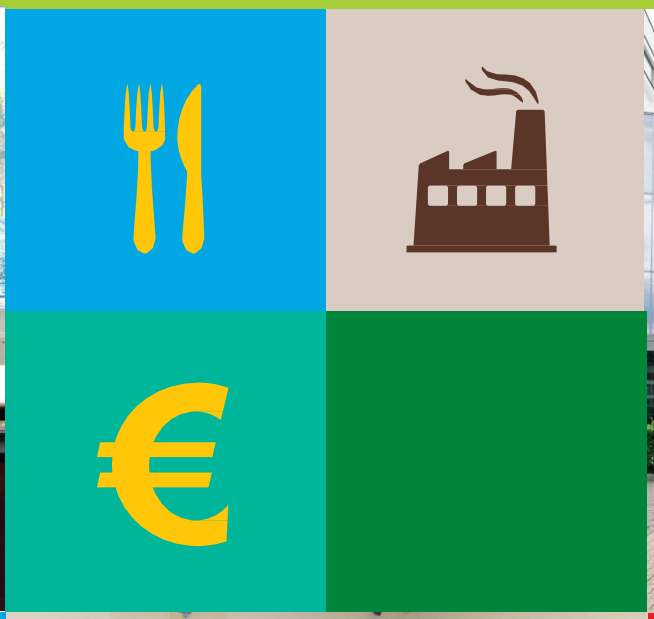
Beroeps- en opleidingsprofiel
Security Management

2014



Kom verder. Saxion.

SAXION

Inhoud

Inleiding

Dit document bevat het beroepsprofiel en het opleidingsprofiel van Security Management. Het beroepsprofiel omvat een beschrijving van de ontwikkelingen op het gebied van security in nationaal en internationaal perspectief. De focus wordt daarbij gelegd op de security van de bedrijfsprocessen van de zogeheten vitale infrastructuur. Verder bevat het een karakteristiek van de security manager, de kerntaken en de competenties. Het opleidingsprofiel omvat een beschrijving van de kennisgebieden en vaardigheden waarover de Bachelor Security Manager moet beschikken om als competente professional te kunnen starten en de kerntaken uit te kunnen voeren, en om door te kunnen groeien tot een expert op het gebied van security. De opleiding leidt op tot de graad van Bachelor Business Administration (BBA) en afgestudeerden voldoen derhalve aan de vier basiskenmerken van deze graad: ze hebben een degelijke theoretische basis, ze hebben vaardigheden op het gebied van onderzoeksmethodologie en statistiek, ze beschikken over professioneel vakmanschap en ze laten zien dat ze verantwoordelijkheid kunnen nemen. Het beroeps- en opleidingsprofiel is opgesteld op basis van onderzoek in het werkveld en een werkveldconferentie waarin de resultaten van het onderzoek zijn voorgelegd aan experts uit het beroepenveld en het onderwijs. De opleiding toetst het beroeps- en opleidingsprofiel nationaal en internationaal:

Juni 2012: International Foundation for Protection Officers (IFPO): positieve validatie met complimenten over de keuze voor de Security Risk Management Body of Knowldge van het Risk Management Institution of Australasia en de American Society of Industrial Security.
December 2012: Positieve screening door de leden van het Landelijk OverlegOrgaan, het HBO-i Platform, van de ontwikkellijn van Beroepsprofiel t/m opleidings module.
2012/2013: Validatie door International Foundation for Protection Officers (IFPO) en American Society of Industrial Security International door benchmark met global profile Chief Security Officer Standard: Next Generation leadership, Business Elements, IT Security Elements, Security organization Elements, Executive leadership Skills, Emerging and Horizon Issues Awareness.

Voorjaar 2013: Beroepsprofiel herbesproken in de Security Management beroepenveldcommissie.
Augustus 2013: Ministerie van Veiligheid en Justitie organiseert een bijeenkomst over nut en noodzaak van ICT en Cyber Security; dit wordt omvat door het beroepsprofiel en het opleidingsprofiel. The Cyber Perspectives 2013, versterkt aandacht voor Security en IT. Keuze voor invoering global IT security standaard CISSP en kwaliteitsmatch met Information Security Management van de HHS.
November 2013: Dochter universiteit van Yale, University of New Haven, toonaangevend inzake critical infrastructure, zoekt contact en beoordeelt vanuit een delegatie met VN, NATO en McKinsey : “impressive”. Suggestie: meer “International Affairs & Political Science”.

Voorjaar 2014: De opleiding neemt vanuit onderzoek de verantwoordelijkheid op zich om jaarlijks de landelijke Security Management Survey uit te voeren en zo ook de landelijke de relevantie van het beroepsprofiel te borgen. Het profiel van de security manager ten opzichte van de voorgaande edities (2010, 2011, en 2012/2013) is niet veel veranderd: er is een lichte stijging van het percentage vrouwen en de gemiddelde leeftijd is iets gezakt.

1 Beroepsprofiel

1.1 Security in de samenleving: ontwikkelingen

In de maatschappij is er sprake van een toename van bedreigingen. De omvang van deze dreigingen beperkt zich niet tot een enkel individu of het voortbestaan van een enkel bedrijf of organisatie. Integendeel, ze strekt zich uit tot bedreigingen van de openbare orde, het gehele maatschappelijke leven en de organisaties die deel uitmaken van de economie binnen die samenleving. Steeds meer wordt duidelijk dat er bijna geen geïsoleerde systemen en processen meer zijn; de huidige samenleving, ons sociaal maatschappelijk en economische leven, zijn zo met elkaar verbonden dat een securityprobleem meteen een inktvlekwerking heeft. In het TNO-rapport 'Bescherming Vitale Infrastructuur (2003)[1], is die afhankelijkheid van diensten en producten in beeld gebracht en gekwantificeerd.

We zien ook dat de angst voor bedreigingen ertoe leidt dat de tolerantie voor risico's in de samenleving afneemt. De Duitse socioloog Ulrich Beck (1986)[2] stelt dat we door de rol van bedreigingen en risico's langzaam maar zeker de maatschappij anders gaan beleven. Volgens hem gaan sociale discussies en incidenten in de maatschappij in toenemende mate over de verdeling van risico's en minder over de verdeling van welvaart. In de risicosamenleving richt men zich op verantwoordelijkheidsvragen bij de gevolgen van crises en catastrofes en over de vraag van beslissingsbevoegdheid over de risico's voor mens, natuur en milieu.

De genoemde bedreigingen leidden tot reacties bij zowel overheid als bedrijfsleven. We noemen enkele belangrijke, te beginnen met de reactie van overheden.

