Actieplan

Informatiebeveiligingsbeleid mbo

V.1.0, 14-05-2014
Opdrachtgever: saMBO-ICT

Inhoudsopgave

Documentgeschiedenis

Versie	Datum	Inhoud	Opstellers
0.3	22-4-2014	Conceptversie besproken met netwerk Informatiemanagers	Jan Bartling
0.4	28-4-2014	Aanpassingen doorgevoerd. Versie is voorgelegd aan Kennisnet en Surf	Jan Bartling Leo Bakker
0.5	1-5-2014	Conceptversie die ter info is verzonden aan OCW en wordt voorgelegd aan bestuur saMBO-ICT	Jan Bartling
1.0	14-5-2014	Vastgesteld voor bestuur	Jan Bartling

1. Inleiding

Informatiebeveiliging 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 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. 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. Informatiebeveiligingsbeleid richt zich op al deze aspecten.

De mbo sector is zich zeer bewust van de urgentie en belang van informatiebeveiliging en veel scholen zijn er intussen concreet mee aan de slag of hebben plannen in die richting op stapel staan.. Recente activiteiten rond ICT en Recht, een themaconferentie en recente publicaties geven wel aan dat de sector de nodige stappen wil zetten.

Dit projectplan zal de ingezette weg verder versterken en scholen helpen om hun informatiebeveiliging op orde te krijgen. Instellingen hebben, via de geëigende netwerken van saMBO-ICT en Kennisnet aangegeven graag te willen dat de acties zoals beschreven in dit projectplan worden uitgevoerd. Wat dat betreft is dit een gedragen projectplan. Instellingen willen graag met menskracht en deskundigheid deelnemen en meewerken aan dit project

2. Doelstelling

2.1. Waarom informatiebeveiligingsbeleid

Het onderwerp informatiebeveiliging is van toenemend belang. Vaak wordt dat belang versterkt gevoeld vanwege incidenten. Examenfraude, digitale inbraak of DDos-aanvallen die zorgen voor verstoring van het onderwijs, zijn voorbeelden uit het recente verleden. Veel instellingen zijn op de een of andere manier bezig met het onderwerp. Maar op de vraag of mbo-instellingen hun beveiliging "op orde" hebben kan niemand beantwoorden.

De behoefte om te kunnen aantonen dat de mbo-sector de informatiebeveiliging goed op orde heeft, wordt door zowel de overheid als de instellingen zelf gevoeld. In de eerste plaats moeten we dan afspraken hebben over wat het betekent om "de zaak op orde" te hebben. We moeten een gezamenlijke norm hanteren, een afspraak van instellingen, maar ook met de overheid die eisen kan stellen.

Om inzichtelijk te maken of de sector voldoet aan de norm, is meting nodig. Instellingen kunnen zelf of door derden controleren, waar de norm wordt behaald en welke onderdelen nog voor verbetering vatbaar zijn. Assessment en audits zijn dan het aangewezen middel, naast het delen van best-practices.

Naast de norm en het meten, zullen mbo-scholen zich ook tactisch en operationeel moeten bezig houden met informatiebeveiliging. Het registreren en delen van incidenten moet ingebed zijn in de organisatie. Ook moeten mbo-scholen wat betreft kennis op niveau zijn. Alleen dan is het mogelijk om informatiebeveiligingsbeleid in de praktijk te brengen.

De praktijk ontstaat niet alleen door technologische maatregelen of het afspreken van processen en protocollen. De mens-kant is minstens zo belangrijk. Cultuur en gedrag zij zeer bepalend voor de uitvoering. Bewustwording is dus essentieel op alle niveaus, van het college van bestuur tot de examenmedewerker. Het bewust zijn van risico's moet echter worden onderhouden. Een eenmalige campagne is niet voldoende, mbo-scholen zullen consequent met het onderwerp bezig moeten zijn.

