Dit document wordt herschreven.
De nieuwe versie is vóór 1 juli 2015 beschikbaar.

Verantwoordingsdocument Informatiebeveiliging (IB) en Privacy in het MBO

IBBDOC1

saMBO-ICT
Kennisnet
TASKFORCE MBO INFORMATIEBEVEILIGING

Inhoudsopgave

1. Inleiding

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 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.

1.1 Aanleiding

Het zal duidelijk zijn dat het thema Informatiebeveiliging en zeker ook Privacy 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 examens in de publiciteit gekomen. 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 imagoschade voorop staat. Het onderwijs wordt geacht op betrouwbare wijze diploma's uit te reiken 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.
Daarom is het in het belang van zowel het onderwijs zelf als van het ministerie van OC&W dat er gemeenschappelijke afsprakenkaders komen, dat die met alle onderwijsinstellingen en ook met de relevante externe partijen worden gedeeld en geïmplementeerd. Pas dan kan er een beeld ontstaan van hoe scholen het doen op deze terreinen en kunnen er verbeteringstrajecten worden ingezet en doelen gesteld worden om een bepaalde graad van beveiliging en bescherming te creëren. In het hoger onderwijs is dit traject al eerder ingezet.
Dit alles heeft er toe geleid dat het ministerie van OC&W de vraag bij de mbo sector heeft neergelegd om een beeld van de stand van zaken in het mbo met betrekking tot informatiebeveiliging en privacy te maken en er voor te zorgen dat er naar een gewenste situatie kan worden toegewerkt. De sector heeft deze uitdaging opgepakt en wil met dit programma de stappen zetten om in het mbo op een volwassen wijze met deze problematiek om te gaan en een acceptabel niveau van beveiliging en bescherming te bieden aan al haar studenten en medewerkers.

1.2 Aanpak

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[1] vanuit saMBO-ICT heeft de aanzet gegeven voor het IB 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.

1.3 Hoe? Zo! publicatie

En er is een zogenaamde Hoe? Zo! publicatie gemaakt door saMBO-ICT en Kennisnet waarin alle aspecten van het IBB aan de orde komen en die vervolgens worden weergegeven in een vraag en antwoord opzet vanuit het perspectief van de bestuurder of onderwijsmanager. Op deze wijze zijn in eerste instantie zoveel mogelijk elementen al op een rij gezet, waarmee deze publicatie als een basis voor eenieder kan dienen. [2]

[1] Projectplan IB – saMBO-ICT, mei 2014, vs 1.0
[2] Hoe? Zo! Informatiebeveiligingsbeleid in het mbo

2. Stakeholders

Binnen het programma is een aantal stakeholders benoemd. Het is van belang om die eerst goed op een rij te zetten zodat de reikwijdte van het programma ook helder wordt.

2.1 MBO instellingen

Als eerste moeten daarbij de mbo instellingen zelf genoemd worden, verenigd in en vertegenwoordigd door de MBO Raad. Het is van belang dat de scholen hun verantwoordelijkheid (kunnen) nemen in deze complexe materie van informatiebeveiliging en privacy en dat zij daar op maatschappelijk verantwoorde wijze mee om weten te gaan. De MBO Raad vertegenwoordigt diverse College van Besturen en hier ligt dan ook de uiteindelijke verantwoordelijkheid van het project. Daarom is van het belang dat het programma bestuurlijk sterk wordt gedragen en dat bestuurders zich bewust zijn van essentie en strekking daarvan. Daar begint het mee.

2.2 Ministerie van OC&W

Ten tweede moet genoemd worden het Ministerie van OCW. Vertegenwoordigers van het Ministerie hebben in een bijeenkomst met het onderwijsveld, in juni 2014, hun zorgen kenbaar gemaakt ten aanzien van informatiebeveiliging (b.v. examens liggen op straat). Zij geven ook aan behoefte te hebben aan meer inzicht in hoe de onderwijs sector er voor staat t.a.v. informatiebeveiliging, dat beeld ontbreekt grotendeels. Het ministerie heeft aangegeven graag te zien dat de mbo-sector dat beeld helder gaat weergeven en dat de sector maatregelen treft om de informatiebeveiliging en bescherming van de privacy te verbeteren. Op grond van afspraken zou de Onderwijsinspectie dan ook in staat moeten zijn om controle uit te oefenen. Het ministerie heeft de sector een jaar de tijd gegeven om een en ander op orde te brengen. Dit programma is daar het vehikel voor.

