ROSA-katern

Privacy en beveiliging

kaders voor het onderwijs

**Versie 0.9.5**

Inhoud

[1. Inleiding 3](#_Toc406068650)

[1.1 Aanleiding 3](#_Toc406068651)

[1.2 Doel 3](#_Toc406068652)

[1.3 Doelgroep 3](#_Toc406068653)

[1.4 Aanpak 4](#_Toc406068654)

[1.5 Scope 4](#_Toc406068655)

[1.6 Verantwoording 5](#_Toc406068656)

[1.7 Positionering 5](#_Toc406068657)

[1.8 Leeswijzer 5](#_Toc406068658)

[2. Raamwerk 7](#_Toc406068659)

[2.1 Kaders: waar wil of moet ik aan voldoen? 7](#_Toc406068660)

[2.2 Normen: hoe voldoe ik hieraan? 7](#_Toc406068661)

[2.3 Compliance of Toezicht: voldoe ik aan de normen? 7](#_Toc406068662)

[2.4 Ketenafspraken: Wat verwacht ik van anderen? 8](#_Toc406068663)

[3. Kaders 9](#_Toc406068664)

[3.1 Basisniveau Privacy en Beveiliging 9](#_Toc406068665)

[3.2 Additionele kaders 10](#_Toc406068666)

[4. Methodiek 11](#_Toc406068667)

[4.1 Aanpak voor formuleren kaders 11](#_Toc406068668)

[4.2 Risico-analyse 11](#_Toc406068669)

[4.3 Risicoclassificatie 13](#_Toc406068670)

[4.4 Toetsingskaders 14](#_Toc406068671)

[Begrippenlijst 17](#_Toc406068672)

[Bijlage: Kaders voor ketenpartijen uit ISO27002:2013 19](#_Toc406068673)

[Bijlage: Maatregelen bij het Basisniveau Privacy en Beveiliging 21](#_Toc406068674)

[Bijlage: Risicoanalyse Toetsen en Examineren 28](#_Toc406068675)

[Bijlage: Gegevenskaarten ketenproces Toetsen en Examineren 31](#_Toc406068676)

# 1. Inleiding

## 1.1 Aanleiding

De informatiehuishouding binnen het onderwijs verloopt steeds meer digitaal. Daardoor groeit de behoefte om op een verantwoorde en betrouwbare wijze binnen de keten gegevens te gebruiken en uit te wisselen. Als (vertrouwelijke) gegevens niet goed beschermd worden dan brengt dat risico’s met zich mee[[1]](#footnote-1). Dit kan leiden tot diverse vormen van schade of beschadiging[[2]](#footnote-2):

Voor de onderwijsinstelling:

* boetes wegens het overtreden van wet- en regelgeving;
* imagoschade, met als gevolg dalende leerlingaantallen en gederfde inkomsten;
* verstoorde onderwijs(logistieke) processen doordat gegevens niet kloppen of doordat processen niet goed verlopen;
* gederfde inkomsten door bekostiging op grond van onjuiste gegevens;
* extra administratieve lasten door verscherpt toezicht;
* extra administratieve lasten en/of boetes als gevolg van juridische geschillen.

Voor de onderwijsvolger:

* verlies aan zelfstandigheid, bijvoorbeeld door beperking van de mogelijkheid om handelingen uit te voeren: onder toezichtstelling, ouderlijke inmenging, uit-huis-plaatsing;
* stigmatisering, bijvoorbeeld op een bepaalde manier behandeld worden op basis van bepaalde kenmerken: dommerik, hulpbehoevend, beperkt, kampbewoner;
* ongelijke behandeling, bijvoorbeeld in verband met achtergrond of land van herkomst;
* beperking van bewegingsvrijheid, bijvoorbeeld beperkt worden in de toegang tot bepaalde gebieden, etablissementen of ruimtes op basis van gedragingen;
* aantasting van eigenwaarde, bijvoorbeeld door afbreuk aan persoonlijkheid;
* ongewenst vindbaar zijn, bijvoorbeeld door uit de ouderlijke macht gezette ouders.

Om deze risico's af te dekken moeten onderwijsinstellingen samen met andere ketenpartijen dus maatregelen nemen die zorgen voor veilig gebruik van - vaak privacygevoelige - gegevens. Die maatregelen zijn voor verschillende onderwijssectoren grotendeels identiek. Het is daarom belangrijk dat er kennis gedeeld wordt en dat ketenpartijen samen optrekken om te werken aan een veiliger keten.

## 1.2 Doel

Het doel van het katern Privacy en beveiliging is om voor de gehele keten kaders te bieden op het gebied van privacy en beveiliging voor ICT-projecten die binnen het onderwijs uitgevoerd worden. Deze kaders zijn gebaseerd op risico’s die relevant zijn voor informatiebeveiliging in het onderwijsdomein.

## 1.3 Doelgroep

Het katern maakt onderdeel uit van de Referentiearchitectuur Onderwijs (ROSA), waarin ook andere architectuurkaders staan geformuleerd die betrekking hebben op *bovensectorale* gegevensuitwisseling binnen het onderwijs. Met bovensectoraal bedoelen we gegevensuitwisseling tussen onderwijssectoren onderling of de uitwisseling met DUO of andere gemeenschappelijke marktpartijen, zoals uitgeverijen en distributeurs.

Met het katern hebben opdrachtgevers binnen de keten (op termijn) een instrument in handen om op basis van relevante risico's de juiste kaders te stellen aan de voorziening voor het veilige digitaal uitwisselen van gegevens binnen de onderwijsketen.

## 1.4 Aanpak

Risico’s kunnen per type gegeven of proces verschillen. Daarom maken we in dit katern onderscheid tussen kaders die voor alle situaties van toepassing zijn en additionele kaders die betrekking hebben op specifieke processen of gegevens (werkingsgebieden).

De kaders zijn vastgesteld op basis van risico-analyse. Dit katern verschaft een methodiek op basis waarvan het katern verder doorontwikkeld kan worden. Voor de eerste vulling van het katern is een risico-analyse uitgevoerd voor het ketenproces Toetsen en examineren.

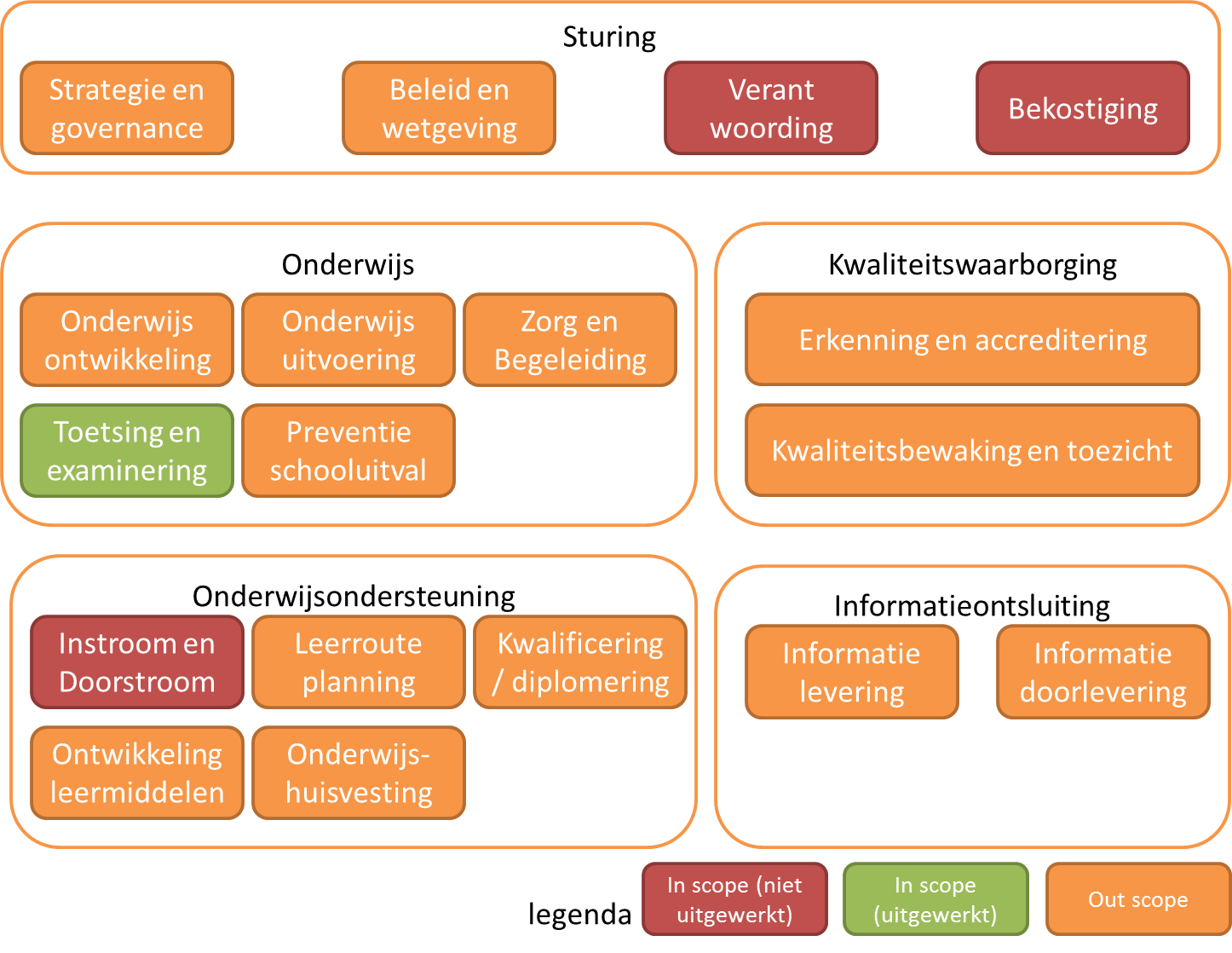
## 1.5 Scope

Voor de te nemen maatregelen verwijzen we naar diverse toetsingskaders, waarmee kan worden vastgesteld of aan de benodigde beheersmaatregelen wordt voldaan. Deze toetsingskaders maken geen onderdeel uit van het katern, maar worden of zijn al wel ontwikkeld voor het onderwijs

Het kader is nog niet af, maar dient in dit stadium vooral als instrument om op een gestructureerde wijze het juiste gesprek met ketenpartijen te voeren. Door het instrument in te zetten binnen ICT-projecten binnen de keten, ontstaat vanuit de ketenprojecten waarschijnlijk een steeds breder (gedragen) gemeenschappelijk kader.

Het kader is alleen van toepassing op gegevensuitwisseling tussen meerdere ketenpartijen binnen het onderwijsdomein. Momenteel zijn de volgende ketenprocessen of ketenfuncties (figuur 1) in scope:

1. Toetsen en Examineren (uitgewerkt)
2. Bekostigen (nog niet uitgewerkt)
3. Digitaal aanmelden en inschrijven (nog niet uitgewerkt)
4. Doorstroom monitoren (nog niet uitgewerkt)
5. Horizontaal verantwoorden (nog niet uitgewerkt)



Figuur 1: Ketenfuncties

## 1.6 Verantwoording

Het katern Privacy en beveiliging is opgesteld binnen het Samenwerkingsplatform Informatie Onderwijs (SION), in samenwerking met SURF, Kennisnet, DUO en het ministerie van OCW. Het katern maakt onderdeel uit van de Referentiearchitectuur Onderwijs (ROSA). De inhoud van het katern is afgestemd met andere initiatieven binnen de keten, waaronder de werkgroep IBO in het hoger onderwijs en de taskforce informatiebeveiliging in het mbo.

## 1.7 Positionering

|  |  |
| --- | --- |
| Normenkader  (ISO 27001:2013 en 27002:2013) | Deze internationale standaard wordt als basis gebruikt voor het ROSA kader en helpt ketenpartijen bij het nemen van maatregelen om te voldoen aan informatiebeveiligingseisen. |
| ROSA kader | Dit betreft een superset van bovenstaand normenkader, aangevuld met kaders vanuit risico-analyses in het onderwijsdomein. Daarbij wordt onderscheid gemaakt tussen een ketenbreed Basisniveau Privacy en Beveiliging, bestaande uit kaders die voor het hele onderwijsdomein gelden, en additionele kaders voor specifieke werkingsgebieden. De informatiebeveiligingsdoelstellingen uit de ISO-standaard zijn in het Basisniveau opgenomen als kaders voor informatiebeveiliging door individuele ketenpartijen. |
| Toetsingskader | Op basis van de geselecteerde maatregelen uit het normenkader (ISO 27001 en ISO 27002), wordt er specifieke bewijslast (evidence) toegevoegd op een aantal volwassenheidsniveaus. |

## 1.8 Leeswijzer

Het katern beschrijft eerst de samenhang en verschillen tussen de verschillende initiatieven op het gebied van privacy en security binnen het onderwijs (hoofdstuk 2 Raamwerk). Daarna wordt een vertaling gemaakt van wetgeving en risico-analyse naar een Basisniveau Privacy en Beveiliging en additionele kaders op basis waarvan relevante normen of maatregelen kunnen worden afgeleid (hoofdstuk 3 Kaders).

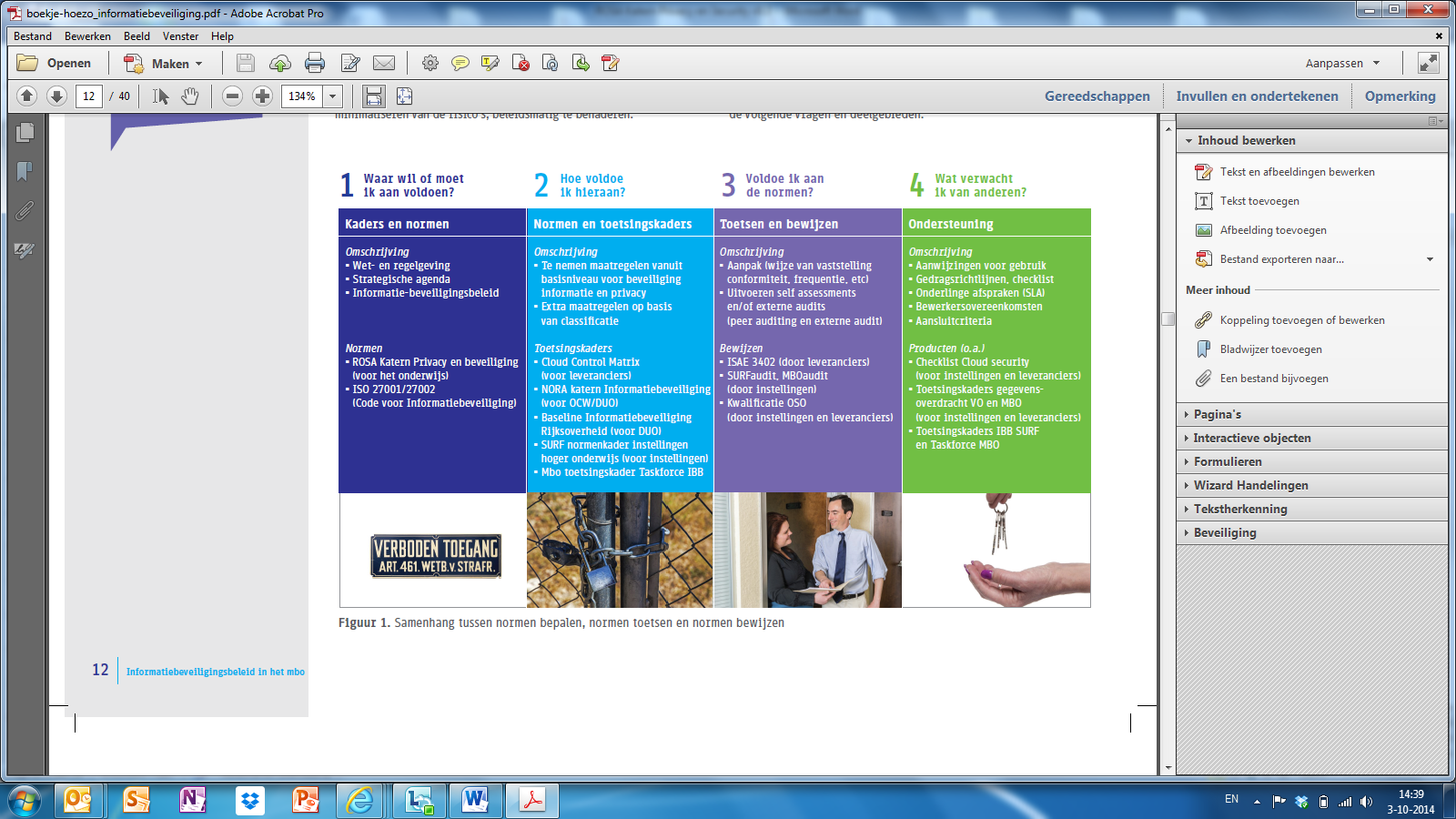
Voor het aanvullen van deze kaders biedt het katern een methodiek om het basisniveau en de additionele kaders aan te vullen en te vertalen naar het normen- en toetsingskader, waarbij ook aandacht wordt besteed aan de verwijzing naar bestaande initiatieven (hoofdstuk 4 Methodiek).

Na hoofdstuk 4 vindt u een begrippenlijst, waarin de in dit document gebruikte begrippen worden verduidelijkt, en een aantal bijlagen:

* de bijlage Kaders voor ketenpartijen uit ISO27002:2013 beschrijft de doelen uit ISO 27002 die, vanuit het Basisniveau Beveiliging, als kader gelden voor de informatiebeveiliging binnen individuele ketenpartijen;
* de bijlage Maatregelen bij het Basisniveau Privacy en Beveiliging beschrijft een selectie van beheersmaatregelen uit ISO27002 :2013 die passen bij de kaders uit het basisniveau;
* de bijlage Risicoanalyse Toetsen en Examineren beschrijft de toepassing van de methodiek voor risicoanalyse op het ketenproces Toetsen en Examineren;
* de bijlage Gegevenskaarten ketenproces Toetsen en Examineren toont detailinformatie voor de verschillende soorten gegevens die in het ketenproces Toetsen en Examineren worden uitgewisseld.

