;

MBO roadmap informatie-beveiligingsbeleid en privacy beleid

saMBO-ICT Kennisnet

TASKFORCE MBO INFORMATIEBEVEILIGING

IBPDOC5

Verantwoording

Bron:

Starterkit Informatiebeveiliging
Stichting SURF
Februari 2015

SURFibo

Het SURF Informatie Beveiligers Overleg is een community of practice binnen SURF samenwerkingsorganisatie met als doelen het actief stimuleren van en richting geven aan informatiebeveiliging binnen het hoger onderwijs en onderzoek (universiteiten, hogescholen, wetenschappelijk onderzoek en universitair medische centra). Dat wordt bereikt door het bevorderen van de samenwerking tussen informatiebeveiligers/kwartiermaker IB en het leveren van praktisch bruikbare adviezen.
Voor meer informatie zie www.surfibo.nl

Herschreven door: Kennisnet / saMBO-ICT

Auteurs

Leo Bakker	(Kennisnet)
Ludo Cuijpers	(saMBO-ICT, Kennisnet en ROC Leeuwenborgh)
Paulo Moekotte	(ROC van Twente)
Casper Schutte	(ROC Midden Nederland)

Review

Bart van den Heuvel	(SURFibo en Universiteit Maastricht)
Charlotte Latjes	(Gartner EMEA Education)
Alf Moens	(SURF)

Met dank aan:

Met dank aan de 40 deelnemers van de Masterclasses.
Juni 2015

Sommige rechten voorbehouden

Inhoudsopgave

Aanpak en samenvatting Roadmap

Totstandkoming

De eerste aanzet voor deze roadmap is gemaakt door onze collega's uit het Hoger Onderwijs (SURFibo) door de publicatie van de Starterkit Informatiebeveiliging. Dit document is helemaal herschreven door de werkgroep Beleid & Organisatie in opdracht van de Taskforce MBO Informatiebeveiliging en Privacy. De Roadmap is tevens onderdeel van de Masterclasses Informatiebeveiliging, waardoor ruim 40 deelnemers hun input (verbeteringen en aanvullingen) hebben kunnen leveren aan dit document. Tot slot is dit document gereviewed door Gartner en een aantal collega's van SURFibo.

Gebruik framework

De "MBO roadmap informatie beveiligingsbeleid en privacy beleid" (kortweg Roadmap) is onderdeel van het framework informatiebeveiliging en privacy in het MBO onderwijs. Dit framework bestaat uit 30 documenten en een aantal best practices. Schematisch als volgt weergegeven:

MBO referentie architectuur (IBPDOC4)							Privacy Compliance kader MBO (IBPDOC2B)	Normenkader Informatiebeveiliging MBO (IBPDOC2A)
	Verantwoordingsdocument informatiebeveiliging en privacy in het MBO onderwijs (IBPDOC1)							
	MBO roadmap informatie beveiligingsbeleid en privacy beleid (IBPDOC5)							
	Model Informatiebeveiligingsbeleid voor de MBO sector op basis van ISO27001 en ISO27002 (IBPDOC 6)			Model beleid verwerking persoonsgegevens op basis van Nederlandse wet- en regelgeving (IBPDOC18)				
	Toetsingskader IB: clusters 1 t/m 6 (IBPDOC3)			Toetsingskader Privacy: cluster 7 (IBPDOC7)				
	Toetsingskader Examinering Pluscluster 8 IBPDOC8	Toetsingskader Online leren Pluscluster 9 IBPDOC9	Toetsingskader VMBO-MBO Pluscluster 10 IBPDOC10	Handleiding Benchmark Coable IBPDOC11	Competenties Informatiebev. en Privacy IBPDOC12	Positionering Informatiebev. en Privacy IBP-DOC13	Handleiding Risico management IBPDOC29	
	Handleiding BIV classificatie IBPDOC14	BIV classificatie Bekostiging IBPDOC15	BIV classificatie HRM IBPDOC16	BIV classificatie Online leren IBPDOC17	PIA Deelnemers informatie IBPDOC19	PIA Personeel Informatie IBPDOC20	PIA Digitaal Leren IBPDOC21	
	Starterkit Identity mngt MBO versie IBPDOC22	Starterkit BCM MBO versie IBPDOC23	Starterkit RBAC MBO versie IBPDOC24	Integriteit Code MBO versie IBPDOC25	Leidraad AUP's MBO versie IBPDOC26	Responsible Disclosure MBO versie IBPDOC27	Cloud computing MBO versie IBPDOC28	
	Implementatievoorbeelden van kleine en grote instellingen				Technische quick scan (APK) IBPDOC30			
	Hoe? Zo! Informatiebeveiligingsbeleid in het MBO en Hoe? Zo! Privacy in het MBO							

Kaderdocumenten Taskforce IBP | realisatie 2015 Taskforce IBP | planning 2016 Taskforce IBP | SURFibo SURFaudit

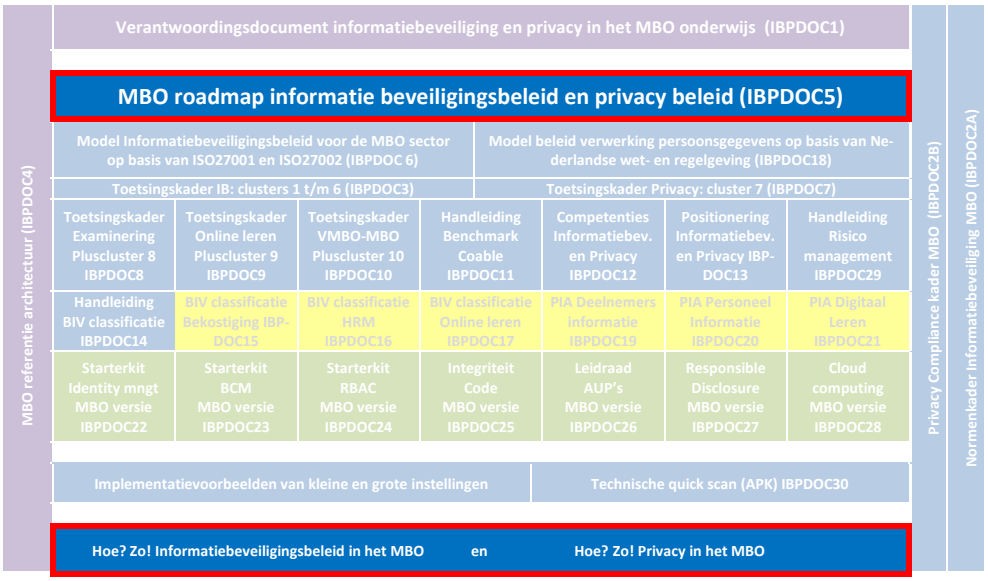
(Tabel 1: Framework Informatiebeveiliging en Privacy in het MBO onderwijs, versie april 2015)

De gemiddelde lezer zal niet vrolijk worden bij de aanblik van dit complexe framework. Toon Hermans maakte in een van zijn shows de volgende opmerking: "De eerste gedachte die 's morgens bij mij opkomt als ik wakker word is koude douche en houthakken, en dan wacht ik tot die gedachte voorbij is en dan neem ik mijn pillen." Ons framework zit, hopelijk, niet in de categorie "koude douche en houthakken". Om ervoor te zorgen dat onze collega's niet al te depressief worden is dan ook een toelichting op zijn plaats. De kern van dit framework is de Roadmap op basis van afspraken die verwoord zijn in het "Verantwoordingsdocument informatiebeveiliging en privacy in het MBO onderwijs (IBPDOC1)", alle overige documenten zijn best practices, voorbeelden, technische verantwoordingsdocumenten en informatieve documenten (zoals de Hoe? Zo! boekjes). En je mag ze gebruiken, maar dat is zeker niet verplicht. Als er een kwalitatief goed privacy beleidsplan binnen je MBO instelling voorhanden

is, dan biedt het document met de code IBPDOC18 (Model beleid verwerking persoonsgegevens op basis van Nederlandse wet- en regelgeving) wellicht geen meerwaarde meer. Het is aan jou om te bepalen welke documenten je wel of niet gebruikt.

Doel van deze roadmap is de mbo instellingen een handreiking te bieden om een begin te maken met opzet en uitvoering van Informatiebeveiliging en privacy beleid. Met dit document is het mogelijk voor een kwartiermaker om in een vijftigtal dagen, uiteraard afhankelijk van de complexiteit van de instelling, aan de hand van een viertal stappen een eerste aanzet te geven voor de inrichting van een Informatiebeveiliging en Privacy organisatie binnen de mbo instelling. Stap vijf beoogt de verankering in de organisatie te regelen.

Vereiste voorkennis
Zoals je gemerkt hebt spreekt dit document je aan in de jij-vorm. Er bewust gekozen voor deze stijl om de afstand tussen de schrijvers en jij als kwartiermaker zo klein mogelijk te maken. De makers van dit document gaan er van uit dat je over voldoende kennis beschikt om deze Roadmap volledig te kunnen toepassen binnen je MBO instelling. Er wordt vanuit gegaan dat je tenminste over de kennis beschikt die in de vijfdaagse Masterclasses Informatiebeveiliging is aangeboden. Elke document dat gebruikt wordt, wordt op de volgende manier geaccentueerd.



Voorgesteld document:
MBO roadmap informatie beveiligingsbeleid en privacy beleid, **(IBPDOC5)**

Bron: *saMBO-ICT / Kennisnet*

Eigenlijk is deze Roadmap een montage handleiding Informatiebeveiliging en privacy. Dus kort samengevat: “Aan de slag en succes!”.

Samenvatting hoofdstukken (stappen)

1. Aanleiding

- Beschrijving urgentie informatiebeveiliging en privacy met als logische vervolgstap het opzetten van Informatiebeveiliging en privacy beleid binnen de MBO instelling.

2. Opdracht

- Formulering van de opdracht voor de kwartiermaker.
- Benoemen van de faciliteiten.
- Vastleggen van de kaders (bijvoorbeeld normenkader ISO 27001-2).

3. Inventarisatie

- Inventarisaties architecturen (proces, data, applicatie en netwerk).
- Gesprekken met medewerkers binnen MBO instelling.
- Eerste globale BIV classificatie en ranking van IT voorzieningen.

4. Nulmeting

- Beleid nulmeting.
- Technische nulmeting.
- Proces nulmeting.

5. Verbeterplan

- Risico's en uitdagingen.
- Verbeterplan.
- Uitvoeren audit(s)

.

1. Aanleiding

1.1 Urgentie

Bedrijven en instellingen zijn in hoge mate afhankelijk van ongestoorde en betrouwbare bedrijfsprocessen. Bij MBO onderwijsinstellingen geldt dit niet alleen voor de processen van bestuur en beheer maar uitdrukkelijk ook voor het onderwijsproces. Informatiebeveiliging en Privacy zijn belangrijke middelen om de risico's op verstoring van de bedrijfsprocessen te voorkomen of te beperken.

Informatiebeveiliging (IB) is een belangrijk thema dat in het mbo hoog op de agenda staat. Het is belangrijk dat het mbo als sector weet om te gaan met pogingen om inbreuk te maken op de beveiliging van systemen. Dat is een kwestie van technologie, processen en gedrag.
Maar informatiebeveiliging gaat verder, het gaat ook om beschikbaarheid, integriteit en vertrouwelijkheid van gegevens. Ook daar zijn maatregelen voor nodig om er voor te zorgen dat alleen bevoegden bij vertrouwelijke informatie komen of om te borgen dat systemen die essentieel zijn voor het onderwijs voldoende beschikbaar zijn en dat de informatie juist, volledig en tijdig aangeleverd wordt. Informatiebeveiligingsbeleid richt zich op al deze aspecten.
Aangrenzend is ook het thema **Privacy (P)** zeer actueel. In het onderwijs worden steeds meer gegevens bijgehouden en het is van groot belang om heel helder te hebben wat er met die informatie gebeurt en op welke wijze die wordt gebruikt. En is het al op basis van de huidige wetgeving zaak om hier heel bewust mee om te gaan en adequate maatregelen te treffen om misbruik van persoonsgegevens in het onderwijs te voorkomen, maar met de nieuwe wetgeving vanuit de Europese Commissie, die naar verwachting in 2016 wordt aangenomen, zal het belang alleen maar toenemen.

