Verantwoordingsdocument informatiebeveiliging en privacy (ibp) in het mbo.

IBPDOC1

Auteurs

Leo Bakker (Kennisnet)
Ludo Cuijpers (Leeuwenborgh Opleidingen)

Versie 2.1 juli 2016

Sommige rechten voorbehouden

Inhoudsopgave

1. Inleiding

Informatiebeveiliging en privacy (ibp) is een onderwerp dat in korte tijd hoog op de agenda van het mbo onderwijs is komen te staan. In het onderwijs worden steeds meer gegevens bijgehouden en de mbo sector is zich er van bewust dat het van groot belang is om op een goede en veilige manier met de verkregen informatie om te gaan. Dit geldt zeker ook voor alle persoonsgegevens die de instelling beheert. Deelnemers en medewerkers mogen er van uitgaan dat de mbo instelling hun gegevens correct behandelen en het geschonken vertrouwen hierbij niet beschaamd wordt. Daarnaast is het van groot belang dat de primaire rol van het mbo onderwijs, namelijk het geven van goed onderwijs en het daarbij behorende diplomeren van haar deelnemers, op een betrouwbare en correcte wijze gebeurt. Diploma's zijn maatschappelijk van grote waarde en mogen nooit ter discussie komen te staan.
De centrale thema's (kwaliteitscriteria) rondom Informatiebeveiliging en privacy zijn beschikbaarheid, integriteit en vertrouwelijkheid van gegevens. Daar zijn beheersmaatregelen voor nodig om er voor te zorgen dat alleen geautoriseerde medewerkers vertrouwelijke informatie kunnen raadplegen of om te borgen dat systemen die essentieel zijn voor het onderwijs voldoende beschikbaar zijn en dat de informatie altijd juist, volledig en tijdig is. Informatiebeveiligingsbeleid richt zich op al deze aspecten. Daarbij is informatiebeveiliging niet alleen een kwestie van technologie, maar vooral ook van processen en gedrag.

Het thema privacy is integraal opgenomen in het programma ibp in het mbo. Reden daarvoor is de grote overlap tussen informatiebeveiliging en privacy. Zonder ib geen privacy en andersom. Steeds vaker zijn hier ook externe partijen en leveranciers bij betrokken en zonder goede afspraken kan de privacy niet geborgd worden. Zeker bij jonge kinderen wordt dit door de maatschappij als onacceptabel beoordeeld. ok voor het ministerie van OCW is het van belang dat informatiebeveiliging en privacy in het onderwijs goed geregeld is. Tot voor kort was de aanpak daarbij nog zeer beperkt en gebrekkig. Er waren afspraken kaders nodig om de te nemen maatregelen te relateren aan normen en compliance kaders en om uiteindelijk ook te kunnen beoordelen in welke mate aan die normen en kaders voldaan wordt. Het programma ibp in het mbo dat hierop een antwoord moest vinden is gestart in september 2014 en heeft haar resultaten in december 2015 opgeleverd. Dit document geeft de verantwoording weer van dat programma en een kort overzicht van de resultaten en de verdere stappen die genomen zijn om ibp in het mbo succesvol verder te implementeren. De bijgaande publicatie in de vorm van de box "Ibp in het mbo" bevat alle relevante documenten, normen en kaders, handreikingen en informatie die voor ibp in het mbo van belang is.