2.3 Externe partijen

Dan zijn er de externe partijen die hierbij een rol spelen. Deze zijn onder te verdelen in de volgende groepen:

- Ondersteunende organisaties voor de sector
- Toezicht (bv. accountants)
- Systeemleveranciers
- Adviseurs en consultancy

Allereerst zijn dat de organisaties Kennisnet en SURF die de mbo sector direct ondersteunen. Zij zijn als zodanig ook op het terrein van informatiebeveiliging en privacy met name aangesproken om hun expertise beschikbaar te stellen om dit programma inhoudelijk te voeden om zodoende te komen tot realisatie van de doelstellingen. Vervolgens mag verwacht worden dat in de komende jaren er een steeds grotere rol is weggelegd voor informatiebeveiliging bij de goedkeurende verklaring bij de jaarrekeningen van de instellingen. Dat betekent dat de externe accountants steeds vaker hier vragen over zullen stellen en dat de behoefte aan standaardisatie en normering groot zal zijn. Ook zullen instellingen met name met hun (software) leveranciers (b.v. van elo's, educatieve software, registratiesystemen) goede afspraken moeten maken over de beveiliging van deze systemen en daarvan afgeleid de verwerking van de persoonsgebonden gegevens. De leveranciers moeten in het kader van de huidige wetgeving al aan een set van criteria voldoen en zullen ook behoefte hebben om hier heldere, breed geaccepteerde kaders voor te kunnen hanteren. Tenslotte hebben instellingen soms behoefte aan ondersteuning door externe bureaus bij de implementatie van beleid of bij het beoordelen van hun situatie op het gebied van informatiebeveiliging. Ook vanuit deze partijen is er behoefte aan duidelijke kaders.

2.4 Maatschappij

Tot slot moet is er het maatschappelijk veld. Leerlingen, studenten, ouders, maar ook medewerkers moeten en mogen er vanuit gaan dat scholen op een veilige manier met hun gegevens omgaan, dat hun privacy wordt gewaarborgd en dat de resultaten van alle inspanningen ook rechtvaardig en correct worden gewaardeerd met certificaten of diploma's met een maatschappelijke waarde die niet ter discussie staat. Zodat een school, met een trots en opgeheven hoofd, een waardige diploma uitreiking kan organiseren. Een en ander wordt gewaarborgd in de Nederlandse en Europese wet- en regelgeving (compliance), die dan ook strikt moet worden toegepast en gecontroleerd op de uitvoer.

3. Van normenkader naar toetsingskader mbo

Als je de vraag wilt beantwoorden of je de informatiebeveiliging goed op orde hebt, dan kan dat alleen als je ook afgesproken hebt wat op orde is en wat niet. Er moet sprake zijn van een norm of een normenkader.

3.1 Vastgesteld normenkader

Daarom moet het veld een normenkader (**Waar wil of moet ik aan voldoen?**) gaan hanteren en dit ook met de externe stakeholders afstemmen. Het heeft ook geen zin om binnen de scholen te werken met een norm om vervolgens getoetst te gaan worden aan een andere norm. Belangrijk is dat de norm aansluit bij andere gekozen standaarden en vooral ook voldoet aan internationale normen. Daarom heeft de taskforce besloten om het normenkader ISO 27001 en 27002 te gaan hanteren. Internationaal is dit een zeer breed gehanteerd normenkader (ook nog eens specifiek voor het mbo bevestigd door de Gartner Group) en daarnaast is het vooral van belang dat het Hoger Onderwijs ook voor dit normenkader heeft gekozen. ISO 207001 is normatief van opzet en beschrijft het normenkader sec, hierin staan de harde eisen, waaraan je als organisatie moet voldoen om gecertificeerd te kunnen worden. De eisen worden beschreven op het niveau van maatregelen welke de organisatie moet treffen in relatie tot de beveiligingsrisico's die je loopt. Wat die maatregelen inhouden, wordt daarin niet uitgewerkt. Daar is ISO 27002 voor, dat is niet-normatief van opzet en bevat best practices voor de implementatie van informatiebeveiliging. Voorgeschreven is alleen het proces via welk de norm tot stand komt: een risicoanalyse, het afspreken van de norm met alle betrokkenen en de instemming van het management.
Tezamen wordt dit ook de Code voor Informatiebeveiliging genoemd.