# 2. Raamwerk

Bij informatiebeveiliging kunnen er op verschillende niveaus vragen worden gesteld over de inrichting hiervan. Het gaat hierbij om de volgende vragen en deelgebieden:



*Figuur 2 Raamwerk initiatieven Privacy en beveiliging*

## 2.1 Kaders: waar wil of moet ik aan voldoen?

In dit katern zijn generieke (juridische) kaders opgenomen op het gebied van beveiliging en privacy die gelden voor alle onderwijssectoren. Deze gemeenschappelijke kaders zijn gebaseerd op wet- en regelgeving en risico-analyse. Vanuit deze kaders, kunnen per onderwijssector of ketenpartij (bestaande) normen of toetsingskaders worden afgeleid. De kaders sluiten daarom nauw aan bij de ISO-standaard 27002, waarvan al veel initiatieven binnen en buiten de onderwijsketen gebruik maken. Door de gemeenschappelijke kaders ontstaat er meer samenhang tussen deze initiatieven.

2.2 Normen: hoe voldoe ik hieraan?   
De normen of toetsingskaders kunnen per sector of ketenpartij verschillen. Het gaat hierbij om een verdere concretisering van de kaders uit dit katern, die aantoonbaar of toetsbaar gemaakt zijn.

Voor het informatiebeveiligingsbeleid in het mbo en ho zijn het SURF normenkader en het daarvan afgeleide mbo-toetsingskader leidend. Voor leveranciers is er vanuit SION een certificeringsschema Edukoppeling opgeleverd, dat kan dienen als toetsingskader. De Rijksoverheid, waar DUO onderdeel van uitmaakt, dient zich te houden aan het toetsingskader Baseline Informatiebeveiliging Rijksoverheid (BIR). De kaders in dit katern vormen de gemeenschappelijke basis voor deze normen- en toetsingskaders

2.3 Compliance of Toezicht: voldoe ik aan de normen?   
Van de kaders in dit katern worden dus concrete normen afgeleid. Of en hoe een onderwijsinstelling deze normen toepast, wordt getoetst door middel van een assessment of audit. Dit kan op drie manieren:

1. Self assessment: de instelling controleert aan de hand van bijvoorbeeld een toetsingsschema of voldaan wordt aan de normen en legt daartoe zelf een verklaring af.
2. Peer-auditing: een collega instelling controleert op onafhankelijke wijze of de instelling voldoet aan het normenkader.
3. Externe audit: hierbij voert een professioneel extern auditor een audit uit in de onderwijsinstelling. Deze geeft daarna een officiële verklaring af.

## 2.4 Ketenafspraken: Wat verwacht ik van anderen?

Als ketenpartijen met elkaar samenwerken of gegevens uitwisselen, is het belangrijk dat zij niet alleen zelf voldoen aan de gestelde normen, maar dat de partijen ook afspraken maken met elkaar. SaMBO-ICT, Kennisnet en SURF bieden ondersteuning voor het maken van deze afspraken. Hierbij gaat het om aanwijzingen voor gebruik, gedragsrichtlijnen en voorbeelddocumenten (sjablonen).

# 3. Kaders

## 3.1 Basisniveau Privacy en Beveiliging

Het basisniveau omvat zaken op het gebied van privacy en beveiliging die hoe dan ook geregeld moeten zijn. De kaders in het basisniveau zijn dus in elke situatie binnen het onderwijs van toepassing en zijn gericht op:

* Ketenbrede waarborging van vertrouwelijkheid en integriteit;
* Ketenbrede waarborging van beschikbaarheid in ketenprocessen;
* Informatiebeveiliging door ketenpartijen.

### Vertrouwelijkheid, integriteit en beschikbaarheid

In de opzet van het basisniveau wordt gerefereerd aan de termen 'vertrouwelijkheid', 'integriteit' en 'beschikbaarheid'. Dit zijn drie algemeen geaccepteerde aspecten van informatiebeveiliging die als volgt worden gedefinieerd:

* **Vertrouwelijkheid** betreft het waarborgen dat informatie alleen toegankelijk is voor degenen die hiertoe zijn geautoriseerd. Met 'toegang hebben tot' wordt zowel het raadplegen als het muteren, toevoegen en/of vernietigen van informatie bedoeld.
* **Integriteit** betreft het waarborgen van de juistheid, volledigheid en tijdigheid van informatie. Informatie waarvoor de integriteit op orde is, is dus informatie die 'klopt'. Merk op dat een aantasting van vertrouwelijkheid (waardoor onbevoegden bijvoorbeeld mutaties kunnen doorvoeren) kan leiden tot een aantasting van integriteit.
* **Beschikbaarheid** betreft het waarborgen dat geautoriseerde gebruikers op de juiste momenten toegang hebben tot informatie en aanverwante bedrijfsmiddelen. Aantasting van beschikbaarheid kan bijvoorbeeld leiden tot aantasting van de continuïteit van bedrijfs- en/of ketenprocessen.

### Ketenbrede waarborging van vertrouwelijkheid en integriteit

1. **Voorkom onrechtmatige toegang of verspreiding**   
   Gegevens met een hoge vertrouwelijkheidsklasse worden zo opgeslagen en getransporteerd dat onrechtmatige toegang of verspreiding onmogelijk wordt gemaakt.
2. **Voorkom aantasting van integriteit**   
   Gegevens met een hoge integriteitsklasse worden zo opgeslagen en getransporteerd dat aantasting van de juistheid, volledigheid en/of tijdigheid onmogelijk worden gemaakt.
3. **Handelingen zijn herleidbaar**   
   Handelingen rondom gegevens met een hoge integriteits- of vertrouwelijkheidsklasse zijn te herleiden naar personen
4. **Valideer persoonsgebonden gegevens**   
   Voor persoonsgebonden gegevens wordt, al dan niet via een terugkoppeling aan de aanleverende partij, gevalideerd of de juist gegevens aan de juiste persoon zijn toegewezen.
5. **Proactief technisch beheer**   
   Systemen die gegevens met een hoge beschikbaarheids-, integriteits- of vertrouwelijkheidsklasse verwerken worden proactief technisch beheerd. Onderdeel van proactief technisch beheer is het uitfaseren van verouderde software.
6. **Gebruik technieken voor veilig programmeren**   
   Systemen die de opslag en verwerking van gegevens met vertrouwelijkheids-/ of integriteitsklasse midden of hoog realiseren, worden ontwikkeld met gebruikmaking van technieken voor veilig programmeren.
7. **Gegevens worden niet langer bewaard dan strikt noodzakelijk**

### Ketenbrede waarborging van beschikbaarheid in ketenprocessen

1. **Notificaties**Correcties en aanvullingen op eerder verstuurde gegevens worden onmiddellijk doorgezet naar afnemers van die gegevens.
2. **Prestatieafspraken**Ketenpartijen in een ketenproces (waarin afhankelijkheden in tijd bestaan) maken duidelijke afspraken over te realiseren prestaties in de tijd en houden zich daaraan.
3. **Continuïteitsplan**Voor gegevens met het beschikbaarheidsniveau hoog, of waarvoor een kritieke tijdsafhankelijke relatie bestaat, is een continuïteitsplan beschikbaar

### 

### Informatiebeveiliging door ketenpartijen

1. **Ketenpartijen conformeren zich aan de 'Code voor informatiebeveiliging' (ISO 27001/27002:2013)**Binnen het basisniveau gelden de doelen uit ISO/IEC 27002:2013 als kaders voor informatiebeveiliging door individuele ketenpartijen. Deze kaders zijn opgenomen als bijlage.

## 3.2 Additionele kaders

In aanvulling op het basisniveau gelden voor specifieke werkingsgebieden additionele kaders. Voor het ketenproces toetsen en examineren zijn deze kaders in de volgende paragraaf opgenomen. Voor andere ketenprocessen, op het vlak van Instroom en Doorstroom, Verantwoording en Bekostiging, zullen op basis van risicoanalyses in de toekomst soortgelijke aanvullingen worden opgesteld.

### Toetsen en examineren

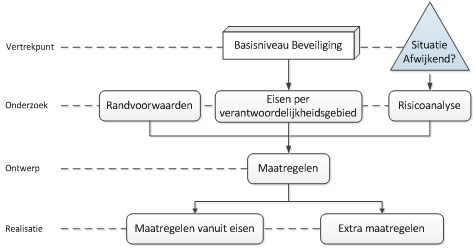
Naast de kaders uit het basisniveau, gelden op het gebied van privacy en beveiliging bij toetsen en examineren de volgende kaders:

1. Gegevens die gebruikt zijn bij de totstandkoming van het toetsresultaat kunnen pas worden verwijderd na het verstrijken van de inzage- en beroepstermijn
2. De afnamerespons wordt onmiddellijk verwijderd na het verstrijken van de inzage- en beroepstermijn
3. De totstandkoming van het toetsresultaat is transparant en valideerbaar.
4. De identiteit van een kandidaat wordt voor de toetsafname vastgesteld
5. De toetslocatie is zo ingericht dat fraude wordt voorkomen

# 4. Methodiek

## 4.1 Aanpak voor formuleren kaders

De kaders uit Hoofdstuk 3 vormen een Basisniveau Beveiliging, voor specifieke contexten aangevuld met additionele kaders. Op basis van deze kaders kunnen beheersmaatregelen worden geselecteerd, bijvoorbeeld uit ISO 27002 of andere raamwerken zoals het NORA Katern Beveiliging[[3]](#footnote-3). Een voorbeeld van zo'n selectie staat in de Bijlage: Maatregelen bij het Basisniveau Privacy en Beveiliging. Deze beheersmaatregelen leiden tot maatregelen in organisaties, processen, applicaties en/of technologie.



Figuur 2: Risicoanalyse (uit NORA Katern Beveiliging)

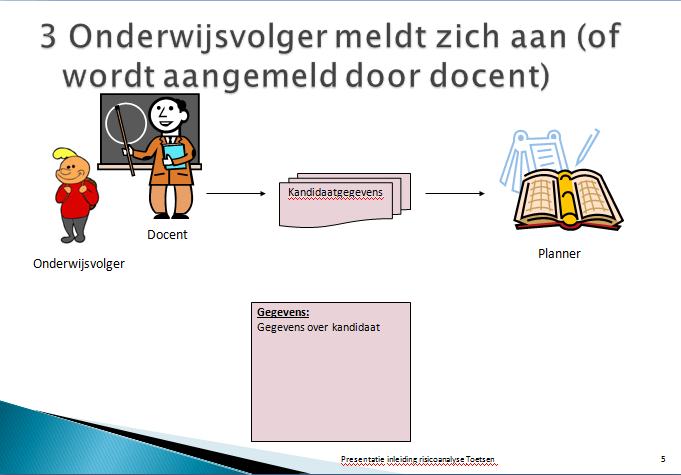
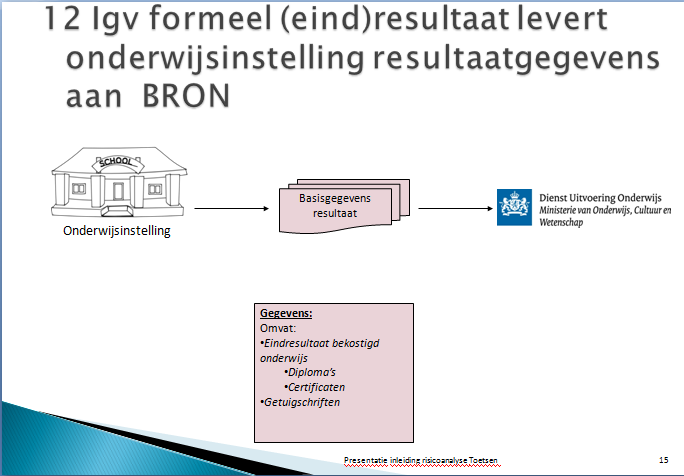
Doet zich een situatie voor die afwijkt van het Basisniveau Beveiliging, dan vindt een risicoanalyse plaats die gericht is op die afwijkende situatie. Zo'n risicoanalyse leidt tot nieuwe kaders. Die gelden dan als aanvullend kader voor die specifieke situatie. Als het opgestelde kader breder geldt, dan wordt het opgenomen in het basisniveau zelf. Zodoende breidt het Basisniveau Beveiliging zich met elke risicoanalyse weer een stap verder uit.

## 4.2 Risico-analyse

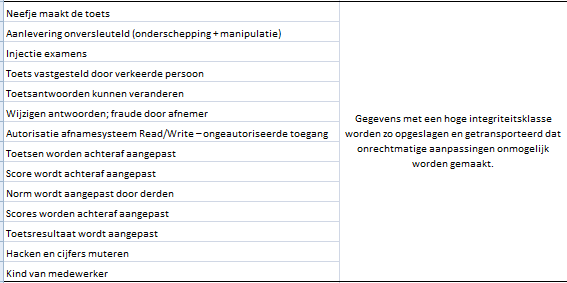
Het Basisniveau Beveiliging wordt gevoed vanuit risicoanalyses. Initieel is (was) het basisniveau nog leeg.Uit een risiconanalyse voor het domein Toetsen en Examineren is de eerste invulling van het basisinveau, zoals dat in Hoofdstuk 3 is beschreven, tot stand gekomen.

Figuur 1 in paragraaf 1.5 geeft aan dat er nog meer gebieden zijn, waarvoor op een soortgelijke manier een risicoanalyse kan worden uitgevoerd. De resultaten van die risicoanalyses kunnen ook ondergebracht worden in het Basisniveau Beveiliging. Door steeds meer resultaten samen te brengen in dit katern ontstaat een steeds breder basisniveau voor privacy en informatiebeveiliging. Ook groeit zo de *body of knowledge* over (de toepassing van) maatregelen om aan dat basisniveau te voldoen.

Een risicoanalyse uitvoeren gaat op hoofdlijnen als volgt:

1. Het ketenproces wordt beschreven in opeenvolgende stappen. In elke ketenprocesstap vindt interactie plaats tussen actoren en bepaalde gegevens.
   1. Voorbeeld (uit ketenproces Toetsen en Examineren): *De onderwijsvolger meldt zich aan voor een toets (of wordt aangemeld door de docent)*.
   2. Voorbeeld (uit ketenproces Toetsen en Examineren): *In geval van een formeel (eind)resultaat levert de onderwijsinstelling de resultaatgegevens aan aan BRON.*
2. Voor elke ketenprocesstap wordt een dia opgesteld die de betrokken actoren en gegevens toont.
   1. Voorbeeld (uit ketenproces Toetsen en Examineren):  
      
   2. Voorbeeld (uit ketenproces Toetsen en Examineren):  
      
3. De dia's worden afgedrukt en krijgen een plaats aan de muur van de workshopruimte.
4. De aanwezige experts benoemen in hun eigen woorden de risico's die samenhangen met het ketenproces. Ze noteren deze risico's op een post-it en plakken deze op de afdrukvan de processtap waarin dat risico optreedt.
5. De geïdentificeerde risico's worden plenair besproken en waar nodig toegelicht door de indiener. Eventueel kunnen risico's na bespreking dan alsnog vervallen.
6. Alle geïdentificeerde risico's worden ter verdere analyse op een risicolijst gezet.

Na deze workshopfase volgt een analysefase. Daarin worden de geïdentificeerde risico's geclusterd. Voor risico's die nog niet door het basisniveau privacy en beveiliging afgedekt zijn, worden kaders geformuleerd omdeze (clusters van) risico's af te dekken. De analyseresultaten worden gedeeld en in een vervolgbijeenkomst besproken met de bij de workshop betrokken experts, opdat hierover overeenstemming wordt bereikt. De tabel hieronder toont een cluster van soortgelijke risico's (linkerkolom) dat door hetzelfde kader (rechterkolom) wordt afgedekt.



Waar mogelijk worden, zoals hierboven, de gestelde kaders zó veralgemeniseerd, dat ze opgenomen kunnen worden in het basisniveau uit paragraaf 3.1. Anders worden ze, zoals hieronder, geformuleerd als aanvullende kaders op het basisniveau voor een specifiek ketenproces (zie paragraaf 3.2).



Op basis van deze kaders kunnen vervolgens passende maatregelen worden geselecteerd, zoals geïllustreerd in Bijlage: Maatregelen bij het Basisniveau Privacy en Beveiliging.

## 4.3 Risicoclassificatie

De zwaarte van de te nemen maatregelen hangt in de regel af van de zogenaamde BIV-classificatie van de gegevens die bij een ketenprocesstap betrokken zijn. In de toekomst zullen alle gegevens waarop informatiebeveiligingsbeleid van toepassing is, geclassificeerd moeten zijn. Het niveau van de beveiligingsmaatregelen is afhankelijk van de klasse.

