**Benchmark informatiebeveiliging in de mbo sector**

****

**IBPDOC11**

**Verantwoording**

**Productie**

Kennisnet / saMBO-ICT

Benchmark is uitgevoerd met behulp van de tool Coable van het bedrijf Coblue Sybersecurity.

Het Hoger Onderwijs (SURF SCIPR) maakt ook gebruik van deze tool.

**Auteurs**

Leo Bakker (Kennisnet)

Ludo Cuijpers (saMBO-ICT, ROC Leeuwenborgh)

Paulo Moekotte (ROC van Twente)

December 2015

**Sommige rechten voorbehouden**

Hoewel aan de totstandkoming van deze uitgave de uiterste zorg is besteed, aanvaarden de auteur(s), redacteur(s) en uitgever van Kennisnet geen aansprakelijkheid voor eventuele fouten of onvolkomenheden.

**Creative commons**

Naamsvermelding 3.0 Nederland

(CC BY 3.0)

**De gebruiker mag:**

* Het werk kopiëren, verspreiden en doorgeven
* Remixen – afgeleide werken maken

**Onder de volgende voorwaarde:**

* Naamsvermelding – De gebruiker dient bij het werk de naam van Kennisnet te vermelden (maar niet zodanig dat de indruk gewekt wordt dat zij daarmee instemt met uw werk of uw gebruik van het werk).

Inhoudsopgave

[Verantwoording 2](#_Toc478709762)

[1. Mbo benchmark; stand van zaken 4](#_Toc478709763)

[1.1 Terugblik 4](#_Toc478709764)

[2. Informatieveiligheid in perspectief 5](#_Toc478709765)

[2.1 Bestuurlijke verantwoordelijkheid en verantwoording 5](#_Toc478709766)

[2.2 Kwaliteitszorg 7](#_Toc478709767)

[2.3 Organisatorische inbedding 8](#_Toc478709768)

[Bijlage 1: Framework informatiebeveiliging en privacy in het mbo 10](#_Toc478709769)

# Mbo benchmark; stand van zaken

## Aanleiding

Medio 2014 is de Taskforce Informatiebeveiliging en privacy van start gegaan met een duidelijke opdracht die verwoord is in het Verantwoordingsdocument[[1]](#footnote-1). De eerste paragraaf spreekt boekdelen:

*… 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 zo zijn redenen. Afgelopen jaren zijn in alle sectoren van het onderwijs incidenten rondom examinering 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 het internet te koop zijn. Een ander voorbeeld is de vraag of het onderwijs met de toenemende registratie van gegevens van leerlingen 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 de privacybescherming 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 Onderwijs, Cultuur en Wetenschap (OCW) 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 OCW 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 schetsen 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….*

Als sector hebben we de afgelopen jaren hard gewerkt om Informatiebeveiliging en privacy in onze sector op de strategische agenda te zetten. Op tactisch niveau hebben we een groot aantal documenten opgeleverd (zie bijlage 1) en is er volop geschoold in de masterclasses informatiebeveiliging en privacy (ibp) waar een vijftigtal mbo instellingen aan hebben deelgenomen. Op operationeel niveau is deze kennis binnen de mbo instellingen vertaald in een actief IBP beleid. Weliswaar staan we als sector aan het begin van een lange weg maar toch hebben we het gevoel dat we een vliegende start hebben gemaakt. We willen nu graag weten waar de mbo sector staat. Daarvoor hebben we in 2015 een eerste benchmark uitgevoerd om de bepalen op welk volwassenheidsniveau we ons nu bevinden. Dat zou je de nulmeting kunnen noemen.

Intussen zijn er drie jaar verstreken waarin de Benchmark ibp in het mbo is uitgevoerd, dat is 2016 – 2018. De resultaten van deze benchmarks kunt u vinden in het nieuwe framework 2.0 ibp in het mbo.

In het tweede hoofdstuk van dit document wordt dieper ingegaan op de achtergronden rond informatieveiligheid en de bestuurlijke verantwoordelijkheden die daarbij horen.

de nulmeting

# Informatieveiligheid in perspectief

## Bestuurlijke verantwoordelijkheid en verantwoording

Informatieveiligheid reikt verder dan mogelijke aanspraken op bestuurlijke verantwoordelijkheid, imagoschade of boetes. Het gaat ook over het effectief en efficiënt gebruik kunnen maken van informatie.

