saMBO-ICT

Kennisnet

SURF

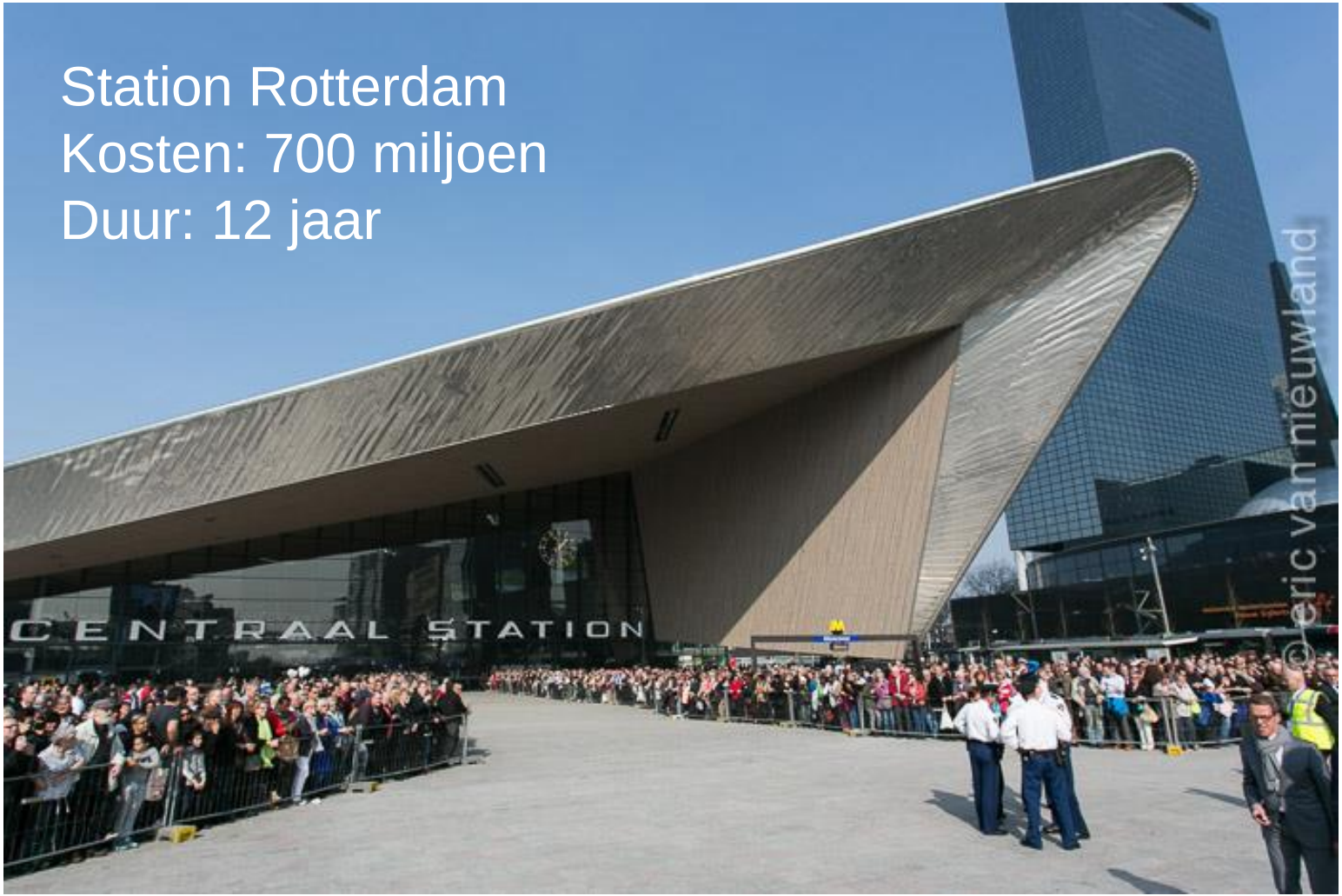
Informatiebeveiliging en privacy beleid binnen de mbo sector
Congres saMBO-ICT te Assen

Auteur Ludo Cuijpers
Datum 5 februari 2016

saMBO-ICT

Inhoud

1. Informatiebeveiliging en privacy in het mbo
2. IBP framework
3. Mens
4. Architectuur
5. Beheer van IBP
6. Audit IBP en de rol van E&Y


Station Rotterdam
Kosten: 700 miljoen
Duur: 12 jaar
CENTRAAL STATION
©eric van nieuwland


Kerkrade Centrum
spoor
2
apg
Topwerkgevers in Limburg
www.banenvanlimburg.nl
sabic
we ict