1.1 Aanpak

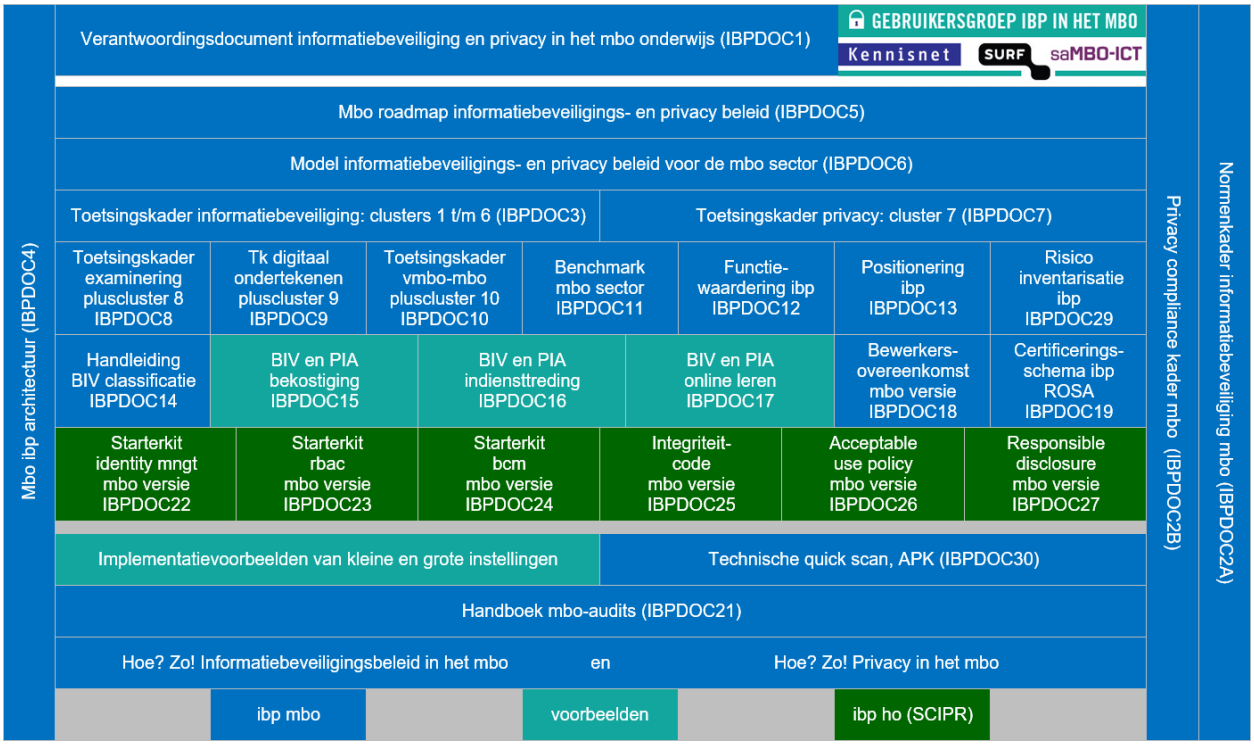
De mbo sector is zich zeer bewust van de urgentie en belang van informatiebeveiliging en privacy beleid en vrijwel alle scholen zijn er intussen concreet mee aan de slag gegaan of hebben plannen op stapel staan. In een brede samenwerking tussen het mbo-onderwijsveld, saMBO-ICT, MBO Raad, Kennisnet en SURF is de afgelopen twee jaar onder leiding van een Taskforce een programma informatiebeveiliging en privacy (ibp) ontwikkeld en tot uitvoer gebracht om als sector een adequaat antwoord op de uitdagingen te geven en de scholen te voorzien van de werkbare normenkaders, handreikingen en tooling om de problematiek op een goede wijze aan te pakken. Het resultaat is samengevat in het zogenaamde "Framework informatiebeveiliging en privacy in het mbo" dat hieronder is weergegeven> Deze complete set aan materialen moet de ibp functionaris van de mbo instelling in staat stellen om op een deels gestandaardiseerde en daarmee vergelijkbare wijze ibp in de instelling te implementeren en objectief te beoordelen. Tevens heeft het framework en de objectieve beoordeling geleid tot een benchmark waarvan de eerste resultaten zijn opgenomen waardoor een goed beeld kan worden gegeven hoe de sector mbo presteert op het terrein van ibp binnen de gestelde kaders.

1.2 Hoe? Zo! publicaties

In de aanloop van het programma ibp in het mbo zijn twee zogenaamde "Hoe? Zo!" publicaties gemaakt door saMBO-ICT en Kennisnet waarin alle aspecten van zowel informatiebeveiliging als privacy aan de orde komen. Deze aspecten worden weergegeven in een vraag en antwoord opzet vanuit het perspectief van de bestuurder of onderwijsmanager. Dit is dan ook de expliciete doelgroep voor deze publicaties en zij dragen hopelijk bij tot een breder begrip ten aanzien van informatiebeveiliging en privacy bij de managers en bestuurders van de mbo instellingen die daar ook verantwoordelijk voor zijn.