Digitalisering vergroot de invloedssfeer van derden (studenten, leveranciers, partners, agentschappen, etc.).

Het slim koppelen van gegevens/slimmer werken in de keten biedt kansen en bedreigingen. De vernetwerking van gegevens heeft bijvoorbeeld studenten en ouders veel gemak in dienstverlening gebracht. Denk aan de informatieoverdracht bij doorstroom in de beroepskolom of aan de inkijkfunctie voor ouders van veel leerlingvolgsystemen. Het toenemend digitaliseren van bedrijfsinformatie en ‑documentatie creëert echter ook nieuwe bedrijfsrisco’s. De maatschappelijke, politieke en organisatorische risico’s die dat met zich meebrengt, vragen om een brede(re) oriëntatie.

***… meer dan de helft van de scholen geen beleid en weet men niet hoe het nu staat met de informatieveiligheid.***

 “Verder valt op dat er scholen zijn die wel maatregelen hebben genomen, maar die geen risico-analyse hebben gemaakt. Ruim 30 procent van de scholen heeft een beleidsplan voor privacy, en iets minder dan 15 procent heeft een privacy officer aangesteld.[[2]](#footnote-2)”

Om te zorgen dat de aandacht niet verslapt, is een systeembenadering belangrijk waardoor je continuïteit borgt:

* informatieveiligheid moet geen bestuurlijke bananenschil worden;
* blik naar binnen: onderwerp moet niet beperkt blijven tot de ‘jongens van de ICT-afdeling’;
* blik naar buiten: ook de tuin van de buurman is van belang.

Het gebruik van normen en kaders betreft in het mbo vooral van de WBP-kaders (71%) de ISO 27001 en ISO 27002 (43%) en SURF juridisch normenkader cloudservices (35%)[[3]](#footnote-3).

Expliciete verantwoording heeft betrekking op enerzijds de kwaliteit van de informatiehuishouding en –voorziening en anderzijds op de veiligheid van de informatiehuishouding en –voorziening.

Bestuurders/directeuren:

* informatieveiligheid gedegen en structureel verankeren in de bedrijfsprocessen;
* het belang van informatieveiligheid binnen alle organisatielagen benadrukken via de lijn van de verplichtende zelfregulering;
* de kwaliteit van informatieveiligheid bespreken met studenten en ouders;
* de dialoog in de sector aangaan over de baseline, maturity levels en wijze van samenwerken;
* de dialoog aangaan met stakeholders (overheid en inspectie) over de vraag hoe ver we gaan in het aanvaarden van onveiligheid.

Waar sprake is van toenemende digitalisering en het ontwerpen en optimaliseren met behulp van architectuurprincipes, is het resultaat een even fijnmazig en meeraderig als kwetsbaar informatielandschap.

|  |
| --- |
| Risico’s m.b.t. de kwaliteit van document gestuurde bedrijfsprocessen (IDC, 2012) |
| 75,9% van de respondenten (n=1516) ondervond tijdens de laatste vijf jaar ernstige bedrijfsrisico’s en/of problemen met naleving als direct gevolg van inefficiënte document gestuurde bedrijfsprocessen. | D:\OneDrive\Werkdocumenten\Examinering\IBB\15.10.08 presentatie\De impact van bedrijfsgestuurde bedrijfsprocessen (RICOH Infographic).jpg |
| gevolgen:36,2% kon niet voldoen aan de vereisten voor naleving;30,2% verloor belangrijke werknemers;24,9% verloor belangrijke klanten;24,8% ondervond problemen met de IT-beveiliging;20,4% moest een grote bedrijfsaudit ondergaan;19,1% kreeg te maken met een ernstige PR-crisis. |
| afhankelijk van het type proces meldden tussen 35,9% en 45,3% van de deelnemers dat de document gestuurde processen waarvan ze persoonlijk kennis hadden niet efficiënt of effectief waren. |

**Resultaten tellen, mensen doen ertoe.**

Het toenemend gebruik van informatie van derden (studenten) met derden (leveranciers, agentschappen) voor derden (agentschappen, gemeenten) vraagt om expliciete verantwoording.

