Leidraad
Functieprofiel Informatiebeveiliger in het Hoger Onderwijs

Deze leidraad is opgesteld door SURF-IBO.
December 2005

SURF-IBO

Het SURF Informatie Beveiligers Overleg is ingesteld door het platform SURF ICT en Organisatie met als doelen het actief stimuleren van en richting geven aan informatiebeveiliging binnen het hoger onderwijs (universiteiten, hogescholen en universitair medische centra).
Dat wordt bereikt door het bevorderen van de samenwerking tussen informatiebeveiligers en het leveren van praktisch bruikbare adviezen.

Meer informatie over SURF-IBO staat op www.surf.nl onder het thema informatiebeveiliging.

Voor meer informatie over de leidraad kan contact worden opgenomen met de secretaris van SURF-IBO, Anita Polderdijk (am.polderdijk-rijntjes@windesheim.nl of 038-4699076).

Inhoudsopgave

Voorwoord

In het hoger onderwijs en onderzoek wordt op grote schaal van ICT gebruik gemaakt. Hierbij doet zich met betrekking tot de informatiebeveiliging een spanningsveld voor. Het onderwijs en onderzoek zelf is gebaat bij een zo groot mogelijke openheid en vrijheid met zo min mogelijk belemmeringen en regels. De bedrijfsprocessen van de instellingen, ook die van onderwijs en onderzoek, stellen echter de nodige eisen aan beveiliging. Door de toegenomen beschikbaarheid en de uiteenlopende toepassingen van ICT is de complexiteit toegenomen. De risico's van inbreuken op de informatievoorziening worden al maar groter, waardoor ook de wet- en regelgeving wordt aangescherpt. Dit alles vereist dat extra maatregelen worden genomen op het gebied van informatiebeveiliging. Om vervolgens toch iedere student en medewerker ongehinderd van de ICT-faciliteiten gebruik te kunnen laten maken is het noodzakelijk hierover regels af te spreken en na te komen.

Het SURF Platform ICT en organisatie acht het zijn taak hierin stimulerend en faciliterend op te treden. Samenwerking tussen de instellingen en bundeling van krachten versterken het proces van verbetering van de informatiebeveiliging.
Het SURF informatiebeveiligers overleg (SURF-IBO) is het platform voor uitwisseling van kennis en ervaring op het gebied van informatiebeveiliging. Hierbij ligt de nadruk op het delen van ervaringen door vanuit "best practices" tot praktische adviezen te komen. Voor belangrijke onderwerpen worden kennis en ervaring gebundeld in een leidraad, die instellingen kan ondersteunen bij het verbeteren van de informatiebeveiliging.
Van harte beveel ik dan ook de leidraad "Functieprofiel Informatiebeveiliger in het Hoger Onderwijs" van SURF-IBO in uw aandacht aan. Deze kan gebruikt worden bij het inrichten van de informatiebeveiligingsfunctie binnen uw instelling .

Verder zou ik iedere instelling binnen het hoger onderwijs willen oproepen om regelmatig een deelnemer af te vaardigen naar bijeenkomsten van SURF-IBO.

Willem Kardux,
voorzitter platform ICT & Organisatie

1 Inleiding

1.1 Aanleiding

SURF ICT en Organisatie heeft in 2003 een inventariserend onderzoek gedaan naar de informatiebeveiligingsfunctie binnen het hoger onderwijs. Een belangrijke aanbeveling betrof de inrichting van een beveiligingsorganisatie, waarbij taken, verantwoordelijkheden en bevoegdheden ten aanzien van het beveiligen van informatie duidelijk zijn belegd. Het nog verder verbeteren van de samenwerking met collega's bij andere instellingen, was ook een belangrijke aanbeveling. Aan dat laatste is concreet gestalte gegeven door de oprichting van het SURF Informatie Beveiligers Overleg. Binnen SURF-IBO blijkt dat de invulling die de diverse deelnemende instellingen geven aan de functie informatiebeveiliger, op het eerste gezicht nogal divers is. Ook de functiebenaming loopt sterk uiteen. Sommige instellingen hebben meer dan één informatiebeveiliger in dienst, andere kennen de functie in het geheel niet.
Voldoende aanleiding om een leidraad te schrijven.

1.2 Doelstelling

Doel van deze leidraad is het verzamelen en structureren van de beschikbare informatie over de functie informatiebeveiliger. Daarmee wil de leidraad een handvat bieden aan degenen die, binnen een instelling voor hoger onderwijs, een informatiebeveiligersfunctie willen instellen of verder gestalte willen geven.
Er is zowel binnen als buiten het hoger onderwijs veel materiaal beschikbaar. Misschien te veel, waardoor het niet eenvoudig is om te weten waar en hoe te beginnen. En, nog een stap terug, of het eigenlijk wel noodzakelijk is een informatiebeveiliger aan te stellen. En zo ja, hoe moet het functieprofiel er dan uit zien? En wat wordt de functiebenaming?
Bij al deze vragen is de leidraad een hulpmiddel om tot een verantwoorde afweging te komen.

1.3 Doelgroep

De leidraad is in eerste instantie bestemd voor degenen binnen een instelling die beslissen of en in welke vorm er een informatiebeveiligersfunctie komt. Uiteindelijk is dat het College van Bestuur of de Raad van Bestuur. Maar personeelszaken en management zullen daarbij een belangrijke adviserende en voorbereidende rol hebben.
In tweede instantie vormt de leidraad een hulpmiddel om te komen tot concrete invulling van de functie. Personeelszaken en management vinden in de leidraad concrete punten waarmee een gewenst functieprofiel kan worden samengesteld.
De beoogde of aangestelde informatiebeveiliger vindt aanknopingspunten om de functie in de praktijk handen en voeten te geven.

1.4 Afbakening

De leidraad is bedoeld, het woord zegt het al, als leidraad om te komen tot een functieprofiel informatiebeveiliger. Het basisprofiel is naar het oordeel van SURF-IBO in principe altijd toepasbaar. Verder bevat de leidraad aanknopingspunten om de functie op gewenste punten aan te scherpen. Naar onze mening zijn alle aandachtspunten die van belang zijn bij het komen tot een functieprofiel informatiebeveiliger in de leidraad opgenomen.

Een functieprofiel informatiebeveiliger zal tot op zekere hoogte echter altijd instellingsspecifiek zijn. Het opzetten van een profiel is op zichzelf een belangrijk proces waardoor een instelling scherp krijgt waar de behoefte van de eigen organisatie ligt. De leidraad zorgt ervoor dat daarbij geen zaken worden vergeten en brengt u wellicht op ideeën.

1.5 Werkwijze en leeswijzer

Bij het opstellen van de leidraad zijn wij begonnen met een literatuurstudie. In **bijlage 3** staat een overzicht met daarbij per item een korte samenvatting.

Vervolgens hebben wij een vragenlijst (**bijlage 2**) opgesteld met als doel te inventariseren hoe de functie informatiebeveiliger op dit moment bij de diverse instellingen is vorm gegeven. Ook hebben wij vragen gesteld over de gewenste situatie. De vragenlijst is ingevuld door veertien leden van SURF-IBO. Verder hebben wij gebruik gemaakt van de inzichten van het Genootschap van Informatie Beveiligers (GvIB). Het GvIB kan gezien worden als de beroepsorganisatie van en voor informatiebeveiligers en is branche-onafhankelijk. Binnen het GvIB is een expertbrief opgesteld over functies in de informatiebeveiliging. Bij de Haagse Hogeschool is een opleidingenmarkt voor aanbieders van opleidingen op het gebied van informatiebeveiliging georganiseerd en er is een thema-avond gehouden waarin diverse functieprofielen (informatiebeveiligingsfunctionaris, security officer, security manager, en andere) zijn uitgewerkt. Uitkomst was dat er vooral verschil is in de functiebenaming en niet zozeer in takenpakket en benodigde kennis en ervaring.
Met voorgaande kennis is een basisfunctieprofiel (**bijlage 1**) opgesteld.
In **hoofdstuk 5** is het functieprofiel per onderdeel verder uitgewerkt.
Omdat we binnen het hoger onderwijs regelmatig worden geconfronteerd met de vraag of het aanstellen van een informatiebeveiliger nodig is, besteden we in **hoofdstuk 4** aan die vraag expliciet aandacht.
Ook wordt ingegaan op de stappen die vooraf (kunnen) gaan aan en leiden tot het opzetten van een functieprofiel informatiebeveiliger (**hoofdstuk 3**).
Maar we beginnen nog een stap terug met een korte inleiding over (de noodzaak van) informatiebeveiliging aan de hand van de Code voor Informatiebeveiliging (**hoofdstuk 2**).

De leidraad is besproken binnen SURF-IBO en is aangeboden aan het platformbestuur van SURF ICT en Organisatie.

2. (De Code voor)Informatiebeveiliging

De Code of Practice (in Nederland vertaald in de Code voor Informatiebeveiliging) is de algemeen geaccepteerde standaard volgens welke een organisatie informatiebeveiliging kan inrichten. De Code voor Informatiebeveiliging is internationaal geaccepteerd als ISO/IEC 17799 standaard.
In deze leidraad gaan we nog uit van de meest recente Nederlandse versie van de Code. Dit jaar (2005) is een nieuwe Engelse versie verschenen; deze zal binnenkort in het Nederlands worden vertaald.
De Code doet uitspraken over 'best practices' ten aanzien van informatiebeveiliging (zie kader 1, Waar begint informatiebeveiliging?).
In de Code komen een groot aantal onderwerpen aan de orde (zie kader 2, Onderwerpen /hoofdstukken). Al deze onderwerpen worden gerekend tot het 'domein' informatiebeveiliging. Het is dus logisch te veronderstellen dat de informatiebeveiliger (het aansturen van) de beveiligingsaspecten binnen al deze gebieden tot zijn/haar taakpakket mag/moet rekenen.

Waar begint informatiebeveiliging? **Kader 1**

Een aantal maatregelen kan worden beschouwd als basisprincipes, die een goed uitgangspunt bieden voor het implementeren van informatiebeveiliging. Ze zijn gebaseerd op essentiële wettelijke eisen of ze worden algemeen beschouwd als "best practice" voor informatiebeveiliging.
Tot de maatregelen die vanuit wettelijke oogpunt van essentieel belang zijn voor een organisatie, behoren:

a) intellectuele eigendomsrechten (zie **12.1.2**);
b) beveiliging van bedrijfsdocumenten (zie **12.1.3**);
c) bescherming van persoonlijke informatie (zie **12.1.4**).

Tot de maatregelen die worden beschouwd als "best practice" voor informatiebeveiliging behoren:

a) beleidsdocument voor informatiebeveiliging (zie **3.1.1**);
b) toewijzing van verantwoordelijkheden voor informatiebeveiliging (zie **4.1.3**);
c) opleiding en training voor informatiebeveiliging (zie **6.2.1**);
d) het rapporteren van beveiligingsincidenten (zie **6.3.1**);
e) continuïteitsbeheer (zie **11.1**).

Deze maatregelen gelden voor de meeste organisaties en in de meeste omgevingen. Er dient echter op te worden gewezen dat hoewel alle maatregelen in dit document belangrijk zijn, de relevantie van een maatregel altijd dient te worden vastgesteld in het licht van de specifieke risico's waarmee de organisatie worden geconfronteerd. Hoewel de bovengenoemde benadering dus wordt beschouwd als een goed uitgangspunt, komt zij niet in de plaats van het selecteren van maatregelen op basis van risicoanalyse.