2. Het framework informatiebeveiliging en privacy in het mbo

Als resultaat van de Taskforce ibp in het mbo is eind december 2015 het zogeheten Framework opgeleverd. Dit framework bevat alle documenten die voor het mbo ontwikkeld zijn met betrekking tot de implementatie van ibp in het mbo. Hierbij heeft het mbo dankbaar gebruik kunnen maken van al in het hoger onderwijs zijn ontwikkeld en in een vergelijkbaar ho framework zijn opgenomen.
Dank zij de documenten van SURF hebben we in het mbo een vliegende start kunnen maken op dit onderwerp.
In het framework zijn alle documenten samengebracht, als een soort encyclopedie. Naast normenkaders, toetsingskader zijn er ook handreikingen, een roadmap, architectuur documentatie en data classificatie voorbeelden en nog veel meer. Binnen bijna elke mbo instelling (90%) is intussen een collega geschoold die daardoor het framework ook daadwerkelijk kan gebruiken. Het framework is op 1 augustus 2016 vastgesteld en in een speciale publicatievorm ter beschikking gesteld aan alle mbo instellingen en ondersteunende organisaties. Uiteraard is het een dynamische boekenkast die voorlopig volop in ontwikkeling zal blijven, niet zozeer wat betreft de kaders maar vooral wat betreft de handreikingen, voorbeelden en modellen.



3. Stakeholders

Binnen het programma is een aantal stakeholders benoemd. De belangrijkste zijn:

3.1 Mbo instellingen

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. Iedereen binnen de instellingen draagt daarbij een verantwoordelijkheid en het bewustzijn daarvan is cruciaal. De uiteindelijke verantwoordelijkheid ligt bij het College van Bestuur. Gezien de sectorale aanpak is het van belang dat ibp bestuurlijk breed wordt gedragen en dat ibp in het mbo in samenspraak met saMBO-ICT en de MBO Raad gemeenschappelijk wordt versterkt. 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.
Als eerste moeten daarbij de mbo instellingen zelf genoemd worden, verenigd in en vertegenwoordigd door de MBO Raad.

3.2 Ministerie van OC&W

Vertegenwoordigers van OCW hebben in een bijeenkomst met het onderwijsveld, in juni 2014, haar zorgen kenbaar gemaakt ten aanzien van informatiebeveiliging (b.v. examens liggen op straat). Zij geven ook aan behoefte te hebben om meer inzicht te krijgen in hoe de onderwijs sector er voor staat t.a.v. informatiebeveiliging, dat beeld ontbreekt nu 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 privacy bescherming te verbeteren en vervolgens te garanderen. Op grond van afspraken zou de Onderwijsinspectie dan ook in staat moeten zijn om controle uit te oefenen. Het ministerie heeft deze sectorale aanpak geaccordeerd en ondersteunt initiatieven om hierbij ook significante voortgang te maken.

3.3 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 ;
- Toezichthouders (bv. Raden van Toezicht, accountants, Inspectie);
- Systeemleveranciers ;
- Adviseurs en consultants.

Kennisnet en SURF ondersteunen de mbo sector vanuit een directe aansturing door een gebruikersgroep ibp in het mbo (zie ook hoofdstuk 6). Op het terrein van informatiebeveiliging en privacy worden zij aangesproken worden om hun expertise beschikbaar te stellen en te ondersteunen bij de realisatie van de doelstellingen in de sector. Er 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 ook 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 (bewerkersovereenkomsten, certificering van leveranciers). 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, waarbij tevens voorkomen wordt .dat dergelijke partijen met eigen kaders werken.

3.4 Maatschappij

Tot slot is er het maatschappelijk veld. Leerlingen, studenten, ouders, maar ook alle 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 hebben die niet ter discussie staat, zodat een school met trots een waardige diploma uitreiking kan organiseren.

4. Van normenkader naar toetsingskader

Als je de vraag wilt beantwoorden of een mbo instelling de informatiebeveiliging en privacy goed op orde hebt, dan kan dat alleen als afspraken meetbaar zijn. Er moet sprake zijn van een norm of een normenkader.

