Competenties informatiebeveiliging en privacy

IBPDOC12

GEBRUIKERSGROEP IBP IN HET MBO

Kennisnet SURF saMBO-ICT

Verantwoording

Auteurs

Leo Bakker (Kennisnet)
Mireille Boonstra-Kints (Kints Fuwa Advies)
Ludo Cuijpers (saMBO-ICT, Kennisnet en ROC Leeuwenborgh)
Casper Schutte (ROC Midden Nederland)
Job Vos (Kennisnet)

Met dank aan:

Met dank aan de 40 deelnemers van de Masterclasses.

Versie 2.0, juli 2015

Sommige rechten voorbehouden

Inhoudsopgave

1

Verantwoording 2
Inleiding 4
1. Informatiebeveiliging en Privacy 6

1.1 Samenhang Informatiebeveiliging en Privacy 6
1.2 Gecombineerde rollen 6
1.3 Voorbeeld overlap Privacy en Informatiebeveiliging 6
1.4 Samenwerking ibp met jurist en applicatie/ict beheer. 7

2. Taken manager ibp 8

2.1 Globaal overzicht 8
2.2 Creëren awareness ○ 8
2.3 In kaart brengen Risico's & Uitdagingen ● 9
2.4 Implementeren Algemeen Beleid ● 9
2.5 Aansturen ibp organisatie ● 9
2.6 Door ontwikkelen ibp architectuur ● 10
2.7 Uitvoeren en reviewen audits ● 10
2.8 Taken coördinator ibp 11

3. Kennis, vaardigheden en contacten 12

3.1 Competenties 12
3.2 Kennis en vaardigheden 12
3.3 Contacten 12
3.4 Functionaris gegevensbescherming (P) 13

3.4.1 Inleiding 13
3.4.2 Melden gegevensverwerking 13
3.4.3 Eisen aan FG 13
3.4.4 Bevoegdheden FG 14

4. Scholing manager ibp 15

4.1 Scholing saMBO-ICT en Kennisnet 15
4.2 Particuliere scholing op hbo niveau 15
4.3 Particuliere scholing op universitair niveau 15

Bijlage 1a: Manager informatiebeveiliging en privacy (voorbeeld functiebeschrijving) 16
Bijlage 1b: Coördinator informatiebeveiliging en pivacy (voorbeeld functiebeschrijving) 19
Bijlage 1c: Functionaris Gegevensbescherming (voorbeeld functiebeschrijving) 22
Bijlage 2: Actieve Masterclasses ibp 25
Bijlage 3: Competentieprofielen ibp functies 27

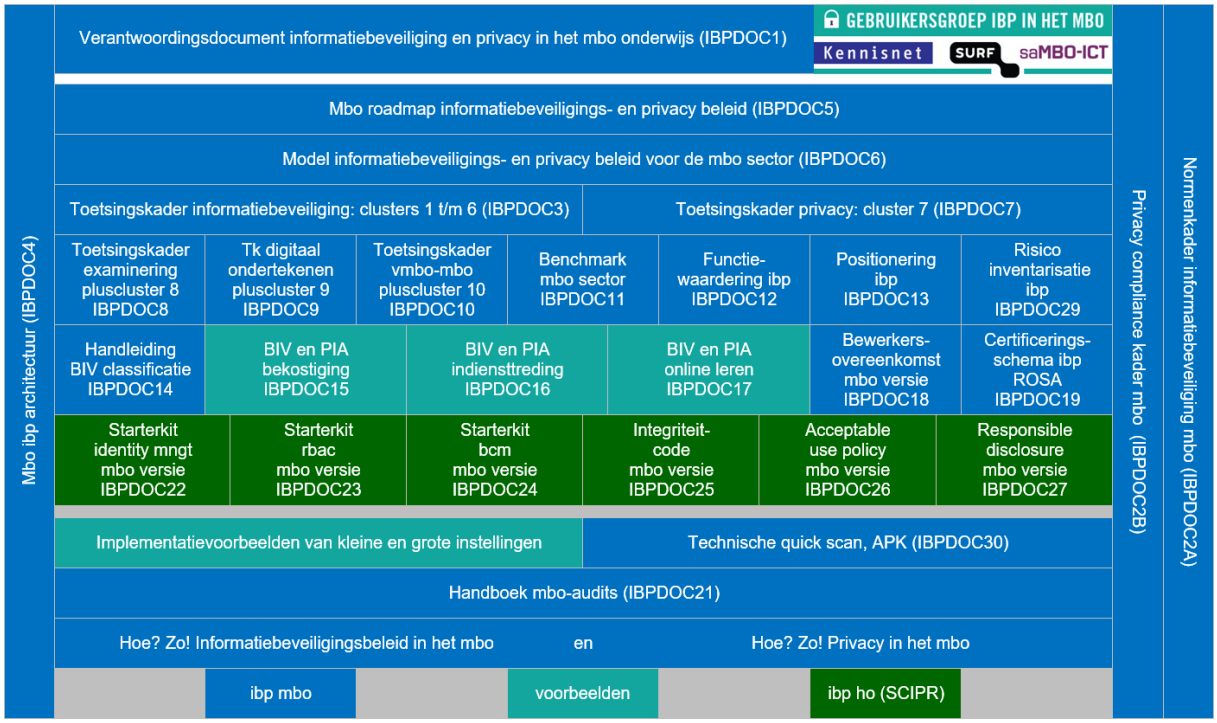
Chief Information Security Officer (CISO) 29
Information Security Officer (ISO) 30
ict-beveiligingsmanager 31
ict-beveiligingsspecialist 32

Bijlage 4a: Opleidingsaanbod op HBO niveau 33
Bijlage 4b: Opleidingsaanbod op universitair niveau (EMITA) 37
Bijlage 5: Framework informatiebeveiliging en privacy in het mbo 41

Inleiding

De mbo sector is zich zeer bewust van de urgentie en belang van informatiebeveiliging en privacy beleid en veel scholen zijn er intussen concreet mee aan de slag gegaan of hebben plannen in die richting op stapel staan. In een brede samenwerking tussen het mbo-onderwijsveld, saMBO-ICT, MBO Raad, Kennisnet en SURF is een programma Informatiebeveiligingsbeleid (IB) ontwikkeld en in uitvoer genomen om als sector een adequaat antwoord op de uitdagingen te geven en de scholen te voorzien van de juiste handreikingen en tooling om de problematiek op een juiste wijze aan te pakken.

Een breed gedragen projectplan vanuit saMBO-ICT heeft de aanzet gegeven voor het IBP programma. Een breed samengestelde taskforce geeft leiding aan het programma en de uitvoering van de diverse activiteiten is door een aantal werkgroepen ter hand genomen. Hierbij leveren de mbo-instellingen zelf een grote bijdrage. Dit document schetst de uitgangspunten voor het programma, de samenhang met externe factoren en het geeft als zodanig ook een verantwoording voor de gekozen aanpak en de gemaakte keuzes. Ook worden de te verwachten resultaten van het programma gepresenteerd.
Om dit alles overzichtelijk te bundelen heeft de taskforce ibp heeft een compleet framework[1] opgesteld waarin is weergegeven welke elementen in het informatiebeveiligingsbeleid en bij privacy van belang zijn, welke documenten die elementen beschrijven en welke handreikingen en tooling er voor het onderwijsveld ontwikkeld wordt. Ook is daarin aangeven welke onderdelen vanuit het SURF programma informatiebeveiliging en privacy direct worden benut.



Het voorliggende document IBPDOC12 Competenties gaat dieper in op de taken, competenties en scholingsmogelijkheden van de informatiebeveiliging en privacy manager (kortweg manager ibp) en de daarvan afgeleide ibp coördinator.

[1] Verantwoordingsdocument programma informatiebeveiliging en privacy (ibp) in het mbo (IBPDOC1).

In hoofdstuk 1: informatiebeveiliging en privacy wordt kort aangegeven waarom de combinatie rollen Informatiemanager en Privacy manager wenselijk is. Indien een mbo instelling kiest voor twee functionarissen dat is mogelijk en kan dit document ook gebruikt worden.
In hoofdstuk 2: worden de taken van de manager ibp beschreven en worden de taken geplot op het framework.
In hoofdstuk 3: worden de gewenste competenties van de manager ibp beschreven.
In hoofdstuk 4: komt het scholingsaanbod aan de orde. Zowel op hbo als universitair niveau.

De bijlagen bevatten functie beschrijvingen, uitgebreide competentie beschrijvingen, scholingsmogelijkheden en functiebeschrijvingen.

1. Informatiebeveiliging en privacy

1.1 Samenhang informatiebeveiliging en privacy

Er is veel overlap tussen informatiebeveiliging en privacy. In het framework ibp voor het mbo zijn 30 documenten genoemd. Een zestal documenten kunnen toegewezen worden aan privacy, een zevental documenten aan informatiebeveiliging en er zijn 17 gemeenschappelijke documenten.

1.2 Gecombineerde rollen

Dit document gaat beschrijft de gecombineerde functie informatiebeveiliging en privacy maar zal wel bij de taken en competenties de letters **IB** (Informatiebeveiliging) en **P** (Privacy) vermelden waardoor een splitsing van de rollen in afzonderlijke functies alsnog mogelijk is.

1.3 Voorbeeld overlap privacy en informatiebeveiliging

Samenvattend kan gesteld worden dat bij privacy de wetgeving centraal staat en dat informatiebeveiliging de uitvoer en beheersing van deze wetgeving mogelijk maakt. Een voorbeeld om een en ander toe te lichten.

Voorbeeld	***Het College van Bestuur van een mbo instelling wil graag de mogelijkheid laten onderzoeken om tijdens ziekte van een medewerker zijn/haar onderwijs gerelateerde mail te mogen gebruiken. De mail omgeving is eigendom van de mbo instelling.***
Privacy beleid	Vanuit de privacywetgeving is dit niet toegestaan. Een oplossing is om aan de OR een voorstel voor te leggen waarbij gegarandeerd wordt dat binnen de e-mail omgeving door de medewerker een map “Privé” wordt aangemaakt. Deze map zal nooit bekeken worden tijdens langdurige ziekte van een medewerker, maar alle andere e-mails mogen door en specifiek daartoe aangewezen functionaris bekeken worden. Als de OR (op basis van WOR, artikel 27, lid k)[2] hiermee akkoord gaat dan kan dit beleid worden geeffectueerd.
Informatiebeveiligingsbeleid:	
	Beleid: Er moet een beleid “e-mail inzage” worden voorgelegd aan de OR en na instemming is dit een aanvulling op de arbeidsovereenkomst.
	Personeel: Personeel en externen moeten worden geïnformeerde en eventueel getraind.
	Toegang: De fysieke toegang tot de exchange server (e-mail) moet goed geregeld zijn om de privacy te waarborgen.
	Continuïteit: Tijdens grote verstoringen moet de e-mail omgeving veilig opgeslagen zijn en eventueel d.m.v. een back up teruggeplaatst worden.
	Applicaties: De toegang tot de e-mail omgeving (applicatie toegang) is alleen voorbehouden aan de eigenaar en in een noodsituatie aan de applicatie beheerder die toegang heeft en kan verschaffen tot de e-mail van een medewerker, behalve de Privé-map.

[2] **WOR, artikel 27, lid k.**
De ondernemer behoeft de instemming van de ondernemingsraad voor elk door hem voorgenomen besluit tot vaststelling, wijziging of intrekking van:
k. een regeling omtrent het verwerken van alsmede de bescherming van de persoonsgegevens van de in de onderneming werkzame personen;

Logging: De eigenaar van de e-mail moet ten allen tijde kunnen controleren wie er toegang heeft gehad tot zijn e-mails. Ook moeten hij kunnen controleren dat de Privé-map niet is bekeken.