Het zal duidelijk zijn dat het thema Informatiebeveiliging en Privacy (IBP) de laatste tijd met een sneltreinvaart in het onderwijs in de belangstelling is komen te staan. Dat heeft ook zijn redenen. Afgelopen jaren zijn in alle sectoren van het onderwijs wel incidenten rond examinering in de publiciteit gekomen (zie ook §1.3. Cyberbedreigingsbeeld Hoger Onderwijs). In sommige gevallen ging dit ook om ernstige incidenten die breed in de media zijn uitgemeten. Dat levert voor het onderwijs veel schade op, waarbij imago- en reputatie schade voorop staat. Het onderwijs wordt geacht op betrouwbare wijze te diplomeren en het kan niet zo zijn dat daar twijfels over bestaan omdat examens op straat liggen dan wel op internet te koop zijn. Een ander voorbeeld is de vraag of het onderwijs met de toenemende registratie van gegevens van leerlingen altijd de bescherming van de privacy nog kan waarborgen. Steeds vaker zijn hier ook externe partijen en leveranciers bij betrokken en zonder goede afspraken hierover kan dit zomaar in het geding zijn. Zeker bij jonge kinderen wordt dit door de maatschappij onacceptabel gevonden. Daar komt bij dat een vraag naar hoe het in de onderwijs sector gesteld is met de informatiebeveiliging en de bescherming van de privacy nauwelijks kan worden beantwoord. Dat beeld is op zijn minst zeer gebrekkig en onhelder te noemen. En om aan te geven of je iets op orde hebt moet je daarover ook eerste afspraken gemaakt hebben over wat dan op orde is. Die afspraken ontbreken vooralsnog. Het "Verantwoordingsdocument informatiebeveiliging en privacy in het MBO onderwijs (IBPDOC1)" gaat hier dieper op in.

1.2 Urgentie vanuit het PO en VO

Niet alleen in de MBO sector staat IBP op de agenda, het thema speelt ook in de PO/VO sector. PWC heeft in opdracht van het OC&W[1] een nulmeting op informatiebeveiliging en privacy uitgevoerd. Doel was het uitvoeren

[1] Ministerie van Onderwijs, Cultuur en Wetenschap, dhr. P. Kantebeen, directie Kennis – Cluster Strategisch Informatiebeleid (Opdrachtgever)
PricewaterhouseCoopers Accountants N.V., Adri de Bruijn RE RA

van een nulmeting die een globaal beeld geeft van de huidige situatie ten aanzien van bescherming van de persoonsgegevens bij DUO en in het veld (primair en voortgezet onderwijs.[2])
De risico's die uit deze bevindingen voortvloeien moeten ook worden beschouwd in het licht van de volgende ontwikkelingen. Deze ontwikkelingen zullen naar onze verwachting de risico's voor de toekomst vergroten:

- Het gebruik van ICT-middelen door onderwijsinstellingen zal in de toekomst toenemen, en daarmee ook de data die verzameld (kunnen) worden over betrokkenen (leerlingen, docenten en ouders). De scholen moeten met het oog op toekomstige ontwikkelingen (bijvoorbeeld Passend Onderwijs) meer en meer gevoelige gegevens vastleggen.
- De technische mogelijkheden om grote hoeveelheden data te combineren en te analyseren, en hieruit zinvolle informatie over individuele personen te destilleren nemen toe. De gesprekken geven aan dat deze ontwikkeling bij scholen en bij de overheid nog in de kinderschoenen staat, het gebruik door leveranciers is niet bekend. Het is onze verwachting dat deze ontwikkeling zich zeker en in snel tempo zal doorzetten, zowel bij onderwijsinstellingen als bij leveranciers.

Het is gezien deze bevindingen en ontwikkelingen van belang dat er in deze fase geacteerd wordt, op een wijze die effectief is voor de sectoren primair en voortgezet onderwijs. Het belang wordt door de onderzochte instellingen erkend.
Het ontbreekt bij hen aan tijd en capaciteit om zich in de materie te verdiepen en additionele capaciteiten zoals regievoering op leveranciers in te richten. Wij zien hier een rol voor koepelorganisaties en belangenorganisaties zoals Kennisnet om een voortrekkersrol in te nemen. Daarnaast is het van belang om de sector PO en VO bewust te maken van privacy en beveiliging, en hen de praktische handreikingen te geven om hun rol als Verantwoordelijke zoals die is omschreven in de Wbp te kunnen nemen. Daarnaast zijn er activiteiten (zoals toezicht op leveranciers) die het best sector breed kunnen worden aangepakt.

1.3 Urgentie vanuit HO (Universiteiten en Hbo-instellingen)

Ook in de HO wordt al een aantal jaren gewerkt aan een IBP beleid. In oktober 2014 heeft SURF een rapport gepubliceerd waarin de bedreigingen die samenhangen met ICT ontwikkelingen worden gepresenteerd.[3]
Het Hoger Onderwijs verwoordt de problemen in de managementsamenvatting als volgt:
Het vertrouwen dat de maatschappij aan onderwijs- en onderzoeksinstellingen schenkt, is groot. De volgende generatie wordt er opgeleid, werkgevers vertrouwen op de kwaliteit van de opleidingen van hun toekomstige werknemers en de toekomst van Nederland als kennisland is ervan afhankelijk. Bij dit vertrouwen hoort de verantwoordelijkheid om informatie adequaat te beschermen en verantwoord om te gaan met de dreigingen in de digitale wereld.

Het risico van deze cyberdreigingen behoort tot de top drie bedrijfsrisico's waarover bestuurders zich het meest druk maken (Lloyds, 2014). Ook in het hoger onderwijs en het wetenschappelijk onderzoek neemt het aantal cyberincidenten onverminderd toe. Daarnaast hebben de gevolgen van deze cyberincidenten een steeds grotere impact.
Het is belangrijk dat de bestuurders van de instellingen hun verantwoordelijkheid hierin herkennen en cybersecurity integraal en gestructureerd aanpakken. Dit Rapport (Cyberbedreigingsbeeld) kan hiervoor een handvat bieden, door een uiteenzetting van het dreigingslandschap, de belangrijkste cyberdreigingen en de te nemen maatregelen te geven.

Het dreigingslandschap wordt vooral omvangrijker en complexer door:
- toenemende connectiviteit,
- groei van de hoeveelheid digitale data,
- toename van het aantal geavanceerde cyberdreigingen en
- de verdere digitalisering van de onderwijs- en onderzoeksinstellingen.

De kwetsbaarheden op het gebied van cybersecurity leiden tot een breed scala aan dreigingen die de instellingen materiële schade kunnen berokkenen. De volgende dreigingen zijn specifiek voor de sector Hoger Onderwijs en het Wetenschappelijk Onderzoek:

- *Verkrijging en openbaarmaking van informatie* – Gevoelige gegevens zoals persoonsgegevens, onderzoeksgegevens en intellectueel eigendom belanden op straat of komen in verkeerde handen.
- *Identiteitsfraude* – Studenten kunnen zich voordoen als een andere student of medewerker om hun eigen studieresultaten te verbeteren of om ongeautoriseerd toegang te krijgen tot geheime informatie, bijvoorbeeld over toetsen.
- *Manipulatie van data* – Manipulatie van data, zoals het wijzigen van studieresultaten door studenten, kan de naam van de gehele instelling in het geding brengen, met ernstige reputatieschade tot (mogelijk) gevolg.
- *Spionage* – Buitenlandse overheden proberen gevoelige informatie te verkrijgen. Vooral onderzoeksinstellingen zijn een interessant doelwit door de aanwezige gevoelige onderzoeksgegevens over bijvoorbeeld nieuwe technologie.

[2] Ministerie van Onderwijs, Cultuur en Wetenschappen
Nulmeting Privacy & Beveiliging Primair en Voortgezet Onderwijs
7 april 2014, 2014-0420a/ADB/ek/jv/ae/ms, Beschikbaar op Kennisnet site
[3] Cyberbedreigingsbeeld, Sector Hoger Onderwijs en Wetenschappelijk Onderzoek.
Het rapport is opgesteld door Deloitte. Referentienummer RS/lb/14-1440-2b. Beschikbaar op SURF site.

- *Verstoring ICT* – DDoS aanvallen, malware en virussen zijn aan de orde van de dag, ook voor onderwijs-als onderzoeksinstellingen.
- *Overname en misbruik ICT* – Onderwijs- en onderzoeksinstellingen hebben vaak toegankelijke ICT-systemen met veel rekenkracht. Deze systemen vormen daarmee een interessant doelwit voor overname en misbruik, bijvoorbeeld door het versturen van spam of het uitvoeren van een DDoS aanval.
- *Bewust beschadigen imago* – Verschillende actoren, waaronder activisten, willen de reputatie van instellingen beschadigen. Bijvoorbeeld door het bekladden van de website of het overnemen van social media accounts.

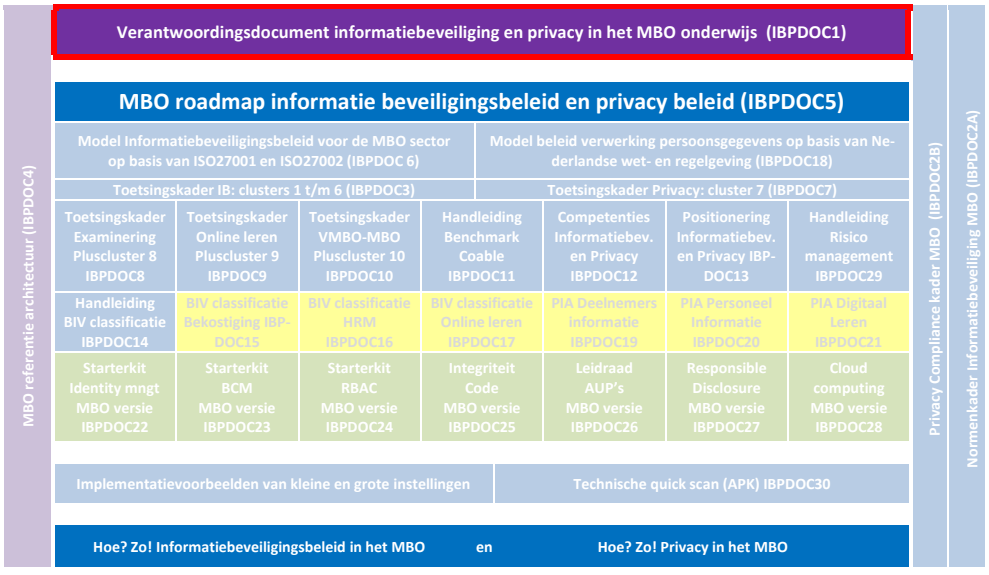
De kans dat deze dreigingen zich voordoen, is zeer reëel. De mogelijke gevolgschade voor onderwijs- en onderzoeksinstellingen kan aanzienlijk zijn. Mogelijke gevolgen van de geïdentificeerde dreigingen zijn:

- financiële schade, bijvoorbeeld aansprakelijkheidsclaims;
- reputatieschade;
- verstoring van de continuïteit van de bedrijfsvoering of de continuïteit van het onderwijs;
- Kamervragen aan de regering;
- aftreden van betrokken bestuurders of andere verantwoordelijke personen.

1.4 Urgentie vanuit het MBO onderwijs

De geschetste bevindingen binnen het PO en VO onderwijs en de beschreven risico's binnen het Hoger Onderwijs zijn ook van toepassing voor de MBO sector (wellicht met uitzondering van *Spionage*).
Bovendien zijn er nog een drietal onderwerpen die beleid aangaande informatiebeveiliging en privacy noodzakelijk maken.

1. **Aanvulling audit kwaliteitszorg m.n. examinering.** Kwaliteitszorg moet kunnen aantonen dat digitale examens voldoen aan allerlei eisen zoals die door de sector in nauw overleg met de Inspectie zijn vastgesteld. Dit toetsingskader toont met hard bewijs aan of een mbo instelling al dan niet voldoet aan de gestelde eisen.
2. **Input accountsverklaring jaarrekening.** Het komt steeds vaker voor dat accountantskantoren inzicht willen hebben in de informatiebeveiliging van een mbo instelling. Dit toetsingskader is afgeleid van een internationaal vastgesteld normenkader (ISO 27001-27002) en dus voor een accountant acceptabel.
3. **Privacy beleid aanzet.** Het CBP verplicht alle onderwijsinstellingen om beleid m.b.t. bescherming Privacyte implementeren, inclusief de benoeming van een Functionaris gegevensbescherming in de nabije toekomst. Toezicht CBP (College bescherming Persoonsgegevens) vindt nu al plaats en zal in de toekomst verscherpt worden.



Voorgesteld document:
Framework informatiebeveiliging en privacy in het MBO onderwijs **(IBPDOC1)**

Bron: *saMBO-ICT / Kennisnet*

Toelichting: Urgentie beschrijving MBO sector.

1.5 Product stap 1: Aanleiding

Een kort document voor het College van Bestuur waarin je de urgentie van een IBP beleid beschrijft.