4.1 Vastgesteld normenkader ibp

Het onderwijs heeft in overleg met alle stakeholders besloten om een normenkader (**Waar wil of moet ik aan voldoen?)** te gaan hanteren voor de informatiebeveiliging. Belangrijk is dat de norm aansluit bij andere gekozen standaarden en vooral ook voldoet aan internationale normen. In navolging van het hoger onderwijs is daarom 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). 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 in ISO 27002 uitgewerkt, 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.
Voor privacy is een dergelijk normenkader niet voorhanden. Daartoe is uit de bestaande wet- en regelgeving een aparte set van normen gedestilleerd die voor het onderwijs van belang en toepasbaar zijn. Dit is overzichtelijk bijeen gebracht in een set van regels waar scholen zich aan moeten houden, het zogenaamde 'Compliance kader Privacy'. Ook voor examinering is een dergelijk kader opgesteld.

4.2 Van normenkader naar toetsingskader

Op basis van het ISO kader is een selectie gemaakt van voor het onderwijs relevante normen. Het betreft een selectie van 79 normen, door vertaald naar 85 statements, uit de gehele set van 114 normen van de versie 2013 van het ISO 27002 normenkader. De normen zijn in een aantal voor het onderwijs relevante clusters verdeeld:

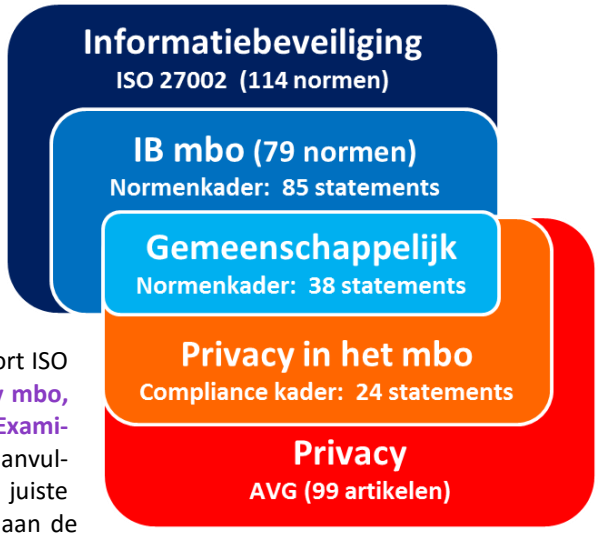
1. beleid en organisatie;
2. personeel en studenten;
3. ruimten en apparatuur;
4. continuïteit;
5. toegangsbeveiliging en integriteit
6. controle en logging.

Vervolgens zijn bij de normen ook de maatregelen beschreven om deze norm te bereiken en om dat ook aan te kunnen tonen (bewijslast). Dit gebeurt in de vorm van een 5 puntenschaal, de zogenaamde 'maturity levels. Met die maatregelen kan die norm dus op een steeds hoger niveau worden gerealiseerd. Het normenkader wordt hiermee toetsbaar. Met andere woorden het normenkader wordt een toetsingskader
Daarbij is niveau 1 het basis niveau, dit biedt dus maar 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. Het toetsingskader ibp in het mbo
Op deze manier ontstaat een geheel dat we het ibp toetsingskader noemen en omdat dit voor het mbo specifiek gemaakt is vanuit het ho model noemen we dit ook het ' ibp toetsingskader mbo'. Daarmee vormt dit toetsingskader het hart van het ibp 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 tot welk niveau genomen kunnen worden 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).

4.3 Aanvullende toetsingskaders

In aanvulling op de informatiebeveiliging spelen er binnen de mbo instellingen nog enkel andere zaken die niet direct samenvallen met informatiebeveiliging maar daar wel een belangrijke relatie mee hebben. Als eerste komt daarbij de bescherming van persoonsgegevens op, de privacy. Privacy is zeker niet hetzelfde als informatiebeveiliging maar er is wel een grote overlap. Zonder informatiebeveiliging is er geen sprake van privacy. Ook voor een onderwerp als examinering geldt dat er een belangrijke overlap is met informatiebeveiliging.