saMBO-ICT Kennisnet
TASKFORCE MBO INFORMATIEBEVEILIGING

Vooraf

5. Beheer IBP

Risico's IBP

1. Beleid IBP

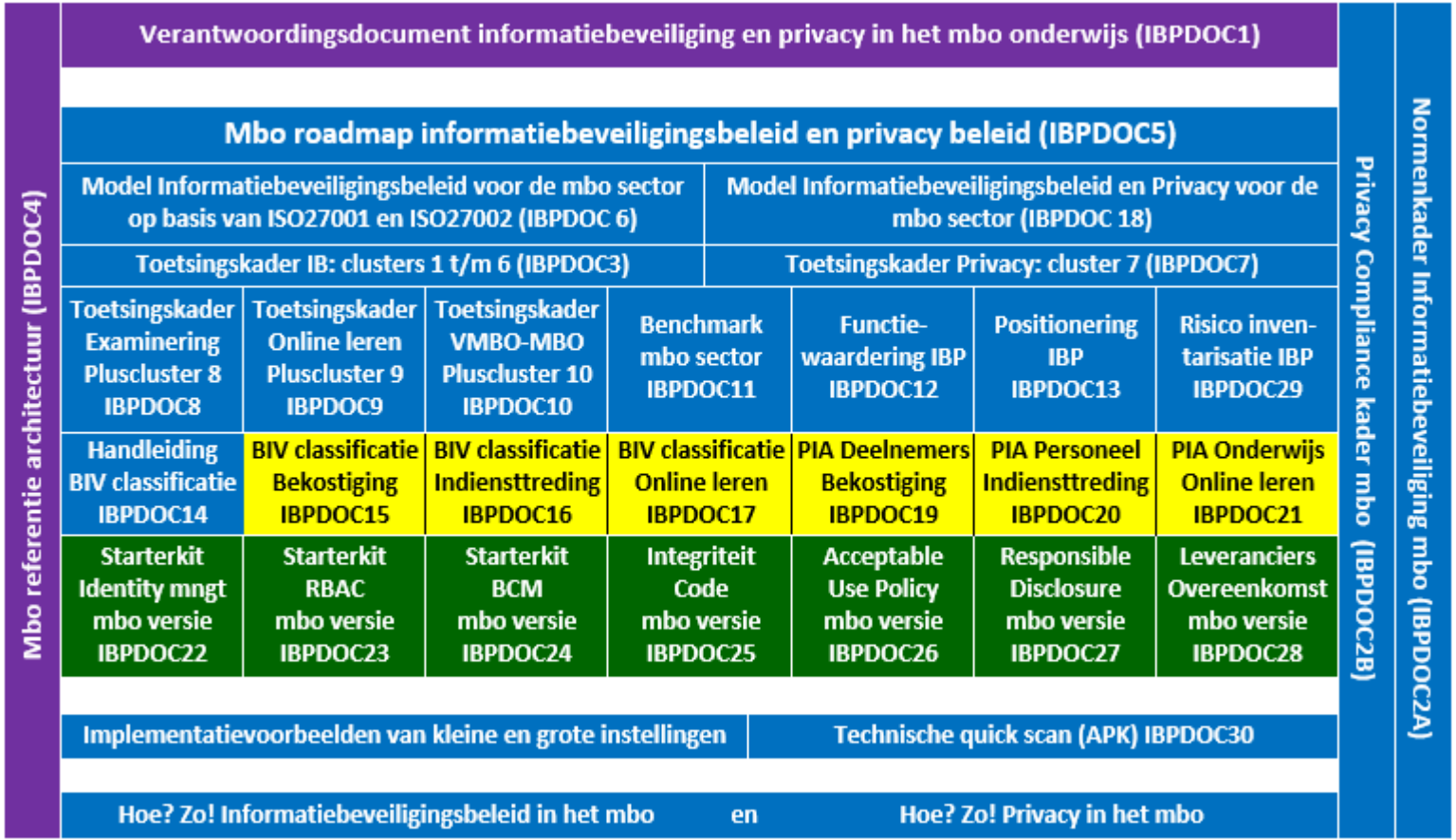
2. Mens

3. Architectuur

4. Audit IBP

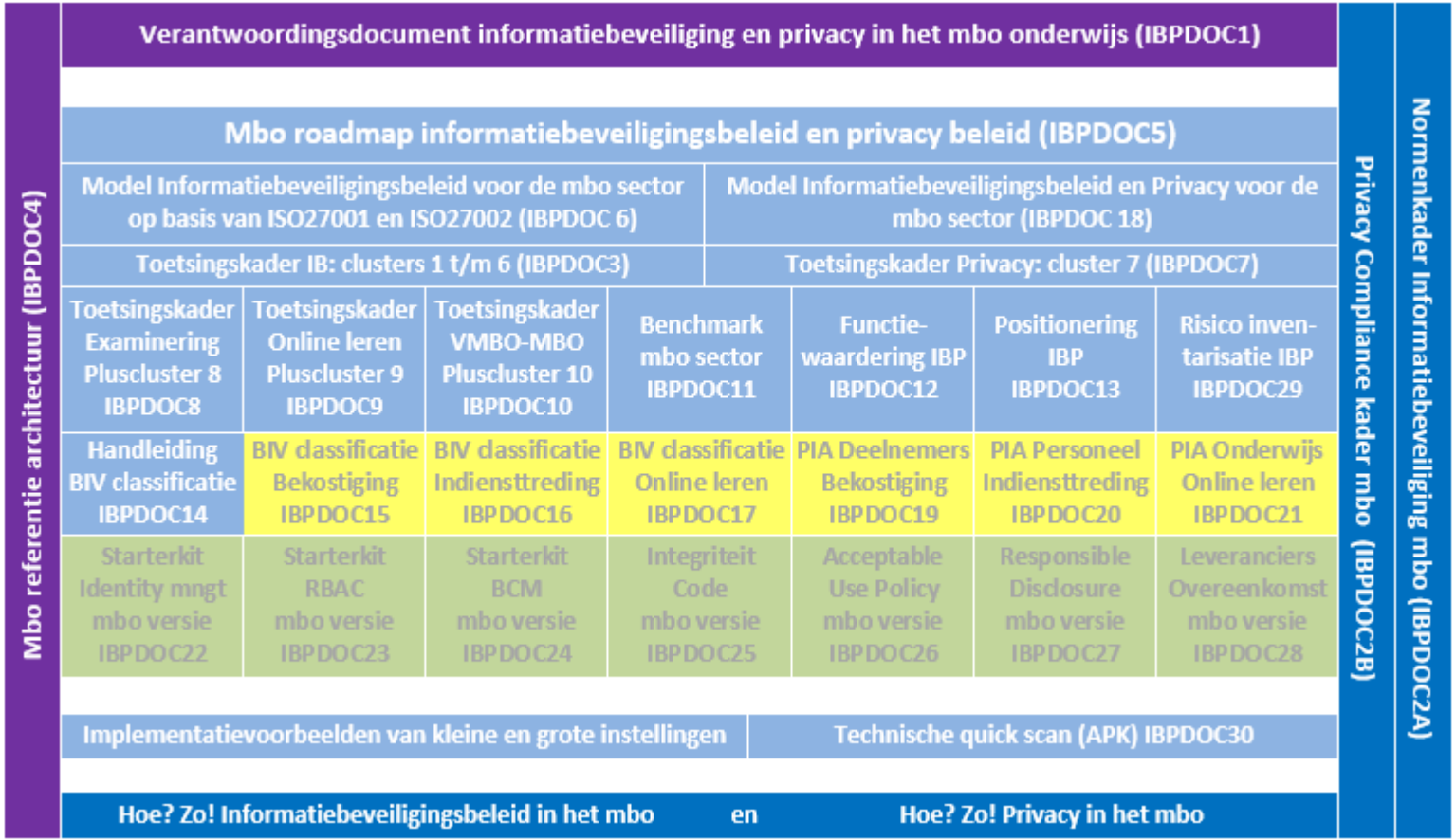
saMBO-ICT Kennisnet
TASKFORCE MBO INFORMATIEBEVEILIGING

