Taskforce Informatiebeveiligingsbeleid.

Cursus 4 2015-2016	Actieve masterclasses Informatiebeveiliging voor de MBO/HO sector
Locatie: Carlton Utrecht plus overnachting	

Aanleiding:
Om het deskundigheidsniveau van instellingen te vergroten, zal een masterclass georganiseerd worden. Deze bestaat uit een serie van vijf volle dagen, elk gericht op een specifiek thema. De doelgroep bestaat uit niet alleen uit IT verantwoordelijken, zoals IT-directeuren, Informatiemanagers, enz., maar ook uit kwartiermakers met een andere achtergrond. Deze masterclasses worden verzorgd door deskundigen op het terrein van Informatiebeveiliging.
Thema's zijn:
- Informatiebeveiligingsbeleid;
- Technologie;
- Juridisch kader;
- Examinering;
- IT-Audit.

De masterclass wordt georganiseerd door Kennisnet, SURF en saMBO-ICT onder verantwoordelijkheid van de taskforce. De totale kosten bedragen € 650, inclusief eten en 2 overnachtingen.
De totale studiebelasting bedraagt 80 uur, te weten de 10 geplande dagdelen (5 dagen) en de voorbereiding, waaronder de te maken opdrachten.
Bron: Actieplan - *Informatiebeveiligingsbeleid mbo - V.1.0, 14-05-2014 -* Opdrachtgever: saMBO-ICT

Opzet van de actieve masterclasses:
Dag 1:
Collega's uit het Hoger Onderwijs (HO) presenteren hun tools, documenten en kaders betreffende IBB (Informatie Beveiligings Beleid). In de middaguren wordt het vakgebied informatiebeveiliging en privacy geïntroduceerd en de inrichting van informatiebeveiliging in het Hoger Onderwijs, en de hierbij gebruikte materialen, toegelicht. In de avonduren worden we bijgepraat over de uitdagingen en successen die verbonden zijn aan de implementatie van IBB.
Dag 2:
Een succesvol IBB traject start met een risico analyse. ISO 27001 (beschrijving IBB) is in feite een beschrijving van allerlei risico's. Collega's uit het bedrijfsleven delen hun ervaring en kennis op dit gebied met de deelnemers. De cursisten worden getraind om de risico's van hun MBO instelling te plotten (koppelen) aan de ISO 27002 (checklist IBB) norm.
Dag 3:
Tijdens het eerste deel van de dag wordt vooral het theoretisch kader uitgewerkt. Begrippen uit het IBB en audit wereld worden toegelicht en aan de hand van sprekende voorbeelden verduidelijkt. Het tweede deel van de dag wordt de starterskit MBO/HO Informatiebeveiligingsbeleid gepresenteerd en worden de deelnemers uitgenodigd om de opgedane kennis toe te passen binnen hun eigen onderwijsinstelling. Vandaag wordt de masterclass verzorgd door collega's uit de MBO sector.
Dag 4:
Op deze dag maken de cursisten kennis met de MBO/HO audit tool. Nadat de tool is toegelicht gaan de deelnemers aan de slag om hun eigen onderwijsinstelling te beoordelen. Een "technische" beoordeling van het netwerk is onderdeel van deze dag. De dag wordt verzorgd door collega's uit de consultancy wereld die MBO instellingen ondersteund hebben bij de implementatie van IBB.
Dag 5:
Tijdens deze dag presenteren de deelnemers het Informatiebeveiligingsplan van hun instelling. De presentatie is vandaag in handen van een MBO en HO collega.

Tips en tricks uit de dagelijkse praktijk worden gepresenteerd. Kennisnet behandelt het toetsingskader examineren op basis van het ISO normenkader. Tot slot wordt de mogelijke vervolgscholing toegelicht.

Planning cursus 1, actieve master classes IBB voor de MBO/HO sector

	Docent	**Thema**
Dag 1, middag 28 januari 2016 13.00 – 16.00 uur	Alf Moens (SURFnet, universiteit Delft)	Toelichting SURF documenten en Privacy beleid
Dag 1, avond 28 januari 2016 17.00 – 20.00 uur	Hans van der Wal (Saxion)	Best practice uit het Hoger Onderwijs
	Hoe? Zo! Informatiebeveiligingsbeleid in het MBO: Hoofdstuk 1: Inleiding Hoofdstuk 4: Hoe kom ik "In control"	
Dag 2, ochtend 29 januari 2016 9.00 – 12.00 uur	Maurits Toet (Cerrix BV)	Risicomanagement vanuit de praktijk
Dag 2, middag 29 januari 2016 13.00-16.00 uur	Martijn Broekhuizen (Noorderpoort)	Gebruik van normen- en toetsingskader binnen Noorderpoort
	Hoe? Zo! Informatiebeveiligingsbeleid in het MBO: Hoofdstuk 2: Waarom informatiebeveiliging? Hoofdstuk 3: Om welke risico's gaat het en hoe ga ik er mee om?	
Dag 3, middag 3 maart 2016 13.00 – 16.00 uur	Ludo Cuijpers (Leeuwenborgh)	Diepgang in IT auditing (scope, beoordeling, kwaliteitsnormen, BIV classificatie, etc.)
Dag 3, avond 3 maart 2016 17.00 – 20.00 uur	Ludo Cuijpers (Leeuwenborgh)	Draaiboek IBB MBO sector
	Hoe? Zo! Informatiebeveiligingsbeleid in het MBO: Hoofdstuk 5: Hoe kan ik het informatiebeveiligingsbeleid oppakken?	
Dag 4, ochtend 4 maart 2016 9.00 – 12.00 uur	Marthe Uiterhoeve (KZA)	Toelichting op SURFaudit
Dag 4, middag 4 maart 2016 13.00 – 16.00 uur	Victor van Hunnik (Grafisch Lyceum Rotterdam)	Technische aspecten van de SURFaudit (pen-test e.d.) SURFcert
	Hoe? Zo! Informatiebeveiligingsbeleid in het MBO: Hoofdstuk 6: Hoe wordt het informatiebeveiligingsbeleid toegepast in de praktijk?	
Dag 5, ochtend 18 maart 2016 10.00 – 13.00 uur	Bart van den Heuvel (Universiteit Maastricht, SURFibo)	Toelichting en operationele toepassing Informatiebeveiligingsbeleid van de Universiteit Maastricht
Dag 5, middag 18 maart 2016 14.00 – 17.00 uur	Leo Bakker (Kennisnet)	Presentatie IBB deelnemers + Voorbeeld toetsingskader examineren
	Hoe? Zo! Informatiebeveiligingsbeleid in het MBO: Hoofdstuk 7: Wat kunnen we sector breed doen?	