Bron: Code voor Informatiebeveiliging

Onderwerpen / hoofdstukken **Kader 2**

3 Beveiligingsbeleid
3.1 Informatiebeveiligingsbeleid
3.1.1 Beleidsdocument voor informatiebeveiliging
3.1.2 Beoordeling en evaluatie
4 Beveiligingsorganisatie
4.1 De organisatorische infrastructuur van informatiebeveiliging
4.1.1 Managementforum voor informatiebeveiliging
4.1.2 Coördinatie van informatiebeveiliging
4.1.3 Toewijzing van verantwoordelijkheden voor informatiebeveiliging
4.1.4 Autorisatieproces voor IT-voorzieningen
4.1.5 Specialistisch advies over informatiebeveiliging

4.1.6 Samenwerking tussen organisaties
4.1.7 Onafhankelijke beoordeling van informatiebeveiliging
4.2 Beveiliging van toegang door derden
4.3 Uitbesteding
5 Classificatie en beheer van bedrijfsmiddelen
6 Beveiligingseisen ten aanzien van personeel
7 Fysieke beveiliging en beveiliging van de omgeving
8 Beheer van communicatie - en bedieningsprocessen
9 Toegangsbeveiliging
10 Ontwikkeling en onderhoud van systemen
11 Continuïteitsbeheer
12 Naleving

Bron: Code voor Informatiebeveiliging

3. Hoe te beginnen?

Informatiebeveiliging binnen het hoger onderwijs wordt steeds belangrijker, omdat we steeds afhankelijker worden van digitale informatievoorziening die veelal tijd en plaats onafhankelijk toegankelijk moet zijn. Ook allerlei (nieuwe) wetgeving legt eisen op aan de informatiebeveiliging van instellingen. Is informatiebeveiliging niet goed geregeld, dan is het management niet alleen verantwoordelijk maar ook aansprakelijk.
Een goed begin om informatiebeveiliging binnen een instelling 'te organiseren', is het aanstellen van een informatiebeveiliger. Wie kan het complete spectrum aan informatiebeveiliging immers beter overzien en coördineren dan een daarvoor speciaal aangestelde (op het vakgebied informatiebeveiliging deskundige) functionaris?

Vaak heeft een instelling in een eerder stadium al een informatiebeveiligingsbeleid opgesteld. Daarin wordt dan op hoofdlijnen beschreven hoe de organisatie van de informatiebeveiliging binnen een instelling moet worden geregeld. Vervolgens moeten taken, verantwoordelijkheden en bevoegdheden met betrekking tot informatiebeveiliging worden vastgesteld en toegewezen aan betrokkenen.
Binnen de Code voor Informatiebeveiliging betreft dat hoofdstuk 3 beveiligingsbeleid en hoofdstuk 4 beveiligingsorganisatie.
Het aanstellen van een functionaris is vaak de eerste logische stap na het opstellen van een informatiebeveiligingsbeleid. Daarvoor kan gebruik worden gemaakt van het basisprofiel. Minimaal moet de plaats in de organisatie duidelijk zijn. Latere wijziging hierin is lastig. Verder kan de informatiebeveiliger, als deze is aangesteld, als eerste taak krijgen om de informatiebeveiligings-organisatie in kaart te brengen en een meer gedetailleerd functieprofiel op te stellen.

Maar ook als er nog geen informatiebeveiligingsbeleid is, is het een goede eerste stap om een informatiebeveiliger aan te stellen. Eén van zijn/haar eerste taken is dan het opstellen van genoemd beleid.

Manager informatiebeveiliging **Kader 3**

Veel organisaties zullen een manager informatiebeveiliging aanstellen, die de algehele verantwoordelijkheid krijgt voor de ontwikkeling en implementatie van de beveiliging en ondersteuning verleent bij het vaststellen van de benodigde maatregelen. De verantwoordelijkheid voor het beschikbaar stellen van middelen en het implementeren van de maatregelen ligt echter vaak bij individuele managers. Het is goed gebruik voor elk informatiesysteem een "eigenaar" aan te wijzen, die vervolgens verantwoordelijk is voor de dagelijkse beveiliging ervan.

Bron: Code voor Informatiebeveiliging

4. Wat is de meerwaarde van een informatiebeveiliger?

Een instelling doet ook zonder dat er een informatiebeveiliger is aangesteld heel veel op het gebied van informatiebeveiliging. Beheerders hebben beveiliging in hun takenpakket. Als er een contract is met SURFnet is er een site security contact. Eindgebruikers moeten zorgvuldig omgaan met hun wachtwoorden. Lijnmanagers zijn verantwoordelijk voor de beveiliging van de informatie waar zij eigenaar van zijn.
Dat roept soms de vraag op waarom het nodig is om een aparte functionaris voor informatiebeveiliging te benoemen. De meerwaarde wordt niet gezien.

Toch is die meerwaarde er wel degelijk. Uitgaande van de Code voor Informatiebeveiliging, de literatuurstudie (bijlage 3) en de resultaten uit de vragenlijst (bijlage 2) blijkt dat een organisatie die zich wil houden aan algemeen geaccepteerde 'good practices' iemand verantwoordelijk moet maken voor informatiebeveiliging. Aarzelt u hier, dan is het misschien goed eerst de vraag te stellen: wat is de meerwaarde van informatiebeveiliging.
Bij de beantwoording van deze vraag komt u al snel bij de taken en verantwoordelijkheden die een instelling heeft op het gebied van informatiebeveiliging. Vervolgens kunt u vaststellen bij wie binnen de instelling deze taken en verantwoordelijkheden zijn belegd. De uitkomsten daarvan kunnen gelegd worden naast de Code voor Informatiebeveiliging. Dan blijkt of er witte plekken zijn.
Vervolgens kunt u besluiten deze door de aanstelling van een informatiebeveiliger in te vullen.
Vaak liggen deze witte plekken namelijk op het gebied van coördinatie (er zijn veel mensen met informatiebeveiliging bezig, maar zonder zaken op elkaar af te stemmen), communicatie/voorlichting (technische maatregelen moeten altijd gebruikt worden door mensen; zij moeten dus kennis, houding en gedrag hebben om deze maatregelen goed toe te passen) en advies (informatiebeveiliger heeft specifieke deskundigheid).

Voordeel van het benoemen van een informatiebeveiliger is dat deze persoon volledig is vrijgemaakt voor deze taak en een organisatiebrede kijk op beveiliging heeft. Het is zijn/haar primaire werk en niet 'iets wat er nog bijkomt'.
Juist in drukke tijden (reorganisaties, deadline project nadert) is het belangrijk iemand te hebben die volledig is vrijgemaakt om informatiebeveiliging aandacht te geven. Achteraf beveiliging 'inbouwen' is moeilijk en in ieder geval duurder dan meenemen bij ontwerp en invoering.

Meerwaarde blijft overigens altijd lastig meetbaar. Maar er zijn meer zaken binnen een instelling die lastig meetbaar zijn en waar toch zonder meer geld aan wordt uitgegeven. Denk bijvoorbeeld aan pro-actief beheer en afgesloten verzekeringen. Het geeft een gevoel van zekerheid. Dat geeft de informatiebeveiliger u ook. De informatiebeveiliger zorgt dat er maatregelen getroffen worden waardoor inbreuken op de beveiliging worden voorkomen. Of, als ze toch voorkomen, de gevolgen binnen de perken blijven. Op basis van risico-analyse maakt de informatiebeveiliger de mogelijke schade die een bedreiging (bijv. aanval hackers) kan toebrengen aan bepaalde informatie en de kans dat het gebeurt, zichtbaar. Het management moet aangeven welke risico's zij aanvaardbaar acht en welke (door maatregelen) moeten worden afgedekt. De informatiebeveiliger heeft kennis van risico-analyse en kan het management ondersteunen bij het opsporen en tot aanvaardbare risico's terugbrengen van kwetsbaarheden binnen 'de business'.

Nieuwe ontwikkelingen binnen onderwijs en onderzoek vragen een deskundige bijdrage van een informatiebeveiliger. Het tijd en plaats onafhankelijk studeren is een ontwikkeling die volop in gang is. De informatiebeveiliger helpt u de kaders vast te stellen en uit te dragen waarmee de integriteit, beschikbaarheid en vertrouwelijkheid van informatie(voorziening) kunnen worden gewaarborgd.

5 Profiel functie informatiebeveiliger

5.1 Inleiding

Functies en rollen
Een **functie** betreft gelijksoortige samengebundelde werkzaamheden met een gemeenschappelijk doel.
Een **beroep** is algemener, het betreft een bepaalde bekwaamheid los van de organisatie.
Een **rol** geeft de invloed van de houder weer; het is de factor in een proces. Voorbeelden van rollen zijn: aanjager, voorzitter, informeel leider.
Bij **taken** gaat het om werkzaamheden, de technische inhoud van een functie.

De term rol wordt niet altijd gebruikt zoals hierboven gedefinieerd. Zo kan men bijvoorbeeld lezen over de beleidsfunctionaris die de rol van informatiebeveiliger heeft. Beter zou zijn de beleidsfunctionaris die taken uitvoert die liggen op het gebied van informatiebeveiliging.

Informatiebeveiliger is volgens voorgaande definitie een beroep. Het is ook een functie binnen een organisatie. Daarbij betreft het alle werkzaamheden die tot doel hebben de informatiebeveiliging binnen een organisatie op voldoende niveau te brengen en te houden.

Functiebenaming en functieprofiel
In deze leidraad kiezen wij voor de algemene functienaam informatiebeveiliger. Deze naam ligt het dichtst bij het doel van de functie, namelijk het zorgdragen voor informatiebeveiliging.
De vele namen die in de praktijk aan de functie van informatiebeveiliger worden gegeven, vertroebelen het beeld: het lijkt om vele functies te gaan, maar feitelijk is het één functie (informatiebeveiliger) met hooguit verschillende accenten (blijkt uit specifieke functienaam).

Wat wel opvalt in het geheel is dat er grofweg twee ‘richtingen’ binnen de functie kunnen worden onderscheiden: de meer technisch gerichte functie en de meer organisatorisch gerichte functie.
Toch menen wij dat het mogelijk is één basisfunctieprofiel op te stellen. Iedere informatiebeveiliger moet namelijk het gehele terrein van informatiebeveiliging kunnen overzien. En daarbij het deelterrein waar hij/zij zich specifiek mee bezighoudt, kunnen plaatsen in relatie tot dat geheel.
Bij het specifieke functieprofiel kunnen sommige taken,verantwoordelijkheden en bevoegheden dan wat meer accent krijgen. De taken, verantwoordelijkheden en bevoegdheden die minder accent krijgen, moeten overigens wel in een ander specifiek functieprofiel worden ingevuld!

Het basisfunctieprofiel is zowel op centraal als op decentraal niveau toepasbaar. De centrale functie zal de functionele aansturing van de decentrale functie verzorgen.

Binnen het functieprofiel komen de volgende onderdelen aan de orde:
- Functienaam (paragraaf 5.2)
- Doel van de functie (paragraaf 5.3)
- Plaats in de organisatie (paragraaf 5.4)
- Resultaatgebieden (taken, werkzaamheden) (paragraaf 5.5)
- Taken, verantwoordelijkheden en bevoegdheden (paragraaf 5.6)
- Contacten (paragraaf 5.7)
- Opleiding, kennis, ervaring en competenties (paragraaf 5.8)
- Functiewaardering (paragraaf 5.9)

5.2 Functienaam

Informatiebeveiliger (IB).
Informatiebeveiligingsfunctionaris (IBF), beveiligingsadviseur, adviseur informatiebeveiliging, beleidsmedewerker (informatiebeveiliging), coördinator informatiebeveiliging, security manager, security officer, information security manager, Corporate Information Security Officer (CISO), Central Information Security Officer, risico-analist, continuïteitscoördinator, autorisatiebeheerder, cryptograaf, security architect, security administrator, ITIL-security manager, technisch specialist security

operations & monitoring, technisch specialist firewall/anti-virus/spyware, ethisch hacker, privacy coördinator, enzovoort.