IBP framework mbo



saMBO-ICT Kennisnet
TASKFORCE MBO INFORMATIEBEVEILIGING

Afspraken



saMBO-ICT Kennisnet
TASKFORCE MBO INFORMATIEBEVEILIGING

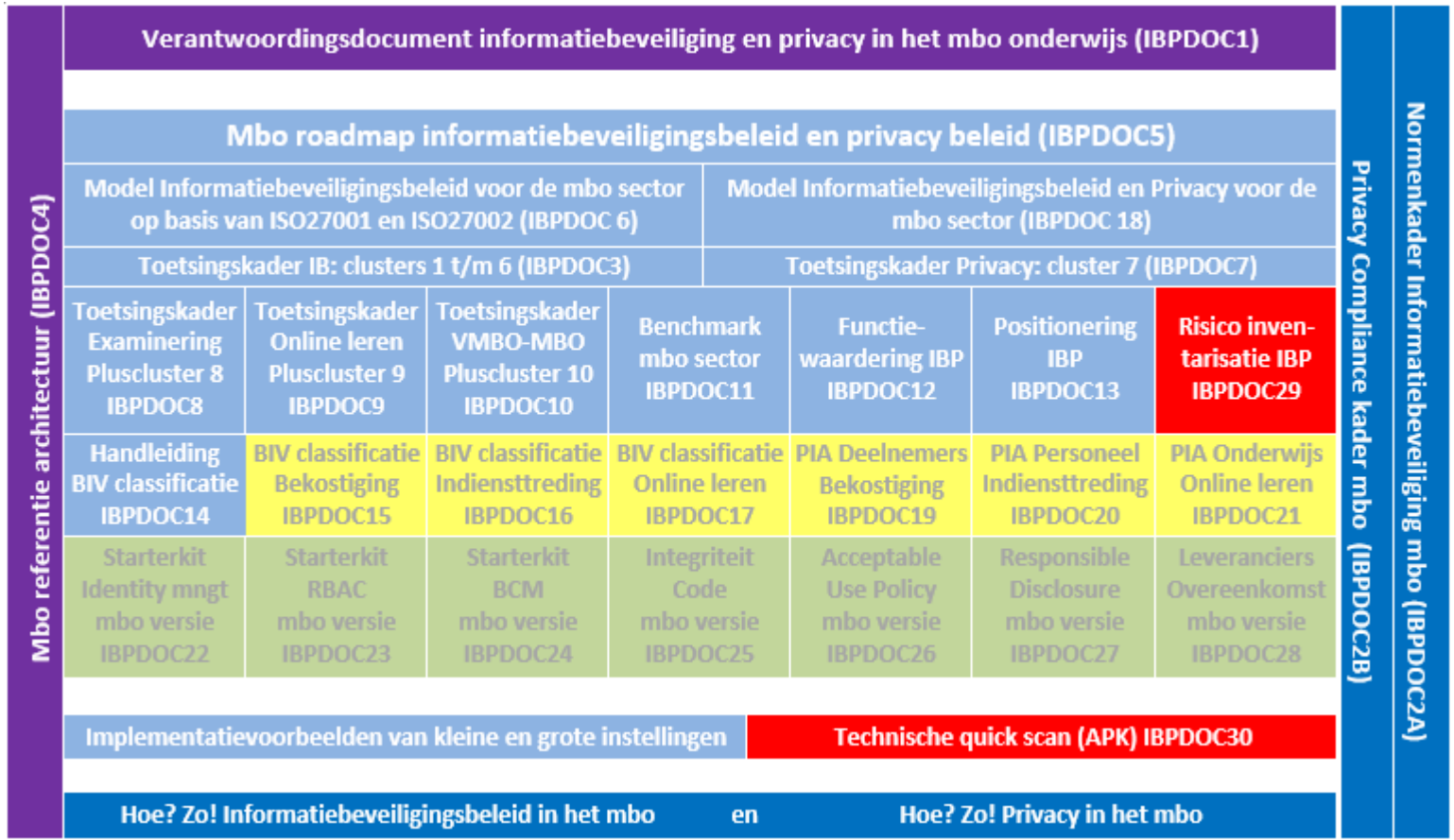
Afspraken

Terugblik

- Medio 2014 problemen examineren
- OCW eist een meetbare aanpak binnen 1 jaar
- MBO Raad versterkt opdracht aan saMBO-ICT
- Opdrachtnemer: Taskforce Informatiebeveiliging
- Partners Taskforce: saMBO-ICT, Kennisnet en SURF
- September 2014: Hoe? Zo! Informatiebeveiliging
- HO aanpak wordt overgenomen (o.a. ISO27001/2)
- Medio 2015 wordt privacy toegevoegd
- Vanaf dan: **i**nformatie**b**eveiliging en **P**rivacy (**IBP**)

saMBO-ICT Kennisnet
TASKFORCE MBO INFORMATIEBEVEILIGING

Risico's

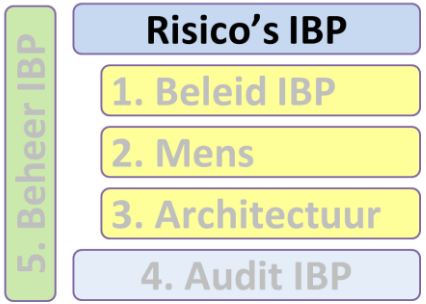


saMBO-ICT Kennisnet
TASKFORCE MBO INFORMATIEBEVEILIGING

Risico’s

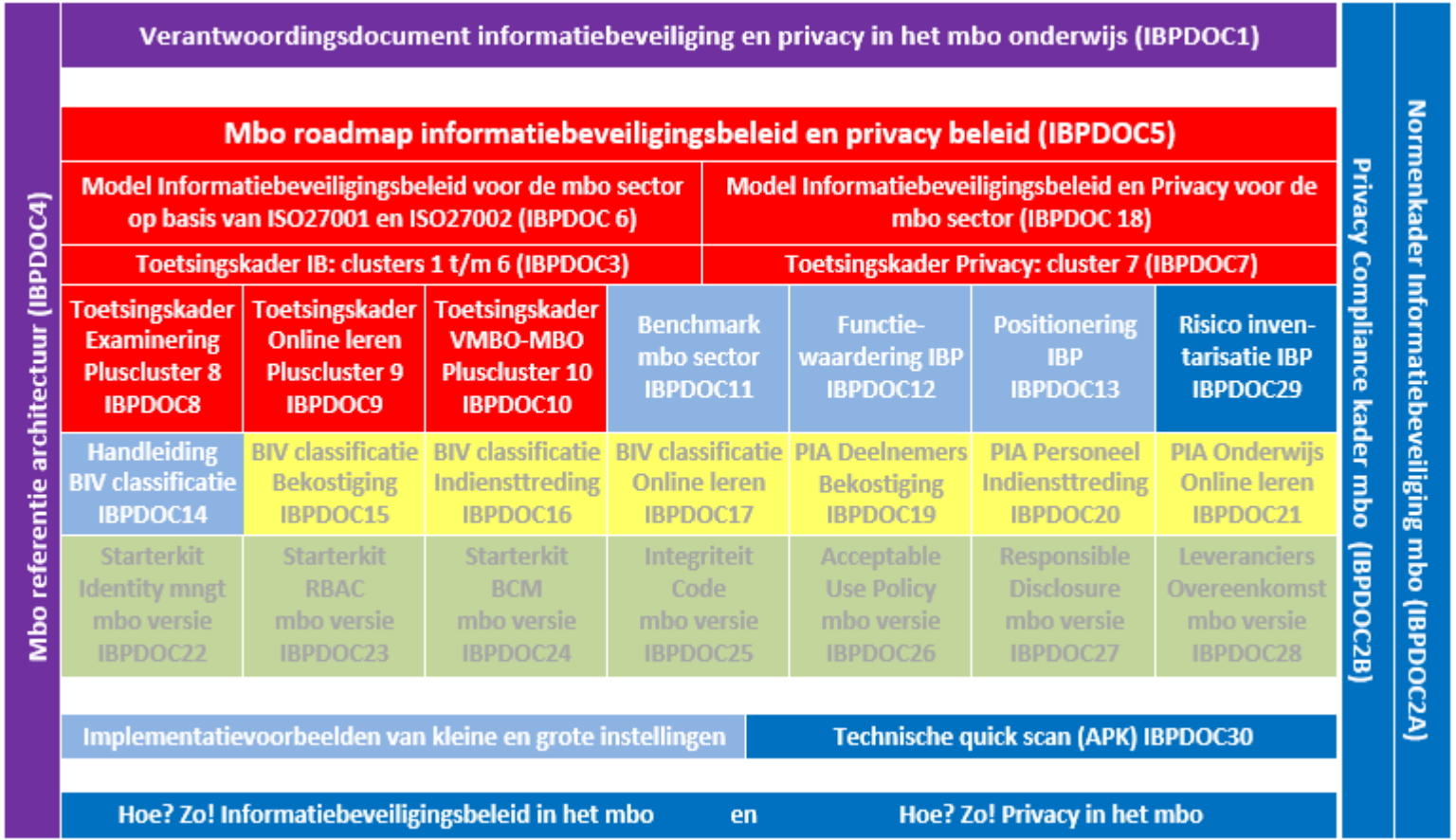
Risico inventarisatie

- 400 risico’s in kaart gebracht
- Risico geclusterd en geplot op ISO27002 (IBPDOC29)
- Handleiding technische QuickScan (IBPDOC30)