1.2 Reactie van overheden op ontwikkelingen

De toename van dreigingen in verschillende segmenten van de samenleving heeft geleid tot belangrijke maatregelen door de overheden:

---

1 Luiijf et.al (2003), TNO-rapport FEL-03-C002 'Bescherming Vitale infrastructuur: Quick-scan naar vitale producten en diensten, (p. 37, 41, 52, en Bijlage C)

2 Beck (1986), 'Risikogesellschaft. Auf dem Weg in eine andere Moderne', Suhrkamp, Frankfurt am Main

- Meer regelgeving: op mondiaal niveau worden in toenemende mate protocollen ontwikkeld, bijvoorbeeld ter bescherming van zee- en luchthavens.
- Meer aandacht van overheden voor onderzoek: nationale en Europese overheden richten zich met hun dreigingsanalyses op de zogenaamde 'vitale infrastructuur'.
- Meer aandacht voor security: op Europees niveau bestaan initiatieven tot ontwikkeling van het European Programme for Critical Infrastructure Protection.
- Meer onderzoek: specifieke onderzoeksprogramma's zijn inmiddels op Europees niveau ontwikkeld. Het Europese FP7 security research programme en de onderliggende analyses van de European Security Research Advisory Board (ESRAB) worden 4 belangrijke missies onderscheiden:
    - Protection against terrorism and crime
    - Security of infrastructure and utilities
    - Border security
    - Restoring security in case of crises
- Nationaal kunnen we in dit verband ook denken aan maatregelen als het instellen van de Nationaal Coördinator Terrorismebestrijding (NCTb) en de invoering van de code Tabaksblat.
- Het project Bescherming Vitale Infrastructuur dat tot doel heeft de kwetsbaarheid van de vitale infrastructuur in Nederland in kaart te brengen en deze waar nodig te verminderen door het treffen van beschermende maatregelen. Het belang van beveiliging van de vitale infrastructuur blijkt uit de definitie van die NCTB hanteert:

  'Producten, diensten of processen behoren tot de vitale infrastructuur als ze bij het uitvallen ervan maatschappelijke ontwrichting kunnen veroorzaken. Van maatschappelijke ontwrichting is sprake als er veel slachtoffers zijn en grote economische schade is toegebracht. Ook bij langdurig herstel of bij afwezigheid van reële alternatieven terwijl de samenleving deze producten niet kan missen, is er sprake van maatschappelijke ontwrichting'
  (NCTB (2007), Wat kan uw bedrijf ondernemen tegen terrorisme?, blz. 89)\

Tot de vitale infrastructuur horen de volgende sectoren:

a. Energie
b. Financiën
c. Telecommunicatie
d. Keren en beheren van oppervlaktewater
e. Voedsel
f. Drinkwater
g. Gezondheidszorg
h. Rechtsorde
i. Chemische/nucleaire energie
j. Openbaar bestuur
k. Transport
l. Openbare Orde en Veiligheid

De oprichting van het Nationaal Adviescentrum Vitale Infrastructuur (NAVI) is een onderdeel van het project Bescherming Vitale Infrastructuur. Het NAVI onderstreept de kwetsbaarheid van de vitale infrastructuur in haar bedrijfsplan als volgt:

> Onze moderne samenleving is afhankelijk van een goed functionerende infrastructuur. Als bepaalde sectoren uitvallen, leidt dat binnen enkele dagen tot grote problemen. Het merendeel van de ondernemingen in deze vitale sectoren is in particuliere handen. Het particuliere bedrijfsleven draagt zorg voor de beveiliging (security) en de continuïteit van de bedrijfsvoering. De bescherming van de vitale infrastructuur – de ruggengraat van onze samenleving – is daarmee ook een zaak van publiek belang. Het is een gezamenlijke verantwoordelijkheid van de overheid en het particuliere bedrijfsleven. De oprichting van het NAVI geeft daaraan uitdrukking. Binnen het NAVI werken overheid en bedrijfsleven nauw samen aan het bevorderen van de security van de vitale sectoren. Het NAVI wil een structurele bijdrage leveren aan de bescherming van de vitale infrastructuur tegen dreigingen als gevolg van moedwillig menselijk handelen. Niet alleen persoonlijke of fysieke dreiging, maar ook dreiging langs digitale weg (cybercrime).

Duidelijk wordt dat verbetering van de beveiliging van de vitale infrastructuur tegen grootschalige dreigingen geen zaak is van de overheid alleen. Het moet in goede samenwerking met het bedrijfsleven worden uitgevoerd. Het NAVI wil dan ook echte publiek-private samenwerking (PPS) tot stand brengen tussen de overheid en de branches en bedrijven binnen de vitale sectoren. (Bedrijfsplan NAVI). Daarom maken we nu de overstap naar de ontwikkelingen in het bedrijfsleven.

1.3 Reactie van bedrijven op ontwikkelingen

Bedrijven/arbeidsorganisaties realiseren zich steeds meer dat beveiliging niet alleen een taak is van de overheid, maar dat ze ook zélf securitybeleid moeten ontwikkelen. Het ultieme doel van de beveiliging van deze organisaties is dat de ‘business continuity’ gewaarborgd blijft. Doel is het voorkomen of beperken van schade in termen van financiële verliezen. Maar zeker zo belangrijk is het voorkomen van imagoschade. Deze toenemende aandacht van bedrijven wordt zichtbaar in de twee volgende ontwikkelingen.

- Security wordt steeds meer een integraal onderdeel van de bedrijfsvoering. Om de bovengenoemde doelen te bereiken staat security steeds hoger op de agenda van organisaties. Was voorheen security nog bijzonder of uitzonderlijk, tegenwoordig krijgt de beveiliging van de organisatie hoge prioriteit: het analyseren van beveiligingsrisico’s, het opstellen van securityplannen/beleid, het nemen van securitymaatregelen, het managen van

risico's, en het continueren of hervatten van bedrijfsvoering in tijden van crisis, met IT als instrument en als risico, het zijn allemaal belangrijke thema's geworden binnen organisaties.

- Security professionals werken steeds vaker fulltime aan deze portefeuille. Voorheen was beveiliging vooral een operationeel vraagstuk, dat men 'erbij' deed, maar tegenwoordig is het voor veel organisaties (in de vitale infrastructuur) een complex strategisch vraagstuk. Securityspecialisten bewegen zich ook steeds hoger in de organisatie, bekleden steeds vaker strategische functies (lijn-/staf) en voeren deze functies fulltime uit.

Dat brengt ons bij het profiel van de security manager.

1.4 De securitymanager

Karakteristiek

Uit inventarisatie blijkt dat de security manager nu nog veelal een man is van rond de 49 jaar, en vaak hoger opgeleid (breed, niet specifiek). De functie is overwegend hoger in de organisatie ondergebracht. Bijna 44% bekleedt een managementfunctie en 21% vervult een directiefunctie. Verreweg de meeste security managers zijn niet alleen verantwoordelijk voor de beveiliging, maar ook voor de integrale veiligheid (43%). De functie van security manager wordt in de praktijk dus ook sterk verschillend vormgegeven. Opmerkelijk is ook dat bijna 10% van de gevallen geldt dat security een expliciete directieverantwoordelijkheid is. Hieruit kan worden afgeleid dat security in toenemende mate een expliciet 'board room' of directievraagstuk is. Immers, voor bijna 70% van de ondervraagden geldt security als bestuurs of directie-aangelegenheid. In 20% van de gevallen is security een verantwoordelijkheid van het (algemeen) management. Voor de overige organisaties (ruwweg 10%) geldt dat de eindverantwoordelijkheid voor security nog niet op managementniveau is belegd.
Bron: Instituut voor Veiligheids en Crisismanagement en het vakblad Security Management

De security manager is dus een hoog opgeleide professional op het gebied van beveiliging/security. De security manager analyseert vanuit bedrijfsmatig perspectief risico's en bedreigingen en adviseert en beslist over passende investeringen in security. Deze professional adviseert vooral op strategisch niveau. Hij beschikt over actuele kennis van methodieken en technieken om dreigingen en risico's te analyseren. Hij is creatief in het bedenken van oplossingen en weet binnen welke juridische (compliance) en bedrijfsmatige

kaders deze oplossingen moeten passen. Hij beschikt ook over relevante praktijkervaring en kennis van het veld. Van deze professionals wordt bovendien verwacht dat hij in staat is om veiligheidsnetwerken te onderhouden en een informatiepositie op te bouwen.