2.2. Doelstellingen

De doelstelling van dit project is:
Het stimuleren en ondersteunen van instellingen bij het ontwikkelen en uitvoeren van informatiebeveiligingsbeleid.

Deze doelstelling kan worden behaald door in te zetten op kennisontwikkeling, bewustwording, ondersteuningsproducten en –activiteiten. Uiteindelijk zullen instellingen in hun reguliere organisatie een continue proces moeten uitvoeren op het terrein van informatiebeveiliging.

Veel instellingen doen al het nodige aan informatiebeveiliging door het uitvoeren van periodieke audits, de aanstelling van een verantwoordelijke op dit terrein (security officer), of door het hebben van een beleidsplan. Het project sluit aan bij deze activiteiten en biedt daarvoor een normenkader, een benchmark en kennisontwikkeling. Daarbij is niet elke instelling even intensief bezig met het onderwerp. De ene mbo-school staat nog aan het begin, terwijl de andere instelling al een voldoende niveau behaalt.

2.3. Betrokken partijen

In het mbo zal gebruik gemaakt gaan worden van materiaal dat beschikbaar is. Het ISO 27002 normenkader is daarbij op hoofdlijnen leidend. Daarnaast worden producten gebruikt die bij Surf voor het hoger onderwijs zijn of worden ontwikkeld. Het is echter belangrijk om te benadrukken dat een document overnemen nog geen

informatiebeveiliging is. Het gaat om een goede implementatie, het onderhouden van de processen en vooral constante aandacht.

In dit project wordt samengewerkt door de volgende partijen:

- Kennisnet
- Surf
- saMBO-ICT
- Mbo-scholen

3. Acties

Het bereiken van een voldoende niveau van informatiebeveiliging zal in eerste instantie in de instellingen zelf plaats moeten vinden. Wel kunnen verschillende acties worden ingezet om instellingen te ondersteunen, in de vorm van tools, voorbeelden, bijeenkomsten, scholing enz. In dit hoofdstuk wordt een opsomming gegeven van deze acties en de producten die worden opgeleverd.

3.1. Samenstellen van Taskforce IBB voor het MBO

De taskforce bestaat uit IT-verantwoordelijken, deskundigen en ondersteunende organisaties:

- IT-verantwoordelijken – 3 personen
- Deskundigen – 3 personen
- Kennisnet – senior adviseur
- Surf – corporate Security Officer
- saMBO-ICT - manager

De taskforce stuurt op het realiseren van de onderstaande acties, maar zal in de loop der tijd ook nieuwe acties of producten oppakken die op dat moment noodzakelijk worden geacht. (zie verder hoofdstuk 5).
In de begroting zijn de kosten voor projectleiding voor het gehele project meegenomen bij dit onderdeel.

3.2. Draagvlak en bewustwording

Er zal de eerste tijd veel aandacht besteed moeten worden aan een breed draagvlak en aan 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 acties rondom het realiseren van draagvlak, zijn gericht op twee aspecten:

- bewustwording landelijke organisaties;
- bewustwording bij verantwoordelijken binnen instellingen.

Bij dit tweede aspect zal het vooral gericht zijn op colleges van bestuur en op het onderwijsmanagement. Daarbij zal worden aangesloten op de acties die instellingen zelf uitvoeren. Om draagvlak binnen de instellingen te stimuleren worden concrete middelen ontwikkeld die informatiebeveiliging op de agenda zetten. Dat kan door het ontwikkelen van voorlichtingsmateriaal, het maken van posters en ander reclame-materiaal. Daarnaast zal een Hoe?Zo! boekje worden gemaakt, gericht op onderwijsmanagers.
De acties zijn gericht op de voortzetting van huidige acties, zoals een thema-conferentie in januari 2014 en bijeenkomsten met colleges van bestuur.