Maar naast de overlap met informatiebeveiliging is het op basis van wet- en regelgeving ook noodzakelijk om aparte, aanvullende normen of statements te formuleren en om aan de hand daarvan maatregelen te treffen om de privacy te waarborgen en om examinering veilig en correct te laten verlopen. Deze aanvullende statements zijn opgenomen in een compliance kader dat is ontwikkeld aan de hand van die relevante wet- en regelgeving en waarin de aanvullende statements voor privacy of voor examinering is weergegeven. In de figuur hiernaast is weergegeven hoe die overlap inzichtelijke gemaakt kan worden.



En net als bij het normenkader voor informatiebeveiliging is vervolgens ook hier op basis van het compliance kader (een soort ISO norm) een toetsingskader voor privacy (**Toetsingskader Privacy mbo, IBPDOC7)** en toetsingskader voor examinering (**Toetsingskader Examinering mbo, IBPDOC8)** ontwikkeld. En daarmee is een set van aanvullende maatregelen beschikbaar om deze thematieken ook op juiste wijze te behandelen en te beveiligen en daarmee te voldoen aan de wet- en regelgeving. Bij deze toetsingskaders is de opbouw gelijk aan die van de informatiebeveiliging met een vijftal maturity levels waarlangs je de uitvoer van de maatregelen kunt afmeten.

Wat je in het onderwijs kunt zien is dat informatiebeveiliging vaak gericht wordt vanuit de kant van de bedrijfsprocessen, met de bedrijfscontinuïteit als belangrijke driver. En dat de privacy aspecten vaak vanuit maatschappelijke druk en de wetgeving worden ge-initialiseerd. Ten aanzien van examinering bestaat er vanuit beide kanten druk om dit goed te regelen. Er zijn ook andere thematieken denkbaar die een aanvullend kader behoeven. Recent is ook digitaal ondertekenen opgenomen in het framework als belangrijke ontwikkeling die echter van een hele goede informatiebeveiliging moet worden voorzien.

Ten aanzien van privacy is het Compliance kader en het toetsingskader geheel up to date in relatie tot de nieuwe Algemene Verordening Privacy (AVG) die de Europese Commissie eind mei heeft gepubliceerd.

4.4 Risico's

In veel gevallen zie je dat binnen instellingen de strategie is om risico's te benoemen en vooral ook te beperken dan wel te vermijden. Vaak wordt dan langs de methodiek van risicomanagement een aanpak opgezet. Op zich niks mis mee, maar het kan heel veel dubbel werk betekenen. In feite is de benadering vanuit het op ISO gebaseerde toetsingskader ook een risico-aanpak. In de handreiking risico inventarisatie zijn alle voorkomende risico's in het mbo al in beeld gebracht en gerelateerd aan de statements in het mbo toetsingskader. Daarmee is een afdoende dekking gerealiseerd om met dit kader de risico's in het mbo te mitigeren. Als belangrijkste risico's in het mbo op dit moment kunnen gezien worden:

- Ongewenste verspreiding van zorgdossiers van leerlingen.
- Ongewenste verspreiding van verslagen voortvloeiend uit de gesprekscyclus (functioneren, beoordelen)
- Ongecontroleerde toegang tot het netwerk en applicaties.
- Verlies van privacy gevoelige data (datalekken).

De verschillende toetsingskaders bieden afdoende maatregelen om deze risico's te beheersen.

5. Assessments, audits en benchmark

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). In het framework ibp in het mbo zijn alle relevante documenten voor deze aanpak bijeengebracht. Concreet worden er voor informatiebeveiliging de volgende fasen onderscheiden:

Fase 1 (plan): Uitvoeren **mbo roadmap informatie beveiligingsbeleid (IBPDOC5)**.
Voorwaarde voor fase 1: brede betrokkenheid binnen instellingen: College van Bestuur, ict management, kwaliteitszorg, afdeling HR, juristen en kwartiermaker ibp.

Fase 2 (do): Inrichting beleid aan de hand van het **Model Informatiebeveiligings- en privacy beleid voor de mbo sector (IBPDOC6)**
Voorwaarde voor fase 2: actieve betrokkenheid van instellingen met de gebruikersgroep ibp in het mbo, werkgroepen en gezamenlijke projecten (saMBO-ICT en Kennisnet)

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

- **Normenkader Informatie Beveiliging mbo (IBPDOC2A) en Compliance kader Privacy (IBPDOC2A)**;
- **Toetsingskader informatie beveiliging mbo (IBPDOC3)**, ook wel Quick scan genoemd (ook digitaal beschikbaar) en **Toetsingskader privacy mbo (IBPDOC7)**,
- **Aanvullende toetsingskaders als die voor examinering (IBPDOC8) en digitaal ondertekenen (IBPDOC9).**

Voorwaarde voor fase 3: aanpak afgestemd met MBO Raad, OCW, externe accountants, externe leveranciers en examencommissies.