Inschrijving en kosten:
De totale kosten bedragen € 650. Inschrijven per mail is mogelijk tot 22-10-2015 via link of bij Tiny Verbeek (tiny.verbeek@sambo-ict.nl).
Voor inhoudelijke informatie kunt u zich wenden tot Ludo Cuijpers, coördinator Actieve Master classes (l.cuijpers@kennisnet.nl).

Dag 1	**Actieve masterclasses Informatiebeveiliging voor de MBO/HO sector**
Locatie: Carlton Utrecht plus overnachting	
Docent: Alf Moens	**SURF documenten en Privacy beleid**
Tijd: 13.00 – 16.00 uur	
Docent: Hans van der Wal	**Best practice uit het Hoger Onderwijs**
Tijd: 17.00 – 20.00 uur	

Doelstelling dag 1:
Collega's uit het Hoger Onderwijs presenteren hun tools, documenten en kaders betreffende IBB (Informatie Beveiligings Beleid). In de middaguren wordt het vakgebied informatiebeveiliging en privacy geïntroduceerd en de inrichting van informatiebeveiliging in het Hoger Onderwijs, en de hierbij gebruikte materialen, toegelicht. In de avonduren worden we bijgepraat over de uitdagingen en successen die verbonden zijn aan de implementatie van IBB.
Op het einde van de dag zijn de volgende leerdoelen gerealiseerd:

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

Te bestuderen documenten:

- *Hoe? Zo! Informatiebeveiligingsbeleid in het MBO (10 pagina's):*
  Hoofdstuk 1: Inleiding
  Hoofdstuk 4: Hoe kom ik "In control"
  (Bijlage 1- Hoe Zo IBB in het MBO)
- *Leidraad informatiebeveiliging (7 pagina's)*
  (Bijlage 2- Leidraad Informatie beveiliging)
- *Model informatiebeveiligingsbeleid (19 pagina's)*
  (Bijlage 3- Model informatiebeveiligingsbeleid)

Te maken opdracht:

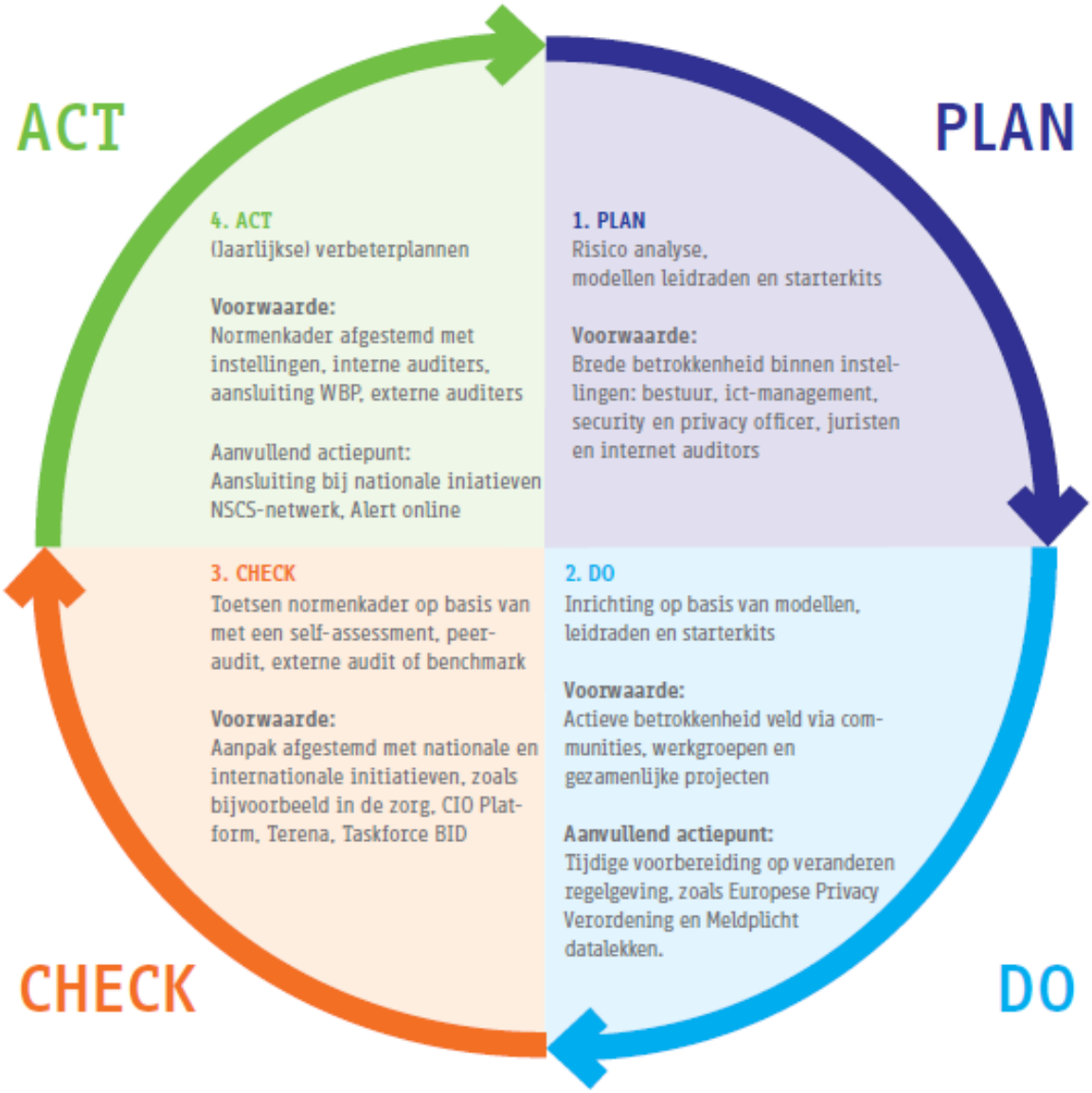
- Beschrijf op een A4-tje de stand van zaken op het gebied van Informatiebeveiligingsbeleid binnen je MBO instelling.

