatie is de verdeling van verantwoordelijkheden en bevoegdheden voor het beslissen, adviseren en controleren van en over informatiebeveiligingsmaatregelen een basisvoorwaarde. Er is dan ook een brede benaderingswijze gekozen om functies in kaart te brengen die hierin een rol spelen. Alleen op die wijze is het mogelijk voldoende helderheid te krijgen over de afbakening van die functies, waarvoor uiteindelijk een profiel in termen van resultaatgebieden en competenties is opgesteld. Hierdoor wordt het ook mogelijk op allerlei verschillende manieren de vertaalslag naar de eigen organisatie en naar opleidingsbehoeften te maken.

Tenslotte worden in het document groeipaden aangegeven voor de onderkende functies.

Van bijrol naar hoofdrol

Informatiebeveiliging heeft zich voor veel organisaties in de afgelopen decennia ontwikkeld van een 'nice to have' tot een 'must have'. In de jaren zestig ontwikkelde het vakgebied zich eerst langs de lijnen van de schoksgewijze ontwikkeling van ICT. Sinds ICT volledig in bedrijfsprocessen is geïntegreerd, volgt informatiebeveiliging juist de ontwikkeling daarin en is het daarmee ook meer gericht op de externe betekenis van die bedrijfsprocessen. Hieronder wordt die ontwikkeling kort geschetst.

IT-beveiliging

In het begin van de jaren zestig en zeventig was ICT puur ondersteunend aan de primaire processen. Vrijwel alle beheersingsmaatregelen lagen nog 'gewoon' in de bedrijfsprocessen. De activiteiten op het gebied van informatiebeveiliging waren uitbesteed aan het 'hoofd rekencentrum'. Fysieke beveiliging was van belang, procedures rond input en output en opdrachten aan het rekencentrum, maar in het centrum van de aandacht stond de technische beveiliging. Deze was voornamelijk gericht op logische toegangsbeveiliging en back-up.

Informatiebeveiliging

De link tussen techniek en de rest van de organisatie werd steeds duidelijker. Vooral de samenwerking met de andere ondersteunende functies werd als noodzakelijk gezien. Deze kaders zijn bekend als de PIOFAH-functies voor Personeel, Informatisering, Organisatie, Financiën, Administratie en Huisvesting. Het aandachtsgebied 'informatiebeveiliging' wordt veelal nog wel getrokken vanuit de IT met de Chief Information Officer (CIO) in de hoofdrol, maar er zijn 'contactpersonen' per kader, met de verantwoordelijkheid om informatiebeveiliging binnen het kader te implementeren. Het verband met de primaire processen was nog uiterst dun. Alleen op het gebied van het beheer van autorisaties was het verband wel duidelijk. Informatiebeveiliging was maatregelgericht en had veelal weinig van doen met de daadwerkelijke risico's.

Risicomanagement - servicegericht

Het begrip service provider (dienstverlener) doet zijn intrede. In het verlengde van de geschiedenis is het eerste dat aandacht krijgt het risico vanuit het perspectief van de geboden service. De risico's die inherent zijn aan een service en aan de aanbieder van de service worden geanalyseerd. De afnemer van een service, de 'gebruiker', is nog niet in beeld, net als de risico's die in het gebruik van de afnemer relevant zijn. Aangezien het object een IT-service is, neemt IT in deze vorm van risicoanalyse veelal de 'lead'. In deze fase wordt het procesdenken steeds belangrijker.

Risicomanagement - organisatie- of klantgericht?

Dan wordt het gat naar de primaire processen gedicht. In het risicomanagement worden de risico's ten aanzien van de primaire processen centraal gesteld. Het verbreedt en dekt de gehele organisatie. Men spreekt van enterprise risk management. De ophanging in de organisatie schuift op naar boven. Veelal is de Chief Financial Officer (CFO) of Chief Executive Officer (CEO) portefeuillehouder voor risicomanagement.

Compliancemanagement

Organisaties zijn steeds minder stabiele, geïsoleerde eilanden. Processen ontwikkelen zich over vele bedrijven heen in ketens, die in meer of mindere mate met elkaar verweven zijn. De noodzaak inzicht te hebben in die afhankelijkheden en de daarmee gepaard gaande risico's, wordt steeds duidelijker. Met de toenemende internationalisatie wordt het daarbij steeds belangrijker ook binnen organisaties zicht te houden op wat er in alle uithoeken van het bedrijf wordt gedaan of juist wordt nagelaten. Dat kan alleen als verantwoordelijkheden laag genoeg belegd zijn en de rapportages hoog genoeg in de organisatie terechtkomen. Een andere drijfveer is de toenemende invloed van belanghebbenden als aandeelhouders en andere financiers, commissarissen en toezichthouders. Al deze ontwikkelingen leiden tot afspraken in de vorm van externe wet- en regelgeving, alsook intern beleid of regels, waarover verantwoording moet worden afgelegd. De verantwoordelijkheid voor het voldoen aan de afspraken wordt primair belegd binnen de bedrijfsprocessen bij de verantwoordelijke managers. Deze managers leggen vervolgens verantwoording af en verklaren te voldoen aan de afspraken. Op basis van een consolidatie en verrijking van deze verklaringen kan ook extern verantwoording worden afgelegd. Het compliancemanagement laat niet alleen zien in hoeverre men 'in control' is ten aanzien van de afspraken en regels, maar ook of deze beheersing aantoonbaar is.

Veranderingen in functies

Het aandachtsgebied dat we aanduiden met informatiebeveiliging is in de laatste vijf decennia verrijkt met nieuwe functies. Dat biedt interessante mogelijkheden voor carrièrepaden. De IT-beveiliger van vroeger kan nu compliance officer zijn. De oude functies blijven bestaan, maar zullen moeten samenwerken met andere, nieuwe functies.

In dit visiedocument wordt recht gedaan aan de verscheidenheid van functies die in organisaties wordt aangetroffen en daarom staat het uitgangspunt dan ook centraal dat de IB-functies deel uitmaken van een groter geheel en niet geïsoleerd kunnen worden gezien.

Voordat de functies die in het vakgebied informatiebeveiliging kunnen worden onderscheiden, geanalyseerd en naar verschillende invalshoeken uitgewerkt worden, zal eerst duidelijk moeten zijn wat onder informatiebeveiliging wordt verstaan. Bepaald moet worden welke afbakening wordt gehanteerd, ook om onderscheid met verwante functies te kunnen maken. Informatiebeveiliging kan als volgt worden gedefinieerd:

Informatiebeveiliging betreft het definiëren, implementeren, onderhouden, handhaven en evalueren van een samenhangend stelsel van maatregelen die de beschikbaarheid, de integriteit, de vertrouwelijkheid en de controleerbaarheid van de (handmatige en geautomatiseerde) informatievoorziening waarborgen.

Het verwerken van gegevens met het oogmerk informatie te kunnen verstrekken ten behoeve van het (be)sturen van organisaties en het kunnen afleggen van verantwoording over het gevoerde beheer beperkt zich nadrukkelijk niet alleen tot ICT, maar speelt evenzeer een rol bij gebruikers van ICT, waar handmatige gegevensverwerking plaatsvindt. Met handmatig wordt bedoeld het uitvoeren van administratieve procedures die in de meeste gevallen niet los kunnen worden gezien van de geautomatiseerde verwerking.

Hieronder worden kort enkele verwante begrippen besproken die geregeld in verband worden gebracht met informatiebeveiliging, maar die strikt genomen niet onder de definitie van informatiebeveiliging vallen. Deze zijn hier dan ook niet meegenomen in de profilering van de IB-functies.

De rijksoverheid positioneert in het Beveiligingsvoorschrift Rijksdienst 2005 het begrip integrale beveiliging, waarbij vanuit een integrale visie op de beveiliging van de Rijksdienst moet worden gekomen tot een afgewogen geheel van organisatorische, personele, bouwkundige en elektronische maatregelen voor de bescherming van de primaire belangen van de rijksoverheid: mensen en informatie. Bedrijfsveiligheid (Safety en Health) maakt daarvan onderdeel uit en het omvat de bedrijfshulpverlening, brandweerzorg, arbeidsomstandigheden en de toepassing van milieuregels. Publieksbeveiliging komt als begrip ook steeds meer naar voren, onder andere bij opleidingsinstituten, waaraan gelijk dan weer het begrip integrale beveiliging wordt gekoppeld. Omdat er voor het behartigen van andere belangen dan informatiebeveiliging diverse aparte, in verenigingen en opleidingen verankerde functies bestaan, is er vooralsnog geen behoefte uit te gaan van dit ruimere beveiligingsbegrip. Bovendien gaat het bij integrale beveiliging vooral ook om een bestuurlijk concept dat meerdere disciplines beoogt samen te brengen en in elk soort organisatie of branche met eigen accenten kan worden ingevuld. In dit visiedocument stellen wij wel de positionering van IB-functies aan de orde, maar niet de bepalende factoren voor de organisatie en besturing van informatiebeveiliging. Hierover buigt zich een aparte expertgroep van GvIB en PI.

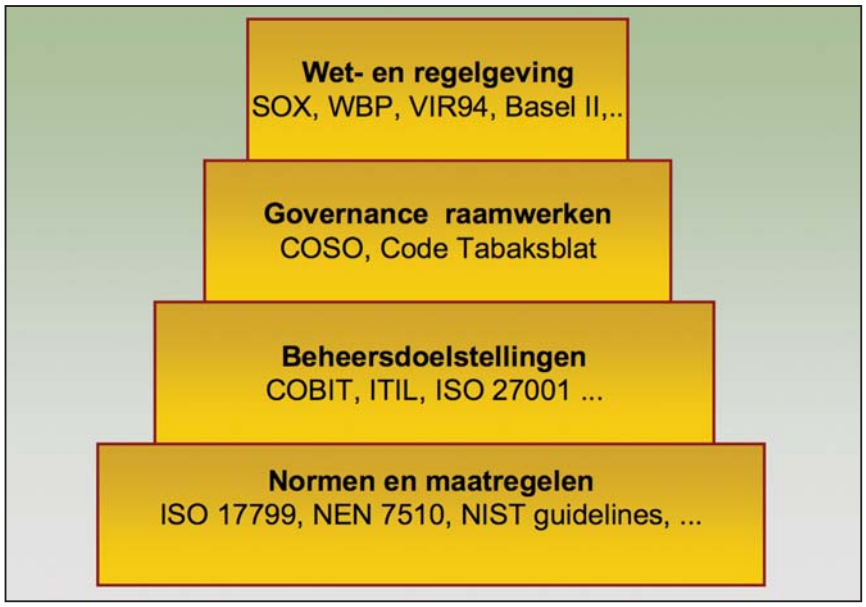
Integriteit kan ook betrekking hebben op integer handelen in het algemeen, zoals bedoeld in geval van ambtelijke integriteit bij overheden of het voorkomen van oneigenlijk gebruik van voorkennis bij beursfondsen en financiële instellingen. De zorg voor het treffen van maatregelen op dit gebied rangschikken wij onder het vakgebied compliance.

Uit de definitie van informatiebeveiliging is niet af te leiden waar de maatregelen moeten worden getroffen die bepalend zijn voor het waarborgen van de vier genoemde aspecten in de definitie van informatiebeveiliging. Dat is uiteraard mede bepalend voor de reikwijdte van de IB-functies. Vanuit de best practices, zoals de Code voor Informatiebeveiliging, kunnen de objectgebieden waarin die maatregelen worden getroffen, afgeleid worden. Zie hiertoe Tabel 1.

Objectgebieden informatiebeveiliging
Beleid (t.b.v. plannen, standaards, classificatie)
Personeel en organisatie
Communicatie (t.b.v. bewustwording)
Gebouwen en ruimten (t.b.v. fysieke beveiliging)
Technische infrastructuur
Toepassingen (inrichting en verwerking)
ITIL-processen (beheer en exploitatie ICT-services)
Systeemontwikkeling
Informatiebeveiligingsincidenten
Business continuity management
Interne controle en audit

Tabel 1 Objectgebieden informatiebeveiliging

Hiermee wordt duidelijk geïllustreerd dat het behartigen van informatiebeveiliging een brede oriëntatie vergt. Dat komt op een andere wijze eveneens tot uitdrukking in de (internationale) standaards en wet- en regelgeving, die het vakgebied steeds meer gaan bepalen. In Figuur 1 zijn deze in een hiërarchie ondergebracht.



Figuur 1 Hiërarchie bepalende kaders voor informatiebeveiliging (vrij naar Gartner)

Hieronder volgt een kort overzicht van de belangrijkste kaders voor informatiebeveiliging.

Wet- en regelgeving:

- Besluit Voorschrift Informatiebeveiliging Rijksdienst (VIR) 1994 (nu in herziening). Geeft een beperkt aantal algemene beheersingsuitgangspunten voor informatiebeveiliging en positioneert de Afhankelijkheids- en Kwetsbaarheidsanalyse.
- Wet Bescherming Persoonsgegevens (WBP) 2001. Geeft regels voor privacybescherming van personen. Op basis van deze wet is een nadere invulling gegeven aan het taakveld van de functionaris voor de gegevensbescherming via een Handreiking in 2001.
- Voorschrift informatiebeveiliging Rijksdienst - bijzondere informatie (VIR-BI) 2004. Geeft voor staatsgeheimen en departementaal vertrouwelijke gegevens beveiligingsmaatregelen per rubriceringsniveau.
- Beveiligingsvoorschrift Rijksdienst 2005. Regelt de taken van de beveiligingsambtenaar (BVA) en beveiligingscoördinator.
- Sarbanes-Oxley Act of 2002 (SOX). Deze wet legt regels op aan bedrijven die aan een Amerikaanse beurs genoteerd zijn (en haar buitenlandse filialen, of een buitenlands bedrijf met een genoteerde vestiging) en heeft consequenties voor informatiebeveiligingsmaatregelen.
- Basel II. Bevat wetgeving op Europees niveau en verplicht banken onder meer tot het beperken van operationele risico's, zoals fraude rond systemen, mensen en processen of uitval van systemen.
- Overige wetten, zoals Wet Computercriminaliteit, Telecomwet, Archiefwet, Auteurswet, Wet Elektronische Handtekening.