3.2 Van normenkader naar toetsingskader

Het normenkader dat de taskforce gebruikt is afgeleid het Hoger Onderwijs toetsingskader dan ook gebaseerd is op de ISO27000 normen, het zogenaamde "HO normenkader". [3]

Dit HO normenkader groepeert de items in een zestal clusters::

1. beleid en organisatie;
2. personeel en studenten;
3. ruimten en apparatuur;
4. continuïteit;
5. toegangsbeveiliging en integriteit
6. controle en logging.

Daarbij is een selectie gemaakt van voor het onderwijs relevante normen (een selectie van 83 normen uit de gehele set van 146 normen). Daarbij worden vervolgens ook de maatregelen beschreven om deze norm te bereiken (en **aan te tonen**) en dit gebeurt in de vorm van een 5 puntenschaal, de zogenaamde Maturity levels. Met die maatregelen wordt die norm dus op een steeds hoger niveau gerealiseerd. Het normenkader wordt hiermee toetsbaar met andere woorden het normenkader wordt een toetsingskader .
Belangrijk onderdeel bij het hanteren van deze systematiek is dat er naast het afspreken van de normen ook bepaald wordt welk maturity level nagestreefd wordt. Zo is niveau 1 altijd haalbaar maar biedt weinig garantie dat het betreffende risico dat in de norm beschreven staat ook afgedekt wordt. Niveau 5 is het hoogst haalbare maar is vaak niet realistisch. En voor een startende instelling is streefniveau 2 al een hele opgave en 3 een forse uitdaging. In de afspraken wordt meestal aangegeven wat het minimum niveau moet zijn en wat het streefniveau is.

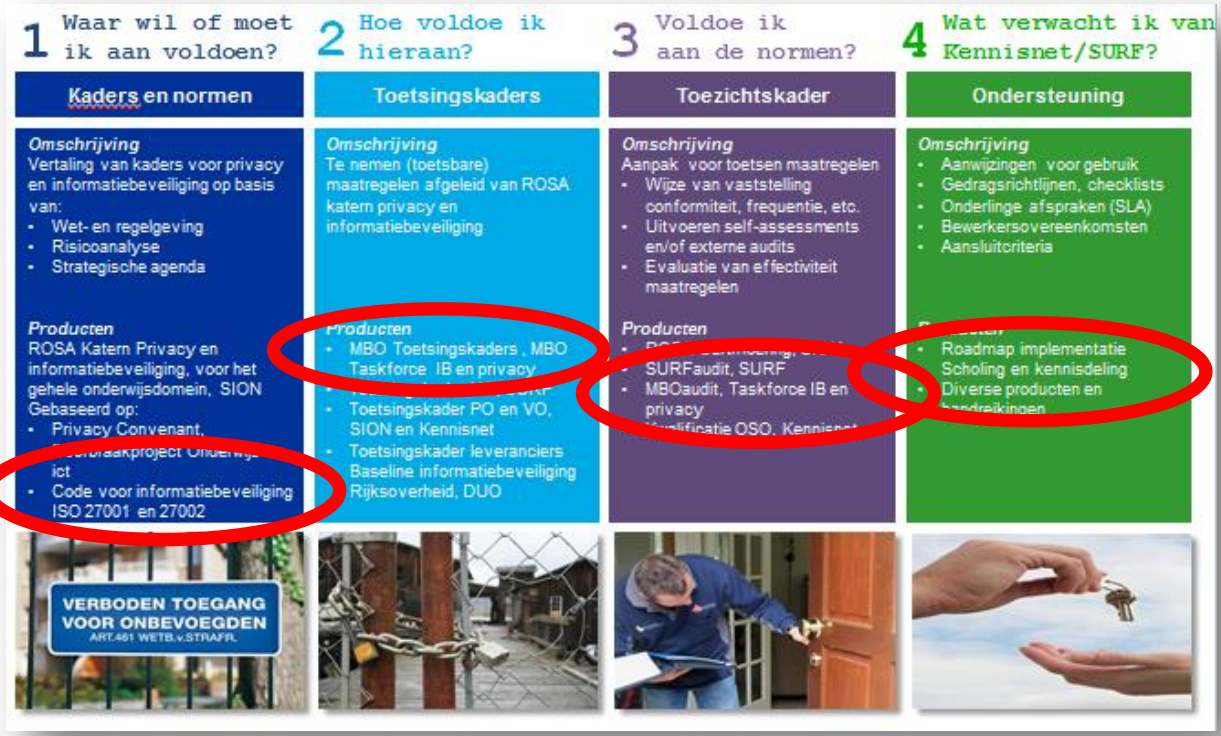
3.3 Aanpak MBO sector

Op deze manier ontstaat een geheel dat we het IB toetsingskader noemen en omdat dit voor het mbo specifiek gemaakt is vanuit het HO model noemen we dit ook het IB toetsingskader mbo. Dit toetsingskader mbo is on-