Alf Moens:
Alf is de Corporate Security Officer van SURFnet. Hij is de founding father van het security compliance framework (SURFaudit) voor het Hoger Onderwijs. Sinds 2007 coördineert Alf compliance and control van informatiebeveiliging voor het Hoger Onderwijs. Daarbij heeft hij breed draagvlak gerealiseerd bij besturen, IT management, overheden en toezichthouders. Voordat hij bij SURF kwam was Alf 8 jaar lang security manager bij TU Delft. Alf heeft een masters degree in Information Security Management

(TUe/UvT) en is bestuurslid van het Platform voor informatiebeveiligers (PvIB), de Nederlandse vakorganisatie voor security professionals.

Hans van der Wal:
Hans is ruim 40 jaar werkzaam in de IT met zowel ervaring in het bedrijfsleven als ook in het Hoger Onderwijs. Bij Saxion is hij 17 jaar manager van de ICT-dienst geweest en 7 jaar werkzaam geweest als informatiemanager, waar hij een grote bijdrage heeft geleverd aan de IT-Governance van de instelling waarmee Saxion in 2011 de Gouden ASL BISL Award heeft gewonnen. Sinds april 2013 is Hans Security Officer bij Saxion en heeft hij de uitdaging op zich genomen om in 2016 Saxion op CMM niveau 3 te hebben. Ook landelijk is hij altijd zeer actief in zowel overleg organen als ook werkgroepen om het HO op landelijk niveau een stapje verder te brengen.

Hoe? Zo! Informatiebeveiligingsbeleid in het MBO.
Pagina 16.



Dag 2	**Actieve masterclasses Informatiebeveiliging voor de MBO/HO sector**
Locatie: Carlton Utrecht	
Docent: Maurits Toet	**Risico management vanuit de praktijk**
Tijd: 9.00 – 12.00 uur	
Docent: Martijn Broekhuizen	**Gebruik van normen- en toetsingskader binnen Noorderpoort**
Tijd: 13.00 – 16.00 uur	

Doelstelling dag 2:
Een succesvol IBB traject start met een risico analyse. ISO 27001 (beschrijving IBB) is in feite een beschrijving van allerlei risico's. Collega's uit het bedrijfsleven delen hun ervaring en kennis op dit gebied met de deelnemers. De cursisten worden getraind om de risico's van hun MBO instelling te plotten (koppelen) aan de ISO 27002 (checklist IBB) norm.
Op het einde van de dag zijn de volgende leerdoelen gerealiseerd:

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

Te bestuderen documenten:

- *Hoe? Zo! Informatiebeveiligingsbeleid in het MBO (7 pagina's):*
  Hoofdstuk 2: Waarom informatiebeveiliging?
  Hoofdstuk 3: Om welke risico's gaat het en hoe ga ik er meer om?
  (Bijlage 1- Hoe Zo IBB in het MBO)
- *NEN-ISO/IEC 27001 nl (31 pagina's)*
  (Bijlage 5- ISO 27001 2013)
- *NEN-ISO/IEC 27002 nl (102 pagina's, alleen eerste 10 pagina's bestuderen)*
  (Bijlage 6- ISO 27002 2013)

Te maken opdrachten:

- Beschrijf de 10 grootste risico's binnen je MBO instelling op een A4-tje.

Maurits Toet MSc
Senior Consultant bij Cerrix B.V. Ik heb 8 jaar werkervaring, met name op het gebied Risicomanagement & Assurance en Finance & Control. Mijn kerncompetenties zijn mijn enthousiasme, resultaatgerichtheid, zelfstandigheid, overtuigingskracht, hands-on mentaliteit en samenwerkend vermogen.
Als consultant heb ik bij diverse financiële instellingen projecten succesvol uitgevoerd. Het betrof hier projecten op het gebied van o.a. Risicomanagement & Assurance (o.a SAS70/ ISAE3402, SOx404, Keurmerk Klantgericht Verzekeren, etc) en Finance & Control (o.a. Interim Controller & Business Analyst, etc).