saMBO-ICT Kennisnet
TASKFORCE MBO INFORMATIEBEVEILIGING

Beleid

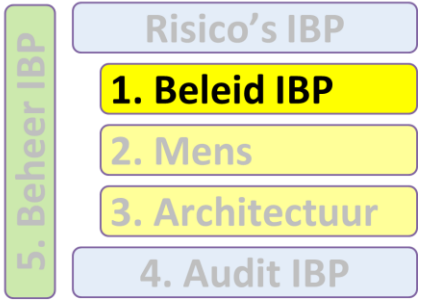


saMBO-ICT Kennisnet
TASKFORCE MBO INFORMATIEBEVEILIGING

Beleid

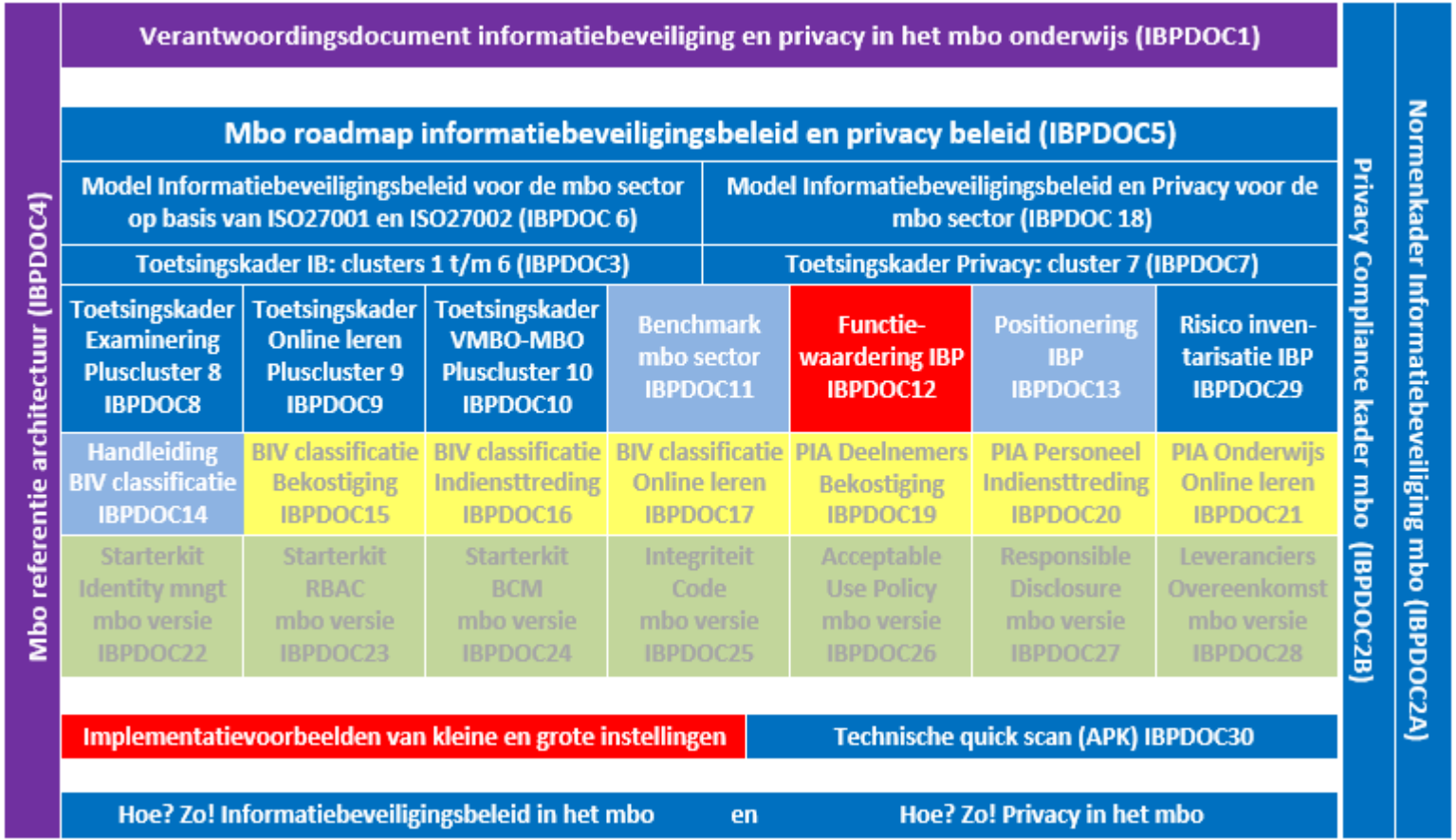
Operationaliseren van het IBP beleid

- Roadmap IBP plus als bijlage PID (IBPDOC5)
- IBP beleidsplan (IBPDOC18)
- Risico geclusterd en geplot op ISO27002 (IBPDOC29)
- Toetsingskader IBP, Privacy en Examineren



saMBO-ICT Kennisnet
TASKFORCE MBO INFORMATIEBEVEILIGING

Mens

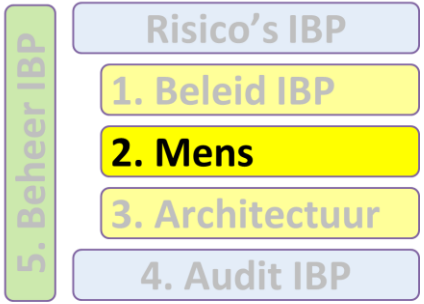


saMBO-ICT Kennisnet
TASKFORCE MBO INFORMATIEBEVEILIGING

Mens

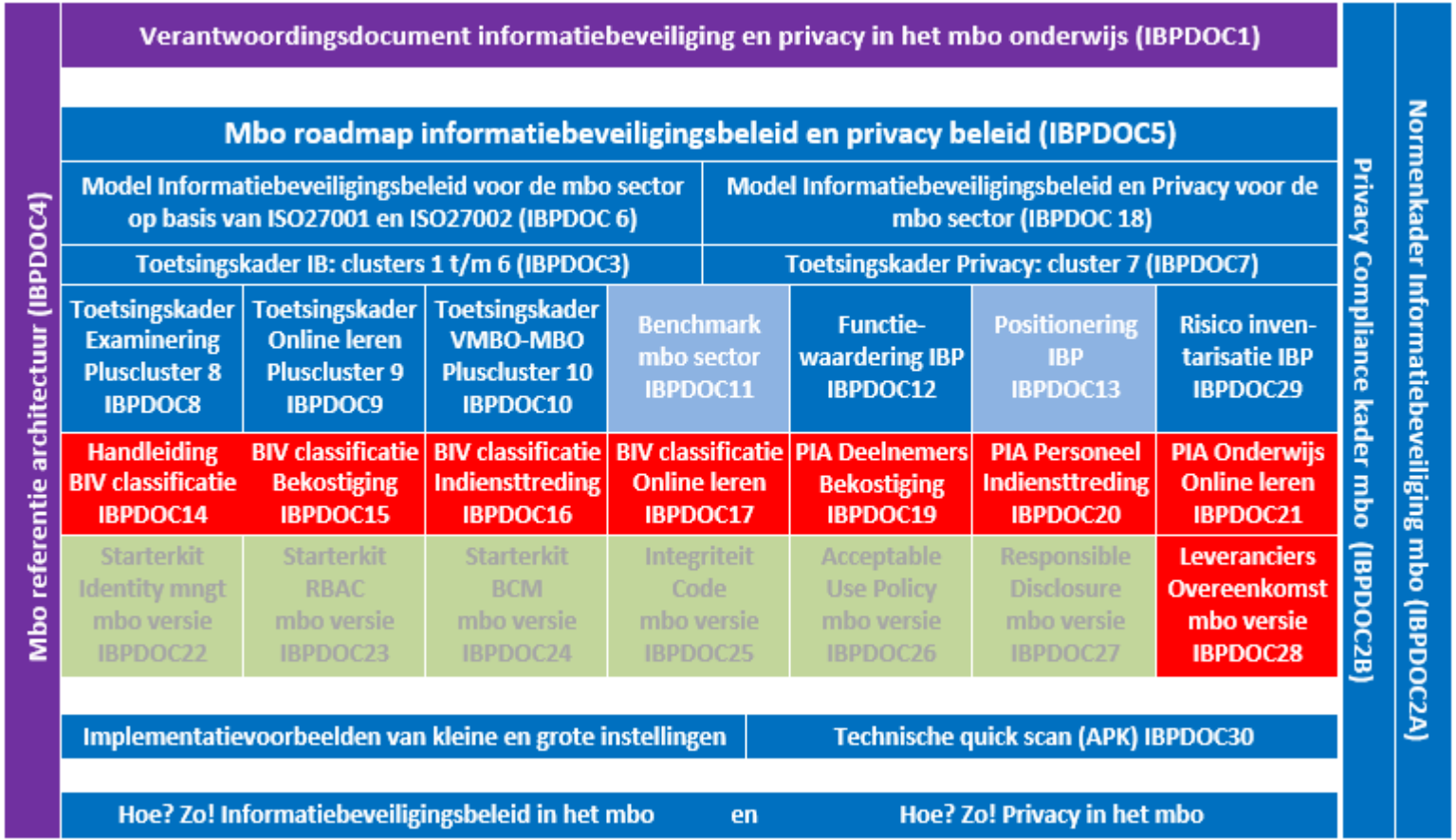
Training en kaders medewerkers

- Masterclasses IBP (5 dagen)
- Masterclasses Privacy (2 dagen)
- Masterclasses Referentie (Enterprise) Architectuur
- Masterclasses Peer Review (laatste 2 zijn gepland)
- Functiebeschrijving IBP manager (IBPDOC12)