2. Opdracht plus mandaat

2.1 Externe opdracht

Op basis van het bovengenoemde (1.5) “Urgentie document” zou het College van Bestuur aan een extern adviskantoor een opdracht kunnen verstrekken om de risico’s rondom informatiebeveiliging en privacy in kaart te brengen. Na een oriënterend gesprek zou dit kantoor waarschijnlijk de volgende vragen beantwoord willen hebben:

- Zijn de IT processen, IT infrastructuur (het IT landschap) gedocumenteerd in uw organisatie?
- Hoe wordt het risicomanagement rondom IT op dit moment uitgevoerd? Geldt dit ook voor IT projecten?
- Is er naar uw mening voldoende risico awareness van het personeel en commitment van de directie en College van Bestuur?
- Welke normenkaders worden binnen IT gehanteerd op dit moment? Zijn deze gedocumenteerd?
- Worden controles gelogd?
- Worden de normenkaders ook intern ge-audit?
- Zijn er bekende gaps in de IT beheersing?

2.2 Interne opdracht

Het kan ook zijn dat de afweging wordt gemaakt om de opdracht intern in de organisatie uit te zetten. Er is iemand die hiervoor geschikt is en hiertoe ook bereid en gefaciliteerd. De opdracht die deze zogenaamde kwartiermaker krijgt, moet duidelijk zijn en te realiseren binnen een tijdspanne een vijftigtal werkdagen (dit is uiteraard indicatief). De volgende onderdelen kunnen in de opdracht worden benoemd:

- Benoem de risico’s op het gebied informatiebeveiliging en privacy binnen onze MBO-instelling;
- Voer een nulmeting uit op het gebied van informatiebeveiliging- en privacy beleid;
- Welk algemeen beleid moet ten minste ontwikkeld worden om deze risico’s te mitigeren (verzachten, matigen);
- Geef aan hoe alle medewerkers bewust worden van de noodzaak van dit beleid;
- Maak een voorstel voor de inrichting van een organisatie zodat informatiebeveiliging en privacy geborgd zijn.

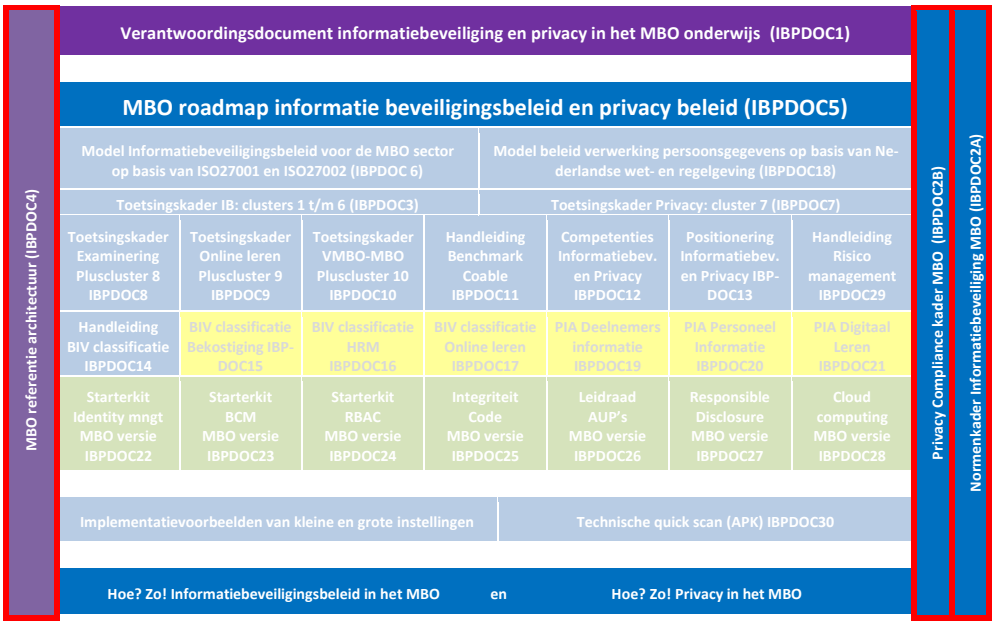
Het is als kwartiermaker van belang dat je de voorgestelde kaders van saMBO-ICT (ISO27001-2, Privacy Compliance Kader, etc.) hanteert en dit als zodanig ook uitvoerig met het CvB communiceert. Dan kun je ook gebruik maken van een brede set aan handreikingen en ondersteuningsmaterialen. Zie hiervoor ook het framework IBP.

2.3 Aanpak

Je kunt de opdracht alleen oppakken of gebruik maken van externe ondersteuning. Als je geen technische achtergrond hebt is het zinvol om een extern bedrijf te laten toetsen (zie APK in $ 4.2) of de technische omgeving voldoet aan een minimum norm. Ook kan het handig zijn om jou bevindingen en aanbevelingen door, de al eerder genoemde, externe deskundige te laten toetsen.

2.4 Verantwoordingsdocument

Het is aan te raden om een verantwoordingsdocument te maken. Dit document bevat verslagen van de interviews die je hebt afgenomen. Het is wenselijk dat je deze verslagen laat lezen door de geïnterviewde collega’s en deze vervolgens voor akkoord laat tekenen.



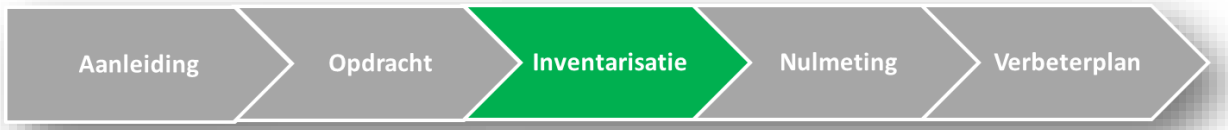
Voorgesteld document:
Normenkader Informatie-beveiliging MBO
(IBPDOC2A)
Privacy Compliance kader MBO
(IBPDOC2B)
MBO referentie architec-tuur
(IBPDOC4)

Bron: *saMBO-ICT / Kennisnet*

2.5 Product stap 2: Opdracht plus mandaat

Je hebt nu een duidelijke opdracht plus mandaat. Deze opdracht bevat een globale tijdsplanning (plus minus 2 - 3 maanden), een aantal onderzoeksvragen, een budget voor de inhuur van externe ondersteuning (€5.000 - €10.000) en de toezegging dat je MBO instelling aansluit bij de voorgestelde kaders van de saMBO-ICT (ISO 27002 normen- en Privacy Compliance kader).

3. Inventarisatie

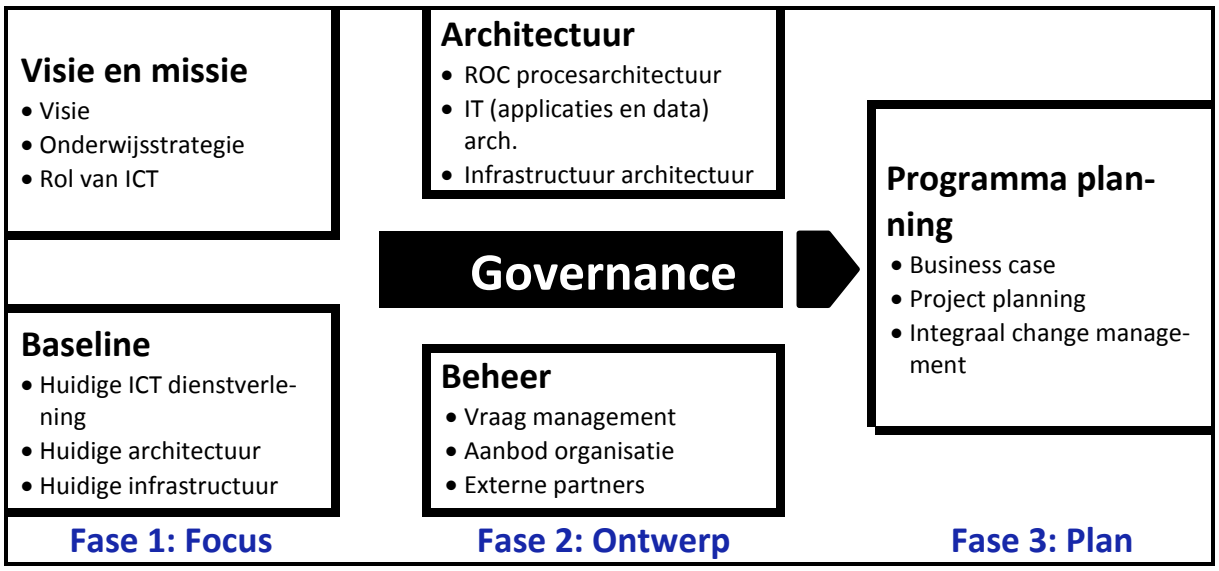


3.1 Inleiding

Nadat de opdracht versterkt is aan de kwartiermaker IBP is het zinvol om een inventarisatie te maken van de ICT omgeving binnen de mbo instelling. Deze foto van de ICT omgeving is erg waardevol voor de volgende fasen.

3.2 Foto ICT omgeving

Het onderstaande schema kan hierbij behulpzaam zijn.



(Bron: Universiteit TIAS Tilburg, Han van der Zee)

De inventarisatie start bij de informatiemanager die de onderstaande, twee groepen, documenten kan aanleveren:
De volgende documenten moeten aanwezig zijn:

- Missie en visie van de onderwijsinstelling.
- Beschrijving van de rol van ICT als afgeleide van de missie en visie.
- Beschrijving huidige ICT dienstverlening (bijvoorbeeld SLA).
- Model proceslandschap (huidig en eventueel toekomstig).
- Model applicatiearchitectuur (huidig en eventueel toekomstig).
- Model netwerkarchitectuur op instellingsniveau (opbouw data center, verbindingen, etc.).
- Model netwerkarchitectuur op locatieniveau (opbouw MER en SER's[4], verbindingen tussen MER en SER's, WLAN architectuur, etc.).

De volgende documenten kunnen aanwezig zijn:

- Visie toekomstige netwerkarchitectuur (eigen beheer, regie organisatie, cloud, etc.)
- Model ICT governance.
- Model ICT beheerorganisatie.

[4] MER Main Equipment Room is de centrale ruimte waar vanuit de services (internet etc.) worden geboden. SER Satellite Equipment Room zijn de decentrale ruimtes die zijn verbonden met de MER.

- ICT projecten portfolio (inclusief business cases).
- Change management procedure (indien voorhanden).

3.3 Kennismaking met stakeholders

Met de bovengenoemde documenten op zak ga je een kennismakingsrondje doen, langs proceseigenaren (primaire- en secundaire processen). functioneel beheerders (kern applicaties) en andere belangrijke functionarissen maken. Denk bijvoorbeeld aan:

- ICT-beheerder(s)
- HRM/P&O
- Financiën
- Onderwijs
- Bedrijfsjurist
- Facilitaire zaken (gebouwbeheer, bedrijfsbeveiliging)
- Kwaliteitszorg
- Planning, & Control en auditing
- Informatiemanagement / CIO of vergelijkbaar
- Deelnemersadministratie
- Examenbureau
- Stage bureau

Tijdens het kennismakingsgesprek stel je met de proceseigenaren een zogenaamde beschikbaarheid classificatie en ranking op van de applicaties die de belangrijkste processen binnen een MBO instelling ondersteunen.

3.3.1 Korte uitleg BIVC

Beschikbaarheid is een van de 3 onderdelen van de zogenaamde BIV classificatie BIV staat voor **B**eschikbaarheid, **I**ntegriteit en **V**ertrouwelijkheid en van informatie. Tegenwoordig wordt ook vaak de term BIVC gebruik waarbij de C voor Controleerbaarheid staat.
De kwaliteitscriteria BIVC kort toegelicht:

Beschikbaarheid: de mate waarin beheersmaatregelen de beschikbaarheid en ongestoorde voortgang van de ict-dienstverlening waarborgen.
Deelaspecten hiervan zijn:

- Continuïteit: de mate waarin de beschikbaarheid van de ict-dienstverlening gewaarborgd is;
- Portabiliteit: de mate waarin de overdraagbaarheid van het informatiesysteem naar andere gelijksoortige technische infrastructuren gewaarborgd is;
- Herstelbaarheid: de mate waarin de informatievoorziening tijdig en volledig hersteld kan worden.

Integriteit: de mate waarin de beheersmaatregelen (organisatie, processen en technologie) de juistheid, volledigheid en tijdigheid van de IT-dienstverlening waarborgen.
Deelaspecten hiervan zijn:

- Juistheid: de mate waarin overeenstemming van de presentatie van gegevens/informatie in IT-systemen ten opzichte van de werkelijkheid is gewaarborgd;
- Volledigheid: de mate van zekerheid dat de volledigheid van gegevens/informatie in het object gewaarborgd is;
- Waarborging: de mate waarin de correcte werking van de IT-processen is gewaarborgd.