1.4 Samenwerking ibp met jurist en applicatie/ict beheer.

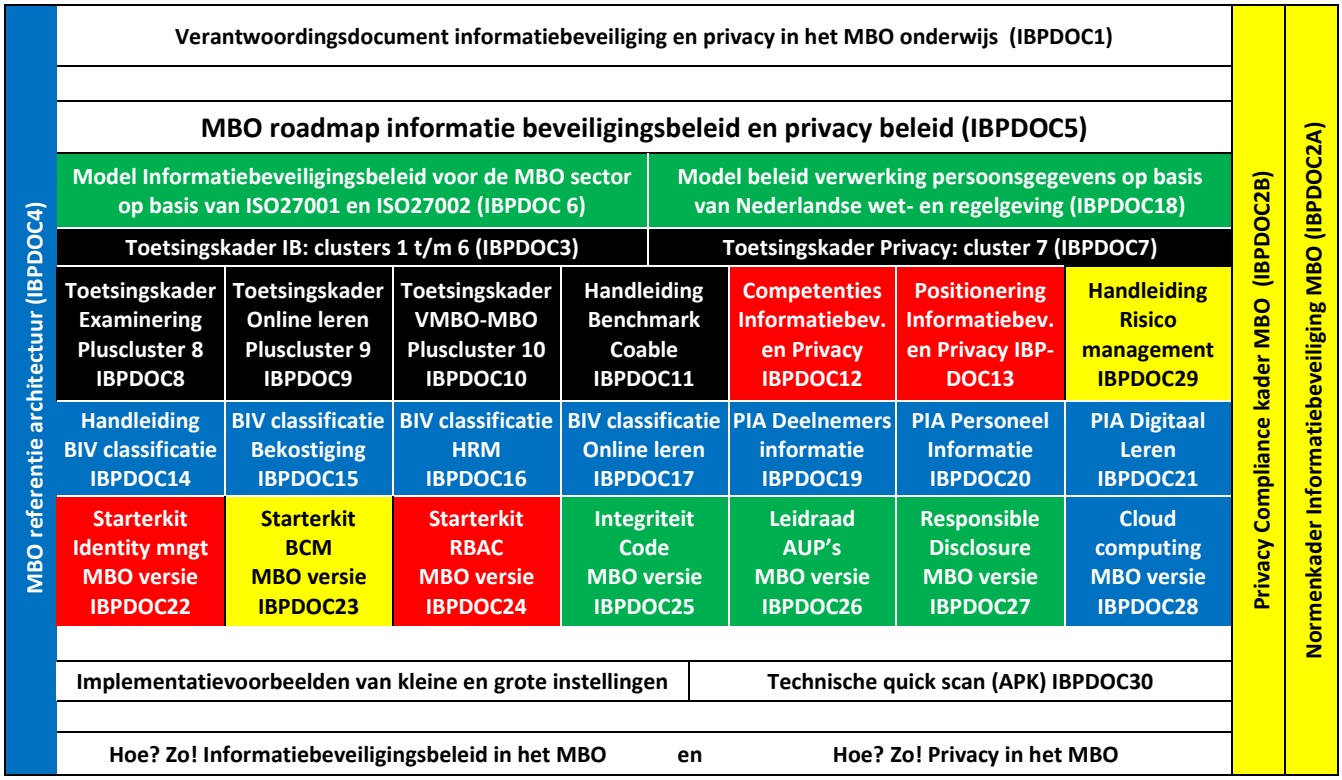
De vervlechting privacy en informatiebeveiliging is in dit document het uitgangspunt. Een en ander vaak ook vanuit kostentechnische overwegingen. Vaak is het voor een mbo instelling financieel niet haalbaar om 2 functionarissen te benoemen. Voorwaarde is wel dat de ibp-manager of ibp-coördinator kan terugvallen op de jurist bij complexe privacy vraagstukken en op het hoofd applicatiebeheer en/of het hoofd ict beheer bij complexe ict vraagstukken.

2. Taken manager ibp

2.1 Globaal overzicht

De volgende taken kunnen voor een manager ibp, zoals beschreven in de roadmap, worden onderscheiden[3]:

- ○ Creëren **Awareness**;
- Inkaart brengen **Risico's & Uitdagingen**;
- Implementeren **Algemeen Beleid**;
- Aansturen **ibp Organisatie**;
- Door ontwikkelen ibp **Architectuur**;
- Uitvoeren en reviewen **Audits**.



2.2 Creëren awareness ○

In eerste instantie moet de manager ibp awareness creëren bij het College van Bestuur. De "Hoe? Zo!' –boekjes kunnen hierbij helpen. Implementatie voorbeelden van andere mbo en hoinstellingen zijn (op termijn) beschikbaar. De mbo roadmap biedt vervolgens de mogelijkheid om de mbo instelling door te lichten om vervolgens met concrete aanbevelingen te komen om te komen tot een gedegen Informatiebeveiliging- en Privacy beleid.
In tweede instantie moet de manager ibp de randvoorwaarden creëren voor een sprankelende awareness campagne.
Deze kan bestaan uit:
Een verplichte awareness campagne ibp voor de ict staf medewerkers;

[3] Bron: Bart van den Heuvel, Corporate Information Security Officer, Universiteit Maastricht.

ibp-scholing voor alle medewerkers van de mbo instelling;
ibp informatie verstekken op de website van de mbo instelling;
Gebruik maken van de SURF CyberSaveYourself Campagne (http://www.surfsites.nl/csy-uk/);
Alle medewerkers deel laten nemen aan de SmartSecureYourself game (licentie noodzakelijk).

De manager ibp kan over de volgende documenten beschikken:

IBPDOC1	Verantwoordingsdocument ib en privacy in het mbo
IBPDOC5	Mbo roadmap informatie beveiligingsbeleid
IBPDOC30	Technische quick scan (APK) en SURF producten **(IB)**
	Implementatievoorbeelden van kleine en grote instellingen
	Hoe? Zo! Informatiebeveiligingsbeleid in het mbo
	Hoe? Zo! Privacy in het mbo

2.3 In kaart brengen Risico's & Uitdagingen

De manager ibp moet risico in kaart brengen voor een mbo instelling. Deze zijn op een viertal hoofdgebieden onder te verdelen:

1A	Beleid, organisatie en personeel Informatiebeveiliging **(IB)**
1B	Beleid, organisatie en personeel Privacy **(P)**
	Cluster: 1, 2 en **7**
2A	Techniek en interne koppelingen
2B	Techniek en externe koppelingen
	Cluster: 3, 4 en 9
3	Applicaties en audit
	Cluster: 5 en 6
4	Examineren
	Cluster: 8

De manager ibp moet de risico's die de bedrijfscontinuïteit kunnen verstoren in kaart brengen en vervolgens beleid ontwikkelen om de gevolgen te minimaliseren.

Uitdagingen, zoals de nieuwe privacy wetgeving, moeten door de manager ibp voortvarend worden opgepakt.

De manager ibp kan over de volgende documenten beschikken:

IBPDOC2A	Normenkader Informatie beveiliging mbo **(IB)**
IBPDOC2B	Compliance kader privacy in het mbo **(P)**
IBPDOC23	Starterkit BCM mbo versie
IBPDOC29	Handleiding Risico management

2.4 Implementeren algemeen beleid

De manager ibp ontwikkelt samen met de proceseigenaren beleid in het kader van Informatiebeveiliging en Privacy. Ook neemt hij het voortouw om ibp beleid te maken dat specifiek gericht is op studenten, medewerkers en ict medewerkers.

De manager ibp kan over de volgende documenten beschikken:

IBPDOC6	Model Informatiebeveiligingsbeleid voor de mbo sector op basis van ISO27001 en 27002 **(IB)**
IBPDOC18	Modelbeleid verwerking persoonsgegevens **(P)**
IBPDOC25	Integriteit Code mbo versie
IBPDOC26	Leidraad AUP's mbo versie
IBPDOC27	Responsible Disclosure mbo versie

2.5 Aansturen ibp organisatie

De manager ibp regelt binnen een mbo instelling 3 zaken:

1. Opzetten van een CSIRT (Computer Security Incident Response Team);

Dit team bestaande uit ict-collega's, functioneel beheerders, communicatiemedewerkers, lid College van Bestuur en proceseigenaren (eventueel aan te vullen met andere medewerkers) zorgt ervoor dat tijdens grote incidenten, onder leiding van de manager ibp, de verstoring zo snel mogelijk wordt hersteld.

2. Inrichten van een ibp incidenten registratie.
   Dit kan, bijvoorbeeld, met behulp van Topdesk. Niet alleen worden de "normaal" voorkomende incidenten geregistreerd, maar ook de speciale incidenten zoals haat mail, bedreigingen en fraude.
3. Vervaardigen van regelmatige ibp rapportages.

De manager ibp kan over de volgende documenten beschikken:

IBPDOC12	Competenties Informatiebeveiliging en Privacy
IBPDOC13	Positionering Informatiebeveiliging en Privacy
IBPDOC22	Starterkit Identity mgt mbo versie
IBPDOC24	Starterkit RBAC mbo versie

2.6 Door ontwikkelen ibp architectuur ●

De manager ibp "verrijkt" de standaard informatie-, applicatie-, proces- en technische architectuur met:

- Classificaties (BIV);
- Assessments (PIA);
- Baselines;
- Cloud kaders;
- Etc.

Niet alleen is de interne organisatie van belang maar ook de beheersing van de keten. Erkenning en accreditering (instelling, opleiding en onderwijspersoneel);

- Leerrouteplanning;
- Ontwikkelen leermiddelen;
- Aanmelden;
- Inschrijven;
- Preventie schooluitval;
- Zorg en begeleiding;
- Onderwijsontwikkeling;
- Beroepspraktijkvorming;
- Kwaliteitsborging en toezicht;
- Toetsen en examinering;
- Informatielevering (deelnemersgegevens en onderwijspersoneel);
- Informatiedoorlevering (van GBA, NHR en BRI aan SUWI, CBS en gemeenten);
- Bekostiging;
- Verantwoording.

De manager ibp kan over de volgende documenten beschikken:

IBPDOC4	Mbo referentie architectuur (inclusief keten)
IBPDOC14	Handleiding BIV classificatie
IBPDOC15	BIV classificatie Bekostiging
IBPDOC16	BIV classificatie HRM
IBPDOC17	BIV classificatie Online leren
IBPDOC19	PIA Deelnemers informatie **(P)**
IBPDOC20	PIA Personeel Informatie **(P)**
IBPDOC21	PIA Digitaal Leren **(P)**
IBPDOC28	Cloud computing mbo versie

2.7 Uitvoeren en reviewen Audits ●

Uiteindelijk moet de manager ibp in staat zijn om de ibp volwassenheid van zijn mbo instelling te beoordelen. Dit kan op basis van een assessment. Een volgende stap kan een volledige audit zijn.

De manager ibp kan over de volgende documenten beschikken:

IBPDOC3	Toetsingskader Informatie Beveiliging **(IB)**
IBPDOC7	Toetsingskader Privacy in het mbo **(P)**
IBPDOC8	Toetsingskader Examinering Pluscluster 8 **(IB)**
IBPDOC9	Toetsingskader Online leren Pluscluster 9 **(IB)**
IBPDOC10	Toetsingskader vmbo-mbo Pluscluster 10 **(IB)**
IBPDOC11	Handleiding Benchmark Coable

2.8 Taken coördinator ibp

In voorkomende gevallen kan het zo zijn dat er gekozen wordt om de (strategische) beleidsmatige taken onder te brengen bij de Informatiemanager of de directeur ict. In deze situatie wordt de implementatie van het Statuut Informatiebeveiliging en de uitvoerende werkzaamheden ondergebracht bij een coördinator ibp. De coördinator ibp zal in de lijn zal worden aangestuurd door een leidinggevende. De coördinator ibp is dan niet verantwoordelijk voor het beleid maar beschrijft het en voert het eventueel uit. Doordat de bijdrage aan het beleid en de verantwoordlijkheden elders zijn belegd heeft deze functionaris een andere inschaling.

3. Kennis, vaardigheden en contacten

3.1 Competenties

In een overleg tussen saMBO-ICT /Kennisnet en Gartner werden de volgende competenties benoemd die van belang zijn voor een goed functionerende manager ibp:

- Kennis van informatiebeveiliging en privacy;
- Kennis van ict ontwikkelingen;
- De taal van het onderwijs spreken;
- Makkelijk aangaan van relaties binnen de mbo instelling;
- Strategisch kunnen denken en werken;
- Beschikken over audit vaardigheden.

In de volgende paragrafen wordt dit uitgewerkt.

3.2 Kennis en vaardigheden[4]

De manager ibp beschikt over de volgende kennis en vaardigheden

- wo werk- en denkniveau;
- kennis van (Informatie)beveiliging en Privacy wetgeving.
- kennis en vaardigheid op het gebied van financiële zaken(begrotingsvoorbereiding, budgetbewaking) met als doel om de kosten van informatiebeveiliging beheersbaar te houden**;**
- kennis van en inzicht in de taak- en doelstelling en de werkwijze van de organisatie van de onderwijsinstelling;
- inzicht in de bedrijfs- en onderwijsprocessen binnen de onderwijsinstelling;
- vaardigheid in het ontwikkelen van adviezen projectresultaten, voorgestelde of gekozen oplossingsrichtingen en alternatieven, nieuwe ideeën of concepten;
- vaardigheid in het omgaan met verschillenden belangen en het kunnen overtuigen op basis van argumenten; vaardigheid in projectmatig werken;
- vaardigheid in het opstellen van beleidsvoorstellen;
- vaardigheid in het initiëren van nieuwe ontwikkelingen op het eigen vakgebied;
- communicatieve vaardigheden**.**

3.3 Contacten

De manager ibp moet investeren in de volgende relaties:

- College van Bestuur;
- Directeuren, met name proceseigenaren;
- Directeur HR;
- Medewerkers;
- Deelnemers;
- Externen;
- Kwaliteitszorg manager;
- Hoofd ict;
- Hoofd applicatiebeheer;
- Bedrijfsjurist;
- Controller;
- Ondernemingsraad;
- Externe dienstverleners (bedrijven);
- saMBO-ICT;
- Kennisnet;
- OCW;

[4] Bron functiebeschrijving informatiemanager.

- etc.