saMBO-ICT Kennisnet
TASKFORCE MBO INFORMATIEBEVEILIGING

Architectuur

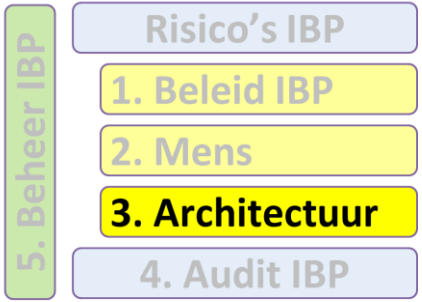


saMBO-ICT Kennisnet
TASKFORCE MBO INFORMATIEBEVEILIGING

Architectuur

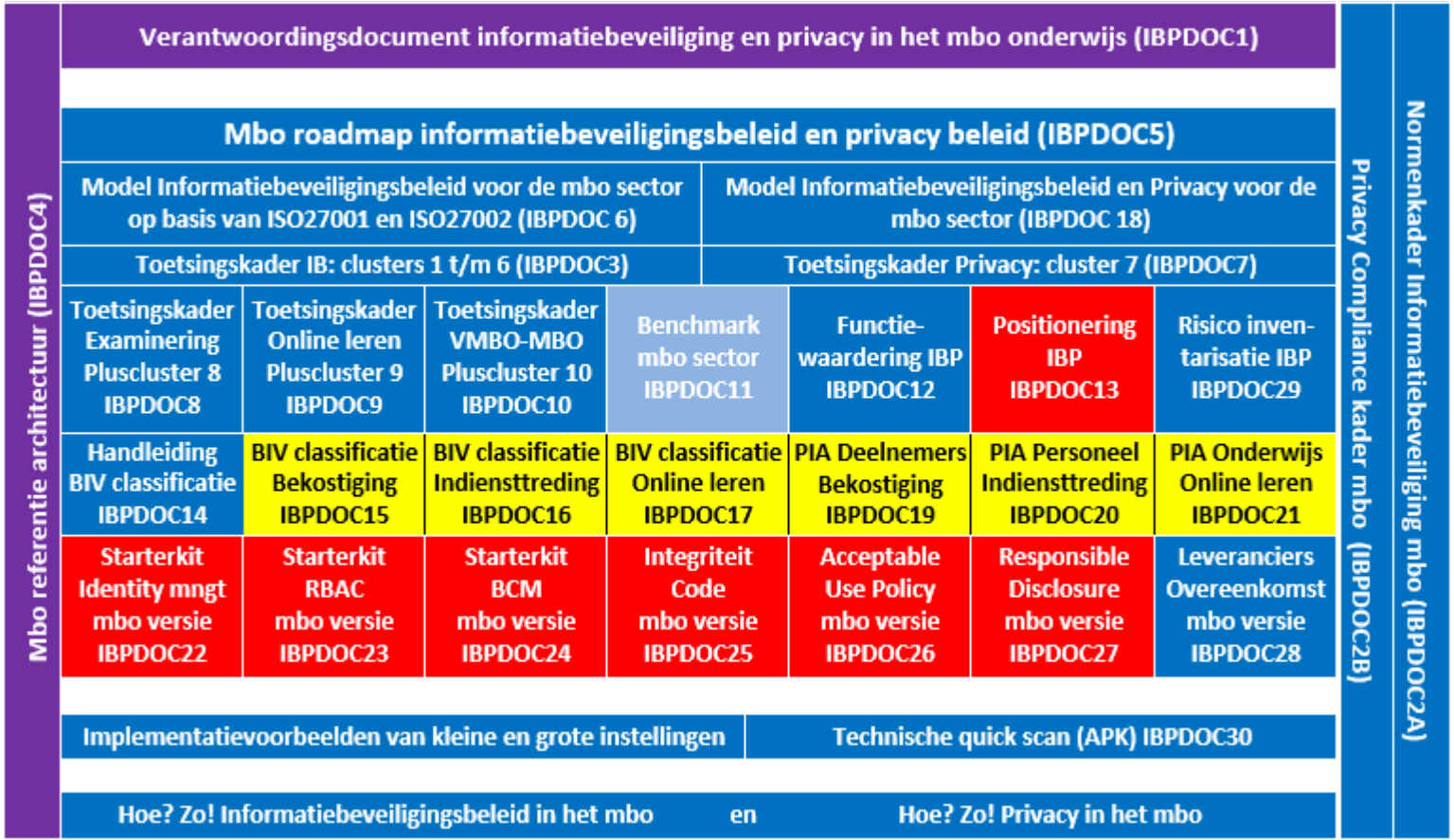
Architectuur uitgangspunten

- Classificatiehandleiding inclusief voorstel (IBPDOC14)
- Voorbeelden BIV classificatie
- Voorbeelden PIA en bewerkersovereenkomsten



saMBO-ICT Kennisnet
TASKFORCE MBO INFORMATIEBEVEILIGING

Beheerorganisatie



saMBO-ICT Kennisnet
TASKFORCE MBO INFORMATIEBEVEILIGING

Beheerorganisatie

Positionering IBP (onderzoek oktober 2015)

Positionering informatiebeveiliging in de mbo sector:

- 1/3 als onderdeel van ICT beheer;
- 1/3 als onderdeel van informatiemanagement of Bestuursbureau (centraal gepositioneerd);
- 1/3 nog niet geregeld.

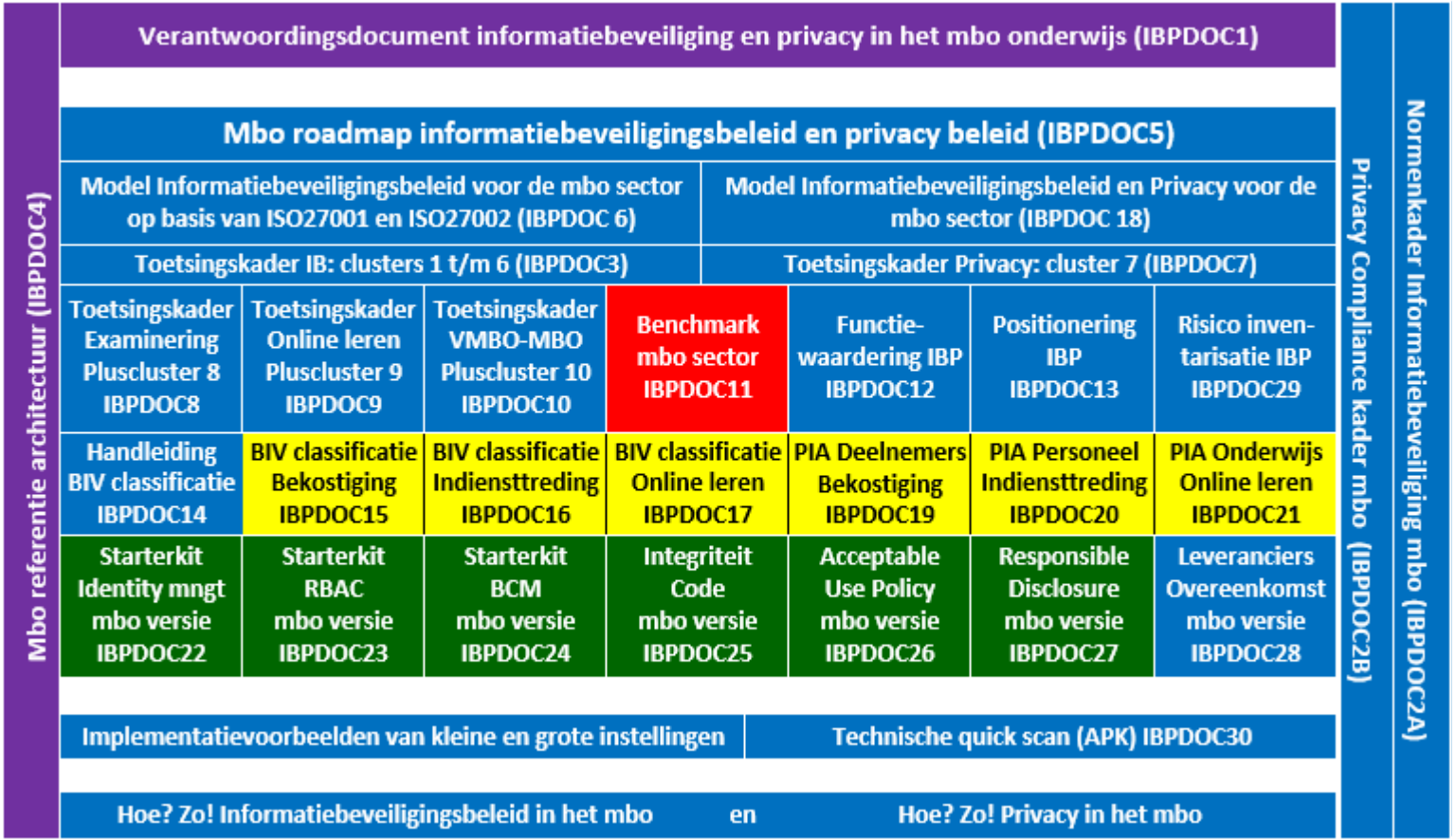
Positionering privacy in de mbo sector:

- ½ heeft privacy “ergens” ondergebracht (zeer divers);
- ½ heeft privacy nog nergens ondergebracht.

5. Beheer IBP
Risico’s IBP
1. Beleid IBP
2. Mens
3. Architectuur
4. Audit IBP

saMBO-ICT Kennisnet
TASKFORCE MBO INFORMATIEBEVEILIGING

Audit



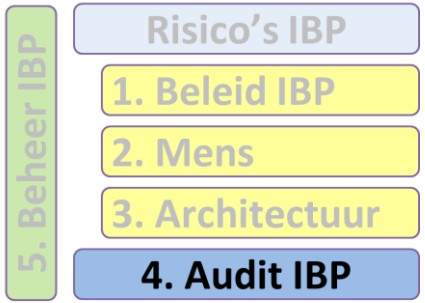
saMBO-ICT Kennisnet
TASKFORCE MBO INFORMATIEBEVEILIGING

Audit

Benchmark mbo sector (19 deelnemers) (IBPDOC11)

Resultaten:

Cluster 1: Beleid en organisatie	**1.7**
Cluster 2: Personeel, studenten en gasten	**1.7**
Cluster 3: Ruimtes en apparatuur	**2.1**
Cluster 4: Continuïteit	**2.0**
Cluster 5: Vertrouwelijkheid en integriteit	**2.0**
Cluster 6: Controle en Logging	**1.6**



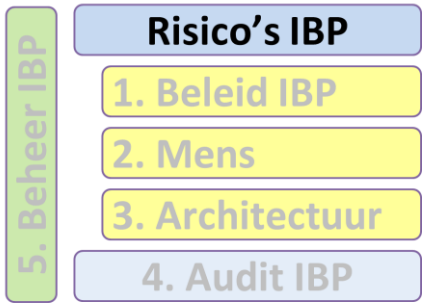
De gemiddelde score van de mbo sector is: **1,9**
Ter vergelijking de score van het Hoger Onderwijs in 2013 was 2,2.

Toekomstige rol E&Y?

saMBO-ICT Kennisnet
TASKFORCE MBO INFORMATIEBEVEILIGING

1. Nulmeting audit

0: Draagvlak bij CvB en vervolgens proceseigenaren, ICT manager, Informatie manager, hoofd functioneel beheer en directeur HR (CvB plus management).
1. Nulmeting audit



saMBO-ICT Kennisnet
TASKFORCE MBO INFORMATIEBEVEILIGING

1. Nulmeting audit

1: Beleid en Organisatie		
MBO nr.	**ISO27002**	**Statement**
1.1	**5.1.1.1**	**Beleidsregels voor informatiebeveiliging:** Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd en goedgekeurd door het bestuur.
1.2	**5.1.1.2**	**Beleidsregels voor informatiebeveiliging**: Het door het bestuur vastgestelde Informatiebeveiligingsbeleid wordt gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.
1.7	**8.2.1**	**Classificatie van informatie:** Informatie behoort te worden geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging.
1.8	**8.2.2**	**Informatie labelen:** Om informatie te labelen behoort een passende reeks procedures te worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.
1.15	**15.1.2**	**Opnemen van beveiligingsaspecten in leveranciersovereenkomsten:** Alle relevante informatiebeveiligingseisen behoren te worden vastgesteld en overeengekomen met elke leverancier die toegang heeft tot IT-infrastructuurelementen ten behoeve van de informatie van de organisatie, of deze verwerkt, opslaat, communiceert of biedt.
1.20	**18.1.4**	**Privacy en bescherming van persoonsgegevens:** Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.

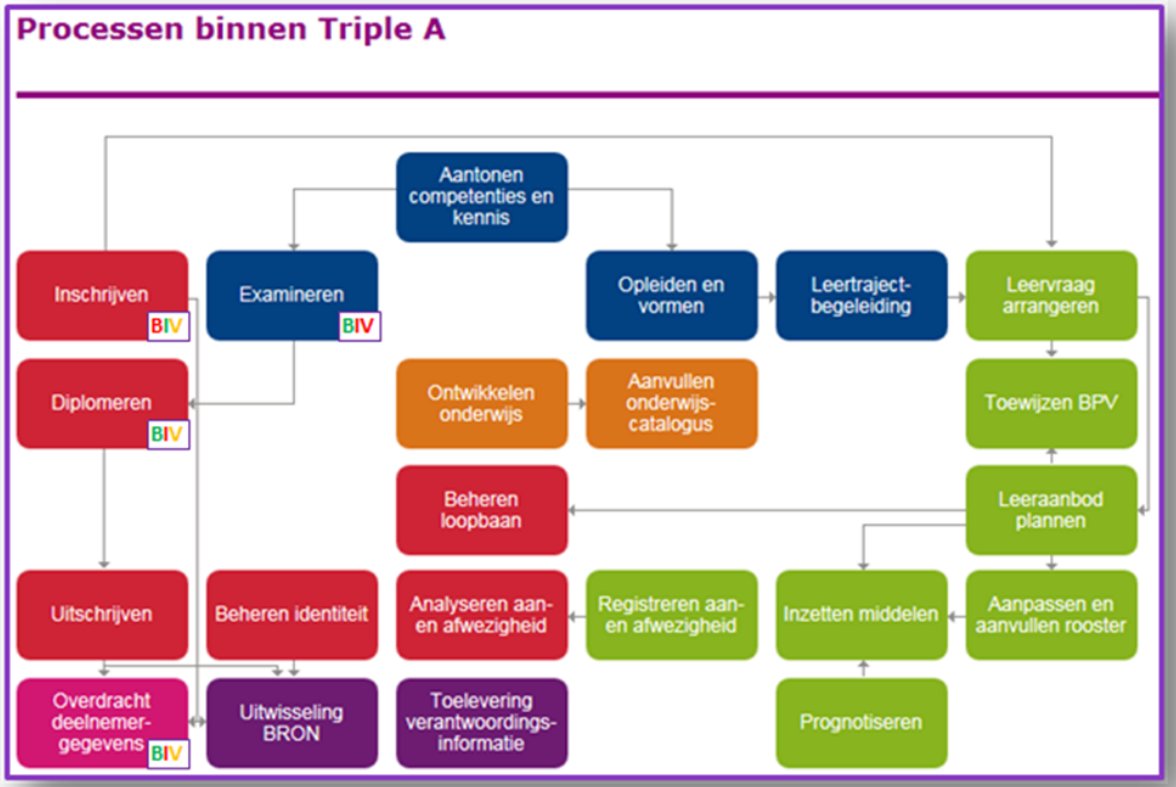
saMBO-ICT Kennisnet
TASKFORCE MBO INFORMATIEBEVEILIGING