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

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 rapportage gepresenteerd, 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.

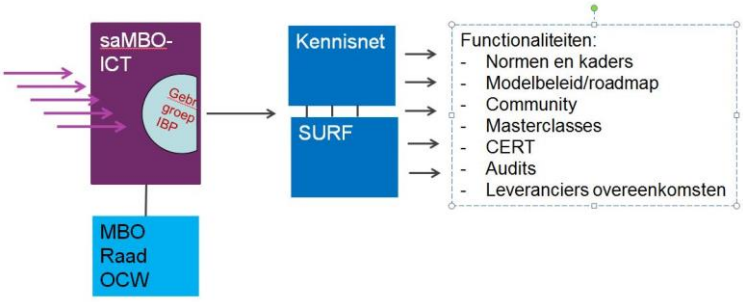
Externe audit
Het is de bedoeling om, net als in het hoger onderwijs, het peer -audit af te wisselen met externe audits. Dat betekent dat aan een externe partij wordt gevraagd om een audit uit te voeren. Om dit te reguleren en te zorgen dat deze audits op vergelijkbare manier plaatsvinden zal een gezamenlijke 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).

6. Samenwerking en afstemming in het mbo

De aanzet vanuit saMBO-ICT om tot een taskforce ibp in het mbo te komen is de eerste stap tot samenwerking in het mbo veld geweest. Er is vanuit het mbo veld heel positief op dit initiatief gereageerd hetgeen geresulteerd heeft in:

- Een grote inspanning vanuit de mbo instellingen om het framework te realiseren (Taskforce, werkgroepen, input van de scholingsprogramma's door de deelnemers)
- Veel aandacht voor de publicaties Hoe? Zo! Informatiebeveiligingsbeleid en Hoe? Zo! Privacy in het mbo;
- Hoge mate van participatie in het scholingsprogramma, de masterclasses (basis IBP, Privcacy, Peer Review)
- Concrete aanpak van de problematiek in het overgrote deel van de mbo instellingen (> 90%)



Het programma en de resultaten zijn eind 2015 overgedragen aan een gebruikersgroep ibp in het mbo, onder de vlag van saMBO-ICT. De groep is gevormd uit vertegenwoordigers vanuit de instellingen (3x) en de ondersteunende organisaties Kennisnet en SURF. In bijgaande figuur is de structuur van de huidige ibp organisatie in het mbo weergegeven. De gebruikersgroep heeft een netwerk ingericht waarin alle instellingen participeren met een contactpersoon, zijnde de ibp manager, security officer, privacy officer of functionaris gegevensbescherming. De regie op het hele proces zal vanuit de gebruikersgroep vorm gegeven worden. En het netwerk zal een cruciale rol spelen in enerzijds de uitwisseling van kennis en ervaring tussen de instelling en anderzijds om de samenwerking tussen de instellingen zo goed mogelijk te faciliteren.

En samenwerking is van groot belang. De thematiek is voor veel instellingen te complex om geheel zelfstandig te handelen. Leren van en met elkaar is noodzakelijk. Als iedereen het wiel moet gaan uitvinden is dat een zware taak. Het gezamenlijke scholingstraject van de masterclasses is een cruciale factor geweest in de enorme vlucht in de mbo instellingen gemaakt heeft. En als ervaringen, ideeën, oplossingen en producten met elkaar gedeeld gaan worden dan scheelt dat aanmerkelijk. En vooral ook in gezamenlijkheid werken aan modellen, overeenkomsten en afspraken kaders is cruciaal om als sector in de gehele informatie keten als goede partner effectief en efficiënt te kunnen functioneren.