Kerntaken van de securitymanager

De werkzaamheden van de securitymanager kunnen worden geclusterd tot zes kerntaken.

1. Analyseren van beveiligingsrisico's (voor de bedrijfsstrategie en de sector)
De security manager analyseert op systematische wijze interne en externe dreigingen en risico's voor de bedrijfsprocessen en de ICT-infrastructuur. Werkzaamheden die hieronder vallen zijn: zorgdragen voor veiligheidsbewustzijn binnen de organisatie, bepalen van relevante informatiebronnen (personen, databanken, internet), maken van scenarioanalyse (analyseren van bedrijfsstrategie, kritische bedrijfsprocessen, de bedrijfscultuur), analyseren van bedreigingen om ten slotte te komen tot een analyse/berekening van risico's (kwalitatief, kwantitatief). Deze analyse mondt uit in een rapportage.

2. Adviseren over beveiligingsplannen en -beleid
De security manager vertaalt gemaakte risicoanalyses naar plannen of beleid om te komen tot (een pakket van) passende securitymaatregelen. Het opstellen van dit soort plannen is een omvattende taak. Hierin passen werkzaamheden zoals: het in kaart brengen van mogelijke (nieuwe) harde en zachte beveiligingstechnieken en, zo nodig, het ontwikkelen van innovatieve, passende beveiligingstechnieken. Hij kom tot een pakket van concrete beveiligingsmaatregelen en alternatieven, met een schets van de kosten-baten afweging van de mogelijk scenario's. Waar mogelijk of nodig gebeurt dit in samenwerking met relevante partners. Deze beroepstaak mondt uit in een beveiligingsplan, waarover de securitymanager advies geeft aan het managementteam of de directie over te nemen acties/investeringen.

3. Leidinggeven aan uitvoering/implementatie van veiligheidsmaatregelen De security manager draagt zorg voor de effectieve inzet van mensen en middelen bij de implementatie. Deze taak heeft zowel een harde/technische kant als een zachte/menskant. We zien dat terug in de werkzaamheden die onderdeel zijn van de ze beroepstaak: opstellen en (laten) uitvoeren van (project)planningen, doen van relevante aanbestedingen: inkopen van beveiligingstechnologie en/of diensten, coördineren tussen betrokkenen, aansturen van team, randvoorwaarden creëren voor de personele zorg en coachend leidinggeven aan operationele

managers / vakspecialisten / projectleiders, opstellen van managementrapportages.

4. Business continuity management
Vanuit deze taak draagt de Securitymanager zorg voor business continuity. Hierbij gaat het om de vraag hoe er voor kan worden gezorgd dat cruciale bedrijfsactiviteiten doorgang vinden in tijden van crises. In dit verband verricht hij o.a. de volgende werkzaamheden: analyseren van uitwijkmogelijkheden, opstellen van protocollen/ afspraken met overheidsdiensten (GHOR, brandweren, veiligheidsorganisaties, BHV), opstellen van oefenplannen, oefenen: deelnemen aan/begeleiden van crisisteam, efficiënt gebruik van technologie, conclusies trekken over benodigde bijstellingen in beveiligingsmaatregelen. Deze beroepstaak leidt tot producten zoals: protocollen, oefenplannen, voorbereide securitymedewerkers, lessons learned, contingentieplan/ crisisscenario's et cetera. De Securitymanager is zich bewust van de hele businesscontinuity keten en de impact van de infrastructuur op de maatschappij.

5. Handhaving/compliance
Steeds meer organisaties hebben te maken met regelgeving waaraan ze zich moeten houden. Dit kunnen afspraken of regelgeving zijn die binnen de branche of sector zijn gemaakt of die door de overheid zijn opgelegd. In dit verband draagt de securitymanager zorg voor overeenstemming met / het voldoen aan wettelijke voorschriften/ overeenkomsten.
Hij voert daartoe de volgende werkzaamheden uit: nalezen van gemaakte afspraken, bestuderen van relevante wet- en regelgeving (incl. jurisprudentie), voorbereiden en uitvoeren van inspecties / audits, ontwikkelen van aanbevelingen (voorstellen, maatregelen), rapporteren aan management (incl. voorstellen voor maatregelen). Deze beroepstaak mondt uit in (rapportages van) uitgevoerde analyses en verbeterplannen.

6. Risicomanagement
In deze beroepstaak staat het voorkomen en beheersen van risico's centraal. De securitymanager draagt zorg voor de systematische analyse en het monitoren van risico's en securitymaatregelen, het monitoren van gedrag, het zorgdragen voor een op veiligheid gerichte bedrijfscultuur en het zorgdragen voor voldoende voorbereiding op crises in en om het bedrijf.
Hij geeft aan deze beroepstaak vorm door het uitvoeren van de volgende werkzaamheden: opzetten / onderhouden van een risicomanagementsysteem (o.a.: vaststellen kritische processen, opstellen van protocollen, vaststellen van veiligheids- en beveiligingscriteria, inrichten van een auditsystematiek,

registreren van incidenten en accidenten, uitvoeren regelmatige van audits/inspectie/ op kritische bedrijfsprocessen en infrastructuur, uitvoeren van regelmatige audits en inspectie van veiligheids- en beveiligingsmaatregelen, vergelijken en prioriteren van risico's, aansturen van de risicocommunicatie (eventueel in samenwerking met communicatieafdeling of -medewerkers) zowel intern als extern. Deze taak leidt tot veiligheidsrisicorapportages aan de board rond kritische bedrijfsprocessen en bezittingen, systemen en mensen. Het betreft zowel externe als interne dreigings- en risicobronnen.

Competenties van de security manager

Om de kerntaken uit te kunnen voeren, moet de securitymanager beschikken over de volgende competenties.

1. De securitymanager is in staat op systematische wijze interne en externe dreigingen en risico's te analyseren binnen de bedrijfsprocessen en de ICT-infrastructuur van de sectoren van de vitale infrastructuur.
2. De securitymanager is in staat risicoanalyses te vertalen naar plannen of beleid om te komen tot (een pakket van) passende securitymaatregelen.
3. De securitymanager kan zorgdragen voor de effectieve inzet van mensen en middelen bij de implementatie van securitymaatregelen en beveiligingsplannen.
4. De securitymanager kan zorgdragen voor de effectieve inzet van IT als beveiligingsinstrument bij de implementatie van securitymaatregelen en beveiligingsplannen.
5. De securitymanager kan ervoor zorgen dat cruciale bedrijfsprocessen doorgaan in tijden van crises: business continuity.
6. De securitymanager kan ervoor zorgen dat de organisatie op het gebied van security voldoet aan de wet- en regelgeving en de afspraken die binnen de sectoren van de vitale infrastructuur zijn gemaakt.
7. De securitymanager kan een risicomanagementsysteem opzetten en implementeren.
8. De securitymanager is in staat zijn ontwikkeling te sturen en reguleren, te reflecteren en verantwoordelijkheid te nemen voor zijn handelen, een (ethische) beroepshouding te ontwikkelen en een bijdrage te leveren aan de eigen professionalisering en de professionalisering van het beroep.