De keuze voor een bepaalde functienaam hangt samen met de cultuur van een instelling (engels/nederlands, generieke functiebenamingen zoals beleidsmedewerker of specifieke benamingen) en de meer concrete functie-invulling die voor ogen staat.
Bij dat laatste is sprake van twee hoofdrichtingen: een organisatorisch gerichte en een technisch gerichte functie. De organisatorische kant richt zich meer op het geheel en de samenhang van beveiligingsmaatregelen; de beleidskant derhalve. De technische kant houdt zich bezig met één of meer technische beveiligingsonderwerpen; de uitvoeringskant. Deze tweedeling sluit overigens ook aan bij de opleidingen die op het gebied van informatiebeveiliging worden gegeven.
Verder zal bij grotere instellingen, met meer dan één informatiebeveiliger, in de functienaam vaak de plaats binnen de organisatie terugkomen (bijvoorbeeld local information security officer en central information security functie).
Bij kleinere instellingen, waar het gaat om een parttime functie, kan combinatie plaatsvinden met een verwante (staf)functie. Dat kan dan leiden tot een meer algemene functiebenaming (bijvoorbeeld beleidsmedewerker).

5.3 Doel van de functie

Het op basis van een algemeen aanvaarde standaard (Code voor Informatiebeveiliging), zorgdragen voor een samenhangend pakket van maatregelen ter waarborging van de vertrouwelijkheid,integriteit en beschikbaarheid van de informatie binnen een instelling.
Risico-analyse, oog voor ‘de business’ (onderwijs, onderzoek, bestuur en beheer) en in achtneming van de wettelijke voorschriften zijn daarbij sleutelbegrippen.

Een instelling heeft beide typen, onder het kopje functienaam geschetste, informatiebeveiligers nodig.
Doel van de meer technisch gerichte functie is om met de bij de functie behorende specialistische kennis en kunde het beveiligingsrisico (dus het risico dat de vertrouwelijkheid, integriteit en/of beschikbaarheid van informatie wordt aangetast) als gevolg van de toepassing van (nieuwe) technologieën op een aanvaardbaar niveau te brengen en te houden. Deze functie heeft een rol bij enerzijds de ontwikkeling van nieuwe projecten/systemen en anderzijds het onderhoud en beheer van bestaande systemen, applicaties en infrastructuur.
De meer beleidsmatig gerichte functie heeft als belangrijkste doel om binnen de instelling voldoende organisatorische beveiligingsmaatregelen te initiëren en wel zodanig dat de technische beveiligingsmaatregelen ook daadwerkelijk effectief zijn. Met andere woorden dient zorg te dragen voor samenhang tussen de technische en organisatorische maatregelen.

Het is mogelijk dat de informatiebeveiliger zich zowel met beleid als uitvoering bezighoudt. Wenselijk is dit niet. Meestal leidt dit er toe dat één van beide gebieden te weinig aandacht krijgt.

5.4 Plaats in de organisatie

Het betreft een staffunctie/verbijzonderde functie direct onder het College van Bestuur of de Raad van Bestuur.
Afhankelijk van de grootte van een instelling is het mogelijk om naast een informatiebeveiliger op centraal niveau ook decentraal informatiebeveiligers aan te stellen. Zij ressorteren direct onder het decentrale management. Functioneel worden zij aangestuurd door de informatiebeveiliger op instellingsniveau.

Leidinggeven komt alleen voor in heel grote organisaties als de functie van informatiebeveiliger door verschillende personen wordt uitgeoefend. Dan kan er één als leidinggevende/baas worden aangesteld. Verder is de informatiebeveiliger alleen functionele baas van decentrale informatiebeveiligers (als deze er zijn).

Bij een kleine instelling zal meestal sprake zijn van één informatiebeveiliger en dan wellicht niet fulltime. Combinatie met een andere functie tot één fulltime functie is mogelijk. Maar deze functies moeten elkaar qua taken, verantwoordelijkheden en bevoegdheden niet ‘bijten’. Ook moet de

positionering van die andere functie conform de gewenste positionering van de informatiebeveiligersfunctie zijn.

Gezamenlijke positionering binnen de organisatie met risico-, veiligheids-, continuïteits, privacy en/of kwaliteitsmanagement kan de functie op een hoger plan brengen.
Positionering bij de (IT) auditfunctie heeft niet de voorkeur, omdat controle/toezicht door de (IT) auditor op de de informatiebeveiliger daardoor wordt bemoeilijkt: de externe auditfunctie (accountant) moet dan een grotere rol krijgen.
Positionering onder een ICT-directeur, informatiemanager of Chief Information Officer is mogelijk, zolang er maar altijd de mogelijkheid bestaat tot directe rapportage aan het College van Bestuur of de Raad van Bestuur. Risico van plaatsing onder de ICT directie is dat de nadruk meer op de technische aspecten van informatiebeveiliging komt te liggen, terwijl juist de mensen in de organisatie veelal de zwakke schakel in het geheel zijn.

De geschetste positie garandeert een zekere, voor de functie noodzakelijke, onafhankelijkheid ten opzichte van de 'gewone' lijnfuncties. Bovendien is deze positie van belang om voldoende gewicht in de schaal te kunnen leggen. Dat is nodig ter compensatie van de 'natuurlijke weerstand' tegen het treffen en handhaven van voldoende beveiligingsmaatregelen.

5.5 Resultaatgebieden (taken, werkzaamheden)

Beleid en coördinatie
Het opstellen en actualiseren van het informatiebeveiligingsbeleid (langere termijn).
Het (laten) opstellen van informatiebeveiligingsplannen voor afdelingen of deelgebieden (jaarplannen).
Het coördineren van de werkzaamheden van personen, afdelingen en instanties die zijn betrokken bij de uitvoering van het informatiebeveiligingsbeleid.

De informatiebeveiliger kan gezien worden als de programmamanager van het (strategisch) programma informatiebeveiliging.

Controle en registratie
Het toezicht houden op de implementatie en naleving van het informatiebeveiligingsbeleid.
Het opstellen van een controleplan, alsmede het leveren van ondersteuning bij het uitvoeren van de daarin gedefinieerde taken.
Het uitvoeren of initiëren van risicoanalyses en interne audits.
Het verzamelen en registreren van informatie over de aanwezige beveiligingsmaatregelen.
Het opzetten of initiëren van een registratie voor beveiligingsincidenten, alsmede het afhandelen van opgetreden incidenten en het nemen van preventieve maatregelen ter voorkoming van dergelijke incidenten.

Communicatie en voorlichting
Het onderhouden van externe en interne contacten op alle niveaus binnen dit kader.
Het organiseren van en deelnemen aan een coördinerend overleg met betrekking tot informatiebeveiliging.
Het verzorgen en coördineren van voorlichting en interne opleidingen van het personeel op het gebied van informatiebeveiliging.
Het stimuleren van het beveiligingsbewustzijn en het opstellen, uitvoeren en onderhouden van een communicatieplan.
Het volgen van nieuwe ontwikkelingen en wetgeving op het gebied van informatiebeveiliging.

Advies en rapportage
Het optreden als projectmanager bij beveiligingsprojecten, waarbij aansturing wordt gegeven aan projectleiders binnen organisatorische eenheden.
Het afstemmen van informatiebeveiliging met lopende projecten binnen de organisatie.
Het uitwerken van beveiligingsplannen ten aanzien van de maatregelen, alsmede het leveren van ondersteuning bij het uitvoeren van de geaccepteerde plannen.
Het geven van gevraagd en ongevraagd advies aan de leiding van de organisatie en het lijnmanagement over de te nemen maatregelen.

Het rapporteren aan de leiding van de organisatie over het gevoerde beleid met betrekking tot informatiebeveiliging, de voortgang van implementatie van nieuwe maatregelen, opgetreden incidenten, ondernomen acties, resultaten van onderzoeken en resultaten van controles.

Onderstaand nog enkele aandachtspunten bij de diverse resultaatgebieden.

Beleid
Beleid opstellen, uitvoeren en toetsen/controleren. Uitvoering en controle op uitvoering gaan niet samen.

Coördineren
Informatiebeveiliging is een aspect dat door de hele organisatie van een instelling heen loopt. Het 'zit in' de infrastructuur, de applicaties, de processen, de beheerders en de gebruikers. Verder gaat het bij informatiebeveiliging om integriteit (zijn/blijven gegevens juist en volledig), beschikbaarheid en vertrouwelijkheid. Dat kan soms tegenstrijdige belangen opleveren.
Fysieke beveiliging en privacy zijn onderwerpen die deels overlap hebben met informatiebeveiliging. Iemand moet dat geheel coördineren. Anders werkt het langs elkaar heen of nog erger elkaar tegen. Dan bereik je niet wat je wil bereiken en wordt, onnodig, geld weggegooid.

Adviseren
Aan wie en waarover.
De informatiebeveiliger is binnen een instelling de deskundige bij uitstek op het gebied van informatiebeveiliging. Bij de invoering van nieuwe of vernieuwde systemen, de toepassing van nieuwe technologieën, procedures, maar ook als zaken in de praktijk niet goed blijken te lopen kan/moet de informatiebeveiliger worden ingeschakeld. Informatiebeveiliging achteraf inbouwen is namelijk vaak een lastige en kostbare zaak.

De informatiebeveiliger heeft veel kennis zelf in huis. Waar de eigen kennis onvoldoende is, weet de informatiebeveiliger waar/bij wie deze kennis wel aanwezig is. Het is dus van belang dat een informatiebeveiliger is aangesloten bij een gremium van vakgenoten. Binnen het hoger onderwijs is dat SURF-IBO. Buiten het hoger onderwijs is dat het GvIB.

Bij adviseren gaat het naast de inhoud van het advies ook over de wijze waarop een advies wordt gegeven. Een informatiebeveiliger moet over goede adviesvaardigheden beschikken. Bij tegengestelde belangen, deadlines die gehaald moeten worden, enz. is hij/zij degene die het informatiebeveiligingsaspect steeds weer naar voren brengt. En wel zodanig dat dit ook wordt geaccepteerd.

Rapporteren
Rapportage is een belangrijk onderdeel van de taak van een informatiebeveiliger. Het zorgt ervoor dat het management weet wat er op het gebied van informatiebeveiliging speelt. Hierdoor blijft het managementcommitment behouden. En dat is misschien wel de belangrijkste voorwaarde om informatiebeveiliging binnen een organisatie van de grond te krijgen en te houden.

Code voor Informatiebeveiliging
De onderwerpen die behoren tot het taakgebied van de informatiebeveiligers 'staan in de Code voor Informatiebeveiliging. Ten aanzien van deze onderwerpen moet een informatiebeveiliger beleid opstellen/coödineren, controleren/registreren, communiceren/voorlichten en adviseren/rapporteren.

Organisatorisch/technisch
De informatiebeveiliger die zich richt op de organisatie van de informatiebeveiliging is overkoepelend aan de meer technisch gerichte informatiebeveiliger. Technisch kan (en moet) er veel geregeld worden op het gebied van informatiebeveiliging. Maar dat is niet voldoende. Uiteindelijk wordt 'de techniek' gebruikt door mensen (medewerkers, studenten). Juist deze kant van informatiebeveiliging (hoe zorg ik dat de dure technische maatregelen effectief worden gebruikt binnen de organisatie) is van belang, maar krijgt vaak nog niet de aandacht die zij verdient.
ICT staat ten dienste van het primaire proces, het lijnmanagement. Zo staat ook informatiebeveiliging ten dienste aan onderwijs en onderzoek.