Vertrouwelijkheid: de mate waarin uitsluitend geautoriseerde personen, programmatuur of apparatuur gebruik kunnen maken van de gegevens of programmatuur, al dan niet gereguleerd door (geautomatiseerde) procedures en/of technische maatregelen.
Deelaspecten hiervan zijn:

- Autorisatie: de mate waarin de adequate inrichting van bevoegdheden gewaarborgd is;
- Authenticiteit: de mate waarin de adequate verificatie van geïdentificeerde personen of apparatuur gewaarborgd is;
- Identificatie: de mate waarin de mechanismen ter herkenning van personen of apparatuur gewaarborgd zijn;

- Periodieke controle op de bestaande bevoegdheden. Het (geautomatiseerd) vaststellen of geïdentificeerde personen of apparatuur de gewenste handelingen mogen uitvoeren.

Controleerbaarheid: de mogelijkheid om kennis te verkrijgen over de structurering (documentatie) en werking van de IT-dienstverlening.
Deelaspecten hiervan zijn:

- Testbaarheid: De mate waarin de integere werking van de IT-dienstverlening te testen is;
- Meetbaarheid: Zijn er voldoende meet- en controlepunten aanwezig;
- Verifieerbaarheid: De mate waarin de integere werking van een IT-dienstverlening te verifiëren is.

De kwaliteitsaspecten effectiviteit en efficiëntie worden verder niet besproken. In een financiële ict-benchmark worden deze onderzocht, maar niet in de SURFaudit.

3.3.2 Toepassing tijdens de kennismakingsronde

De BIV classificatie is een onderdeel van het toetsingskader dat je in de volgende hoofdstukken gaat toepassen. In de toekomst zullen alle gegevens waarop dit Informatiebeveiligingsbeleid van toepassing is, geclassificeerd moeten zijn. Het niveau van de beveiligingsmaatregelen is afhankelijk van de klasse.
Tijdens de kennismakingsronde zullen we alleen het kwaliteitscriterium beschikbaarheid classificeren.
Ten aanzien van de **beschikbaarheid**seisen worden de volgende klassen onderscheiden:

Klasse	Basisprincipes	Beveiligingsniveau
1: Niet vitaal	algeheel verlies of niet beschikbaar zijn van deze informatie gedurende langer dan 1 week brengt geen merkbare (meetbare) schade toe aan de belangen van de instelling, haar medewerkers of haar klanten	Basisbescherming
2: Vitaal	algeheel verlies of niet beschikbaar zijn van deze informatie gedurende langer dan 1 week brengt merkbare schade toe aan de belangen van de instelling, haar medewerkers of haar klanten	Basisbescherming +
3: Zeer vitaal	algeheel verlies of niet beschikbaar zijn van deze informatie gedurende langer dan 1 etmaal brengt merkbare schade toe aan de belangen van de instelling, haar medewerkers of haar klanten	Basisbescherming ++

De classificatie dient door of namens de eigenaar van het betreffende informatiesysteem te worden bepaald. Daar waar de basisbescherming niet voldoende is moeten voor elk informatiesysteem individueel afgestemde extra maatregelen worden genomen. Met basisbescherming + wordt dus een hoger beveiligingsniveau bedoeld dan bij basisbescherming.
Basisbescherming ++ is het hoogste beschermingsniveau bij een mbo- instelling.
(Bron: Starterskit Identity Management(IBPDOC22))

Proces / Applicatie			
	B	I	V
Elektronische Leeromgeving (bijv. Blackboard)	2	n.v.t.	n.v.t.
Mail	3	n.v.t.	n.v.t.
Website	3	n.v.t.	n.v.t.
Deelnemersvolgsysteen (Eduarte, PS, Magister, etc)	2	n.v.t.	n.v.t.
Financieel pakket	1	n.v.t.	n.v.t.
HRM pakket	1	n.v.t.	n.v.t.
Roosterpakket	1	n.v.t.	n.v.t.
Aan- en afwezigheidsregistratie pakket	1	n.v.t.	n.v.t.
……			

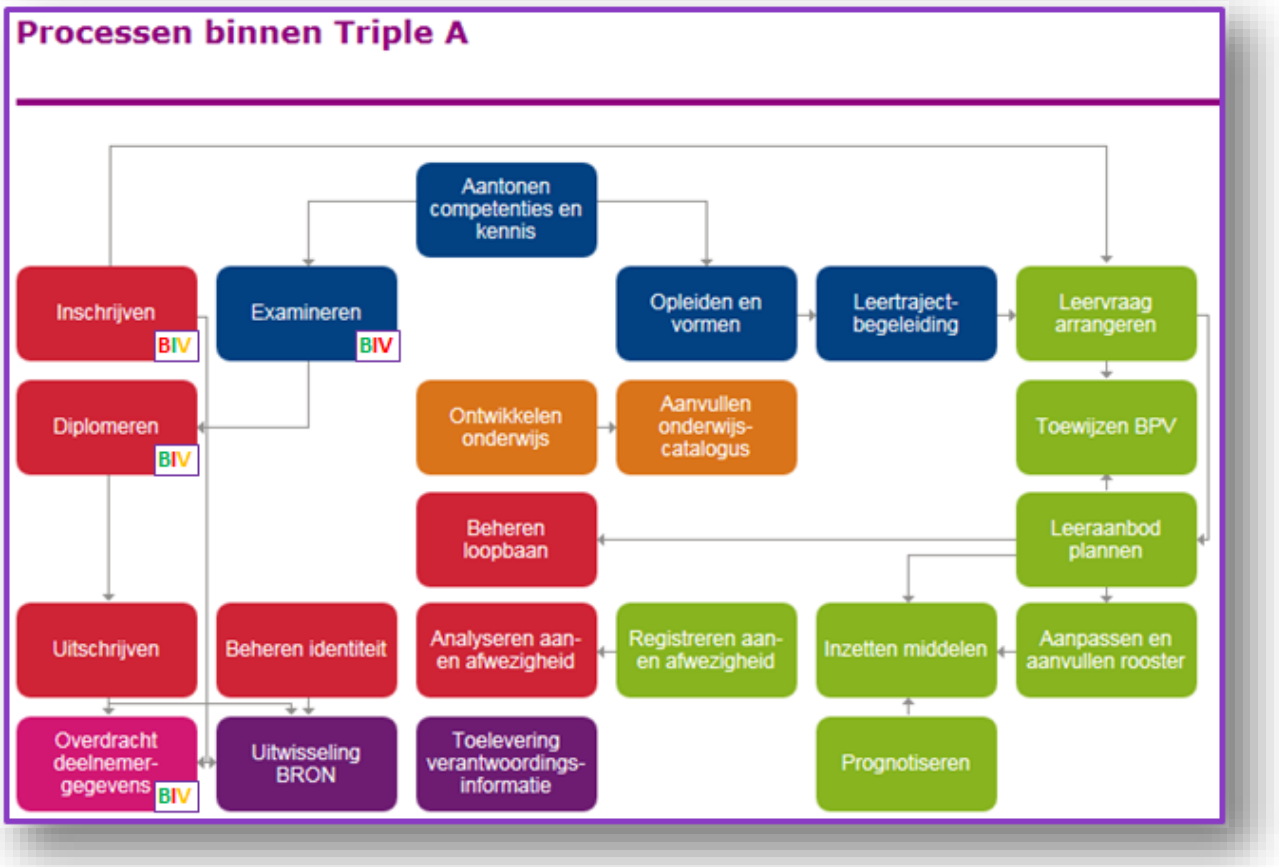
B= Beschikbaarheid I= Integriteit
V= Vertrouwelijkheid

Volgende stap is om met de proceseigenaren om tafel te gaan zitten en vervolgens de verschillende applicaties te gaan rangschikken op basis van BIV en prioritering. De volgende vraag zou je kunnen stellen: "Welke applicatie moet als eerste weer beschikbaar zijn , welke als tweede, enzovoort als ons datacenter volledig zou uitbranden?"

Op basis van ervaringen uit de HO sector zou de volgorde kunnen zijn:
1. *Website (i.v.m. communicatie)*
2. *E-mail omgeving*
3. *ELO*
4. *Etc.*

En vul verder maar in. Dit is een aardige sessie waardoor je informatiebeveiliging voor de eerste maal onderdeel van discussie en dus beleid maakt.

In de nabije toekomst ga je de architectuur van jouw MBO instelling verrijken met een BIV classificatie. Die zou er als volgt uit kunnen zien. Het document Handleiding BIV classificatie (IBPDOC14) gaat hier uitvoerig op in.



3.4 Aanpak tijdens gesprekken

In een situatie dat je je werk probeert uit te voeren zonder dat jouw toekomstige rol duidelijk is heb je een bepaalde attitude nodig om het maximale uit de situatie te halen, zonder je toekomstige positie te schaden. Je houding naar je gesprekspartners moet gekenmerkt worden door een dienstverlenende klantgerichte stijl: "Vertel me hoe jouw processen in elkaar zitten en tegen welke problemen je aanloopt, dan kan ik wellicht in een vervolgfase helpen die problemen op te lossen". Let er wel op dat je geen toezeggingen doet die je in de toekomst niet kunt waarmaken. Wellicht gaat een ander jouw startsituatie verder uitwerken.

3.5 Product stap 3: Inventarisatie

Je hebt met de stakeholders gesproken en hun wensen geïnventariseerd. Je hebt de architectuur in kaart gebracht of ontdekt dat hier werk aan de winkel is. Tot slot heb je al een voorzichtige BIV classificatie gemaakt en een ranking afgesproken bij een grote calamiteit.

4. Nulmeting

4.1 Terugblik

Je hebt inmiddels al een ICT foto en een eerste beschikbaarheid classificatie en ranking gemaakt. Alvorens je de nulmeting kunt uitvoeren is het zinvol dat je een idee hebt over de betrouwbaarheid en correcte werking van de technische componenten die onderdeel zijn van de informatiebeveiliging en privacy. Daartoe is een checklist gemaakt samen met IT bedrijven, SURF en een aantal MBO instellingen. Deze zogenaamde APK keuring op de technische omgeving kun je zelf uitvoeren of laten uitvoeren, bijvoorbeeld door één van de bedrijven die meegewerkt hebben aan het opstellen van deze “keuring”.

4.2 APK keuring technische omgeving

4.2.1 Techniek dreigingen extern

- Welke firewalls worden gebruikt om het verkeer vanaf buitenaf tegen te houden?
- Is er een Demilitariseerde Zone ingericht waarin uitsluitend componenten staan die toegang moeten hebben tot het publieke netwerk (en geen productiegegevens)?
  Opmerking: Ook productiegegevens kunnen in de DMZ toegestaan zijn, zoals de activiteitenkalender.
- Zijn er maatregelen ingericht tegen Denial-of-Service aanvallen?

4.2.2 Techniek dreigingen intern

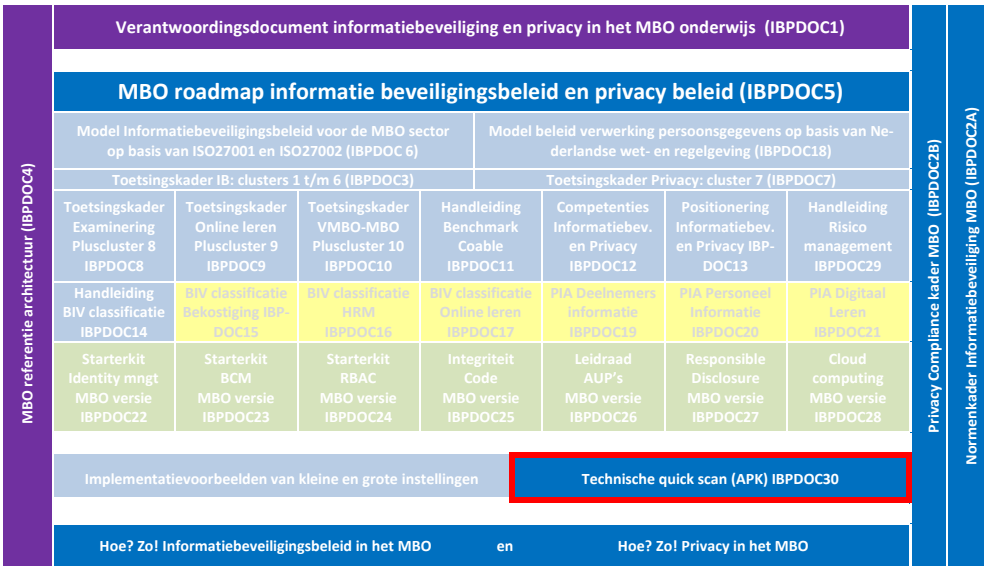
- Hoe "open" staat jullie wireless omgeving? Voor iedereen toegankelijk of niet? Maken jullie gebruik van 802.1x en/of andere methoden voor netwerktoegangscontrole?
- Hoe "open" staat jullie wired netwerk? Voor iedereen toegankelijk of niet? Maken jullie gebruik van 802.1x en/of andere methoden voor netwerktoegangscontrole?
- Hoe wordt geborgd dat besmette werkplekken worden gedetecteerd? Worden er naast antivirus nog andere technieken ingezet? Hoe rapporteren of zien jullie momenteel het vreemde/afwijkende/verdachte verkeer?
- Welke opvolging wordt er gegeven op gedetecteerd vreemd/afwijkend/verdacht verkeer? Zijn hiervoor technische maatregelen ingericht?
- Zijn de essentiële verbindingen (bijvoorbeeld voor beheer) voldoende beveiligd? Van welke encrypties maken jullie gebruik?
- Hoe is jullie dat center ingericht? In house of out house? Welke fysieke beveiligingsmaatregelen zijn hierbij genomen?
- Zijn er maatregelen genomen tegen Single-Points-of-Failure (SPOFs) door essentiële componenten (bijvoorbeeld core switches) dubbel uit te voeren?
- Worden interne verkeerstromen ook onderling gefilterd?