3.4 Functionaris gegevensbescherming (P)

In het Privacy Compliance kader (IBPDOC2B) is de norm opgenomen dat de instelling een functionaris voor gegevensbescherming (FG) benoemt. Slechts indien dat niet wenselijk of mogelijk is, stelt de instelling een privacy officer (PO) aan. Het belangrijkste verschil is dat de FG een in de wet verankerde functie, ontslagbescherming geniet. Indien er gekozen is om in plaats van een FG een PO aan te stellen, kan deze voor (een selectie van) de hierna te noemen werkzaamheden in de plaats komen van de FG.

Het is logisch en verdedigbaar dat de manager ibp / coördinator ook de rol van functionaris gegevensbescherming krijgt toegewezen. Maar het is zeker geen must. Een korte beschrijving van de specifieke taken van de FG. Deze taken komen op hoofdlijnen overeen met de taken zoals die beschreven zijn in hoofdstuk 2.

3.4.1 Inleiding

(Branche)organisaties hebben de mogelijkheid zelf een interne toezichthouder op de verwerking van persoonsgegevens aan te stellen. Zo iemand wordt een functionaris voor de gegevensbescherming (FG) genoemd. De FG houdt binnen de organisatie toezicht op de toepassing en naleving van de Wet bescherming persoonsgegevens (Wbp). Tussen haakjes staan de vergelijkbare taken zoals die beschreven zijn in hoofdstuk 2:

- toezicht houden op de naleving van wet- en regelgeving, alsmede op naleving van het privacy beleid, met inbegrip van de toewijzing van verantwoordelijkheden (2.5 Aansturen ibp organisatie);
- (ongevraagd) adviseren van het CvB en alle bij gegevensverwerkingen betrokken medewerkers over hun (wettelijke) verplichtingen (2.5 Aansturen ibp organisatie);
- inventarisaties van gegevensverwerkingen maken (2.5 Aansturen ibp organisatie);
- registeren van gegevensverwerkingen (2.5 Aansturen ibp organisatie);
- vragen en klachten van mensen binnen en buiten de organisatie afhandelen (2.5 Aansturen ibp organisatie);
- interne regelingen ontwikkelen (2.4 Implementeren Algemeen Beleid);
- adviseren over en uitvoeren van gegevensbeschermingseffectbeoordelingen (2.6 door ontwikkelen ibp architectuur);
- toezien op de uitvoering van audits (2.7 uitvoeren en reviewen audits);
- adviseren over technologie en beveiliging (privacy by design) (2.6 Door ontwikkelen ibp architectuur) ;
- bewustwording stimuleren en opleiding van het bij de verwerking betrokken medewerkers (2.2 creëren awareness);
- input leveren bij het opstellen of aanpassen van een gedragscode (2.4 Implementeren Algemeen Beleid).

3.4.2 Melden gegevensverwerking

Een organisatie die persoonsgegevens verwerkt, moet dit melden bij de Autoriteit Persoonsgegevens (voorheen CBP genaamd). Maar is een FG aangesteld, dan kan de organisatie de verwerkingen bij de FG melden in plaats van bij de AP.
Organisaties kunnen zelf bepalen hoe zij het meldingsproces inrichten, voor zover zij zich daarbij aan de wettelijke regels houden. FG's kunnen een speciale versie van het Wbp-Meldingsprogramma van de AP gebruiken.

Let op: is voor een gegevensverwerking een zogeheten voorafgaand onderzoek nodig? Zoals in het geval van heimelijke (camera)observaties of bij het registreren van strafrechtelijke gegevens, dan moet de organisatie de verwerking wél bij de AP melden.

3.4.3 Eisen aan FG

De AVG stelt een aantal eisen aan FG's.
1. Een FG moet een natuurlijk persoon zijn. Een ondernemingsraad of commissie komt dus niet in aanmerking.
2. Een FG wordt geselecteerd op grond van zijn professionele kwaliteiten en, in het bijzonder, zijn deskundigheid op het gebied van de wetgeving en de praktijk inzake gegevensbescherming. Een FG hoeft echter geen jurist te zijn.

3. Een FG moet in staat zijn om onafhankelijk te kunnen handelen, adviseren en toezicht te houden op alle verwerkingen van persoonsgegevens binnen de instelling.
4. Een FG moet voldoende kennis hebben van de organisatie en interne relaties en verhoudingen binnen de organisatie.
5. Een FG moet betrouwbaar zijn, wat zich onder meer uit in een geheimhoudingsplicht.

3.4.4 Bevoegdheden FG

Een FG heeft in de wet verankerde formele sanctiebevoegdheden. Daarnaast moet de organisatie de FG de nodige controlebevoegdheden geven, en om de FG de nodige middelen ter beschikking te stellen om zijn bevoegdheden naar behoren uit te oefenen. Anders dan een PO, heeft een FG bevoegdheid om ruimtes te betreden, zaken te onderzoeken en inlichtingen en inzage te vragen (vorderen). Deze inzage of toegang is niet afhankelijk van (incidentele) toestemming van een CvB. Het heeft de voorkeur om een reglement vast te stellen voor de taken en bevoegdheden van de FG (PO). De FG moet in onafhankelijkheid zijn werkzaamheden kunnen verrichten binnen een organisatie.
Een door het CvB aangestelde FG heeft, anders dan een PO, dezelfde ontslagbescherming als leden van een ondernemingsraad. Dit betekent dat hij pas ontslagen kan worden na toestemming van de kantonrechter.

4. Scholing manager ibp

4.1 Scholing saMBO-ICT en Kennisnet

Allereerst is zijn er de masterclasses ibp die verzorgd worden door saMBO-ICT en Kennisnet, waar de volgende onderdelen aan de orde komen.

- Creëren **Awareness**;
- In kaart brengen **Risico's & Uitdagingen**;
- Implementeren **Algemeen Beleid**;
- Aansturen **ibp organisatie**;
- Door ontwikkelen ibp **architectuur**;
- Uitvoeren en reviewen **audit;**
- **Privacy.**

Bijlage 1 beschrijft de inhoud van de Actieve Masterclasses ibp.
In de toekomst zullen er (waarschijnlijk) ook specifieke scholingen worden aangeboden op het gebied:

- Risico management;
- Ibp architectuur;
- Peer auditing;
- Privacy.

4.2 Particuliere scholing op HBO niveau

Vervolgens zijn er de commerciële scholingsmogelijkheden zoals die aangeboden worden door verschillende (gerenommeerde) onderwijsinstellingen.
In bijlage 2 worden de competenties van de volgende beroepsprofielen beschreven:

- Chief Information Security Officer (CISO);
- Information Security Officer (ISO);
- ICT-beveiligingsmanager;
- ICT-beveiligingsspecialist.

Bijlage 3 geeft voorbeelden van scholingen op HBO niveau.

4.3 Particuliere scholing op universitair niveau

Universitaire opleidingen op het gebied IT auditing worden aangeboden door:

- TIAS Tilburg;
- ESAA (Erasmus Universiteit);
- Amsterdam Business School (UvA) ;
- Vrije Universiteit Postgraduate school.

Bijlage 4 beschrijft de inhoud van de universitaire EMITA (Executive Master of IT-Auditing) opleiding.

Bijlage 1a: Manager informatiebeveiliging en privacy (voorbeeld functiebeschrijving)

Functie-informatie

Functienaam:	Manager informatiebeveiliging en privacy
Codering:	
Organisatie:	Mbo instelling
Onderdeel:	Centrale Organisatie (rechtstreek onder College van Bestuur)
Salarisschaal:	12
Indelingsniveau:	IVc
Werkterrein:	Control
Activiteiten:	Ontwikkelen, ontwerpen en beheren van structuren en systemen en het adviseren hierover. Coördinatie van activiteiten en processen.
Kenmerkscores:	44443 443344 43 44
Somscore:	52
Uitvoerder:	M. A. Boonstra-Kints
Datum:	24 juni 2015
FUWASYS-versie:	2002.1.40.08
Status:	Nieuwe functie

Functiebeschrijving

CONTEXT

De werkzaamheden worden verricht binnen een instelling voor beroepsonderwijs en volwasseneneducatie (ROC/AOC of Vakschool)). De manager informatiebeveiliging en privacy legt verantwoording af aan het College van Bestuur en is agenda lid van het directieberaad. De onderwijsinstelling streeft naar een maximale kwaliteit van haar informatiebeveiliging en heeft daartoe een statuut informatiebeveiliging vastgesteld. De manager informatiebeveiliging en privacy is verantwoordelijk voor ontwikkeling en uitvoering van een stelsel van ondersteunende processen en de integrale beveiliging van informatie. De manager informatiebeveiliging en privacy geeft gevraagd en ongevraagd advies aan het College van Bestuur en directeuren m.b.t. informatiebeveiliging, de kwaliteit van beveiliging van gegevens en mogelijke verbeteringen op dit terrein. De manager informatiebeveiliging en privacy rapporteert periodiek over de onderwijsinstelling brede stand van zaken van de beveiliging aan het College van Bestuur. Het College van Bestuur kan deze rapportage benutten om zo nodig verantwoording af te leggen aan Raad van Toezicht.
De manager informatiebeveiliging en privacy kan worden bijgestaan door een functionaris gegevensbescherming.

RESULTAATGEBIEDEN

1. Resultaatgebied ontwikkeling instelling breed stelsel van informatiebeveiliging

- Is verantwoordelijk voor de beleidsontwikkeling met betrekking tot informatiebeveiliging en privacy van de instelling.
- Adviseert over de specifieke beleidszaken met betrekking tot informatiebeveiliging aan het College van Bestuur.
- Doet voorstellen m.b.t. de informatiebeveiligingsstrategie, gebaseerd op een risicomanagement benadering en rekening houdend met het informatiebeveiligingsdreigingen -beelden, trends en organisatiebehoeften.
- Analyseert relevante ontwikkelingen op zijn eigen beleidsterrein en vertaalt deze naar doelstellingen voor de onderwijsinstelling.
- Toetst en bewaakt de naleving van wettelijke voorschriften, regelingen en binnen de onderwijsinstelling vastgesteld beleid dan wel overeengekomen afspraken.
- Toetst de implicaties van wettelijke en beleidsmatige ontwikkelingen op het terrein van informatiebeveiliging en privacy op gevolgen voor de onderwijsinstelling, brengt daarmee samenhangende risico's in kaart, analyseert deze en geeft alternatieven voor oplossingen aan de organisatie als geheel dan wel aan

het betreffende onderdeel.
- Wordt door interne en externe stakeholders beschouwd als de deskundige op het gebied van informatiebeveiligingsstrategie.
- Anticipeert op ontwikkelingen binnen een tijdshorizon van maximaal 2 jaar.

2. Resultaatgebied uitvoering

- Richt de informatiebeveiligingsorganisatie in, bepaalt de daarvoor benodigde middelen en legt dit ter besluitvorming voor aan het College van Bestuur.
- Organiseert en stuurt de informatiebeveiliging van de organisatie overeenkomstig de behoeften en de risicobereidheid van de organisatie aan.
- Draagt zorg voor de implementatie van informatiebeveiliging in de gehele organisatie en houdt toezicht op de wijze van uitvoering.
- Adviseert over te gebruiken methoden, instrumenten en technieken op het terrein van informatiebeveiliging en privacy;
- Zorgt voor een geschikt niveau van informatiebeveiliging en informatiebeveiligingsbewustzijn in de organisatie, gebaseerd op de behoeften en de risicobereidheid van de organisatie.
- Stelt interne en externe rapportages en verantwoordingsdocumenten op het terrein van informatiebeveiliging en privacy op.
- Leidt overlegvormen, projecten en samenwerkingsverbanden op het eigen beleidsterrein.
- Voert overleg over de uitvoering van het Statuut Informatiebeveiliging met medewerkers en directeuren.
- Organiseert het collectief denken over informatiebeveiliging.
- Stuurt functioneel de functionaris gegevensbescherming aan.

3. Resultaatgebied control

- Bewaakt de kwaliteit van het niveau van informatiebeveiliging binnen de instelling.
- Voert informatiebeveiligingsassessments, -tests, -reviews en –audits uit.
- Informeert zich over het niveau van de informatiebeveiliging in de verschillende organisatieonderdelen en verricht waar nodig daarop gericht onderzoek.
- Vormt zich een oordeel zowel over kwaliteit in de verschillende organisatieonderdelen als over plannen ter verbetering daarvan.
- Stelt interne en externe jaarrapportages en verantwoordingsdocumenten op over het niveau van de informatiebeveiliging.
- Adviseert directeuren op basis van de uitkomsten van onderzoek over noodzakelijke verbeteracties.
- Ziet toe op naleving van de eisen en architectuur voor informatiebeveiliging.
- Adviseert het College van Bestuur over de in relatie tot de informatiebeveiliging te bespreken punten in plannings- en verantwoordingsgesprekken.