Governance raamwerken:

- COSO Internal Control - Integrated Framework. Een wereldstandaard voor interne beheersing, die zich richt op het vestigen van een eenduidige begripsbepaling voor interne beheersing en het opstellen van een standaard voor het beoordelen van interne beheersingssystemen.
- Code Tabaksblat. Bevat zowel principes als concrete bepalingen die de bij een vennootschap betrokken personen (onder andere bestuurders en commissarissen) en partijen (onder andere institutionele beleggers) tegenover elkaar in acht zouden moeten nemen. De principes kunnen worden opgevat als algemene opvattingen over goede corporate governance. De principes zijn uitgewerkt in concrete 'best practice'-bepalingen.

Beheersdoelstellingen:

- Control Objectives for Information and related Technology (CobiT), versie 4 is een procesgericht managementinstrument voor de beheersing van de volledige IT-omgeving en dekt alle aspecten van informatie en de ondersteunende technologie af.
- ITIL is een procesgerichte 'best practice'-benadering voor IT-beheer. Binnen het ITIL-raamwerk geeft het proces Security Management de structurele inpassing van beveiliging in de beheerorganisatie van ICT. ITIL Security Management refereert voor de normen en maatregelen aan de Code voor Informatiebeveiliging.
- ISO/IEC FDIS 27001:2005 Information technology - Security techniques - Information security management systems - Requirements. Een management raamwerk waarvan ISO/IEC 17799: 2005 (zie hierna) een nadere invulling geeft en dat onder meer wordt gebruikt voor certificering.

Normen en maatregelen:

- ISO/IEC 17799: 2005 Information technology - Security techniques - Code of practice for information security management. Beter bekend als de Code voor Informatiebeveiliging. De de facto standaard/best practice voor het vakgebied.
- Het National Institute of Standards and Technology (NIST) stelt voor de belangrijkste IT-producten uitgebreide en actuele implementatierichtlijnen voor informatiebeveiliging gratis beschikbaar.
- Branchespecifieke normen en maatregelen, zoals:
  * NEN 7510, gebaseerd op de Code voor Informatiebeveiliging en gericht op de zorgsector met een drietal Toetsbare Voorschriften.
  * Toetsingskader business continuity planning betalings- en effectenverkeer gepubliceerd door De Nederlandse Bank.
- Soortspecifieke normen en maatregelen, zoals:
  * Gedragscodes (ook voor branches) en handreikingen van het College Bescherming Persoonsgegevens.
  * ISO 15489, standaard voor informatie- en archiefmanagement.

3.1 Verantwoordelijkheden

Informatiebeveiliging is primair een verantwoordelijkheid van het (lijn-)management. De IB-functies ondersteunen het management daarbij. De manager is de enige die verantwoord kan beslissen over de mogelijk tegenstrijdige belangen tussen informatiebeveiliging, efficiency in de procesvoering en de gebruiksvriendelijkheid van informatiesystemen. Informatiebeveiliging kan leiden tot beperkingen van het gebruik van ICT-middelen en gegevens, terwijl organisaties ook belang hebben bij open communicatie en gebruiksvriendelijke toepassingen. Bij het doen van investeringen in ICT en het halen van deadlines moeten vaak lastige keuzen worden gemaakt tussen informatiebeveiliging, functionaliteit en tijdige oplevering. Daarbij komt nog dat het inbouwen van informatiebeveiligingsmaatregelen in een latere fase meestal aanzienlijk meer inspanningen vergt. Van uitstel komt vaak afstel.
Het naleven van informatiebeveiligingsmaatregelen roept bij gebruikers van informatie en informatiesystemen vaak weerstand op in verband met de toegangsbeperkingen. Alleen het management heeft de mogelijkheden die beperkingen in het dagelijkse werk van het personeel aan te brengen en te handhaven.
Tenslotte is informatiebeveiliging niet los te zien van de context waarin de maatregelen moeten functioneren, zodat daarvoor dus ook geen aparte primaire verantwoordelijkheden (los van die context) zijn te definiëren. Dat geldt niet alleen op managementniveau, maar ook op uitvoerend niveau.

Enkele voorbeelden ter illustratie:
- Het is zinvol alleen de receptie, die bezoekers opvangt om ze te verwijzen naar hun plek van bestemming, te belasten met het verstrekken van toegangspasjes.
- Alleen de systeemontwerper kan de functionele eisen voor integriteitscontroles zinvol vertalen in een functioneel ontwerp en alleen de programmeur kan deze daadwerkelijk inbouwen in de programmatuur.
- Gebruikers hebben een eigen verantwoordelijkheid voor het naleven van gedragscodes voor het vertrouwelijk houden van hun wachtwoorden.

Informatiebeveiliging is een integraal aspect van ieders functie, zodat uiteindelijk ook iedereen naar rato verantwoordelijk is voor de informatiebeveiligingsaspecten die aan zijn functie of verantwoordelijkheidsgebied worden toegewezen. De IB-functies zijn ervoor om die toewijzing van verantwoordelijkheden binnen een organisatie te expliciteren, te ondersteunen en de doelgerichtheid en evenwichtige samenhang van de maatregelen te bevorderen. De IB-functies zullen hierbij voortdurend de dynamiek van organisaties en hun omgeving evalueren.

3.2 Scheiden van taken

Het management zal taken en bevoegdheden (niet de eindverantwoordelijkheden) delegeren naar andere functies. Daarbij moet het management ervoor zorgen dat er aansluitend op de bestaande arbeidsverdeling op een efficiënte en effectieve wijze wordt gebruikgemaakt van mogelijkheden om tegengestelde belangen in de organisatie te creëren. Hierdoor kan compliance (het naleven van wettelijke, maatschappelijke en contractuele verplichtingen) worden bevorderd.

Met betrekking tot het toekennen van taken en bevoegdheden bij informatiebeveiliging betekent dit het volgende:
- Scheiding van beleidsvoorbereiding (in casu planning en normering c.q. regelgeving) en uitvoering (inclusief dagelijks monitoren) van maatregelen.
- Naar analogie daarvan scheiden van kaderstellende functies en ontwerpfuncties binnen de architectuur.
- Beslissen over maatregelen scheiden van advies, toezicht of controle van die maatregelen.
- Het primair adviseren en houden van toezicht scheiden van primair controleren.
- Bij voldoende schaalgrootte scheiden van functionele en technische taken.

Toezicht versus controle

Toezicht houden is iets anders dan controleren. Iemand die adviezen verstrekt of normen stelt zonder na te gaan (toezicht te houden) of ze worden begrepen en nagevolgd door diegenen die het betreft, komt uiteindelijk in een vacuüm terecht met zijn werk, omdat hij dan geen terugkoppeling krijgt. Toezicht houden op de naleving van adviezen of normen kan plaatsvinden door eigen waarneming, door gesprekken met betrokkenen of door documentatie te bestuderen. Het kan ook indirect plaatsvinden door gebruik te maken van ingestelde controles door anderen. Toezicht houden is er niet primair op gericht een objectief en onafhankelijk oordeel te geven. Daar is in organisaties, zeker in het kader van compliance, in veel gevallen nadrukkelijk behoefte aan. Voor een dergelijke oordeelsvorming is vakkennis nodig vanwege het controleren en een onafhankelijke positie. Een medewerker die primair adviseert en anderen ondersteunt bij de selectie van maatregelen zit niet in een ideale positie om onafhankelijk en objectief vast te stellen of de juiste maatregelen zijn getroffen, omdat hij dan zijn eigen adviezen kan tegenkomen. Een controleur die tevens wil adviseren, zal zijn adviezen dan ook moeten beperken tot de omissies die hij heeft vastgesteld vanuit zijn controlefunctie. Hij zal zijn adviezen open en globaal moeten houden, dat wil zeggen; het management de keuze moeten laten.

Mandatering

In het licht van het voorgaande is het van belang de mandatering van IB-functies aan de orde te stellen. De effectiviteit van een IB-functie kan door het management namelijk aanzienlijk bevorderd worden door bijvoorbeeld in procedures op te nemen dat mijlpaaldocumenten van de proces- en systeemontwikkeling en risicovolle changes in het ICT-exploitatieproces door de IB-functie moeten worden goedgekeurd voordat er mee mag worden doorgegaan. Deze goedkeuringen moeten goed worden verstaan door de organisatie, omdat ze geen beslissende functie mogen inhouden. Als een

mijlpaalproduct door een IB-functie wordt afgekeurd, moet dat beschouwd worden als een negatief advies aan het management, die de uiteindelijke beslissing over het al dan niet goedkeuren moet nemen. Deze uiteindelijke beslissing kan overigens gedelegeerd zijn aan een stuurgroep of Change Board, waarin alle belangen vertegenwoordigd zijn en de verschillende aspecten in onderlinge samenhang gewogen kunnen worden ten behoeve van evenwichtige besluitvorming.

3.3 Uitbesteding van ICT

De uitwerking van de functieprofielen is transparant voor uitbesteding van ICT. Enerzijds betekent uitbesteding dat de IB-functies gewoon mee uitbesteed worden en als zodanig niet veranderen. Anderzijds zullen sommige taken van IB-functies anders uitgevoerd moeten worden als gevolg van uitbesteding. Vooral communicatiepatronen zullen anders zijn en er komt veel meer nadruk te liggen op het contractueel regelen van onderlinge relaties. Tegelijkertijd kan worden gesteld dat er ook binnen grote organisaties gewerkt kan worden op onderlinge contractbasis, waardoor het verschil met uitbesteding gering zal zijn. Daarnaast komt het veelvuldig voor, zeker bij de ICT-organisatie, dat er sprake is van gedeeltelijke uitbesteding van ICT-diensten.
Wij volstaan hier met een korte opsomming van de aandachtsgebieden, die hiermee samenhangen:
- Eisen op het gebied van informatiebeveiliging opnemen in verzoeken om offertes.
- Afspraken maken over informatiebeveiliging, inclusief governance-aspecten in contracten.
- Overleg voeren over service-level-rapportages en verantwoordingen over naleving van informatiebeveiligingsnormen.
- Evalueren en bijstellen van de contractuele bepalingen.

3.4 Functie-afbakening

In de praktijk van organisaties zijn er veel soorten medewerkers die beveiliging of equivalenten daarvan in hun functiebenaming hebben staan.

Voorbeelden:
- *Security Administrator:* de functionaris die de logische toegangsbeveiliging van een platform beheert.
- *Beveiligingsfunctionaris:* de functionaris in uniform, die receptie- en bewakingsdiensten levert.
- *Register Security Expert (RSE):* de specialist in het (doen) beschermen van personen en objecten.

De vraag is wat bepaalt of er sprake is van een informatiebeveiligingsfunctie, zoals die in dit visiedocument wordt bedoeld. Hoewel het lastig is hiervoor scherp afgebakende criteria te hanteren, is de belangrijkste overweging dat er in ieder geval sprake moet zijn van een functie passend binnen de definitie van informatiebeveiliging (zie 2.2. Begrippen en kaders).

Beroep, functie, rol
In dit document staat het begrip 'functie' centraal. Dat roept de vraag op of we hier ook kunnen spreken over een rol? En wanneer spreken we dan over een beroep?
De Werkgroep Functies Bestuurlijke Informatica (WFBI) van het NGI (Nederlands Genootschap van Informatici) die de NGI-publicatie 'Taken, functies, rollen en competenties in de informatica' beheert, formuleert het als volgt: 'Een beroep is de algemeen onderscheiden aanduiding van het geheel aan activiteiten, die geacht worden te behoren tot de door de beoefenaar van dat beroep te verrichten activiteiten'. Tegenover het begrip beroep staat het begrip functie, dat wordt gezien als een organisatie- of branchespecifieke aanduiding van het geheel van iemands beroepsmatige activiteiten. Er bestaan dus ook een functierol, functieresultaten en een functieprofiel.
Een rol geeft de positie weer die de houder ervan aanneemt ten opzichte van bepaalde werkzaamheden, bijvoorbeeld uitvoeren, leiden, onderzoeken of adviseren. Een rol kan bepaalde (rol)specifieke competenties vereisen en mede bepalend zijn bij het onderscheid van beroepsniveaus. Wij voegen daaraan toe dat een rol vaak gekoppeld is aan het uitvoeren van bepaalde samenhangende activiteiten in een proces. Dat sluit aan bij het beheersen van logische toegangsbeveiliging, waarbij ook het begrip rol wordt gebruikt.

Vooralsnog past het begrip functie het best bij de doelstelling en gekozen benadering van dit visiedocument. Dat neemt niet weg dat de nu onderscheiden functies in kleinschaliger situaties dan waarvan in dit document wordt uitgegaan, vaak als deeltaak door een andere functie kan worden uitgevoerd. In veel organisaties spreekt men dan van het vervullen van een rol. Bij het uitvoeren van een deel van de bij de functies behorende taken, zal in dit visiedocument worden gesproken over taakveld om het onderscheid met rol te behouden.

De primaire, uitvoerende verantwoordelijkheden voor informatiebeveiliging maken onderdeel uit van functies die over het algemeen in organisaties voorkomen. Daartoe worden in tabel 2 de objectgebieden voor informatiebeveiliging uitgesplitst zoals deze in hoofdstukken en paragrafen naar voren komen in de Code voor Informatiebeveiliging (ISO/IEC 17799: 2005).

De taken, die bij deze primaire verantwoordelijkheden horen, betreffen in het kort:
- Het geven van opdracht tot het treffen van informatiebeveiligingsmaatregelen.
- Ervoor zorgdragen dat deze maatregelen in stand blijven, dan wel aangepast worden aan gewijzigde omstandigheden.
- Het instellen van interne controle op het naleven van de maatregelen, voor zover ze onderdeel uitmaken van menselijk handelen.