Martijn Broekhuizen, Informatiemanager
Als informatiemanager bij het Noorderpoort ondersteun ik de Security Officer, met name met betrekking tot de PDCA-cyclus rondom informatiebeveiliging. Samen met de Security specialist bij de Dienst ICT zorgen we met z'n drieën voor een continue proces waarin zowel de technische als organisatorische kant van informatiebeveiliging wordt gemonitord en, daar waar veel risico is, verbeterd.

Hoe? Zo! Informatiebeveiligingsbeleid in het MBO.
Pagina 10.

Met welke concrete risico's kan een mbo-instelling worden geconfronteerd?

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. Kernregistratie-systeem	Het risico op fraude of onrechtmatige invoer in kernregistratiesysteem.	Onvoldoende controles en functiescheiding in het systeem.	Frauduleuze handelingen kunnen plaatsvinden, reputatieschade.
3. Cijferregistratie-systeem	Het risico op fraude bij invoer/mutatie van cijfers in cijferregistratiesysteem.	Onvoldoende ingebouwde controles (functiescheiding, 4-ogen principe).	Een onjuiste beoordeling van deelnemers, reputatieschade.
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 (bij-voorbeeld door hackers) tot de IT-infrastructuur.	Onvoldoende technische beveiligingen.	Niet beschikbaar zijn, onbetrouwbaarheid en diefstal van gegevens, reputatieschade.
6. Studentenvolg-systeem	Het studentenvolgsysteem is niet beschikbaar.	Het niet redundant uitvoeren van de database server (mogelijk in de cloud).	Studenten/medewerkers/docenten die 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, reputatieschade 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, reputatieschade.
9. Ongeautoriseer-de toegang	Het risico op ongeautoriseerde toegang.	Onvoldoende volwassenheid/bewustzijn over IT-beveiliging bij medewerkers door bv. deling van wachtwoorden.	Fraude, diefstal, reputatieschade.
10. Dataverlies	Het risico op dataverlies.	Een gebrek aan back ups (procedures) of calami-teitenplan.	Gebrek aan beschikbaarheid, reputatieschade.

Tabel 1. Risico's op het gebied van gegevens waar een mbo-instelling mee te maken kan krijgen.

Dag 3	**Actieve masterclasses Informatiebeveiliging voor de MBO/HO sector**
Locatie: Carlton Utrecht plus overnachting	
Docent: Ludo Cuijpers	**Diepgang in IT auditing**
Tijd: 13.00 – 16.00 uur	
Docent: Ludo Cuijpers	**Draaiboek Informatiebeveiligingsbeleid in de MBO sector**
Tijd: 17.00 – 20.00 uur	

Doelstelling dag 3:
Tijdens het eerste deel van de dag wordt vooral het theoretisch kader uitgewerkt. Begrippen uit het IBB en audit wereld worden toegelicht en aan de hand van sprekende voorbeelden verduidelijkt. Het tweede deel van de dag wordt de Roadmap MBO Informatiebeveiligingsbeleid gepresenteerd en worden de deelnemers uitgenodigd om de opgedane kennis toe te passen binnen hun eigen onderwijsinstelling. Vandaag wordt de masterclass verzorgd door collega's uit de MBO sector.
Op het einde van de dag zijn de volgende leerdoelen gerealiseerd:

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

Te bestuderen documenten:

- *Hoe? Zo! Informatiebeveiligingsbeleid in het MBO (4 pagina's):*
  Hoofdstuk 5: Hoe kan ik het informatiebeveiligingsbeleid oppakken?
  (Bijlage 1- Hoe Zo IBB in het MBO)
  Bijlage 4: Roadmap

Te maken opdrachten:

- De cursist heeft op een A4-tje de 10 belangrijkste informatie en informatiesystemen binnen zijn MBO instelling opgesomd.

Ludo Cuijpers MIM, MSc
Ludo is een ervaren ICT manager binnen het beroepsonderwijs in Nederland. Zowel regionaal en nationaal is hij betrokken bij ICT vernieuwingen binnen het onderwijs. Zijn kerncompetenties zijn z'n enthousiasme, resultaatgerichtheid, innovatief vermogen, overtuigingskracht, motiveren van medewerkers en samenwerkend vermogen.
Als ICT manager heeft hij zowel binnen de eigen onderwijsinstelling als landelijk diverse projecten succesvol afgerond. Hij was projectleider van het grote landelijke netwerk Kennisnet en het project Educatieve Contentketen. Begin 2014 heeft hij de universitaire opleiding IT Audit afgerond, met als afstudeeropdracht het Hoger Onderwijs audit kader.
Hij is betrokken bij alle werkgroepen van de Taskforce Informatiebeveiliging in de MBO sector en is tevens voorzitter van de werkgroep Kennisontwikkeling (o.a. Masterclasses). Hij is mede auteur van het Hoe? Zo! boekje "Informatiebeveiligingsbeleid in de MBO sector".