Producten:

- foldermateriaal;
- posters;
- materiaal tbv bewustwording

3.3. Opzetten masterclasses (5x) voor mbo-scholen

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 IT verantwoordelijken, zoals IT-directeuren, Informatiemanagers, enz. Deze masterclasses worden verzorgd door deskundigen op het terrein van Infromatiebeveiliging. Mogelijke 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. Deelnemers kunnen gratis deelnemen, maar verplichten zich tot deelname aan alle vijf de masterclasses (voor een masterclass waar niet aan deel wordt genomen, zal een bedrag van 200 euro in rekening worden gebracht).

Producten:

- Programma masterclasses;
- Studiemateriaal;
- Themasite binnen sambo-ict.nl

3.4. Hoe? Zo! boekje Informatiebeveiliging

In nauwe samenwerking tussen Kennisnet en saMBO-ICT worden jaarlijks een aantal boekjes uitgebracht. Deze zijn concreet gericht op het beantwoorden van vragen die onderwijsmanagers zich stellen. Thema's zijn bijvoorbeeld "ICT en Recht" of "BYOD". In deze serie wordt een boekje uitgebracht "Hoe?Zo! Informatiebeveiliging". Doel van het boekje is de bewustwording van de onderwijsorganisatie, maar ook antwoord op vragen zoals:

- waarom Informatiebeveiliging?
- Wie is er eigenlijk verantwoordelijk voor?
- waarom moet je er als onderwijsmanager iets mee?
- Welke aspecten zijn er van informatiebeveiling allemaal
- Welke juridische zaken spelen er mee
- Hoe pak je het aan binnen de eigen instelling?
- Enz.

Het boekje wordt geïntroduceerd tijdens de september-conferentie van saMBO-ICT in 2014.

Producten:

- Hoe?Zo! boekje Informatiebeveiliging;

3.5. Generiek stappenplan

Naast het Hoe?Zo! boekje is er een stappenplan noodzakelijk om informatiebeveiliging daadwerkelijk en in de volle breedte te implementeren binnen de instellingen. Op basis van het stappenplan dat voor het hoger onderwijs is ontwikkeld, wordt een generiek plan voor de mbo-scholen gemaakt. Dat stappenplan beschrijft wat een instelling moet doen. Onderdeel van dit onderwerp, is een generiek beleidsplan. Een dergelijk plan is voor de instellingen een referentie 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.

Producten:

- Generiek stappenplan;
- Referentiebeleid Informatiebeveiliging.

3.6. Aanpassen normenkader Surf naar mbo

Naast het hebben van een informatiebeveiligingsbeleid, is het belangrijk om te weten wanneer het beleid voldoende is, dus aan welke norm het moet voldoen. Een normenkader geeft de normen weer waaraan instellingen moeten voldoen. Dit normenkader is gebaseerd op de ISO 27002 norm. Het bevat normen met betrekking tot:

- beleid en organisatie;
- personeel en studenten;
- ruimten en apparatuur;
- continuiteit;
- toegangsbeveiliging en integriteit
- controle en logging.

Naast een serie normen, wordt ook de mate waarin moet worden voldaan beschreven aangegeven. Dit gebeurt in de vorm van een 5 puntenschaal.

Onderdeel van deze actie is het vaststellen van de onderwerpen in het normenkader en het gewenste niveau. Daarbij wordt onderscheid gemaakt tussen minimum en streefniveau.
Het normenkader is onderdeel van overleg met de sector mbo en met het ministerie van OCW. Uiteindelijk worden gezamenlijke normen vastgesteld.

Producten:
- Normenkader mbo.

3.7. Aanpassen selfassessmenttool (Coable)

Het meten van de vastgestelde norm is belangrijk voor de instelling om te weten naar welke onderwerpen vooral aandacht naar uit moet gaan. Met behulp van een bestaande tool kan het normenkader getoetst worden. Deze bestaande tool van CoAble zal aangepast moeten worden voor het normenkader, toelichtingen zullen beschreven moeten worden, enz.
Naast het aanpassen van de tool zal deze uitgezet worden bij alle mbo-scholen. 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 ook voor de sector als geheel. Daarmee is het een eerste benchmark voor de mbo-sector.
Instellingen zullen gestimuleerd worden om de tool zelf in te vullen. De sector-resultaten worden gepubliceerd.