5.6 Taken, verantwoordelijkheden en bevoegdheden

Taken en verantwoordelijkheden

1. Is verantwoordelijk voor het opstellen, bijstellen, vernieuwen en herzien van het informatiebeveiligingsbeleid en de daaruit voortvloeiende *informatie(beveiligings)plannen*.
2. Treedt op als informatiebeveiligingsadviseur (voor het management) bij nieuwe ICT-voorzieningen en bij ingrijpende veranderingen in de ICT-infrastructuur.
3. Adviseert het (lijn)management bij de uitwerking van het informatiebeveiligingsbeleid in informatiebeveiligingsplannen voor hun verantwoordelijkheidsgebieden en bij de implementatie van deze plannen.
4. Initieert of (laat) periodieke beveiligingsaudits, risico-, afhankelijkheids- en kwetsbaarheidsanalyses uitvoeren.
5. Coördineert en adviseert bij beveiligingsincidenten en treedt zo nodig op bij calamiteiten.
6. Blijft op de hoogte van ontwikkelingen op het gebied van informatiebeveiliging en komt zo nodig met voorstellen voor aanvullingen of verbeteringen van producten, methodieken of werkwijzen met betrekking tot de informatiebeveiliging.
7. Opzetten en initiëren van (periodieke) informatiebeveiligingsbewustzijnprogramma's en adviseert over voorlichting en training van gebruikers in het correct omgaan met informatie(systemen).
8. Dient ten allen tijde een open deur te hebben voor de gebruikersorganisatie indien deze buiten de hiërarchie om een beveiligingsincident wil melden.
   Bij voorkeur zou de informatiebeveiliger het formele en bij iedereen in de organisatie bekende aanspreekpunt voor 'informatiebeveiligingszaken' moeten zijn.
9. Leidt projecten die als doel hebben beveiligingsmaatregelen te implementeren of de kwaliteit van de beveiliging op langere termijn te handhaven en waar nodig te verbeteren.
10. Controleert de werking en naleving van informatiebeveiligingsbeleid en daaruit voortvloeiende maatregelen.
11. Rapporteert periodiek beveiligingsincidenten en de afhandeling daarvan aan de portefeuillehouder van het CvB.
12. Vertegenwoordigt de instelling in externe overleggremia.
13. (Laat) rapportages op het gebied van de beveiliging beoordelen.

Bevoegdheden

De belangrijkste bevoegdheid is om op elke plek binnen de organisatie gevraagd en ongevraagd onderzoek te kunnen (laten) doen en zonodig zaken voor te schrijven.
Dat laatste staat soms haaks op de decentralisatie en kritische omgeving ('eigen' keuzes maken) die het hoger onderwijs veelal kenmerkt.
Bij informatiebeveiliging is het echter noodzakelijk om centraal keuzes te maken.

Bij (grote) beveiligingsincidenten/-risico's heeft de informatiebeveiliger de bevoegdheid zo nodig direct in te grijpen (met verantwoording achteraf richting management[1]).

Voorwaarde om de functie informatiebeveiliger volledig te kunnen vormgeven, is de bevoegdheid om gevraagd en ongevraagd te mogen rapporteren aan College of Raad van Bestuur.

Bevoegdheid zonder budget werkt in de praktijk niet. Een eigen budget voor informatiebeveiliging is dus een andere belangrijke voorwaarde voor het goed functioneren.

5.7 Contacten

Zowel intern als extern.
Intern moet de informatiebeveiliger contact onderhouden met andere informatiebeveiligers binnen zijn/haar instelling. De informatiebeveiliger op instellingsniveau heeft daarbij de verantwoordelijkheid dit contact te structureren in vaste en ad-hoc overlegvormen.

[1] De managementlaag waaraan verantwoording wordt afgelegd, is afhankelijk van type, omvang en impact van het incident.

Verder onderhoudt de informatiebeveiliger intern contact met lijnmanagers, projectmanagers en auditors.

Met het in kaart brengen van de interne contacten, wordt in feite de beveiligingsorganisatie van een instelling beschreven.

Extern contact is er met auditors/toezichthouders (accountant, ministerie), service providers (denk aan SURFnet) en politie/justitie.

Extern wisselt de informatiebeveiliger kennis en ervaring uit met vakgenoten van andere instellingen (SURF-IBO) en met vakgenoten van buiten het onderwijs (lidmaatschap Genootschap van Informatiebeveiligers).
Om op de hoogte te blijven van nieuwe technologische ontwikkelingen is contact met leveranciers (beurzen, lidmaatschap gebruikersgroepen van bepaalde producten) tevens van belang.

Binnen een instelling is er naast de informatiebeveiliger nog een aantal functies dat zich bezighoudt met aan informatiebeveiliging gerelateerde gebieden.

De 'functionaris gegevensbescherming' (FG) ook wel privacy officer genoemd.
De FG houdt binnen de organisatie toezicht op de toepassing en naleving van de Wet bescherming persoonsgegevens (WBP). De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de organisatie. Een instelling is niet verplicht een FG te hebben, maar het geeft wel bepaalde voordelen.
Meer informatie en het openbaar register van FG's is te vinden op de site van het CBP (www.cbpweb.nl).
De functie van FG kan eventueel worden gecombineerd met de functie van informatiebeveiliger. In ieder geval moet er onderling overleg zijn. Het aspect vertrouwelijkheid van informatie behoort immers ook tot het taakgebied van de informatiebeveiliger.

De (IT-)auditor
De auditor voert onafhankelijk controleactiviteiten uit, veelal in nauwe samenwerking met de externe accountant. Er is afstemming nodig met betrekking tot de planning van activiteiten. De informatiebeveiliger wordt geïnformeerd over de uitkomsten van de controles. De auditor kan zich bij zijn/haar controles voor een deel baseren op de door de informatiebeveiliger uitgevoerde controles en voortgangsrapportages.

De (bedrijfs)beveiliger, portier
Deze functionaris is belast met de fysieke beveiliging van gebouwen en ruimten binnen een instelling. Er is zeker een relatie met informatiebeveiliging, bijvoorbeeld daar waar het de beveiliging van computerruimten betreft.
In contacten met politie/justitie is het ook mogelijk dat de bedrijfsbeveiliger en de informatiebeveiliger dit gezamenlijk afhandelen.
In de Code voor Informatiebeveiliging is één van de onderdelen de fysieke beveiliging (met als doel 'het voorkomen van ongeautoriseerde toegang tot, schade aan of verstoring van de gebouwen en informatie van de organisatie.'). De gebouwen binnen het hoger onderwijs zijn over het algemeen vrij toegankelijk en niet voorzien van slagbomen of toegangscontrole. Dat heeft wel als consequentie dat de informatiebeveiliger zich moet richten op zoveel mogelijk fysieke en logische beveiliging bij de bron. Dus bijvoorbeeld niet de ruimte tot studieplekken beveiligen, maar het apparaat (laptop) zelf.

Directeur ICT, informatiemanager, Chief Information Officer
Daar waar zij verantwoordelijk zijn voor ICT-beleid, respectievelijk informatiebeleid, is duidelijk dat informatiebeveiliging daarvan een onderdeel is.

Personeelsfunctionaris
Er is een relatie tussen personeelsbeleid en informatiebeveiliging, bijvoorbeeld daar waar het de selectie en het ontslag van personeel betreft. Ook bij het opstellen van gedragsregels met betrekking tot het veilig omgaan met informatie is er overlap. Tenslotte kan personeelszaken een belangrijke bijdrage leveren aan informatiebeveiliging door te zorgen dat bij beoordelingsgesprekken met

medewerkers expliciet beoordeeld wordt op de wijze waarop de betreffende medewerker met zijn/haar verantwoordelijkheid ten aanzien van de beveiliging van informatie van de instelling is omgegaan.

Juridische zaken
Op het gebied van informatiebeveiliging is veel wet- en regelgeving. In het uiterste geval kan het management van een organisatie aansprakelijk worden gesteld als zij onvoldoende heeft gedaan aan informatiebeveiliging. Reden genoeg voor de informatiebeveiliger om bij het opstellen van beleid en de implementatie van maatregelen te toetsen of daarmee wordt voldaan aan alle geldende wet- en regelgeving. Juridische zaken kan daarbij behulpzaam zijn.

Persvoorlichter
In geval van beveiligingsincidenten kan het raadzaam zijn dat er vooraf overleg is geweest tussen informatiebeveiliger en persvoorlichter hoe daar naar buiten mee moet worden omgegaan.

De site security contact
Iedere instelling die een contract heeft bij SURFnet is verplicht een site security contact aan te wijzen. Deze wordt ingeschakeld bij incidenten. Het rapporteren van beveiligingsincidenten behoort tot het taakgebied van de informatiebeveiliger. Ook zal de informatiebeveiliger op instellingsniveau een rol hebben in de escalatieprocedure.

De kwaliteitsfunctionaris
Kwaliteitszorg richt zich op de continue verbetering van de bedrijfsprocessen teneinde de gewenste kwaliteit te kunnen leveren. Informatiebeveiliging richt zich op de vertrouwelijkheid, integriteit en beschikbaarheid van informatie. Daarmee levert de informatiebeveiliger een bijdrage aan de kwaliteit van de bedrijfsvoering. Afstemming is nodig om ‘de neuzen dezelfde kant op te zetten’ en om dubbel werk te voorkomen.

5.8 Opleiding, kennis, ervaring en competenties

Opleiding, kennis en ervaring
- HBO/Academisch werk- en denkniveau
- Kennis en ervaring op het gebied van bestuurs-/bedrijfskunde en/of informatica
- Kennis van de actuele stand van zaken en mogelijkheden van ICT (besturingssystemen, netwerken, standaarden, ontwikkel- en beheermethoden)
- Kennis en ervaring op het gebied van informatiebeveiliging en risico-analyse
- Kennis van de Code voor Informatiebeveiliging
- Kennis van specialistische beveiligingstechnieken, zoals encryptie
- Kennis en ervaring op het gebied van adviseren en organisatiekunde
- Kennis en ervaring op het gebied van onderwijs, onderzoek en/of patiëntenzorg (laatste alleen bij universitair medische centra) (pré)
- Kennis van technische infrastuctuur samen met de business inschatting van de kwetsbaarheid
- Kennis en ervaring met projectmatig werken en projectmanagement.

Competenties
Met competenties wordt bedoeld het in staat zijn om weloverwogen de juiste kennis, vaardigheden en attitude in te zetten op het juiste moment in authentieke situaties.
- goede communicatieve vaardigheden, zowel mondeling als schriftelijk
- goed kunnen samenwerken met verschillende disciplines op verschillende niveaus
- alert, initiatiefrijk, omgevingsbewust
- integer
- overtuigingskracht
- bereid tot permanente scholing.

5.9 Functiewaardering

De meest gebruikte functiewaarderingsmethode binnen het hoger onderwijs is de Hay methode. De universiteiten gebruiken het Universitair Functie Ordeningssysteem (UFO).
Binnen de gebruikte functiewaarderingsmethoden bestaat geen informatiebeveiligers functie en ook geen functie die daarbij in de buurt komt.

Inschaling blijkt in de praktijk veelal afhankelijk te zijn van de functie waaraan de taak van informatiebeveiliger is toebedeeld. Daarbij kan het bijvoorbeeld gaan om de volgende functies: beleidsmedewerker, stafmedewerker, docent, projectleider informatiemanagement, beheerder, consultant.

De functie waaraan de taak van informatiebeveiliger fulltime dan wel parttime wordt toebedeeld, is in die zin van belang dat de plaats van die functie in het organisatieplaatje ook de plaats van de informatiebeveiligersfunctie binnen de organisatie bepaalt. En zoals elders vermeld, is de positie binnen de organisatie deels bepalend voor het welslagen van de functie.