Casper Schutte:

Sinds 2007 werkzaam bij ROC Midden Nederland, begonnen als Hoofd/Directeur ICT, daarna (2009) als kwartiermaker van een nieuw te vormen Dienst Onderwijsontwikkeling, Informatie & Innovatie. Directeur OI&I tot maart 2013. Na een reorganisatie (opdelen Dienst OI&I) terecht gekomen bij de nieuwe Dienst ICT & Informatiemanagement. Bij afdeling IM actief op de gebieden Beleidsontwikkeling, Informatiemanagement Onderwijs, Change Management en Informatiebeveiliging.

Hoe? Zo! Informatiebeveiligingsbeleid in het MBO.

Pagina 21 en 22.

Fase 1 bestaat dan ook uit het voeren van kennismakingsgesprekken met eigenaren en beheerders van bedrijfsprocessen, informatiesystemen, applicaties, e.d.
Als dat inzicht is verkregen (en gedocumenteerd), wordt in overleg met die eigenaren bekeken hoe kwetsbaar de bedrijfsprocessen zijn voor verstoringen in de ict voorziening: voor de belangrijkste applicaties wordt voor beschikbaarheid, integriteit en vertrouwelijkheid gescoord op een schaal van 1 (nog niets aan beveiliging gedaan) tot 3 (voldoende gedaan).
Dit is bekend als de zogenaamde BIV-classificatie. Daarnaast wordt geïdentificeerd voor welke onderdelen van Informatiebeveiliging beleid en procedures bestaan. Denk hierbij onder meer aan de aanwezigheid van een goedgekeurd beleidsdocument, het hebben van een beveiligingsorganisatie waarin iedereen zijn of haar verantwoordelijkheden kent, een gebruiksreglement, een incident registratiesysteem, viruscontrole, etc. Meestal zijn er al technische voorzieningen op beveiligingsgebied getroffen zoals bijvoorbeeld het gebruik van viruscheckers, maar is de informatiebeveiligingsorganisatie nog niet gerealiseerd en het beleid niet vastgesteld.

Fase 2: Korte termijn verbeteringen en opstellen plan van aanpak
Om aan het bestuur aan te kunnen tonen dat het loont om structureel aandacht aan informatiebeveiliging te geven worden de meest lonende maatregelen doorgevoerd (laaghangend fruit). Deze zijn afgeleid uit de inventarisatie van kwetsbaarheden en de stand van zaken m.b.t. te nemen maatregelen. In deze fase wordt ook een plan van aanpak voor de lange termijn opgesteld, waarin alle aspecten van informatiebeveiliging aan de orde komen. In dat plan komen projectvoorstellen te staan die de komende jaren uitgevoerd moeten worden. Denk hierbij aan het opstellen van een baseline informatiebeveiliging, het inrichten van de informatiebeveiligingsorganisatie en maatregelen op het gebied van bedrijfscontinuïteit.

Fase 3: De dialoog met bestuurders
In deze fase is het belangrijk om commitment van het bestuur te krijgen. Kan de informatiebeveiliger het bestuur overtuigen van het belang van structurele aandacht voor informatiebeveiliging?
In principe kan dit op basis van de al eerder genomen maatregelen (laaghangend fruit) en de risicoverlaging die daarmee gerealiseerd is. Verschillende gesprekken en presentaties zijn nodig om duidelijk te maken dat informatiebeveiliging helpt om de overall doelstellingen van de onderwijsinstelling te realiseren. Aandacht voor de Wet Bescherming persoonsgegevens, aansprakelijkheidsclaims van opdrachtgevers, reputatieschade, het niet 'in control' zijn, zijn doorgaans zaken die tot inzicht kunnen leiden. Het is wenselijk om te wijzen op de ontwikkelingen die in gang zijn gezet door Kennisnet en saMBO-ICT. Deze organisaties vergroten door conferenties en presentaties de bewustwording van de bestuurders. Uiteindelijk ontstaat er betrokkenheid en worden middelen (menskracht en euro's) ter beschikking gesteld voor de uitvoering van het gepresenteerde plan van aanpak.

Fase 4: Projectmatige uitvoering plan van aanpak
Informatiebeveiliging moet beheersbaar gemaakt worden. Daarvoor is aansluiting op de budgetcyclus noodzakelijk. Dus zal er naast het opstellen van beleid en het inrichten van een informatiebeveiligingsorganisatie waarin rollen en verantwoordelijkheden zijn beschreven, ook gewerkt moeten worden aan het inrichten van de Plan-Do-Check-Act-cyclus voor informatiebeveiliging. Dat geeft ook mogelijkheden om delen van het plan van aanpak in de jaarbegroting op te nemen. Verder moet er gewerkt worden aan de inrichting van een risico-methodiek, het incident managementproces, het inrichten van een communicatie- en rapportagestructuur en de uitvoering van diverse deelprojecten uit het plan van aanpak. Het is uiteraard noodzakelijk dat iedere medewerker doordrongen is van de noodzaak van informatiebeveiliging en daar dan ook vanzelfsprekend zijn steentje aan bijdraagt.

Fase 5: Beheer
Het is cruciaal de status van informatiebeveiliging in de instelling te monitoren en, bij geconstateerde tekortkomingen, maatregelen te treffen. Dit kan door het uitvoeren van nieuwe risicoanalyses, door het (laten) uitvoeren van audits, door het inhuren van een 'mystery-guest' die de vinger op de zere plekken legt, etc. Onderdeel van beheer is ook de bevordering van bewustwording. Dat kan middels trainingen via een intranetsite, posters en/of e-learning. Waar het om gaat is dat het beleid bekend wordt gemaakt en wordt gehandhaafd. Dit vergt de nodige aandacht. Mensen kennen de risico's onvoldoende en doen, soms uit behulpzaamheid, dingen die beter achterwege gelaten kunnen worden (social engineering) en daar moet op getraind worden. Controle, naleving en sancties vormen het

onvermijdelijke sluitstuk van een serieus informatiebeveiligingstraject. Interne en externe accountants kunnen daarbij behulpzaam zijn.