KADER, BEVOEGDHEDEN EN VERANTWOORDELIJKHEDEN

Verantwoording schuldig aan: het College van Bestuur over de bruikbaarheid van de bijdrage aan beleidsontwikkeling met betrekking tot informatiebeveiliging en privacy van de instelling, de voorstellen m.b.t. de informatiebeveiligingsstrategie, de inrichting van de organisatie van informatiebeveiliging en de wijze waarop uitvoering gegeven is aan het vastgestelde statuut informatiebeveiliging, tot het te vormen instelling brede onderwijskwaliteitsbeleid, het stelsel van kwaliteitszorg en de uitvoering ervan.
Kader: Wettelijke richtlijnen en specifiek geformuleerde beleidskaders van de onderwijsinstelling
Beslist over/bij:, het uitbrengen van adviezen aan het College van Bestuur omtrent de door het College van Bestuur vast te stellen Statuut Informatiebeveiliging, het vertalen van het statuut naar richtlijnen, werkwijzen en uitgangspunten voor organisatieonderdelen, het bestuderen van ontwikkelingen in de informatiebeveiliging op mogelijke consequenties voor de instelling en het opstellen van verbeterplannen en bij het uitvoeren van monitorings- of controle trajecten.

Kennis en vaardigheden

De manager ibp beschikt over de volgende kennis en vaardigheden

- Wo werk- en denkniveau.
- Brede of gespecialiseerde theoretische kennis van (Informatie)beveiliging en Privacy wetgeving.

- Kennis en vaardigheid op het gebied van financiële zaken(begrotingsvoorbereiding, budgetbewaking) met als doel de kosten van informatiebeveiliging beheersbaar te houden**.**
- Kennis van en inzicht in de taak- en doelstelling en de werkwijze van de organisatie van de onderwijsinstelling.
- Inzicht in de bedrijfs- en onderwijsprocessen binnen de onderwijsinstelling.
- Vaardigheid in het ontwikkelen van adviezen, projectresultaten, voorgestelde of gekozen oplossingsrichtingen en alternatieven.
- Vaardigheid in het omgaan met verschillenden belangen en het kunnen overtuigen op basis van argumenten;
- Vaardigheid in projectmatig werken.
- Vaardigheid in het opstellen van beleidsvoorstellen.
- Vaardigheid in het initiëren van nieuwe ontwikkelingen op het eigen vakgebied.
- Communicatieve vaardigheden.

Contacten

De manager ibp moet investeren in de volgende relaties:

- Met het College van Bestuur over de adviezen, voorstellen om informatie te geven, te adviseren en deze te (kunnen) beargumenteren.
- Met directeuren (proceseigenaren) van de onderwijsinstelling voor het creëren van draagvlak voor de implementatie van het Statuut Informatiebeveiliging.
- Met directies en medewerkers van over richtlijnen, procedures, processen en werkwijzen voor het gebruik van bestaande, aangepaste of nieuwe voorzieningen, methoden en/of technieken op het terrein van informatiebeveiliging om hen te informeren, vragen te beantwoorden en om de doelmatigheid en effectiviteit ervan te onderzoeken en te controleren.
- Met het management met betrekking tot informatiebeveiliging over inhoudelijke, organisatorische, procedurele en beheersmatige aspecten om zaken te regelen en tot afspraken te komen voor zover het eigen mandaat gaat.
- Met medewerkers over de wijze waarop de werkzaamheden dienen te worden uitgevoerd, de evaluatie van de resultaten daarvan, verbetervoorstellen en om informatie uit te wisselen en tot afstemming te komen.
- Met het ministerie van OC&W, de onderwijsinspectie en andere externe partijen over de stand van zaken met betrekking tot informatiebeveiliging binnen de instelling en/of de verbetering daarvan.

Bijlage 1b: Coördinator Informatiebeveiliging en Privacy (voorbeeld functiebeschrijving)

Functie-informatie

Functienaam:	Coördinator Informatiebeveiliging en Privacy
Codering:	
Organisatie:	Mbo instelling
Onderdeel:	Medewerker afdeling ICT, functioneel beheer, Informatie management of kwaliteitszorg
Salarisschaal:	10
Indelingsniveau:	IVc
Werkterrein:	Control
Activiteiten:	Beheren van structuren en systemen en het adviseren hierover. Coördinatie van activiteiten en processen.
Kenmerkscores:	43443 43333 33 34
Somscore:	47
Uitvoerder:	M.A. Boonstra-Kints
Datum:	24 juni 2015
FUWASYS-versie:	2002.1.40.08
Status:	Nieuwe functie

Functiebeschrijving

CONTEXT

De werkzaamheden worden verricht binnen een instelling voor beroepsonderwijs en volwasseneneducatie (ROC/AOC of Vakschool)). De coördinator informatiebeveiliging en privacy (ibp) legt verantwoording af aan de verantwoordelijke portefeuillehouder Informatiebeveiliging (Informatiemanager of directeur ict). De onderwijsinstelling streeft naar een maximale kwaliteit van haar informatiebeveiliging en heeft daartoe een statuut informatiebeveiliging vastgesteld. De coördinator ibp is verantwoordelijk voor de implementatie van het vastgestelde beleid m.b.t. informatiebeveiliging, de beveiliging van gegevens en doet voorstellen voor mogelijke verbeteringen op dit terrein. De coördinator ibp levert een bijdrage aan de rapportages m.b.t de stand van zaken van de beveiliging van informatie.
Binnen de onderwijsinstelling kan naast de coördinator informatiebeveiliging en privacy ook een functionaris gegevensbescherming werkzaam zijn.

RESULTAATGEBIEDEN

1. *Resultaatgebied bijdrage aan ontwikkeling instelling breed stelsel van informatiebeveiliging*
   - Levert een bijdrage aan de voorgestelde beleidsontwikkeling met betrekking tot informatiebeveiliging en privacy van de instelling.
   - Levert een bijdrage aan voorstellen m.b.t. de informatiebeveiligingsstrategie, rekening houdend met het informatiebeveiligingsdreigingen -beelden, trends en organisatiebehoeften.
   - Ziet toe op de naleving van wettelijke voorschriften, regelingen en binnen de onderwijsinstelling vastgesteld beleid dan wel overeengekomen afspraken.
   - Signaleert en rapporteert over de stand van de informatiebeveiliging in onderdelen van de instelling aan de betreffende leidinggevende;
   - Maakt afwijkingen van voorgenoemde voorschriften, regelingen bespreekbaar en maakt afspraken met de verantwoordelijke functionaris;
   - Adviseert en ondersteunt onderdelen van de onderwijsinstelling bij de verbetering en evaluaties m.b.t. informatiebeveiliging (verloop, inhoud en resultaat) en maakt daarbij gebruik wordt van de PDCA-cyclus;
   - Anticipeert op ontwikkelingen binnen een tijdshorizon van maximaal 2 jaar.

2. *Resultaatgebied implementatie en uitvoering*

- Levert een bijdrage aan het ontwerpen, bewaken en evalueren van procedures, planningen en instrumenten op het gebied informatiebeveiliging en privacy;
- Doet onderzoek naar de naleving van de eisen m.b.t. informatiebeveiliging en privacy en het bewaken ervan;
- Leidt of neemt deel aan overlegvormen, projecten en samenwerkingsverbanden op het gebied van de informatiebeveiliging en privacy;
- Coördineert en/of voert werkzaamheden m.b.t. informatiebeveiliging en privacy uit;
- Fungeert als (eerste) aanspreekpunt voor zaken betreffende informatiebeveiliging en privacy voor (een onderdeel van) de onderwijsinstelling;
- Is verantwoordelijk voor de uitvoering van de informatiebeveiliging in (een onderdeel van) de onderwijsinstelling;
- Levert een bijdrage aan interne en externe rapportages en verantwoordingsdocumenten op het terrein van informatiebeveiliging en privacy;
- Neemt deel aan overleg over de uitvoering van het Statuut Informatiebeveiliging

3. *Resultaatgebied control*

- Levert een bijdrage aan de kwaliteit van het niveau van informatiebeveiliging binnen de instelling.
- Levert een bijdrage aan informatiebeveiligingsassessments, -tests, -reviews en –audits uit.
- Levert een bijdrage aan interne en externe jaarrapportages en verantwoordingsdocumenten over het niveau van de informatiebeveiliging.
- Informeert de verantwoordelijke portefeuillehouder Informatiebeveiliging m.b.t de naleving van de eisen en architectuur voor informatiebeveiliging.

KADER, BEVOEGDHEDEN EN VERANTWOORDELIJKHEDEN

Verantwoording schuldig aan: de portefeuillehouder ibp over de kwaliteit van de bijdrage aan de ontwikkeling van de informatiebeveiligingsstrategie, het toezicht op naleving van wettelijke voorschriften, de rapportages m.b.t. de stand van zaken van de informatiebeveiliging en de bijdrage aan het ontwerpen, bewaken en evalueren van procedures, planningen en instrumenten op het gebied informatiebeveiliging en privacy, de uitgevoerde audits en controles en de bruikbaarheid van de verleende ondersteuning en de resultaten waar ze toe hebben geleid.
Kader: Wettelijke richtlijnen, relevante wet- en regelgeving, kwaliteitsstandaarden, richtlijnen en specifiek geformuleerde beleidslijnen ten aanzien van informatiebeveiliging en privacy.
Beslist over/bij:, de bijdrage aan de ontwikkeling van de informatiebeveiliging, het ontwerpen, bewaken en evalueren van procedures en planningen op het gebied van informatiebeveiliging, het uitvoeren van werkzaamheden m.b.t. informatiebeveiliging en monitorings- of controle trajecten.

Kennis en vaardigheden

De coördinator ibp beschikt over de volgende kennis en vaardigheden

- Hbo werk- en denkniveau.
- Algemeen theoretische en praktische kennis van (Informatie)beveiliging en Privacy wetgeving.
- Kennis van en inzicht in de taak- en doelstelling en de werkwijze van de organisatie van de onderwijsinstelling.
- Inzicht in de bedrijfs- en onderwijsprocessen binnen de onderwijsinstelling.
- Vaardigheid in projectmatig werken.
- Vaardigheid in het uitvoeren van informatiebeveiligingsassessments, -tests, -reviews en –audits
- Vaardigheid in het opstellen van verbetervoorstellen en adviezen.
- Communicatieve vaardigheden.

Contacten

De coördinator ibp moet investeren in de volgende relaties:

- Met directeuren (proceseigenaren) van de onderwijsinstelling om met uiteenlopende belangen om te gaan, informatie te geven en de implementatie van het Statuut Informatiebeveiliging af te stemmen;
- Met directies en medewerkers over de toepassing van richtlijnen, procedures, processen en werkwij-

zen voor het gebruik van bestaande, aangepaste of nieuwe voorzieningen, methoden en/of technieken op het terrein van informatiebeveiliging om hen te informeren, vragen te beantwoorden en zorg te dragen voor een goede samenwerking;
- Met de portefeuillehouder ibp over de wijze waarop de werkzaamheden dienen te worden uitgevoerd, de evaluatie van de resultaten daarvan, verbetervoorstellen en om informatie uit te wisselen en tot afstemming te komen.

Bijlage 1c: Functionaris Gegevensbescher-ming (voorbeeld functiebeschrijving)

Functie-informatie

Functienaam:	Functionaris Gegevensbescherming
Codering:	
Organisatie:	Mbo instelling
Onderdeel:	Medewerker afdeling ICT, functioneel beheer, Informatiemanagement of kwaliteitszorg, afdeling juridische zaken/bedrijfsvoering
Salarisschaal:	10
Indelingsniveau:	IV c
Werkterrein:	Control
Activiteiten:	Beheren van structuren en systemen en het adviseren hierover. Coördinatie van activiteiten en processen.
Kenmerkscores:	43443 43333 33 34
Somscore:	47
Uitvoerder:	M.A. Boonstra-Kints
Datum:	24 juni 2015
FUWASYS-versie:	2002.1.40.08
Status:	Nieuwe functie

Functiebeschrijving

CONTEXT

De werkzaamheden worden verricht binnen een instelling voor beroepsonderwijs en volwasseneneducatie (ROC/AOC of Vakschool)). De functionaris gegevensbescherming legt verantwoording af aan de portefeuillehouder informatiebeveiliging en privacy binnen het College van Bestuur. De onderwijsinstelling streeft naar een maximale kwaliteit van haar informatiebeveiliging en heeft daartoe een statuut informatiebeveiliging vastgesteld. De functionaris gegevensbescherming houdt onafhankelijk toezicht op de toepassing en naleving van de Wet Bescherming Persoonsgegevens, is verantwoordelijk voor het toezicht op de uitvoering van het vastgestelde beleid op het terrein van gegevensbescherming en privacy en doet voorstellen voor mogelijke verbeteringen op dit terrein. De functionaris gegevensbescherming levert een bijdrage aan de rapportages m.b.t de stand van zaken van de beveiliging van informatie.
Binnen de onderwijsinstelling kan naast de functionaris gegevensbescherming ook een manager informatiebeveiliging en privacy of een coördinator informatiebeveiliging en privacy werkzaam zijn.