4.2.3 Aanvullende dumps en scans

- Dump van de AD (Microsoft omgeving) om deze te analyseren. Hieruit haal je:
  - Wachtwoordbeleid, en of dit consequent wordt toegepast;
  - Aantal beheerders en andere accounts met additionele privileges.
- MSBA rapportage (Microsoft omgeving) om patch management van het OS te valideren, een kleine steekproef is voldoende.
- Liefst een basale kwetsbaarhedenscan van 2-3 interne en externe systemen, bijvoorbeeld met OpenVas o.i.d. (thermometer gehalte).
- Liefst een NIST-scan voor controleren hardening maatregelen. Aan deze tooling zijn enige out-of-pocket kosten verbonden.

4.2.4 Correctie en herstel

- Welke back up tooling wordt er gebruikt, worden alle servers hierin meegenomen?
- Zijn er voor de netwerkcomponenten zoals de firewall, etc. ook back ups van de configs?
- Wordt de DMZ ook gebackuped?
- Is de back up gescheiden opgezet van het productienetwerk?



Voorgesteld document:
Technische quick scan (APK)
(IBPDOC30)

Bron: *saMBO-ICT / Kennisnet Met ondersteuning ICT bedrijven*

Deze technische inventarisatie geeft een eerste indruk van de betrouwbaarheid en correcte werking van het netwerk. Een kort rapport beschrijft een algemene indruk van het netwerk en geeft aanbevelingen op die punten die snel opgepakt moeten worden. Als het onderzoek niet door een externe partij is uitgevoerd dan is een review van het rapport door een extern adviesbureau gewenst.

4.3 Nulmeting op basis van toetsingskader IBP

Kenmerkend voor het vakgebied auditing is dat een onderzoek plaatsvindt ten opzichte van een eerder opgesteld en afgestemd normenkader. Zonder normenkader is een onderzoek feitelijk geen audit.
In vogelvlucht is deze nulmeting als volgt tot stand gekomen:

1. MBOaudit hanteert het generieke internationale normenkader voor informatiebeveiliging ISO27001 en de daarvan afgeleide set van best practices ISO 27002. In de literatuur is dit normenkader bekend onder de titel "Code voor Informatiebeveiliging". Dit normenkader bestaat uit 114 statements die verdeeld zijn over 14 hoofdstukken.
2. Het normenkader HO/MBO maakt gebruik van 79 statements uit het ISO 27002 normenkader, terwijl 35 statements (nog)[5] niet gebruikt worden. Een zestal statements worden in het HO/MBO normenkader gesplitst waardoor er in totaal 85 statements zijn opgenomen.

[5] SURFibo is voornemens in 2017 alle 114 statements te gaan gebruiken.

Schematisch als volgt weergegeven:

Hoofdstukken ISO-27002	ISO-27002	Clusterindeling Hoger Onderwijs						
		1: Beleid	**2**: personeel	**3**: Ruimten	**4**: Continuïteit	**5**: Toegang	**6**: Controle	Niet gebruikt
5. Informatiebeveiligingsbeleid	**2**	2						
6. Organiseren van informatiebeveiliging	**7**	4		0				3
7. Veilig personeel	**6**		3					3
8. Beheer van bedrijfsmiddelen	**10**	2		1				7
9. Toegangsbeveiliging	**14**		1			9	1	3
10. Cryptografie	**2**	1				1		
11. Fysieke beveiliging en beveiliging van de omgeving	**15**	1	1	12				1
12. Beveiliging bedrijfsvoering	**14**			1	7	1	2	3
13. Communicatiebeveiliging	**7**	2	1			4		
14. Acquisitie, ontwikkeling en onderhoud van informatiesystemen	**13**	1			1	1	3	7
15. Leveranciersrelaties	**5**	2			1		1	1
16. Beheer van informatiebeveiligingsincidenten	**7**	2	1		2		1	1
17. Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer	**4**				2			2
18. Naleving	**8**	2					2	4
	114	**19**	**7**	**14**	**13**	**16**	**10**	**35**
Clustertotaal inclusief splitsing (85)		21	7	15	15	17	10	

(tabel 2: samenhang ISO-27002 normenkader en HO/MBO normenkader)

Het normenkader HO/MBO is beschreven in het document "**Normenkader Informatiebeveiliging MBO (IBP-DOC2A)**". Een samenvatting is als document beschikbaar onder de naam: **Handboek MBO audit (IBPDOC3+).**

3. Het normenkader HO/MBO wordt verrijkt tot het Toetsingskader Informatiebeveiliging-MBO door er bewijslast aan toe te voegen. Het toetsingskader is net als het normenkader ingedeeld in clusters.
   De clusterindeling is gebaseerd op een logische indeling die goed bruikbaar is voor het mbo- onderwijs. Per cluster zijn ook kwaliteitsaspecten af te leiden.

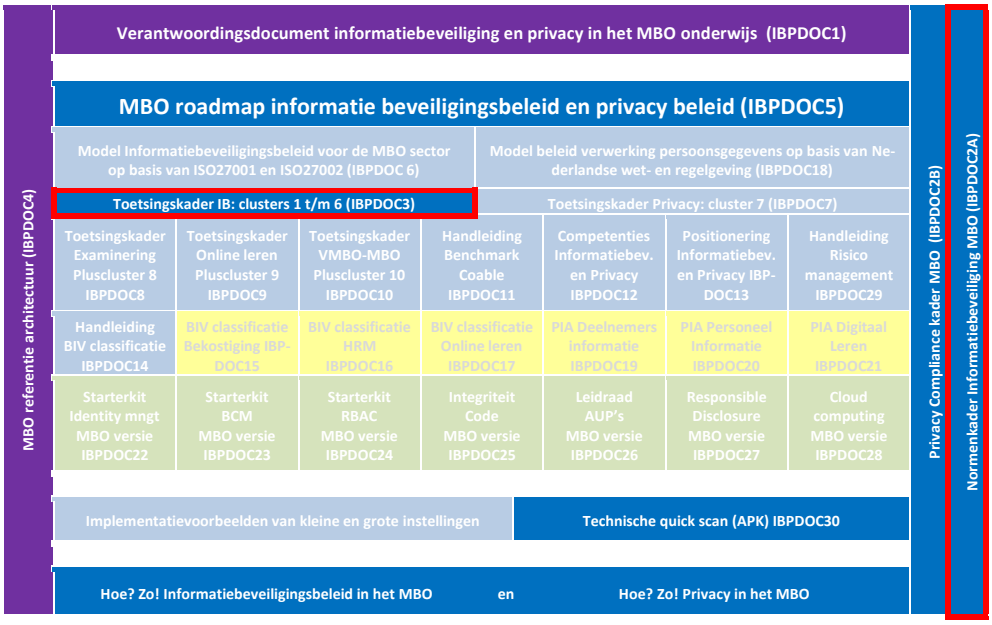
Schematische samenvatting:

Cluster	Onderwerpen (o.a.)	Kwaliteitsaspecten	Betrokkenen
1. Beleid en Organisatie	Informatiebeveiligingsbeleid Classificatie Inrichten beheer	• Beschikbaarheid • Integriteit • Vertrouwelijkheid • Controleerbaarheid	College van Bestuur Directeuren
2. Personeel, studenten en gasten	Informatiebeveiligingsbeleid Aanvullingen arbeidsovereenkomst Scholing en bewustwording	• Integriteit • Vertrouwelijkheid	College van Bestuur Dienst HR Ondernemingsraad Studentenadministratie
3. Ruimte en Apparatuur	Beveiligen van hardware, devices en bekabeling	• Beschikbaarheid • Integriteit	College van Bestuur ict dienst of afdeling
4. Continuïteit	Anti virussen, back up, bedrijf continuïteit planning	• Beschikbaarheid	College van Bestuur ict dienst of afdeling Functioneel beheer
5. Toegangsbeveiliging en Integriteit	Gebruikersbeheer, wachtwoorden, online transacties, sleutelbeheer, validatie	• Integriteit • Vertrouwelijkheid	College van Bestuur Functioneel beheer ict dienst of afdeling
6. Controle en logging	Systeemacceptatie, loggen van gegevens, registreren van storingen, toetsen beleid	• Controleerbaarheid	College van Bestuur Stafmedewerker informatiebeveiliging Kwaliteitszorg

4. Kort samengevat heb je gezien dat het normenkader uit 114 statements bestaat, waarvan wij er 85 als MBO statements gebruiken. In deze nulmeting ga je deze statements onderzoeken. Je zou daarbij kunnen beginnen met een beperkte set die de hoogste prioriteit heeft, bijvoorbeeld de 15 statements die hieronder staan. De bewijslast vind je in het document: **Toetsingskader Informatiebeveiliging: clusters 1 t/m 6 (IBPDOC3)**. De groene vakjes hebben ook betrekking op het privacy onderzoek.

1: Beleid en Organisatie		
MBO nr.	**ISO27002**	**Statement**
1.1	**5.1.1.1**	**Beleidsregels voor informatiebeveiliging:** Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd en goedgekeurd door het bestuur.
1.2	**5.1.1.2**	**Beleidsregels voor informatiebeveiliging**: Het door het bestuur vastgestelde Informatiebeveiligingsbeleid wordt gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.
1.7	**8.2.1**	**Classificatie van informatie:** Informatie behoort te worden geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging.
1.8	**8.2.2**	**Informatie labelen:** Om informatie te labelen behoort een passende reeks procedures te worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.
1.15	**15.1.2**	**Opnemen van beveiligingsaspecten in leveranciersovereenkomsten:** Alle relevante informatiebeveiligingseisen behoren te worden vastgesteld en overeengekomen met elke leverancier die toegang heeft tot IT-infrastructuurelementen ten behoeve van de informatie van de organisatie, of deze verwerkt, opslaat, communiceert of biedt.
1.20	**18.1.4**	**Privacy en bescherming van persoonsgegevens:** Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.
2: Personeel, studenten en gasten		
MBO nr.	**ISO27002**	**Statement**
2.1	**7.1.2**	**Arbeidsvoorwaarden:** De contractuele overeenkomst met medewerkers en contractanten behoort hun verantwoordelijkheden voor informatiebeveiliging en die van de organisatie te vermelden.
2.2	**7.2.2**	**Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging:** Alle medewerkers van de organisatie en, voor zover relevant, contractanten behoren een passende bewustzijnsopleiding en -training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie.
4: Continuïteit		
MBO nr.	**ISO27002**	**Statement**
4.13	**16.1.5**	**Respons op informatiebeveiligingsincidenten:** Op informatiebeveiligingsincidenten behoort te worden gereageerd in overeenstemming met de gedocumenteerde procedures.
4.14	**17.1.2**	**Informatiebeveiligingscontinuïteit implementeren:** De organisatie behoort processen, procedures en beheersmaatregelen vast te stellen, te documenteren, te implementeren en te handhaven om het vereiste niveau van continuïteit voor informatiebeveiliging tijdens een ongunstige situatie te waarborgen.
5: Toegangsbeveiliging en integriteit		
MBO nr.	**ISO27002**	**Statement**
5.1	**9.1.1**	**Beleid voor toegangsbeveiliging:** Een beleid voor toegangsbeveiliging behoort te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen.
5.2	**9.1.2**	**Toegang tot netwerken en netwerkdiensten:** Gebruikers behoren alleen toegang te krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.