Dag 4	**Actieve masterclasses Informatiebeveiliging voor de MBO/HO sector**
Locatie: Carlton Utrecht	
Docent: Marthe Uitterhoeve	**Toelichting op audit**
Tijd: 9.00 – 12.00 uur	
Docent: Victor van Hunnik	**Technische aspecten van de audit (pen test, SURFcert, e.d.)**
Tijd: 13.00 – 16.00 uur	

Doelstelling dag 4:
Op deze dag maken de cursisten kennis met de MBO audit tool. Nadat de tool is toegelicht gaan de deelnemers aan de slag om hun eigen onderwijsinstelling te beoordelen. Een "technische" beoordeling van het netwerk is onderdeel van deze dag. De dag wordt verzorgd door collega's uit de consultancy wereld die MBO instellingen ondersteund hebben bij de implementatie van IBB.
Op het einde van de dag zijn de volgende leerdoelen gerealiseerd:

- De cursist kent de clusteropbouw van de MBOaudit;
- De cursist kan de bewijsvoering (evidence) binnen de MBOaudit toepassen binnen zijn eigen MBO instelling;
- De cursist kan de audit tool "Coable" toepassen;
- De cursist heeft kennis van technische aspecten als PEN test, BCM, SURFcert, etc.;
- De cursist onderkent de menselijke risico's van de ICT afdeling.

Te bestuderen documenten:

- *Hoe? Zo! Informatiebeveiligingsbeleid in het MBO (9 pagina's):*
  Hoofdstuk 6: Hoe wordt het informatiebeveiligingsbeleid toegepast in de praktijk?
  (Bijlage 1- Hoe Zo IBB in het MBO)
- *Leidraad integriteitscode ICT beheerders (9 pagina's)*
  (Bijlage 10- Leidraad integriteitscode)
- *Bijlage 9: Toetsingskader MBO*

Te maken opdrachten:

- De cursist heeft de MBOaudit voor zijn MBO instelling ingevuld zonder daarbij de bewijslast aan te tonen.

Marthe Uitterhoeve:
Marthe is Master Technische Bedrijfskunde, Register EDP auditor en CISSP (informatiebeveiliging) gecertificeerd. Marthe is werkzaam als Principal Consultant bij KZA. Ze heeft 8 jaar werkervaring, met name op het gebied van IT Risicomanagement, IT audit en assurance bij IT outsourcing. Hiervan heeft ze 6 jaar bij Deloitte gewerkt en 2 jaar bij KZA. Ruim de helft van haar opdrachten lagen in de HBO en MBO sector. Dit waren voornamelijk IT audits, IT risk assessments, BIV classificaties en adviesopdrachten. In haar werk is ze proactief, resultaatgericht, enthousiast en verbindend. Ze helpt graag organisaties verder met IT risk & control en denkt mee in pragmatische oplossingen.

Victor van Hunnik:
Proces- en Informatiebeveiligingsanalist (en eigenaar) bij Sense. Mijn specialisme is het analyseren van bedrijfsprocessen en het inzichtelijk maken van processen en de informatiebeveiliging voor alle betrokkenen.
Ik maak in mijn werk gebruik van inmiddels 20 jaar ervaring op het gebied van procesanalyses en informatiebeveiliging. Deze kennis en ervaring heeft ertoe geleidt dat ik aan de hand van een unieke werkwijze praktische producten lever. De werkwijze en de producten leiden tot o.a. inzicht, overzicht en bewustwording bij de betrokkenen wat tot gevolg heeft dat mensen productiever en effectiever gaan werken.
De unieke werkwijze en de producten zijn inmiddels met succes ingezet bij o.a.:

- De overheid
- Het MBO
- Software bedrijven
- En banken

Hoe? Zo! Informatiebeveiligingsbeleid in het MBO.
Pagina 24.

Hoe werkt een IT-Audit?[14]

IT-auditing is het vakgebied dat zich bezighoudt met het beoordelen van de automatisering van de organisatie en de organisatie van de automatisering. IT-auditing is een specialisme binnen het auditing-vakgebied. Het specialisme wordt meer en meer gevraagd bij uitvoering van accountantscontroles.

Tot enkele jaren geleden heette het vakgebied EDP-Auditing, ofwel beoordeling van Electronic Data Processing. De laatste decennia heeft IT-auditing zich verbreed tot de relatie bedrijfsprocessen en ict en richt de aandacht zich minder op het rekencentrum en systeemontwikkelafdelingen. Aanleiding voor het ontstaan van het vakgebied is de toenemende automatiseringsgraad. Doordat de verwerking van administratieve processen steeds meer binnen geautomatiseerde informatiesystemen plaatsvond, kon een accountant veelal onvoldoende zekerheid meer krijgen omtrent de getrouwheid van de financiële verslaglegging van organisaties. Het doorgronden van geautomatiseerde informatiesystemen vergt andere kennis dan alleen bedrijfseconomie en administratieve organisatie.

Hoe wordt het normenkader toegepast?

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.

SURFaudit 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". Het operationele toetsingskader van de SURFaudit is afgeleid van ISO 27002.