RESULTAATGEBIEDEN

1. *Resultaatgebied bijdrage aan ontwikkeling instelling breed stelsel van informatiebeveiliging*
   - Signaleert en rapporteert over de stand van zaken m.b.t. de naleving van de Wet Bescherming Persoonsgegevens in onderdelen van de instelling aan de betreffende directeur en portefeuillehouder ibp;
   - Maakt afwijkingen van voorgenoemde voorschriften en regelingen bespreekbaar en maakt afspraken met de verantwoordelijke functionaris;
   - Adviseert en ondersteunt onderdelen van de onderwijsinstelling bij de verbetering en evaluaties m.b.t. naleving van de Wet Bescherming Persoonsgegevens (verloop, inhoud en resultaat) en maakt daarbij gebruik van de PDCA- cyclus;
   - Anticipeert op ontwikkelingen binnen een tijdshorizon van maximaal 2 jaar.

2. *Resultaatgebied uitvoering Wet Bescherming Persoonsgegevens*
   - Levert een bijdrage aan het ontwerpen, bewaken en evalueren van procedures, planningen en instrumenten met betrekking tot de Wet Bescherming Persoonsgegevens
   - Doet onderzoek naar de naleving van de Wet Bescherming Persoonsgegevens en het bewaken ervan;

- Leidt of neemt deel aan overlegvormen, projecten en samenwerkingsverbanden op het gebied van de informatiebeveiliging en privacy;
- Fungeert als (eerste) aanspreekpunt voor zaken betreffende de Wet Bescherming persoonsgegevens (een onderdeel van) de onderwijsinstelling;
- Levert een bijdrage aan interne en externe rapportages en verantwoordingsdocumenten op het terrein van informatiebeveiliging en privacy;
- Houdt toezicht op, rapporteert over en adviseert over de verwerking van persoonsgegevens binnen alle onderdelen van de organisatie.;
- Draagt zorg voor de toepassing van de Wet Bescherming Persoonsgegevens en zorgt voor een passend niveau van beveiliging van de informatiehuishouding;
- Neemt maatregelen gericht op het beperken van (het gebruik van) persoonsgegevens.
- Houdt een bestand van meldingsverplichtingen bij;
- Behandelt vragen en klachten m.b.t. de Wet Bescherming Persoonsgegevens;
- Geeft voorlichting over het gebruik van persoonsgegevens en bevordert awareness bij medewerkers rondom hun verplichtingen bij het verwerken van persoonsgegevens;
- Treedt op als intermediair tussen de organisatie en de Autoriteit Persoonsgegevens;
- Neemt deel aan overleg over de uitvoering van het Statuut Informatiebeveiliging.

3. Resultaatgebied control

- Levert een bijdrage aan de kwaliteit van het niveau van informatiebeveiliging binnen de instelling.
- Levert een bijdrage aan informatiebeveiligingsassessments, -tests, -reviews en –audits uit.
- Levert een bijdrage aan interne en externe jaarrapportages en verantwoordingsdocumenten over het niveau van de informatiebeveiliging.
- Informeert de portefeuillehouder ibp m.b.t de naleving van de eisen m.b.t de Wet Bescherming Persoonsgegevens.

KADER, BEVOEGDHEDEN EN VERANTWOORDELIJKHEDEN

Verantwoording schuldig aan: de portefeuillehouder ibp binnen het College van Bestuur over de kwaliteit van de rapportages m.b.t. de naleving van de Wet Bescherming Persoonsgegevens, de afspraken met de verantwoordelijke functionaris, de bijdrage aan het ontwerpen, bewaken en evalueren van procedures, planningen en instrumenten en het onderzoek naar de naleving van de Wet Bescherming Persoonsgegevens;
Kader: De Wet Bescherming Persoonsgegevens, de Algemene Verordening Gegevensbescherming, andere relevante wet- en regelgeving, kwaliteitsstandaarden, richtlijnen en specifiek geformuleerde beleidslijnen ten aanzien van informatiebeveiliging en privacy.
Beslist over/bij:, de rapportages, interne en externe verantwoordingsdocumenten m.b.t. de naleving van de Wet Bescherming Persoonsgegevens en adviezen over de verwerking van persoonsgegevens binnen alle onderdelen van de organisatie.

Kennis en vaardigheden

De functionaris gegevensbescherming beschikt over de volgende kennis en vaardigheden

- Hbo of wo werk- en denkniveau.
- Algemeen theoretische en praktische kennis van (Informatie)beveiliging en Privacy wetgeving.
- Kennis van en inzicht in de taak- en doelstelling en de werkwijze van de organisatie van de onderwijsinstelling.
- Inzicht in de bedrijfs- en onderwijsprocessen binnen de onderwijsinstelling.
- Vaardigheid in het toezicht houden op gebruik van ict-systemen waarbinnen persoonsgegevens worden verwerkt.
- Vaardigheid in projectmatig werken.
- Vaardigheid in het uitvoeren van informatiebeveiligingsassessments, -tests, -reviews en –audits
- Vaardigheid in het opstellen van verbetervoorstellen en adviezen.
- Communicatieve vaardigheden.

Contacten

De functionaris gegevensbescherming moet investeren in de volgende relaties:

- Met directeuren (proceseigenaren) van de onderwijsinstelling om met uiteenlopende belangen om te

gaan, informatie te geven en de uitvoering af te stemmen;

- Met directeuren (proceseigenaren) van de onderwijsinstelling om informatie te geven en de naleving van de Wet Bescherming Persoonsgegevens af te stemmen;
- Met directies en medewerkers over de toepassing van richtlijnen, procedures, processen en werkwijzen voor het gebruik van bestaande, aangepaste of nieuwe voorzieningen, methoden en/of technieken op het terrein van informatiebeveiliging om hen te informeren, vragen te beantwoorden
- Met de portefeuillehouder ibp over de wijze waarop de werkzaamheden dienen te worden uitgevoerd, de evaluatie van de resultaten daarvan, verbetervoorstellen en om informatie uit te wisselen en tot afstemming te komen.

Bijlage 2: Actieve Masterclasses IBP

Doelstelling dag 1:

Surf documenten

Best practice uit het hoger onderwijs

Collega's uit het Hoger Onderwijs presenteren hun tools, documenten en kaders betreffende ibp (informatie beveiligings- en privacybeleid). In de middaguren wordt het vakgebied informatiebeveiliging en privacy geïntroduceerd en de inrichting van informatiebeveiliging in het hoger onderwijs, en de hierbij gebruikte materialen, toegelicht. In de avonduren worden we bijgepraat over de uitdagingen en successen die verbonden zijn aan de implementatie van IBP.

Op het einde van de dag zijn de volgende leerdoelen gerealiseerd:

- De cursist heeft een algemeen beeld van het vakgebied informatiebeveiliging
- De cursist heeft inzicht in de belangrijkste aspecten van de implementatie van informatiebeveiliging in een organisatie
- De cursist kent de achtergrond van de opzet van het informatiebeveiligingsbeleid binnen de HO instellingen.
- De cursist kent ontwikkelingen binnen het ho op het gebied van privacy beleid.
- De cursist heeft kennis genomen van een best practice binnen het HO onderwijs en kent problemen en uitdagingen die samen gaan met de implementatie van een informatiebeveiligingsbeleid binnen een onderwijsinstelling.

Doelstelling dag 2:

Risicomanagement vanuit de praktijk

Gebruik van normen- en toetsingskader binnen een mbo instelling

Een succesvol ibp traject start met een risico analyse. ISO 27001 (beschrijving ibp) is in feite een beschrijving van allerlei risico's. Collega's uit het bedrijfsleven delen hun ervaring en kennis op dit gebied met de deelnemers. De cursisten worden getraind om de risico's van hun mbo instelling te plotten (koppelen) aan de ISO 27002 (checklist ibp) norm.

Op het einde van de dag zijn de volgende leerdoelen gerealiseerd:

- De cursist kan risico's benoemen en de impact daarvan bepalen.
- De cursist kent de methodiek die ten grondslag ligt aan de ISO 27001 en ISO 27002 normenkader.
- De cursist kan de risico's plotten op de ISO norm.
- De cursist kent de 20 belangrijkste risico's binnen de mbo sector.
- De cursist weet hoe het normen- en toetsingskader binnen een mbo instelling wordt toegepast als onderdeel van een jaarlijkse "compliance" ronde.

Doelstelling dag 3:

Diepgang in IT auditing

Draaiboek Informatiebeveiligingsbeleid in de mbo sector

Tijdens het eerste deel van de dag wordt vooral het theoretisch kader uitgewerkt. Begrippen uit het de en audit wereld worden toegelicht en aan de hand van sprekende voorbeelden verduidelijkt. Het tweede deel van de dag wordt de starterskit mbo informatiebeveiligings- en privacy beleid gepresenteerd en worden de deelnemers uitgenodigd om de opgedane kennis toe te passen binnen hun eigen onderwijsinstelling. Vandaag wordt de masterclass verzorgd door collega's uit de mbo sector.

Op het einde van de dag zijn de volgende leerdoelen gerealiseerd:

- De cursist kent de volgende begrippen in het kader van ibp: opdrachtgever, scope, diepgang, onderzoekperiode, kwaliteitsnormen, audit-standaard, internationaal normenkader en assurance.
- De cursist kan informatie en informatiesystemen classificeren (BIV classificatie).
- De cursist kan de starterkit mbo toepassen.

Doelstelling dag 4:

Toelichting op mbo audit

Op deze dag maken de cursisten kennis met de mbo audit tool. Nadat de tool is toegelicht gaan de deelnemers aan de slag om hun eigen onderwijsinstelling te beoordelen. Een “technische” beoordeling van het netwerk is onderdeel van deze dag. De dag wordt verzorgd door collega’s uit de consultancy wereld die MBO instellingen ondersteund hebben bij de implementatie van ibp.
Op het einde van dit dagdeel zijn de volgende leerdoelen gerealiseerd:

- De cursist kent de clusteropbouw van de SURFaudit.
- De cursist kan de bewijsvoering (evidence) binnen de SURFaudit toepassen binnen zijn eigen mbo instelling.
- De cursist kan de audit tool “Coable” toepassen.
- De cursist heeft kennis van technische aspecten als PEN test, BCM, SURFcert, etc.
- De cursist onderkent de menselijke risico’s van de ict afdeling.

Toelichting op privacy in het mbo

Een succesvol privacy traject is een vervolg op een succesvol informatiebeveiligingstraject. Tijdens dit dagdeel wordt de samenhang tussen informatiebeveiliging en privacy besproken. Ook worden alle documenten besproken die zijn opgeleverd door de Taskforce ibp. De middagsessie gaat dieper in op de verankering van privacy, de governance, binnen een onderwijsinstelling.

- De cursist kent de algemene beginselen van privacy (bijv. keuzevrijheid);
- De cursist kan de verschillende rollen binnen privacy onderscheiden (bijv. bewerker);
- De cursist kent alle privacy principes (bijv. grondslag);
- De cursist kan het begrip integrale veiligheid toelichten;
- De cursist heeft kennis genomen van het Juridisch Normenkader Cloudservices;
- De cursist kent de gevolgen van een datalek.

Doelstelling dag 5:

Toelichting en beoordeling ibp van de universiteit Maastricht

Presentatie ibp deelnemers + voorbeeld toetsingskader examineren

Tijdens deze dag presenteren de deelnemers het Informatiebeveiligingsplan van hun instelling. De presentatie is vandaag in handen van een mbo en ho collega.
Tips en trics uit de dagelijkse praktijk worden gepresenteerd. Kennisnet behandelt het toetsingskader examineren op basis van het ISO normenkader. Tot slot wordt de mogelijke ver-volgscholing toegelicht.
Op het einde van de dag zijn de volgende leerdoelen gerealiseerd:

- De cursist kan het normenkader ISO 27002 vertalen naar een toetsingskader examineren.
- De cursist kent de mogelijke vervolgopleidingen.
- De cursist kan een informatiebeveiligingsbeleid schrijven op basis van het ho format.
- De cursist kan de functie van ibp-functionaris beschrijven.

Bijlage 3: Competentieprofielen ibp functies

Aanleiding[5]

In de huidige informatiemaatschappij wordt het steeds belangrijker dat iedere organisatie zorgvuldig omgaat met informatie. Organisaties moeten steeds meer informatie beschermen tegen een steeds complexer dreigingsbeeld. Hiervoor zijn goed opgeleide en ervaren informatiebeveiligers nodig. Kwalificaties zijn een middel om de kennis en ervaring van professionals in de informatiebeveiliging inzichtelijk te maken.

In de afgelopen jaren is op het gebied van kwalificatie van informatiebeveiligers een chaotische situatie ontstaan met een groot aantal onderling moeilijk vergelijkbare certificaten en titels. Daardoor kunnen informatiebeveiligers met hun titels en de bijbehorende certificaten niet duidelijk maken welke kennis en ervaring zij hebben. Werkgevers kunnen niet zien wanneer zij een goed opgeleide en ervaren informatiebeveiliger voor zich hebben. En opleidingsinstellingen denken nog een keer extra na alvorens te investeren in nieuwe opleidingen op het gebied van informatiebeveiliging.