Onderstaand een op de huidige praktijk gebaseerde indicatie voor inschaling:

	Meer technisch	Meer organisatorisch
Kleine instelling	10/11	11/12
Grote instelling	11/12	11(junior)/12(senior)

Bijlage 1 Basisprofiel functie informatiebeveiliger

Functienaam
Algemene functienaam: Informatiebeveiliger (IB).
Specifieke functienaam: door de instelling te kiezen.

Doel van de functie
Het op basis van een algemeen aanvaarde standaard (Code voor Informatiebeveiliging), zorgdragen voor een samenhangend pakket van maatregelen ter waarborging van de vertrouwelijkheid,integriteit en beschikbaarheid van de informatie binnen een instelling.

Plaats in de organisatie
Het betreft een staffunctie.
Organigram van de organisatie (en de beveiligingsorganisatie daarbinnen) opnemen.

Resultaatgebieden (taken, werkzaamheden)
Beleid en coördinatie
Controle en registratie
Communicatie en voorlichting
Advies en rapportage

Aangeven op welke informatiebeveiligingsgebieden uit de Code voor Informatiebeveiliging deze werkzaamheden concreet betrekking hebben.

Verantwoordelijkheden en bevoegdheden
De belangrijkste bevoegdheid is om op elke plek binnen de organisatie gevraagd en ongevraagd onderzoek te kunnen (laten) doen en zonodig zaken voor te schrijven.

Contacten
Zowel interne als externe als externe contacten opnemen.

Opleiding, kennis, ervaring en competenties
Opleiding, kennis en ervaring
- HBO/Academisch werk- en denkniveau
- Kennis en ervaring op het gebied van bestuurs-/bedrijfskunde en/of informatica
- Kennis van de actuele stand van zaken en mogelijkheden van ICT (besturingssystemen, netwerken, standaarden, ontwikkel- en beheermethoden)
- Kennis en ervaring op het gebied van informatiebeveiliging en risico-analyse
- Kennis van de Code voor Informatiebeveiliging
- Kennis van specialistische beveiligingstechnieken, zoals encryptie
- Kennis en ervaring op het gebied van adviseren en organisatiekunde
- Kennis en ervaring op het gebied van onderwijs, onderzoek en/of patiëntenzorg (laatste alleen bij universitair medische centra) (pré)
- Kennis van technische infrastuctuur samen met de business inschatting van de kwetsbaarheid
- Kennis en ervaring met projectmatig werken en projectmanagement.

Competenties
- goede communicatieve vaardigheden, zowel mondeling als schriftelijk
- goed kunnen samenwerken met verschillende disciplines op verschillende niveaus
- alert, initiatiefrijk, omgevingsbewust
- integer
- overtuigingskracht
- bereid tot permanente scholing

Functiewaardering
Afhankelijk van de zwaarte schaal 10, 11 of 12.

Bijlage 2 Verwerking vragenlijst functieprofiel informatiebeveiliger

Inleiding
De deelnemers aan SURF-IBO (Informatie Beveiligers Overleg) hebben een vragenlijst ontvangen met het verzoek deze in te vullen. Van de binnen SURF-IBO vertegenwoordigde instellingen (28) zijn 14 ingevulde vragenlijsten terug ontvangen. Het betreft 7 universiteiten, 5 HBO-instellingen en twee UMC's. De instellingen die de vragenlijst niet hebben ingevuld, gaven veelal als reden dat de functie van informatiebeveiliger nog onvoldoende was uitgekristalliseerd.

HUIDIGE PRAKTIJK
a. Omvang en naamgeving IB-functie

Instelling	Aantal studenten	Aantal medewerkers	Fte IB functie (1= fulltime)	Combinatie met	Functiebenaming
Universitair	20.000	5.000	0,5	Docent	Security manager
Universitair	5.000	4.000	1	Continuïteitsmanagement	Security manager
Universitair	24.600	7.800	0,5	-	Corporate information security officer
Universitair	13.300	4.400	1	-	Security manager
Universitair	20.000	700	0,3	Quality assurance	Security officer
Universitair	12.000	3.000	0,5	Senior adviseur operations	Central information security officer
Universitair	23.500	3.200	0,5	Projectmanager gegevensbeheer	Security officer
UMC	1.900	8.000	0,4	Kwaliteits medewerker	Medewerker informatie beveiliging
UMC	4.300	10.000	1	-	Security officer
HBO	10.000	1.000	-	-	Consultant onderwijssystemen
HBO	29.500	2.600	>0,4	Functionaris gegevensbescher-ming	Security officer
HBO	22.000	2.500	0,8	Kwaliteitszorg	Stafmedewerker
HBO	20.000	2.000	0,1	Project medewerker	Security officer
HBO	16.000	1.300	0,5	-	Netwerkbeheerder/ Security manager

b. Functiewaardering

Binnen de universiteiten wordt de Hay methode (UFO) gebruikt. Eén HBO noemt de Hay methode; bij de overige HBO's en UMC's worden fuwavaz, fuwasys en de HBO-CAO genoemd.
De gebruikte functiewaarderingssystemen kennen geen IB-functie. Functies die worden genoemd zijn: beleidsmedewerker, senior beleidsmedewerker, service level manager en projectmanager.
Inschaling vindt plaats in schaal 10, 11 of 12.

c. Ontstaan van de functie

Vaak is er een bepaalde directe aanleiding om een IB te benoemen. Genoemd worden:

- Aanbeveling accountant (driemaal genoemd)
- Vanuit een Europees project (toetsen van een Europese norm voor informatiebeveiliging aan de praktijk) verder uitgebouwd
- Collegiaal overleg
- Samenvoegen van een onderzoeks- en onderwijsorganisatie met conflicterende belangen tav openbaarheid van informatie
- Groei van het aantal incidenten
- Professionalisering
- Herinrichting netwerk en majeur incident
- Geboekte beveiligingsresultaten op meer operationeel niveau en behoefte dit in te bedden in beleid.

d. Loopbaanperspectieven

De instellingen hebben geen van alle de loopbaanperspectieven vanuit de functie/rol IB gedefinieerd. Eén IB is geneigd de functie een eindpositie te noemen, een andere IB ziet eventueel doorgroeimogelijkheden naar CIO of hoofd ICT.

e. Functiebeschrijving

Van de 14 instellingen zijn er 3 die een functie-/taakbeschrijving IB kennen. De overige hebben geen of een heel summiere/algemene beschrijving.

	1997	2000	2002	2003	2004	2005
Functie bestaat sinds	1 instelling	1 instelling	5 instellingen	2 instellingen	3 instellingen	2 instellingen

De meeste IB's zijn vanaf het bestaan van de functie/rol 'in functie'.

f. Achtergrond (opleiding, e.d.) van de IB

Het opleidingsniveau is over het algemeen HBO en soms WO. De meesten hebben een informatica of bedrijfskundige achtergrond met vaak zeer veel jaar ervaring.
Binnen één UMC wordt HBO verpleegkunde genoemd met als toegevoegde waarde een goede kennis van de cultuur van de gezondheidszorg.
Eén IB is gecertificeerd (CISM); bij twee is certificering gepland.
De volgende lidmaatschappen worden genoemd: GvIB (5), NGI (1), ISACA (2), NOREA (2), PI (via SURF). Acht van de veertien IB's zijn van geen enkele beroepsorganisatie lid.

g. Taken, verantwoordelijkheden en bevoegdheden (TVB)

TVB	**TVB wordt genoemd door instelling x** (zoek dezelfde cijfers bij elkaar en u heeft het takenpakket van één instelling)
Adviseren directie rekencentrum	1
Adviseren management (centraal en decentraal)	3
Adviseren management ICT, portefeuillehouder ICT van CvB	6
Adviseren	4
Adviseren over wijzigingen in beleid	5
Adviseren over nieuwe maatregelen	5

Adviseren (gevraagd en ongevraagd) lijnmanagement en beheerorganisatie m.b.t. de gevolgen voor de informatiebeveiliging van voorgenomen wijzigingen	5, 9
Adviseren in projecten	6, 8, 9
Beoordelen twijfelgevallen wijzigingsverzoeken rond security 'services' als firewall, webfiltering en virusscanning	11
Meedraaien in belangrijke hogeschoolbrede infraprojecten	11
Permanent aanspreekpunt	5
Coördinatie van een goede en voor gebruiker zichtbare beveiligingsorganisatie	6
Opstellen informatiebeveiligingsbeleid (IBB)	3, 4, 11, 8, 9
Uitdragen informatiebeveiligingsbeleid	3
Actief uitdragen van belang informatiebeveiliging	11
Bevorderen van de awareness rondom informatiebeveiliging	6, 8
Stimuleren beveiligingsbewustzijn en opstellen/uitvoeren/onderhouden van een communicatieplan	9
Verzorgen/coördineren voorlichting en interne opleidingen personeel	9
Onderhouden / actueel houden informatiebeveiligingsbeleid	3, 11, 8, 9
Beleidsvoorbereiding en – implementatie	7
Beleidsvoorbereiding en opstellen procedures	8
Opstellen/uitvoering beveiligingsplan	13
Ontwikkeling informatiebeveiligingsbeleid en vervolgtraject ontwikkelen	12
Ontwikkelen en managen informatiebeveiliging programma, waarin opgenomen beleid, standaarden en richtlijnen	6, 9
Ontwikkelen en managen van informatie risicoanalyse en audit	6, 9
(laten) Uitvoeren van risico-inventarisatie(s)	8, 9
Eventueel uitvoering informatiebeveiligingsbeleid	12
Coördinatie en facilitering beveiligingsproces (planning, uitvoer, control) op instellingsniveau	6
Toezicht op uitvoering/controle op naleving informatiebeveiligingsbeleid	3, 4, 8, 9
Toetsen maatregelen aan het informatiebeveiligingsbeleid	5
Controle implementatie vastgestelde beveiligingsmaatregelen	5
Uitvoeren van monitoringprogramma's om vast te kunnen stellen hoe succesvol de implementatie van het beleid verloopt	6
Coördinatie van alle evaluatie activiteiten en audits op het gebied van informatiebeveiliging	6, 9
Rapporteren aan (portefeuillehouder ICT binnen) CvB	6, 8, 9
Rapporteren aan CIO	7
Rapporteren omtrent beveiligingsincidenten, waarschuwingen van CERT-NL en implementatie maatregelen.	5
Bewaken security hoofdstuk in SLA met IT afdeling	11
Continuïteit van de ict-bedrijfsvoering	2
Escalatiemanagement in geval van calamiteiten	6
Aansturen van informatiemanagers m.b.t. uitvoering taken op het gebied van informatiebeveiliging binnen de beheerseenheden	6
Aansturen site security team en CERT	4
Coördineren en deelnemen in de rol van SEP (security entry point) in het kader van deelname aan SURFNET	6
Voorzitter (informatiebeveiligingscrisisteam) CERT	6
Bewaken afhandeling waarschuwingen CERT-NL	5
Bewaken afhandeling meldingen beveiligingsincidenten	5
Spelen rol in afhandeling security incidenten	11, 6
Beslist in geval van (grote) beveiligingsincidenten / risico's wat te doen	9

(laten) Bijhouden van overzicht met beveiligingsincidenten, uitvoeren van analyses op basis van deze registratie	8, 9
Bevoegdheid tot toegang tot incidenten- en wijzigingenadministratie	5
Bevoegdheid tot inschakeling ICT-specialisten	5
Bevoegdheid tot, indien nodig, escalatie/ongevraagd advies naar/aan Bestuurlijk Informatie Adviseur, (portefeuillehouder ICT) CvB, CIO	1, 3, 4, 5, 6, 7, 11, 12
Bevoegdheid tot ingrijpen in alle ict-bedrijfsprocessen	2
Bevoegdheid om maatregelen te nemen tegen inbreuken op het beveiligingsbeleid	3
Adviseur en contactpersoon voor de Privacy functionaris	5
Afstemmen en afspraken maken met fysieke beveiligingsafdeling in het kader van overlap van informatiebeveiligingsproblemen met algemene beveiligingszaken	6
Afstemmen en afspraken maken met de interne Audit- en ICT afdeling over de uitkomsten van de security controles en audits	6
Afstemmen en afspraken maken met de personeelsafdeling over de eisen die vanuit informatiebeveiliging worden gesteld aan personeel	6
Coördinatie van de werkzaamheden van personen, afdelingen en instanties die zijn betrokken bij de uitvoering van het informatiebeveiligingsbeleid	9
Organisatie van / deelname aan coördinerend overleg	9
(laten) inventariseren van binnen de organisatie in gebruik zijnde informatiesystemen	8
Op de hoogte blijven van (nieuwe) ontwikkelingen en wetgeving op het gebied van informatiebeveiliging	8, 9
Onderhouden externe en interne contacten op alle niveaus	9

Bevoegdheden liggen in de meeste gevallen in de sfeer van gevraagd en ongevraagd adviseren van de RvB en rapporteren aan de RvB (meestal via de directeur ICT).
Eén IB geeft aan te beschikken over een bepaald budget met daarbij wel de aantekening dat het budget grotendeels opgaat aan vaste componenten.