[3] normenkader Hoger Onderwijs, SURF december 2010

derdeel van overleg met de sector mbo en met het ministerie van OCW. Uiteindelijk moeten dit toetsingskader mbo en te hanteren volwassenheid niveaus (minimum- en streefniveau) gezamenlijk worden vastgesteld.
Daarmee vormt dit toetsingskader het hart van het IB programma. Zetten we de belangrijkste elementen op een rij dan begint het met de normen of normenkaders, aangevuld met eventuele wet- en regelgeving. Van daaruit wordt dus het toetsingskader ontwikkeld, waarin aangegeven welke maatregelen en tot welk niveau je kan nemen om de informatiebeveiliging en de bescherming van de privacy op orde te brengen. Daarna ga je ook daadwerkelijk toetsen of meten of je aan de normen voldoet en de benodigde maatregelen ook daadwerkelijk genomen hebt (de assessments). In een overzichtelijk schema hieronder is deze samenhang weergegeven en is ook aangegeven wat je van externe partijen kunt verwachten op dit gebied, met name van de in het programma samenwerkende partijen saMBO-ICT, Kennisnet en SURF. Dit schema is in samenwerking met de ROSA kerngroep ontwikkeld. ROSA staat voor Referentie Onderwijssector Architectuur en dit platform houdt zich bezig om voor de gehele onderwijssector de architectuur en de kaders voor informatiebeveiliging en privacy te bundelen en te borgen.

3.4 Schematisch weergegeven



4. Assessments en audits

Beheersing en ontwikkeling van informatiebeveiliging kan binnen de MBO sector, in navolging van het hoger onderwijs, opgezet worden als een iteratief proces. Daarbij wordt gebruik gemaakt van de 4 fasen van de Deming cirkel (plan-do-check-act). Concreet worden er voor informatiebeveiliging de volgende fasen onderscheiden:

Fase 1 (plan): Uitvoeren **MBO roadmap informatie beveiligingsbeleid (IBBDOC5)**.
Voorwaarde voor fase 1: brede betrokkenheid binnen instellingen: College van Bestuur, ict management, kwaliteitszorg, juristen en kwartiermaker IB.

Fase 2 (do): Inrichting **Model Informatiebeveiligingsbeleid voor de MBO sector (IBBDOC 6).**
Voorwaarde voor fase 2: actieve betrokkenheid van instellingen via communities, werkgroepen en gezamenlijke projecten (saMBO-ICT en Kennisnet)
Aanvullend actiepunt: tijdige voorbereiding op veranderen regelgeving, zoals Europese Privacy Verordening en Meldplicht datalekken

Fase 3 (check): Toetsing normenkader met een self assessment, peer-audit, externe audit of benchmark op basis van:

- **Normenkader Informatie Beveiliging MBO (IBBDOC2)**;
- **Toetsingskader Informatie Beveiliging MBO (IBBDOC3)**, ook wel Quick scan genoemd (ook digitaal beschikbaar);
- **Aanvullende toetsingskaders Examinering (IBBDOC7) en Privacy (IBBDOC8)**.

Voorwaarde voor fase 3: aanpak afgestemd met MBO Raad, Ministerie van OC&W, externe accountants, externe leveranciers en examencommissies.