Producten:
- Aangepaste tool voor het mbo;
- Benchmark Informatiebeveiliging mbo.

3.8. Inrichten peer-to-peer assessment binnen de sector

Voor een instelling is het selfassessment 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 behaalt dat wordt beoogd. In een peer-to-peer assessment beoordelen instellingen elkaar met betrekking tot het niveau. Er worden peer-to-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 weer een 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 behoort ook bij het leerproces van de mbo sector.
Instellingen (assessors) worden getraind om deze taak goed te kunnen uitoefenen.

Producten:
- Planningsschema assessoren;
- Training assessoren Informatiebeveiliging;
- Benchmark Informatiebeveiliging.

3.9. Gezamenlijke externe IT Audit inkopen en organiseren

Het is de bedoeling om, net als in het hoger onderwijs, het peer-to-peer-assessment 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 een voordeel opleveren in de kosten voor de instellingen zelf.

Het inkopen van deze diensten zal samen met de FSR plaatsvinden. Bij de aanbesteding wordt juridische kennis betrokken. Uiteindelijk zullen de instellingen zelf moeten betalen voor de audit zelf.

Producten:

- Programma van eisen;
- Aanbestedingsdocumenten;
- Aanbod aan instellingen.

3.10. Processclassificatie TripleA en Procesarchitectuur examineren

De TripleA architectuur is een referentie architectuur voor alle mbo-scholen en beschrijft de hoofdprocessen van het onderwijs, van de administratieve processen tot en met stage en logistiek. Het geeft in de vorm van use cases deze processen weer. Hetzelfde geldt meer gedetailleerd voor de examenprocessen in een verdere verdieping geven van TripleA: de Procesarchitectuur Examinering.

In de architecturen van TripleA en de Procesarchitectuur Examinering worden belangrijke processen beschreven, deze architectuurbeschrijvingen kunnen gebruikt worden voor de inventarisatie van risico's. Op basis daarvan kunnen maatregelen genomen worden. Aan de hand van beide architecturen kunnen verschillende niveaus van beveiliging worden beschreven. Deze worden in de architectuur vastgelegd. Met het opnemen van deze niveaus in de architectuur wordt een referentie neergelegd die instellingen kunnen gebruiken bij het beveiligen van eigen systemen.

Producten:

- Analyse van TripleA en Procesarchitectuur Examinering;
- Toevoegen aan deze architecturen van een classificatie per (deel)proces.

3.11. Vervolg op het project

Wanneer het project is afgerond, zal de aanpak en het niveau overeenstemmen met de aanpak en niveau in het hoger onderwijs. Dat betekent dat, volgens afspraak met Surf, aangesloten zal worden bij de structuren van Surf, zoals SurfIbo, SurfAudit en SurfCECRT. Gedurende het project zal Surf meewerken aan de totstandkoming van de producten. Ook zal direct worden gewerkt aan samenwerking op het gebied van tooling, audits, enz. Doel is dat het mbo daarna snel kan aanhaken bij de acties van Surf. Deze acties vinden plaats in reguliere overleggen tussen Surf, Kennisnet en saMBO-ICT.