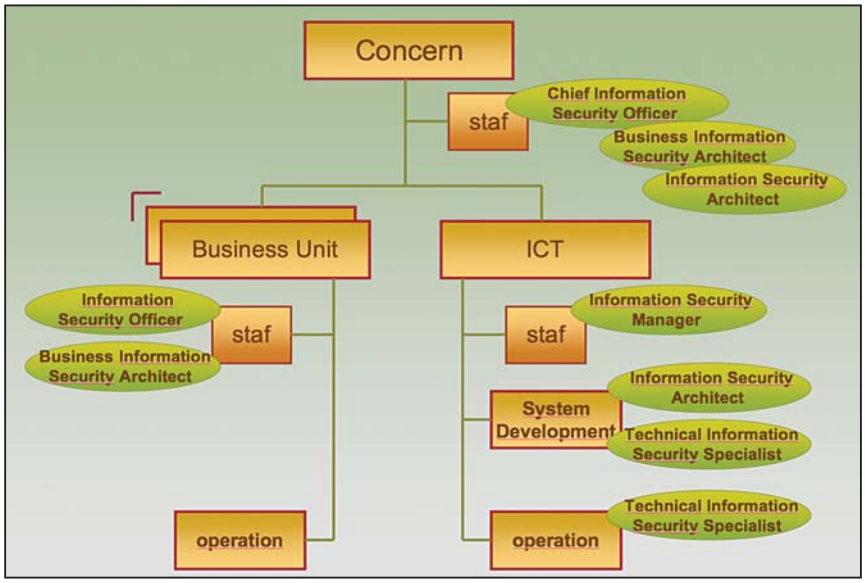
Hoofdstukken Code	Paragrafen	Algemene functies
5 Beveiligingsbeleid		Lid concerndirectie
6 Organisatie van de informatiebeveiliging		Lid concerndirectie
7 Beheer van de bedrijfsmiddelen		Aangewezen eigenaar van die middelen
8 Personele beveiligingseisen		Hoofd HRM
9 Fysieke beveiliging en beveiliging van de omgeving	9.1.1 Fysieke beveiliging van de omgeving 9.1.2 Fysieke toegangsbeveiliging 9.1.3 Beveiligen van kantoren, ruimten en voorzieningen 9.1.4 Bescherming tegen externe bedreigingen en omgevingsgevaren 9.1.6 Publiek toegankelijke ruimten, los- en laadruimten 9.2.1 Plaatsing en beveiliging van apparatuur 9.2.2 Ondersteuningshulpmiddelen 9.2.3 Beveiliging van kabels 9.2.4 Onderhoud van apparatuur	Hoofd Facilitaire dienst
	9.2.1 Plaatsing en beveiliging van apparatuur 9.2.2 Ondersteuningshulpmiddelen 9.2.4 Onderhoud van apparatuur 9.2.6 Veilig verwijderen of hergebruiken van apparatuur 9.2.7 Verwijdering van bedrijfseigendommen 9.2.5 Beveiliging van apparatuur buiten het terrein	Lid managementteam ICT
	9.1.5 Werken in beveiligde ruimten 9.2.5 Beveiliging van apparatuur buiten het terrein	Operationeel managers met ondersteuning HRM
10 Beheer van communicatie- en bedieningsprocessen	10.1 Bedieningsprocedures en verantwoordelijkheden 10.2 Beheer van de dienstverlening door een derde partij 10.3 Systeemplanning en acceptatie 10.4 Bescherming tegen kwaadaardige en 'mobile code' 10.5 Reservekopieën 10.6 Beheer van de netwerkbeveiliging 10.7 Behandeling van media 10.10 Controleren	Lid managementteam ICT
	10.7 Behandeling van media	Operationeel managers met ondersteuning HRM
	10.8 Uitwisseling van informatie 10.9 Diensten op het gebied van elektronische handel	Niet éénduidig toewijsbaar
11 Toegangsbeveiliging	11.1 Bedrijfseisen ten aanzien van toegangsbeveiliging	Lid concerndirectie of lid managementteam Business Unit
	11.3 Verantwoordelijkheden van gebruikers	Operationeel managers met ondersteuning HRM
	11.2 Beheer van toegangsrechten van gebruikers 11.4 Toegangsbeveiliging voor netwerken 11.5 Toegangsbeveiliging voor besturingssystemen 11.6 Toegangsbeveiliging voor toepassingen en informatie	Lid managementteam ICT (in afstemming met lid concern-directie) of lid managementteam Business Unit
12 Ontwikkeling en onderhoud van systemen	12.1 Beveiligingseisen voor informatiesystemen 12.2 Correcte verwerking in toepassingen	Business Unit/Information managent c.q. proceseigenaar
	12.3 Cryptografische beheersmaatregelen 12.4 Beveiliging van systeembestanden 12.5 Beveiliging bij ontwikkelings- en ondersteunings-processen 12.6 Beheer van technische kwetsbaarheid	Lid managementteam ICT

Hoofdstukken Code	Paragrafen	Algemene functies
13 Beheersing van informatiebeveiligings-incidenten		Lid concerndirectie of lid management team Business Unit
14 Beheer van bedrijfscontinuïteit		Lid concerndirectie of lid management team Business Unit
15 Naleving		Lid concerndirectie (in afstemming met lid managementteam ICT)

Tabel 2 Indicatie primaire taakverdeling voor informatiebeveiliging

5.1 De zes IB-functies en hun positionering

Voor het uitwerken van de IB-functies en hun positionering worden grote en complexe informatieverwerkende organisaties als uitgangspunt genomen. Denk daarbij aan banken en verzekeringsbedrijven, grote industriële multinationals en omvangrijke uitvoeringsorganen van de overheid, voor welke het toepassen van ICT in de primaire bedrijfsprocessen een centrale plaats inneemt. Vooral in grote organisaties ontstaat namelijk de problematiek van de afbakening (wie doet wat), van de samenhang (hoe sluiten functies op elkaar aan) en de coördinatie (welke functies zijn richtinggevend aan de andere). Er is van afgezien om vanuit een groei- of volwassenheidsmodel te laten zien hoe de verscheidenheid aan IB-functies is ontstaan, omdat zowel in de praktijk als in theorie veel ontwikkelingspaden zijn gevolgd. Daarnaast zullen er ook kleinere, volwassen organisaties zijn die het prima afkunnen met slechts één of twee IB-functies.De grootste gemene deler van de functies, die in grote, complexe organisaties zijn aan te treffen, zijn gepositioneerd binnen een eenvoudig principeplaatje van een organisatie (zie figuur 2).



Figuur 2 Positionering IB-functies

In dit principeplaatje van een organisatie worden de volgende functies met hun afkortingen en Nederlandse namen onderkend, die in 5.2 verder worden toegelicht:

IB-functies	Afk.	Nederlandse namen
Chief Information Security Officer	CISO	Concernmanager Informatiebeveiliging
Information Security Officer	ISO	Functionaris Informatiebeveiliging
Business Information Security Architect	BISA	Procesarchitect Informatiebeveiliging
Information Security Manager	ISM	Manager Informatiebeveiliging
Information Security Architect	ISA	Informatiebeveiligingsarchitect
Technical Information Security Specialist	TISS	Technisch Informatiebeveiligingsspecialist

Tabel 3 De IB-functies

Voor de naamgeving is zoveel mogelijk aangesloten bij de internationale terminologie. Met betrekking tot ITIL Security Management hebben we de term Information toegevoegd aan de daar gebruikte functiebenamingen (Security Manager en Security Officer), passend binnen onze benadering om het onderscheid te maken met de (fysieke) beveiligingsfuncties. Bij het onderscheid tussen de functies zijn er twee hoofdlijnen te onderkennen:

- Het niveau van het organisatiedeel (strategisch, tactisch of operationeel).
- Het werkveld: business of ICT (of beide).

Het onderscheid naar niveau vloeit voort uit het belang van centrale sturing op het aspectgebied. Het onderscheid naar de werkvelden business en ICT heeft te maken met het verschil in het kennisgebied en de aard van de te treffen informatiebeveiligingsmaatregelen.

De Technical Information Security Specialist wordt binnen de ICT-organisatie als een operationele functie beschouwd, die kan optreden als ontwerper of technisch beheerder.

In omvangrijke organisaties, zowel aan de business- als de ICT-kant, kan er behoefte bestaan ook op het operationele niveau functies in te stellen met overeenkomstige taken als de Information Security Officer en de Information Security Manager. In die gevallen kan in functiebenaming onderscheid worden gemaakt door ze aan te duiden als Local Information Security Officer (LISO) en Local Information Security Manager (LISM). Uiteraard krijgen de functies op het tactische niveau als gevolg daarvan dan meer coördinerende taken.

In de nu gevolgde benadering voor het onderscheiden van IB-functies is er voor gekozen alleen functies te benoemen binnen organisaties. Dat lijkt geen recht te doen aan de consultancyfuncties die diensten op het gebied van informatiebeveiliging aanbieden aan andere organisaties. Hierover kan opgemerkt worden dat consultancyfuncties meestal ingeschakeld worden om onvoldoende kwalitatieve of kwantitatieve bezetting van de interne IB-functies op te vangen, dan wel éénmalige taken als maatwerk te vervullen, die zich niet lenen voor functieprofilering. Het nu ontwikkelde functieraamwerk kan echter wel gebruikt worden als referentiekader in de consultancypraktijk om gevraagde taken af te bakenen. Bovendien kan geïnventariseerd worden of er sprake is van randvoorwaardelijke taakvervulling door andere IB-functies. Hierdoor kunnen verschillen in verwachtingspatronen tussen vraag en aanbod worden voorkomen.

5.2 Toepassen van het organisatiemodel

Uitgaande van het betrekkelijk maximale onderscheid in IB-functies, dat als uitgangspunt voor dit visiedocument is genomen, is de vraag interessant hoe met deze functies moet worden omgegaan binnen kleinere organisaties of als informatiebeveiliging minder belangrijk wordt geacht. Er is in dit visiedocument niet voor gekozen om normatieve modellen te ontwikkelen met daarin de optimale verdeling van IB-functies. Er zijn namelijk veel factoren te onderkennen die de inrichting van een organisatie en dus ook de invulling van IB-functies bepalen. Wij verwijzen hiervoor naar de recent uitgebrachte Expertbrief 'Het inrichten van een beveiligingsorganisatie', waarvoor nog vervolgactiviteiten gepland zijn.

In plaats daarvan is naast het principeplaatje voor de organisatorische positionering van de IB-functies (figuur 2) een relatietabel (zie figuur 4) ontwikkeld die gebruikt kan worden voor het positioneren van IB-functies in kleinere organisaties. De relatietabel gaat uit van de algemene functies die door de IB-functies worden ondersteund. Specialistische functies zullen pas ontstaan als er voldoende schaalgrootte in de organisatie is of het belang van het specialisme daarom vraagt. In de relatietabel zijn alleen die algemene functies opgenomen, waarvoor de IB-functies primair hun ondersteuning leveren. Er zijn dus minder algemene functies in de relatietabel opgenomen dan in tabel 2. Opgemerkt wordt dat niet alleen managers door IB-functies worden ondersteund, maar ook algemene uitvoerende functies.

Voorbeelden daarvan:

- Een architect informatiebeveiliging ondersteunt een ICT-architect en niet het ICT-management. De architect informatiebeveiliging is te beschouwen als een verbijzondering van de ICT-architect.
- Een security administrator is een verbijzondering van een systeem- of toepassingsbeheerder.

Een kleinere organisatie zal wellicht niet het onderscheid in drie niveaus kennen, maar bijvoorbeeld twee niveaus, waardoor de tactische IB-functies óf niet van toepassing zijn óf naar het operationele niveau verschuiven.

Het belang van het leggen van een relatie met verwante functies, die tevens in de relatietabel zijn opgenomen, heeft te maken met mogelijkheden tot samenvoeging van verschillende taakvelden in één functie bij kleinere organisaties. Bij grote organisaties kan overigens langs de horizontale lijn in de relatietabel nagedacht worden over teamvorming, waarbij verschillende specialismen elkaar kunnen versterken. Wij komen hierop nog terug in dit visiedocument.

In de praktijk worden ook functies aangetroffen, bijvoorbeeld op basis van regelgeving, waarbij een deelgebied van de informatiebeveiliging als specialisme wordt uitgeoefend. Zie de kolom Taakvelden en deelgebieden informatiebeveiliging in de relatietabel. Dat kan een gedeelte zijn van het beveiligingsproces (zie paragraaf 6.1), zoals een beleidsmedewerker die kan vervullen of een gedeelte van de objectgebieden, zoals bij de Functionaris voor de Gegevensbescherming. Voornamelijk de Technical Information Security Specialist zal op operationele deelgebieden van informatiebeveiliging worden ingezet. Ook hierop wordt nog teruggekomen.

grotere organisaties → FUNCTIESPECIALISATIE

GELAAGDHEID ORGANISATIE ↓

Algemene functies met informatiebeveiligingstaak	Deels overlappende en verwante functies	Functies Informatiebeveiliging	Taakvelden en deelgebieden informatiebeveiliging
STRATEGISCH NIVEAU			
- Lid concerndirectie	- Risico Manager - Business Continuity Manager - Compliance Officer - Quality Assurance Manager - Intern of IT-auditor (niet met IB-functies combineren!)	**Chief Information Security Officer**	- Beleidsmedewerker Informatiebeveiliging - Functionaris Gegevens-bescherming (volgens WBP)
- Enterprise Information Architect		**Business Information Security Architect**	
- IT-architect		**Information Security Architect**	
TASTISCH NIVEAU BUSINESS UNIT			
- Lid managementteam	- Interne Controle medewerker - AO (/IC) functionaris	**Information Security Officer**	
- Information Architect		**Business Information Security Architect**	
TACTISCH NIVEAU/DEVELOPMENT ICT			
- Lid managementteam	- Interne Controle medewerker - AO (/IC) functionaris - Kwaliteitsmedewerker	**Information Security Manager**	
- IT-architect		**Information Security Architect**	
OPERATIONEEL NIVEAU ICT			
- Systeem Specialist - Applicatie beheerder - Technisch beheerder		**Technical Information Security Specialist**	- Cryptografie specialist - Security Administrator - CERT-medewerker - Ethisch hacker, etc.