2. Opleidingsprofiel

2.1 Standaard Bachelor of Business Administration

De opleiding Security Management leidt op voor de graad Bachelor of Business Administration. Dat betekent dat afgestudeerden voldoen aan vier basiskenmerken: ze hebben een stevige theoretische basis, ze hebben vaardigheden op het gebied van onderzoek, ze beschikken over vakmanschap en ze tonen verantwoordelijkheid. Hieronder wordt kort toegelicht op welke wijze studenten deze kenmerken in de opleiding realiseren.

Gedegen theoretische basis
De theoretische basis bestaat uit een aantal vakgebieden. De belangrijkste daarvan zijn securitykunde en risicomanagement. Daarnaast verwerven studenten inzicht in relevante concepten, principes en modellen op het gebied van accounting, business law and ethics, economics en finance, management information systems, organizational en social behavior, quantitative techniques, strategic management en operations management. De inhoud van deze vakgebieden is de zogeheten Body of Knowledge & Skills van de opleiding. Deze wordt beschreven in paragraaf 2.3.

Onderzoekend vermogen
In de opleiding wordt veel aandacht besteed aan analyse en toegepast onderzoek. Studenten leren op systematische wijze security-vraagstukken, dreigingen en risico's te analyseren (competentie 1), oplossingsrichtingen te verkennen en oplossingen te construeren (competentie 2). Kennis van onderzoeksmethodologie en statistiek leren studenten gebruiken om de uitkomsten van onderzoek te beoordelen, zodat ze in staat zijn beproefde modellen en instrumenten te selecteren voor de aanpak van security-vraagstukken (zie paragraaf 2.3: Onderzoeksmethodologie en statistiek).

Professioneel vakmanschap
Belangrijk onderdeel van het werk van de securitymanager is het adviseren en overtuigen van de board van ondernemingen en instellingen omtrent security-risico's en het treffen van effectieve maatregelen om deze te reduceren. De securitymanager is dus gesprekspartner van de board, maar ook van medewerkers op de werkvloer waar het gaat om de implementatie van securitymaatregelen. In de opleiding wordt daarom veel aandacht besteed aan adviesvaardigheden en communicatieve vaardigheden. Een ander belangrijke

competentie die studenten in de opleiding verwerven, is het vermogen om de eigen professionaliteit verder te ontwikkelen (competentie 8), en om een bijdrage te leveren aan de ontwikkeling van het nog relatief jonge vakgebied securitymanagement.

Verantwoord handelen
Aan bijna alle security-vraagstukken zitten juridische, morele en ethische kanten. De studenten leren in de opleiding daarvoor oog te hebben. Ze verwerven inzicht in de wet- en regelgeving, en ze maken kennis met afspraken die zijn gemaakt binnen de verschillende sectoren van de vitale infrastructuur. Verder leren ze ervoor zorg te dragen dat de implementatie van securitymaatregelen en -plannen in overeenstemming is met de vigerende wet- en regelgeving, en met de afspraken die binnen de verschillende sectoren van de vitale infrastructuur zijn gemaakt (competentie 6).

2.2 Opleidingscompetenties

In de bacheloropleiding Security Management ontwikkelen studenten acht opleidings-competenties. Elke competentie is op twee niveaus uitgewerkt:

Niveau 1. Oriëntatie en reproductie (propedeuse)
De student beschikt over basiskennis en vaardigheden en kan deze gebruiken om in een overzichtelijke, vereenvoudigde context onder begeleiding eenvoudige, standaard vraagstukken te analyseren en (delen van) oplossingen te construeren.

Niveau 2: Productie (tot en met de afstudeerfase)
De student beschikt over verdiepende en deels specialistische kennis en vaardigheden en kan deze grotendeels zelfstandig toepassen bij het aanpakken en oplossen van min of meer complexe securityvraagstukken.

De competenties en competentieniveaus zijn:

1. De securitymanager is in staat op systematische wijze interne en externe dreigingen en risico's te analyseren binnen de bedrijfsprocessen en de ICT-infrastructuur van de sectoren van de vitale infrastructuur.

   Niveau 1. De student heeft inzicht in de risico's en dreigingen die zich binnen de vitale infrastructuur kunnen voordoen en in de methoden en instrumenten om die risico's en dreigingen te inventariseren en te analyseren.

Niveau 2. De student kan op systematische wijze interne en externe dreigingen en risico's binnen de sectoren van de vitale infrastructuur inventariseren en analyseren.

2. De securitymanager is in staat risicoanalyses te vertalen naar plannen of beleid om te komen tot (een pakket van) passende securitymaatregelen.

   Niveau 1. De student kan op basis van een risicoanalyse een plan opstellen met concrete beveiligingsmaatregelen voor een eenvoudige situatie binnen de vitale infrastructuur.

   Niveau 2. De student kan op basis van risicoanalyses een beveiligingsplan of -beleid opstellen en het management een onderbouwd advies geven over te nemen maatregelen en investeringen binnen de vitale infrastructuur.

3. De securitymanager kan zorgdragen voor de effectieve inzet van mensen en middelen bij de implementatie van securitymaatregelen en beveiligingsplannen.

   Niveau 1. De student kan een plan opstellen voor de effectieve inzet van mensen en middelen bij de implementatie van securitymaatregelen en beveiligingsplannen.

   Niveau 2. De student kan bij de implementatie van securitymaatregelen en beveiligingsplannen op een effectieve manier mensen en middelen inzetten, en daarbij rekening houden met de kosten en baten.

4. De securitymanager kan zorgdragen voor de effectieve inzet van IT als beveiligingsinstrument bij de implementatie van securitymaatregelen en beveiligingsplannen.

   Niveau 1. De student kan een plan opstellen voor de effectieve inzet van IT bij de implementatie van securitymaatregelen en beveiligingsplannen.

Niveau 2. De student kan bij de implementatie van securitymaatregelen en beveiligingsplannen op een effectieve manier IT inzetten, en daarbij rekening houden met de kosten en baten.

5. De securitymanager kan ervoor zorgen dat cruciale bedrijfsprocessen doorgaan in tijden van crises: business continuity.

   Niveau 1. De student kan een plan opstellen om de cruciale bedrijfsprocessen door te laten gaan in een crisissituatie.

   Niveau 2. De student kan een plan voor business continuity implementeren waardoor cruciale bedrijfsprocessen in een crisissituatie doorgang kunnen vinden en houdt daarbij rekening met de hele business continuity keten.

6. De securitymanager kan ervoor zorgen dat de organisatie op het gebied van security voldoet aan de wet- en regelgeving en de afspraken die binnen de sectoren van de vitale infrastructuur zijn gemaakt.

   Niveau 1. De student heeft inzicht in de wet- en regelgeving en afspraken op het gebied van security binnen de verschillende sectoren van de vitale infrastructuur.

   Niveau 2. De student kan ervoor zorg dragen dat de implementatie van securitymaatregelen en -plannen in overeenstemming is met de wet- en regelgeving en afspraken binnen de verschillende sectoren van de vitale infrastructuur.