Daarbij komt nog bij de doelstelling die we als onderwijssector hebben uitgesproken en ook afgesproken met OCW, namelijk die van zelfregulatie. De sector heeft het op zich genomen om informatiebeveiliging en privacy op een adequate wijze binnen de sector te regelen. Dat betekent dat de sector de ruimte krijgt om het op haar eigen manier te regelen. Maar ook de verplichting om te laten zien hoe de sector hierin ook presteert. Concreet betekent dit dat wel als sector afspraken moeten maken over de te hanteren standaarden, de daarin te bereiken ' baseline', waaraan moeten alle instellingen minimaal voldoen. Maar ook over de ambitie, waar willen we over een bepaalde periode staan m.b.t. ibp. En dat betekent ook transparantie, er moet helder in beeld gebracht worden wat de stand van zaken in het mbo is door middel van assessments en audits. De benchmark zal hierin een cruciale rol spelen. Pas dan kan er met OCW een bindende afspraak gemaakt worden over de wijze waarop ibp in het mbo gestalte krijgt.

7. De praktijk

In de praktijk is dit allemaal beste wel complex. Dat geldt zowel voor de verantwoordelijken als voor de uitvoerders. In dit hoofdstuk willen wel hen dan ook graag aan het woord laten.
Twee interviews zijn er gehouden. Een met een voorzitter van een College van bestuur en een met een ibp manager die de afgelopen jaren hard gewerkt heeft aan implementatie van het ibp verhaal.
Ben Geerdink is naast voorzitter van het CvB van het Rijn IJssel College ook voorzitter van het bestuur van saMBO-ICT en heeft als zodanig ook een heel duidelijk perspectief van de samenwerking van alle mbo instellingen op dit gebied. Martien van Beekveld is verantwoordelijk voor de implementatie van ibp in het Summa College in Eindhoven, een mbo instelling die al een aantal jaren actief is om ibp binnen de school vorm te geven.

1. interview met Ben Geerdink.
2. Interview met Martien van Beekveld.

Deze interviews worden in de loop van augustus 2016 in het document verwerkt.

Overzicht:

Documenten en publicaties Framework ibp in het mbo, 1/8/2016

Nummer omschrijving

- IBPDOC1 Verantwoordingsdocument informatiebeveiliging en privacy in het mbo onderwijs
- IBPDOC2A Normenkader informatiebeveiliging mbo
- IBPDOC2B Privacy compliance kader mbo
- IBPDOC3 Toetsingskader informatiebeveiliging: clusters 1 t/m 6
- IBPDOC4 Mbo ibp architectuur
- IBPDOC5 Mbo roadmap informatiebeveiligings- en privacy beleid
- IBPDOC6 Model informatiebeveiligings- en privacy beleid voor de mbo sector
- IBPDOC7 Toetsingskader privacy: cluster 7
- IBPDOC8 Toetsingskader examinering pluscluster 8
- IBPDOC9 Toetsingskader digitaal ondertekenen pluscluster 9
- IBPDOC10 Toetsingskader vmbo-mbo pluscluster 10 (nog in ontwikkeling)
- IBPDOC11 Benchmark mbo sector
- IBPDOC12 Functiewaardering ibp
- IBPDOC13 Positionering ibp
- IBPDOC14 Handleiding BIV classificatie
- IBPDOC15 BIV en PIA bekostiging
- IBPDOC16 BIV en PIA indiensttreding
- IBPDOC17 BIV en PIA online leren
- IBPDOC18 Bewerkersovereenkomst mbo versie
- IBPDOC21 Handboek mbo-audits: normenkader ib, compliance kader privacy, normenkader examineren en normenkader digitaal ondertekenen
- IBPDOC22 Starterkit identity management mbo versie
- IBPDOC23 Starterkit rbac mbo versie
- IBPDOC24 Starterkit bcm mbo versie
- IBPDOC25 Integriteitcode mbo versie
- IBPDOC26 Acceptable use policy mbo versie
- IBPDOC27 Responsible disclosure mbo versie
- IBPDOC29 Risico inventarisatie ibp
- IBPDOC30 Technische quick scan (APK)

Andere producten:

- Programma Informatiebeveiliging 2015
- Hoe? Zo! Informatiebeveiligingsbeleid in het mbo
- Hoe? Zo! Privacy in het mbo