De beroepsvereniging Platform voor Informatiebeveiliging (PvIB), streeft naar het professionaliseren van de beroepsgroep van informatiebeveiligers en daarbij hoort een overzichtelijke en transparante situatie op het gebied van kwalificatie. Een uniform kwalificatiestelsel voor informatiebeveiligers voor ziet daarin.

Om professionals in informatiebeveiliging uniform te kunnen kwalificeren, moet eerst duidelijk zijn welke beroepen binnen het vakgebied informatiebeveiliging voorkomen, wat deze beroepen inhouden en welke competenties (kennis, vaardigheden en houding) daarvoor nodig zijn. Dit wordt beschreven in zogenaamde beroepsprofielen.

Doelstelling

Dit document beschrijft beroepsprofielen voor beroepen binnen het vakgebied informatiebeveiliging.

Afbakening

Informatiebeveiliging is een onderwerp waar iedereen in elke organisatie in meer of mindere mate mee te maken heeft. Voor de meeste mensen in een organisatie is informatiebeveiliging slechts één van de aspecten van het dagelijkse werk, waaraan voldoende aandacht besteed moet worden, maar het speelt geen hoofdrol. Voor een aantal mensen is informatiebeveiliging echter ‘core business’. Deze mensen, de professionals in informatiebeveiliging, hebben een specificerende, uitvoerende, ondersteunende, adviserende en/of controlerende rol op het gebied van informatiebeveiliging. Bij hen is informatiebeveiliging het belangrijkste aandachtspunt, of ten minste één van de belangrijkste aandachtspunten.
De professionals in informatiebeveiliging werken samen met andere mensen in andere functies waarin informatiebeveiliging een minder prominente plaats inneemt. Verscheidene van hen zijn cruciaal voor het functioneren van de professionals in informatiebeveiliging, bijvoorbeeld omdat ze leiding of sturing geven, of onontbeerlijke input of ondersteuning geven. Hieronder vallen de Chief Executive Officer, de Chief Information Officer, de Enterprise Architect en verscheidene anderen.
De in dit document beschreven beroepsprofielen hebben alleen betrekking op professionals in informatiebeveiliging, dus degenen waarvoor informatiebeveiliging ‘core business’ is.

---

[5] Opdrachtgever: Platform voor Informatiebeveiliging (PvIB) en programma Qualification of Information Security (QIS)
Auteurs: Marcel Spruit en Fred van Noord
Versie: 1.0 Nederlands
Publicatiedatum: 15 mei 2014
Uitgever: PvIB, © 2014 (www.pivb.nl)

Uitgangspunten

Voor het beschrijven van beroepsprofielen voor beroepen binnen het vakgebied informatiebeveiliging worden de volgende uitgangspunten gehanteerd:

- De beroepsprofielen worden breed gedragen binnen het vakgebied informatiebeveiliging.
- De beroepsprofielen specificeren de benodigde kennis, vaardigheden en ervaring.
- De beroepsprofielen zijn geschikt als basis voor een uniform kwalificatiestelsel voor informatiebeveiligers.
- De beroepsprofielen zijn gebaseerd op het Europees e-Competence Framework 3.0 (e-CF).3

Verantwoording

Dit document is op verzoek van het bestuur van PvIB opgesteld door de Werkgroep Kwalificatie van informatiebeveiligers van PvIB. De beroepsprofielen in dit document zijn bedoeld om gebruikt te wo- den als input voor het programma QIS (Qualification of Information Security) dat ze kan gebruiken om te komen tot een uniform kwalificatiestelsel voor professionals in de informatiebeveiliging.

Een randvoorwaarde voor beroepsprofielen is brede acceptatie van de profielen door enerzijds de be- trokken beroepsgroep en anderzijds de werkgevers en opleidingsinstellingen die de profielen kunnen gebruiken voor respectievelijk de werving en selectie van professionals en het inrichten van opleidingen. Om brede acceptatie te ondersteunen is dit document gereviewed door een representatie van de PvIB, de stuurgroep en klankbordgroep van het programma QIS, functionarissen die werkzaam zijn in functies waar de hier beschreven profielen betrekking op hebben, alsmede opleiders op het gebied van informatiebeveiliging.

Competentieprofielen

Hieronder volgen de beschrijving van de volgende competentie profielen:

- CISO
- ISO
- Ict beveiligingsmanager
- Ict beveiligingsspecialist

Chief Information Security Officer (CISO)

Profieltitel	CHIEF INFORMATION SECURITY OFFICER (CISO)		
Samenvatting	Definieert de informatiebeveiligingsstrategie en organiseert en stuurt de informatiebeveiliging van de organisatie overeenkomstig de behoeften en de risicobereideid van de organisatie.		
Missie	Definieert de informatiebeveiligingsstrategie, gebaseerd op een risicomanagementbenadering en rekening houdend met het informatiebeveiligingsdreigingen- beeld, trends en organisatiebehoefte. Richt de informatiebeveiligingsorganisatie in, bepaalt de daarvoor benodigde middelen en wijst deze toe. Initieert de implementatie van informatiebeveiliging voor de gehele organisatie en houdt daar toezicht op. Zorgt voor een geschikt niveau van informatiebeveiliging en informatiebeveiligingsbewustzijn in de organisatie, gebaseerd op de behoeften en de risicobereidheid van de organisatie. Wordt door interne en externe stakeholders beschouwd als de deskundige op het gebied van informatiebeveiligingsstrategie.		
Producten	**Eindverantwoordelijk**	**Realiseert**	**Draagt bij**
	• Informatiebeveiligingsstrategie • Implementatie van informatiebeveiliging • Organisatie van informatiebeveiliging en expertise daarvoor • Naleving van de eisen en architectuur voor informatiebeveiliging • Informatiebeveiligingsbewustzijn over de hele organisatie • Voorbereid zijn op toekomstige informatiebeveiligingsrisico's en ict- beveiligingsrisico's • Informatierisicoanalyses, beveiligingsontwerpen en oplossingen • Informatiebeveiligings-assessments, -tests, -reviews en –audits	• Projectportfolio voor informatiebeveiliging • Organisatie brede informatiebeveiligingsactiviteiten en -projecten • Informatiebeveiligings- calamiteitenorganisatie • Gecoördineerde reactie op ernstige informatie- beveiligings- of ict- incidenten • Organisatie brede richtlijnen, standaarden, methoden en technieken voor informatiebeveiliging	• Risicomanagementbeleid • Informatiesysteem- governance • Service Level Agreements • Informatiebeveiligingsarchitectuur
Kerntaken	• Definieert de informatiebeveiligingsstrategie voor de organisatie • Zorgt voor een projectportfolio voor informatiebeveiliging • Organiseert informatiebeveiliging en de daarvoor benodigde expertise • Initieert organisatie brede informatiebeveiligingsactiviteiten en -projecten • Zorgt voor organisatie brede richtlijnen, standaarden, methoden en technieken voor informatiebeveiliging • Borgt de kwaliteit van informatierisicoanalyses, beveiligingsontwerpen en oplossingen • Borgt het naleven van de eisen en architectuur voor informatiebeveiliging • Borgt informatiebeveiligingsbewustzijn binnen de organisatie • Borgt dat de organisatie voldoende voorbereid is op toekomstige informatiebeveiligingsrisico's en ict-beveiligingsrisico's • Borgt de kwaliteit van informatiebeveiligingsassessments, -tests, -reviews en -audits • Zet een informatiebeveiligingscalamiteitenorganisatie op • Coördineert de reactie op ernstige informatiebeveiligings- of ict incidenten • Doet aanbevelingen aan senior algemeen management		

Information Security Officer (ISO)

Profieltitel	INFORMATION SECURITY OFFICER (ISO)		
Samenvatting	Implementeert informatiebeveiliging in overeenstemming met de informatiebeveiligings-strategie van de organisatie.		
Missie	Implementeert informatiebeveiliging in de organisatie. Zorgt in het kader van informatiebeveiliging voor een beveiligingsplan, risicoanalyses, risicomonitoring, incidentenregistratie, hulpmiddelen, training en evaluatie. Initieert en bestuurt kleine informatiebeveiliging- en bewustwordingsprojecten. Wordt door interne en externe stakeholders beschouwd als de deskundige op het gebied van informatiebeveiliging.		
Producten	**Eindverantwoordelijk**	**Realiseert**	**Draagt bij**
	• Gedocumenteerde kennisverzameling voor informatiebeveiliging • Registratie, analyse en rapportage van informatiebeveiligings- incidenten	• Implementatie van informatiebeveiliging • Kleine informatiebeveiligingsprojecten • Training en opleiding voor informatiebeveiligingsbewustzijn • Risicoanalyses voor informatiesystemen, beveiligingsontwerpen en oplossingen • Monitoring van en rapportage over informatiebeveiligingsrisico's • Informatiebeveiligings-assessments, -tests, -reviews en -audits	• Informatiebeveiligingsstrategie • Projectportfolio voor informatiebeveiliging • Informatiebeveiligingsarchitectuur • Risicomanagementbeleid • Organisatie brede informatiebeveiligingsactiviteiten en -projecten • Organisatie brede richtlijnen, standaarden, methoden en technieken voor informatiebeveiliging
Kerntaken	• Implementeert informatiebeveiliging in de organisatie • Voorziet in een gedocumenteerde kennisverzameling voor informatiebeveiliging • Zorgt voor adequate registratie, analyse en rapportage van informatiebeveiligings- incidenten • Initieert en managet kleine informatiebeveiligingsprojecten • Zorgt voor training en opleiding voor informatiebeveiligingsbewustzijn • Voert risicoanalyses voor informatiesystemen uit • Zorgt voor informatiebeveiligingsontwerpen en -oplossingen • Monitort informatiebeveiligingsrisico's en rapporteert daarover • Realiseert en monitort informatiebeveiligingsassessments, -tests, -reviews en -audits • Doet aanbevelingen aan het management met betrekking tot informatiebeveiliging en -risico's		

ict-beveiligingsmanager

Profieltitel	ICT SECURITY MANAGER		
Samenvatting	Definieert de ict-beveiligingsrichtlijnen voor de organisatie in overeenstemming met de informatiebeveiligingsstrategie en -architectuur van de organisatie en orga- niseert en managet de ict-beveiliging van de organisatie.		
Missie	Definieert de ict-beveiligingsrichtlijnen, rekening houdend met het ict- beveiligingsdreigingenbeeld, trends, de ict van de organisatie en toekomstige behoeften. Richt de ict-beveiligingsorganisatie in bepaalt de daarvoor benodigde middelen en wijst deze toe. Managet de implementatie van ict-beveiliging voor alle ict-systemen. Zorgt voor een geschikt niveau van ict-beveiliging, gebaseerd op de behoeften en risicobereidheid van de organisatie. Wordt door interne en ex- terne stakeholders beschouwd als de deskundige op het gebied van ict- beveiligingsbeleid.		
Producten	**Eindverantwoordelijk**	**Realiseert**	**Draagt bij**
	• ict-beveiligings- richtlijnen en implementatie daarvan • ict-beveiligings- organisatie en expertise • ict-beveiligings-projecten • ict-beveiligings- assessments, -tests, -reviews en -audits	• Projectportfolio voor ict-beveiliging • Procedures voor ict- beveiliging • Risicoanalyses voor ict • Monitoring van en rapportage over ict-risico's • ict-continuïteitsplan • Opleidingsbeleid voor ict-beveiliging	• Risicomanagementbeleid • Informatiebeveiligings-strategie • Informatiebeveiligings-architectuur • Implementatie van informatiebeveiliging • Integratievoorstellen voor nieuwe technologie
Kerntaken	• Definieert de ict-beveiligingsrichtlijnen voor de organisatie in overeenstemming met de informatiebeveiligingsstrategie en -architectuur van de organisatie • Managet de implementatie van de ict-beveiligingsrichtlijnen • Zorgt voor een projectportfolio voor ict-beveiliging • Definieert het opleidingsbeleid voor ict-beveiliging • Definieert en implementeert procedures ten behoeve van ict-beveiliging • Organiseert ict-beveiliging en de daarvoor benodigde expertise • Volgt technologische ontwikkelingen op het gebied van ict-beveiliging • Voert risicoanalyses voor ict uit • Monitort ict-risico's en rapporteert daarover • Zet het ict-continuïteitsplan op • Initieert and managet ict-beveiligingsprojecten • Borgt de kwaliteit van de ict-beveiligingsassessments, -tests, -reviews en -audits • Informeert senior algemeen management over de status van ict-beveiliging en incidenten		

ict-beveiligingsspecialist

Profieltitel	ICT-BEVEILIGINGSSPECIALIST		
Samenvatting	Geeft invulling aan de ict-beveiligingsrichtlijnen van de organisatie.		
Missie	Doet voorstellen voor en implementeert de benodigde beveiligingsmaatregelen. Adviseert, ondersteunt en informeert om ict veilig te laten werken. Neemt directe actie om systemen en netwerken of delen daarvan te beveiligen. Wordt door vak- genoten beschouwd als de deskundige op het gebied van technische ict- beveiliging.		
Producten	**Eindverantwoordelijk**	**Realiseert**	**Draagt bij**
	• Gedocumenteerde kennisverzameling voor ict-beveiliging	• Integratievoorstellen voor nieuwe technologie • ict-beveiligingsmaatregelen en -updates • Selectie en implementatie van beveiligingshulpmiddelen • ict-beveiligingsassessments, -tests, -reviews en -audits • Monitoring van de ict- beveiliging	• Risicomanagement-beleid • ict-beveiligings- richtlijnen en implementatie daarvan • Risicoanalyses voor ict • ict-continuïteitsplan
Kerntaken	• Volgt technologische ontwikkelingen op het gebied van ict-beveiliging • Stelt voorstellen op voor integratie van nieuwe technologie • Voorziet in een gedocumenteerde kennisverzameling voor ict-beveiliging • Implementeert benodigde beveiligingsmaatregelen en beveiligingsupdates • Selecteert en implementeert beveiligingshulpmiddelen • Realiseert en monitort ict-beveiligingsassessments, -tests, -reviews en -audits • Monitort de beveiliging van de ict en evalueert ict-beveiligingsrisico's • Test het ict-continuïteitsplan • Doet aanbevelingen aan het lijnmanagement met betrekking tot ict-beveiliging en -risico's		

Bijlage 4a: Opleidingsaanbod op HBO niveau

Opleiding information security essentials[6]

Deze 5-daagse basisopleiding informatiebeveiliging behandelt alle aspecten die u als aankomend security specialist nodig heeft om informatiebeveiliging in uw organisatie op de kaart te zetten en te borgen.