6: Controle en logging		
MBO nr.	**ISO27002**	**Statement**
6.1	**9.2.5**	**Beoordeling van toegangsrechten van gebruikers:** Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen.
6.3	**12.4.3**	**Logbestanden van beheerders en operators:** Activiteiten van systeembeheerders en -operators behoren te worden vastgelegd en de logbestanden behoren te worden beschermd en regelmatig te worden beoordeeld.
6.9	**18.2.2**	**Naleving van beveiligingsbeleid en –normen:** Het management behoort regelmatig de naleving van de informatieverwerking en -procedures binnen haar verantwoordelijkheidsgebied te beoordelen aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.



Voorgesteld document:
Normenkader Informatiebeveiliging MBO
(IBPDOC2A)
Toetsingskader IB: clusters 1 t/m 6
(IBPDOC3)

Bron: *saMBO-ICT / Kennisnet*
.

4.4 Product stap 4: Nulmeting

Je hebt nu een eerste inventarisatie van de technische en beleidsmatige stand van zaken van de informatiebeveiliging en privacy van je MBO instelling. Mogelijke bevindingen zouden kunnen zijn dat er geen beleidsplan voorhanden is, dat er niet gelogd wordt. Eén van de aanbevelingen zou dan moeten zijn dat er zo snel mogelijk een beleidsplan Informatiebeveiliging en/of privacy geschreven gaat worden of dat er een systeem van logging en control moet worden ingericht.

5. Verbeterplan

Verbeterplan

Je opdracht, als kwartiermaker verwoord in §2.2, heb je inmiddels voortvarend opgepakt. De opdrachten leiden al tot concrete acties. Nogmaals het overzicht, nu aangevuld met een verdieping in paars.

1. Benoem de risico's op het gebied informatiebeveiliging en privacy binnen onze MBO-instelling;
   Niet alleen zijn de ***risico's*** benoemd maar ook de ***uitdagingen*** *(§5.1)*;
2. Voer een nulmeting uit op het gebied van informatiebeveiliging- en privacy beleid;
   Het uitvoeren van ***audits*** *(§5.2)* is een vast onderdeel van je taak; bovendien heb je een technisch scan (APK) uitgevoerd.
3. Welk algemeen beleid moet ten minste ontwikkeld worden om deze risico's te mitigeren;
   De vastgestelde documenten van saMBO-ICT en Kennisnet kunnen je helpen om het ***algemeen beleid*** *(§5.3)* binnen je MBO instelling vorm te geven;
4. Geef aan hoe **alle** medewerkers bewust worden van de noodzaak van die beleid;
   Awareness *(§5.4)* van het personeel **en** studenten is een onderwerp dat voortdurend op de scholingsagenda moet staan. "Informatiebeveiliging is geen democratie; Op zijn best een vriendelijke dictatuur"
5. Maak een voorstel voor de inrichting van organisatie zodat informatiebeveiliging en privacy geborgd zijn.
   Niet alleen moet de staande organisatie worden ingericht, zeg maar de "schooluren" organisatie maar ook een organisatie die snel reageert op informatiebeveiliging en privacy incidenten op basis van 7x24, we noemen dit de ***IBP-organisatie*** *(§5.5)*.

5.1 Risico's & Uitdagingen

Op basis van je bevindingen uit hoofdstuk 3 en 4 kun je nu de risico's samen met de proceseigenaren gaan benoemen. Dit is geen makkelijk taak. Als sociaal vaardige kwartiermaker ga je met veel enthousiasme aan de slag. Maar vaak blijkt dat je collega's niet op jou zitten te wachten. Regelmatig krijg je dan te horen dan te horen:

- je veel te negatief bent, het zal wel allemaal meevallen;
- je de moeilijkheid van het werk duidelijk overschat, er is geen risicomanagement nodig;
- het moment waarop risico's worden aangedragen is nooit goed;
- je moet je geen zorgen maken, veel zaken worden al beheerst.

Maar hou vast!

Ter overdenking; lijst met bruikbare principes

- Doelen en risico's horen bij elkaar;
- Risicomanagement geeft vertrouwen;
- Als je alles onder controle hebt, ga je niet hard genoeg;
- Een manager zonder risico's is een slechte manager;
- Een goede manager neemt risico's en communiceert erover;
- Als je niet naar risico's vraagt, krijg je ze ook niet te horen;
- Twee weten meer dan één;
- Wie zijn risico's niet kent, heeft geen keuze;
- Risico's worden het best beheerst door hen die er belang bij hebben;
- Wie niet reflecteert op successen en fouten, is gestopt met leren;
- Risicomanagement gaat om expliciteren van kennis;
- Risicomanagement is geen doel op zich;
- Innovatie en risicomanagement gaan goed samen;

- 90% van de risico's heeft als oorzaak menselijk handelen;
- Fouten maken doe je niet alleen;
- Een auto zonder remmen gaat niet hard;
- Ondernemen is risico's nemen en van fouten leren.[6]

Binnen de MBO sector hebben we alle mogelijke risico's in kaart gebracht. Het document Handleiding Risico management (IBPDOC29) beschrijft de meest voorkomende risico's binnen een MBO instellingen op een viertal gebieden, te weten:

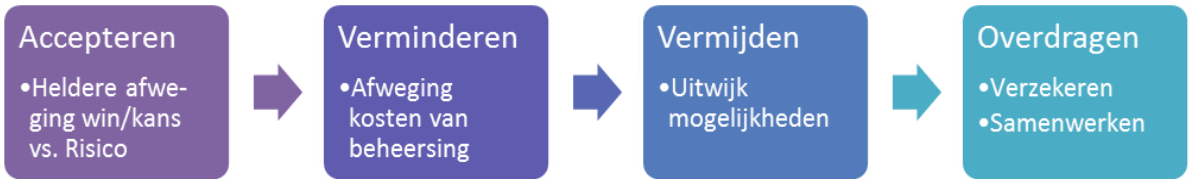
1A Beleid, organisatie en personeel Informatiebeveiliging
1B Beleid, organisatie en personeel Privacy
Cluster: 1, 2 en **7**
2 Techniek en externe koppelingen
Cluster: 3, 4 en 9
3 Applicaties en audit
Cluster: 5 en 6
4 Examineren
Cluster: 8

Deze inventarisatie is tot stand gekomen tijdens de masterclasses groep 1 en 2 (40 deelnemers) en is dus vrij volledig.
Een korte (voorbeeld) opsomming:

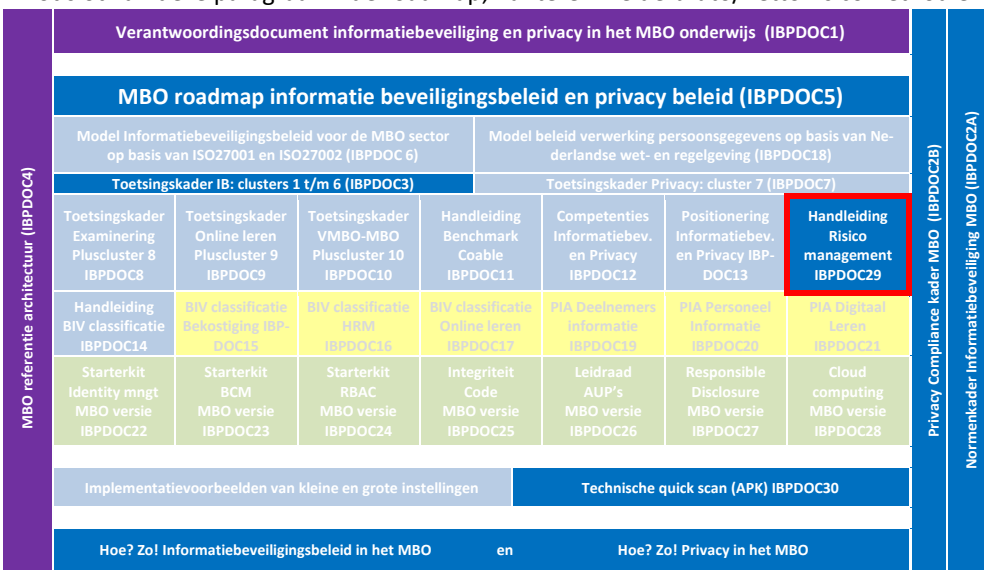
Onderdeel	Risico omschrijving	Oorzaak	Gevolg
1. Privacy	Het risico dat data onrechtmatig wordt opgeslagen en onvoldoende bescherming van persoonsgegevens	Onvoldoende scheiding van rechten over groepen van personen	niet nakomen van de privacy wetgeving
2. Kernregistratiesysteem	Het risico op fraude of onrechtmatige invoer in kernregistratiesysteem.	Onvoldoende controles en functiescheiding in het systeem	frauduleuze handelingen kunnen plaatsvinden reputatie schade)
3. Cijferregistratiesysteem	Het risico op fraude bij invoer/mutatie van cijfers in cijferregistratiesysteem.	Onvoldoende ingebouwde controles (functiescheiding, 4-ogen principe)	een onjuiste beoordeling van deelnemers reputatie schade
4. Beschikbaarheid netwerk	Het risico op uitval van IT Infrastructuur	Gebrek aan redundante (dubbele) uitvoer (stroom, servers, netwerk apparatuur etc.)	geen beschikbaarheid
5. Ongeoorloofd gebruik/toegang	Het risico op ongeoorloofd gebruik/toegang (bijvoorbeeld door hackers) tot de IT infrastructuur	Onvoldoende technische beveiligingen	niet beschikbaar zijn, onbetrouwbaarheid en diefstal van gegevens reputatie schade
6. Studentenvolgsysteem	Het studentenvolgsysteem is niet beschikbaar	Het niet redundant uitvoeren van de database server (mogelijk in de cloud)	studenten/medewerkers/docenten niet bij hun gegevens kunnen.
7. Elektronische leeromgeving	Het risico op ongeautoriseerd gebruik van de elektronische leeromgeving	Een gebrek aan procedures en/of het opvolgen daarvan	fraude, diefstal, reputatie schade etc.
8. Onvolledige dienstverlening door leveranciers	Het risico op onvolledige dienstverlening door leveranciers.	Een gebrek aan vastleggen van afspraken (SLA) of een te veel aan vertrouwen (geen monitoring)	niet beschikbaar zijn voor de klant, reputatie schade.
9. Ongeautoriseerde toegang	Het risico op ongeautoriseerde toegang	Onvoldoende volwassenheid/bewustzijn over IT-beveiliging bij medewerkers door bv. deling van wachtwoorden	fraude, diefstal, reputatie schade
10. Dataverlies	Het risico op dataverlies	Een gebrek aan back ups (procedures) of calamiteitenplan	Gebrek aan beschikbaarheid Reputatie schade

Een, wellicht overbodige, opmerking: de ISO 27001 en 27002 is een best practice op basis van risico analyses van wereldwijd opererende bedrijven. Met andere woorden als je ISO geïmplementeerd hebt, dan heb je feitelijk alle bekende risico's op het gebied van informatievoorziening en privacy gemitigeerd. Als je een nulmeting hebt uitgevoerd en je hebt een aantal risico's beschreven dan wil dat nog niet zeggen dat je deze dan gaat elimineren. Er zijn meerdere oplossingen mogelijk, zoals hieronder schematisch weergegeven:

[6] Ton van Gessel (KPMG): Risk Assessment en Policies (presentatie SURFibo congres 2015)



Tot slot van deze paragraaf in de roadmap, hanteren we de bruto/netto risicomethodiek.