Tabel 4 Relatietabel functies in de informatiebeveiliging

5.3 De zes IB-functies nader toegelicht

Chief Information Security Officer (CISO)

De Chief Information Security Officer acteert op het hoogste managementniveau en moet dus in de eerste plaats de taal van het management verstaan en spreken. Hij communiceert zowel met de concernleiding als de leiding van Business Units en met de leiding van ICT. In hoeverre hijzelf als direct leidinggevende fungeert, hangt af van eventuele centrale teamvorming van beveiligingsfunctionarissen, waarbij aan medewerkers met verschillende achtergrond en specialisatie leiding moet worden gegeven. De Chief Information Security Officer geeft functioneel leiding aan het werk van de IB-functies op lagere niveaus. Op het gebied van informatiebeveiliging is hij duidelijk een generalist, die op hoofdlijnen de verbanden tussen de verschillende bedrijfs- en beveiligingsbelangen moet kunnen leggen. Hij bestrijkt alle objectgebieden, zie Tabel 1. Hij moet in staat zijn tegengestelde belangen met elkaar te verenigen, waarbij hij de adviezen van verschillende deskundigen en de belangen van het management op hun waarde moet kunnen beoordelen. Dit alles om een goede adviseur te zijn voor de concernleiding.

Information Security Officer (ISO)

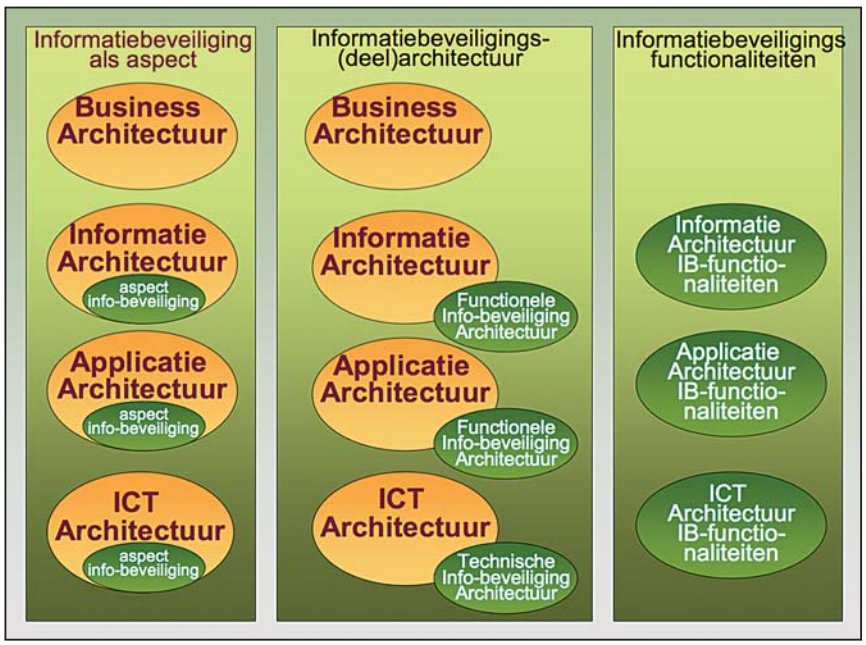
De Information Security Officer werkt vanuit kaders die op concernniveau worden vastgesteld. Uiteraard zal hij bij het onderhoud van die kaders worden betrokken, maar hij richt zich toch vooral op de naleving daarvan in de operationele processen. De Information Security Officer ontleent zijn toegevoegde waarde aan zijn kennis van de Business Unit en de vertaalslag die moet worden gemaakt van algemene IB-normen naar de specifieke bedrijfssituatie. Die algemene IB-normen hebben vooral betrekking op personeel en organisatie, communicatie (ten behoeve van bewustwording), gebouwen en ruimten (ten behoeve van fysieke beveiliging), informatiebeveiligingsincidenten en de invulling van business continuity management in de Business Unit.

Business Information Security Architect (BISA)

De Business Information Security Architect heeft als beveiligingsspecialist de business en processen als werkveld. Als hij op concernniveau acteert, nemen de generieke concerntoepassingen daarbij uiteraard een belangrijke plaats in, zoals Enterprise Resource Planning pakketten, functionele aspecten van internet, mail, portals, elektronische berichtendiensten en dergelijke. De Business Information Security Architect is vooral actief in de eerste fasen van proces- en systeemontwikkeling. In onderhouds- en evaluatiefasen van processen en informatiesystemen zal hij toezien op het handhaven van informatiebeveiligingsuitgangspunten.

De Business Information Security Architect kan meerdere invalshoeken kiezen voor zijn taakvervulling, zie figuur 3. Hij kan een informatiebeveiligings-(deel)architectuur opleveren en onderhouden en verder adviseren en toezien op implementatie daarvan in andere architecturen en in proces- en ICT-ontwerpen. Binnen deze benadering is het globaal ontwerpen van generieke beveiligingsfunctionaliteiten een verdergaande invulling. Als de Business Information Security Architect zich daarentegen in eerste instantie als adviseur en toezichthouder opstelt, zal dat betekenen dat de functie ertoe bijdraagt dat in alle andere architecturen informatiebeveiliging wordt ingebed als één van de kwaliteitsaspecten. Wel dient het aspect apart zichtbaar te worden gemaakt in de architecturen en ontwerpen, bijvoorbeeld in een beveiligingsparagraaf.

Op basis van de eerder geformuleerde uitgangspunten wordt er bij deze functie vanuit gegaan dat het opstellen van ontwerpkaders op het hoogste niveau en het uitoefenen van toezicht op de naleving daarvan bij voorkeur is te scheiden van het ontwerpen van deelarchitecturen en functionele ontwerpen op het gebied van informatiebeveiliging. Deze onverenigbaarheid komt het meest naar voren bij het ontwerpen van IB-functionaliteiten.



Figuur 3 Invalshoeken informatiebeveiliging in relatie tot de architecturen

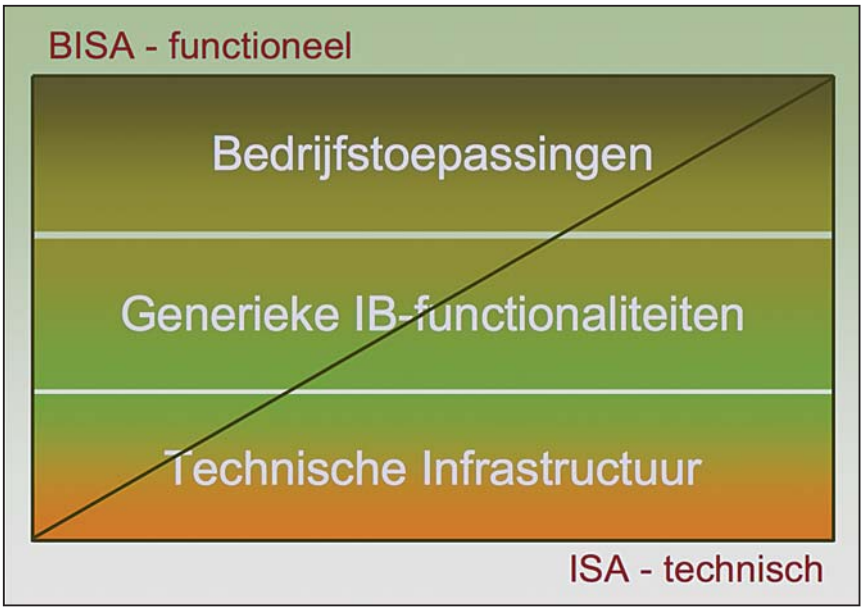
Information Security Manager (ISM)

De Information Security Manager heeft binnen het werkveld ICT soortgelijke taken als de Information Security Officer. Hij heeft echter niet alleen de algemene concernrichtlijnen op het gebied van informatiebeveiliging te borgen zoals die voor Business Units gelden, maar ook die specifiek zijn voor de ICT-organisatie. Belangrijke aandachtgebieden daarbij zijn de interne beheer- en exploitatieprocessen van ICT en de technische infrastructuur. Meer dan bij Business Units zal hij te maken kunnen krijgen met uitbestedingssituaties en het ten behoeve van derden aantonen dat de beveiligingsnormen

ook daadwerkelijk worden nageleefd. Ook zal het eerder aan de orde komen dat hij functioneel leiding moet geven aan andere IB-functies. Mede om dergelijke redenen is in zijn functieprofiel uit gegaan van zwaardere competentie-eisen.

Information Security Architect (ISA)

Wat hiervoor is vermeld over de Business Information Security Architect is in hoge mate eveneens van toepassing op de Information Security Architect. Met betrekking tot ICT betreft het verschil met de Business Information Security Architect de technische oriëntatie van de Information Security Architect en de grotere nadruk op de technische infrastructuur. In Figuur 4 wordt dit op andere wijze duidelijk gemaakt.



Figuur 4 Samenhang en onderscheid IB-architectenfuncties

Technical Information Security Specialist (TISS)

De Technical Information Security Specialist vervult in beginsel taken op het operationele niveau binnen de ICT-organisatie. In dit visiedocument dient deze functie als overkoepelende kapstok voor een reeks functies, die verder worden toegelicht in paragraaf 5.5 Specialistische functies.

5.4 Verwante functies

In de praktijk kan een grote verscheidenheid aan verwante en/of overlappende functies worden aangetroffen al naar gelang omvang, volwassenheid of branche van een organisatie. Om tot een effectieve en efficiënte taakvervulling (ook voor de verwante functies) te komen, is het noodzakelijk de samenhang en de verschillen goed af te bakenen. Door hun onderlinge posities goed te regelen, kunnen functies elkaar versterken, maar ze kunnen elkaar ook verzwakken als ze - al dan niet doelbewust - elkaars functies (deels en met andere uitgangspunten) vervullen. Daarom wordt hier een korte typering van die verwante en/of overlappende functies gegeven om zo het onderscheid met de functies in de informatiebeveiliging goed te kunnen maken. In de figuren 5 en 7 is op zeer vereenvoudigde wijze in kernwoorden aangegeven welke overeenkomsten en verschillen te onderkennen zijn binnen de verwante vakgebieden ten opzichte van de IB-functies.

De Risicomanager (Risk Manager)

De Risicomanager heeft een breder werkveld dan informatiebeveiliging, want risico's zijn niet alleen verbonden aan gegevensverwerking, maar ook inherent aan de bedrijfsvoering. Er zijn tal van bedrijfsrisico's, zoals projectrisico's, milieurisico's, financieringsrisico's, productrisico's, politieke en maatschappelijke risico's. De Risicomanager zal de diverse managementlagen in de organisatie ondersteunen bij het beheersen van deze risico's door risicoanalyses te faciliteren, de plancyclus op gang te brengen en te houden en het toezien op de rapportage daarover. Al naar gelang de bedrijfstypologie zal de toepassing van ICT hierbij een belangrijk aandachtspunt vormen.

De Business Continuity Manager (BCM)

De Business Continuity Manager behartigt onder meer een deelaspect van de informatiebeveiliging. Het doel van Business Continuity Management is het nastreven van de continuïteit van bedrijfsprocessen bij calamiteiten. Door het laten uitvoeren en begeleiden van business impact analyses en risicoanalyses zal hij de uitgangspunten voor de continuïteitsmaatregelen onderbouwen. Dat betekent onder andere dat hij die activiteiten goed zal moeten afstemmen met de Risk Manager.

De Business Continuity Manager is vooral gericht op de repressieve (schadebeperkende) maatregelen op het gebied van beschikbaarheid onder meer voor alle objecten, die ook voor informatiebeveiliging in beschouwing worden genomen. Andere objecten betreffen bijvoorbeeld productiemiddelen in het primaire productieproces. Vaak worden ook de op de veiligheid van het personeel gerichte maatregelen (zoals ontruiming) meegenomen in geval van calamiteiten. De Business Continuity Manager zal de tactische en de operationele richtlijnen ten aanzien van de continuïteitshandhaving ontwikkelen en onderhouden.

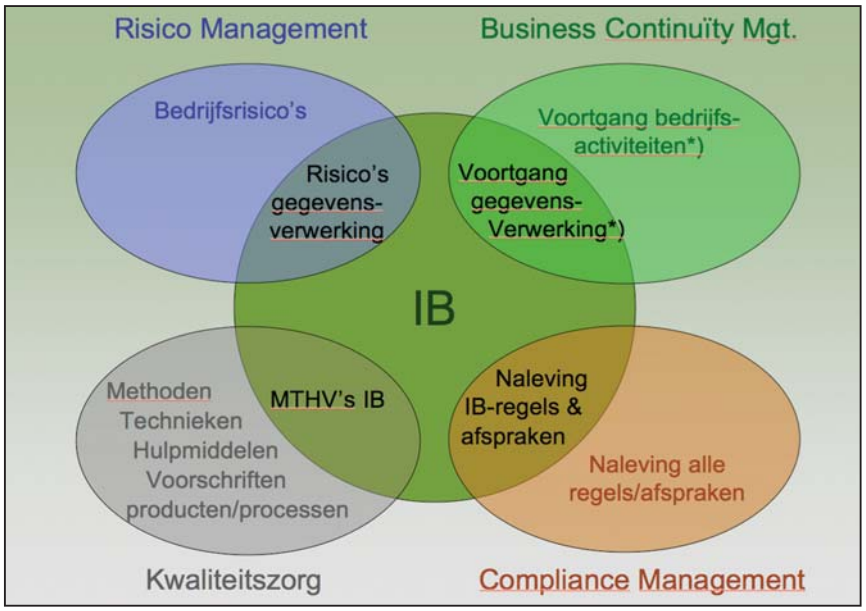
De Business Continuïty Manager neemt niet alleen de Risk Manager, maar uiteraard ook de IB-functies een belangrijk taakveld uit handen, dat als apart specialisme is te beschouwen, ook gezien de eigen internationale standaards en instituten. Met de IB-functies zal hij zijn werkzaamheden goed moeten afstemmen, omdat deze laatsten de preventieve beschikbaarheidsmaatregelen (wellicht beter kunnen) behartigen onder meer vanwege hun betrokkenheid bij architecturen en ontwerpen.