De meerwaarde van deze opleiding

Met het volgen van deze opleiding Information Security Essentials krijgt u een introductie in het brede speelveld van de informatiebeveiliging. De opleiding haakt sterk in op de actualiteit waardoor u in staat bent de diverse dreigingen (DDos aanvallen, hacking van websites, etc.) te vertalen naar risico's in uw eigen omgeving.
Deze opleiding is bedoeld voor cursisten die zich gaan bezighouden met informatiebeveiliging en over een gedegen basiskennis willen beschikken.
De Security Academy aanpak
De opleiding Information Security Essentials is uniek omdat er een perfecte mix aan onderwerpen is geselecteerd waarmee u voldoende kennis verkrijgt om zowel met de IT-er als met de (lijn)manager op niveau over het onderwerp informatiebeveiliging te kunnen praten.
Doordat de lessen wekelijks worden gegeven en maximaal twee domeinen per week behandeld worden, is er voldoende gelegenheid de informatie uit te diepen en u eigen te maken zodat u de lesstof in de praktijk ook daadwerkelijk kunt toepassen. Na 5 lesdagen wordt de opleiding afgesloten met een examen.
Als u de opleiding Information Security Essentials heeft afgerond kunt u de Post-HBO vervolgopleiding **Information Security Management Professional** volgen.

De opleiding bestaat uit 5 modules:

Module 1: Introductie & Speelveld Informatiebeveiliging
Introductie in het speelveld van de informatiebeveiliging Internationale standaarden zoals de ISO 27001/ 27002, NEN 7510. Omgaan met wet- & regelgeving zoals de Wet bescherming persoonsgegevens
Module 2: De Organisatie van informatiebeveiliging
De positionering van informatiebeveiliging binnen uw organisatie De informatiebeveiligingsprocessen in uw organisatie Risicoanalyse (kwalitatieve en kwantitatieve risicoanalyse) Certificeringen en omgaan met audits op informatiebeveiliging
Module 3: De Menselijke aspecten van informatiebeveiliging
De mens als belangrijkste schakel in uw informatiebeveiliging. Procedures rondom informatiebeveiliging. Security bewustwording/ Security awareness
Module 4: De Technische aspecten van informatiebeveiliging
Het speelveld en de werkwijze van hackers en cybercriminelen. De beveiliging van uw IT-infrastructuur. Netwerkprotocollen zoals VPN, SSL
Module 5: De nieuw IT-omgeving & Proefexamen
Cloud Security. Mobile Security. Het nieuwe werken en informatiebeveiliging.

Examen en exameneisen

Er gelden geen specifieke toelatingseisen om deel te kunnen nemen aan deze opleiding. Het theoretisch examen wordt afgenomen één week na de laatste lesdag. Het examen bestaat uit een combinatie van multiple choice vragen, open vragen en een casus. Na succesvolle afronding van de opleiding ontvangt u het diploma 'Information Securiy Essentials' .

[6] https://www.securityacademy.nl/opleidingen/cursus-information-security-the-basics.html.
Security Academy

Cyber Security Management (post-hbo-opleiding)[7]

Optimale informatievoorziening is voor organisaties onmisbaar en een bedrijfskritisch middel. Als informatie- of IT-manager draagt u bij aan het waarborgen van de kwaliteit van die informatievoorziening. Betrouwbaarheid is hierbij essentieel. Cyberaanvallen en andere cyberdreigingen zorgen dat deze betrouwbaarheid steeds meer onder druk komt te staan. Voor de continuïteit van de organisatie is aandacht hiervoor noodzakelijk. U kent uw verantwoordelijkheid op dit vlak en wilt adequate cyber security realiseren op operationeel, tactisch en strategisch niveau. De professional course Cyber Security Management aan De Haagse Hogeschool biedt u hiertoe kwalitatieve methoden en modellen. U krijgt inzicht in standaarden en *best practices* en ontwikkelt vaardigheden voor de effectieve implementatie van cyber security.

Krijg advies van ervaren cybersecurityexperts

Kenmerkend aan deze opleiding is de continue koppeling tussen praktijk en theorie. Meeneemopdrachten voert u uit in relatie tot uw eigen werksituatie. Uw werkgever en uzelf hebben dus direct profijt van de investering. Dankzij de feedback van ervaren cybersecurityexperts en docenten krijgt uw organisatie waardevolle en praktische adviezen.

Integreren van security in de dagelijkse business

Tijdens de opleiding Cyber Security Management leert u situaties analyseren, beoordelen en vertalen naar passende maatregelen op zowel technisch als organisatorisch vlak. Daarbij houdt u gedegen rekening met de menselijke factor en het integreren van security in de dagelijkse business. U vertaalt theoretische modellen probleemloos naar uw beroepspraktijk en bent een volwaardig gesprekspartner voor het management.

Praktische informatie opleiding Cyber Security Management

Onderwijstype	Post-hbo
Onderwijsvorm	Deeltijd
Voertaal	Nederlands
Toelatingseisen	Hbo- of wo-diploma en ten minste twee jaar relevante werkervaring
Duur	15 weken

Diploma

Certificaat Cyber Security Management

[7] http://www.dehaagsehogeschool.nl/professional-courses/overzicht-opleidingen-trainingen/cyber-security-management/in-het-kort

CISO Masterclass programma[8]

Dag 1

SHARED VALUES; Welke invloed hebben de kenmerken en waarden van jouw organisatie op de information security beleving, de focus en de wijze van besturing.
STRATEGY; Welke bedrijfsstrategie en strategische doelen hanteert jouw organisatie en hoe ondersteun je deze met security strategie en doelen op strategisch, tactisch en operationeel niveau. Aan de hand van een overzicht van de verschillende strategische modellen vul je dit gedurende dit blok met de docenten en medecursisten zelf in.
STRUCTURE**;** Hoe is een organisatie opgebouwd, hoe functioneert die, hoe kan je security hierin positioneren en hoe oefen je dan binnen die organisatie op zodanige wijze invloed uit dat je je doelen bereikt.

Dag 2

STABILITY; Op een actieve wijze ondervinden wat de invloed van houding, intentie, zelfvertrouwen en omgaan met je energie en die van anderen op je resultaten kan zijn. – gastdocent
STYLE**;** Herken en hanteer diverse leiderschaps- en managementstijlen en communicatievormen en leer deze inzetten om op harmonieuze wijze resultaten te bereiken binnen je organisatie en je team.
SKILLS**;** Information Security verkoop je net als de meeste andere producten; met de juiste verkoopaanpak, door de taal van de business te spreken, de juiste boodschap te brengen en de juiste vorm te gebruiken en deze effectief te presenteren.
MEESTERSTUK**;** Jouw bevindingen die je hebt vastgelegd in je werkboek, vormen de basis voor je meesterstuk; samen met je medecursisten de aanpak en het plan toegespitst op jouw organisatie vormgeven. Hiermee kun je terug op je werkplek, direct aan de slag om informatiebeveiliging in jouw organisatie succesvol te gaan verbeteren, in goede harmonie met de business en rekening houdend met het breder belang van de organisatie.

Dag 3

SYSTEMS**;** Als CISO wordt je geconfronteerd met een veelheid aan systemen, standaarden en methodieken uit het eigen vakgebied en de aanpalende disciplines ; bezie samen met je mede cursisten wat de meest relevante voor jou zijn en maak het beeld compleet van wat volgens hun de belangrijke links en referenties zijn, hoe deze samenhangen en hoe je hier je voordeel mee kunt doen.
STAFF; In de CISO functie heb je een bijzondere rol binnen de organisatie en krijg je vanuit die rol te maken met uitdagende integriteitsvraagstukken. We bespreken met elkaar wat ons hierin op menselijk vlak beweegt en hoe verstandig om te gaan met dergelijke vraagstukken.

[8] https://cisomasterclass.nl/

Opleiding Architectuur en informatiebeveiliging[9]

In de opleiding Architectuur van Informatiebeveiliging komt alles aan de orde wat specifiek van belang is voor de architect die zich bezighoudt met informatiebeveiliging.

Raamwerken voor informatiebeveiliging

Informatiebeveiliging (IB) is hot, ook in IT-architectuur. Andersom vormt IT-architectuur een cruciaal onderdeel van een goede informatiebeveiliging. Daarbij rijst de vraag hoe je informatiebeveiliging een plaats geeft in de architectuur. Of, moet je juist een architectuur van je informatiebeveiliging maken? Tijdens deze opleiding leer je welke raamwerken je kunt gebruiken en kom je erachter of informatie vanuit de architectuur voldoende is beveiligd. Ook heel praktische overwegingen komen aan bod, zoals de keuze voor een encryptiealgoritme en omgaan met ontwikkelingen als Cloud Computing.

Dag 1: Fundamenten van de IB-architectuur

De dag begint met een korte historie van informatiebeveiliging en beveiligingsprincipes. Via technische beveiligingsfuncties wordt gewerkt naar de toepassing van patronen en bouwblokken in de informatiebeveiliging.

Dag 2: IB architectuurraamwerken

Gedurende de dag worden architectuurraamwerken besproken zoals het Sherwood Applied Business Security Architecture (SABSA), Open Security Architecture (OSA) en de beveiligingskatern van NORA. Daarnaast bespreken we Jericho 2.0 en de praktische toepassing daarvan in de beveiligingsarchitectuur.

Dag 3: Technische beveiligingsmaatregelen en Cloud Computing

Deze dag staat in het teken van technische beveiligingsmaatregelen zoals toegangsbeheer, identiteitsmanagement en netwerkbeveiliging. Naast de technische aspecten komen ook de organisatorische aspecten van deze onderwerpen aan de orde. Alles komt samen in een bespreking van trends als Cloud Computing. Hoe ga je als security architect om met dergelijke hypes?

Dag 4: Cryptologie en PKI

We gaan in op cryptologie, waarbij de toepassingsgebieden maar ook sterke en zwakke punten van de belangrijkste encryptie-algoritmen aan de orde komen. Symmetrische en asymmetrische encryptie worden besproken, inclusief de vraag hoe je komt tot een gefundeerde keuze voor een algoritme en sleutellengte. Nadat encryptie is besproken, wordt ingegaan op Public Key Infrastructure (PKI) en de belangrijkste aandachtspunten voor deze technologie.

Dag 5: Software ontwikkeling en architectuurbeoordeling

De dag begint met veiligheid van software, waarbij wordt uitgelegd hoe de veiligheid van software te borgen tijdens het ontwikkelproces. Open Web Application Security Project (OWASP) en kwaliteitsattributen van software vormen hiervoor een belangrijke basis. De opleiding wordt afgesloten met het beoordelen van de beveiligingsarchitectuur: we sluiten de lus en komen terug bij de volgende iteratie voor de beveiligingsarchitectuur.
Kortom een uitgebreid programma waarin alle vaardigheden aan de orde komen die de rol van de beveiligingsarchitect uniek maken ten opzichte van andere informatiebeveiligers.

[9] http://www.cibit.nl/nl/ict-opleidingen/opleiding-cissp-information-security/

Bijlage 4b: Opleidingsaanbod op universitair niveau (EMITA)

1. Enterprise Risk Management & Internal Control

Binnen het IT-auditing programma biedt TiasNimbas een innovatief en intensief onderdeel Enterprise Risk Management & Internal Control (ERM/IC). Het behandelt moderne (COSO) theoretische concepten, maar ook klassieke concepten (Starreveld) worden behandeld. We staan nadrukkelijk stil bij de mogelijkheden van IT voor het effectief en efficiënt ontwerpen en evalueren van de bestuurlijke informatieverzorging met een duidelijke focus op praktische uitwerkingen binnen de kaders van Corporate Governance (en SOx). De verworven kennis biedt de mogelijkheid tot het maken van een goede beoordeling van interne risicobeheersing systemen.