De BIV classificatie is afgeleid van de volgende kwaliteitsaspecten:

* **B**eschikbaarheid
* **I**ntegriteit
* **V**ertrouwelijkheid

Ten aanzien van de **beschikbaarheid**seisenworden de volgende klassen onderscheiden:

|  |  |  |
| --- | --- | --- |
| Klasse | Basisprincipes | Beveiligingsniveau |
| LAAG (Niet vitaal) | algeheel verlies of niet beschikbaar zijn van deze informatie gedurende langer dan 1 week brengt geen merkbare (meetbare) schade toe aan de belangen van ketenpartijen, hun medewerkers of hun klanten | Basisbescherming  (Laag) |
| MIDDEN (Vitaal) | algeheel verlies of niet beschikbaar zijn van deze informatie gedurende langer dan 1 week brengt merkbare schade toe aan de belangen van ketenpartijen, hun medewerkers of hun klanten | Basisbescherming +  (Midden) |
| HOOG (Zeer vitaal) | algeheel verlies of niet beschikbaar zijn van deze informatie gedurende langer dan 1 etmaal brengt merkbare schade toe aan de belangen van ketenpartijen, hun medewerkers of hun klanten | Basisbescherming ++  (Hoog) |

Voor **integriteit** en **vertrouwelijkheid** worden de volgende indeling gevolgd.

|  |  |  |
| --- | --- | --- |
| Klasse | Basisprincipes | Beveiligingsniveau |
| LAAG (Openbaar) | · Iedereen mag de gegevens inzien, bijvoorbeeld de website van een onderwijsinstelling  · Een geselecteerde groep mag deze gegevens wijzigen | Basisbescherming |
| MIDDEN (Intern) | · Iedereen die aan een instelling is verbonden als medewerker of student mag deze gegevens inzien; toegang kan zowel binnen als buiten de instelling (remote) worden verleend, bijvoorbeeld lesroosters of Elektronische leeromgeving  · Een geselecteerde groep mag deze gegevens wijzigen | Basisbescherming |
| HOOG (Vertrouwelijk) | · Er is expliciet aangegeven wie welke rechten heeft t.a.v. de raadpleging en de verwerking van deze gegevens, bijvoorbeeld Kernregistratie systeem. | Basisbescherming + |

Welk beveiligingsniveau geschikt is voor een bepaald informatiesysteem hangt af van de classificatie van de informatie die het systeem verwerkt. De classificatie wordt bepaald door of namens de eigenaar van het betreffende informatiesysteem.

## 4.4 Toetsingskaders

Hieronder volgt een opsomming van relevante toetsingskaders met (selecties van) maatregelen. Instellingen die willen voldoen aan kaders uit het basisniveau en/of aanvullende kaders kunnen daaruit putten.

### 4.4.1 ISO 27002

*Werkingsgebied: gehele onderwijsdomein  
Toepassingsgebied: (interne) organisatie*

ISO 27002 omvat beheersmaatregelen voor het implementeren van een managementsysteem voor informatiebeveiliging conform ISO27001. Deze maatregelen dienen ook als leidraad voor organisaties die algemeen aanvaarde beheersmaatregelen op het gebied van informatiebeveiliging willen invoeren. Het College voor Standaardisatie heest ISO27001 en 27002 op de lijst met 'pas toe of leg uit'-standaarden geplaatst. Overheden en semi-overheden zijn daarom verplicht om deze standaard toe te passen.

### 4.4.2 NORA-katern beveiliging

*Werkingsgebied: (semi-)overheid  
Toepassingsgebied: massale verwerking van persoons- en financiële gegevens*

NORA staat oor Nederlandse Overheid Referentie Architectuur. Het NORA-katern Beveiliging omvat beheersmaatregelen en implementatierichtlijnen (samengenomen onder de noemer 'eisen') voor de beveiliging van massale verwerking van persoons- en financiële gegevens, uitgaande van het basisniveau informatiebeveiliging voor de e-overheid. Het NORA-katern is afgeleid van de werkgebieden informatiebeveiliging en bedrijfscontinuïteit uit ISO 27002. De aspecten fysieke beveiliging en personele integriteit blijven in dit katern buiten beschouwing.

### 4.4.3 BIR

*Werkingsgebied: rijksoverheid  
Toepassingsgebied: (interne) organisatie*

De BIR (Baseline Informatiebeveiliging Rijksdienst) beschrijft de invulling van ISO27001 en 27002 voor de Rijksoverheid. Het bestaat uit een - binnen de Rijksoverheid verplicht toe te passen - tactisch normenkader (een superset van ISO 27002/maatregelen) en een niet-verplichte operationele baseline die bestaat uit best practices.

### 

### 4.4.4 Normenkader SURFaudit

*Werkingsgebied: ho-instellingen  
Toepassingsgebied: (interne) organisatie*

Het SURFaudit normenkader omvat een selectie van maatregelen uit ISO 27002. Het zijn zaken rond bescherming van veiligheid en continuïteit van bedrijfsgegevens en de privacy van studenten en medewerkers die een onderwijsinstelling ten minste geregeld moet hebben. De maatregelen zijn geclusterd; bij een assessment of audit wordt per cluster het volwassenheidsniveau van de instelling bepaald.

### 

### 4.4.5 SURF Juridisch normenkader cloudservices hoger onderwijs

*Werkingsgebied: hoger onderwijs  
Toepassingsgebied: afnemen van clouddiensten*

Dit normenkader geeft een overzicht van de best practice clausules voor overeenkomsten met leveranciers van clouddiensten in het hoger onderwijs. Het juridisch normenkader omvat clausules die in lijn zijn met actuele nationale en Europese regelgeving op het gebied van o.a. gegevensbescherming en privacy.

### 

### 4.4.6 CSA Cloud Controls Matrix

*Werkingsgebied: gehele onderwijsdomein  
Toepassingsgebied:aanbieden en afnemen van clouddiensten*

De Cloud Controls Matrix (CCM) van de Cloud Security Alliance (CSA) legt een relatie tussen de negen grootste risico's van cloud computing en de maatregelen ('controls') die een effectieve bescherming vormen tegen deze risico's. De CCM richt zich enerzijds op het bieden van beveiligingsrichtlijnen aan cloudleveranciers, en anderzijds op het ondersteunen van cloudafnemers bij het beoordelen van de veiligheidsrisico's van een cloudleverancier.

### 4.4.7 Certificeringsschema Edukoppeling

*Werkingsgebied: gehele onderwijsdomein  
Toepassingsgebied: aanbieden van clouddiensten via Edukoppeling*

Het Certificeringsschema Edukoppeling is bedoeld voor leveranciers van clouddiensten. Een cloudleverancier moet aan de normen in dit schema voldoen, vóórdat de betreffende clouddienst binnen de context van Edukoppeling mag worden ingezet.

### 4.4.8 CBP Compliance-instrumenten

*Werkingsgebied: gehele onderwijsdomein  
Toepassingsgebied: (interne) organisatie*

Het CBP heeft een viertal compliance-instrumenten ontwikkeld die gebruikt kunnen worden als handreiking voor het naleven van de geldende wet- en regelgeving:

* Quickscan
* Wbp Zelfevaluatie
* Raamwerk Privacy Audit
* Handreiking bij het Raamwerk Privacy Audit

### 4.4.9 NCSC Beveiligingsrichtlijnen

*Werkingsgebied: gehele onderwijsdomein  
Toepassingsgebied: technologie*

Het Nationaal Cyber Security Center publiceert beveiligingsrichtlijnen naar aanleiding van trends en (actuele) dreigingen en op basis van best practices :

* ICT-beveiligingsrichtlijnen voor webapplicaties (feb. 2012)
* Beveiligingsrichtlijnen voor mobiele apparaten (nov. 2012)
* ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) (nov. 2014)

### 4.4.10 Kennisnet Checklist privacy-afspraken voor scholen

*Werkingsgebied: onderwijsinstellingen  
Toepassingsgebied: afnemen van clouddiensten*

Met deze checklist kan worden vastgesteld of de afspraken tussen scholen en softwareleveranciers voldoen aan de wettelijke eisen.

# Begrippenlijst

De begrippen die in dit document worden gebruikt sluiten zo veel mogelijk aan bij definities uit bestaande begrippenlijsten. Bij elk begrip hieronder is een verwijzing naar de bron van de definitie opgenomen.

**Audit** Systematisch, onafhankelijk en gedocumenteerd proces voor het verkrijgen en objectief evalueren van bewijs teneinde vast te stellen in hoeverre aan een toetsingskader is voldaan.  
 *ISO 27001:2014 (audit)*

**Assessment** Zie ***Audit***

**Beheersmaatregel** Maatregel die risico wijzigt  
 *ISO 27000:2014 (control)*

**Beschikbaarheid** De eigenschap van het toegankelijk en bruikbaar zijn op aanvraag van een geautoriseerde entiteit  
 *ISO 27000:2014 (availability)*

Beschikbaarheid betreft het waarborgen dat geautoriseerde gebruikers op de juiste momenten toegang hebben tot informatie en aanverwante bedrijfsmiddelen. Aantasting van beschikbaarheid kan bijvoorbeeld leiden tot aantasting van de continuïteit van bedrijfs- en/of ketenprocessen.

**Beveiliging** Behoud van vertrouwelijkheid, integriteit en beschikbaarheid van informatie  
 *ISO 27000:2014 (information security)*

**Bewijs** Feitelijke verklaringen of andere informatie die controleerbaar is en relevant voor een toetsingskader.   
 *ISO 19011:2011 (audit evidence)*

**Integriteit** De eigenschap van juistheid en volledigheid.  
 *ISO 27000:2014 (integrity)*

Integriteit betreft het waarborgen van de juistheid, volledigheid en tijdigheid van informatie. Informatie waarvoor de integriteit op orde is, is dus informatie die 'klopt'. Merk op dat een aantasting van vertrouwelijkheid (waardoor onbevoegden bijvoorbeeld mutaties kunnen doorvoeren) kan leiden tot een aantasting van integriteit.

**Kader** Verzameling beleid, procedures en/of eisen  
 *zie ook* ***Normenkader****,* ***Toetsingskader***

**Ketenpartij** Een partij die een rol speelt in een ketenproces

**Ketenproces** Een samenwerking tussen entiteiten die dient om een (gezamenlijk) doel te realiseren.

**Maatregel** Handeling of ingreep met een bepaald doel  
 *Van Dale*

**Norm** Beleid, procedure of eis gebruikt als referentie  
 *zie ook* ***Normenkader****,* ***Toetsingskader***

**Normenkader** Verzameling beleid, procedures en/of eisen gebruikt als referentie  
 *zie ook* ***Toetsingskader***

**Privacy** Het recht om in de beslotenheid van de persoonlijke levenssfeer met rust te worden gelaten, waaronder het recht op zorgvuldige behandeling van persoonlijke gegevens.  
 *zie Grondwet, artikel 10*

**Risico** Effect van onzekerheid op doelstellingen.  
 *ISO 27000:2014 (risk)*

**Risicoanalyse** Proces om de aard van risico te begrijpen en het risiconiveau te bepalen  
 *ISO 27000:2014 (risk analysis)*

**ROSA** Referentiearchitectuur van het onderwijs

**Toetsingskader** Verzameling beleid, procedures en/of eisen gebruikt als referentie waartegen bewijs uit een audit wordt vergeleken.  
 *ISO 19011:2011 (audit criteria)*

**Vertrouwelijkheid** De eigenschap dat informatie niet beschikbaar wordt gesteld of ter kennis komt van onbevoegde personen, entiteiten of processen  
 *ISO 27000:2014 (confidentiality)*

Vertrouwelijkheid betreft het waarborgen dat informatie alleen toegankelijk is voor degenen die hiertoe zijn geautoriseerd. Met 'toegang hebben tot' wordt zowel het raadplegen als het muteren, toevoegen en/of vernietigen van informatie bedoeld.

# Bijlage: Kaders voor ketenpartijen uit ISO27002:2013

1. Ketenpartijen hebben directieaansturing van en -steun voor informatiebeveiliging in overeenstemming met bedrijfseisen en relevante wet- en regelgeving.
2. Ketenpartijen stellen een beheerkader vast om de implementatie en uitvoering van de informatiebeveiliging binnen hun organisatie te initiëren en te beheersen.  
   *Toelichting: het beheerkader is gericht op het in de organisatie inbedden van de beleidsregels die komen vanuit de directieaansturing.*
3. Ketenpartijen waarborgen de veiligheid van telewerken en het gebruik van mobiele apparatuur.
4. Ketenpartijen waarborgen dat medewerkers en contractanten hun verantwoordelijkheden begrijpen en geschikt zijn voor de functies waarvoor zij in aanmerking komen.
5. Ketenpartijen zorgen ervoor dat medewerkers en contractanten zich bewust zijn van hun verantwoordelijkheden op het gebied van informatiebeveiliging en deze nakomen.
6. Ketenpartijen beschermen de belangen van hun organisatie als onderdeel van de wijzigings- of beëindigingsprocedure van het dienstverband.
7. Ketenpartijen identificeren bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten en stellen van deze bedrijfsmiddelen een inventaris op en onderhouden deze.
8. Ketenpartijen bewerkstelligen dat informatie een passend beschermingsniveau krijgt dat in overeenstemming is met het belang ervan voor hun organisatie.
9. Ketenpartijen voorkomen onbevoegde openbaarmaking, wijziging, verwijdering of vernietiging van informatie die op media is opgeslagen.
10. Ketenpartijen beperken toegang tot informatie en informatieverwerkende faciliteiten.
11. Ketenpartijen bewerkstelligen toegang voor bevoegde gebruikers en voorkomen onbevoegde toegang tot systemen en diensten.
12. Ketenpartijen maken gebruikers verantwoordelijk voor het beschermen van hun authenticatie-informatie.
13. Ketenpartijen voorkomen onbevoegde toegang tot systemen en toepassingen.
14. Ketenpartijen zorgen voor correct en doeltreffende gebruik van cryptografie om de vertrouwelijkheid, authenticiteit en/of integriteit van informatie te beschermen.
15. Ketenpartijen voorkomen onbevoegde fysieke toegang tot, schade aan en interferentie met informatie en informatieverwerkende faciliteiten van hun organisatie.
16. Ketenpartijen voorkomen verlies, schade, diefstal of compromittering van bedrijfsmiddelen en onderbreking van de bedrijfsvoering van hun organisatie.
17. Ketenpartijen waarborgen correcte en veilige bediening van informatieverwerkende faciliteiten.
18. Ketenpartijen waarborgen dat informatie en informatieverwerkende faciliteiten beschermd zijn tegen malware.
19. Ketenpartijen beschermen zich tegen het verlies van gegevens.
20. Ketenpartijen leggen gebeurtenissen vast en verzamelen bewijs.
21. Ketenpartijen waarborgen de integriteit van operationele systemen.
22. Ketenpartijen voorkomen de benutting van technische kwetsbaarheden.
23. Ketenpartijen maken de impact van auditactiviteiten op uitvoeringssystemen zo gering mogelijk.
24. Ketenpartijen waarborgen de bescherming van informatie in netwerken en de ondersteunende informatieverwerkende faciliteiten.
25. Ketenpartijen handhaven de beveiliging van informatie die wordt uitgewisseld binnen hun organisatie en met een externe identiteit.
26. Ketenpartijen waarborgen dat informatiebeveiliging integraal deel uitmaakt van informatiesystemen in de gehele levenscyclus. Hiertoe behoren ook de eisen voor informatiesystemen die diensten verlenen via openbare netwerken.
27. Ketenpartijen bewerkstelligen dat informatiebeveiliging wordt ontworpen en geïmplementeerd binnen de ontwikkelingslevenscyclus van informatiesystemen.
28. Ketenpartijen waarborgen bescherming van gegevens die voor het testen zijn gebruikt.
29. Ketenpartijen waarborgen de bescherming van bedrijfsmiddelen van de organisatie die toegankelijk zijn voor leveranciers.
30. Ketenpartijen handhaven een overeengekomen niveau van informatiebeveiliging en dienstverlening in overeenstemming met de leveranciersovereenkomsten.
31. Ketenpartijen bewerkstelligen een consistente en doeltreffende aanpak van het beheer van informatiebeveiligingsincidenten, met inbegrip van communicatie over beveiligingsgebeurtenissen en zwakke plekken in de beveiliging.
32. Ketenpartijen bedden informatiebeveiligingscontinuïteit in in de systemen van het bedrijfscontinuïteitsbeheer van hun organisatie.
33. Ketenpartijen bewerkstelligen beschikbaarheid van informatieverwerkende faciliteiten.
34. Ketenpartijen voorkomen schendingen van wettelijke, statutaire, regelgevende of contractuele verplichtingen betreffende informatiebeveiliging en beveiligingseisen.
35. Ketenpartijen verzekeren dat de informatiebeveiliging wordt geïmplementeerd en uitgevoerd in overeenstemming met de beleidsregels en procedures van hun organisatie.  
    *Toelichting: Dit impliceert dat de genomen maatregelen toetsbaar en controleerbaar zijn, en dat er zowel interne controle is op de naleving van het beveiligingsbeleid als dat er, waar nodig, onafhankelijke (externe) beoordelingen worden uitgevoerd.*

# Bijlage: Maatregelen bij het Basisniveau Privacy en Beveiliging

De kaders uit het basisniveau geven aan wat er, op het gebied van privacy en security, hoe dan ook geregeld moet zijn. Aan deze kaders kan op verschillende wijzen invulling worden gegeven. Beheersmaatregelen kunnen worden geselecteerd uit bestaande normen, zoals ISO/IEC-27002, of uit andere overzichten van beheersmaatregelen, zoals de eisen uit het NORA-katern Beveiliging. Ook kunnen eigen, organisatie- of onderwijsketenspecifieke maatregelen of richtlijnen worden ontwikkeld.

Voor de kaders uit het basisniveau is hieronder ter illustratie een selectie van maatregelen uit ISO 27002 weergegeven, waarbij in de formulering van de beheersmaatregelen aangesloten is bij de vertaling van de ISO beheersmaatregelen naar de onderwijscontext zoals die in het SURFaudit normenkader is

vormgegeven.