De Compliance Officer

Het betreft hier een relatief nieuwe en ruimere functie dan een IB-functie, die is ontstaan vanuit de vergaande regelgeving waaraan organisaties moeten of willen voldoen. Compliance, het aantoonbaar naleven van regelgeving, kan per organisatie een verschillende betekenis hebben. Het kan gaan om wettelijke regelingen, bijvoorbeeld op het gebied van kartelvorming, marktmisbruik en in dat kader de Regeling Privé-beleggingtransacties (Complianceregeling AFM), branchegebonden regels (Basel II voor de banken), ondernemerscodes voor Corporate Governance, zelf opgelegde regels (bijvoorbeeld ISO 900x.-serie voor kwaliteit in algemene zin), interne policies en het naleven van contracten. Vooral bij het handhaven van de persoonlijke integriteit van medewerkers op gevoelige functies kunnen aan de Compliance Officer op grond van wettelijke regelingen (bijvoorbeeld bij financiële instellingen) speciale bevoegdheden zijn toegekend om zijn taak uit te oefenen.
Het beheersingsproces om aan regels te voldoen, vertoont vanuit de compliance benadering per definitie verwantschap met het proces van informatiebeveiliging, waarbij normen nageleefd moeten worden. Daarnaast impliceren sommige regelingen tevens regels voor informatiebeveiliging. Afhankelijk van het werkveld van de Compliance Officer zal afstemming met de IB-functies noodzakelijk zijn.

De Manager Kwaliteitszorg (Quality Assurance Manager)

Kwaliteit heeft met inherente eigenschappen van processen en producten te maken, waarbij informatiebeveiliging als subset van het geheel van de te onderkennen aspecten en eigenschappen kan worden gezien. Als een organisatie aan veel genormeerde kwaliteitsaspecten moet voldoen, bijvoorbeeld vanuit wettelijke, branche- of marktgerichte eisen, kan dat voor organisaties betekenen dat hiervoor een kwaliteitssysteem met bijbehorende medewerkers voor advies en toetsing in het leven moet worden geroepen. In dergelijke situaties kan het een voordeel voor de informatiebeveiliging zijn om daarop 'mee te liften' en (deels) hierin te integreren.



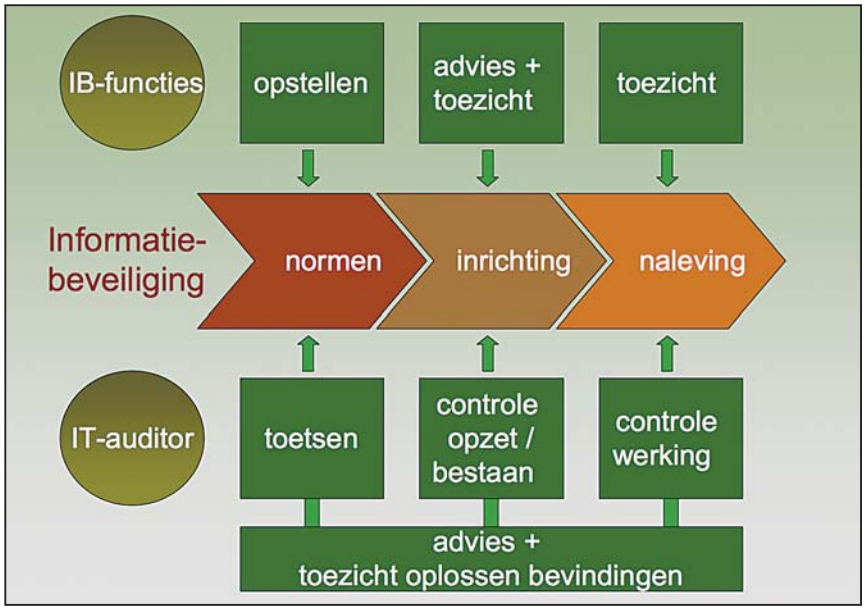
Figuur 5 Samenhang en onderscheid met verwante functies - 1

De Beveiligingsmanager

Bij de afbakening van het begrip informatiebeveiliging in paragraaf 2 is al de link gelegd met de diverse, andere beveiligingsbegrippen, die betrekking kunnen hebben op fysieke, publieke, personen-, bedrijfs- of integrale beveiliging. In het verlengde daarvan zijn evenzoveel functies ontstaan onder de noemer van 'beveiliging' al dan niet voorzien van verschillende adjectieven. In ieder geval bestaat er bij het objectgebied fysieke beveiliging een overlap. Afhankelijk van de wijze van invulling van het beveiligingsbegrip in een organisatie of branche kan er wellicht meer overlap van objectgebieden zijn.
Onderlinge afstemming is dus noodzakelijk en gezamenlijk optrekken of aangestuurd worden, kan tot wederzijds voordeel strekken omdat er zodoende meer gewicht in de schaal kan worden gelegd.

De IT Auditor

De (interne) IT-auditor vervult primair een controlerende functie. Dit in tegenstelling tot de IB-functies (met uitzondering van de Technical Information Security Specialist), die primair een adviserende rol hebben. De IT-auditor bestrijkt tenminste dezelfde objectgebieden als die van de IB-functies. Indien de controle op naleving van normen voor informatiebeveiliging in Business Units door (interne) algemene auditors in plaats van IT-auditors wordt uitgevoerd, maken we daar in dit visiedocument omwille van de eenvoud geen onderscheid in.
De IT-auditor geeft naar aanleiding van geconstateerde bevindingen zodanige adviezen, dat de voor informatiebeveiliging primair verantwoordelijken zelf de implementatiekeuze kunnen maken. Figuur 6 brengt de verschillende taken van beide functiegebieden in relatie tot informatiebeveiliging in beeld.



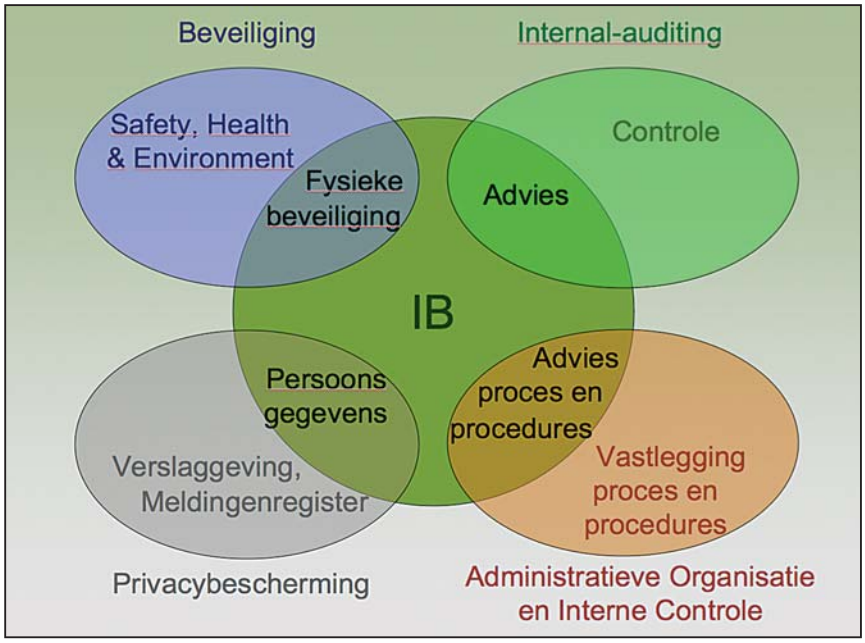
Figuur 6 Verschillende taken voor hetzelfde objectgebied

In hoofdlijnen kan de IT-auditor zijn functie op twee wijzen vervullen. Of op een terughoudende wijze, waarbij hij altijd gevraagd moet worden om een opdracht te vervullen. Of op proactieve wijze, waarbij hij namens het topmanagement permanent in de gaten houdt of er blijvend aan informatiebeveiligingsnormen wordt voldaan en hierover adviezen uitbrengt. Bij certificering van informatiebeveiliging, vooral ten behoeve van derden en dat is bij informatiebeveiliging veelvuldig aan de orde, past daarentegen een wat meer terughoudende taakvervulling. In dat geval zal hij zijn advieswerk zoveel mogelijk beperken.

De proactieve invulling van taken door de IT-auditor kan betekenen dat hij (in plaats van de IB-functie) een goedkeurende rol vervult ten aanzien van IB-aspecten in ontwerpen van ICT-voorzieningen of door het uitvoeren van audits op vitale ICT-projecten, waarvoor hij een permanente opdracht heeft. Hij wordt geacht dan zelf vanuit managementoptiek belangrijke ontwikkelingen in de gaten te houden en audits in te stellen wanneer hij dat vanuit de bedrijfsbelangen nodig acht. Dit vergt overigens wel een nadrukkelijk mandaat van het topmanagement en een hoge beschikbaarheid van de functie. De IT-auditor kan bijvoorbeeld ook de architecturen mede als toetsingskader gebruiken.
De proactieve benadering hangt samen met de behoefte van het management om zo objectief mogelijk zekerheden te krijgen dat tijdig de juiste IB-maatregelen worden getroffen. Het mag duidelijk zijn dat de mate waarin er een proactieve rol van de IT-auditor wordt gevraagd mede afhankelijk is van de bedrijfstypologie en de wijze waarop de IB-functies in het ontwikkeltraject worden ingezet en zijn gepositioneerd. De twee functies kunnen elkaar goed aanvullen, maar ook voor een deel overlappend werk doen. Er zullen dus goede afspraken moeten worden gemaakt over de onderlinge positionering.

De medewerker Administratieve Organisatie en Interne Controle (AO/IC-medewerker)
Een functionaris die op een geheel andere wijze van betekenis kan zijn voor de informatiebeveiliging is de medewerker Administratieve Organisatie en Interne Controle, verder aan te duiden als AO/IC-medewerker. Deze functionaris vervult een adviserende rol bij de inrichting van bedrijfsprocessen, terwijl hij meestal ook registratieve taken vervult door het systematisch vastleggen van processen en soms ook werkinstructies. Als de ontwerpen voor procesinrichting door procesarchitecten worden gemaakt, zal hij meer op het operationele niveau in een organisatie(deel) werkzaam zijn en een toetsende rol kunnen vervullen om vast te stellen dat de procesbeschrijving compleet en logisch is, aansluit bij andere processen binnen een organisatiedeel en dat bijvoorbeeld aan eisen van functiescheiding wordt voldaan. Als specialist op het gebied van operationele processen en handmatige procedures kan hij zorgdragen voor verankering van de handmatige IB-maatregelen in de dagelijkse werkprocessen. Tenslotte kan hij een toezichthoudende rol vervullen ten aanzien van het tijdig en volledig documenteren van procesbeschrijvingen bij organisatieveranderingen en invoering van nieuwe of gewijzigde informatiesystemen. Kortom; een voor de beheersing van een deelgebied van de informatiebeveiliging onmisbare functie.

De Kwaliteitsmedewerker bij systeemontwikkeling (Quality Assurance medewerker IT)
Veel ICT-organisaties kennen de functie van kwaliteitsmedewerker binnen het proces van ontwerp en onderhoud van processen en ICT-voorzieningen. De Kwaliteitsmedewerker richt zich zowel op het proces van ontwerpen en onderhouden als op de daaruit voortkomende producten, zoals fasedocumenten. Hij draagt zorg voor de Methoden, Technieken, Hulpmiddelen en Voorschriften (MTHV's) en adviseert in de ontwikkelings- en onderhoudsprojecten over de toepassing hiervan. Hij hoeft zelf niet altijd voor alle aspecten de inhoudelijke specialist te zijn op het gebied van productkwaliteit, maar hij is wel belast met de zorg dat deze in voldoende mate worden meegenomen in de ontwerpen. Hij heeft ook een toezichthoudende taak op de naleving van de voorschriften. Als de kwaliteitsmedewerker zich baseert op ISO 9126 voor productkwaliteit in ICT ontstaat er overlapping en mogelijk frictie met productgerichte normen vanuit informatiebeveiliging omdat definities van deelaspecten niet altijd overeenstemmen.
De Kwaliteitsmedewerker kan voor de informatiebeveiliging in ieder geval de belangrijke taak vervullen om te borgen dat er voldaan wordt aan de procesgerichte IB-normen. Duidelijk is dat de twee soorten functies hun werk onderling moeten afstemmen.



Figuur 7 Samenhang en onderscheid met verwante functies - 2

De Interne Controle-medewerker (IC-medewerker)

De functionaris belast met Interne Controlewerkzaamheden richt zich vooral op de routinematige controles op de werking van processen ofwel de naleving van processen en procedures zoals die door de AO/IC-medewerker worden gedocumenteerd. De IT-auditor kan onder voorwaarden goed gebruikmaken van deze functie. Naar aanleiding van zijn bevindingen kan de IC-medewerker ook advies geven. Een werkverdeling met de algemene IB-functies zou kunnen zijn dat de beoordeling van en advisering bij de inrichting van processen tot de taak van de IB-functie wordt gerekend, omdat deze het geheel en de onderlinge samenhang van de IB-maatregelen wil bewaken. Dat geldt vooral bij processen waarbij ICT en informatiebeveiliging belangrijk zijn.
De IC-medewerker kan dan adviseren bij nalevingsvraagstukken (de werking van de processen). De controlebevindingen van de IC-medewerker zijn input voor de evaluatie van de IB-functie.

5.5 Specialistische functies

In de relatietabel (tabel 4) is een aantal functies weergegeven, die als een specialisme binnen de IB-functies kunnen worden aangemerkt. Dat kan betekenen dat een gedeelte van de taken wordt uitgevoerd, al dan niet in combinatie met andere specifieke taken, of dat de taken zich op specifieke objecten of deelgebieden richten. Ook combinaties daarvan komen voor. Enkele bekende functies worden hier kort toegelicht.

Beleidsmedewerker Informatiebeveiliging

In grote organisaties en vooral bij overheidsinstellingen komt het voor dat speciale afdelingen zich richten op het ontwikkelen en onderhouden van beleid, terwijl de uitvoering daarvan wordt overgelaten aan werkmaatschappijen of uitvoeringsorganen. De Chief Information Security Officer zal zich in dergelijke omstandigheden hoofdzakelijk beperken tot het resultaatgebied Beleid (zie hoofdstuk 6).