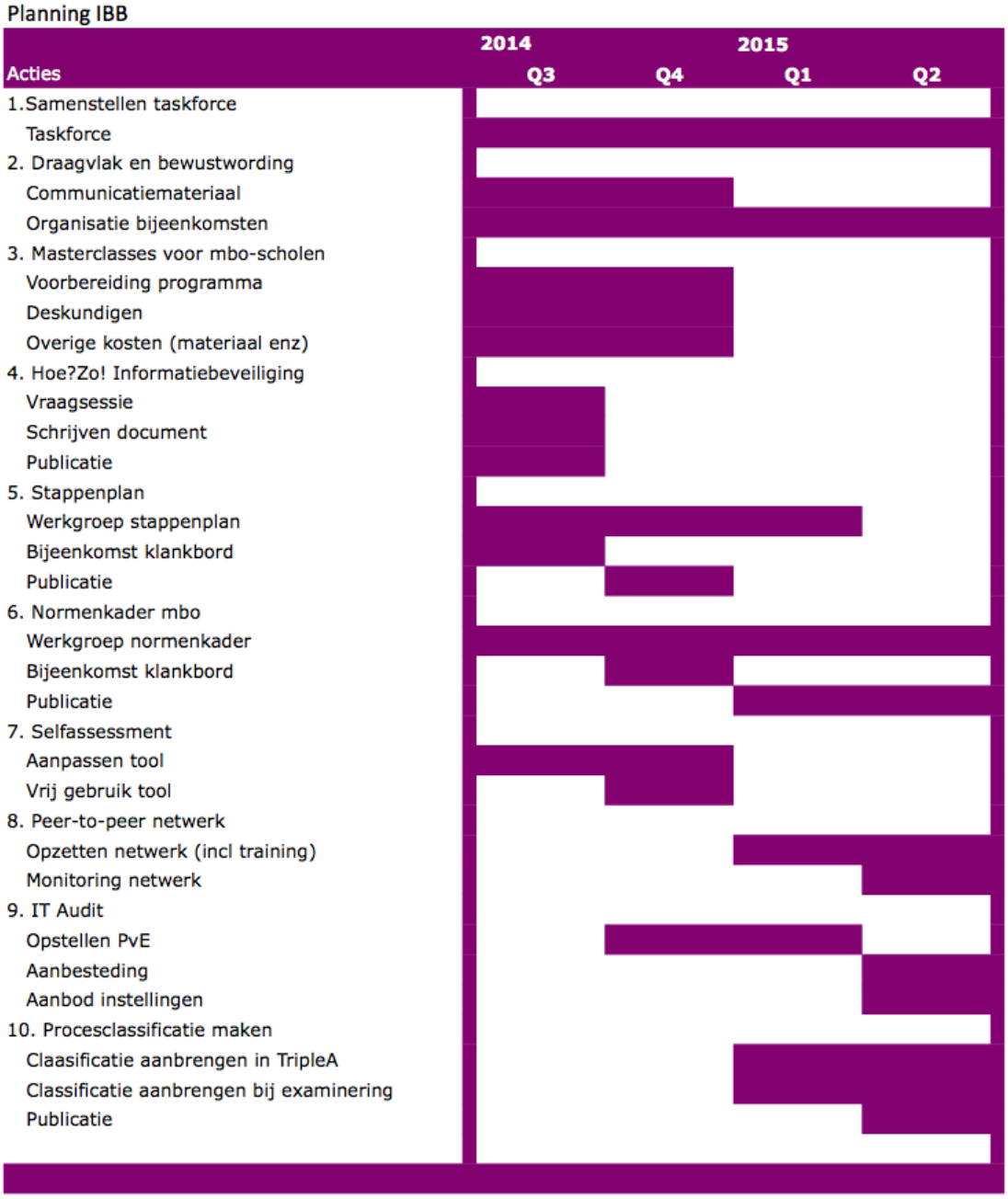
Daarnaast zullen Kennisnet, Surf en saMBO-ICT zorg dragen voor de bundeling van inhoudelijke informatie voor de professionals binnen de scholen. Dat gebeurt in de vorm van themasites en een publicatie waarin alle deelpublicaties zijn opgenomen.