### Ketenbrede waarborging van vertrouwelijkheid en integriteit

**Gegevens met een hoge vertrouwelijkheidsklasse worden zo opgeslagen en getransporteerd dat onrechtmatige toegang of verspreiding onmogelijk wordt gemaakt.**

*betreft: (onderdelen van) toetspackages (toets, afnamevoorschrift, correctievoorschrift) tot het moment van afname; afnamerespons, toetsresultaat, basisgegeven resultaat; gegevens die zouden kunnen leiden tot de ongewenste vindbaarheid van (de verblijfsplaats van) een onderwijsvolger*

*Rationale:*

* *Toetsen en toetspackages bevatten tot het moment van afname (zeer) vertrouwelijke informatie. Door schending van die vertrouwelijkheid kunnen (groepen) personen bij afname van de toets onheus bevoordeeld worden. Vroegtijdige openbaarmaking (door bijvoorbeeld diefstal, lekken of onbevoegde inzage) moet daarom worden voorkomen.*
* *Afnamerespons en resultaatgegevens zijn gevoelige (persoons)gegevens.*

**ISO 27002 beheersmaatregelen**

* **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.*
* **8.3.1 Beheer van verwijderbare media***Voor het beheren van verwijderbare media behoren procedures te worden geïmplementeerd in overeenstemming met het classificatieschema dat door de organisatie is vastgesteld.*
* **8.3.2 Verwijderen van media***Media behoren op een veilige en beveiligde manier te worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures.*
* **8.3.3 Media fysiek overdragen***Media die informatie bevatten, behoren worden beschermd tegen onbevoegde toegang, misbruik of corruptie tijdens transport.*
* **9.1.2 Toegang tot netwerken en netwerkdiensten**  
  *Gebruikers behoren alleen toegang te krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.*
* **9.4.1 Beperking toegang tot informatie***Toegang tot informatie en systeemfuncties van toepassingen behoort te worden beperkt in overeenstemming met het beleid voor toegangscontrole.*
* **10.1.1 Beleid inzake het gebruik van cryptografische beheersmaatregelen***Ter bescherming van informatie behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.*
* **11.1.1 Fysieke beveiligingszone***Beveiligingszones behoren te worden gedefinieerd en gebruikt om gebieden te beschermen die gevoelige of essentiële informatie en informatieverwerkende faciliteiten bevatten.*
* **11.1.2 Fysieke beveiligingszone***Beveiligde gebieden behoren te worden beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.*
* **12.4.1 Gebeurtenissen registreren***Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.*
* **12.4.3 Logbestanden van beheerders en operators***Activiteiten van systeembeheerders en -operators behoren te worden vastgelegd en de logbestanden behoren te worden beschermd en regelmatig te worden beoordeeld.*
* **13.2.1 Beleid en procedures voor informatietransport***Ter bescherming van het informatietransport, dat via alle soorten communicatiefaciliteiten verloopt, behoren formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht te zijn.*
* **13.2.2 Overeenkomsten over informatietransport***Overeenkomsten behoren betrekking te hebben op het beveiligd transporteren van bedrijfsinformatie tussen de organisatie en externe partijen.*
* **13.2.3 Elektronische berichten** *Informatie die is opgenomen in elektronische berichten behoort passend beschermd te zijn.*
* **13.2.4 Vertrouwelijkheids- of geheimhoudingsovereenkomst***Eisen voor vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie betreffende het beschermen van informatie weerspiegelen behoren te worden vastgesteld, regelmatig te worden beoordeeld en gedocumenteerd.*

**Gegevens met een hoge integriteitsklasse worden zo opgeslagen en getransporteerd dat aantasting van de juistheid, volledigheid en/of tijdigheid onmogelijk worden gemaakt.**

*betreft: (onderdelen van) toetspackages (toets, afnamevoorschrift, correctievoorschrift), afnamerespons, score, normering, normeringsadvies, toetsresultaat, basisgegeven resultaat*

*Rationale: Door onrechtmatige aanpassingen kunnen (groepen) personen bij afname van de toets onheus bevoordeeld of benadeeld worden.*

**ISO 27002 beheersmaatregelen**

* **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.*
* **8.3.1 Beheer van verwijderbare media***Voor het beheren van verwijderbare media behoren procedures te worden geïmplementeerd in overeenstemming met het classificatieschema dat door de organisatie is vastgesteld.*
* **8.3.3 Media fysiek overdragen***Media die informatie bevatten, behoren worden beschermd tegen onbevoegde toegang, misbruik of corruptie tijdens transport.*
* **9.1.2 Toegang tot netwerken en netwerkdiensten**  
  *Gebruikers behoren alleen toegang te krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.*
* **9.4.1 Beperking toegang tot informatie***Toegang tot informatie en systeemfuncties van toepassingen behoort te worden beperkt in overeenstemming met het beleid voor toegangscontrole.*
* **10.1.1 Beleid inzake het gebruik van cryptografische beheersmaatregelen***Ter bescherming van informatie behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.*
* **11.1.1 Fysieke beveiligingszone***Beveiligingszones behoren te worden gedefinieerd en gebruikt om gebieden te beschermen die gevoelige of essentiële informatie en informatieverwerkende faciliteiten bevatten.*
* **11.1.2 Fysieke beveiligingszone***Beveiligde gebieden behoren te worden beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.*
* **12.4.1 Gebeurtenissen registreren***Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.*
* **12.4.3 Logbestanden van beheerders en operators***Activiteiten van systeembeheerders en -operators behoren te worden vastgelegd en de logbestanden behoren te worden beschermd en regelmatig te worden beoordeeld.*
* **13.2.1 Beleid en procedures voor informatietransport***Ter bescherming van het informatietransport, dat via alle soorten communicatiefaciliteiten verloopt, behoren formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht te zijn.*
* **13.2.2 Overeenkomsten over informatietransport***Overeenkomsten behoren betrekking te hebben op het beveiligd transporteren van bedrijfsinformatie tussen de organisatie en externe partijen.*
* **13.2.3 Elektronische berichten** *Informatie die is opgenomen in elektronische berichten behoort passend beschermd te zijn.*
* **13.2.4 Vertrouwelijkheids- of geheimhoudingsovereenkomst***Eisen voor vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie betreffende het beschermen van informatie weerspiegelen behoren te worden vastgesteld, regelmatig te worden beoordeeld en gedocumenteerd.*

**Handelingen rondom gegevens met een hoge integriteits- of vertrouwelijkheidsklasse zijn te herleiden naar personen**

*Rationale: In geval van incidenten waardoor de vertrouwelijkheid of integriteit zijn geschonden, dient te kunnen worden achterhaald door wie die schending heeft plaatsgevonden.*

**ISO 27002 beheersmaatregelen**

* **9.2.1 Registratie en uitschrijving van gebruikers***Een formele registratie- en uitschrijvingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.*
* **12.4.1 Gebeurtenissen registreren***Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.*
* **12.4.2 Beschermen van informatie in logbestanden***Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang.*
* **12.4.3 Logbestanden van beheerders en operators***Activiteiten van systeembeheerders en -operators behoren te worden vastgelegd en de logbestanden behoren te worden beschermd en regelmatig te worden beoordeeld.*
* **12.4.4 Kloksynchronisatie***De klokken van alle relevante informatieverwerkende systemen binnen een organisatie of beveiligingsdomein behoren te worden gesynchroniseerd met één referentietijdbron.*

**Voor persoonsgebonden gegevens wordt, al dan niet via een terugkoppeling aan de aanleverende partij, gevalideerd of de juist gegevens aan de juiste persoon zijn toegewezen.**

Betreft: kandidaatgegevens (aanmelding), afnamerespons, score, toetresultaat, basisgegevens resultaat

*Rationale: wanneer persoonsgebonden gegevens foutief worden verwerkt, wordt de desbetreffende persoon direct geraakt met mogelijk grote en soms lastig te herstellen persoonlijke gevolgen zoals het niet deel kunnen nemen aan een toets of het niet uitgereikt kunnen krijgen van een diploma.*

**ISO 27002 beheersmaatregelen**

* **13.1.3.1 Scheiding in netwerken**

*Groepen van informatiediensten, -gebruikers en -systemen behoren in netwerken te worden gescheiden*

* **9.4.2.1 Beveiligde inlogprocedures**

*Indien het beleid voor toegangsbeveiliging dit vereist, behoort toegang tot systemen en toepassingen te worden beheerst door een beveiligde inlogprocedure.*

* **9.4.1.1 Beperking toegang tot informatie**

*Toegang tot informatie en systeemfuncties van toepassingen behoort te worden beperkt in overeenstemming met het beleid voor toegangsbeveiliging.*

**Systemen die gegevens met een hoge beschikbaarheids-, integriteits- of vertrouwelijkheidsklasse verwerken worden proactief technisch beheerd.**

*Rationale: Wanneer systemen onvoldoende technisch beheerd worden, en bijvoorbeeld security-patches niet onmiddellijk worden doorgevoerd of rechteninstellingen niet actief worden bijgehouden, ontstaan mogelijke beveiligingslekken die de beschikbaarheid, integriteit en vertrouwelijkheid van de gegevens in gevaar kan brengen.*

**ISO 27002 beheersmaatregelen**

* **12.2.1 Beheersmaatregelen tegen malware***Ter bescherming tegen malware behoren beheersmaatregelen voor detectie, preventie en herstel te worden geïmplementeerd, in combinatie met een passend bewustzijn van gebruikers.*
* **12.5.1 Software installeren op operationele systemen***Om het op operationele systemen installeren van software te beheersen behoren procedures te worden geïmplementeerd.*
* **12.6.1 Beheer van technische kwetsbaarheden***Informatie over technische kwetsbaarheden van informatiesystemen die worden gebruikt behoort tijdig te worden verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden te worden geëvalueerd en passende maatregelen te worden genomen om het risico dat ermee samenhangt aan te pakken.*
* **13.1.1 Beheersmaatregelen voor netwerken***Netwerken behoren te worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen.*
* **14.2.3 Technische beoordeling van toepassingen na wijzigingen bedieningsplatform***Als bedieningsplatforms zijn veranderd, behoren bedrijfskritische toepassingen te worden beoordeeld en getest om te waarborgen dat er geen nadelige impact is op de activiteiten of de beveiliging van de organisatie.*
* **14.2.4 Beperkingen op wijzigingen aan softwarepakketten***Wijzigingen aan softwarepakketten moeten worden ontraden, beperkt tot noodzakelijke veranderingen en alle veranderingen moeten strikt worden gecontroleerd*

**Systemen die de opslag en verwerking van gegevens met vertrouwelijkheids- of integriteitsklasse midden of hoog realiseren, worden ontwikkeld met gebruikmaking van technieken voor veilig programmeren.**

*Rationale: Deze systemen moeten de vertrouwelijkheid en integriteit van die gegevens waarborgen.*

**ISO 27002 beheersmaatregelen**

* **12.1.4 Scheiding van ontwikkel-, test- en productieomgevingen***Ontwikkel-, test- en productieomgevingen behoren te worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen.*
* **14.2.1 Beleid voor beveiligd ontwikkelen***Voor het ontwikkelen van software en systemen behoren regels te worden vastgesteld en op ontwikkelactiviteiten binnen de organisatie te worden toegepast.*
* **14.2.2 Procedures voor wijzigingsbeheer met betrekking tot systemen***Wijzigingen aan systemen binnen de levenscyclus van de ontwikkeling behoren te worden beheerst door het gebruik van formele controleprocedures voor wijzigingsbeheer.*
* **14.2.5 Principes voor engineering van beveiligde systemen***Principes voor de engineering van beveiligde systemen behoren te worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle verrichtingen betreffende het implementeren van informatiesystemen*
* **14.2.6 Beveiligde ontwikkelomgeving***Organisaties behoren beveiligde ontwikkelomgevingen vast te stellen en passend te beveiligen voor verrichtingen op het gebied van systeemontwikkeling en integratie die betrekking hebben op de gehele levenscyclus van de systeemontwikkeling.*
* **14.2.7 Uitbestede softwareontwikkeling***Uitbestede systeemontwikkeling behoort onder supervisie te staan van en te worden gemonitord door de organisatie.*
* **14.2.8 Testen van systeembeveiliging***Tijdens ontwikkelactiviteiten behoort de beveiligingsfunctionaliteit te worden getest.*
* **14.2.9 Systeemacceptatietests***Voor nieuwe informatiesystemen, upgrades en nieuwe versies behoren programma’s voor het uitvoeren van acceptatietests en gerelateerde criteria te worden vastgesteld.*
* **14.3.1 Bescherming van testgegevens***Testgegevens behoren zorgvuldig te worden gekozen, beschermd en gecontroleerd.*

**Gegevens worden niet langer bewaard dan strikt noodzakelijk**

*Rationale: Van gegevens die niet langer beschikbaar zijn kan de vertrouwelijkheid en integriteit niet meer in het geding komen.*

**ISO 27002 beheersmaatregelen**

* **18.1.1 Vaststellen van toepasselijke wetgeving en contractuele eisen***Alle relevante wettelijke statutaire, regelgevende, contractuele eisen en de aanpak van de organisatie om aan deze eisen te voldoen behoren voor elk informatiesysteem en de organisatie expliciet te worden vastgesteld, gedocumenteerd en actueel gehouden.*
* **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.*

### Ketenbrede waarborging van continuïteit in ketenprocessen

**Correcties en aanvullingen op eerder verstuurde gegevens worden onmiddellijk doorgezet naar afnemers van die gegevens.**

*Rationale: Het op tijd verwerken van bijvoorbeeld (last-minute) correcties en errata vereist dat die gegevens zo snel mogelijk door de keten heen gecommuniceerd worden.*

**ISO 27002 beheersmaatregelen**

* **9.2.1.1 Registratie en afmelden van gebruikers**

*Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.*

* **9.2.2.1 Gebruikers toegang verlenen**

*Een formele gebruikerstoegangsverleningsprocedure behoort te worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.*

* **9.2.3.1 Beheren van speciale toegangsrechten**

*Het toewijzen en gebruik van speciale toegangsrechten behoren te worden beperkt en beheerst.*

* **9.2.4.1 Beheer van geheime authenticatie-informatie van gebruikers**

*Het toewijzen van geheime authenticatie-informatie behoort te worden beheerst via een formeel beheersproces.*

**Ketenpartijen in een ketenproces (waarin afhankelijkheden in tijd bestaan) maken duidelijke afspraken over te realiseren prestaties in de tijd en houden zich daaraan..***Rationale: Het ontwikkelen, vaststellen, afnemen, corrigeren, scoren en normeren van een toets omvat een keten waarin elke schakel afhankelijk is van de voorgaande. Wanneer één van de betrokken partijen niet, of niet op tijd, levert, kan de beschikbaarheid van de toets op het moment van afname in gevaar komen, of kan het eindoordeel niet op tijd vastgesteld worden.*

**ISO 27002 beheersmaatregelen**

* **15.1.3 Toeleveringsketen van informatie- en communicatietechnologie***Overeenkomsten met leveranciers behoren eisen te bevatten die betrekking hebben op de informatiebeveiligingsrisico’s in verband met de toeleveringsketen van de diensten en producten op het gebied van informatie- en communicatietechnologie.*
* **15.2.1 Monitoring en beoordeling van dienstverlening van leveranciers***Organisaties behoren regelmatig de dienstverlening van leveranciers te monitoren, te beoordelen en te auditen.*
* **15.2.2 Beheer van veranderingen in dienstverlening van leveranciers***Veranderingen in de dienstverlening van leveranciers, met inbegrip van handhaving en verbetering van bestaande beleidslijnen, procedures en beheersmaatregelen voor informatiebeveiliging, behoren te worden, beheerd, rekening houdend met de kritikaliteit van bedrijfsinformatie, betrokken systemen en processen en herbeoordeling van risico’s.*

**Voor gegevens met het beschikbaarheidsniveau hoog, of waarvoor een kritieke tijdsafhankelijke relatie bestaat, is een continuïteitsplan beschikbaar**

*Rationale: Bepaalde resources móeten beschikbaar zijn op het moment van afname. Dat geldt bijvoorbeeld voor het afnamesysteem (bij digitaal toetsen). Maar ook het lokaal waar de toetsafname plaats vindt, de afnameleider die de afname begeleidt en niet in de laatste plaats de toets zelf moeten beschikbaar zijn. Door calamiteiten kunnen één of meer resources uitvallen. In een continuïteitsplan is vastgelegd hoe de vereiste beschikbaarheid (bijvoorbeeld door uitwijk) in zo'n geval alsnog wordt gerealiseerd.*

**ISO 27002 beheersmaatregelen**

* **11.1.4 Beschermen tegen bedreigingen van buitenaf***Tegen natuurrampen, kwaadwillige aanvallen of ongelukken behoort fysieke bescherming te worden ontworpen en toegepast.*
* **17.2.1 Beschikbaarheid van informatieverwerkende faciliteiten***Informatieverwerkende faciliteiten behoren met voldoende redundantie te worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.*