*Zorg voor kinderen betekent dus ook zorgen voor de veiligheid van hun gegevens.*
(Erik Gerritsen, Bureau Jeugdzorg Agglomeratie Amsterdam)

Als bestuurder vertegenwoordig je ook de belangen van ouders door werk te maken van de veiligheid van de gegevens van hun kinderen.

Wat vinden ouders eigenlijk van het gebruik van informatie door scholen? Of wat willen ze ‘zeker’ weten?

**De meerderheid van ouders (n=1002) kent bezwaren t.a.v. veiligheid en privacy, en wel daar een elektronisch leerlingdossier (leeftijd kinderen van 0-17 jaar):**

* **kan worden gehackt of gestolen (87%);**
* **door de school of een medewerker kan worden gebruikt tegen het kind (68%)**[[4]](#footnote-4)**.**



**Bijna 9 van de 10 ouders ondersteunen het verzamelen en gebruiken van elektronische leerling gegevens, wanneer ze weten dat een school/dienstverlener:**

* **veiligheidsgaranties kan afgeven (85%)**
* **elektronische leerling gegevens alleen gebruikt voor onderwijsdoeleinden (87%).**

Maak ouders (en studenten) bewust van de waarborgen die er al zijn en hoe deze werken.

## Kwaliteitszorg

Kwaliteitszorg helpt verantwoordelijkheden van instellingen te benadrukken, intensiveert kritische reviews van externen en stimuleert aandacht voor de onderwijsfunctie en didactische methoden binnen instellingen. Tevens versterkt kwaliteitszorg de organisatie, zo worden studenten ‘empowered’ doordat naar ze wordt geluisterd en worden organisatieonderdelen gestimuleerd om transparant en open te zijn over hun keuzes en beslissingen. Ook kan het een bijdrage leveren aan groeiend vertrouwen van de maatschappij in instellingen[[5]](#footnote-5).

**Systeembenadering**

Verantwoordelijkheid dragen voor informatieveiligheid vereist een goed functionerende PDCA cyclus. Centraal staat de aansluiting van informatieveiligheid op de reguliere Plan-Do-Check-Act cyclus, waardoor een systeem van zelfregulering op het gebied van informatieveiligheid wordt gerealiseerd.

Een systeembenadering draagt er ook aan bij dat kwaliteit wordt verbeterd zonder de regeldruk te verhogen:

* geen aparte datasets;
* geen aparte cycli;
* geen aparte controles.

**Benchmark** informatieveiligheid

Een benchmark wordt ingezet als instrument of methode om binnen een sector voortdurende verbetering na te streven. In de profit sector ligt daarbij het accent vooral op concurrentie en het vergroten van het onderscheidend vermogen. Binnen de non profit sector ligt het accent vooral op transparantie en het vergroten van het regulerend vermogen.

Organisaties moeten informatieveiligheid leren te beschouwen als een vast onderdeel van de dagelijkse praktijk. Informatieveiligheid moet worden ingericht als een doorlopend proces van leren en verbeteren, dat onder de bestuurlijke verantwoordelijkheid valt. Hiertoe creëren we als sector gezamenlijk enkele handige en goede kaders die middels een benchmark worden ingezet als toetssteen.

Met de opbrengsten van de taskforce in handen is ieder bestuur in staat om de gewenste zelfregulering verder vorm en inhoud te geven. Het is de verantwoordelijkheid van bestuurders om dit proces tot een succes te maken.

**Baseline** (normen, grenswaarden en standaarden)

Het is belangrijk om de informatiehuishouding goed op orde te hebben. Eén van de hulpmiddelen hierbij is de implementatie van een baseline informatiebeveiliging*[[6]](#footnote-6)*. Met een baseline hebben bestuur en management een instrument in handen waarmee zij in staat zijn om te meten of de organisatie ‘in control’ is op gebied van informatieveiligheid.

Een groeiende digitale onderwijskundige infrastructuur is gebaat bij passende regelgeving en onderlinge afspraken en garanties, zoals richtlijnen voor het gebruik van elektronische informatie, gedragscodes en voorschriften voor de beveiliging. De beschikbaarheid en de continuïteit van de dienstverlening en de bescherming van gegevens hebben daarbij de allerhoogste prioriteit.