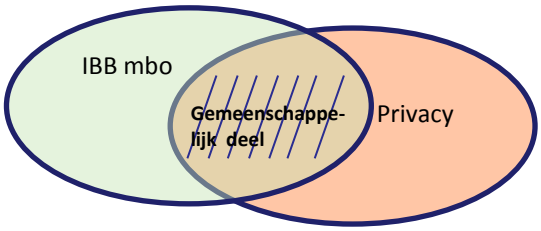
Self-assessment
Voor een instelling is het self assessment een nulmeting met betrekking tot informatiebeveiliging in de eigen instelling. Daarbij is het niet noodzakelijk om ook echt, met procedures en protocollen, aan te tonen dat men het niveau behaald is dat wordt beoogd. Bovengenoemde quick scan biedt hier een hulpmiddel toe.
Peer audit
In een peer audit beoordelen instellingen elkaar met betrekking tot het niveau. Er worden peer-kringen ingericht waarbij instelling A door instelling B wordt beoordeeld, vervolgens zal B weer door C worden beoordeeld, enz. De beoordelingen worden in de tool ingevuld, zodat een meer getrouw beeld van de sector ontstaat. Deze kringen zorgen voor een bewustwording bij de beoordeelde en bij de assessor. Het is dus niet alleen een beoordeling, maar is ook onderdeel van het leerproces binnen de mbo sector.
Externe audit
Het is de bedoeling om, net als in het hoger onderwijs, het peer -audit af te wisselen met externe audits. Dat betekent dat aan een externe partij wordt gevraagd om een audit uit te voeren. Om dit te reguleren en te zorgen dat deze audits op vergelijkbare manier plaatsvinden zal een gezamenlijke aanbesteding plaatsvinden voor de instellingen in het mbo. Daarnaast kan het ook een voordeel opleveren in de kosten voor de instellingen zelf.
Benchmark
Het meten van de situatie binnen een instelling op basis van vastgestelde toetsingskader is belangrijk voor de instelling om te weten naar welke onderwerpen vooral aandacht uit moet gaan. Met behulp van een bestaande tool (quick scan) kan de instelling aan het toetsingskader worden afgemeten. De tool maakt het mogelijk om de eigen situatie af te zetten tegen het gemiddelde in de mbo-sector. Het zal een duidelijk beeld geven voor de instelling zelf, maar bij voldoende deelname ook voor de sector als geheel. Daarmee is het een eerste benchmark voor de mbo-sector (nulmeting).

Fase 4 (act): (jaarlijkse) verbeterplannen
Voorwaarde voor fase 4: normenkader afgestemd met instellingen, interne auditors, aansluiting WBP, externe auditors

5. Privacy

5.1 Positionering

Privacy is zeker niet hetzelfde als informatiebeveiliging. Wel is er een zekere overlap. Deze overlap is reden om de vraag te stellen in hoeverre het van belang of nuttig zou kunnen zijn om deze twee binnen één programma te bundelen. Gezien de dynamiek en het draagvlak van de taskforce IB, de benodigde capaciteit om dergelijke programma's uit te voeren en het gegeven dat het grotendeels gaat om dezelfde organisaties en experts is besloten om de thematieken binnen het programma te bundelen.



IB wordt vaak gericht vanuit de kant van de bedrijfsprocessen, met de bedrijfscontinuïteit als belangrijke driver. De privacy komt vaak vanuit de maatschappelijke richting en de wetgeving.

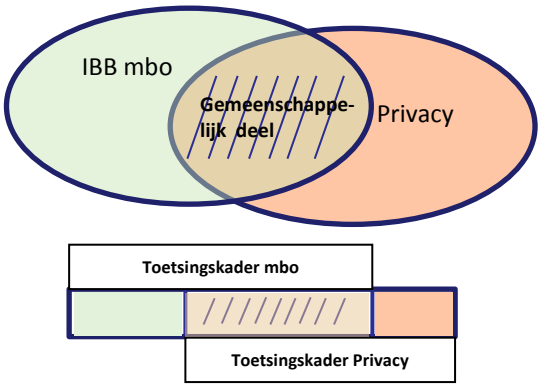
Vanuit de privacy komen de volgende aspecten op die in het programma moeten worden uitgewerkt:

- architectuur en ontwerp, welke gegevens worden verwerkt;
- inventaris op orde, waar is wat, en waarom;
- processen en procedures, inzagerechten op orde;
- passende beveiliging van persoonsgegevens toepassen (met name een IB aspect);
- bewustwording alle studenten en medewerkers (geldt voor beide thema's).

Uit al deze aspecten blijkt hoezeer de onderwerpen verweven zijn. Je zou grofweg kunnen zeggen dat vanuit privacy wordt aangegeven waarom en vanuit IB het hoe.