Clustering naar zes thema's

SURFaudit heeft de 84 onderdelen ingedeeld in zes clusters. De clustering is gebaseerd op een logische indeling die goed bruikbaar is voor het mbo-onderwijs. Per cluster zijn ook de kwaliteitsaspecten toegevoegd.

Cluster	Onderwerpen (o.a.)	Kwaliteitsaspecten	Betrokkenen
1. Beleid en Organisatie	Informatiebeveiligingsbeleid Classificatie Inrichten beheer	Beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid	College van Bestuur Directeuren
2. Personeel, studenten en gasten	Informatiebeveiligingsbeleid Aanvullingen arbeidsovereenkomst Scholing en bewustwording	Beschikbaarheid en integriteit	College van Bestuur Dienst HR Ondernemingsraad
3. Ruimte en Apparatuur	Beveiligen van hardware, devices en bekabeling	Integriteit en beschikbaarheid	College van Bestuur Ict dienst of afdeling
4. Continuïteit	Anti virussen, back up, bedrijfscontinuïteit planning	Beschikbaarheid	College van Bestuur ict dienst of afdeling Functioneel beheer
5. Toegangs-beveiliging en Integriteit	Gebruikersbeheer, wachtwoorden, online transacties, sleutelbeheer, validatie	Integriteit en 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 informatie-beveiliging

Tabel 2. Clustering naar thema's

Dag 5	Actieve masterclasses Informatiebeveiliging voor de MBO/HO sector
Locatie: MBO Raad Woerden	
Docent: Bart van den Heuvel	**Toelichting en beoordeling IBB van de Universiteit Maastricht**
Tijd: 10.00 – 13.00 uur	
Docent: Leo Bakker	**Presentatie IBB deelnemers + Voorbeeld toetsingskader examineren**
Tijd: 14.00 – 17.00 uur	

Doelstelling dag 5:
Tijdens deze dag presenteren de deelnemers het Informatiebeveiligingsplan van hun instelling. De presentatie is vandaag in handen van een MBO en HO collega.
Tips en trics uit de dagelijkse praktijk worden gepresenteerd. Kennisnet behandelt het toetsingskader examineren op basis van het ISO normenkader. Tot slot wordt de mogelijke vervolgscholing toegelicht.
Op het einde van de dag zijn de volgende leerdoelen gerealiseerd:

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

Te bestuderen documenten:

- *Hoe? Zo! Informatiebeveiligingsbeleid in het MBO (5 pagina's):*
  Hoofdstuk 7: Wat kunnen we sector breed doen?
  (Bijlage 1- Hoe Zo IBB in het MBO)
- *Leidraad Model Acceptable Use Policy voor studenten (8 pagina's)*
  (Bijlage 12- Leidraad AUP studenten)
- *Model Acceptable Use Policy voor studenten (8 pagina's)*
  (Bijlage 13- Model AUP studenten)
- *Leidraad Model Acceptable Use Policy voor werknemers (8 pagina's)*
  (Bijlage 14- Leidraad AUP werknemers)
- *Model Acceptable Use Policy voor werknemers (12 pagina's)*
  (Bijlage 15- Model AUP werknemers)
- *Leidraad functieprofiel informatiebeveiliger (31 pagina's)*
  (Bijlage 16- Functieprofiel informatiemanager)

Te maken opdrachten:

- De cursist presenteert het Informatiebeveiligingsbeleidsplan van zijn MBO instelling.

Vervolgopleidingen:
Security Academy
https://www.securityacademy.nl/opleidingen/cursus-information-security-the-basics.html.
(5 dagen)

Haagse Hogeschool, post-HBO/executive master?, nieuw, start najaar 2014

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

Training Dick Brandt, https://cisomasterclass.nl/

EUROcio CISO master (vanaf voorjaar 2015, CISO, eerste ronde 3 maal 3 dagen)
CISSP (bv
http://www.cibit.nl/nl/ict-opleidingen/opleiding-cissp-information-security/)

Ing. Bart van den Heuvel, CISM; CISO Universiteit Maastricht
Bart is een ervaren expert op het gebied van informatiebeveiliging. Zijn primaire focus ligt op het beleid en de organisatie van informatiebeveiliging. Zo'n 10 jaar geleden heeft hij informatiebeveiliging bij de Universiteit Maastricht als uitdaging opgepakt en inmiddels uitgebouwd tot een samenhangend beleid. Samenwerken is een grote drijfveer. Bart zet zich dan ook enthousiast in om SURFibo op de kaart te zetten als Community of Practice op gebied van IB Beleid binnen de sector Hoger Onderwijs in Nederland.
Zijn technische achtergrond en zijn operationele rol als voorzitter van UM-CERT zorgen ervoor dat Bart een goede verbinding kan leggen tussen strategische, tactische en operationele processen en adviezen kan geven vanuit een pragmatische insteek. Zijn kennisveld is door participatie in lokale en landelijke projecten uitgebreid met o.a. Privacy, Integrale Veiligheid, Identity Management, Audit en Juridische aspecten.

Leo Bakker
Leo is al heel lang werkzaam in en voor het onderwijs. Als docent, curriculum ontwikkelaar, manager, hoofd ICT en de laatste 10 jaar bij Kennisnet als programma manager ict en onderwijs voor het mbo. Hij is als zodanig betrokken bij vele verschillende projecten en programma's rond de inzet van ict in de verschillende onderwijsprocessen: van innovatieve onderwijstrajecten tot ontwikkelen van informatiemanagement in het mbo, van het opzetten van een ict monitor tot het stimuleren van de inzet van groene ict en van professionaliseringstrajecten tot het schrijven van informatieve Hoe?Zo! boekjes voor het onderwijsmanagement in het mbo. Hierbij staat het verbinden van de praktijk met de theorie en het samenwerken en verbinden van verschillende betrokkenen en experts altijd centraal.