7. De securitymanager kan een risicomanagementsysteem opzetten en implementeren.

   Niveau 1. De student kan een bijdrage leveren aan het opzetten en inrichten van een risicomanagementsysteem.

   Niveau 2. De student kan een risicomanagementsysteem implementeren en zorgdragen voor een op veiligheid gerichte bedrijfscultuur.

8. De bachelor is in staat zijn ontwikkeling te sturen en reguleren, te reflecteren en verantwoordelijkheid te nemen voor zijn handelen, een (ethische) beroepshouding te ontwikkelen en een bijdrage te leveren aan de eigen professionalisering en de professionalisering van het beroep.

   Niveau 1. Ontwikkelt een beeld van het beroep en studiehouding.

   Niveau 2. Neemt op basis van een ethische beroepshouding standpunten in en reflecteert op eigen werk. Kan een kritisch oordeel geven en ontvangen en kan gemotiveerd zijn handelen al dan niet aanpassen. Draagt bij aan de professionalisering van het beroep.

2.3 Body of knowledge and skills (BoKS)

Zonder kennis en vaardigheden kan er geen sprake zijn van competentie. Om die reden wordt in de opleiding veel aandacht geschonken aan de verwerving van inzicht in concepten, modellen, instrumenten en de achterliggend theorieën, alsook aan de toepassing van deze kennis in praktijksituaties. Het gaat om de volgende vakgebieden.

Accounting

Accounting is verankerd in de vakgebieden security management, risk management, en informatiemanagement. In feite genereert de securitymanager belangrijk informatie voor de beheersing van bedrijfsprocessen en uiteindelijk het voortbestaan van een onderneming. De securitymanager zorgt ervoor dat cruciale bedrijfsactiviteiten doorgang kunnen vinden in tijden van crises (Business Continuity). De securitymanager inventariseert en analyseert risico's, maakt plannen en implementeert maatregelen. Hierbij maakt hij gebruik van concepten en methodieken op het gebied van risicomanagement, kwaliteitszorg, compliance, controle en protocol, en van informatiesystemen en informatiemanagement.

Business law and ethics

Business law and ethics liggen verankerd in de vakgebieden Recht, Communicatie & Ethiek, en binnen de Sociale Wetenschappen. Bij de ontwikkeling en implementatie van securitybeleid moet de securitymanager rekening houden met de vigerende wet- en regelgeving. De securitymanager heeft basiskennis van recht, evenals de vaardigheid zich verder te verdiepen in sectorspecifieke, nationale en internationale wet- en regelgeving. Ook moet hij gesprekspartner

kunnen zijn van juridische specialisten binnen een bedrijf en op integere wijze met informatie om kunnen gaan.
Daarnaast krijgt de securitymanager in zijn werk te maken met de ethische kanten van security, zoals het privacy-beleid bij internetgebruik, het omgaan met persoonlijke gegevens, videobewaking en cameratoezicht, het controleren van medewerkers, criminologische analyse en profilering, en gedragsanalyse in bedrijven. De securitymanager moet oog hebben voor deze aspecten en deze betrekken bij de ontwikkeling en invoering van securitybeleid.

Economics
Economics is verankerd in het vakgebied economie en security management. De security manager zorgt voor de security van mensen, bedrijfsprocessen en bedrijfsbezittingen in de vitale infrastructuur. Uitval van producten, diensten of processen in de vitale infrastructuur veroorzaakt maatschappelijke ontwrichting en macro- economische schade. Binnen het bedrijf maakt de security managers economische afwegingen in de keuze tussen risico strategieën en bijbehorende maatregelen.

Finance
Finance is verankerd in het vakgebied economie. Een heel belangrijke taak van de securitymanager is het belang van security onder de aandacht van de board te brengen en te houden. Alleen op die manier zal de board de benodigde middelen reserveren die nodig zijn om de bedrijfsprocessen veilig te stellen. De security manager zal in samenspraak met de financiële deskundigen een kosten-baten analyse moeten kunnen maken van securitymaatregelen en -beleid.

Management information systems
Management information systems is verankerd in het vakgebied Informatie management. De securitymanager moet in staat zijn systematisch informatie te verzamelen omtrent veiligheidsontwikkelingen ten einde risico's te identificeren en securityvraagstukken op de agenda te kunnen plaatsen.

Marketing
Marketing behoort niet tot de core-business van de securitymanager. Binnen de (meestal grote) organisaties is marketing een zaak voor specialisten. In breder perspectief kan marketing ook worden gezien als het "verkopen" en verduidelijken van je diensten aan managers en beslissers. Tevens zal de security manager in het kader van changemanagement het vermogen moeten hebben om draagvlak te creëren voor veranderingen. Deze aspecten zijn verankerd in de vakgebieden Communicatie en ethiek, en Managementvaardigheden.

Organizational behavior

Organizational behavior is verankerd in het vakgebied Sociale Wetenschappen. Security heeft in de kern te maken met het gedrag van individuen en groepen binnen en buiten organisaties. De security manager moet in staat zijn dit gedrag te analyseren en mogelijke risico's voor crimineel gedrag op te sporen. Bij het beveiligen van organisaties speelt het gedrag in organisaties ook een cruciale rol. Bijvoorbeeld bij het creëren van draagvlak bij de board en medewerkers, en bij het bewerkstelligen van gedragsverandering bij medewerkers.

Quantitative techniques

Quantitative techniques is verankerd in het vakgebied Onderzoeksmethodologie en statistiek. Een belangrijke taak van de securitymanager is het inventariseren en analyseren van securityrisico's. Daarvoor heeft hij allerlei technieken ter beschikking op het gebied van onderzoek, methodologie en statistiek. Ook moet hij in staat zijn onderzoeksrapporten op te stellen en te interpreteren.

Strategic management

Strategic management is verankerd in de vakgebieden Security Management, Risico management en Managementvaardigheden. De strategische doelen van een bedrijf hebben consequenties voor het securitybeleid. De securitymanager moet in staat zijn het strategische beleid te vertalen naar een securityplan voor de onderneming.

Operations management

Operations management is verankerd in Security Management en Risico Management. Securitymanagement raakt aan de operations management want securityplannen en -maatregelen hebben doorgaans consequenties voor het verloop van de productieprocessen van goederen en diensten. De securitymanager moet daarom op de hoogte zijn van belangrijke principes op het gebied van operations management.

In de tabellen hieronder zijn de vakgebieden verder uitgewerkt. In de linker kolom staan de vakgebieden zoals ze binnen de opleiding worden genoemd, daaronder de corresponderende kernvakgebieden uit het BBA-profiel.