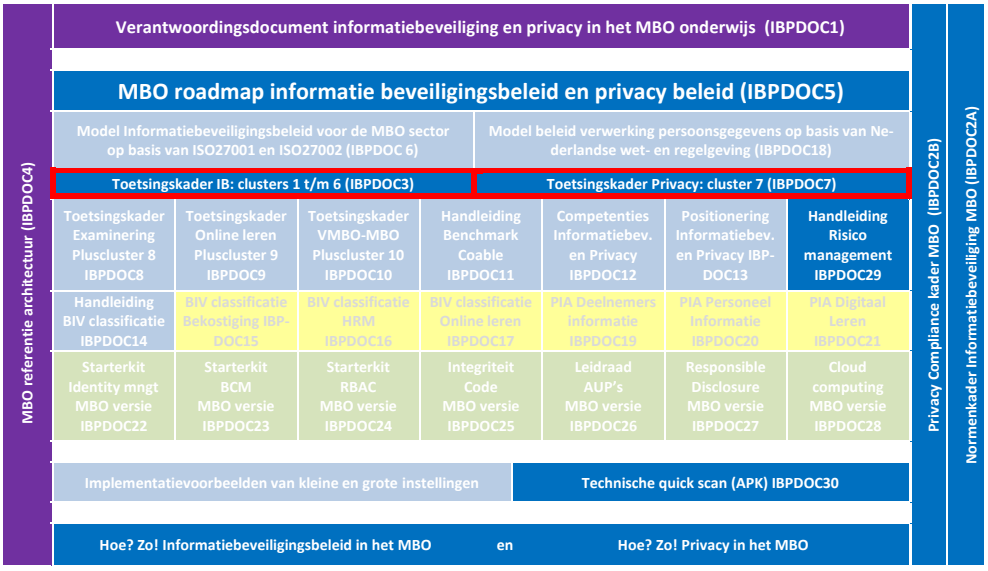


Voorgesteld document:
Handleiding Risico Management
(IBPDOC29)

Bron: *saMBO-ICT / Kennisnet*

5.2 Audits

De eerste audit die je uitvoert is de nulaudit. Je hebt weliswaar al een beperkte audit (nulmeting) uitgevoerd. Het is nu zinvol om de volledige audit uit te voeren, zodat je op basis van volwassenheidsniveaus kunt bepalen waar je instelling staat. Weliswaar heb je al 15 statements in de vorige fase onderzocht, je gaat nu alle 85 statements onderzoeken. Het document Toetsingskader IB: clusters 1 t/m 6 (IBPDOC3) leidt je door de ISO 27002 vragen heen en geeft je bovendien een handreiking om een en ander aan te tonen (evidence). Aanvullend is ook het Toetsingskader Privacy: cluster 7 beschikbaar om ook op privacy gebied een eerste nulmeting uit te voeren. Een volledige audit kost je 5 tot 10 dagen. De medewerking van de informatiemanager, applicatie beheer, ICT beheer, personeelszaken, huisjurist en een aantal proceseigenaren is vereist om deze audit succesvol uit te voeren. Als je de audit uitvoert zonder de bewijzen (evidence) op te eisen en te onderzoeken kun je deze, beperkte, audit in een halve dag uitvoeren met behulp van hoofd ICT en applicatiebeheer. In de rol van kwartiermaker is deze beperkte aanpak zeker acceptabel.



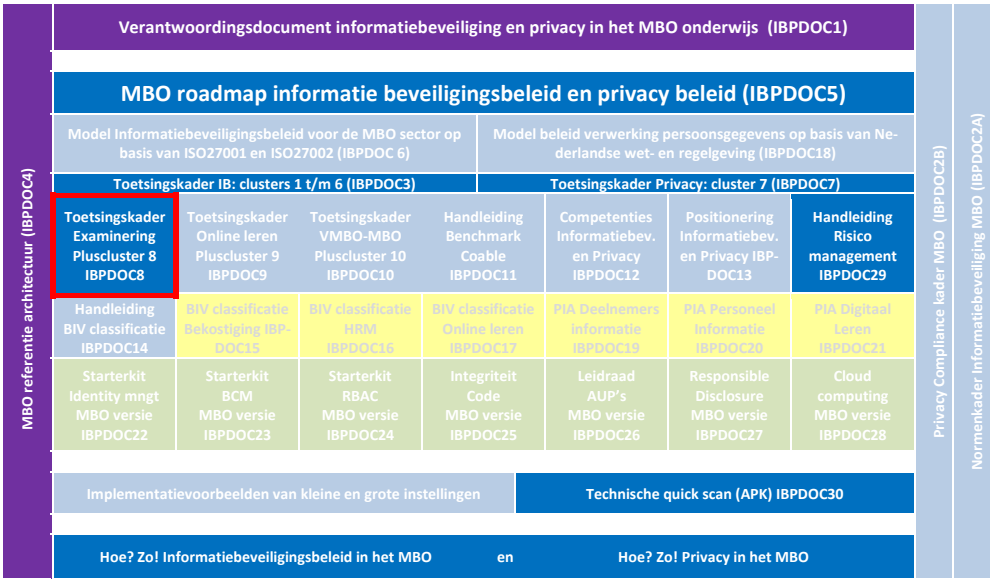
Voorgesteld document:
Toetsingskader IB: clusters 1 t/m 6
(IBPDOC3)
Toetsingskader Privacy: cluster 7
(IBPDOC7)

Bron: *saMBO-ICT / Kennisnet*

Bovenop het generiek toetsingskader zijn er ook nog, speciaal voor de MBO sector, een aantal aanvullende toetsingskaders ontwikkeld:

- Toetsingskader Examinering Pluscluster 8 (IBPDOC8).

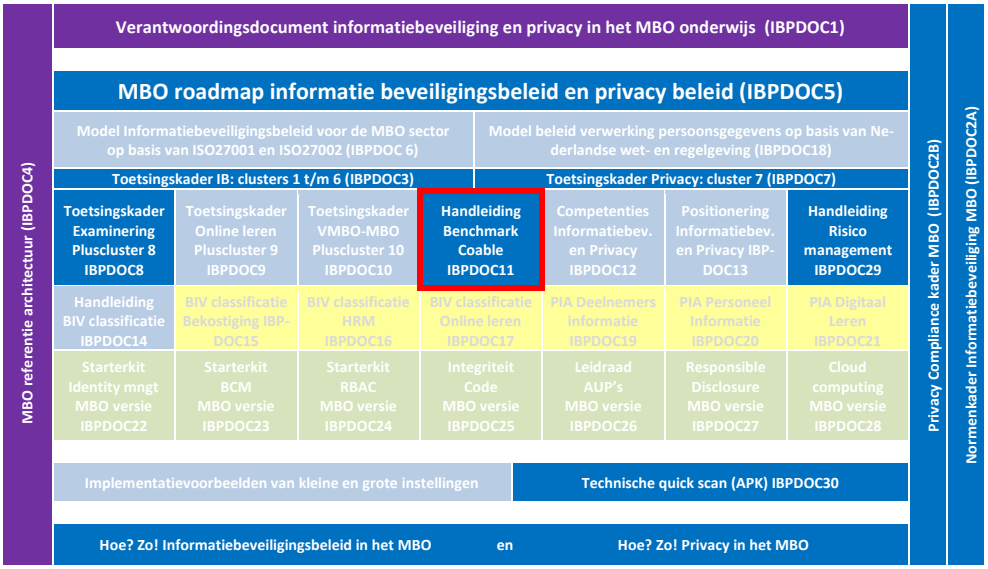
Dit is een omvangrijke klus en wellicht is het verstandiger om deze audit in een later stadium uit te voeren.



Voorgesteld document:
Toetsingskader Examinering: Pluscluster 8
(IBPDOC8)
Toetsingskader Online leren: Pluscluster 9
(IBPDOC9)
Toetsingskader VMBO-MBO: Pluscluster 10
(IBPDOC10)

Bron: *saMBO-ICT / Kennisnet*

In een volgende fase kun je een peer audit (samen met andere MBO instellingen) uitvoeren en op termijn zelfs een externe audit door, bijvoorbeeld, een van leden van de "Big 4" (KPMG, Deloitte, PWC en Ernst & Young). De door jou uitgevoerde audit methodiek zal in de toekomst erkend worden door deze accountantskantoren. De wens is dat zij dan alleen het proces auditen en niet de producten.
SaMBO-ICT en Kennisnet hebben het bovendien mogelijk gemaakt om een benchmark op te zetten door de inzet van een tool (Coable). Document Handleiding Benchmark Coable IBPDOC11 helpt je om dit hulpmiddel snel en eenvoudig in te zetten binnen je MBO instelling. In de toekomst kun je op basis van deze uitkomsten je eigen MBO instelling vergelijken met de MBO cijfers die tot stand komen door de resultaten van de deelnemende MBO instellingen anoniem te presenteren.



Voorgesteld document:
Handleiding Benchmark
(IBPDOC11)

Bron: *saMBO-ICT / Kennisnet*

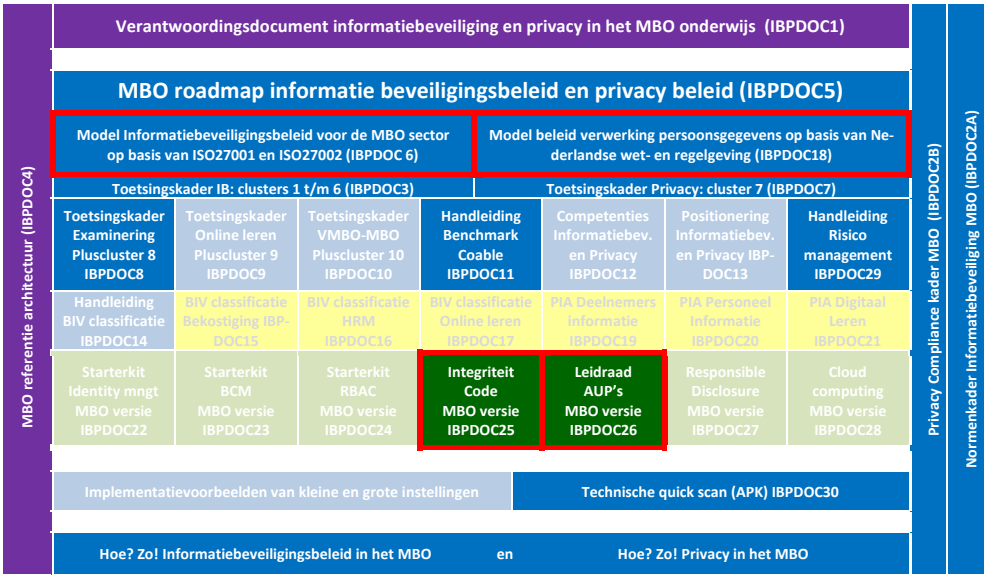
Toelichting: Urgentie beschrijving MBO sector.

5.3 Algemeen Beleid

Uit de nulmeting zou naar voren kunnen komen dat er geen of weinig beleid is ten aanzien van informatiebeveiliging en privacy. Weliswaar kan het zijn dat er eigen (wel of niet vastgestelde) documenten voorhanden zijn, dan nog is het aan te bevelen om die documenten te toetsen aan de referentiedocumenten zoals die ontwikkeld zijn door SURFibo, bewerkt door saMBO-ICT / Kennisnet en soms gereviewed door de Gartner Group.

De volgende documenten kunnen vrij snel worden opgeleverd en vastgesteld (opzet en bestaan[7]) en zijn een belangrijke voorwaarde om het IBP beleid te implementeren:

- Model Informatiebeveiligingsbeleid voor de MBO sector op basis van ISO27001 en ISO27002 (IBPDOC 6);
- **Model beleid verwerking persoonsgegevens op basis van Nederlandse wet- en regelgeving (IBPDOC18);**
- Leidraad Acceptable Use Policy's (verantwoord ICT gebruik) MBO versie (IBPDOC26);
- Integriteit Code (ICT gedragscode voor beheerders) MBO versie (IBPDOC25).