1. Nulmeting audit

2: Personeel, studenten en gasten		
MBO nr.	**ISO27002**	**Statement**
2.1	**7.1.2**	**Arbeidsvoorwaarden:** De contractuele overeenkomst met medewerkers en contractanten behoort hun verantwoordelijkheden voor informatiebeveiliging en die van de organisatie te vermelden.
2.2	**7.2.2**	**Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging:** Alle medewerkers van de organisatie en, voor zover relevant, contractanten behoren een passende bewustzijnsopleiding en -training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie.

saMBO-ICT Kennisnet
TASKFORCE MBO INFORMATIEBEVEILIGING

2. Proceslandschap mbo

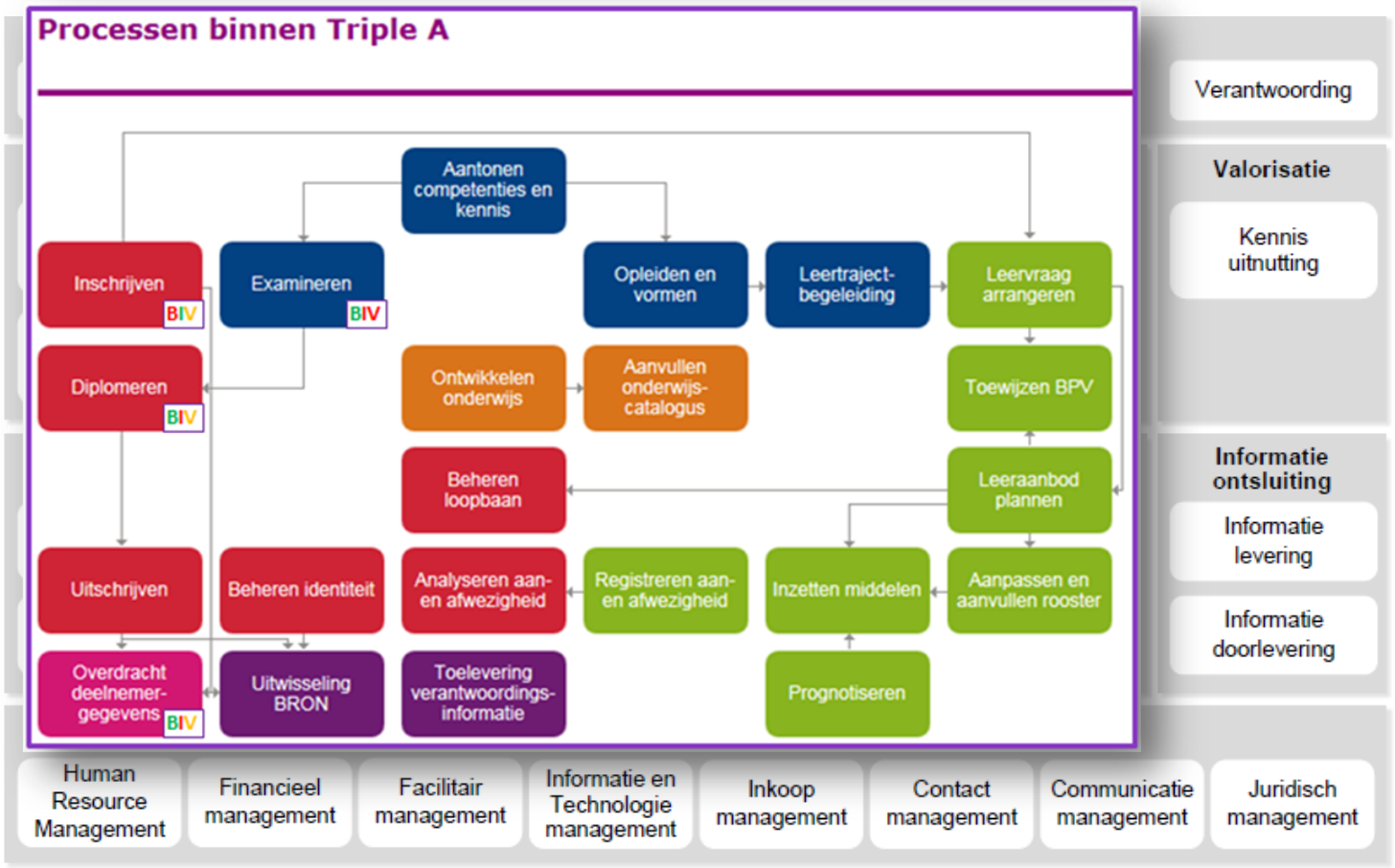


5. Beheer IBP

- Risico's IBP
- 1. Beleid IBP
- 2. Mens
- **3. Architectuur**
- 4. Audit IBP

saMBO-ICT Kennisnet
TASKFORCE MBO INFORMATIEBEVEILIGING

2. Proceslandschap mbo



saMBO-ICT Kennisnet
TASKFORCE MBO INFORMATIEBEVEILIGING

3. IBP training

IBP training voor CvB en management. (4 uur)

- Aanleiding
- Praktijkvoorbeelden
- Kennis privacy
- Classificatie
- Governance
- Samenstelling IBP (crisis-) team

5. Beheer IBP

Risico's IBP
1. Beleid IBP
2. Mens
3. Architectuur
4. Audit IBP

saMBO-ICT Kennisnet
TASKFORCE MBO INFORMATIEBEVEILIGING

4. Beleidsplan IBP

Samen met IBP team “Beleidsplan Informatiebeveiliging en Privacy beleid” opstellen en ter goedkeuring voorleggen aan de Ondernemingsraad.

Onderdelen:

- Inleiding
- Beleidsprincipes informatiebeveiliging en privacy
- Classificatie
- Wet- en regelgeving
- Governance informatiebeveiligingsbeleid
- Melding en afhandeling van incidenten
- Bijlage 1: Privacy reglement deelnemers
- Bijlage 2: Privacy reglement medewerkers

5. Beheer IBP

Risico’s IBP

1. Beleid IBP

2. Mens

3. Architectuur

4. Audit IBP

saMBO-ICT Kennisnet
TASKFORCE MBO INFORMATIEBEVEILIGING

5. Classificatie

Classificatie indeling	Classificatie gevolg
Beschikbaarheid **Laag**	Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende langer dan **1 week** brengt geen merkbare (meetbare) schade toe aan de belangen van de instelling, haar medewerkers of haar studenten of klanten.
Beschikbaarheid **Midden**	Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende langer dan **48 uur** brengt merkbare schade toe aan de belangen van de instelling, haar medewerkers of haar studenten of klanten.
Beschikbaarheid **Hoog**	Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende langer dan **4 uur** brengt merkbare schade toe aan de belangen van de instelling, haar medewerkers of haar studenten of klanten.

Voorwaarde is BCM.

- Verbindingen
- Datacenter
- Mer's en Ser's
- Applicaties
- Data opslag

5. Beheer IBP
Risico's IBP
1. Beleid IBP
2. Mens
3. Architectuur
4. Audit IBP

saMBO-ICT Kennisnet
TASKFORCE MBO INFORMATIEBEVEILIGING

5. Classificatie

Integriteit **Laag**	Het bedrijfsproces staat **enkele** integriteitsfouten toe.	1 Application controls
Integriteit **Midden**	Het bedrijfsproces staat **zeer weinig** integriteitsfouten toe. Bescherming van integriteit is absoluut noodzakelijk.	2 Application controls 3 Manual controls
Integriteit **Hoog**	Het bedrijfsproces staat **geen** integriteitsfouten toe.	4 Application controls 5 Manual controls 6 4 ogen principe