**Volwassenheid**

De volwassenheid van de sector en de instellingen waaruit de sector bestaat, kan worden afgelezen aan de hand waarop met technologieën op een verantwoorde wijze wordt geëxperimenteerd. Het invullen van een experimenteerruimte vergt allereerst een kader voor de risicogebieden of clusters waarop kan worden geëxperimenteerd. Wanneer is vallen en opstaan acceptabel? Welke risico’s kunnen worden geaccepteerd? Wie bepaalt dat en hoe wordt dat bepaald? In het algemeen kan worden gesteld dat de ernst van de risico’s bepaalt in welke mate er ruimte kan worden gegeven om te experimenteren.

Voor een beeld van de volwassenheid van de hele sector is een vorm van benchmarking noodzakelijk opdat kan worden vastgesteld of er sprake is van een normale distributie.

Belangrijke vraag die op alle niveaus beantwoord dient te worden:

Hoe ver gaan we in het aanvaarden van onveiligheid?
(Michel van Eeten, Hoogleraar Governance van Cybersecurity)

Het is niet aan te geven waar onze samenleving zich bevindt in dit traject van aanvaarding, omdat dit sterk verschilt per risicogebied. Het optimale niveau van onveiligheid bepalen we van geval tot geval. Zowel het gebruiken van nieuwe technologieën als het niet-gebruiken ervan leidt tot risico’s onzekerheden en problemen rondom verantwoordelijkheden.

Als sector kunnen we de verplichte zelfregulering oriënteren op een groeiperspectief waarbij sprake is van een genormeerde experimenteerruimte[[7]](#footnote-7):

*in bepaalde gevallen en onder bepaalde (proces)condities de mogelijkheid te krijgen om te experimenteren met nieuwe technologieën.*

De baseline voor ons denken en handelen m.b.t. informatieveiligheid is bepaald door wet- en regelgeving, noties omtrent maatschappelijk verantwoord ondernemen en regels van goed fatsoen. Daarnaast wordt een tijdelijke gedoogzone gecreëerd om nieuwe technologieën te ontwikkelen zonder dat een onderwijsinstelling zich direct overgeeft aan deze nieuwe technologieën.

**Peer review**

Een peer review heeft vooral tot doel met en van elkaar te leren. Door middel van een peer review kan meer de nadruk worden gelegd op waarderende en stimulerende vormen van verkenning en onderzoek. Door middel van een peer review wordt het lerend vermogen van de sector vergroot.

Het is hierbij cruciaal dat externe experts geaccepteerd worden als onbevooroordeelde specialisten en dat deze specialisten naar gelang het doel van het bezoek variëren (bijvoorbeeld managementexperts als het gaat om instellingsaudits)[[8]](#footnote-8).

## Organisatorische inbedding

Werkvloer (implementatie)

**Uitgangspunten** voor implementatie

* vanuit een baseline niveau op een verantwoorde wijze stapsgewijs streven naar maximale volwassenheid[[9]](#footnote-9);
* gaat niet om de techniek maar om de structuur en de verantwoordelijkheidsverdeling binnen organisaties;
* minstens zo belangrijk is het gedrag van de medewerkers, hoe gaan docenten/medewerkers met informatie en dossiers om en met nieuwe technologieën, zoals sociale media.

Succesfactoren voor implementatie:

* beschouw een dergelijk project als een ingrijpend veranderingstraject en niet als een technisch project;
* begin niet zonder de nadrukkelijk commitment van de leiding;
* zorg voor een transparant en zichtbaar project;
* beleg project niet uitsluitend bij externe adviseurs;
* benoem op sleutelposities in het project eigen medewerkers met voldoende kennis, tijd en mandaat;
* voorkom als (te) star ervaren digitale werkprocesondersteuning;
* start nooit een pilotimplementatie zonder dat door-en-door getest is;
* Zorg voor voldoende financiële reserves.