5.2 Activiteiten privacy

- Er is op drie vlakken noodzaak tot actie: privacy beleid, relateren aan een normenkader, waar mogelijk ook aan het toetsingskader mbo
- volgen van de regelgeving, met name van de EC, noodzaak van een privacy officer
- kennisniveau en draagvlak verhogen.



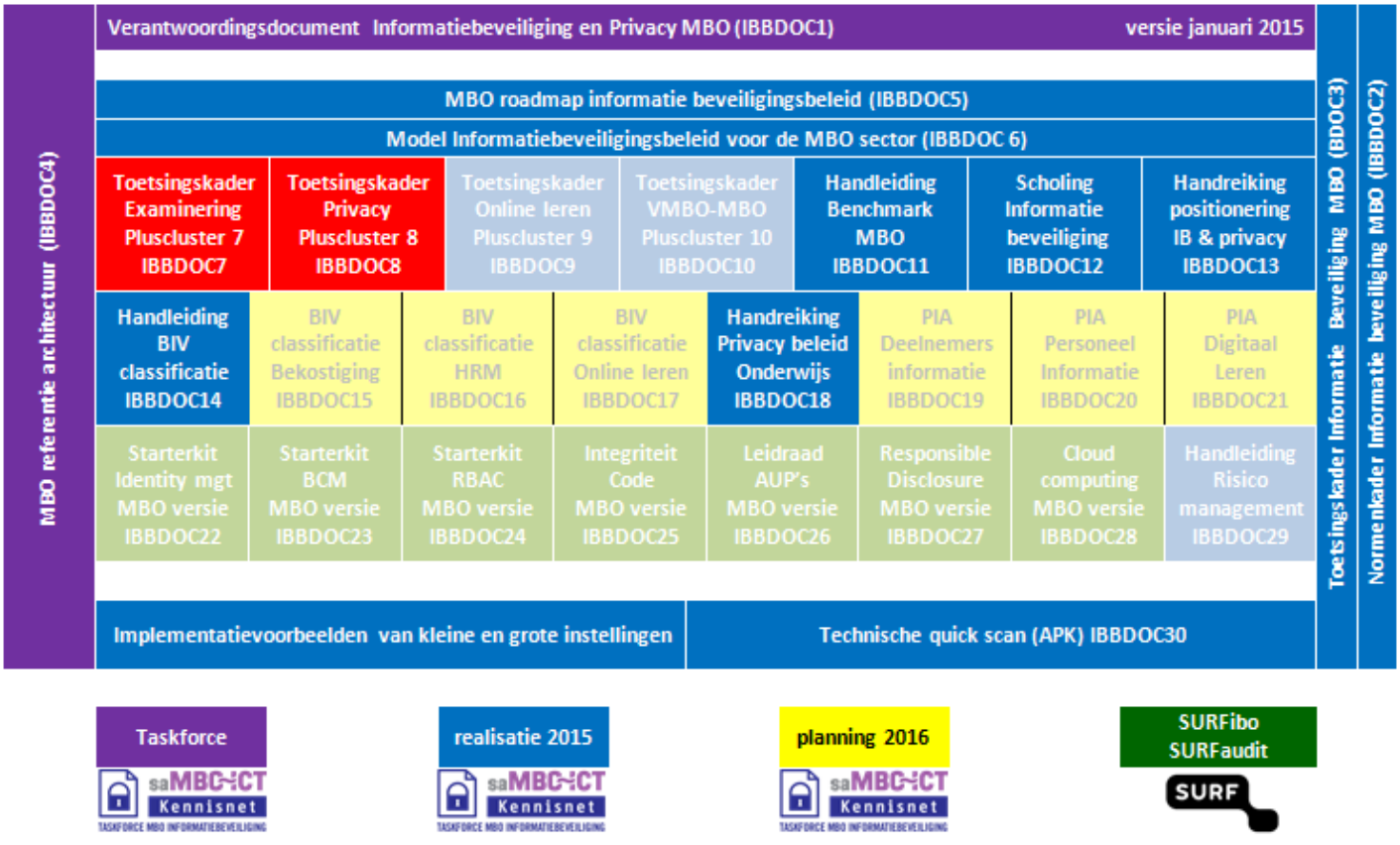
Ook die onderwerpen lopen direct parallel aan het IB programma.