Taken en verantwoordelijkheden met	
Accent op beleid	5 instellingen
Accent op uitvoering (operationeel)	1 instelling
Combinatie van beleid en uitvoering	7 instellingen

In de praktijk blijken operationele taken soms veel tijd te vergen.
Uitvoering gebeurt niet altijd door de IB zelf; hij/zij kan ook zaken laten uitvoeren.

Scope van de functie/rol	
Instellingsbreed	8
ICT	4

Vaak ligt het genuanceerder: formeel wel ICT maar in de praktijk instellingsbreed of juist andersom, dus formeel instellingsbreed, maar in de praktijk vooral ICT.

h. Inschakeling bij projecten

Achtergrond van deze vraag is dat informatiebeveiliging bij voorkeur vanaf het begin moet worden ‘ingebouwd’.
Uit de antwoorden blijkt dat inschakeling wel gebeurt, maar niet per definitie of (te) laat in het traject, of alleen op eigen initiatief van de IB of afhankelijk van de projectleider.
In één geval zijn er formeel afspraken: de IB wordt ingeschakeld in voortraject, na functioneel ontwerp en voor in productiename.

i. Beveiligingsorganisatie

Drie instellingen kennen (nog) geen beveiligingsorganisatie. Bij twee instellingen is het er wel, maar alleen voor ICT of het wordt niet specifiek zo genoemd.
Eén IB geeft aan het als zijn taak te zien een dergelijke organisatie tot stand te brengen.

Bij een andere instelling is er wel een calamiteitenorganisatie en een afdeling Veiligheid en Milieu (fysieke en sociale veiligheid).
Twee instellingen kennen een beleidsadviesgroep of organisatiebrede commissie informatiebeveiliging. Deze laatste heeft echter geen duidelijke taken en bevoegdheden.
Mogelijkheden voor verankering in de organisatie worden besproken door RvB.

Plaats van IB in de organisatie	**ICT**	**Stafdienst (gebruikersorganisatie) Informatiemanagement**	**(portefeuillehouder) CvB/RvB of CIO**
Hiërarchisch	11	2	
Functioneel (rapportage)	6	3	4

j. Andere medewerkers met informatiebeveiligingsfunctie/-rol

Naast de IB worden de volgende functies genoemd:

- Site Security Contact
- Service desk, security entry point
- Bestuurlijke informatiebeveiliger (gebruikerskant)
- Security manager bij IT Support (ITIL term)
- Change manager (ITIL term)
- Systeem- en netwerkbeheerders, ICT-beheerders
- fysieke en technische beveiligers
- beleidsmedewerker infrastructuur
- hoofd centrale faciliteiten (I&A)
- hoofd techniek en wetenschappen (I&A)
- afdeling veiligheid en milieu (fysieke en sociale veiligheid)
- locale/decentrale IB's of informatiemanagers bij beheerseenheden
- aanspreekpunt ICT per faculteit/dienst
- CERT
- Functionaris gegevensbescherming

k. Gesprekspartners

Genoemd worden:

- Hoger management
- Middle management
- Managementoverleg met faculteitsdirecties en CvB
- IT-management
- ICT-medewerkers
- Leden 'security kerngroep'
- Decentrale informatiebeveiligers (zo aanwezig)
- Personeel
- studenten

"De medewerkers" en "de studenten" zijn in de praktijk een lastig te benaderen groep. Vandaar dat dat bij in ieder geval één instelling via contactpersonen/vertegenwoordigers loopt.

GEWENSTE SITUATIE
Antwoorden zijn ongewijzigd overgenomen.

I Heeft elke instelling een informatiebeveiligingsfunctie nodig?

1. Ja, zonder een coördinerende functionaris op RvB-nivo blijkt het in de praktijk erg moeilijk om met name de medewerkers bewust te maken van de noodzaak van informatiebeveiliging en de organisatie rondom informatiebeveiliging van de grond te krijgen. Het blijft dan erg een technische aangelegenheid.
2. Ja, Informatiebeveiliging overstijgt afdelingen / instituten, en speelt zich af op allerlei niveaus. Het is noodzakelijk dat dit gecoördineerd wordt.
3. Ja; deze is er ook
4. Ik geloof het wel. Om de relatie informatiebeleid, operationeel beheer en bedreigende trends in de buitenwereld te bewaken.
5. Gezien de cruciale rol van informatie in de primaire en ondersteunende/bestuurlijke processen van de instellingen is de functie geen overbodige luxe.
6. Ja, in deze tijd waar men steeds afhankelijker wordt van elektronische informatieverwerking en er steeds hogere eisen voeden gesteld aan de toegankelijkheid van de informatie dient er iemand te zijn die het totaal overzicht heeft en dit in goede banen leidt.
7. Indien er gebruik wordt gemaakt van open toegang tot het Internet zou 't wel praktisch zijn.
8. Ja, maar kan afhankelijk van de hoeveelheid en de aard van de informatie ingebed zijn in een andere functie
9. Ja.
10. Elke instelling beschikt over een immer groeiende hoeveelheid informatie; bedrijfsprocessen worden steeds afhankelijker van infomatie(verwerking). Bedreigingen nemen toe. Een beveiligingsfunctionaris (met de juiste opdracht) kan in een, over het algemeen gedecentraliseerde, organisatie, de informatiebeveiliging op een hoger plan brengen en borgen.
11. Ja, als aanspreekpunt en coördinatiepunt
12. Ja. Aandacht voor informatiebeveiliging stimuleren, maatregelen coördineren en informatie vetrstrekken.
13. Ja, er moet een aanspreekpunt zijn en iemand die initiatieven kan nemen vanuit het IB-vakgebied. Iemand de het management scherp kan houden op gebied van verantwoordelijkheid voor informatie(beveiliging)
14. In principe wel. Elke instelling kent eigen problematiek t.a.v. infrastructuur en applicaties, organisatie etc.

II Is het mogelijk één functieprofiel informatiebeveiliger te maken of is het nodig verschillende profielen te onderscheiden. En, indien het laatste, waar zit het onderscheid dan in?

1. Één functieprofiel lijkt mij voldoende. In dit profiel zou ik de nadruk leggen op beleid. Middels een toevoeging in diverse functiebeschrijvingen (bijv. beheerder, kwaliteitsmedewerker, stafadviseur en ontwikkelaar) zou vervolgens wel het operationele deel van informatiebeveiliging geborgd moeten worden.
2. Ik vind dat er 2 moeten zijn: Security Officer aan gebruikerszijde Security Manager aan IT zijde (als ITIL procesmanager)
3. Eén profiel per org. Volstaat. Echter het profiel verschilt per ontwikkelingsfase / volwassenheidsniveau van de organisatie. Naarmate evaluatie van eigen functioneren in de org. meer gemeengoed is zal trendvolging de controlerende taak verdringen. Een eigenverantwoordelijkheidsbesef bij gebruikers verminderd drastisch het aantal incidenten.
4. Ik denk dat er onderscheid moet worden gemaakt in beleidstaken en uitvoeren de taken.
5. vermoedelijk zijn de lokale cultuurverschillen (hbo, universiteiten , medische centra etc. te groot om 1 profiel te maken. Ook binnen organisaties zijn de verschillen groot, waardoor standaardisatie waarschijnlijk niet mogelijk is. Belangrijk lijkt me dat de positie onafhankelijk is en relatief hoog in de organisatie gesprekspartners heeft.
6. Het onderscheid zou kunnen zitten in het niveau, beleidsmarig, tactisch of uitvoerend. Hoewel dat laatste in een kleine organisatie ook in een beheersfunctie zou kunnen worden opgenomen, waarmee één profiel voldoende kan zijn. Maar het is aan te bevelen de verschillende rollen in meerdere functies onder te brengen.
7. één profiel met nuanceverschillen. Verschillen zijn de plaats in de organisatie en bevoegdheden. De taken zijn m.i.gelijk.

8. Meerder profielen. In elk geval onderscheid tussen strategisch niveau en operationeel niveau.
9. Moet je aan P&O vragen.
10. 1 profiel zou moeten kunnen. Het zal wel zo zijn dat per instelling wellicht een rol/persoon-splitsing wordt aangehouden op basis van persoonlijke kwaliteiten, omvang van instelling, history, beschikbare mensen etc. Soms zal functie b.v .gecombineerd worden met fysieke beveiliging of privacy, terwijl juist privacy ook bij b.v. juridische zaken belegd kan worden. Een ander voorbeeld is een Business-continuity-plan, dat zou b.v. bij hoofd operations van ICT belegd kunnen worden. Awareness kan deels bij opleiding ondergebracht worden. Etc. Maar alle taken kunnen in 1 functieprofiel staan (al of niet geclusterd) zodat een instelling ervoor kan (c.q. zou moeten) zorgen dat alle taken ook dadwerkelijk belegd worden
11. Er zou een set van taken, bevoegdheden en verantwoordelijkheden (tbv's) op strategisch, tactisch en operationeel niveau moeten worden gedefinieerd, waaruit voor individuele situaties één of meer profielen samengesteld zouden kunnen worden.

III Op welke punten zou de huidige invulling van uw functie kunnen worden verbeterd?

1. Verankering in de organisatie en beschrijving verantwoordelijkheden
2. Tijd
3. Zelf structureel wat meer tijd in stoppen;Meer audit/reviews uitvoeren Beschikking hebben over een instrument om (informatiebeveiliging) meetbaar en aantoonbaar effectief te maken. Nu vaak: hoe beslis ik of een maatregel zijn geld waard is? Op goed gevoel/good practice gronden vaak wel duidelijk, maar zelden hard aantoonbaar.
4. Meer tijd (dus geld), mogelijkheden krijgen voor het vrijstellen van medewerkers
5. Het aanstellen van een beveiligingsfunctionaris op beleidsniveau die direct onder het CVB valt.
6. Minder breed taakveld.
7. Meer capaciteit beschikbaar stellen.Vervanging is op dit moment niet geregeld.
8. Meer middelen om aan security awareness te kunnen doen
9. Bewustwording bij het management van de risico's die ze lopen.
10. Meer menskracht (verdubbeling). Inrichting organisatie met CIO en Informatie-Managers.
11. Verder formaliseren en communiceren

IV Hoe zou een instelling die een informatiebeveiligingsfunctie wil gaan inrichten, het best te werk kunnen gaan?