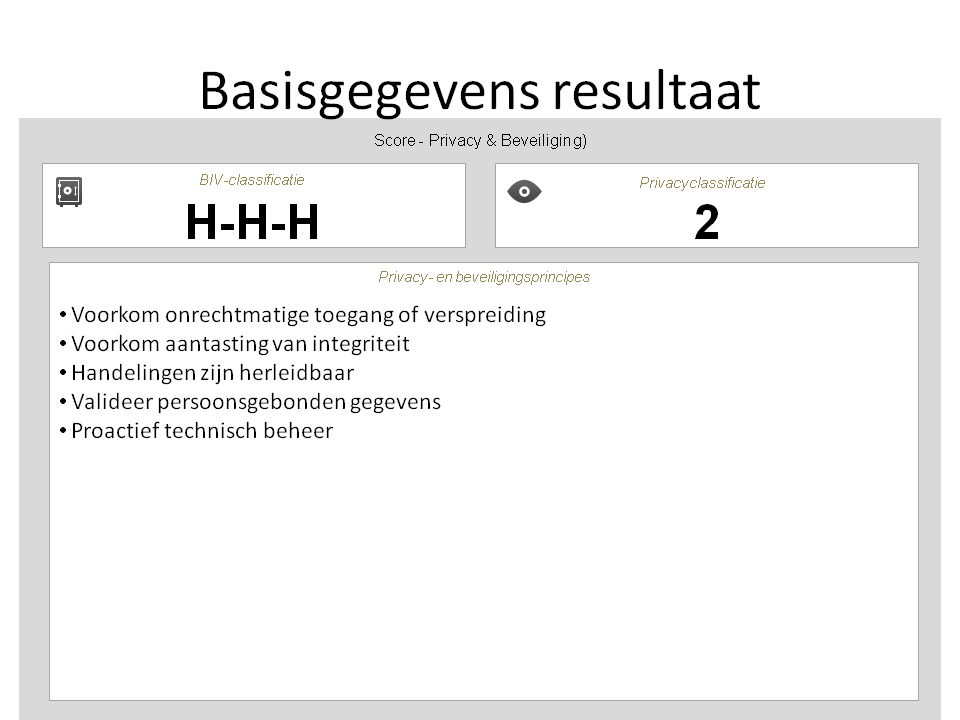
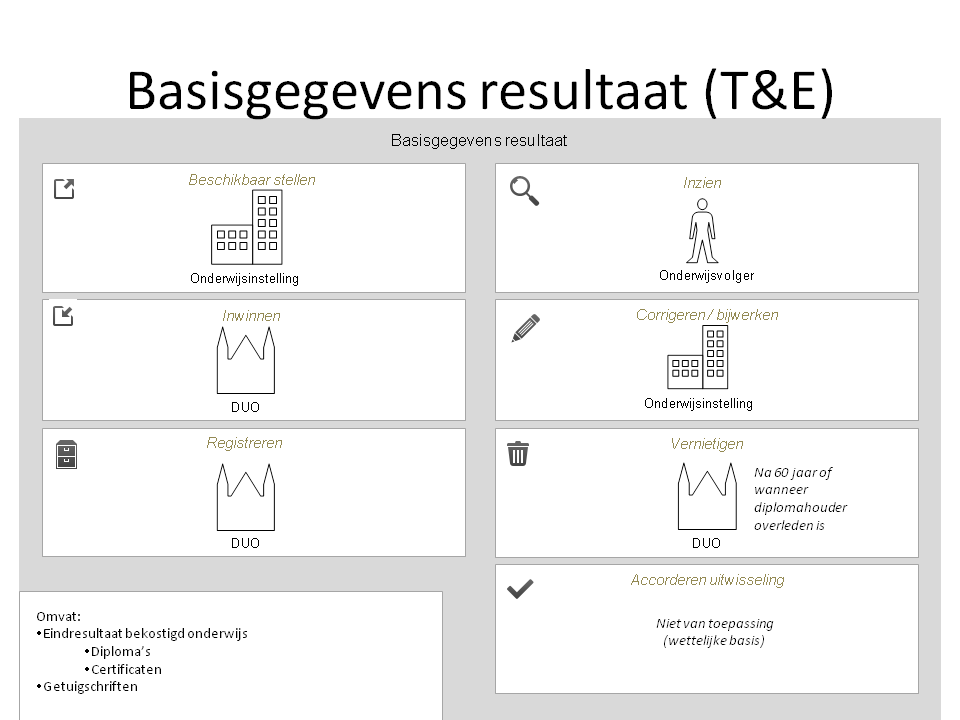
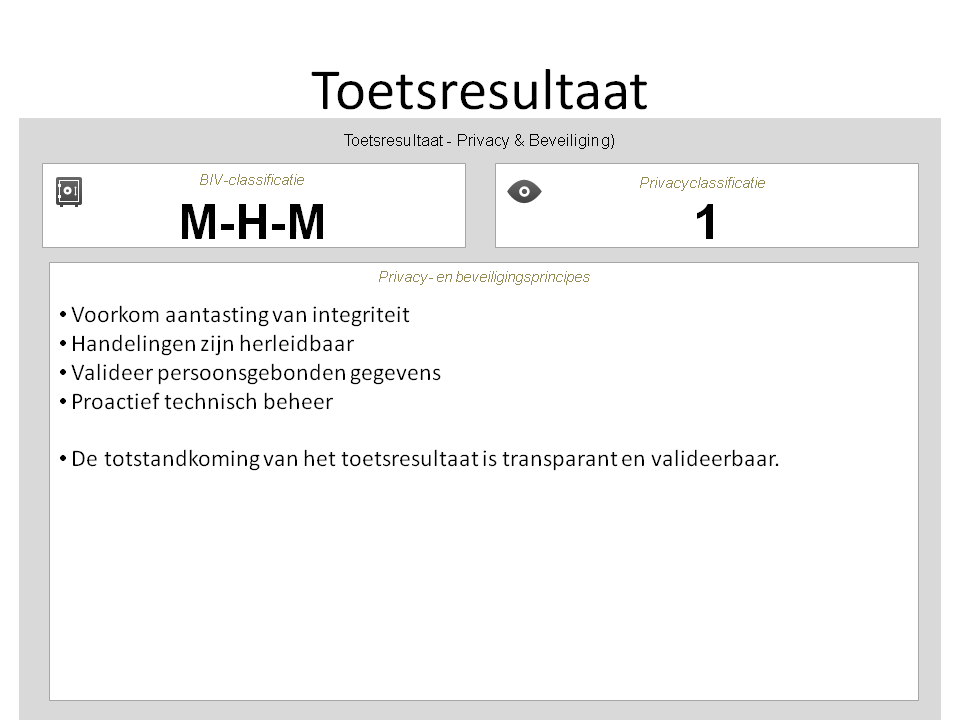
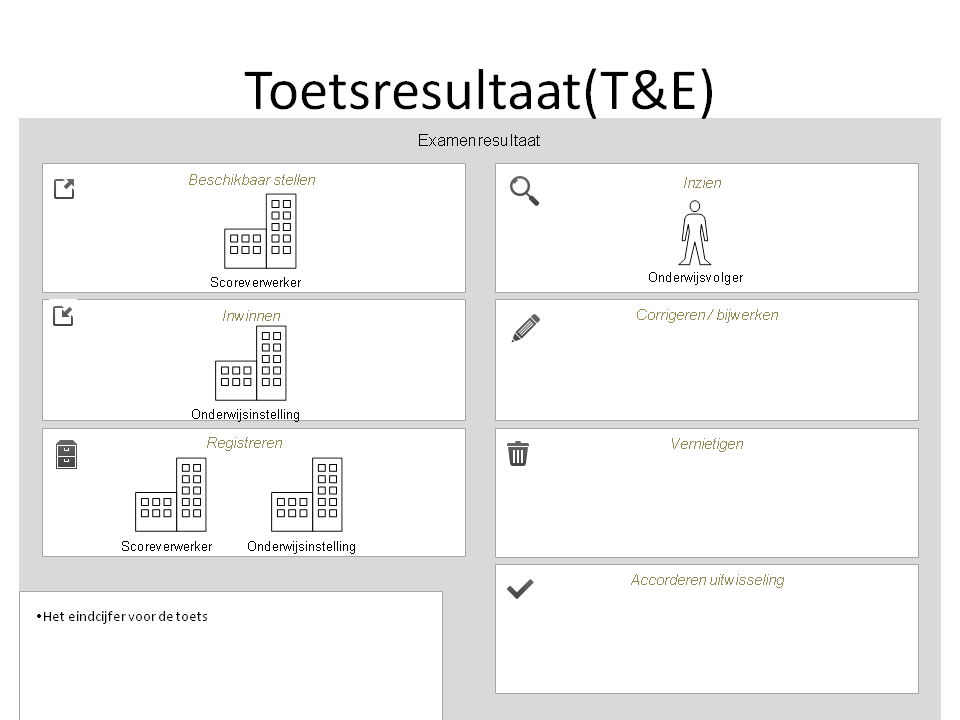
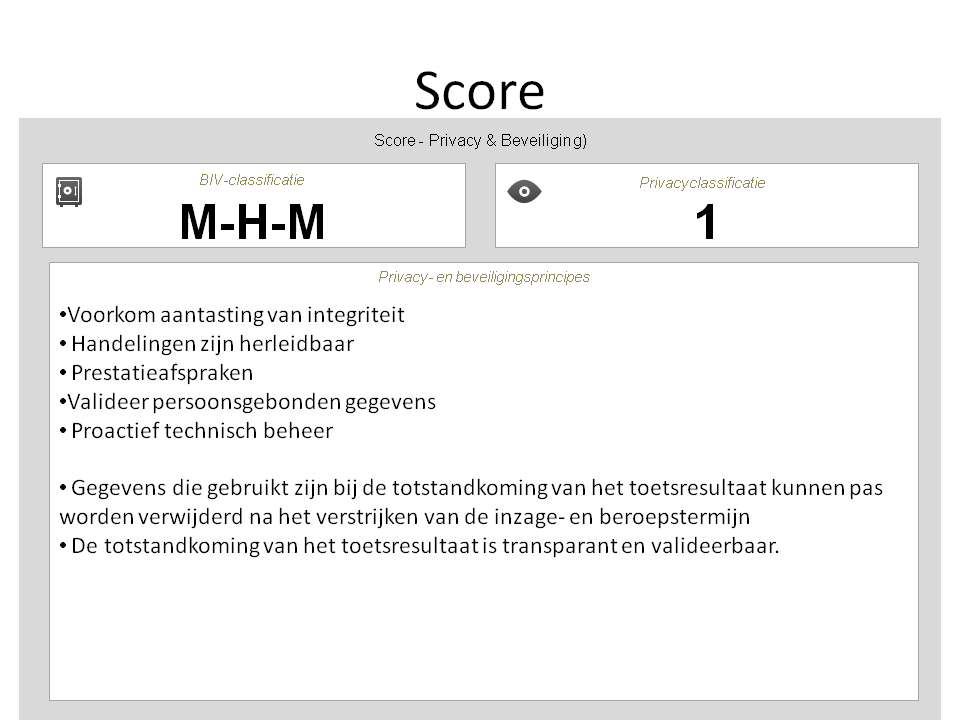
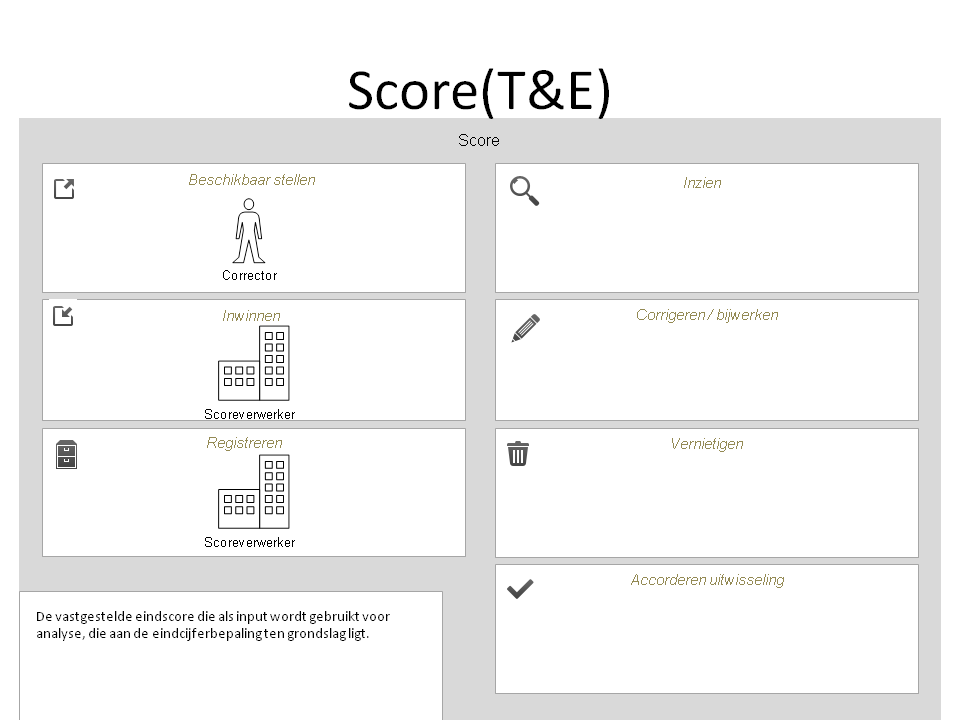
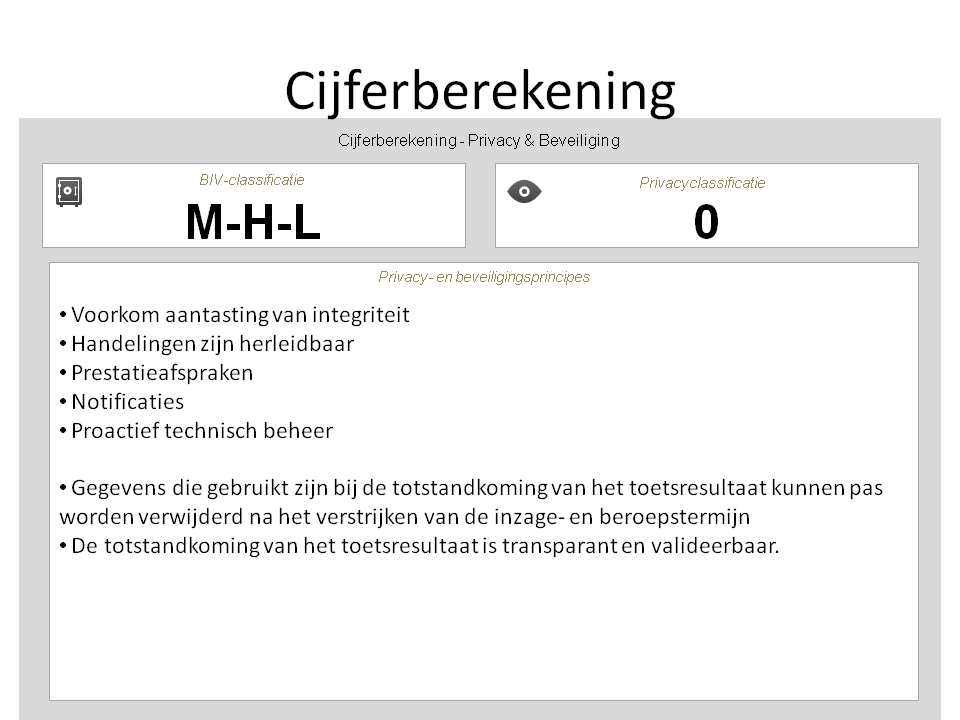
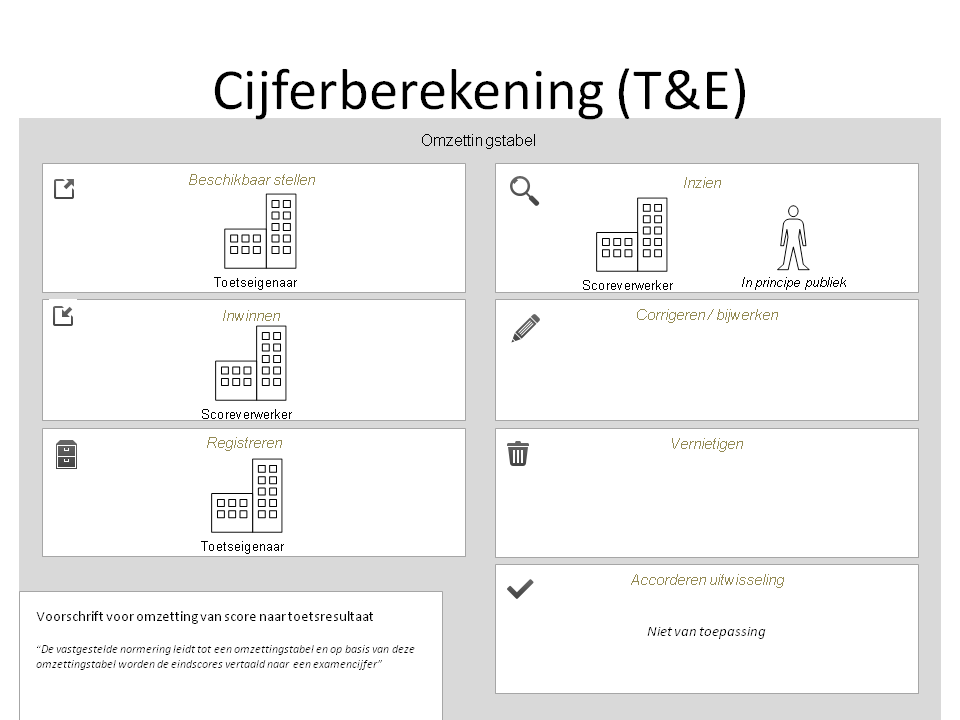
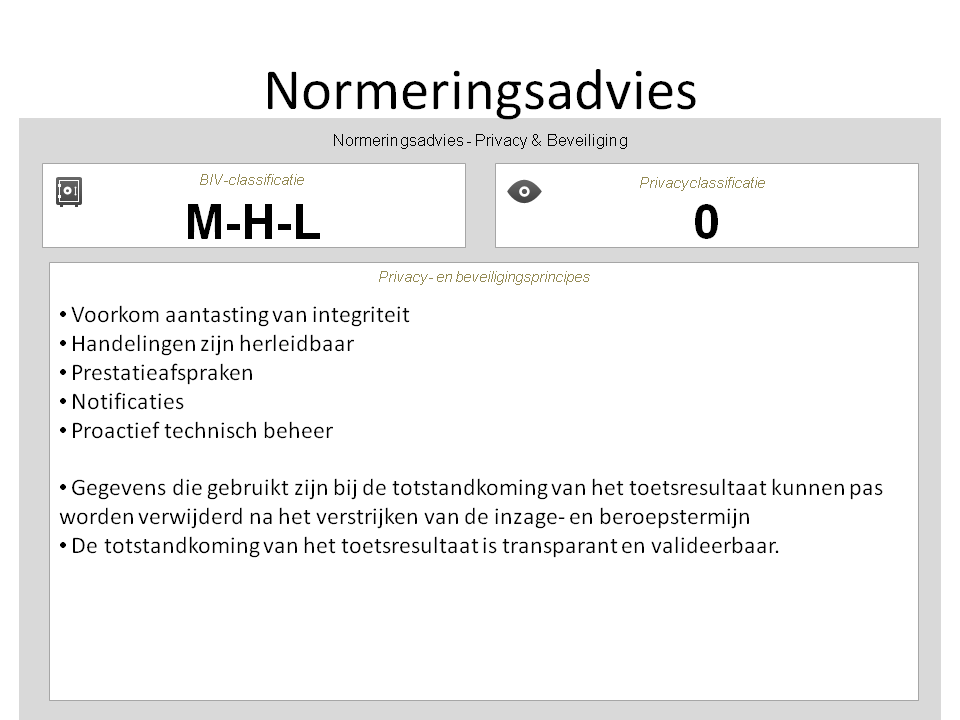
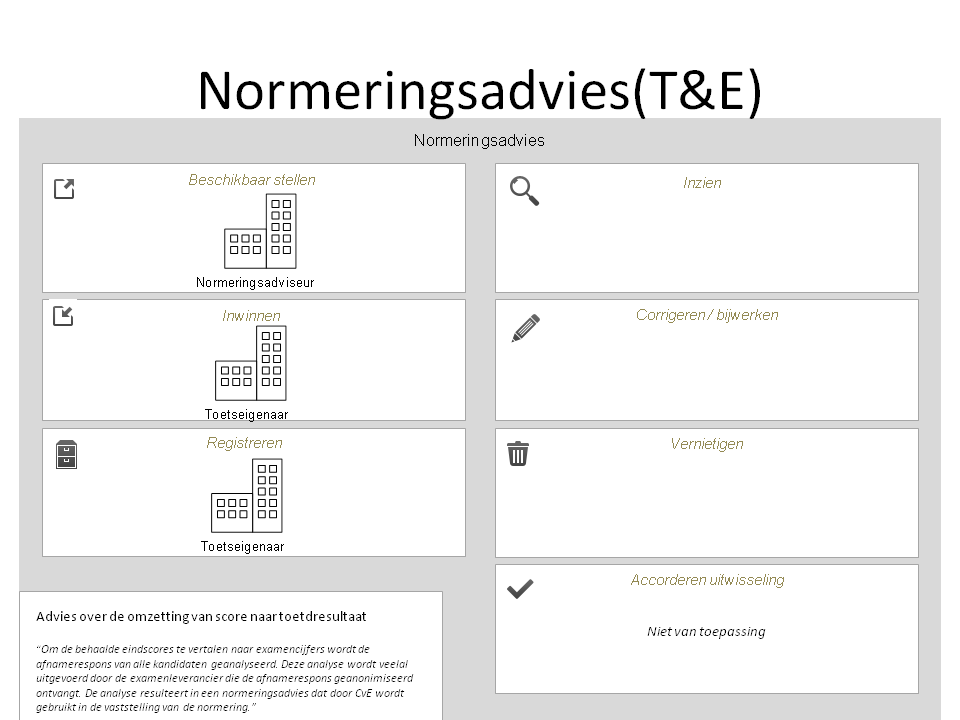