Doel van het programma is de ontwikkeling van een toetsingskader voor de Privacy (**Toetsingskader Privacy Pluscluster8, IBBDOC8**), zoals dat ook kan gelden voor andere specifieke onderwerpen die we vanuit IB extra willen belichten, bijv Examinering of Online leren. Feitelijk zijn dit doorsneden van het algemene toetsingskader mbo, maar dan specifiek gericht op een apart thema en waar nodig voorzien van aanvullingen uit andere kaders zoals wetgeving, sectoraal- of instellingsbeleid en maatschappelijke ontwikkelingen.

6. Samenhang en Productschema IB programma mbo

Zoals reeds aangegeven is het belangrijk om in te zien wat de samenhang van de verschillende elementen in het programma is. Allereerst is er de lijn waarlangs het denken over informatiebeveiliging loopt. Het begint met de normen of normenkaders (IBBDOC2). Vanuit wet- en regelgeving en de keuze voor een standaard normering worden deze kaders aangegeven en bieden als zodanig het uitgangspunt voor verder handelen. Denk hierbij aan de ISO norm 27001/2, wet en regelgeving vanuit overheden en Europa, het ROSA katern waarin het onderwijsveld haar uitgangspunten verder gedefinieerd heeft. Tweede stap is vervolgens de vertaling naar een toetsingskader (IBBDOC3), welke maatregelen en tot welk niveau ga je nemen om de beveiliging en bescherming van de privacy op orde te brengen. Hierbij hanteren we in het mbo dus het IB toetsingskader mbo. de volgende stap is dan om te toetsen of je ook aan die maatregelen voldoet, je gaat meten aan de hand van het toetsingskader (assessment) en daarmee kan je laten zien of voldoet aan de afspraken (niveau) of niet. Bij dit alles hoef je als school niet zelf het wiel uit te vinden maar zijn er vele handreikingen en tools die daarbij ondersteunen. In een overzichtelijk plaatje zijn deze kernstappen weergegeven, dit wordt intussen in alle gremia rond IB in het mbo gebruikt.

Daarnaast heeft de taskforce IB heeft een compleet framework opgesteld waarin is weergegeven welke elementen in het informatiebeveiligingsbeleid en bij privacy allemaal 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 direct worden benut. Deze zijn door de groep security officers/beveiligingsexperts in het HO, verenigd in het SURFibo (SURF informatie beveiliging officers) ontwikkeld en worden daarin ook onderhouden. Deze documenten zijn door de werkgroepen van het IB programma wel van een vertaling naar de setting van het mbo voorzien. De documenten (IBBDOC) zijn helder in het onderstaande overzicht weergegeven. De verantwoordelijk Informatie Beveiliging medewerkers krijgen ook de beschikking over allerlei waardevolle documenten die zij kunnen inzetten om het beleid uit te voeren (vaag gearceerde cellen).



7. Samenwerking en afstemming in het mbo

Zoals aangegeven is de aanzet vanuit saMBO-ICT om tot een taskforce IB te komen de eerste stap tot samenwerking in het mbo veld geweest. Er is vanuit het mbo veld enthousiast gereageerd middels:

- Een grote belangstelling bij de eerste presentatie op de saMBO-ICT conferentie in september 2014;
- Een forse aanmelding van vele (deskundige) betrokkenen uit de instellingen voor de taskforce en de werkgroepen;
- Veel interesse voor de publicatie Hoe? Zo! Informatiebeveiligingsbeleid in het mbo;
- Een grote belangstelling voor de opgezette scholing.

Vanuit het programma IB wordt vervolgens sterk geëntameerd dat die samenwerking wordt gecontinueerd en dat daar ook consequenties uit worden getrokken.

Allereerst is het van belang dat het veld de gemaakte keuzes voor standaarden, het toetsingskader mbo, de voorgestelde methodieken voor assessments en inhoudelijke handreikingen ook omarmt en gaat gebruiken/toepassen. En dat het veld daarbij als één geheel in de afstemming met het ministerie van OCW optreedt en tot goede afspraken over ambities en te bereiken resultaten komt. Dat helpt de individuele instellingen enorm en geeft duidelijkheid naar de overheid toe. Het biedt ook de kans om met een benchmark de stand van zaken in het veld adequaat weer te geven.

De vervolgstap is dat ook naar de andere externe partijen deze kaders worden gehanteerd zodat er sprake is van eenheid, bundeling van kennis en expertise en eenduidige afsprakenkader met bijvoorbeeld leveranciers. Daarbij moet gedacht worden aan softwareleveranciers en leveranciers van clouddiensten en -producten, uitgeverijen en dergelijke. Iedereen is gebaat bij een eenduidige afspraken kader met al deze partijen.