Vakgebied	Omschrijving	Onderwerpen	Literatuur
Security-management BBA: Accounting	In dit vak verwerven studenten kennis van concepten en methodieken voor het analyseren van beveiligingsrisico's, het opstellen van securityplannen/beleid, het nemen van securitymaatregelen, het managen van risico's/risicomanagement, en het continueren en hervatten van bedrijfsvoering in tijden van crisis.	• Concepten safety, security, risico's (typologieën) • Historie • Veiligheidskaart Nederland • Risicoanalysemethodieken • Vitale infrastructuur en haar kenmerken • Capita selecta	• Certified Protection Officer. Uitgave van IFPO • Jakeman, M. en J. Talbot. (2007). Security Risk Management Body of Knowledge
Risico-management BBA: Accounting	Risicomanagement is de wetenschappelijke benadering van bedrijfsrisico's met als doel deze te reduceren of te elimineren. Bij risicomanagement leren studenten verschillende methodieken toe te passen uit de economie, bedrijfswetenschappen, sociale wetenschappen, systems-engineering en statistiek. Doelstelling is de intern en extern veroorzaakte risico's voor de organisatie op systematische manier te identificeren, te meten en te evalueren. Op grond van deze analyse leren studenten keuzes te maken voor een te hanteren strategie: risico's voorkomen, risico's nemen, risico's verminderen of risico's overdragen.	• Selectie van doelstellingen • Risico identificatie • Risico evaluatie • Maatregelen en besluitvorming • Risicocontrole en beheersing Voor als er toch iets gebeurt: • Crisisbeheersing • Contingency planning • Business continuïty-management	• Claes, P. (2008). Risicomanagement, Noordhoff Uitgevers, 4e druk • Hiles, A. (2007). The definitive handbook of business continuïty management, John Wiley, 2e druk • Vaughan, E.J. (1997). Risk Management, John Wiley

Vakgebied	Omschrijving	Onderwerpen	Literatuur
Informatie-management BBA: Accounting	Een belangrijk vraagstuk waarmee de securitymanager te maken krijgt, is: hoe kunnen de informatiesystemen zo worden ingericht dat zij passen binnen de organisatie en tegelijkertijd beheersing van de security-risico's mogelijk maken? Informatiesytemen en het beheer daarvan zijn niet meer weg te denken in de moderne bedrijfsvoering en in onze samenleving. Enerzijds leveren deze systemen waardevolle informatie op basis waarvan beslissingen worden genomen en waarmee transacties tot stand worden gebracht. Anderzijds kunnen bedreigingen van deze vitale systemen een groot bedrijfsrisico vormen.	• Informatie systemen • Beveiliging van informatiesystemen • Afhankelijkheid- en kwetsbaarheidanalyse • ISO/IEC standaarden o.a. 27001 en 11770	• Boddy, David (2004). Managing informationsystems: an organisational perspective. Prentice Hall • Wemmenhove, P., J. Schreij, en M. Arends (2008). Information Risk Management in de praktijk. Tutein Noltenius
Sociale wetenschappen BBA: Organizational behavior	Sociale wetenschappen zijn een belangrijk gereedschap van de securitymanager om dreigingen te kunnen analyseren. Dreigingen zijn immers het gevolg van opzettelijk menselijk gedrag. Maar ook voor de implementatie van beveiligingsmaatregelen zijn inzichten uit de sociale wetenschappen (met name sociologie en psychologie) van groot belang. De securitymanager dient alert te zijn op het	Selectie uit: • Sociologie • Psychologie • Criminologie/ Criminalistiek	• Dijk, J.J.M. van, I. Sagel-Grande, L. Toornvliet (2005). Actuele criminologie. SDU Juridisch, 5e druk • Wijsman, E. (2005). Psychologie en sociologie. Noordhoff Uitgevers, 4e druk • Reader (website of quickplace). Actuele nationale en internationale veiligheidsrapportages • Reader. Denkers over veiligheid, (o.a. Beck, Wildavsky, Patton, Luhman, Giddens)

Vakgebied	Omschrijving	Onderwerpen	Literatuur
	voorkomen of beheersen van risicovol en crimineel gedrag. Inzicht in deze gedragsvormen en achtergronden daarvan, alsmede kennis van maatschappelijke tendensen helpt de securitymanager tijdig passende pro-actieve, preventieve of repressieve maatregelen te nemen. In deze stroom wordt in het bijzonder ingegaan op gedrag van individuen en groepen zowel binnen de organisatie als daarbuiten. Hoe kan risicovol of crimineel gedrag worden herkend (criminologie), en met welke maatregelen is dit gedrag te beïnvloeden of uit te sluiten? De student maakt kennis met de belangrijkste stromingen en denkers, en met actuele criminalistiek en (inter)nationale veiligheidsrapportages.		

Vakgebied	Omschrijving	Onderwerpen	Literatuur
Recht BBA: Business law and ethics	Met wet- en regelgeving stelt de overheid kaders voor het handelen van burgers en bedrijven. De securitymanager dient op de hoogte te zijn van de voornaamste rechtsgebieden waarin wetten en regels zijn vastgelegd voor zijn handelen en dat van de rechtspersoon waarvoor hij/zij werkt. In de opleiding is bovendien aandacht voor ondernemingsrecht, omgevingsrecht, arbeidsrecht en aansprakelijkheid, aangezien de securitymanager moet zorgdragen voor de bescherming van personen en goederen.	• Burgerlijk recht. In het bijzonder goederen-, ondernemings-, verbintenissen- en arbeidsrecht. • Wettelijke aansprakelijkheid van rechtspersonen. • Wet- en regelgeving m.b.t. opsporingsmethoden, privacy en inzet van beveiligingsorganisaties • (bijzonder) bestuursrecht • Sectorspecifieke wet- en regelgeving • Publiek Private Samenwerking	• Loonstra, C.J. (2007). Hoofdlijnen van het Nederlands Recht. Noordhoff Uitgevers, 8e druk • Groenhuijsen M.S, B. Kortman, A.I.M. van Mierlo e.a. (2008). Verzameling Nederlandse Wetgeving (VNW) relevant studiejaar. • Klaassen, C., R.J.N. Schlössels, G. van Solinge (2003). Aansprakelijkheid in beroep bedrijf of ambt. SDU Juridisch. • Broek, J.H.G. van den (2008). Wegwijzer Wabo en omgevingsvergunning. Kluwer, 2e druk • Voor vitale sectoren relevante (inter)nationale wet- en regelgeving m.b.t. safety en security. (zie ook propedeuse)
Economie BBA: Economics; Finance	Bij het maken van een keuze tussen risicostrategieën en bijbehorende securitymaatregelen spelen verwachte kosten en opbrengsten een belangrijke rol. De securitymanager zal deze in kaart moeten brengen en moeten nagaan welke investeringen en exploitatiekosten aan het nemen van maatregelen zijn verbonden. De securitymanager is in staat om bij zijn advies een passende begroting aan te bieden.	• Costing • Balans en Resultatenrekening • Investering en exploitatie • Begrotingssystematieken • Kosten/baten analyse	• Boer, P. de , M. Brouwers, W. Koetsier (2008). Basisboek bedrijfseconomie. Noordhoff Uitgevers, 8e herziene druk