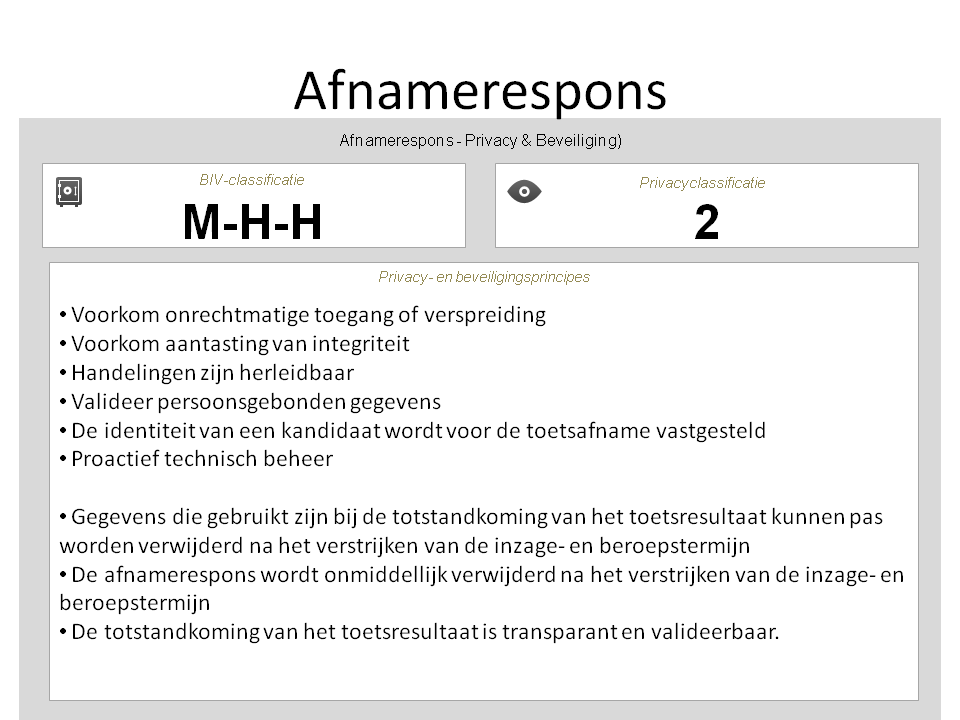
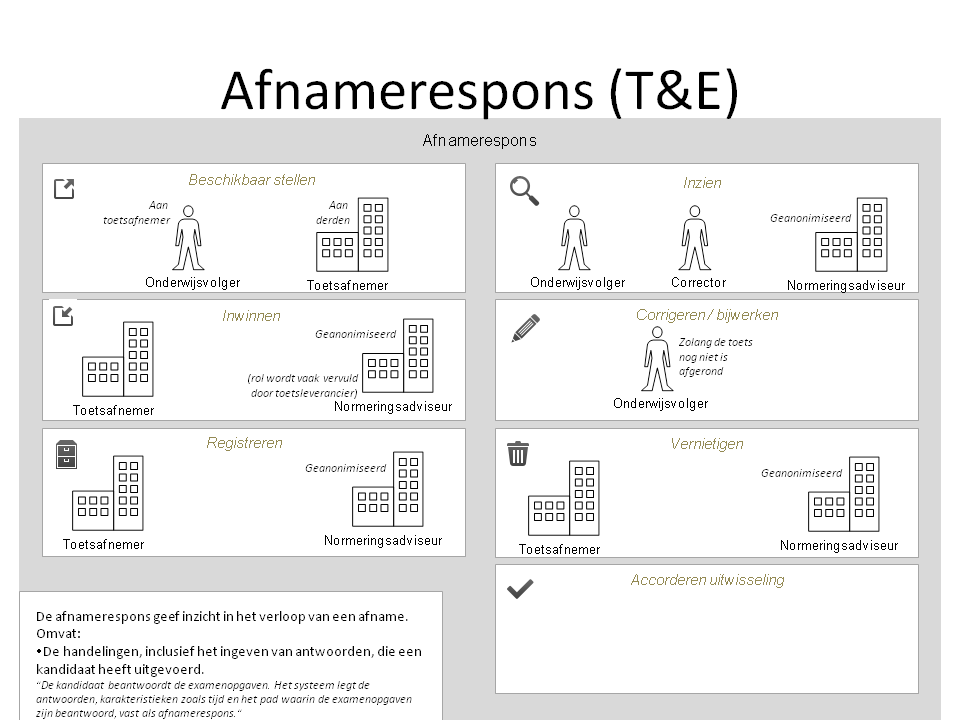
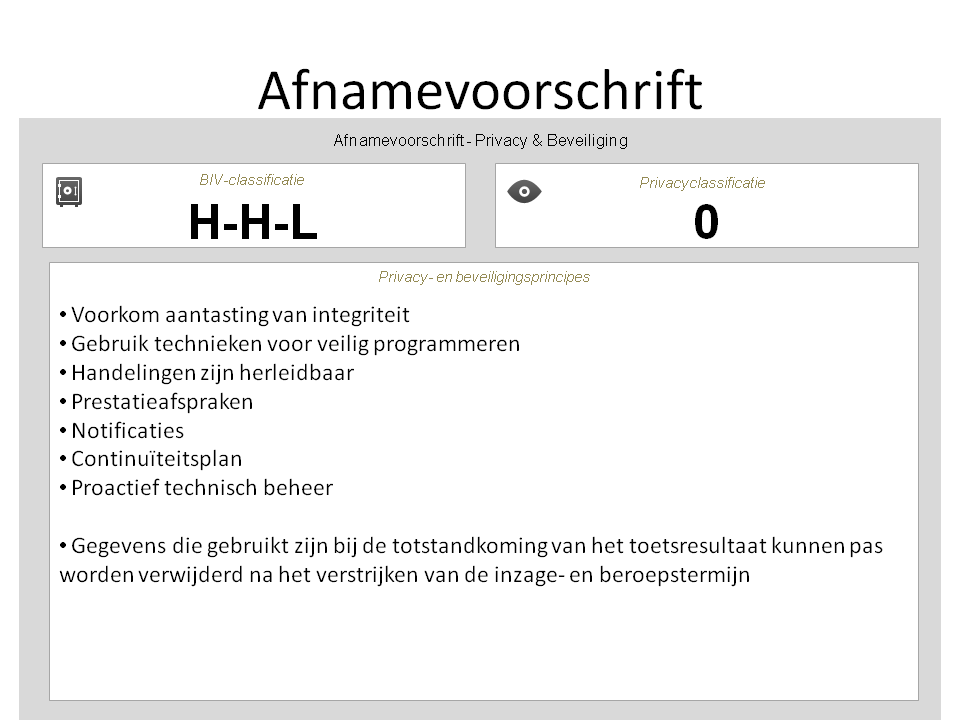
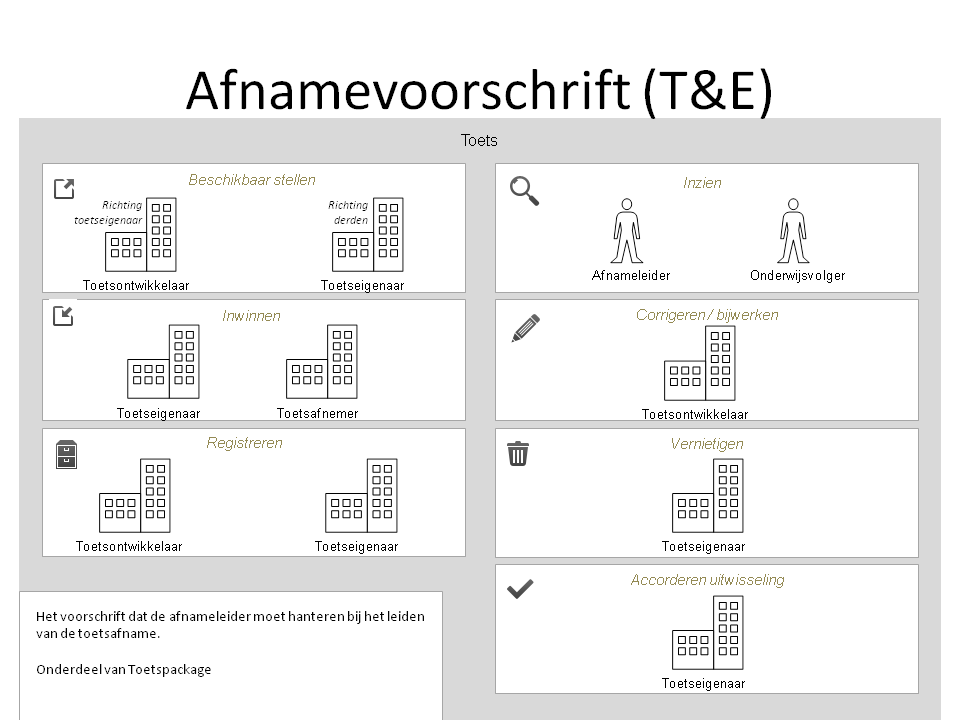
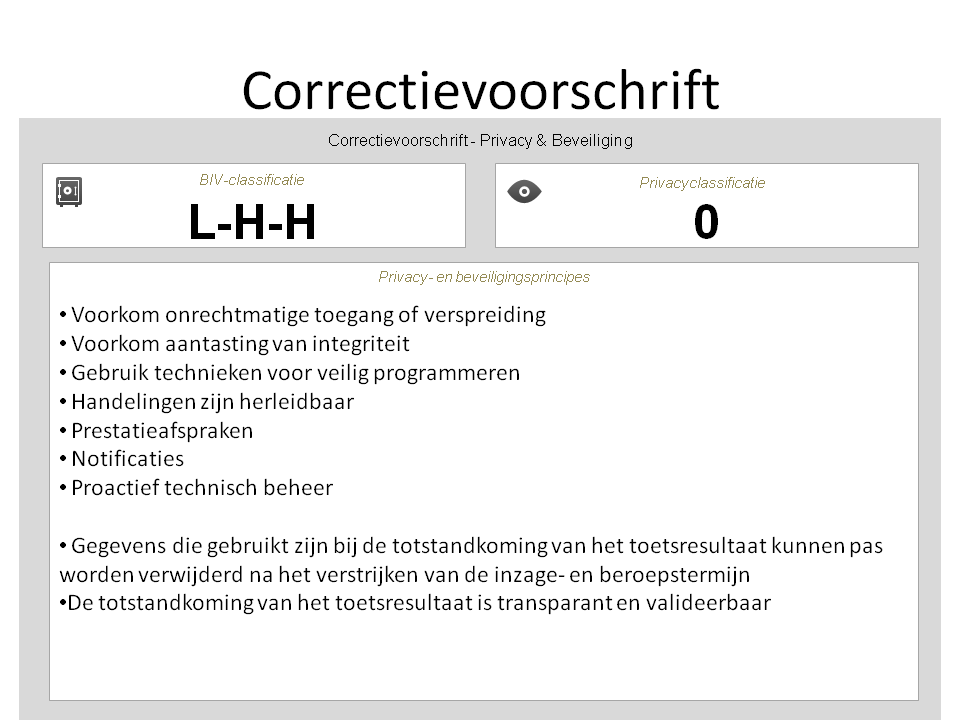
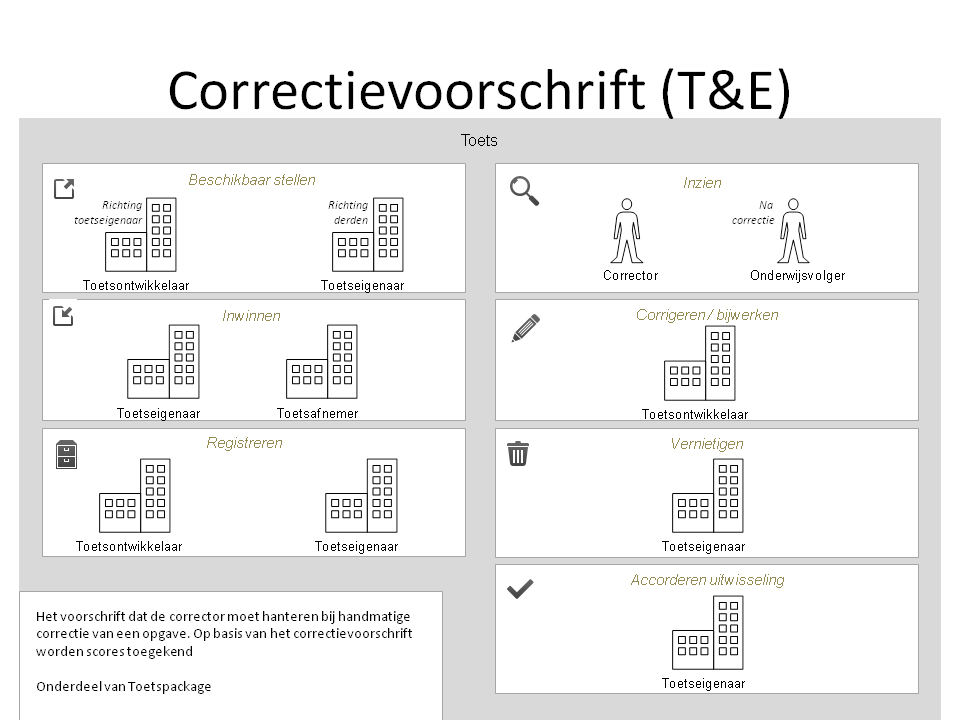
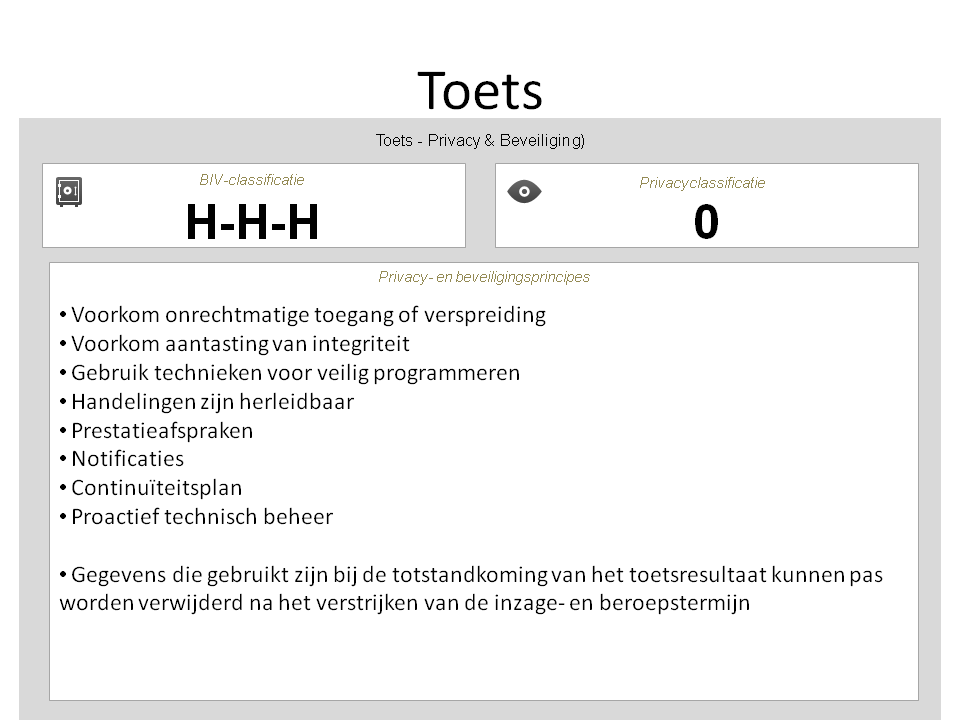
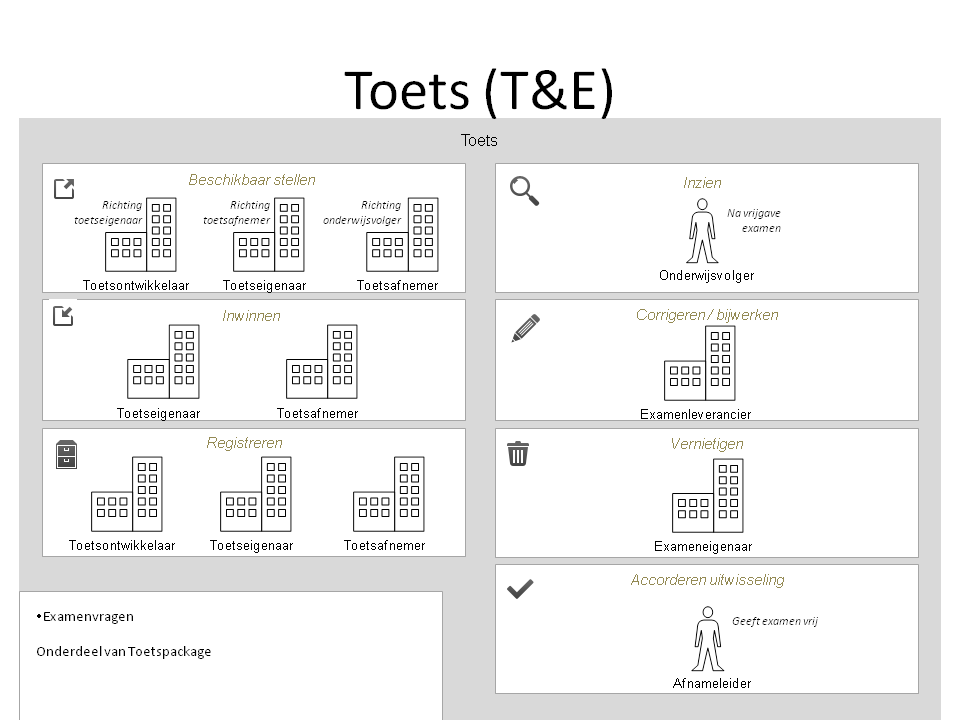
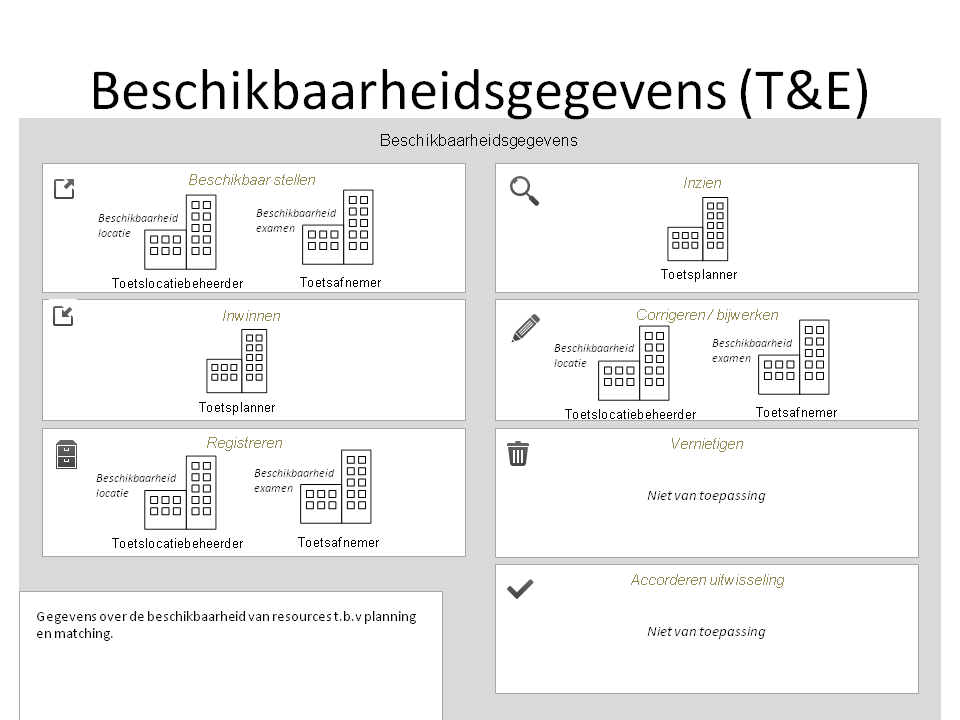
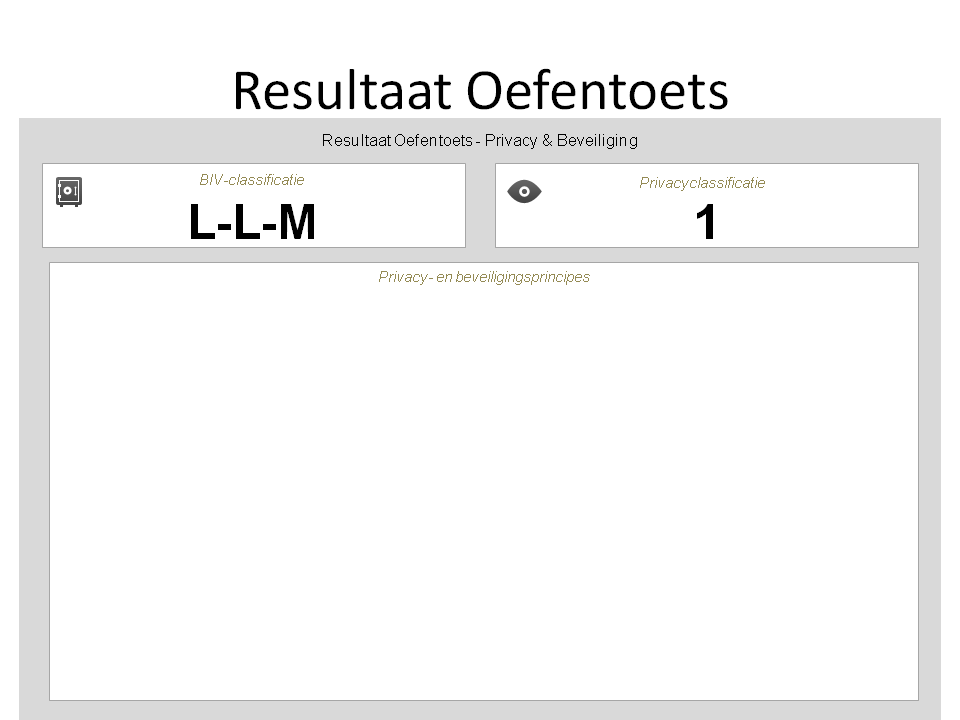
