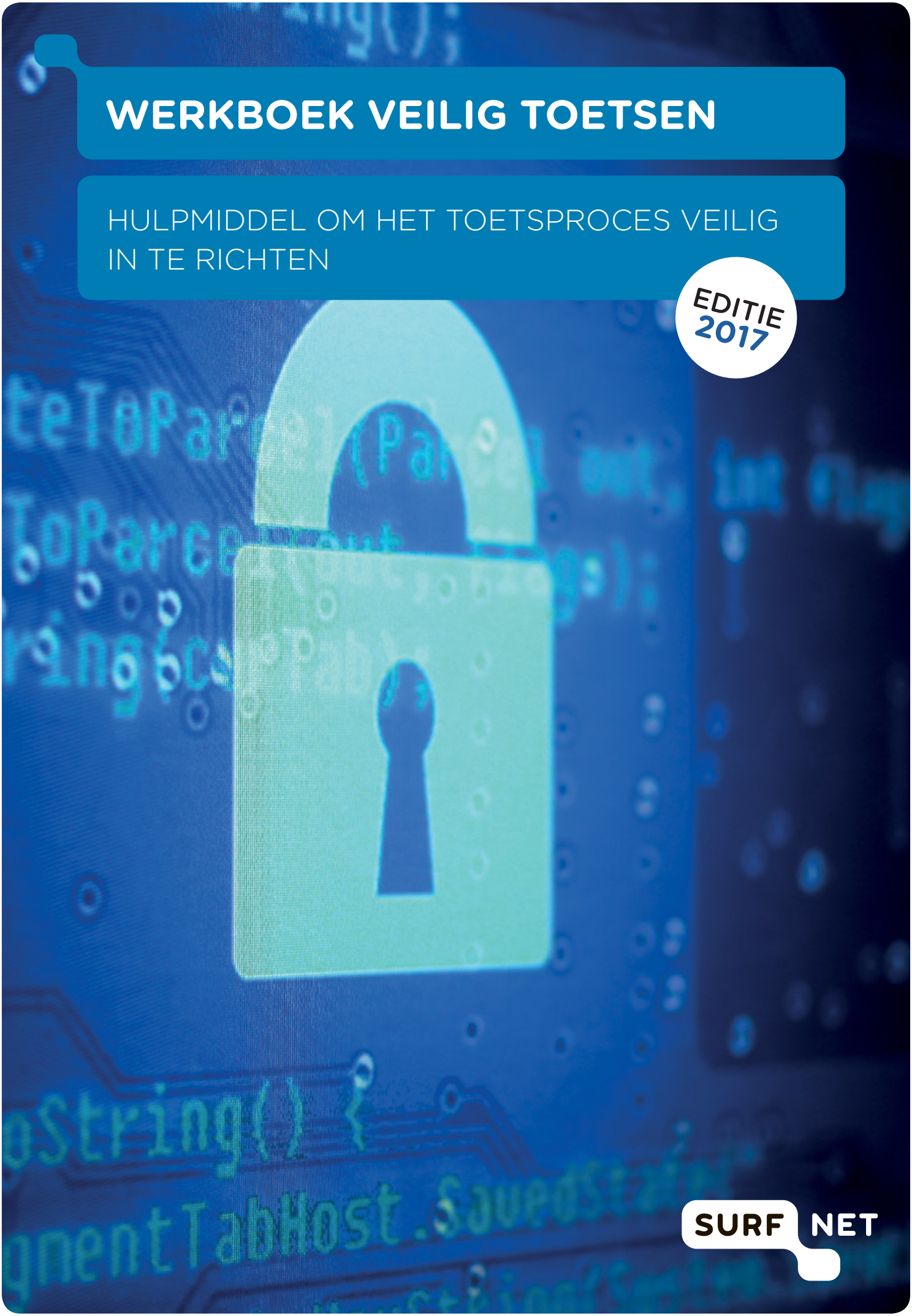
WERKBOEK VEILIG TOETSEN

HULPMIDDEL OM HET TOETSPROCES VEILIG IN TE RICHTEN

EDITIE 2017



SURF NET

INHOUDSOPGAVE

1 INLEIDING

Met de opmars van digitaal toetsen groeit het bewustzijn van instellingen dat de beveiliging van het toetsproces steeds belangrijker wordt. De behoefte om veilig te toetsen strekt verder dan alleen digitaal toetsen, al is het maar omdat docenten ook bij de voorbereiding van papieren toetsen veelvuldig gebruik maken van ICT. Het veilig maken van het toetsproces is niet eenvoudig; er bestaat helaas geen alomvattende ingreep waarmee dit in een keer op te lossen is. Om instellingen te ondersteunen bij het veilig maken van het toetsproces heeft SURFnet samen met experts uit verschillende hogeronderwijsinstellingen dit werkboek ontwikkeld. Daar waar in de tekst 'we' staat bedoelen we deze kerngroep.