4. Planning

Hoewel er druk is om binnen het mbo snel met resultaten te komen, moet men zich realiseren dat informatiebeveiliging ook te maken heeft met gedrag en cultuur. Bekend is dat dergelijke processen tijd nodig hebben en ook niet het karakter kunnen hebben van een eenmalige actie. Informatiebeveiliging is een continue proces binnen de instellingen en verdient constante aandacht op de niveaus van technologie, processen en gedrag.

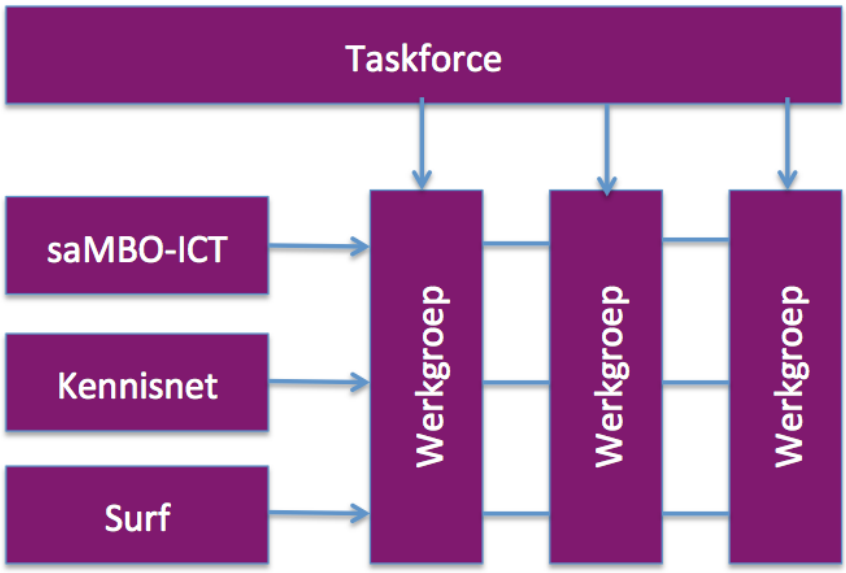
De planning is gebaseerd op acties die het komende cursusjaar zullen worden uitgevoerd. Het project zal n de zomer van 2015 worden afgerond. Instellingen kunnen dan gebruik kunnen maken van de mbo specifieke tools en aanpakken (gebaseerd op het Surf materiaal). De instellingen moeten dan zelf de acties uitvoeren en hun beleid verder ontwikkelen en implementeren.

Planning IBB



5. Organisatie

Voor dit project treedt saMBO-ICT op als penvoerder. De sturing van het project zal plaatsvinden vanuit de taskforce. De taskforce wordt ondersteund door een projectleider. De inzet van de projectleider is opgenomen in de begroting, de uren van de deelnemers aan de taskforce niet. De activiteiten worden in werkgroepen uitgevoerd, die elk een of meerdere producten zullen opleveren. Geprobeerd wordt, door middel van combinaties, gebruik te maken van deskundigheid bij de instellingen. Daarnaast wordt in de samenwerking van saMBO-ICT met Kennisnet en Surf voldoende kennis ingebracht.



6. Financiën

De begroting is in de bijlage opgenomen.

Samengevat is de begroting:

1.Samenstellen taskforce	35.040
2. Draagvlak en bewustwording	17.760
3. Masterclasses voor mbo-scholen	17.820
4. Hoe?Zo! Informatiebeveiliging	15.932
5. Stappenplan	8.596
6. Normenkader mbo	15.864
7. Selfassessment	80.820
8. Peer-to-peer netwerk	29.012
9. IT Audit	21.640
10. Procesclassificatie maken	19.760
Totaal	262.244

In de begroting zijn de uren die mbo-scholen ter beschikking stellen niet meegenomen. Instellingen hebben al aangegeven graag te willen meewerken aan het maken van producten of het inbrengen van deskundigheid.

Alle producten die worden ontwikkeld zijn publiekelijk beschikbaar. Daar zijn voor instellingen geen kosten aan verbonden.