Model Informatiebeveiligingsbeleid voor de MBO sector op basis van ISO27001 en ISO27002 **(IBPDOC6)**
Model beleid verwerking persoonsgegevens op basis van Nederlandse wet- en regelgeving **(IBPDOC18)**
Bron: *saMBO-ICT / Kennisnet*
Integriteit Code MBO versie **(IBPDOC25)**
Leidraad AUP's MBO versie **(IBPDOC26)**
Bron: *SURFibo*

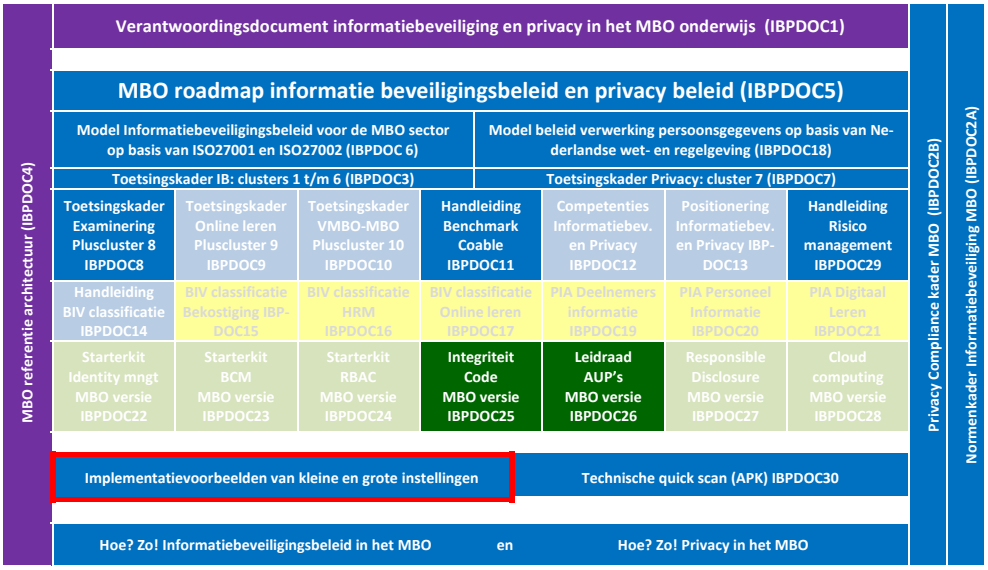
5.4 Awareness

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van informatiebeveiliging uit te sluiten. In de praktijk blijkt de mens meestal de belangrijkste speler. Daarom moet het bewustzijn voortdurend worden aangescherpt, zodat kennis van risico's wordt verhoogd en het (veilig en verantwoord) gedrag wordt aangemoedigd. Onderdeel van het beleid zijn de regelmatig terugkerende bewustwordingscampagnes voor medewerkers, studenten en gasten. Zulke campagnes kunnen aansluiten bij landelijke campagnes in het MBO onderwijs, zo mogelijk in afstemming met beveiligingscampagnes voor ARBO, milieu en fysiek. Verplichte awareness training management en ICT medewerkers.
Speerpunten van het "awareness" beleid zijn:

- Generieke scholing voor alle medewerkers;
- Specifieke scholing voor management en ICT personeel;
- Campagnes op het gebied van informatiebeveiliging en privacy;
- Informatiebeveiliging en privacy onderdeel maken van de gesprekscyclus in het kader van HR beleid;
- Aanvullingen op de arbeidsvoorwaarden in goed overleg met de Medezeggenschap Raad (WOR);
- Transparante documenten die voor iedereen ter inzage zijn op de website van de onderwijsinstelling.

[7] Een vaak gemaakte kanttekening bij het informatiebeveiligingsbeleid is: het staat nu wel op papier maar wordt het ook toegepast?
De diepgang van het informatiebeveiligingsbeleid kent drie volgtijdelijke niveaus, te weten:

Opzet:	vaststellen dat er beheersmaatregelen aanwezig zijn die waarborgen dat er een continue, integere en exclusieve IT-dienstverlening omtrent de in scope zijnde diensten is. Tevens vaststellen in hoeverre deze beheersmaatregelen schriftelijk zijn vastgelegd.
Bestaan:	vaststellen dat de in beschreven beheersmaatregelen op het moment van onderzoek ook in de praktijk zijn geïmplementeerd.
Werking:	dagelijks toepassen van het informatiebeveiligingsbeleid door zowel de beheerders als door de overige medewerkers.



Voorgesteld document: Implementatievoorbeelden van kleine en grote instellingen.
Bron: *saMBO-ICT / Kennisnet*

Tip (Surfnet advertentie)

Je kunt gebruik maken van het onderstaande aanbod:

… Eén van de speerpunten van SURFnet is beveiliging. Per 1 januari 2015 is Cybersave Yourself daarom toegevoegd aan het dienstenpakket. Maak gebruik van de campagnematerialen uit de toolkit of geef een presentatie aan uw medewerkers. Of speel met uw medewerkers de security awareness game Smart Secure Yourself.

Nieuwe dienst Cybersave Yourself (CSY)

Wilt u uw medewerkers en studenten beter bewust maken van de gevaren op internet? Maak dan gebruik van Cybersave Yourself, de beveiligingscampagne voor het hoger onderwijs en onderzoek. SURFnet biedt onder andere een Edugroepen-toolkit met materialen die u kunt aanpassen aan de huisstijl van uw eigen instelling. Toegang krijgen?
Meld u aan via info@cybersaveyourself.nl. Meer informatie is te vinden op: www.surf.nl/cybersaveyourself

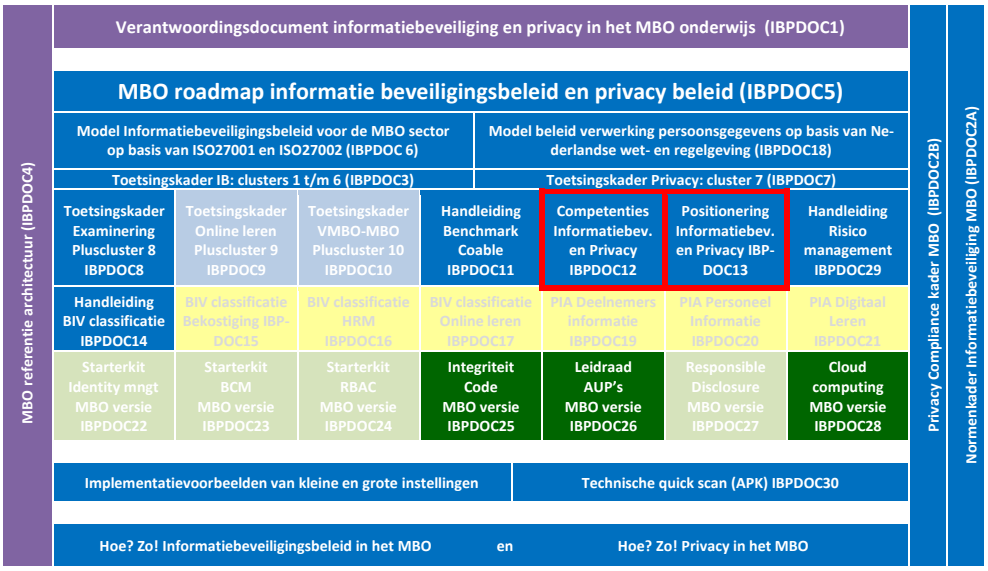
Smart Secure Yourself

Veilig omgaan met gevoelige informatie is actueler dan ooit. De security awareness game SmartSecureYourself leert uw medewerkers hoe ze dit goed kunnen doen. De game is binnen Cybersave Yourself ontwikkeld in samenwerking met de informatiebeveiligers van 8 onderwijsinstellingen.
Inloggen gebeurt via SURFconext. De game is verkrijgbaar via SURFmarket voor een periode van 1 tot 3 jaar. Alle prijsinformatie vindt u na inloggen op Mijn SURFmarket: http://ow.ly/Krhps …

5.5 IBP Organisatie

Het is belangrijk dat je vastlegt waar de verantwoordelijkheden ten aanzien van informatiebeveiliging liggen. Iemand van het management is eindverantwoordelijk. Aan die persoon moet ook worden gerapporteerd. Een IBP manager (jij wellicht) is verantwoordelijk voor de beleidsvoorbereiding en voor de uitvoering van het beleid. De IBP manager moet wel ondersteund worden door een bijvoorbeeld een Taskforce op de eigen MBO instelling. Door hier ook vertegenwoordigers van de gebruikersgroep in op te nemen wordt het draagvlak vergroot.

- Voorbeelden positionering, zie Positionering Informatie Beveiliging (IBPDOC13)
- Functiebeschrijving en functiewaardering IBP manager, zie Scholing Informatie Beveiliging (IBPDOC12)

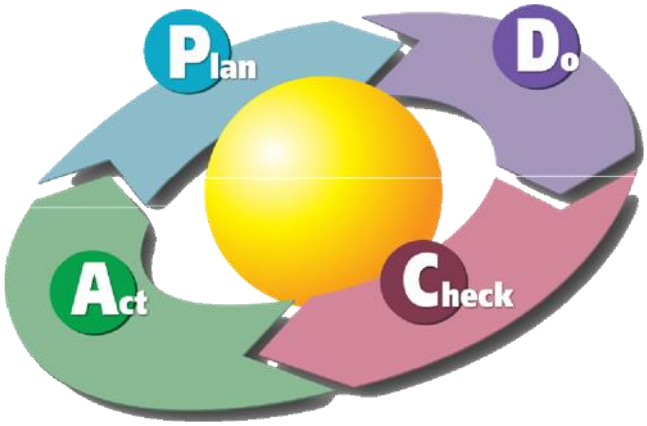


Voorgesteld document:
Competenties Informatiebeveiliging en Privacy (inclusief functiebeschrijving en –waardering) **(IBPDOC12)**
Positionering Informatiebeveiliging en Privacy **(IBPDOC13)**

Bron: *saMBO-ICT / Kennisnet*
.

5.5.1 Inrichten van de PDCA-cyclus[8]

Informatiebeveiliging is geen statisch geheel. Je hebt beleid gemaakt. Vervolgens wordt het beleid geïmplementeerd. Na implementatie wordt er gecontroleerd op naleving en wordt op basis van nieuwe inzichten of nieuwe risico's het beleid aangepast. Op die manier ontstaat een cyclus, ook wel de PDCA-cyclus van Deming genoemd waarbij PDCA staat voor Plan, Do, Check en Act. Schematisch ziet dit er als volgt uit:



Hoe je in de praktijk voor informatiebeveiliging en privacy zo'n cyclus inricht lijkt lastig, maar vermoedelijk bestaat iets dergelijks al voor de jaarlijkse budgetplanning. Nu je ook voor informatiebeveiliging en privacy kunt beschikken over een budget ligt het voor de hand daarbij aan te sluiten. Dat doe je ook met je voortgangsrapportages. Informatiebeveiliging en privacy wordt zo integraal onderdeel van de budgetcyclus en dat heeft als voordeel dat het onderwerp zichtbaar is en blijft.

5.5.2 Inrichten van het incidentmanagementproces

Een goed georganiseerd incidentbeheer, inclusief escalatieniveaus, helpt om erger te voorkomen. Een minimale invulling is het bijhouden van een incidentadministratie en te leren van wat er gebeurt. Richt dus een meldpunt in en communiceer dit met medewerkers en studenten.

Voor de incidentafhandeling kan een incident responseteam worden ingericht. Vergeet hierbij niet goed vast te leggen wie in voorkomende gevallen de communicatie op zich neemt. Bij calamiteiten waarbij bijvoorbeeld het imago van de instelling in het geding kan komen, is het verstandig om iemand van de communicatieafdeling verantwoordelijk te maken voor de communicatie met de pers.

Zorg daarnaast dat er periodiek in de rapportages gemeld wat voor soort incidenten zijn voorgekomen en hoe daarmee is omgesprongen.

[8] Advies opnemen, om dit onderdeel door Planning & Control te laten doen. De onderdelen uit de cyclus zijn de verantwoordelijkheid van IB en kunnen aan P&C aangeleverd worden

Een gedegen aanpak gaat uit van preventie, detectie en respons.

Preventie

Preventie begint met governance en organisatie. Het gaat naast technische maatregelen onder andere om het beleggen van de verantwoordelijkheid voor cybercrime in de organisatie en om bewustwordingstrainingen voor belangrijke medewerkers.

Detectie

Een organisatie kan door het monitoren van kritieke gebeurtenissen en centrale veiligheidsincidenten en -gebeurtenissen de technologische detectiemaatregelen versterken. Monitoring en data mining vormen samen een uitstekend instrument om vreemde patronen in het gegevensverkeer op het spoor te komen, te signaleren waar de aanvallen zich concentreren en de systeemprestaties te observeren.

Respons

Bij respons gaat het om het in werking stellen van een plan zodra zich een aanval voordoet. Bij een aanval moet de organisatie alle getroffen technologie direct buiten werking kunnen stellen. Bij de ontwikkeling van een respons- en herstelplan doet een organisatie er goed aan (informatie)beveiliging te zien als een continu proces en niet als eenmalige oplossing.

	Preventie	Detectie	Respons
Beheer en Organisatie	Toewijzen van verantwoordelijkheden voor Cybercrime Verzorgen van training beveiligingsbewustzijn	Borgen van 24 x 7 stand-by crisis organisaties	Inzetten van forensische analyse vaardigheden
Processen	Uitvoeren cybercrime respons test (simulatie) Uitvoeren periodieke scans en penetratietesten	Uitvoeren procedures voor opvolging van incidenten	Uitvoeren cybercrime respons plan
Technologie	Realiseren van adequate Desktopbeveiliging Realiseren van netwerksegmentatie	Implementeren logging van kritieke processen Implementeren centraal monitoren van beveiligingsincidenten	Stoppen of verbreken van aangevallen IT-diensten

5.6 Product stap 5: Verbeterplan

In je verbeterplan heb je een aantal zaken gedaan, te weten:

- De uitvoer van een risico (en uitdagingen) analyse;
- De uitvoer van een (globale) audit;
- Een eerste aanzet voor algemeen beleid;
- Een opzet voor een awareness campagne;
- Een voorstel voor de inrichting van een IBP organisatie;
- Een voorstel voor de inrichting van een incidentenmanagement proces.