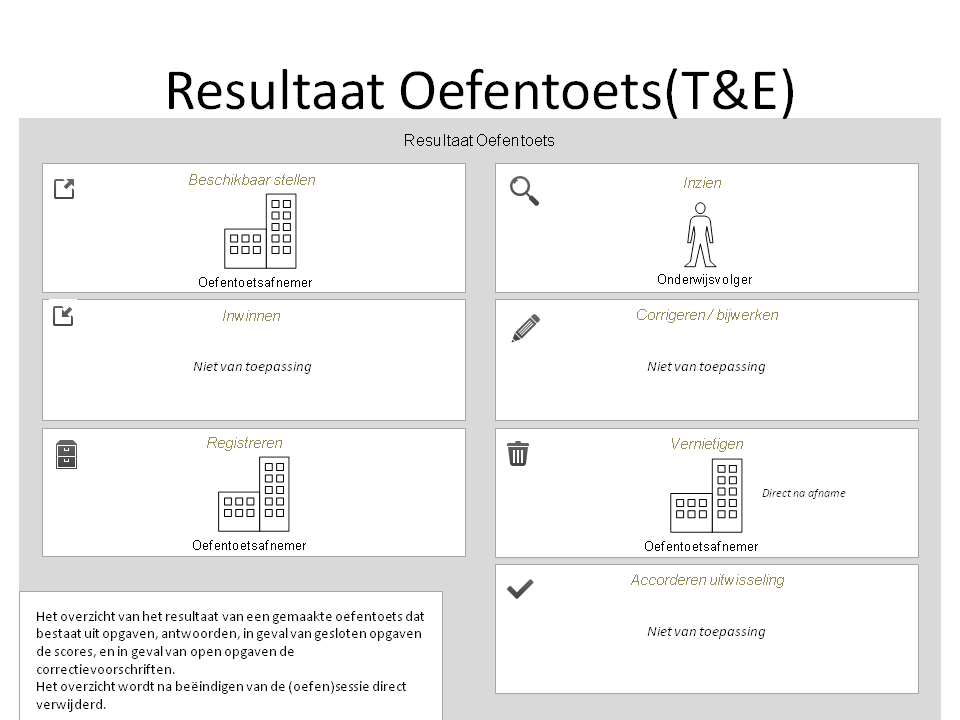
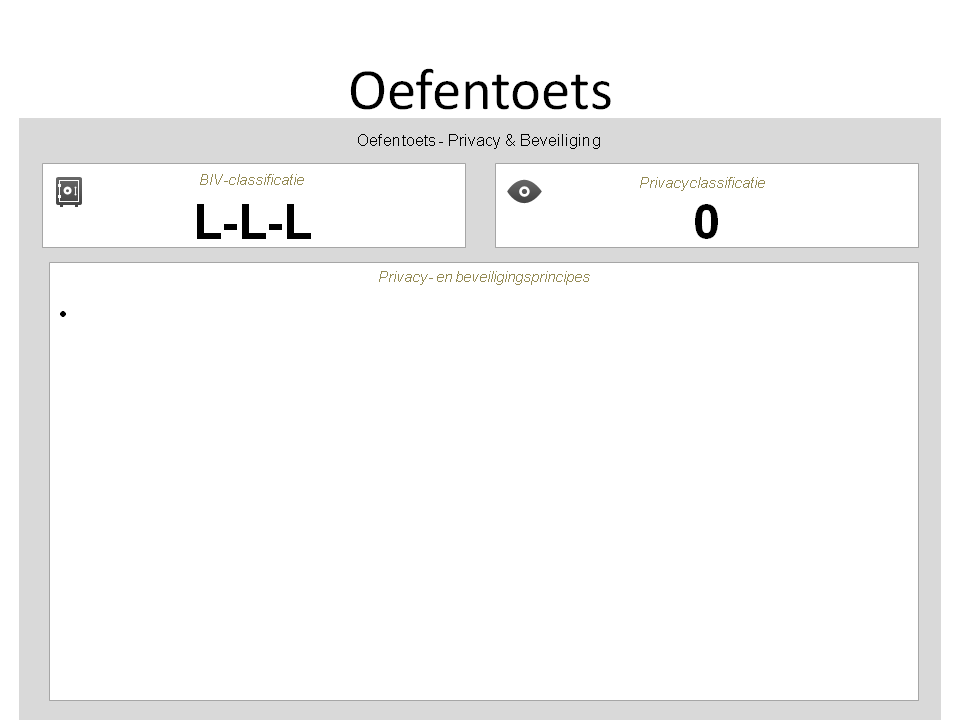
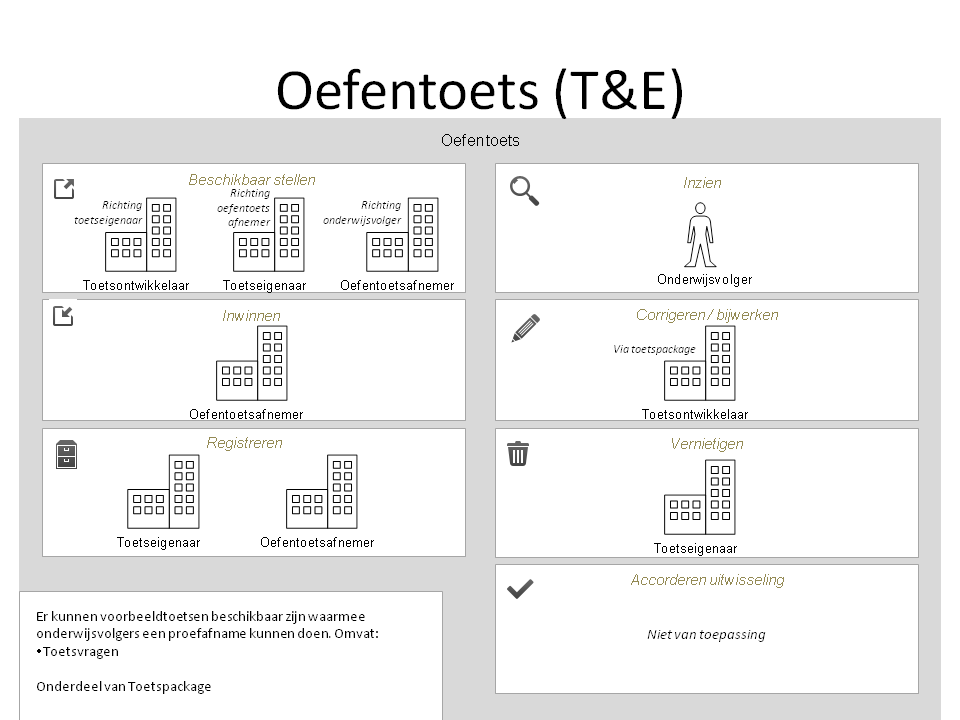
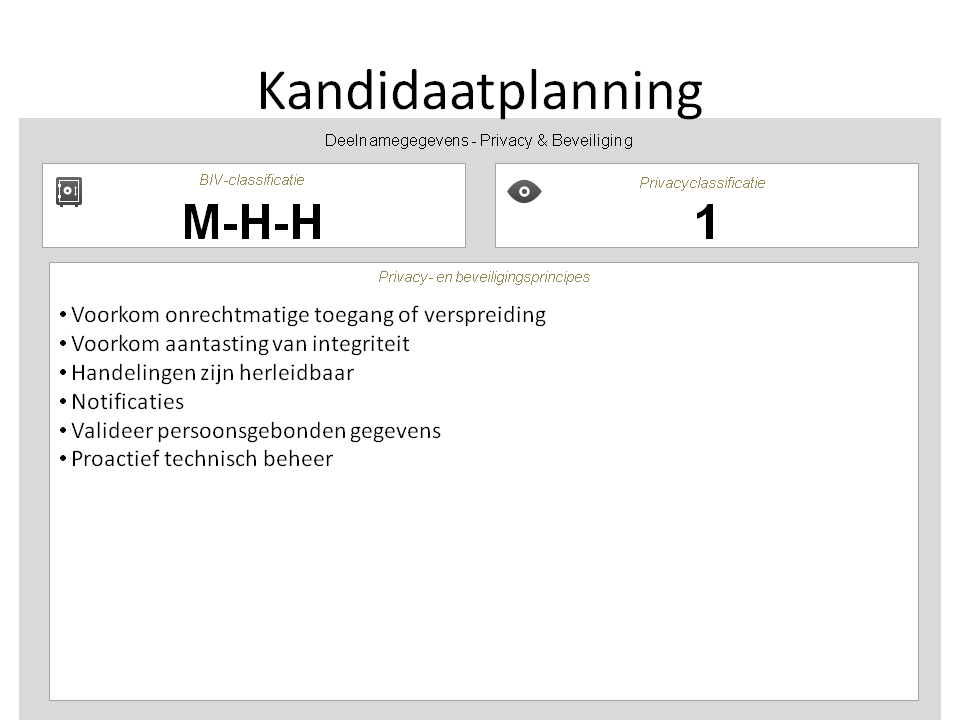
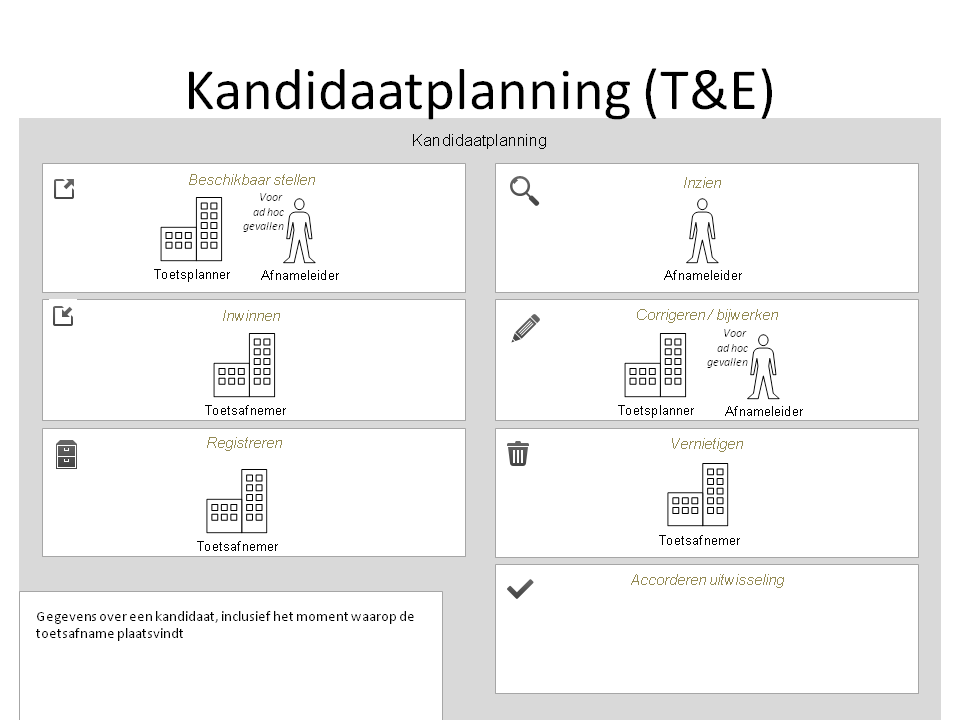
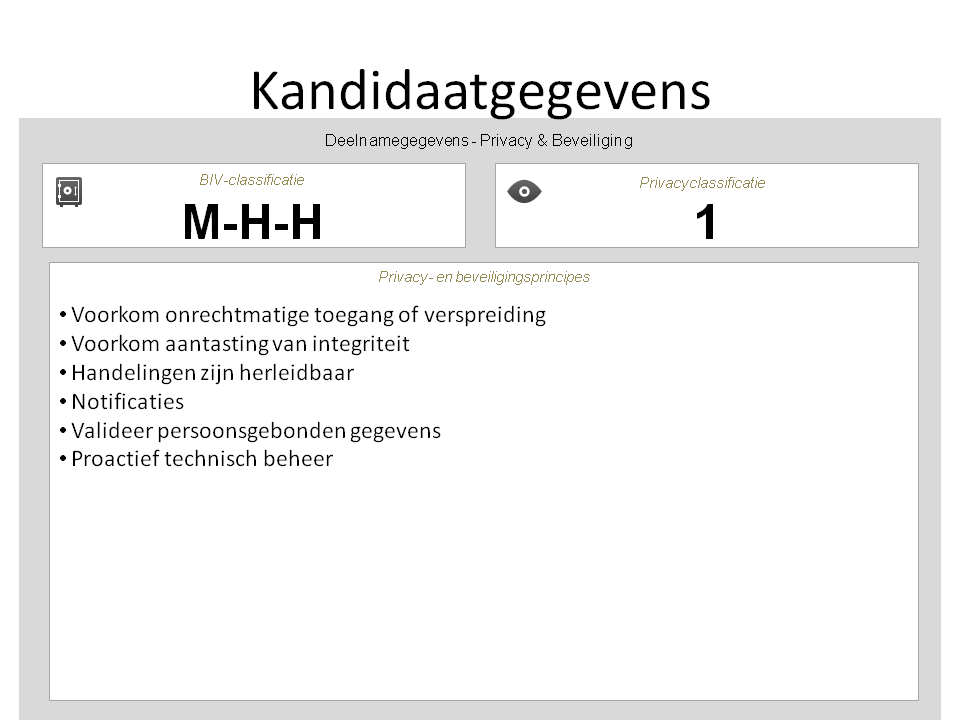
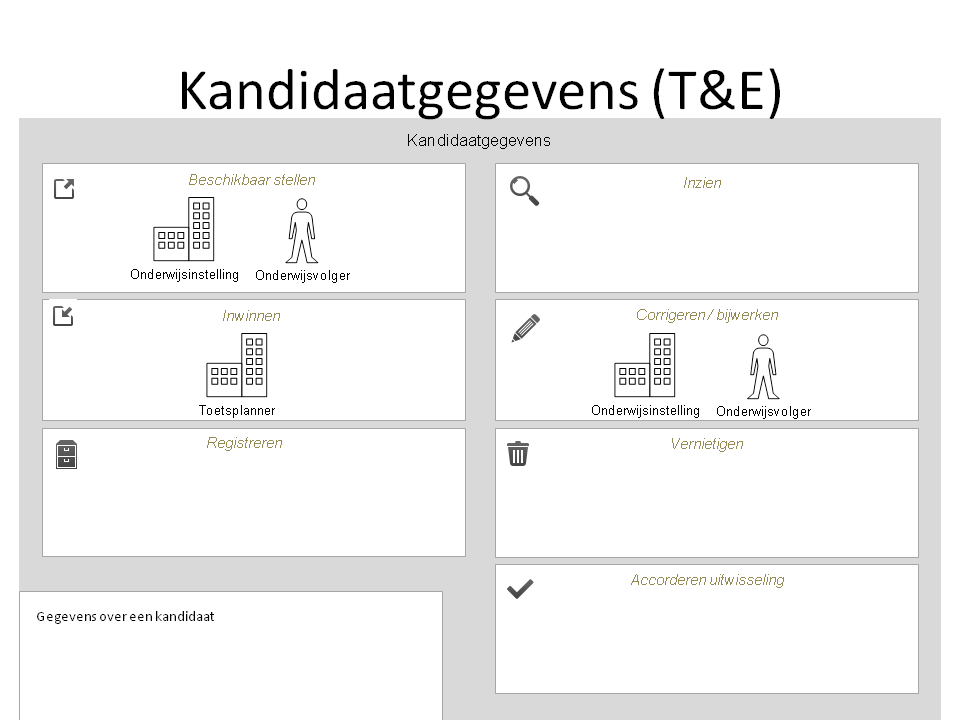
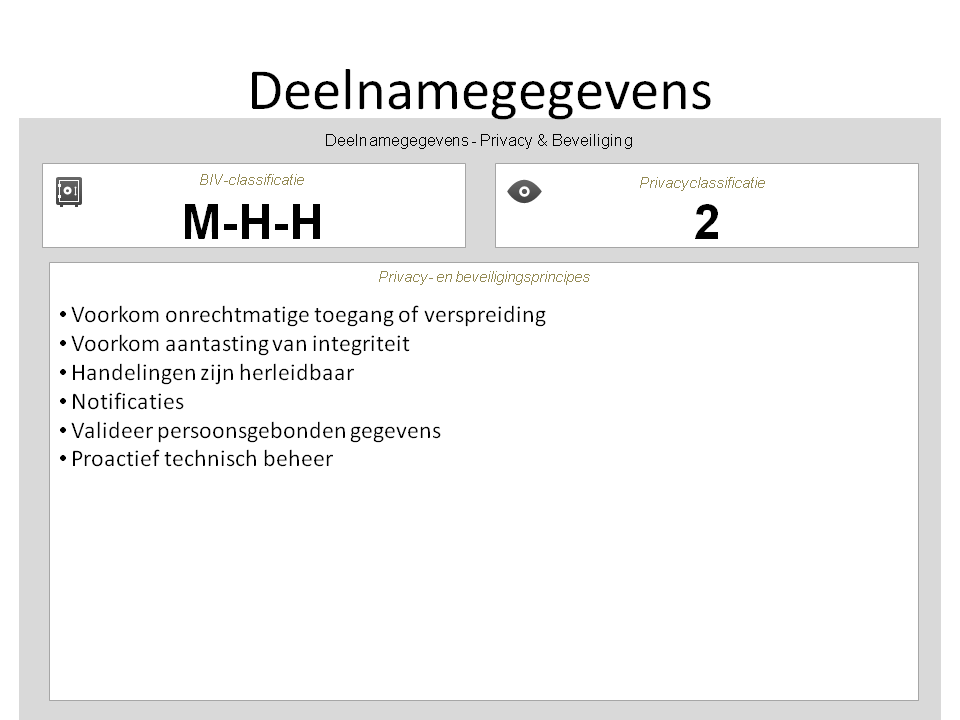
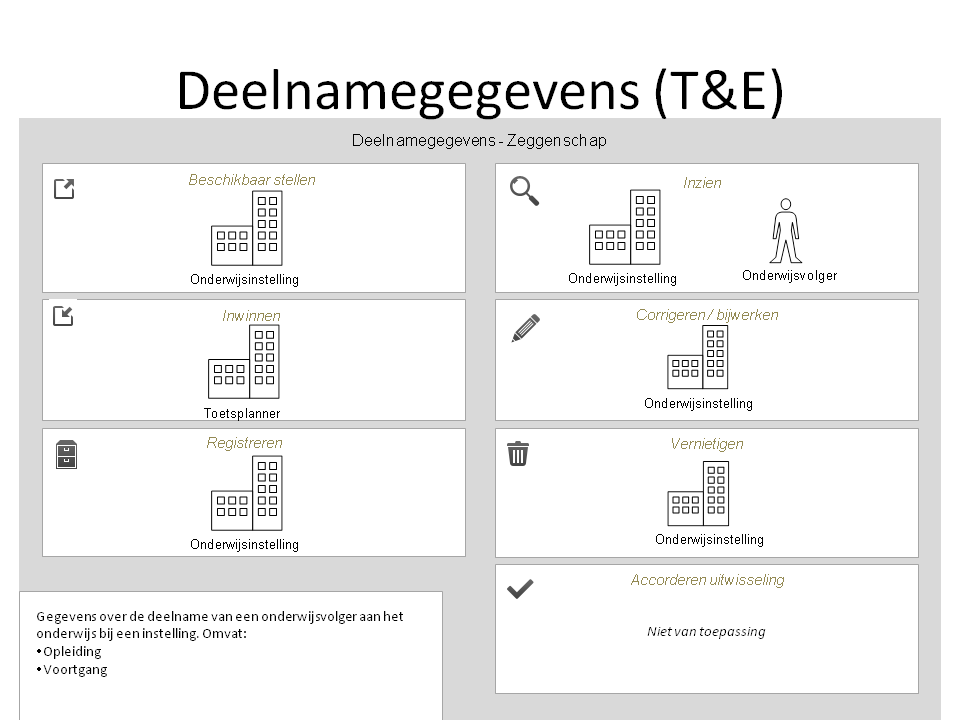
### Informatiebeveiliging door ketenpartijen