1.1. Voor wie

Dit werkboek biedt instellingen handvatten om het gehele toetsproces veilig in te richten. Deze handvatten sluiten zoveel mogelijk aan op bestaande, gangbare beveiligingsrichtlijnen en -normeringen. Het geeft een overzicht van concrete maatregelen om de veiligheid te verhogen.

Het is bedoeld voor medewerkers in instellingen in het hoger onderwijs die zich bezighouden met toetsveiligheid, zoals leden van examen- en toetscommissies, medewerkers van het toetsbureau, functioneel beheerders van toetssoftware en security officers (CISO).

1.2. Scope

Dit werkboek behandelt de volledige toetscyclus (zie figuur 1 op pagina 10) en neemt daarbij ook niet-digitale processtappen in ogenschouw, die nodig zijn om papieren toetsen af te nemen. Daarbij richten we ons met name op die toetsvormen, waar de opgaven vóór de afname van de toets geheim moeten blijven. Dit is van toepassing bij vrijwel alle high stake[1] toetsen die op papier, digitaal of mondeling worden afgenomen. Bij toetsvormen als scripties en andere werkstukken zijn de opgaven doorgaans niet vooraf geheim. Ook bij de verwerking van de resultaten van dergelijke toetsen zal een instelling de processtappen willen volgen: het kan niet de bedoeling zijn dat bijvoorbeeld cijfers onrechtmatig worden gemanipuleerd of dat gearchiveerde toetsen zoekraken.

Dit werkboek maakt gebruik van de gangbare begrippen uit de informatiebeveiliging. In het bijzonder beschikbaarheid, integriteit en vertrouwelijkheid (BIV), controleerbaarheid en privacy. Zie tabel 1 voor de uitleg van de gebruikte termen.

- *Privacy:* een thema dat steeds meer aandacht vraagt, vooral onder invloed van de nieuwe Algemene Verordening Gegevensbescherming. Vanzelfsprekend is dit thema ook bij toetsen aan de orde en in het bijzonder bij digitaal toetsen. In dit werkboek gaan we hier niet nader op in.

In dit werkboek gaan we in geval van digitale afname uit van het gebruik van computerapparatuur van de instelling en van afname binnen de muren van de instelling.

[1] High stake toetsen zijn toetsen waar voor de student veel van afhangt, bijvoorbeeld een toets die leidt tot een eindcijfer van een vak.

Aan onderstaande aspecten wordt daarom niet specifiek aandacht besteed:

- *Bring Your Own Device (BYOD)* in relatie tot digitaal toetsen: enkele instellingen verkennen deze aanpak, maar er is nog onvoldoende kennis over en ervaring mee om het dit werkboek op te nemen.
- *Online proctoring:* deze oplossing maakt een gestage groei door. Voor de specifieke aspecten die ermee gepaard gaan verwijzen we naar aparte publicaties over dit onderwerp.[2]

Term	Betekenis
BIV-classificatie	Een BIV-classificatie of BIV-indeling is een indeling waarbij beschikbaarheid (continuïteit), integriteit (betrouwbaarheid) en vertrouwelijkheid (exclusiviteit) van informatie en systemen wordt aangegeven.[3] Deze indeling wordt veel gebruikt in het kader van informatiebeveiliging.
Beschikbaarheid	Geeft aan in hoeverre een ICT-dienst, -systeem of -component toegankelijk is voor de geautoriseerde gebruikers. Beschikbaarheid wordt in de regel als een percentage gepresenteerd.
Integriteit	Het in overeenstemming zijn van informatie met de werkelijkheid: informatie is juist, volledig en actueel.
Vertrouwelijkheid	Is een kwaliteitskenmerk van gegevens. Vertrouwelijkheid betekent dat een gegeven alleen te benaderen is door iemand die hiervoor gemachtigd is.