Ook is verdere samenwerking in de gehele onderwijsketen van belang. Hierbij kunnen belangrijke voordelen gehaald worden door het delen van kennis, het benutten van elkaars producten en expertise, het eenduidig opereren naar de markt enz. enz.

Tot slot moet als belangrijke mogelijkheid om effectief en efficiënt in deze te opereren de samenwerking op het gebied van scholing, kennisontwikkeling en kennisdeling genoemd worden. Een overzicht laat alle scholingsmogelijkheden zien en van daaruit kunnen initiatieven worden ontplooid om naast de reeds geïntroduceerde masterclasses meer initiële opleidingen en vervolgscholing te ontwikkelen en te volgen.
Ook uitwisseling van kennis en ervaringen tussen instellingen is van groot belang. Een IB & Privacy community kan hierin faciliteren, waarbij naast virtuele uitwisseling op een community platform ook een IB & Privacy Conferentie voor het mbo veld een belangrijke rol speelt.

Het is goed om tot slot te vermelden dat zonder de samenwerking met het hoger onderwijs het mbo nooit dit programma zo voortvarend had kunnen oppakken en uitvoeren. In het programma is de meerwaarde van samenwerking in de onderwijsketen al als zeer productief en nuttig ervaren.

Verantwoording

Auteurs

Hans Doffegnies (voorzitter Taskforce MBO Informatiebeveiliging)
Leo Bakker (Kennisnet)
Jan Bartling (saMBO-ICT)
Ludo Cuijpers (Leeuwenborgh)

Januari 2015

Overzicht documenten en publicaties Taskforce IB

nummer	omschrijving	realisatie
IBBDOC1	**Verantwoordingsdocument IB en Privacy in het MBO**	**Q1-2015**
IBBDOC2	Normenkader Informatie beveiliging MBO / MBO audit	Q1-2015
IBBDOC3	Toetsingskader Informatie Beveiliging	Q1-2015
IBBDOC4	MBO referentie architectuur	
IBBDOC5	MBO roadmap informatie beveiligingsbeleid	Q2-2015
IBBDOC6	Model Informatiebeveiligingsbeleid voor de MBO sector op basis van ISO27001 en ISO27002	Q2-2015
IBBDOC7	Toetsingskader Examinering Pluscluster 7	Q1-2015
IBBDOC8	Toetsingskader Privacy Pluscluster 8	Q2-2015
IBBDOC9	Toetsingskader Online leren Pluscluster 9	Q4-2015
IBBDOC10	Toetsingskader VMBO-MBO Pluscluster 10	Q4-2015
IBBDOC11	Handleiding Benchmark Coable	Q2-2015
IBBDOC12	Scholing Informatie beveiliging	Q1-2015
IBBDOC13	Positionering Informatie management	Q2-2015
IBBDOC14	Handleiding BIV classificatie	Q1-2015
IBBDOC18	Handreiking Privacy beleid Onderwijs	Q1-2015
IBBDOC29	Handleiding Risico management	Q2-2015
IBBDOC30	Technische quick scan (APK) en SURF producten	Q2-2015

Voor een eventueel vervolgprogramma IB voor het mbo zouden de volgende documenten bij het opstellen daarvan moeten worden opgenomen:

IBBDOC15	BIV classificatie Bekostiging	Planning 2016
IBBDOC16	BIV classificatie HRM	Planning 2016
IBBDOC17	BIV classificatie Online leren	Planning 2016
IBBDOC19	PIA Deelnemers informatie	Planning 2016
IBBDOC20	PIA Personeel Informatie	Planning 2016
IBBDOC21	PIA Digitaal Leren	Planning 2016
IBBDOC22	Starterkit Identity mngt MBO versie	MBO ombouw 2016
IBBDOC23	Starterkit BCM MBO versie	MBO ombouw 2016
IBBDOC24	Starterkit RBAC MBO versie	MBO ombouw 2016
IBBDOC25	Integriteit Code MBO versie	MBO ombouw 2016
IBBDOC26	Leidraad AUP's MBO versie	MBO ombouw 2016
IBBDOC27	Responsible Disclosure MBO versie	MBO ombouw 2016
IBBDOC28	Cloud computing MBO versie	MBO ombouw 2016