Het onderdeel ERM/IC wordt vanuit een managementoptiek benaderd en is primair gericht op het inrichten van adequate beheersing van bedrijfsprocessen. Het vak is sterk case georiënteerd. Dat betekent dat de cursisten een aantal cases uitwerken en presenteren. In deze cases staan het organiseren van een effectieve besturing, beheersing en verantwoording van de interne organisatie centraal. Uitwerkingen van cases worden voorafgaand aan de colleges voorbereid (per laptop en per e-mail) en tijdens de colleges besproken.

De opzet van de uitwerkingen sluit direct aan op wat auditors in hun praktijk moeten vaststellen. Op basis van procesbeschrijvingen worden risico's geïdentificeerd, beheer doelstellingen gedefinieerd en de bestuurlijke informatieverzorging en de beheersmaatregelen beschreven, inclusief de verantwoording over de werking van beheersmaatregelen als grondslag voor een interne beheersingsverklaring.

Learning Objectives

- Inzicht in de typen risico's voor organisaties op het gebied van strategie, organisatie, bedrijfsprocessen en informatieverzorging
- Kunnen uitwerken van een algemene risicoanalyse voor organisatie en processen (organisatieanalyse, procesanalyse, risico-identificatie en risicoanalyse [oorzaak-gevolg]
- Kunnen formuleren van beheer doelstellingen op basis van risicoanalyse
- Uitwerken van beheersmaatregelen per beheer doelstelling (AO/IC)

2. Grondslagen IT-Governance

Dit blok is een introductie van de beheersing van de inzet van IT in de realisatie van de bedrijfsdoelstellingen en de beheersbaarheid van bedrijfsprocessen en bestaat uit:

- Informatieprocessen en de toepassing van Enterprise Resources Planning (ERP)
- De ERP-colleges hebben primair als doelstelling u inzicht te geven in en begrip van de processen die met name in logistiek georiënteerde bedrijven voorkomen, en de ondersteuning door ERP hierbij. Een apart college wordt gewijd aan de bedrijfsprocessen in 'gegevensverwerkende organisaties'. We behandelen de AO/IC concepten voor ERP systemen aan de hand van de uitwerking in SAP, waarbij bijzondere aandacht wordt gegeven aan de aspecten betrouwbaarheid en beveiliging.
- CobiT
- Gelet op het belang van deze normenset voor zowel externe als interne IT auditors wordt de opbouw van deze normen inclusief de toepasbaarheid daarvan in de praktijk toegelicht.
- Controllability
- Voor iedere functie binnen IT moet de kwaliteit bewaakt en/of beheerst worden. IT-auditing beoordeelt deze controllabillity en daarom is het voor het uitvoeren van de IT-auditing van primair belang om de beheersbaarheid van de kwaliteit van de automatisering te leren praktiseren.
- Betrouwbaarheid
- Er wordt ingegaan op betrouwbaarheidsaspecten, -eisen en methodieken/ technieken voor betrouwbaarheidsonderzoeken.
- Beveiliging
- Er wordt uitvoerig ingegaan op de vraag op welke wijze de beveiligingsfunctie in verschillende omgevingen ingevuld kan worden en hoe de voor specifieke omgevingen een geschikte invulling wordt gekozen.

- Effectiviteit en efficiency
- Met betrekking tot de doeltreffendheid (effectiviteit) van de IT schenken we aandacht aan de presentatie van informatie conform de gebruikerswensen, de interactiegraad tussen gebruikers en informatiesystemen en het belang van de informatie voor de ontvangers.

Learning Objectives
- Inzicht in de principes van Corporate Governance en IT-Governance
- Inzicht in modellen voor IT-Control en standaarden voor IT-Security
- Inzicht in risicomanagement voor IT processen , systemen en projecten
- Inzicht in beheersing van bedrijfsprocessen en de toepassing ERP
- Inzicht in de typen IT-risico's op het gebied van IT-processen en IT- projecten
- Kunnen uitwerken van een risicoanalyse voor bedrijfsprocessen en IT-objecten (afhankelijkheidsanalyse en kwetsbaarheid analyse)
- Kunnen formuleren van IT-beheer doelstellingen op basis van risicoanalyse
- Kunnen uitwerken van IT-beheersmaatregelen per beheer doelstelling.

3. Grondslagen IT-Auditing / Wetenschappelijk paper

Een introductie van IT-auditing, een goede basis voor de uit te voeren IT-audits bestaande uit:

- IT-auditing
  We gaan in op verschillende facetten van dit vakgebied. behandelen de kwalificatie-eisen van de IT-auditor en de door hem te hanteren normen en standaarden. Ook komen relevante assurance frameworks aan bod.
- Kwaliteitsstandaarden/normen
  In dit college behandelen we de begrippen 'standaarden en normen' en hun onderlinge verhouding aan de hand van de voor IT auditors relevante IFAC standaarden. Ook is er aandacht voor andere normenstelsels en hun toepasbaarheid.
- Uitvoeringsstandaarden/normen
  Na het volgen van deze module kunt u IT-audits toelichten met aandacht voor opdrachten, doelgroepen, objecten, criteria, voordeel en aanpak.
- Aanpak en methodiek
  Aan de hand van praktijkvoorbeelden wordt de 'aanpak' van verschillende soorten IT-auditopdrachten duidelijk gemaakt.
- Rapportering
  Via praktijkvoorbeelden en diverse casusposities gaan we in op een uiterst belangrijk onderdeel van elke IT-auditopdracht.

Learning Objectives
- Inzicht in het auditproces en de auditaanpak
- Kennis van auditbeginselen en auditmethodologie
- Kennis van auditstandaarden / controlestandaarden
- Inzicht in de typen audits en de soorten opdrachtgevers
- Kunnen toepassen van toetsings- en uitvoeringsnormen
- Toepassen van oordeelsvorming en interpretatie van uitkomsten van audits
- Toepassen van onderzoeksmethoden en –technieken

4. Vraagzijde van de IT

IT is in toenemende mate verweven met alle aspecten van het zakendoen en het effectief en efficiënt vormgeven van de bedrijfsvoering. Het nemen van strategische en tactische beslissingen over de inzet, kwaliteit en de inrichting van IT is een cruciaal onderdeel geworden van het aandachtsveld van het top- en middle management. In dit blok komen daarom de volgende onderwerpen aan bod:

- IT Beleid en Assessment:
  Een optimale informatievoorziening draagt bij aan het succesvol zijn van de organisatie. Deze module gaat in op methoden, technieken en het proces om vast te stellen wat de huidige status van de informatievoorziening is, en hoe deze, vanuit een business perspectief, verbeterd kan worden.

- IT Governance, IT Architecture, IT Organisatie en Informatiemanagement
  Een module waarin we de strategische, tactische en organisatorische aspecten van de besturing van IT vanuit de business bespreken. Wie is, gezien vanuit de "IT life cycle" (richten, inrichten, verrichten) waarvoor verantwoordelijk, wie is waartoe bevoegd, welke besluitvormingsprocessen en organisatieprincipes kunnen bijdragen aan een adequate inrichting van de IT architecture, IT demand management, etc.
- Aansturing van de IT aanbodzijde:
  IT-diensten worden door leveranciers geleverd; interne maar ook externe leveranciers wanneer (een deel van) de IT aanbodzijde is ge-outsourced. Deze module gaat in op de relatie tussen in- en outsourcende partijen, en de wijze waarop IT-diensten kunnen worden gespecificeerd en de levering gecontroleerd. Onder andere het belang en de kwaliteitsborging van SLA's komt aan de orde.
- Pakketselectie en –implementatie:
  In toenemende mate wordt de informatievoorziening "ingevuld" met standaardpakketten. In deze module komen methoden aan de orde voor het uitvoeren en beoordelen van het selectieproces van standaardpakketten, evenals de implementatie van deze pakketten.

Learning Objectives

- Onderkennen en toepassen van principes en methoden om de inzet van IT, vanuit een business perspectief, te optimaliseren, te sturen en te structureren. Zowel in op zich zelf staande, autonome organisaties (IT Beleid en Assessment), alsook in ketens en bedrijfsnetwerken (IT in de Netwerkeconomie).
- Uitdiepen van beheersingsmaatregelen om de besturing van IT aan de vraagzijde te organiseren en te managen (IT Governance, IT Organisatie en Informatiemanagement).
- Onderkennen van risico's van uitbesteding en het vormgeven van relevante beheersingsmaatregelen, waaronder SLA's.
- Kunnen beoordelen van risico's en toepassen van beheersingsmaatregelen bij pakketselecties en -implementaties.

5. Techniek

In dit blok is aandacht voor de belangrijkste componenten en de samenhang daartussen binnen de technische infrastructuur. Gestart wordt met het schetsen van de plaats van die componenten en de aandachtspunten die voor de IT-auditor van belang zijn:

Datacommunicatie

Hoe kunnen bedreigingen en risico's voldoende worden ingeperkt? De algemene problematiek komt aan de orde bij de behandeling van de diverse netwerk typologieën en externe koppelingen voor bijvoorbeeld Remote Access. Verder wordt ingegaan op de risico's van internet en de wijze waarop een organisatie zich tegen de bedreigingen daarvan kan wapenen. Bij alle onderwerpen wordt stilgestaan bij de audit-aspecten die van belang zijn.

Operating Systemen

De meest voorkomende operatingsystemen worden besproken: z/OS (IBM), Unix (SUN) en Windows (Microsoft). IT-auditors uit de praktijk vertellen u over de audit-aspecten van elk platform, met de nadruk op de risico's.

Database managementsystemen

Gegevensbeheer, betrouwbaarheid en continuïteitsaspecten van database managementsystemen komen aan de orde. Een leverancier verzorgt een gastcollege en na het schetsen van de componenten van de technische infrastructuur wordt ingegaan op de manier waarop een auditor een oordeel kan geven over de gehele technische infrastructuur.

Deze componenten en aandachtsgebieden staan niet op zichzelf, maar hebben een samenhang. Het vertrekpunt is daarom een visie op de architectuur. Daarbij wordt stilgestaan bij:

- Architectuurrisico's
- Bedreigingen, risico's en maatregelen, doelmatigheid en doeltreffendheid, beveiliging en betrouwbaarheid.

Learning Objectives

- Inzicht verkrijgen in infrastructuur en beheersing.
- Onderkennen van IT risico's en beheersingsmaatregelen.
- Het kunnen uitvoeren van IT-audits in technisch bereik.

6. IT-processen

De organisatie van de aanbodzijde komt in dit blok als volgt aan bod:
Systeemontwikkeling
Product en organisatie, bepaling en beoordeling van de functionaliteit, controle van de kwaliteit van applicaties in technisch opzicht en van systeemontwikkelingsprocessen.
Verwerkingsorganisatie: beheersing
In dit blok leert u om zelfstandig een beheersingsmodel te ontwikkelen voor het inrichten en beoordelen van rekencentra.
Verwerkingsorganisatie: audit
Het beheersingsmodel dat u in het vorige blok heeft ontwikkeld gebruiken we om verschillende vormen van audits aan de orde te stellen. Eén of meer van deze audits werken we uit aan de hand van praktijksituaties.

Learning Objectives

- Inzicht verkrijgen in processen betreffende infrastructuur en beheersing.
- Onderkennen van IT-risico's en beheersingsmaatregelen.
-

7. Opdrachtgevers van IT-audits

In dit blok komen de volgende onderwerpen aan bod:

- De accountant als opdrachtgever: accountants, integrated audits. Inleiding door een accountant samen met een IT-auditor.
- Toezichthouders als opdrachtgever: toezichthouders als opdrachtgever c.q. de invloed van toezichthouders op werk IT-auditor.
- De CIO als opdrachtgever: de problemen en vraagstellingen op terrein van IT compliance en IT performance worden toegelicht door aantal CIO's vanuit verschillende bedrijven.
- De CFO als opdrachtgever: de vragen van de CFO inzake IT compliance vanuit invalshoek van de CFO.
- Samenwerking met de Risk Management-functie: de rol van IT-audit binnen de vraagstellingen van risk management in organisaties.
- Samenwerking met juristen

Learning Objectives

- Onderkennen van verschillende opdrachtgevers en hun vraagstellingen.
- Leren vertalen van vragen van opdrachtgevers in auditvragen.
- Leren onderkennen van e toegevoegde waarde van IT-audits en het bediscussiëren daarvan met opdrachtgevers.
- Het onderkennen van samenwerkingsverbanden met andere specialismen.
- Het verwerven van basiskennis op de juridische terreinen privacy, contracten & ict en Intellectueel eigendomsrecht.

Bijlage 5: Framework informatiebeveiliging en privacy in het mbo