Voor de selectie van beheersmaatregelen conform ISO, zie de relatie tussen doelen en beheersmaatregelen in ISO 27002:2013.

# Bijlage: Risicoanalyse Toetsen en Examineren

|  |  |
| --- | --- |
| ***Risico*** | ***Kader*** |
| Geen expertise ogv veilig programmeren | Systemen die de opslag en verwerking van toetsen en toetspackages realiseren, worden ontwikkeld met gebruikmaking van technieken voor veilig programmeren |
| Toetsontwikkelaar levert te laat | Actoren in het toetsproces maken duidelijke afspraken over te realiseren prestaties in de tijd en houden zich daaraan. |
| Kwaliteit toets onvoldoende |
| Beschikt niet over nodige informatie voor normbepaling |
| Neefje maakt de toets | Gegevens met een hoge integriteitsklasse worden zo opgeslagen en getransporteerd dat onrechtmatige aanpassingen onmogelijk worden gemaakt. |
| Aanlevering onversleuteld (onderschepping + manipulatie) |
| Injectie examens |
| Toets vastgesteld door verkeerde persoon |
| Toetsantwoorden kunnen veranderen |
| Wijzigen antwoorden; fraude door afnemer |
| Autorisatie afnamesysteem Read/Write – ongeautoriseerde toegang |
| Toetsen worden achteraf aangepast |
| Score wordt achteraf aangepast |
| Norm wordt aangepast door derden |
| Scores worden achteraf aangepast |
| Toetsresultaat wordt aangepast |
| Hacken en cijfers muteren |
| Kind van medewerker |
| Aanlevering onversleuteld (onderschepping + openbaarmaking) | Gegevens met een hoge vertrouwelijkheidsklasse worden zo opgeslagen en getransporteerd dat onrechtmatige toegang of verspreiding onmogelijk wordt gemaakt. |
| Toets op straat, inhoud examen voortijdig bekend, toets lekt uit |
| Speelt bewust vragen door |
| Examens gestuurd naar verkeerde ontvanger |
| Toets lekt uit, veilig/geheim tot afname |
| Toets niet vertrouwelijk opgeslagen |
| Toets en/of antwoorden lekken uit; toets wordt gestolen |
| Patriot Act, privacy niet geborgd, toetsresultaten zijn gevoelig - 2+ gegevens |
| Antwoorden zijn tijdens toets in te zien |
| Vindbaarheid leerling |
| Uitlekken afnamerespons op persoonsniveau |
| Cijfers lekken uit |
| Openbaarheid uitslagen |
| Vindbaarheid in centrale DB |
| Per ongeluk of te vroeg verwijderen van examens | Gegevens die gebruikt zijn bij de totstandkoming van het toetsresultaat kunnen pas worden verwijderd na het verstrijken van de inzage- en beroepstermijn |
| Toets is kwijt |
| Respons wordt te vroeg verwijderd |
| Respons te laat verwijderd | De afnamerespons wordt onmiddellijk verwijderd na het verstrijken van de inzage- en beroepstermijn |
| Handelingen zijn niet te herleiden naar personen | Handelingen rondom gegevens met een hoge integriteits- of vertrouwelijkheidsklasse zijn te herleiden naar personen |
| Spookaanmeldingen |
| Handelingen niet vastgelegd |
| Last minute correcties | Correcties en aanvullingen op eerder verstuurde gegevens worden onmiddellijk doorgezet naar afnemers van die gegevens. |
| Onjuiste gegevens, score aangepast | De totstandkoming van het toetsresultaat is transparant en valideerbaar. |
| Subjectiviteit normering |
| Rekenfouten bij vaststellen normering |
| Onjuiste gegevens bij normering |
| Score wordt aangepast |
| Bij niet schriftelijk: norm en afname controleerbaar - bevoordeling |
| Onjuiste gegevens score of id, bewust of onbewust |
| Subjectiviteit correctie |
| Verkeerde correctoren toegewezen |
| Bevoordeelt bekenden |
| Onjuiste berekening |
| Bevoordeling bekenden |
| Rekenfout in programmatuur |
| Geen extra in- en uitvoerchecks |
| Inzage onderwijsvolger = transparantie = controleerbaarheid |
| Controleerbaarheid van de uitslag |
| Calamiteit/uitval, DDOS aanval, Toetssysteem niet beschikbaar | Voor resources die op het moment van toetsafname beschikbaar moeten zijn, of waarnaar in aanloop naar de toetsafname een kritieke tijdsafhankelijke relatie bestaat, is een continuïteitsplan beschikbaar |
| Verkeerde toets staat klaar |
| Fouten in afnamegroep |
| De planner is ziek / kapot |
| Plansysteem niet beschikbaar |
| Geen continuiteitsplan |
| Dubbel geboekt |
| Beschikbaarheid wijzigt op laatste moment |
| Uitval docent / ruimte |
| Fout ingepland |
| Mismatch respons-kandidaat | Voor persoonsgebonden gegevens wordt, al dan niet via een terugkoppeling aan de aanleverende partij, gevalideerd of de juist gegevens bij de juiste persoon zijn geregistreerd |
| Niet goed geregistreerd bij aanmelden |
| Wel aangemeld, niet ingepland |
| Onjuiste persoon of koppeling |
| Verkeerde examenresultaten naar DUO |
| Onvoldoende technisch beheer afnamesysteem (patchen, rechten, SQL-injections) | Systemen die gegevens met een hoge beschikbaarheids-, integriteits- of vertrouwelijkheidsklasse verwerken worden proactief technisch beheerd. |
| Identiteitsfraude door onderwijsvolger | De identiteit van een kandidaat wordt voor de toetsafname vastgesteld |
| Integriteit van locatie kan niet gewaarborgd worden - fraude op toilet | De toetslocatie is zo ingericht dat fraude wordt voorkomen |
| Toegang tot locatie niet afgeschermd |
| Afkijken, hulp op afstand |
| Zelfde toets als vorige keer | Buiten scope van beveiliging en privacy |
| Afnamevoorschrift niet te handhaven |
| Toets te laat ingeleverd |
| Worden de juiste en volledige afnamevoorschriften gebruikt? | Integer handelen |
| Afnameleider niet integer |
| Bekenden bevoordelen |
| Frauduleuze medewerker |
| Tweede controle voor menselijke tussenkomst eindoordeel |

# Bijlage: Gegevenskaarten ketenproces Toetsen en Examineren



1. Zie bijvoorbeeld het rapport *Cyberdreigingsbeeld Sector Hoger Onderwijs en Wetenschappelijk Onderzoek* (oktober 2014) voor een inventarisatie van dreigingen in de HO-sector. [↑](#footnote-ref-1)
2. Zie ook het rapport *Nulmeting Privacy & Beveiliging Primair en Voortgezet Onderwijs* (7 april 2014) waarin een inventarisatie is opgenomen van risico's op het gebied van privacy en beveiliging voor instellingen en leerlingen. [↑](#footnote-ref-2)
3. In het NORA Katern Beveiliging zijn beheersmaatregelen en implementatierichtlijnen samengenomen onder de noemer *eisen*. Onder die naam komen ze ook terug in Figuur 2. [↑](#footnote-ref-3)