Functionaris voor de Gegevensbescherming (FG)

Bedrijven, brancheorganisaties, overheden en instellingen hebben de mogelijkheid zelf een interne toezichthouder op de verwerking van persoonsgegevens aan te stellen: de Functionaris voor de Gegevensbescherming. Deze functionaris houdt dan binnen de organisatie toezicht op de toepassing en naleving van de Wet Bescherming Persoonsgegevens (WBP) en heeft wettelijke taken en bevoegdheden en daarmee een onafhankelijke positie in de organisatie.
Het Genootschap van Functionarissen van de Gegevensbescherming geeft in een handreiking een beschrijving van de taken, die wij hier verkort weergeven:
Verplichte taken:
- Toezicht: de functionaris ziet toe op de naleving van de wettelijke regels over het verwerken van persoonsgegevens binnen zijn organisatie.
- Verslaggeving: de FG heeft de wettelijke taak jaarlijks een verslag op te stellen van zijn werkzaamheden en bevindingen.
- Meldingenregister: als een organisatie een FG heeft aangesteld, kunnen de verwerking(en) van persoonsgegevens bij de FG worden gemeld, in plaats van bij het College Bescherming Persoonsgegevens (CBP).

Optionele taken:
- Inventarisatie: de FG kan een ondersteunende rol vervullen bij het in kaart brengen van alle verwerkingen van de organisatie en daarbij aangeven wat daarbij 'verwerkingen' zijn in de zin van de WBP.
- Voorlichting: binnen zijn organisatie kan de FG voorlichting geven over de omgang met persoonsgegevens en adviseren over kwesties die samenhangen met het verwerken daarvan.
- Technologie en beveiliging: de FG kan de organisatie adviseren bij het realiseren van het passende niveau van informatiebeveiliging.
- Klachtbehandeling en bemiddeling: de behandeling van klachten over het gebruik van persoonsgegevens kan deel uitmaken van het takenpakket van een FG.
- Normontwikkeling: binnen een organisatie of een branche kan behoefte ontstaan aan normen/gedragscodes die zijn toegesneden op de specifieke verwerkingen binnen de organisatie of branche. De FG kan die ontwerpen.

Persoonsgegevens maken onderdeel uit van de gegevens waarvoor een organisatie informatiebeveiligingsmaatregelen treft. Bij een volwaardige invulling van de IB-functies in een organisatie is er een duidelijke overlap in taakvelden te constateren. De taakvelden van de FG kunnen in principe geheel worden ondergebracht bij die van een Chief Information Security Officer of Information Security Officer. Ook is het bijvoorbeeld mogelijk de taken met betrekking tot verslaggeving, meldingenregister en klachtbehandeling van de FG onder te brengen bij een medewerker van Juridische Zaken, uiteraard in nauwe samenwerking dan wel afstemming met de hiervoor genoemde IB-functies.

Verschijningsvormen van Technical Information Security Specialist

De Technical Information Security Specialist kan zich op veel verschillende objectgebieden en bij diverse processen manifesteren. De behoefte aan zijn specialisme zal afhangen van de stand van de techniek, de schaal waarop wordt gewerkt en het belang dat informatiebeveiliging heeft. Volstaan wordt met een indicatieve opsomming. Bekende objectgebieden betreffen:

- Cryptografie
- Netwerkbeveiliging, waaronder firewalls, intrusion detection en prevention, malware, informatiebeveiliging in protocollen
- Informatiebeveiliging in applicaties
- Logging en monitoring
- Incidentonderzoek en afhandeling, bijvoorbeeld bij een Computer Emergency Response Team
- Logische toegangsbeveiliging (Identificatie-, Authenticatie- en Autorisatietoepassingen)

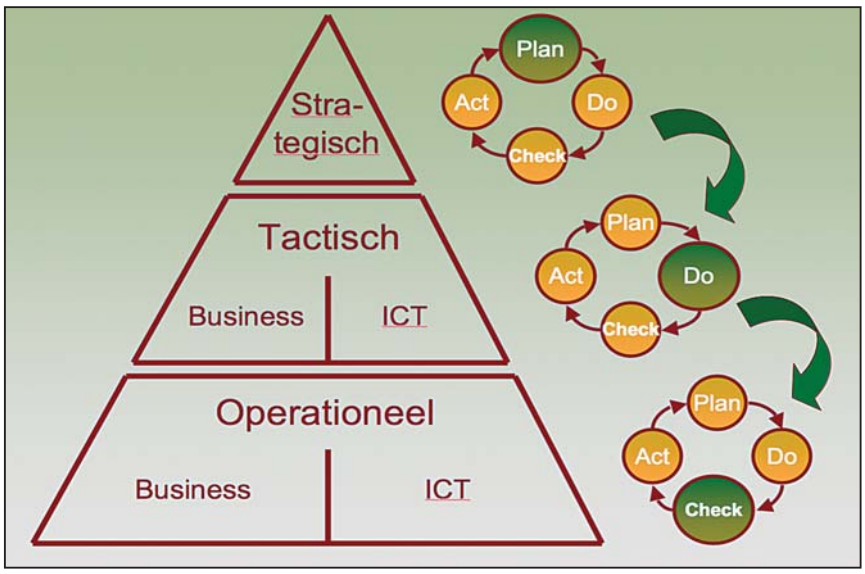
Deze objectgebieden kunnen aan de orde zijn bij systeemontwikkeling en -onderhoud, maar ook bij implementatie, beheer en exploitatie. Dat betekent dat de Technical Information Security Specialist als ontwerper, technisch beheerder, maar ook als Security Administrator voor logische toegangsbeveiliging of certificatenbeheerder bij Public Key Infrastructures kan optreden. Een specifieke functie-invulling is ook die van Ethisch Hacker, waarbij hij vanuit een onafhankelijke positie in live-situaties de beveiliging van infrastructuren en internetapplicaties kan testen en advies verstrekt om geconstateerde leemten op te lossen. Een andere invulling betreft de Digitale Rechercheur, die een grondige kennis moet hebben van veel van de hiervoor vermelde objectgebieden en die bijvoorbeeld ook binnen particuliere organisaties zijn werkveld kan hebben.
In dit visiedocument is het minder passend te streven naar een volledige en actuele opsomming van deze operationele, gespecialiseerde functies.

5.6 Teamvorming

In de praktijk worden vaak teams van specialisten uit meerdere disciplines gevormd om op diverse fronten synergie te bereiken. Het kan ervoor zorgen dat activiteiten beter op elkaar worden afgestemd, dat er onderlinge stimulansen ontstaan en dat éénzelfde aanpak wordt gevolgd bij het benaderen van de doelgroepen, die vaak hetzelfde zijn. Ook uit de éénduidige aansturing van dergelijke specialisten kan een belangrijk voordeel voor een organisatie worden behaald. Een team heeft meestal een sterkere positie dan een éénling in een organisatie. Een team kan zich onafhankelijker opstellen en zich beter naar het management op de diverse niveaus binnen een organisatie profileren. En last but not least: een team kan de nadelen van ver doorgevoerde functiedifferentiatie beter opvangen. Op uitvoerend niveau ziet men vaak door de bomen het bos niet meer als men advies wil of een probleem opgelost wil hebben. Bij wie van de vele verschillende soorten deskundigen moet men te rade gaan?
Het combineren van functies kan zowel betrekking hebben op de combinatie met verwante functies als op het samenbrengen van IB-functies zelf. Dat laatste kan aan de orde zijn als een ICT-organisatie of Business Unit te groot is voor een enkele Information Security Manager, dan wel Information Security Officer. Indien er een team van IB-specialisten wordt gevormd, ontstaan er mogelijkheden tot specialisatie en wel naar de verschillende objectgebieden of naar vestigingen, afdelingen of resultaatgebieden. Binnen een team ontstaan ook goede mogelijkheden voor het volgen en begeleiden van carrièrepaden of het voorbereiden op IB-functies elders binnen de organisatie.
Bij teamvorming is het van belang om attent te zijn op onverenigbare functies (zie hoofdstuk 3 Uitgangspunten). Teamvorming zal gevolgen hebben voor de organieke plaats. Deze is bij voorkeur neutraal ten opzichte van de belangrijkste belanghebbenden om bevoordeling van of een onevenwichtige beïnvloeding door één organisatiedeel te voorkomen. Tegelijkertijd kan de organisatorische afstand weer een zeker risico vormen bij de acceptatie van richtlijnen, adviezen of uitkomsten van toetsingen.

6.1 Resultaatgebieden

Voor het beschrijven van functies worden taken gegroepeerd naar resultaatgebieden. Voor het onderkennen van de resultaatgebieden van informatiebeveiliging wordt aangesloten bij de processtappen van de cyclus: Plan - Do - Check - Act, zie figuur 8. Op de drie niveaus in de organisatie liggen de accenten per fase niet gelijk. Op strategisch niveau is Plan het belangrijkste, op het tactisch niveau Do en op operationeel niveau Check. Op elk niveau is de inhoud van de fasen in de cyclus uiteraard een andere, maar ze moeten wel op elkaar aansluiten. Alleen bij de Technical Information Security Specialist is deze cyclische benadering van de resultaatgebieden in een functie minder van toepassing gezien de verscheidenheid aan inzetmogelijkheden die op deze functie van toepassing is. Verder past nog de kanttekening dat de Do-fase voor de meeste IB-functies betekent dat zij daar hun adviserende en toezichthoudende taken vervullen, omdat de implementatie van informatiebeveiligingsmaatregelen zelf een uitvoerende taak is.



Figuur 8 Resultaatgebieden in het proces informatiebeveiliging.

De taken per resultaatgebied worden hieronder in trefwoorden weergegeven in tabel 5, waarbij de naamgeving enigszins is aangepast aan meer gangbare termen voor functieprofielen. De vier processtappen van de cyclus worden in het Nederlands aangeduid met: Beleid - Implementatie - Evaluatie - Onderhoud. Daar wordt Leidinggeven als extra resultaatgebied aan toegevoegd.

Resultaatgebied	Kernbegrippen in taakstelling
Beleid (Plan)	- Opstellen IB-strategie en -architectuur - Ontwikkelen IB-normenkaders en -uitvoeringsvoorschriften - Maken informatiebeveiligingsplan
Leidinggeven	- Functioneel leidinggeven - Optreden als projectleider IB-projecten
Implementeren (Do)	- Implementatie IB-maatregelen (alleen TISS) - Adviseren en toezien op implementatie IB-maatregelen - Bevorderen IB-bewustzijn - Uitvoeren risicoanalyse
Evalueren (Check)	- Toezien dat interne controle en audits plaatsvinden en bevindingen worden opgelost - Uitvoeren eigen onderzoek - Afhandelen informatiebeveiligingsincidenten
Onderhouden (Act)	- Aanpassen Beleid - Aanpassen (adviezen) Implementeren IB-maatregelen

Tabel 5 Taakoverzicht op hoofdlijnen per resultaatgebied

In het navolgende hoofdstuk worden de functieprofielen van de in dit visiedocument onderkende IB-functies nader uitgewerkt.

6.2 Functiemodel

Naast de hiervoor besproken resultaatgebieden als de kern van het functieprofiel wordt daaraan voorafgaand het doel van de functie in één regel gedefinieerd, aangegeven aan welke functie er in principe wordt gerapporteerd en de functiecontext weergegeven. Met dit laatste wordt de functie in zijn omgeving gepositioneerd en de belangrijkste functiebestanddelen en eventuele bijzondere omstandigheden kort aangeduid.

De resultaatgebieden worden op basis van tabel 5 kernachtig uitgewerkt en aangevuld met een opsomming van de interne en externe contacten, die door de functie worden onderhouden. Tenslotte worden de competenties in termen van opleidingsniveau, vereiste kennisgebieden en vaardigheden uitgewerkt. De vaardigheden, die voor het geheel aan IB-functies relevant zijn, worden in de bijlage nader toegelicht. De functieprofielen zijn in Word-formaat te downloaden van de websites www.gvib.nl en www.pi4ib.nl

6.3 Functieprofielen

Functienaam: Chief Information Security Officer (CISO) | **Afdeling:** Concernstaf | **Rapporteert aan:** lid concerndirectie			
Doel van de functie	Het ontwikkelen van strategie en beleid gericht op informatiebeveiliging. Bevorderen en coördineren van de ontwikkeling van uitvoeringsrichtlijnen en toezien op de realisatie van het beleid.		
Functiecontext	Functioneert als zelfstandig opererend intern beleidsadviseur, ressorterend onder het lid van het concern management-team verantwoordelijk voor informatiebeveiliging. Geeft functioneel leiding aan informatiebeveiligingsmedewerkers in de gehele organisatie door het geven van richtlijnen en sturing op interne rapportages over de uitvoering van het informatiebeveiligingsbeleid en het naleven van uitvoeringsrichtlijnen. Moet weerstand overwinnen om het beleid en richtlijnen te laten naleven, die vaak als belemmerend worden ervaren in de uitvoering van het werk.		
Resultaatgebieden	Beleid - Vormt zich een visie op de betekenis van informatiebeveiliging voor het concern door voortdurende beeldvorming over risico's en oplossingsrichtingen voor maatregelen passend bij het concernbeleid. - Stelt doelen voor informatiebeveiliging voor. - Ontwikkelt een strategie om die doelen te bereiken. - Ontwikkelt beleid ter uitvoering van de strategie en stelt concernbeleids- en jaarplan samen mede op basis van de deelplannen informatiebeveiliging. Leidinggeven - Geeft functioneel leiding aan Information Security Officers en Information Security Manager. - Treedt op als projectleider of opdrachtgever voor concernbrede projecten op het gebied van informatiebeveiliging. - Organiseert en faciliteert concernoverleg voor sturing en coördinatie op het gebied van informatiebeveiliging. Implementeren - Bevordert het ontwikkelen van uitvoeringsrichtlijnen en geeft hieraan richting. - Initieert voorlichtings- en IB-bewustzijnsprogramma's en geeft hieraan richting. - Initieert en faciliteert risicoanalyses op concernniveau. - Toetst uitvoeringsrichtlijnen aan het beleid en adviseert zonodig over verbetering. - Bereidt concernbeslissingen op het gebied van informatiebeveiliging voor. - Adviseert de leiding van concern, Business Units en ICT bij beleid(sbeslissingen) met consequenties voor informatiebeveiliging. Evalueren - Beoordeelt rapportages van Information Security Officers en Information Security Manager over de naleving van uitvoeringsrichtlijnen. - Beoordeelt rapportages van in- en externe auditinstanties op relevantie voor informatiebeveiliging. - Geeft opdrachten tot het verrichten van interne onderzoeken en audits. - Houdt een centrale registratie bij van informatiebeveiligingsincidenten en de afhandeling. - Beoordeelt ontwikkelingen in de maatschappij, de branche en het vakgebied. Onderhouden - Stelt IB-visie, -strategie en -beleid bij en bevordert aanpassing van uitvoeringsrichtlijnen op basis van evaluaties. Contacten - Intern: concernleiding, concernstaf, leiding Business Units en ICT, tactische IB-functies. - Extern: auditors, branche- en beroepsgenoten.		
Competenties	Werk- en denkniveau - Master Kennisgebieden - ICT en informatiebeveiliging (breed) - Organisatie van informatievoorziening - Business processen (breed)	**Vaardigheden**	- Integriteit - Leiderschap - Omgevingsbewustzijn - Organisatiesensiviteit - Overtuigingskracht - Stressbestendigheid - Visie