Vakgebied	Omschrijving	Onderwerpen	Literatuur
Onderzoeks-methodologie en statistiek BBA: Quantitative techniques	De securitymanager voert in de praktijk onderzoek uit, of verstrekt opdracht daartoe. Ook zal hij regelmatig onderzoeksresultaten van anderen onder ogen zien en moeten beoordelen. Het op een wetenschappelijke verantwoorde manier opzetten en uitvoeren van onderzoek is van groot belang voor de validiteit en betrouwbaarheid van de uitkomsten. De securitymanager is geen specialist in onderzoek, maar kan de kwaliteit van onderzoek evalueren en beoordelen, beschrijvende statistieken begrijpen en inschatten wanneer onderzoek het best kan worden uitbesteed.	• Probleemstelling en onderzoeksvragen • Onderzoeksdesign • Onderzoeksfasering • Dataverzamelingsmethoden • Statistische analyse	• Baarda J., M. de Goede (2006). Basisboek methoden en technieken. Stenfert Kroese, 4e druk • Buis, A. (2008). Statistiek om mee te werken. Noordhoff Uitgevers, 8e druk • Boeije, H . (2005). Analyseren in kwalitatief onderzoek. Boom Uitgevers
IT en security	Richt zich op het kunnen opstellen van ICT-beveiligingsbeleid en het kunnen aansturen / bevragen / evalueren van beveiligingsplannen van ICT-beheerders en (diensten)leveranciers ICT is een basis maar tegelijkertijd een risico voor een goede voortgang van bedrijfsprocessen, inclusief informatievoorziening, en de beveiliging van bedrijfsprocessen. In deze kennislijn staat centraal: Het kunnen analyseren en adviseren op het	• ICT security risico's van ICT-trends en de impact op de bedrijfsprocessen; • Het opstellen van een ICT securityplan en internetbeveiliging; • Het implementeren van security maatregelen; ICT risicofactoren, cybercrime en de impact op de vitale infrastructuur; • ICT en Business continuity:	• Trend in business en IT 2012/2013, Barry Derksen • Business Continuity Management Cazemier, J. / Leegwater • Aoufi, S.E. (2011). Cryptografie en ICT: theorie en praktijk. SDU. • GAO-03-251 report - effecten op ICT-gerelateerde business continuity in de financiële sector na de 09/11 aanslagen in de VS; veel voorbeelden (cases) voor algemene blik op security management

Vakgebied	Omschrijving	Onderwerpen	Literatuur
	gebied van beveiligingsattitude en gerelateerde procedures voor gebruikers en ICT en proactief risicoaspecten kunnen inventariseren en maatregelen treffen.	bedrijfsprocessen en informatievoorziening; • Informatiemanagement; • Beveiliging van informatiesystemen; • Adviseren over veilige infrastructuur. • Ook: analyse afhankelijkheden van vitale infrastructuur, elektronische, fysieke en overige bouwkundige beveiliging, brandcompartimentering + brandmeldcentrale + blusmiddelen, personele beveiliging, uitwijkplannen/redundantie, opzet en uitvoeren van inspecties.	• Vitale infra en grote incidenten/ emergency managemen • Hogewoning, K.(2007). Internet security: de beveiliging van aan internet gekoppelde netwerken. HGM. • Luiijf, H.A.M. Understanding Cyber Threats and Vulnerabilities. In: J. Lopez, R. Setola, S.D.Wolthusen (eds), Critical Information Infrastructure Security, Lecture Notes in Computer Science (LNCS) 7130, Springer, 2012. pp. 52-67. • Muller, E.R., Rosenthal, U. en de Wijk, R. (september 2008). Brede 'terrorismebijbel' Bundel Terrorisme, edsKluwer • Wat is procescontrole? Waar zit het en waarom moet ik iets aan beveiliging doen? - NICC Bewustwordingsboekje • Luiijf, H.A.M. (2009). Process Control Security in het Informatieknooppunt Cybercrime. NICC • http://www.samentegencybercrime.nl/UserFiles/File/WT_PCS_brochure-web.pdf

Vakgebied	Omschrijving	Onderwerpen	Literatuur
Communicatie en ethiek BBA: Business law and ethics	De securitymanager moet in staat zijn om op een effectieve manier over securityrisico's, -plannen en -maatregelen zowel schriftelijk als mondeling te communiceren (zowel in het Nederlands als in het Engels). Daarnaast zal de securitymanager vaak in onderhandelingssituaties terecht komen. De security manager moet dan effectief kunnen onderhandelen en daarbij de wederzijdse belangen in het oog houden. Uiteindelijk zal de securitymanager op een professionele manier de raad van bestuur, of de companyboard moeten adviseren. Tot slot komen morele en ethische vraagstukken aan de orde die betrekking hebben op het eigen functioneren en dat van anderen binnen de organisatie.	• Rapporteren • Presenteren • Adviseren • Onderhandelen • Reflecteren op ethische vraagstukken	• Steehouder, M., Jansen, C., Maat, K. (2006). Leren communiceren. Noordhoff Uitgevers, 5e druk • Nathans, H. (2005). Adviseren als tweede beroep. Kluwer, 3e druk • Mastenbroek, W.F.G. (1992). Onderhandelen. Het Spectrum, 5e druk • Dalen, W. van (2007). Basisboek ethiek, morele consequenties voor jonge professionals. Noordhoff Uitgevers
Management-vaardigheden BBA: Organization behavior	De implementatie van maatregelen heeft consequenties voor medewerkers, gebruikers, toeleveranciers en afnemers. Het veranderen van organisatie, werkwijzen of cultuur vereist specifieke vaardigheden gericht op het vergroten van betrokkenheid en de omgang met weerstanden (changemanagement). In de praktijk wordt vaak gebruik gemaakt van een	• Projectmanagement • Changemanagement	• Caluwé, L., & Vermaak, H. (2006), Leren veranderen. Kluwer • Onna, M. van, & Koning A.(2007). De kleine Prins2. Gids voor projectmanagement. Academic Service

	projectmatige manier van werken. Voor een effectieve toepassing van projectmanagement zijn diverse tools en vaardigheden ontwikkeld die kunnen helpen om nieuwe creatieve oplossingen voor security problemen te vinden (projectmanagement). Binnen de opleiding is ook ruime aandacht voor samenstelling van het team, gesprekstechnieken en het onderhouden van de relaties naar andere geledingen van de organisatie.	

Bijlage 1. Kernbegrippen 'security' en 'safety'

Bij 'security' sluit het begrip 'beveiliging' nauw aan. Security verwijst naar specifieke maatregelen die worden getroffen om een persoon of systeem te beveiligen. Het gaat om acties of voorzieningen die gericht zijn tegen een van buiten het betreffende systeem of de persoon komende dreigingsbron, of tegen het wegnemen van effecten van een van buiten komende dreigingsbron. Bij een systeem kan een bedreiging ook van binnen komen. Voorbeelden van security van systemen zijn: bordersecurity, homeland security, beveiliging van netwerken & infrastructuur.
De begripsbepaling van Security sluit aan bij de definitie zoals gehanteerd door de European Security Research Advisory Board (ESRAB):

> ….activities that aim at identifying, preventing, deterring, preparing and protecting against unlawful or intentional malicious acts harming European societies; human beings, organisations or structures, material and immaterial goods and infrastructures, including mitigation and operational continuity after such an attack (also applicable after natural/industrial disorder)[3].

De opleiding Security Management richt zich daarom op het managen van security van personen, systemen en bedrijfsprocessen, en bezittingen, en business continuity (privaat) van bedrijven en organisaties in de sectoren van de vitale infrastructuur.