1. Belangrijkste is dat RvB, CvB noodzaak van een functionaris inziet en ook daadwerkelijk wil ondersteunen. Wanneer er geen commitment is, is invulling van de functie wel mogelijk, maar zal de nadruk waarschijnlijk op techniek komen te liggen.Vervolgens plaats in de organisatie bepalen en functieprofiel opstellen waarbij met name verantwoordelijkheden en bevoegdheden zijn benoemd.
2. In elk geval benoemen. Dat is bij ons niet het geval. Het is dus niet ingebed in de organisatie.
3. IB beleid opstellen, met daarin doelstelling IB en doelstelling en TBV's van een informatiebeveiligingsfunctionaris. De IB beleid laten goedkeuren door College van Bestuur, waarna IBF invulling kan geven aan functie. Dan periodiek (eerste 2 jaar ieder half jaar) met leidinggevende een evaluatie van functie en voortgang implementatie.
4. Het zou eerst moeten weten wat het wil veiligstellen, wat is het minimum aanvaardbare niveau en welke inspanning wil het daarvoor leveren.
5. stel een medewerker aan die e.e.a op poten moet gaan zetten en laat de medewerker bij andere instellingen op bezoek gaan om concrete ideeen op te doen.
6. Eerst overeenstemming en commitment in het management zien te bereiken aan de hand van een inventarisatie van de risisco's. Deze zijn namelijk bepalend voor de noodzaak zowel als het benodigde type functionaris(sen) (beleidsmatig cq. uitvoerend).
7. Eerst duidelijk vastellen waarom informatiebeveiliging en waarom een aparte functionaris en niet in de staande organisatie. Vervolgens vaststellen wat van een ibf verwacht wordt (alleen organisatorisch of technisch of….). Ibf laten inventariseren wat er al gebeurd is op het gebied van informatiebeveiliging. Vervolgens vandaar uit verder werken.
8. Eerst een raamwerk opzetten om het eens te worden over de plaats en rol van infomatiebeveiliging binnen de organisatie
9. Beleid- en organisatievoorstel maken en hiervoor top-management-commitment vragen; hiervoor m.n. duidelijk maken wat de risico's zijn en wie de verantwoordelijken zijn. Een business-case maken. Vooral het wiel niet uitvinden maar putten uit beschikbare info collega-instellingen

10. Inrichten van de functie en taakgebied op hoofdlijnen, nader uitwerken, bekrachtigen en communiceren.

V Wat zijn de kritische succesfactoren ten aanzien van de functie/rol?

1. Commitment vanuit de RvB, CvB zowel in woord, daad als financiën
2. Nog te weinig ervaring mee.
3. Echt commitment van hoger management (functie niet als hamerstuk ingesteld); 1 of 2 sponsors binnen de organisatie in hoger management.
4. Communicatieve kwaliteiten hebben, en denken in; Wens, organisatie, beleid, doel, methode, gebruik, resultaat.
5. commitment van het CVB, beveiligingsbewustzijn van de organisatie/medewerkers
6. Beperking in de mate van vrijheid in de uitvoering (consequent handelen), en commitment van het management tav maatregelen.
7. Voldoende commitment vanuit het management Duidelijke opdracht Een (informatiebeveiligings-)plan De juiste skills
8. Breed draagvlak, quick wins, periodieke rapportage
9. Vertrouwen van het management en een paar flinke incidenten.
10. Top-management-commitment en bijbehorende krachtdadige stellingname
11. Gedragen door hoogste management; Voldoende speelruimte Tijdige betrokkenheid bij ontwikkelingen

VI Welke mogelijke valkuilen onderkent u?

1. Teveel vanuit de techniek redeneren en te weinig aandacht hebben voor het organisatiedeel van informatiebeveiliging
2. Te weinig tijd toegekend krijgen. Het is zaak goed op papier te zetten wat de ambities van de instelling zijn.
3. Vooral denkend vanuit de techniek (dus: techneut als Security Officer); ontbreken van sponsor. Ontbreken sponsor m.i. nog erger dan instelling Security Officer als hamerstuk).
4. Gebrek aan overzicht, met als gevolg ontbreken van samenhang resulterent in onevenredige dekking van gebieden.
5. Als gebruikers zich niet bewust zijn van de risico's en niet actief aan de uitvoering van het beveiligingsplan meewerken gaat het niet lukken. Alternatief is beveiliging afdwingen door middel van techniek maar dit zal worden gezien als te grote inperking van de vrijheden van de gebruiker.
6. Het opstellen van teveel regels en het ontkennen van de eigen verantwoordelijkheid van de uitvoerenden en de eigenaars van informatie.
7. Tegenovergestelde van de bij vorige vraag genoemde zaken
8. Onvoldoende communiceren: met een beveiligingsbeleid ben je er nog niet, dat moet worden uitgedragen.
9. Het ontbreken daarvan
10. Afnemende interesse in organisatie

VII Bent u het eens met de stelling dat de voornaamste taak van een informatiebeveiliger is ´het instellingsbreed coördineren van alle zaken rond informatiebeveiliging´?

1. Ja
2. Ja.
3. Geheel mee eens! Een belangrijke meerwaarde van een overall coördinator is dat inzicht in alle risico's en maatregelen kan leiden tot samenhang in alle activiteiten/maatregelen. Bij beveiliging geldt, m.i. meer nog dan andere aandachtsgebieden: de ketting is zo sterk als de zwakste schakel. Over coördineren: misschien moet hier zelfs staan verantwoordelijk voor. Maar met een goede sponsor heeft een coördinator al erg veel meerwaarde.
4. Ja, hier ben ik het mee eens.
5. Ja omdat informatiebeveiliging een instellingsbreed (lijn)managementvraagstuk is.
6. Ik denk dat de taken zijn coördineren, regisseren en controleren.
7. nee. Ik ben van mening dat de belangrijkste taak van de functionaris het wijzigen van de mentaliteit t.a.v. ICT security moet zijn. Coordinatie komt wel wanneer de neuzen dezelfde kant op staan.
8. Ja, de primaire taak is alle belanghebbenden bijeen en met elkaar in overleg te brengen. Zonder bewustzijn van de risico's is elk beleid gedoemd te mislukken.

9. Ja. Is de enige manier om informatiebeveiliging goed in te richten en op een hoger plan te brengen
10. Dit is de voornaamste taak van de SENIOR informatiebeveiliger. Deze moet een spin in het weg zijn en overal oren en ogen hebben.
11. Dat hangt erg af van de omvang van de instelling en de interne organisatie.
12. Ja
13. Nee, te vaag, zowel wat betreft taak/rol informatiebeveiliger als wat betreft “alle zaken”. Om e.e.a. te expliciteren een soort IB statuut maken, waarin op hoofdlijnen de “ IB opdracht” is opgenomen.

VIII Heeft u verder nog opmerkingen/suggesties?

Informatiebeveiliging is geen eiland. Het lijkt een tegengesteld belang te hebben aan ICT of algemene processen maar allen dienen uiteindelijk hetzelfde doel. Stem de te nemen maatregelen af op het belang hiervan voor de organisatie.

Bijlage 3 Literatuuroverzicht

1. **Ing. Jacques E. Cazemier et al., *Best Practice for Security Management*, uit de serie ITIL Managing IT Services, TSO, 1999, pp 58 en 59**
   De Security Manager is verantwoordelijk voor het Security Management Proces. De interactie met de gebruikersorganisatie onderhoudt hij eventueel via Security Officers. Indien beide functies en/of rollen voorkomen, moeten de verschillende rollen helder gespecificeerd worden. De Security Manager is verantwoordelijk voor de naleving van beveiligingsafspraken in de SLA's, ofwel direct, ofwel gedelegeerd via de Service Level Manager. De Security Manager is betrokken bij de afhandeling van specifeke beveiligingsincidenten en problemen met beveiligingsaspecten. Over het algemeen is hij niet persoonlijk betrokken bij de implementatie van beveiligingsmaatregelen, of het opstellen van richtlijnen en handboeken. De Security Officer coördineert risico-analyes en auditing op het gebied van informatiebeveiliging (welke door de integrale business manager uitgevoerd worden).

2. **Paul Overbeek, Edo Roos Lindgreen, Marcel Spruit, 2000, Informatiebeveiliging onder controle, Pearson Education Uitgeverij BV. ISBN 90-430-0289-5**
   De organisatorische aspecten die noodzakelijk zijn voor een succesvol informatiebeveiligingsbeleid:
   het opstellen, uitdragen en onderhouden van informatiebeveiligingsbeleid en –plan;
   het ontwikkelen en implementeren van procedures;
   het organiseren van informatiebeveiligingsmaatregelen;
   het beïnvloeden van gedrag (motivatie).
   De invulling van deze organisatorische aspecten is zeer organisatiespecifiek. Gesteld kan worden dat informatiebeveiliging in eerste plaats een bedrijfskundige discipline is. Op blz.61 is een lijst opgenomen met punten waar de Security Manager zich op kan richten. Afhankelijk van de omvang van het takenpakket van de Security Manager kan de functie door één persoon ingevuld worden, of door een groep personen. In het laatste geval duidt men de personen die aan de Security Manager toegevoegd worden veelal aan met Security Officer of beveiligingsfunctionaris. De Security Manager zal in de praktijk als gelijkwaardig gesprekspartner van het hoger management zijn. In elk geval dient de Security Manager relatief onafhankelijk te worden gepositioneerd van de interne automatiseringsactiviteiten, omdat deze een belangrijk object vormen voor de advisering en oordeelsvorming.

3. **M&I/Partners BV, 2000, Functieprofiel ICT-manager in het HBO, COMIT**
   Info bij secretariaat COMIT (deijkers@surf.nl)

4. **NEN, *Nederlandse norm NEN-ISO/IEC 17799*, = Code voor informatiebeveiliging (ISO/IEC17799:2000), pp. 11, 12, 13**
   De code beschrijft een manager informatiebeveiliging, die de algehele verantwoordelijkheid krijgt voor de ontwikkeling en implementatie van de beveiliging. Hij verleent ondersteuning bij het identificeren van de benodigde maatregelen. De verantwoordelijkheid voor het beschikbaar stellen van middelen en het implementeren van de maatregelen ligt bij individuele managers.

5. **Ernst J. Oud, *Praktijkgids Code voor Informatiebeveiliging*, november 2002, pp.107/108**
   Afhankelijk van de grootte van de organisatie is het advies een kleine of een wat grotere beveiligingsorganisatie door te voeren. In de beveiligingsorganisatie voor vrijwel alle maatregelen verantwoordelijkheden te onderscheiden op strategisch, tactisch en operationeel niveau. Op strategisch niveau is dat bijvoorbeeld het vaststellen van beleid, werkinstructies en de controle op naleving. Op tactisch niveau moet iemand verantwoordelijk zijn voor het opstellen van de procedures die het beleid vertalen en op operationeel niveau moeten er werkinstructies geschreven worden. Bij grotere organisaties *(niet nader gespecificeerd, schr.)* zijn veelal in de gebruikersorganisatie meerdere Security Officers aangesteld, onder leiding van een Security Manager. Er is een duidelijk onderscheid tussen de functienaam Security Manager als hoofd van de afdeling beveiliging en ITIL Security Manager als verantwoordelijke voor beveiligingsbeheer binnen de ICT-organisatie. Wanneer er nog geen expliciete

staffunctie Security Manager en/of Security Officer aanwezig is, dan is het raadzaam die te benoemen. Indien geen dagtaak, dan beveelt Oud aan de activiteiten onder te brengen bij een andere staffunctie of desnoods een lijnmanager waar al verantwoordelijkheden liggen voor bijvoorbeeld kwaliteit, administratieve organisatie of auditing. Het is van belang er rekening mee te houden dat beveiligingsbeheer een staffunctie is. Het vereist onafhankelijkheid en gezien de controlefunctie is plaatsing in de lijn niet aan te raden. Pp. 107 functiebeschrijving Security Officer.