<table>
<tr><th colspan="4">Functienaam: Information Security Officer (ISO) | Afdeling: Business Unit | Rapporteert aan: lid management team of hoofd Business Unit</th></tr>
<tr><td>Doel van de functie</td><td colspan="3">Het ontwikkelen van beleid gericht op het naleven van concernkaders voor informatiebeveiliging, ondersteunen van het management hierbij en toezien op de realisatie van het beleid.</td></tr>
<tr><td>Functiecontext</td><td colspan="3">Functioneert namens het management van de Business Unit als zelfstandig adviseur op het gebied van informatiebeveiliging. Houdt toezicht op het naleven van uitvoeringsrichtlijnen. Moet weerstand overwinnen om het beleid en richtlijnen te laten naleven, die vaak als belemmerend worden ervaren in de uitvoering van het werk.</td></tr>
<tr><td>Resultaatgebieden</td><td colspan="3">Beleid
- Stelt jaarlijks het informatiebeveiligingsplan voor de Business Unit op.
- Draagt bij aan concern beleidsplannen voor informatiebeveiliging vanuit het perspectief van de Business Unit.
Leidinggeven
- Geeft eventueel functioneel of direct leiding aan Local Information Security Officers.
Implementeren
- Draagt uitvoeringsrichtlijnen op het gebied van informatiebeveiliging actief uit in de organisatie.
- Adviseert over uitvoeringsrichtingen op het gebied van informatiebeveiliging.
- Initieert voorlichtings- en IB-bewustzijnsprogramma's en geeft hieraan richting.
- Voert risicoanalyses uit binnen zijn competentiegebied.
- Adviseert het management bij besluitvorming met gevolgen voor informatiebeveiliging.
Evalueren
- Beoordeelt interne rapportages.
- Beoordeelt rapportages van in- en externe controle en auditinstanties.
- Adviseert het management inzake het verrichten van interne onderzoeken en audits.
- Houdt een registratie bij van informatiebeveiligingsincidenten en beoordeelt de afhandeling.
Onderhouden
- Stelt het IB-jaarplan bij op basis van zijn evaluaties.
Contacten
- Intern: management Business Unit op alle geledingen, eigen Business Information Security Architect, Chief Information Security Officer en andere Information Security Officers.
- Extern: auditors.</td></tr>
<tr><td>Competenties</td><td>Werk- en denkniveau
- Bachelor
Kennisgebieden
- Informatiebeveiliging
- Business processen
- Interne regelgeving</td><td>Vaardigheden</td><td>- Doorzettingsvermogen
- Integriteit
- Organisatiesensitiviteit
- Overtuigingskracht
- Voortgangsbewaking</td></tr>
</table>

Functienaam: Business Information Security Architect (BISA) | **Afdeling:** Business Unit (evt. Concern) **Rapporteert aan:** lid management team Business Unit of Hoofd Business Process Management			
Doel van de functie	Het ontwikkelen en actueel houden van een visie of deelarchitectuur voor het aspect informatiebeveiliging in de enterprise of procesarchitectuur als concretisering van een deel van het strategisch IB-beleid en de positionering van generieke beveiligingsfunctionaliteiten daarbinnen.		
Functiecontext	Procesarchitect met als specialisatie informatiebeveiliging. Vertaalt beleidskaders voor informatiebeveiliging naar enterprise of procesarchitectuur en vervult daarbij zowel een architecten- als adviseursrol. Treedt met name op als procesarchitect voor generieke beveiligingsfunctionaliteiten, bijvoorbeeld op het gebied van logische toegangsbeveiliging, encryptie, logging en auditing. Ziet toe op naleving van architectuurprincipes voor informatiebeveiliging. Houdt voortdurend zicht op marktontwikkelingen op het gebied van informatiebeveiligingsproducten.		
Resultaatgebieden	<u>Beleid</u> - Vormt zich een visie op de betekenis van informatiebeveiliging in het kader van de enterprise of procesarchitectuur en houdt daarbij rekening met de concernstrategie voor informatiebeveiliging. - Draagt bij aan de concernstrategie voor informatiebeveiliging vanuit het perspectief van procesontwikkeling. - Draagt bij aan de beleidsvorming en jaarplannen ter uitvoering van deze strategie binnen zijn competentiegebied. <u>Leidinggeven</u> - Treedt op als projectleider voor projecten op het gebied van informatiebeveiliging. <u>Implementeren</u> - Ontwerpt zelfstandig deelarchitectuur van de enterprise of procesarchitectuur voor het domein informatiebeveiliging of draagt bij aan het expliciet maken van het aspect informatiebeveiliging als integraal onderdeel van deze architectuur. - Voert risicoanalyses uit binnen zijn competentiegebied. - Toetst procesontwerpen aan architectuuruitgangspunten voor informatiebeveiliging en adviseert zonodig over verbetering van die ontwerpen. - Toetst ontwerpen voor generieke beveiligingsfunctionaliteiten aan architectuuruitgangspunten voor informatiebeveiliging en adviseert zonodig over verbetering van die ontwerpen. <u>Evalueren</u> - Beoordeelt procesmatige ontwikkelingen in de bedrijfsvoering met mogelijke gevolgen voor IB-aspecten. - Beoordeelt IT-audit rapportages, rapportages over informatiebeveiligingsincidenten en gebruikersevaluaties van generieke beveiligingsfunctionaliteiten. <u>Onderhouden</u> - Draagt zorg voor het bijstellen van het aspect informatiebeveiliging in de enterprise of procesarchitectuur of implementaties daarvan op basis van zijn evaluaties. <u>Contacten</u> - Intern: enterprise/procesarchitecten, procesontwerpers, informatiemanagers, projectleiders voor procesmatige vernieuwingen, andere IB-functies, IT-auditors. - Extern: branche- en beroepsgenoten.		
Competenties	<u>Werk- en denkniveau</u> - Master <u>Kennisgebieden</u> - ICT en informatiebeveiliging - Organisatie van informatievoorziening - Architectuurprincipes - Business processen (breed en diep)	**Vaardigheden**	- Analytisch vermogen - Creativiteit - Initiatief - Omgevingsbewustzijn - Organisatiesensitiviteit - Samenwerken - Visie

Functienaam: Information Security Manager (ISM) | **Afdeling:** ICT | **Rapporteert aan:** lid managementteam of Hoofd ICT			
Doel van de functie	Het ontwikkelen van beleid gericht op informatiebeveiliging binnen de ICT-organisatie, ondersteunen van management, zorgdragen voor de ontwikkeling van uitvoeringsrichtlijnen en toezien op de realisatie van het beleid.		
Functiecontext	Functioneert namens het ICT-management als zelfstandig en breed opererend adviseur en toezichthouder op het gebied van informatiebeveiliging. Geeft functioneel leiding aan informatiebeveiligingsmedewerkers in de ICT-organisatie door het geven van richtlijnen en sturing op interne rapportages over de uitvoering van het informatiebeveiligingsbeleid en het naleven van uitvoeringsrichtlijnen. Moet weerstand overwinnen om het beleid en richtlijnen te laten naleven, die vaak als belemmerend worden ervaren in de uitvoering van het werk.		
Resultaatgebieden	Beleid - Stelt jaarlijks het informatiebeveiligingsplan voor de ICT-organisatie op. - Draagt bij aan de concernstrategie en -beleidsplannen voor informatiebeveiliging vanuit het perspectief van de ICT-organisatie. Leidinggeven - Geeft eventueel functioneel of direct leiding aan andere IB-functies binnen de ICT-organisatie. - Organiseert en faciliteert overleg om maatregelen en evaluaties binnen de ICT-organisatie op het gebied van informatiebeveiliging op elkaar af te stemmen. Implementeren - Draagt zorg voor actuele uitvoeringsrichtlijnen op het gebied van informatiebeveiliging. - Initieert voorlichtings- en IB-bewustzijnsprogramma's en geeft hieraan richting. - Voert risicoanalyses uit binnen zijn competentiegebied en op concernniveau als vertegenwoordiger van de ICT-organisatie. - Adviseert de leiding van de ICT-organisatie bij besluitvorming met gevolgen voor informatiebeveiliging. - Ziet toe op navolging adviezen/controlebevindingen bij certificeringsprocessen. Evalueren - Beoordeelt afdelings- en procesrapportages binnen de ICT-organisatie. - Beoordeelt rapportages van in- en externe controle en auditinstanties. - Geeft opdrachten tot het verrichten van interne onderzoeken en audits. - Beoordeelt of participeert in de afhandeling van informatiebeveiligingsincidenten. Onderhouden - Stelt het IB-jaarplan en IB-uitvoeringsrichtlijnen bij op basis van zijn evaluaties. Contacten - Intern: concernleiding, concernstaf, leiding Business Units en ICT, andere IB-functies. - Extern: auditors, branche- en beroepsgenoten.		
Competenties	Werk- en denkniveau - Master Kennisgebieden - ICT en informatiebeveiliging - Organisatie van informatievoorziening - ITIL	**Vaardigheden**	- Doorzettingsvermogen - Integriteit - Leiderschap - Overtuigingskracht - Organisatiesensitief - Omgevingsbewustzijn

Functienaam: Information Security Architect (ISA) **| Afdeling:** ICT | **Rapporteert aan:** hoofd Systeemontwikkeling/Architectuur			
Doel van de functie	Het ontwikkelen en actueel houden van het aspect informatiebeveiliging binnen de ICT-architectuur dat zowel gericht is op het voldoen aan het IB-beleid en de IB-voorschriften als op de generieke beveiligingsfunctionaliteiten binnen de technische infrastructuur. Daarbij hoort het toepasbaar maken van deze architectuur op hoofdlijnen (systeemschets) van het ontwerp en het onderhoud van de generieke beveiligingsfunctionaliteiten.		
Functiecontext	ICT-architect met als specialisatie informatiebeveiliging in relatie tot ICT. Vertaalt beleidskaders voor informatiebeveiliging naar ICT-architecturen en vervult daarbij zowel een architect- als adviseursrol. Treedt met name op als ICT-architect voor generieke beveiligingsfunctionaliteiten, bijvoorbeeld op het gebied van logische toegangsbeveiliging, encryptie, logging- en auditing. Ziet toe op naleving van architectuurprincipes voor informatiebeveiliging. Houdt voortdurend zicht op marktontwikkelingen op het gebied van informatiebeveiligingsproducten.		
Resultaatgebieden	Beleid - Vormt zich een visie op de betekenis van informatiebeveiliging voor ICT vanuit de concernstrategie door voortdurende beeldvorming over risico's en oplossingsrichtingen voor maatregelen passend bij het concernbeleid. - Draagt bij aan de concernstrategie voor ICT in relatie tot informatiebeveiliging. - Draagt bij aan de beleidsvorming en jaarplannen ter uitvoering van deze strategie binnen zijn competentiegebied. Leidinggeven - Treedt op als projectleider voor projecten op het gebied van informatiebeveiliging. Implementeren - Ontwerpt zelfstandig deelarchitectuur van het ICT-complex voor het domein informatiebeveiliging of draagt bij aan het expliciet maken van het aspect informatiebeveiliging als integraal onderdeel van de ICT-architecturen. - Treedt op als ICT-architect voor generieke beveiligingsfunctionaliteiten. - Toetst ICT-ontwerpen aan architectuuruitgangspunten voor informatiebeveiliging en adviseert zonodig over verbetering van die ontwerpen. Evalueren - Beoordeelt ontwikkelingen in de ICT-markt t.a.v. nieuwe IB-risico's en generieke oplossingen van leveranciers. - Beoordeelt interne ontwikkelingen binnen de ICT met mogelijke gevolgen voor IB-aspecten in de ICT. - Beoordeelt IT-audit rapportages, rapportages over informatiebeveiligingsincidenten en gebruikersevaluaties van generieke beveiligingsfunctionaliteiten. Onderhouden - Draagt zorg voor het bijstellen van het aspect informatiebeveiliging in ICT-architecturen op basis van zijn evaluaties. Contacten - Intern: ICT-architecten, ICT-ontwerpers, projectleiders ICT, andere IB-functies, IT-auditors. - Extern: ICT-leveranciers en beroepsgenoten.		
Competenties	Werk- en denkniveau - Master Kennisgebieden - ICT en informatiebeveiliging - Architectuurprincipes - Standaards inzake informatiebeveiliging	**Vaardigheden**	- Analytisch vermogen - Creativiteit - Initiatief - Omgevingsbewustzijn - Samenwerken - Visie