Hoe? Zo! Informatiebeveiligingsbeleid in het MBO.
Pagina 34.

Hoe kunnen we samenwerken?

Het bereiken van een voldoende volwassenheidsniveau van informatiebeveiliging zal in eerste instantie in de instellingen zelf plaats moeten vinden. Wel kunnen verschillende gezamenlijke acties worden ingezet om instellingen te ondersteunen, in de vorm van tools, voorbeelden, bijeenkomsten, scholing enz. Wat is er op dit gebied allemaal al ingezet en op welke wijze kunnen instellingen daar gebruik van maken en aan bijdragen?

Samenwerken:

Voor de mbo-sector is een Taskforce Informatiebeveiligingsbeleid (IBB) actief. Deze is samengesteld uit informatiebeveiliging verantwoordelijken, deskundigen en vertegenwoordigers van Kennisnet, SURF en saMBO-ICT. De Taskforce IBB werkt aan het realiseren van een set van gezamenlijke activiteiten die voor het hele mbo-veld relevant zijn in het kader van informatiebeveiligingsbeleid. Daarbij wordt vooral uitgegaan van de expertise die bij het hoger onderwijs door SURF is ontwikkeld. Maar ook bovensectoraal wordt er binnen SION (Samenwerkingsplatform Informatie Onderwijs) samengewerkt aan sector overstijgende vraagstukken over gegevensuitwisseling in het onderwijs.

Draagvlak en bewustwording:

Er wordt in het begin veel aandacht besteed aan het creëren van een breed draagvlak en bewustwording. Niet alle lagen binnen instellingen zijn zich bewust van risico's van het gebruik van digitale middelen. Datzelfde geldt voor landelijke organisaties, zoals de MBO Raad of examenleveranciers.
De activiteiten rondom het realiseren van draagvlak, zijn gericht op twee aspecten:
1. Bewustwording bij landelijke organisaties;
2. Bewustwording bij verantwoordelijken binnen instellingen.

Bij dit tweede aspect richt de aandacht zich vooral op Colleges van Bestuur, op het onderwijsmanagement en op de ondersteunende organisatieonderdelen.

Kennisontwikkeling en kennisdeling:

Om het deskundigheidsniveau van het mbo als sector in het algemeen en van de instellingen specifiek te vergroten, wordt een aantal activiteiten gestart. De sector maakt daarbij volop gebruik van de kennis en ervaring die het hoger onderwijs al eerder hebben opgedaan. In specifieke bijeenkomsten voor kwartiermakers, beveiligingsmedewerkers en security officers, maar ook in bestaande netwerken zoals het informatiemanagersnetwerk zal IBB kennis en ervaring gedeeld worden. Op termijn zou het mbo ook kunnen aansluiten bij de SURF structuur voor IBB, zoals het netwerk SURFibo en beveiligingsconferentie die zij organiseren.
Ook wordt er aandacht aan training en scholing besteed. Er worden masterclasses georganiseerd.

Hoe kunnen we het mbo benchmarken?

Naast deze Hoe?Zo! publicatie is een stappenplan noodzakelijk om informatiebeveiliging daadwerkelijk in de volle breedte te implementeren binnen de instellingen. Op basis van de Starterkit die voor het hoger onderwijs is ontwikkeld, wordt een generiek plan voor de mbo-scholen gemaakt. Dat stappenplan beschrijft wat een instelling kan doen. Onderdeel van dit stappenplan, is een generiek beleidsplan (Informatiebeveiligingsbeleid). Een dergelijk plan is voor de instellingen een referentie (aanzet) om het eigen beleid vorm te geven. Het is geen invuloefening of trucje om snel een document klaar te hebben liggen. Het gaat tenslotte niet alleen om het hebben van documenten of procedures, het belangrijkste is gedrag en cultuur.

Toetsingskader mbo

Naast het hebben van een informatiebeveiligingsbeleid, is het belangrijk te weten wanneer het beleid afdoende is, dus aan welke norm het moet voldoen en hoe dit getoetst kan worden. Een toetsingskader geeft op basis van normen weer aan waar instellingen aan moeten voldoen om op een bepaald volwassenheidsniveau te kunnen scoren. Dit toetsingskader is gebaseerd op de ISO 27002 norm (Code voor Informatiebeveiliging). De mbo-sector sluit hierbij aan.
In het toetsingskader wordt ook de mate, waarin aan een norm moet worden voldaan, beschreven. Dit gebeurt op basis van een 5 puntenschaal. Daarbij wordt onderscheid gemaakt tussen een minimumniveau en het streefniveau. Het toetsingskader is onderdeel van overleg tussen de mbo-sector en het ministerie van OC&W. Doel is om uiteindelijk gezamenlijke normen vast te stellen. Verder wordt er met alle sectororganisaties, het ministerie van OC&W en DUO samengewerkt aan het ontwikkelen van een katern 'Privacy en security', als onderdeel van de Referentie Onderwijs Sector Architectuur (ROSA). Ook is er de standaard Edukoppeling ontwikkeld die beschrijft aan welke eisen de elektronische berichtenuitwisseling van SaaS-leveranciers moet voldoen.