Het begrip 'safety' sluit nauw aan bij het Nederlandse 'veiligheid'. Het verwijst naar een toestand waarin voor een persoon of een object geen (kans op) een voorval bestaat die het voortbestaan in gevaar kan brengen. We spreken bij objecten bijvoorbeeld over veilige gebouwen en veilige informatienetwerken. Gebruikelijk is om bij personen een onderscheid te maken tussen objectieve en subjectieve veiligheid. Objectieve veiligheid wordt afgemeten aan een toestand in de omgeving van de persoon. In die omgeving kunnen dreigingen zijn die de integriteit of voortleven van de persoon in gevaar brengen. Subjectieve veiligheid heeft betrekking op de denkbeelden die een persoon zelf heeft over dreigingen uit de omgeving.
De opleiding Integrale Veiligheidskunde leidt op tot dienstverlener, projectmanager beleidsmedewerker; de veiligheidskundige analyseert hoe mensen zich in hun omgeving fysiek en sociaal veilig voelen en brengt partijen integraal bij elkaar om tot oplossingen te komen. Veiligheidskundigen werken bij overheidsinstanties, non-profit of beveiligingsbedrijven.

De scheiding die traditioneel binnen organisaties bestaat tussen 'security' enerzijds en 'safety' anderzijds vraagt een specifieke benadering. Een integrale benadering van veiligheid waarbij dreigingen van buitenaf of van binnenuit worden geanalyseerd en in verband worden gebracht met veiligheidseffecten en -risico's voor de voortgang van de bedrijfsprocessen vormt de basis voor een bedrijfsmatige afweging van te nemen securitymaatregelen. Dit betekent ook dat traditionele cultuurverschillen tussen security-organisatieonderdelen overwonnen moeten worden en er afstemming moet zijn met externe partijen zoals politie en brandweer.
De verhouding tussen safety en veiligheidseffecten enerzijds en security-risico's en bedrijfsmatige business continuity anderzijds is een aandachtspunt binnen de bacheloropleiding Security Management.

De toenemende rol van IT maakt ook dat er een inspirerende kwalitatieve connectie is met ict security. Er is een keuze voor de invoering van onderwerpen uit de global IT security standaard CISSP gemaakt en de kwaliteitsmatch met Information Security Management van de HHS.

Bijlage 2. Opleidingscompetenties en Dublindescriptoren

	Opleidingscompetenties							
Dublindescriptoren	1 Analyseren interne en externe risico's	2 Securityplannen en -beleid ontwikkelen	3 Inzetten van mensen en middelen	4 Inzetten van IT	5 Zorgdragen voor business continuity	6 Toepassen binnen wet- en regelgeving	7 Opzetten en implementeren risicomanagement-systeem	8 Zelfsturing en professionalisering
Kennis en inzicht	+	+	+	+	+	+	+	+
Toepassen kennis en inzicht	+	+	+	+	+	+	+	
Oordeelsvorming	+	+	+	+	+	+		
Communicatie			+		+		+	
Leervaardigheden								+

Kennis en inzicht

Heeft aantoonbare kennis en inzicht van een vakgebied, waarbij wordt voortgebouwd op het niveau bereikt in het voortgezet onderwijs en dit wordt overtroffen; functioneert doorgaans op een niveau waarop met ondersteuning van gespecialiseerde handboeken, enige aspecten voorkomen waarvoor kennis van de laatste ontwikkelingen in het vakgebied vereist is.

De benodigde kennis, inzicht en vaardigheden waarover de security manager moet beschikken om de competenties te kunnen ontwikkelen, is vastgelegd in de Body of Knowledge en Skills (zie paragraaf 2.3). Het vakgebied van security is nog relatief jong waardoor ontwikkelingen elkaar in snel tempo opvolgen. De opleiding maakt gebruik van de meest actuele literatuur op het gebied van security en security-management. Deze literatuur is aangedragen door specialisten uit het werkveld van security. De beroepenveldcommissie van de opleiding wordt nauw betrokken bij het regelmatig actualiseren van de BoKS en de literatuurlijst naar aanleiding van ontwikkelingen in het werkveld.

Toepassen kennis en inzicht

Is in staat om zijn/haar kennis en inzicht op dusdanige wijze toe te passen, dat dit een professionele benadering van zijn/haar werk of beroep laat zien, en beschikt verder over competenties voor het opstellen en verdiepen van argumentaties en voor het oplossen van problemen op het vakgebied.

De opleidingscompetenties 1 t/m 7 (paragraaf 2.2) weerspiegelen de professionele benadering van het werk. Deze kan worden gekenmerkt als het systematisch oplossen van securityvraagstukken. Deze aanpak begint met een gedegen analyse van het vraagstuk in een brede context. De analyse mondt uit in aangrijpingspunten voor oplossingen in de vorm van securitybeleid en -plannen.

Oordeelsvorming

Is in staat om relevante gegevens te verzamelen en interpreteren (meestal op het vakgebied) met het doel een oordeel te vormen dat mede gebaseerd is op het afwegen van relevante sociaalmaatschappelijke, wetenschappelijke of ethische aspecten.

Het verzamelen, interpreteren en beoordelen van gegevens ligt met name plaats besloten in competentie 1. Deze competentie houdt onder andere in dat de securitymanager uit een grote hoeveelheid data die gegevens kan inventariseren en analyseren die relevant zijn voor de beveiliging van bedrijven en sectoren in de vitale infrastructuur.

Het maken van afwegingen ligt besloten in competentie 2, 3 en 4, met name op niveau 2. De securitymanager moet hier zorgvuldige afwegingen maken bij de inzet van mensen en middelen, en hierbij rekening houden met de geldende wet- en regelgeving. Oordeelsvorming wordt in de opleiding ook ontwikkeld in de onderzoeksvakken (BoKS), met name bij het interpreteren van onderzoeksresultaten, het trekken van conclusies en het doen van aanbevelingen op basis van de conclusies. In de opleiding wordt verder ook aandacht besteed aan morele en ethische vraagstukken die betrekking hebben op het functioneren van de securitymanager en dat van anderen binnen een organisatie.

Communicatie

Is in staat om informatie, ideeën en oplossingen over te brengen op publiek bestaande uit specialisten of niet-specialisten.

Deze descriptor wordt met name geborgd door competentie 3, 5 en 7, en de BoKS van de opleiding. De securitymanager moet zorgdragen dat security hoog op de agenda staat van de board van een bedrijf of onderneming. Dat betekent dat de securitymanager moet overtuigen in woord en geschrift. Daarnaast moet de securitymanager zorgdragen voor de effectieve inzet van mensen en middelen bij de implementatie van securitymaatregelen, beveiligingsplannen en risicomanagementsystemen. Gedragsverandering is daarbij een sleutelwoord. In de BoKS van de opleiding is veel aandacht voor mondelinge en schriftelijke communicatieve vaardigheden (zowel in het Nederlands als in het Engels), alsook voor managementvaardigheden.

Leervaardigheden

Bezit de leervaardigheden die noodzakelijk zijn om een vervolgstudie die een hoog niveau van autonomie veronderstelt aan te gaan.

De leervaardigheden van de securitymanager zijn geborgd door competentie 8. Het gaat hier om het leervermogen en de loopbaanvaardigheden. Het leervermogen heeft betrekking op de vaardigheden van de student (en toekomstig security-manager) doelen te stellen, informatie te zoeken en te verwerken, en het leerproces te evalueren en bij te sturen. Bij de loopbaanvaardigheden gaat het om het identificeren van ambities en motieven, het vaststellen van eigen kwaliteiten en het maken van keuzes in opleiding en loopbaan die passen bij de eigen ambities en professionele kwaliteiten.

[3] ESRAB (2006), Meeting the challenge, the European Security Research Agenda, blz. 18