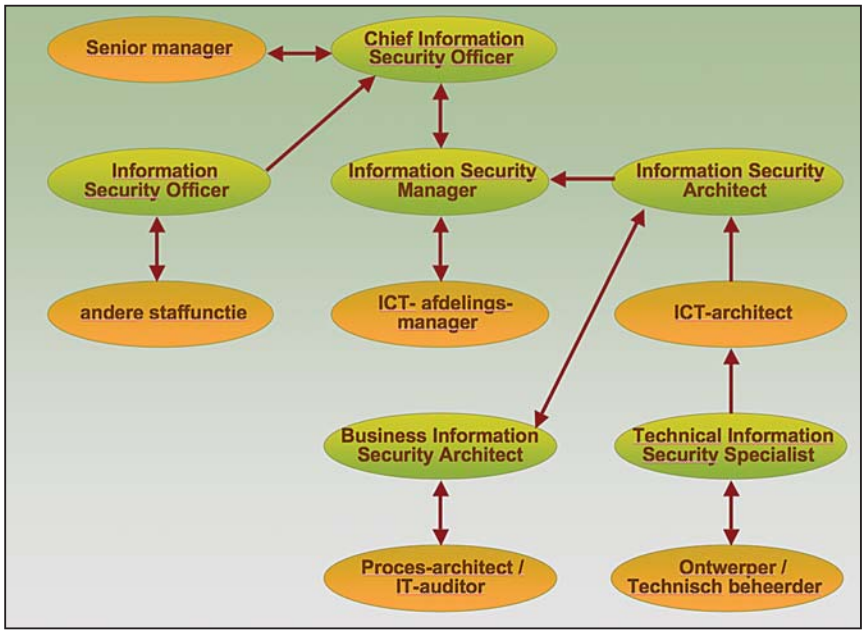
Functienaam: Technical Information Security Specialist (TISS) **| Afdeling:** ICT | **Rapporteert aan:** afhankelijk van plaats tewerkstelling			
Doel van de functie	Het verrichten van ontwikkel-, beheer- of advieswerkzaamheden in een ICT-organisatie, die vragen om een diepgaande technische kennis van ICT en informatiebeveiliging.		
Functiecontext	Deze functie kan veel verschillende verschijningsvormen hebben en kan hier slechts in algemene zin worden geduid. De betekenis van de functie hangt nauw samen met de wijze waarop deze in de ICT-organisatie wordt ingezet en waar de stand van de techniek en de bedrijfs- of ICT-typologie om vraagt. De kern van de functie betreft de deskundigheid om op het snijvlak van ICT-techniek en informatiebeveiliging te opereren. Zowel als ontwerper, adviseur of implementeerder van (generieke) beveiligingsfunctionaliteiten, als bij het dagelijkse beheer van complexe omgevingen waarbij een hoog niveau van informatiebeveiliging moet worden gehandhaafd. Beveiligingsfunctionaliteiten kunnen betrekking hebben op logische toegangsbeveiliging, encryptie, logging en auditing, bescherming van netwerken tegen indringers of malware, incidentafhandeling, live testen van de robuustheid van beveiliging en dergelijke.		
Resultaatgebieden	Beleid - Niet van toepassing. Leidinggeven - Niet van toepassing. Implementeren - Ontwerpt of beheert zelfstandig informatiebeveiligingsaspecten van de technische infrastructuur of (generieke) informatiebeveiligingsfunctionaliteiten daarin. - Adviseert over het implementeren van informatiebeveiligsaspecten van de technische infrastructuur of (generieke) informatiebeveiligingsfunctionaliteiten. Evalueren - Voert zelfstandig live testen uit om vast te stellen of er zich leemten m.b.t. de informatiebeveiliging voordoen in de technische infrastructuur, al dan niet in combinatie met toepassingssoftware, voor zover hij niet is betrokken bij het ontwerp, implementatie of beheer van de te testen omgeving. - Is betrokken bij het analyseren en afhandelen van informatiebeveiligingsincidenten. Onderhouden - Draagt er zorg voor dat ontstane leemten blijkend uit informatiebeveiligingsincidenten en -testen worden opgelost. Contacten - Intern: ICT-architecten, -projectleiders, -ontwerpers en -beheerders, andere IB-functies. - Extern: ICT-leveranciers.		
Competenties	Werk- en denkniveau - Bachelor Kennisgebieden - ICT en informatiebeveiliging - ICT Platformen - Technische standaards voor informatiebeveiliging	**Vaardigheden**	- Analytisch vermogen - Creativiteit - Doorzettingsvermogen - Kwaliteitsgerichtheid - Leervermogen - Resultaatgerichtheid

6.4 Groeipaden

Bij de IB-functies zijn drie niveaus onderscheiden (strategisch, tactisch, operationeel), en de focus kan liggen op business of op ICT. Hierdoor zijn er binnen de functies groeipaden te onderkennen. Daarnaast is het ook van belang na te gaan welke andere functies in aanmerking komen voor doorstroming naar de IB-functies en omgekeerd. Omdat informatiebeveiliging een breed vakgebied is waarbij overal in de organisatie contacten moeten worden onderhouden, kan het aantrekkelijk zijn om een IB-functie te vervullen als onderdeel van een carrièrepad.

Daarbij hoeft het natuurlijk niet altijd om bevordering naar een hogere functie te gaan: horizontale doorstroming kan eveneens aan de orde zijn, waarbij informatiebeveiliging verbreding van de horizon kan geven.

Een aantal voor de hand liggende groeipaden is opgenomen in figuur 9. Daarbij kan opgemerkt worden dat het voor een IB-functie interessant kan zijn om zich op andere objectgebieden binnen dezelfde soort functie te gaan richten, waardoor hij breder gaat functioneren. Ook kan het vervullen van een ander soort IB-functie een tussenstap zijn om naar een heel andere functie te groeien, bijvoorbeeld als een Information Security Architect met belangstelling voor de managementkant eerst een functie als Information Security Manager gaat vervullen om vervolgens door te groeien naar een algemene managementfunctie binnen ICT.



Figuur 8 Resultaatgebieden in het proces informatiebeveiliging.

Afhankelijk van zijn afkomst zal de in- of doorstromer naar IB-functies extra kwalificaties moeten ontwikkelen. In Tabel 6 is daarvan een overzicht opgenomen.

IB-functie	afkomst	ontwikkelrichting
Chief Information Security Officer	Senior manager	oriënteren op informatiebeveiliging
	Information Security Manager	oriënteren op de business en/of concern
Information Security Officer	andere staffunctie	oriënteren op informatiebeveiliging
Business Information Security Architect	procesarchitect	oriënteren op informatiebeveiliging
	IT-auditor	oriënteren op architectuur
Information Security Manager	ICT-afdelingsmanager	oriënteren op informatiebeveiliging
	Information Security Architect	oriënteren op ICT-processen (ITIL) en -organisatie
	Business Information Security Architect	oriënteren op ICT-processen (ITIL) en -organisatie
Information Security Architect	ICT-architect	oriënteren op informatiebeveiliging
	Technical Information Security Specialist	als ontwerper: oriëntatie op architectuur en evt. verbreden kennis informatiebeveiliging
Technical Information Security Specialist	ontwerper/ technisch beheerder	oriënteren op informatiebeveiliging

Tabel 6 Groeipaden en ontwikkelrichting

Voor opleidingsdoeleinden kan een tweetal oriëntatielijnen voor de IB-functies onderkend worden. Het betreft enerzijds de organisatie- en management-gerichte oriëntatie, de managementrichting, en anderzijds de meer specialistische ICT-oriëntatie. Daarnaast zouden de functies op verschillende niveaus moeten worden uitgevoerd. In Tabel 7 zijn de IB-functies op deze oriëntaties en niveaus uitgesplitst.

Type onderwijs	Management gericht	Technisch gericht
Master	Chief Information Security Officer	Information Security Architect
	Information Security Manager	
	Business Information Security Architect	
Bachelor	Information Security Officer	Technical Information Security Specialist

Tabel 7 Oriëntatie op het onderwijs.

De functieprofilering zoals in dit visiedocument uitgewerkt, is nieuw. Dat betekent dat afstemming van deze profielen met het onderwijsaanbod nog niet heeft plaatsgevonden.
Gezien de dynamiek in het onderwijsveld wordt in het visiedocument nog geen overzicht opgenomen van de onderwijsinstellingen met hun aanbod voor informatiebeveiligingsopleidingen. Dit wordt als een vervolgstap gezien, waarvan het doelmatiger is de resultaten hiervan op de verenigingswebsite te plaatsen, zodat het overzicht eenvoudiger actueel kan worden gehouden. Daarbij kan tevens worden gezorgd voor genoemde afstemming tussen profielen en onderwijsaanbod.

Analytisch vermogen	In staat zijn om vraagstukken op een systematische manier te onderzoeken. Maakt onderscheid tussen hoofd- en bijzaken. Verbanden kunnen leggen, oorzaken kunnen opsporen en informatie verwerken tot hanteerbare eenheden.
Besluitvaardigheid	Keuzen maken op basis van informatie en ervaring. Het afwegen van de voor- en nadelen van een beslissing. Zich vastleggen door middel van het uitspreken van meningen.
Creativiteit	Met oorspronkelijke ideeën komen voor vraagstukken die met de functie verband houden. Zich met een onderzoekende en nieuwsgierige geest richten op toekomstige vernieuwing van strategie, producten, diensten en markten.
Doorzettingsvermogen	Zich gedurende langere tijd intensief met een taak bezig kunnen houden, ook bij tegenslag. Volharden in een plan totdat het beoogde doel bereikt is.
Leiderschap	Het stimuleren, motiveren, beïnvloeden en begeleiden van anderen bij het bereiken van doelen: doelen stellen, richtinggeven.
Initiatief	Alert zijn en anticiperen op kansen, nieuwe situaties of problemen en er in een vroeg stadium naar handelen. Zelf actie ondernemen.
Integriteit	Handhaven van algemeen aanvaarde sociale en ethische normen in activiteiten die met de functie te maken hebben.
Kwaliteitsgerichtheid	Gericht zijn op het leveren van goede producten en diensten en waar mogelijk het verbeteren van de kwaliteit van producten en diensten.
Leervermogen	Nieuwe informatie en ideeën snel kunnen opnemen, analyseren en verwerken en deze effectief kunnen toepassen in de werksituatie.
Omgevingsbewustzijn	Laten blijken goed geïnformeerd te zijn over organisatorische, maatschappelijke en politieke ontwikkelingen of andere omgevingsfactoren (binnen of buiten de organisatie).
Organisatiesensitiviteit	Waarnemen van en zicht hebben op de invloed en de gevolgen van beslissingen en gedragingen van mensen in een organisatie.
Overtuigingskracht	Gedrag dat erop gericht is anderen te overtuigen van een bepaald standpunt en instemming te krijgen met bepaalde plannen, ideeën of zaken.
Resultaatgerichtheid	Zich ondanks problemen, tegenslag, tegenwerking of afleidingen blijven richten op het bereiken van het doel.
Samenwerken	Bijdragen aan een gezamenlijk resultaat door een optimale afstemming tussen de eigen kwaliteiten en belangen en die van de groep/de ander.
Visie	Een richtinggevend toekomstbeeld op hoofdlijnen voor de organisatie / afdeling / producten / diensten ontwikkelen en uitdragen.
Voortgangsbewaking	Opstellen, volgen en uitvoeren van procedures om de goede voortgang van processen, taken of activiteiten van medewerkers en van zichzelf zeker te stellen.

'Beveiliging moet los van IT', Tijdschrift CIO IT-strategie voor managers, IDG Communications Nederland, jaargang 2, nummer 4, april 2003

Bokhorst Bart, *Functies in de informatiebeveiliging, een visie op ordening, deel 1 en 2* , Informatiebeveiliging 7 (2004) en Informatiebeveiliging 1 (2005)

Cazemier Jacques A, Overbeek Paul, e.a. (1999), *Security Management,* CCTA

Coul J. C. op de (2001), *Taken, functies, rollen en competenties in de informatica*, Den Haag

Dunn Lex, Kuiper Renato (2003), *Security-architectuur, modekreet of bruikbaar?*, Informatiebeveiliging 8

ECABO (2004), *Beroepscompetentieprofiel* Digitaal Rechercheur, www.ecabo.nl

GvIB, Expertbrief *'Functies en rollen in de informatiebeveiliging'*, maart 2005

GvIB, Expertbrief *'Het inrichten van een beveiligingsorganisatie*', juli 2006

Hoek Cobie van der, Koppen Leo van, Spruit Marcel (2004), *Competenties van de Informatiebeveiliger*, Tinfon 4

Nederlands Genootschap van Functionarissen voor de Gegevensbescherming, *'Informatieblad - Taken van de FG'*, december 2005, www.ngfg.nl

NEN, *Nederlandse norm NEN-ISO/IEC 17799 (nl) Code voor informatiebeveiliging (ISO/IEC17799:2005)*

Oud Ernst J., *Praktijkgids Code voor Informatiebeveiliging*, november 2002, pp.107/108

Overbeek Paul, Roos Lindgreen Edo, Spruit Marcel (2000), *Informatiebeveiliging onder controle*, Pearson Education

Stichting SURF (december 2005), *Leidraad functieprofiel Informatiebeveiliger in het hoger onderwijs*

Figuren

Tabellen

APPENDIX GEBRUIKTE LICENTIEVORM

Dit visiedocument wordt gepubliceerd onder de volgende licentie:
http://creativecommons.org/licenses/by-sa/2.5/

creative commons

COMMONS DEED

Attribution-ShareAlike 2.5

You are free:

- to copy, distribute, display, and perform the work
- to make derivative works
- to make commercial use of the work

Under the following conditions:

BY: **Attribution.** You must attribute the work in the manner specified by the author or licensor.

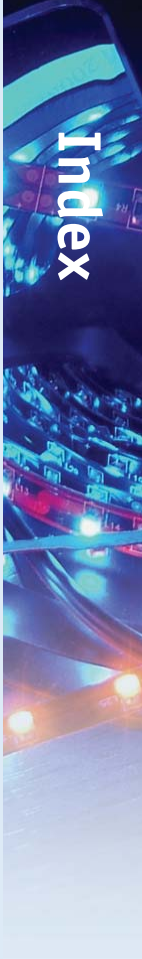
Share Alike. If you alter, transform, or build upon this work, you may distribute the resulting work only under a license identical to this one.

- For any reuse or distribution, you must make clear to others the license terms of this work.
- Any of these conditions can be waived if you get permission from the copyright holder.

Your fair use and other rights are in no way affected by the above.

This is a human-readable summary of the Legal Code (the full license).

Disclaimer



Begrippen

Functies in de informatiebeveiliging is een uitgave van:

Genootschap van Informatie Beveiligers

www.gvib.nl

Platform Informatiebeveiliging

www.pi4ib.nl

ISBN-10: 90-78786-01-9
ISBN-13: 978-90-78786-01-6