Benchmark als activiteit/proces inbedden in de staande kwaliteitszorgorganisatie (single information single audit - SISA) en –cultuur

Werkvloer (houding)

Cultuur: appelleert aan de intrinsieke motivatie van docenten en medewerkers om in‑ en extern hoogwaardige kennis en ervaring te ontwikkelen, in te zetten en te delen.

*Het is van het grootste belang dat de organisatiecultuur een positieve houding kent ten aanzien van informatieveiligheid in de gehele organisatie. Het is bovendien van belang dat activiteiten binnen de organisatie op een consistente wijze beantwoorden aan praktijken van een informatieveiligheidscultuur*[[10]](#footnote-10).

Kwaliteitscultuur is een onderdeel van de organisatiecultuur. Ze wordt inmiddels erkend als een van de meest essentiële factoren van kwaliteit. Kwaliteitscultuur vormt een uitdrukking van onderhuidse individuele en collectieve waarden in het perspectief van effectief presteren als professional en onderwijsorganisatie. Categorieën als gedrevenheid, betrokkenheid en collectiviteit worden, hoewel niet altijd meetbaar, gezien als belangrijke graadmeters voor de identificatie van de kwaliteitscultuur[[11]](#footnote-11). De informatieveiligheidscultuur is een onderdeel van die kwaliteitscultuur en dient voor een ‘*spillover*’ te zorgen naar handelingsstrategieën en -repertoire als uitingen van organisatiebewustzijn en ‑gedrag.



Figuur 1 Model van Berings (2010)

Bijlage 1: Framework informatiebeveiliging en privacy in het mbo



1. Zie IBPDOC1: Verantwoordingsdocument Informatiebeveiliging en privacy (ibp) in het mbo. [↑](#footnote-ref-1)
2. Stichting Kennisnet (2015). *ICT monitor mbo 2014 Vergelijking van ICT organisatie, visie, infrastructuur, applicaties, projecten, personeel en financiën van mbo instellingen*. Zoetermeer: Stichting Kennisnet. [↑](#footnote-ref-2)
3. Onderwijs Innovatie Groep (2015). *Onderzoeksrapport Standaarden en beveiliging in het po, vo, mbo en ho*. Uitgevoerd in opdracht van de directie Kennis van het Ministerie van Onderwijs Cultuur en Wetenschap. Utrecht: Onderwijs Innovatie Groep. [↑](#footnote-ref-3)
4. Future of Privacy Forum (2015). Beyond The Fear Factor. Parental Support For Technology and Data Use in Schools. Washington DC: Future of Privacy Forum. [↑](#footnote-ref-4)
5. Leest, B.,Mommers, A., Sijstermans, E., & Verrijt, T. (2015). Kwaliteitszorg en kwaliteitscultuur in het hoger onderwijs. Literatuurstudie. Nijmegen: ITS, Radboud Universiteit. [↑](#footnote-ref-5)
6. Baselines vormen een instrument om de informatieveiligheid van (overheids)organisaties te verbeteren en zijn gebaseerd op algemeen geaccepteerde kaders, zoals de NEN- ISO-27001/2 . [↑](#footnote-ref-6)
7. Broeders, D., Cuijpers, M. K. C., & Prins, J. E. J. (Eds.). (2011). *De staat van informatie* (Vol. 25). Wetenschappelijke Raad voor het Regeringsbeleid. Amsterdam: Amsterdam University Press. [↑](#footnote-ref-7)
8. Leest, B.,Mommers, A., Sijstermans, E., & Verrijt, T. (2015). Kwaliteitszorg en kwaliteitscultuur in het hoger onderwijs. Literatuurstudie. Nijmegen: ITS, Radboud Universiteit. [↑](#footnote-ref-8)
9. Bollaert, L. (2014). Quality Assurance (Qa) in Europe (2005–2015). From Internal and Institutional to External and International. *Journal of the European Higher Education Area*, 3, 1-24. [↑](#footnote-ref-9)
10. Alnatheer, M., & Nelson, K. (2009). Proposed framework for understanding information security culture and practices in the Saudi context. [↑](#footnote-ref-10)
11. Bollaert, L. (2014). Quality Assurance (Qa) in Europe (2005–2015). From Internal and Institutional to External and International. *Journal of the European Higher Education Area*, 3, 1-24. [↑](#footnote-ref-11)