6. ***GrIB: een methode om beveiligingsmaatregelen succesvol te implementeren*, tijdschrift** Informatiebeveiliging, GvIB, Academic Service, maart 2003
   http://www.grib.org/
   Er is inmiddels ook een boek: Geïntegreerde informatiebeveiliging..

7. ***Informatiebeveiligingsbeleid, werk voor diplomaten?,* presentatie van Jo Koppes van PinkRoccade op de bijeenkomst van het Platform Security Officers op 13 maart 2003**
   http://www.surf.nl/bijeenkomsten/index6.php?oid=56
   Artikel beschrijft de praktijk (wat is een Security Officer?) en de theorie (wat is informatiebeveiliging?). Vele identiteiten met bijpassende bezigheden/taken/vaardigheden passeren de revu: Spin in het web (coördineren, multidisciplinair), stafmedewerker/adviseur, handhaver (controleren, motiveren/sanctioneren), projectleider (tijdelijk, doelgerichte uitvoering), objectbeheerder, auditor, veranderingsmanager (psycholoog). Doel van informatiebeveiliging: beheersen van risico's, treffen en beheren van maatregelen. Plaats in de organisatie: security management op tactisch/strategisch niveau binnen ICT, risico-managementproces op alle niveaus binnen de organisatie.

8. ***'Beveiliging moet los van IT'*, tijdschrift CIO IT-strategie voor managers, IDG Communications Nederland, jaargang 2, nummer 4, april 2003**
   Erik Ubels, CIO van Deloitte & Touche zegt in dit artikel dat beveiliging een van de belangrijkste, maar een van de de meest verwaarloosde issues is van zijn beroepsgroep. Beveiliging, zowel van de infrastructuur als van het gebouw, is zo belangrijk dat personeel hiermee permanent bezig moet zijn.

9. **Carlo van Wordragen, *Gevraagd: Security Manager (m/v) Organisator met communicatieve talenten,* tijdschrift Infosecurity.nl, jaargang 4, nummer 2, 2e kwartaal 2003, Uitgever IDG Communications Nederland**
   http://www.aranea.nl/gevraagd_securitymanager_mv.htm
   De taak van de Security Manager is beveiliging als probleem aankaarten, maar ook oplossingen aanreiken. De directie delegeert de coördinatie naar de Security Manager, die vervolgens de uitvoering op deelgebieden belegt bij de afdelingshoofden. De uitvoering wordt gedelegeerd, de bestuurlijke (eind)verantwoordelijkheid blijft ten allen tijden bij de directie. De Security Manager is een sturende coördinerende en controlerende functie, met informatiebeveiliging als specifiek aandachtsgebied.
   Het is belangrijk dat de Security Manager een heldere doelstelling meekrijgt. Wat is zijn of haar missie, wat moet er na één jaar bereikt zijn, meten we resultaten? Het is zaak om de onbestuurbare opdracht uiteen te rafelen in overzichtelijke, realistische en vooral meetbare stappen. Een beveiligingsplan zorgt voor de samenhang, de planning en sturing.
   De Security Manager treedt op als projectleider en stimuleert de eigen organisatie om informatiebeveiliging serieus te nemen als onlosmakelijk onderdeel van de eigen verantwoordelijkheid. De Security Manager dient een open deur te hebben voor medewerkers die buiten de hiërarchie om aandacht voor security issues vragen.

10. **Ir. Johan C. Op de Coul, 2001, *Taken, functies, rollen en competenties in de Informatica,* Ten Hagen&Stam Uitgevers, Den Haag ISBN 90-440-0343-7**
    De gelijknamige CD bevat voorbeeldfuncties.

11. **Security: geen maatregelen maar risicoreductie**
    Artikel over security awareness bij het management van organisaties. Heeft het topmanagement echt geen aandacht voor de beveiliging van informatiesystemen of zijn

adviseurs niet in staat hun boodschap over te brengen in de taal van het management? http://www.zbc.nu/main.asp?ChapterID=1329

12. **SURF ICT en Organisatie, *Het IABB-procesmodel voor een gestructureerde aanpak***
De taken van een informatiebeveiligingsfunctionaris staan opgesomd op blz 37. Enkele voorbeelden van taken zijn:
beveiligen van informatiesystemen en het toetsen van het informatiebeveiligingsbeleid aan operationele situaties en de blijvende goede werking van de geïmplementeerde informatiebeveiligingsmaatregelen;
geven van voorlichting over informatiebeveiliging;
beoordelen van rapportages op het gebied van het beveiligen van informatiesystemen en het doen van voorstellen;
betrokken zijn bij en beoordelen van veranderingen die gevolgen kunnen hebben op de betrouwbaarheid;
bewaken controleplan;
periodiek rapporteren aan de houder van het informatiesysteem.

13. **Stichting SURF, september 2003 *Vinger in de dijk en toch natte voeten, inventariserend onderzoek naar de Informatiebeveiligingsfunctie (IBF) binnen het hoger onderwijs,***
Er zijn ten tijde van dit rapport bij vijf van de twaalf onderzochte HBO/WO-instellingen informatiebeveiligingsfunctionarissen aangesteld. Er zijn instellingen die meer dan 1 functionaris kennen (bijv. Security Manager en Security Officers en/of Administrators). Sommige instellingen maken onderscheid tussen functie/taken en rollen/taken, waarbij de rol wordt toegewezen aan een bestaande functie van bijv. beleidsmedewerker of staffunctionaris. Inschaling is bij alle instellingen afhankelijk van vorige functie. Bij geen van de instellingen is sprake van een volledige dagtaak. Positionering vaak aan de automatiseringskant, eenmaal bij P&O. IBF is adviserend/signalerend, CvB en lijnmanagement zijn (eind)verantwoordelijk voor informatiebeveiliging. De IB-er heeft over het algemeen geen specifieke opleiding op gebied van informatiebeveiliging. Voor functieprofielen wordt verwezen naar de NGI-publicatie (2001), het IABB procesmodel en de CvIB. Taakbeschrijving vanaf pp 29.

14. **Bhold Company, *Role Based Identity Management, Olie tussen Organisatie en Informatiebeveiliging***
http://www.surf.nl/download/Stultjens.pdf, Presentatie door Bhold van ROI-systeem. Gewezen wordt op de rollen, (conflicterende) belangen en het gevaar van spaghetti van identiteiten binnen een organisatie in relatie tot de informatievoorziening. Belang van functiescheiding wordt benadrukt, alsmede het mogelijk ontstaan van hiaten. Perceptie en belangen van informatiebeveiliging versus organisatie blijkt nogal te verschillen. Dit is een valkuil voor het bereiken van een gewenste situatie (SOLL) vanuit de huidige situatie (IST).

15. **GvIB, *expertbrief 'Functies en rollen in de informatiebeveiliging',* maart 2005**
Dit artikel beschrijft voornamelijk de rol- en competentie aspecten van de informatiebeveiliger. Het doel van dit artikel is duidelijkheid te creëren over functienamen in informatiebeveiliging en risicomanagement en de competenties, taken en verantwoordelijkheden die bij een functie horen. Gekeken wordt ook naar opleidingsbehoefte en loopbaanontwikkelingsmogelijkheden. Vanuit organisatieperspectief wordt onderscheid gemaakt naar gewone functies en verbijzonderde functies. Voor wat betreft de gewone functies worden gewone medewerkers, managers onderscheiden. Voor verbijzonderde functies wordt de wildgroei in aanduidingen als een hindernis ervaren. Er is maar één bijzondere functie, namelijk de information Security Manager. Daarnaast zijn er specialistische (of gewone) rollen, waarbij een 'rol' gedefinieerd is als een onderdeel van een takenpakket. De information Security Manager is, net als een gewone manager, of ITIL-manager, dus een gewone procesmanager. Het enige bijzondere is wellicht dat veel van de activiteiten van het security management proces binnen andere processen worden uitgevoerd, wat een extra beroep doet op coördinerende kwaliteiten.
Vanuit individueel perspectief wordt de ontwikkeling van een informatiebeveiliger op drie niveaus gedefinieerd:
1e niveau: aanstormend talent zonder veel relevante ervaring;
2e niveau: een ethisch allround professional met relevante kennis en ervaring;
3e niveau: specialisatie naar security management of beveiligingsarchitectuur of andere

vakinhoudelijke kennis.
Informatiebeveiliging heeft naast de vakinhoudelijke aspecten ook kenmerken vanuit de sociaal-wetenschappelijke disciplines zoals organisatieontwikkeling en –verandering en psychologie. Dat vraagt het vermogen interdisciplinair vraagstukken op te lossen in de beroepspraktijk. Er zitten allerlei aspecten in: organisaties, mens, techniek, juridische aspecten. Zowel vanuit de alfa als de bèta hoek is er genoeg te beleven.

16. ***Informatiemanagement (scheiding tussen beleid en uitvoering is noodzakelijk)***
http://www.dto.tudelft.nl/algemeen/item/uitgaven/03-01/ict.htm

17. ***Profielen voor functies in het werkveld Security,*** **White paper, Seneca Risk & Security, Lisa van Valkenburg, Februari 2003, versie 0.8.**
Afhankelijk van de grootte van de organisatie, de waarde van informatie en de daarmee samenhangende bedreigingen en organisatiecultuur wordt een security functionaris aangesteld. Organisaties waarbij complexe bedreigingen een rol spelen, wordt geadviseerd de functie op te splitsen. De taken en verantwoordelijkheden van de security functionaris worden daarbij verspreid over meerdere functionarissen, die elk opereren op een ander niveau in de organisatie. Een mogelijke indeling zou zijn:
Security Manager
Richt zich op beveiligingsaspecten op strategisch niveau, met name m.b.t. beleid op langere termijn en (nieuwe) beveiligingsvraagstukken;
Security Officer
Richt zich op beveiligingsaspecten op tactisch niveau, met name m.b.t. verdere detaillering van het beleid en de daadwerkelijke uitvoering / implementatie hiervan (met deels een technisch aspect);
Security Administrator
Richt zich op de uitvoering en dagelijkse controle van de beveiligingsmaatregelen.
Wanneer een Security Officer alleen wordt aangesteld binnen een organisatie komen de functiebeschrijving en –eisen nagenoeg overeen met de functie van Security Manager. Bevat gedetailleerde functiebeschrijving.

18. **Functiebeschrijving (advies aan de directeur IM), TU Delft; Beleidsadviesgroep Toegang & Beveiliging, 19-11-2003.**
De *Security Manager* coördineert de vorming van informatiebeveiligingsbeleid, ziet instellingsbreed toe op de naleving daarvan en van de daaruit voortvloeiende maatregelen, onderzoekt en adviseert in complexe beveiligingsvraagstukken, bewaakt de afstemming van gedistribueerde en/of specifieke beveiligingsplannen met de generieke plannen op instellingniveau, initieert security-audits, organiseert instellingsbrede security-awareness campagnes en opleidingen en vervult een adviserende rol naar het instelingsbestuur.
De *Security Officer* rapporteert aan de Security Manager en richt zich met name op de implementatie en uitoefening van maatregelen op het niveau van gemeenschappelijke voorzieningen of organisatieonderdelen. Bijkomende taken zijn het adviseren bij de selectie van producten en methoden, het uitvoeren van trendanalyses en het management van ITIL-processen op het gebied van beveiliging.
De *security administrator* legt verantwoording af aan de Security Officer en ziet met name toe op de incidentafhandeling. Bijkomende taken zijn het opleiden/assisteren van gebruikers van ICT-voorzieningen in het omgaan met maatregelen, het classificeren van incidenten en routeren naar oplosgroepen en het monitoren van de effectiviteit van technische maatregelen.