5. Beheer IBP

Risico's IBP

1. Beleid IBP

2. Mens

3. Architectuur

4. Audit IBP

saMBO-ICT Kennisnet
TASKFORCE MBO INFORMATIEBEVEILIGING

5. Classificatie

Vertrouwelijkheid **Laag**	Informatie die toegankelijk mag of moet zijn voor **alle of grote groepen** medewerkers of studenten. Vertrouwelijkheid is gering.	1	Generieke toegangsbeveiliging
Vertrouwelijkheid **Midden**	Informatie die alleen toegankelijk mag zijn voor een **beperkte groep** gebruikers. De informatie is vertrouwelijk.	2	Autorisatiematrix
Vertrouwelijkheid **Hoog**	Dit betreft zeer vertrouwelijke informatie, alleen bedoeld voor **specifiek benoemde personen**, waarbij onbedoeld bekend worden buiten deze groep grote schade kan toe brengen.	3 4 5	Autorisatiematrix Soft token Encryptie

Eventueel toevoegen:

- Hoog: Autorisatiematrix en encryptie
- Zeer hoog: Autorisatiematrix, encryptie en soft token.
- Extreem: Alleen op papier

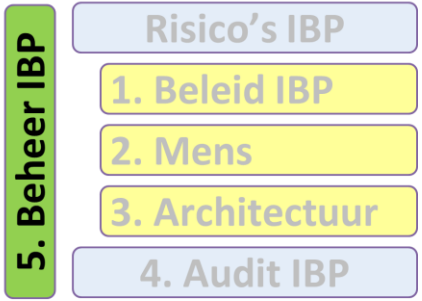
5. Beheer IBP

Risico's IBP
1. Beleid IBP
2. Mens
3. Architectuur
4. Audit IBP

saMBO-ICT Kennisnet
TASKFORCE MBO INFORMATIEBEVEILIGING

6. Benoeming FG

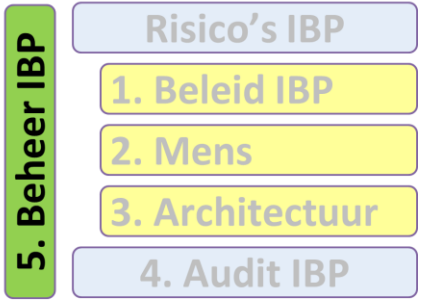
- toezicht houden (2.5 Aansturen IBP Organisatie);
- inventarisaties van gegevensverwerkingen maken (2.5 Aansturen IBP Organisatie);
- meldingen van gegevensverwerkingen bijhouden (2.5 Aansturen IBP Organisatie);
- vragen en klachten van mensen binnen en buiten de organisatie afhandelen (2.5 Aansturen IBP Organisatie);
- interne regelingen ontwikkelen (2.4 Implementeren Algemeen Beleid);
- adviseren over technologie en beveiliging (privacy by design) (2.6 Door ontwikkelen IBP Architectuur) ;
- input leveren bij het opstellen of aanpassen van een gedragscode (2.4 Implementeren Algemeen Beleid).



7. Opzet IBP-team

Het IPCT van <naam MBO instelling> heeft de volgende opdracht:

- Het signaleren en registreren van alle beveiligingsincidenten en datalekken, het coördineren van de bestrijding en het toezien op de oplossing van problemen die tot incidenten hebben geleid of door de incidenten zijn veroorzaakt (of het bieden van ondersteuning daarbij);
- Het geven van voorlichting en het doen van algemene aanbevelingen aan netwerkbeheerders, systeembeheerders, ontwikkelaars en eindgebruikers door het verspreiden van informatie;
- Het leveren van managementrapportages aan directeur ICT, directeur HR en de Informatiemanager over de beveiligingsincidenten en het doen van voorstellen tot betere preventie van of curatie op incidenten



saMBO-ICT Kennisnet
TASKFORCE MBO INFORMATIEBEVEILIGING

7. Opzet IBP-team

Het IPCT bij <naam MBO instelling> levert de volgende diensten bij calamiteiten:

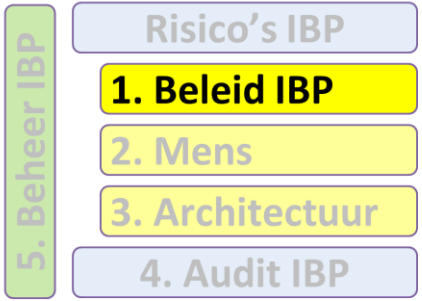
- Afhandelen van binnenkomende e-mails
- Afhandelen van binnenkomende telefoons
- Inrichten en operationeel houden van een meldpunt voor alle beveiligingsincidenten en het coördineren en bewaken van een adequate afhandeling daarvan.
- De bereikbaarheid van de IPCT (tijden/middelen) worden bekend gemaakt aan alle betrokkenen.
- Geven van voorlichting aan IT-gebruikers, –ontwikkelaars en – beheerders over preventie van incidenten en actuele bedreigingen
- Adviseren over instelling brede beveiligingsaspecten
- Periodiek opstellen van managementrapportages;
- Optie: Onderhoudt contacten met SURFcert.

saMBO-ICT Kennisnet
TASKFORCE MBO INFORMATIEBEVEILIGING

8. Bewerkersovereenkomsten en PIA's

1. BRON
2. VO-VMBO-HBO
3. Educatieve uitgeverijen en applicatie leveranciers
4. Gemeenten
5. Stage verlenende organisatie

Tip: doe niets en wacht op Kennisnet en SURF.



saMBO-ICT Kennisnet
TASKFORCE MBO INFORMATIEBEVEILIGING

9. Scholing personeel

1 uur training.

5. Beheer IBP
- Risico's IBP
- 1. Beleid IBP
- **2. Mens**
- 3. Architectuur
- 4. Audit IBP

saMBO-ICT Kennisnet
TASKFORCE MBO INFORMATIEBEVEILIGING

10. Audit in PDCA cyclus

1: Beleid en Organisatie		
MBO nr.	**Maturity**	**Statement**
1.1	**1 naar 3 of 4**	**Beleidsregels voor informatiebeveiliging:** Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd en goedgekeurd door het bestuur.
1.2	**1 naar 3**	**Beleidsregels voor informatiebeveiliging**: Het door het bestuur vastgestelde Informatiebeveiligingsbeleid wordt gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.
1.7	**1 naar 3 of 4**	**Classificatie van informatie:** Informatie behoort te worden geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging.
1.15	**1 naar 3**	**Opnemen van beveiligingsaspecten in leveranciersovereenkomsten:** Alle relevante informatiebeveiligingseisen behoren te worden vastgesteld en overeengekomen met elke leverancier die toegang heeft tot IT-infrastructuurelementen ten behoeve van de informatie van de organisatie, of deze verwerkt, opslaat, communiceert of biedt.
1.20	**1 naar 3**	**Privacy en bescherming van persoonsgegevens:** Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.

5. Beheer IBP
R
1. I
2. Mens
3. Architectuur
4. Audit IBP

saMBO-ICT Kennisnet
TASKFORCE MBO INFORMATIEBEVEILIGING

10. Audit in PDCA cyclus

2: Personeel, studenten en gasten		
MBO nr.	**ISO27002**	**Statement**
2.1		**Arbeidsvoorwaarden:** De contractuele overeenkomst met medewerkers en contractanten behoort hun verantwoordelijkheden voor informatiebeveiliging en die van de organisatie te vermelden.
2.2		**Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging:** Alle medewerkers van de organisatie en, voor zover relevant, contractanten behoren een passende bewustzijnsopleiding en -training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie.
4: Continuïteit		
MBO nr.	**ISO27002**	**Statement**
4.13		**Respons op informatiebeveiligingsincidenten:** Op informatiebeveiligingsincidenten behoort te worden gereageerd in overeenstemming met de gedocumenteerde procedures.
4.14		**Informatiebeveiligingscontinuïteit implementeren:** De organisatie behoort processen, procedures en beheersmaatregelen vast te stellen, te documenteren, te implementeren en te handhaven om het vereiste niveau van continuïteit voor informatiebeveiliging tijdens een ongunstige situatie te waarborgen.

saMBO-ICT Kennisnet
TASKFORCE MBO INFORMATIEBEVEILIGING

Kennisnet

SURF

saMBO-ICT

E l.cuijpers@kennisnet.nl
M 0611627656