Tabel 1. Gebruikte termen

1.3. Verantwoording

Bij het samenstellen van dit werkboek hebben we gebruik gemaakt van het Begrippenkader voor digitaal toetsen[4] en het richtsnoer Veilige digitale toetsafname[5]. Het richtsnoer gaat in detail in op het proces van digitale toetsafname. Dit werkboek richt zich op de beveiliging van de gehele toetsketen en beperkt zich niet tot digitale toetsafname. Beide uitgaven kun je naast elkaar gebruiken.

Daarnaast sluit dit werkboek nauw aan op het gedachtegoed zoals dat wordt gehanteerd in Normenkader Informatiebeveiliging Hoger Onderwijs[6]. Dit normenkader is te beschouwen als fundament onder het werkboek veilig toetsen.

Als startpunt voor dit werkboek zijn de toetsprocessen van vijf instellingen geanalyseerd. Op basis hiervan is samen met toetsexperts van deze instellingen het 'model' toetsproces (bijlage 1) uitgeschreven. Het modeltoetsproces is vervolgens gebruikt om in detail de risico's per stap in de toetscyclus in kaart te brengen en daarbij maatregelen te formuleren. Deze uitwerking is voorgelegd aan de eerdergenoemde toetsexperts uit de instellingen en aan een aantal security officers in het hoger onderwijs. Zie het colofon voor een overzicht van alle betrokkenen die hebben bijgedragen aan dit werkboek.

Versie 2
Deze tweede versie van dit werkboek is op grond van gebruikerservaringen een aantal kleine verbeteringen en correcties doorgevoerd.

Daarnaast is in deze versie het aspect Beschikbaarheid opgenomen en is het proces 'Beheer' vrij ingrijpend herzien.

[2] https://www.surf.nl/themas/onderwijsinnovatie-met-ict/digitaal-toetsen/digitale-toetsafname/index.html
[3] https://nl.wikipedia.org/wiki/BIV-classificatie
[4] Begrippenkader voor digitaal toetsen (SURF, 2013) https://www.surf.nl/kennisbank/2013/begrippenkader-voor-digitaal-toetsen.html
[5] Richtsnoer Veilige digitale toetsafname (SURF, 2014) https://www.surf.nl/kennisbank/2013/richtsnoer-veilige-digitale-toetsafname.html
[6] https://www.surf.nl/binaries/content/assets/surf/nl/2015/normenkader-informatiebeveiliging-ho-2015-v1.3.pdf

INTERMEZZO

SCHETSEN UIT DE TOETSPRAKTIJK: RISICO'S EN AANDACHTSPUNTEN

Aan de hand van een aantal praktijksituaties laten we zien waar risico's en aandachtspunten in het toetsproces kunnen liggen. De voorbeelden zijn uitsluitend bedoeld ter illustratie, in werkelijkheid zullen ook andere risico's aan de orde kunnen zijn. Elke situatie wordt eerst geschetst vanuit een instelling die toetsveiligheid niet op orde heeft en vervolgens vanuit een instelling waar dit wel het geval is.

SAMEN TOETSVRAGEN MAKEN EN REVIEWEN

Twee docenten van een hogeronderwijsinstelling maken samen toetsvragen voor een vak.

Onveilige praktijk

Beide docenten maken de toetsvragen regelmatig op hun privé-tablet in de trein via de NS-wifi. Eén van hen heeft in het verleden een Word-document gemaakt en dit document versturen ze via e-mail naar elkaar. Om-en-om vullen ze dit document aan en geven het document een versienummer zodat ze de draad niet kwijtraken. De één slaat het document op in Dropbox en de ander gebruikt Google Drive. De vragen laten ze reviewen door een collega die bijna altijd op dezelfde werkplek zit. Deze collega blokkeert nooit haar beeldscherm. Ook doet ze haar kamer niet op slot als ze weggaat om bijvoorbeeld koffie te halen.

Veilige praktijk

Beide docenten werken op verschillende locaties. Als de twee docenten samenwerken gebruiken ze de speciaal ingerichte veilige toetsomgeving van de instelling. Hierin plaatsen zij hun gedeelde document. Een collega-docent (toetsexpert) reviewt de toetsvragen voor hen. Deze collega werkt bijna altijd op dezelfde werkplek. De reviewende collega-docent heeft geen toegang tot de beveiligde map van de twee docenten en vraagt een reviewversie via e-mail. Zij versturen het Word-document versleuteld naar hem via e-mail en het wachtwoord voor het document per SMS. Om te voorkomen dat onbevoegden zich ongeoorloofd toegang verschaffen tot werkplekken, blokkeren de beeldschermen van de werkplekken altijd automatisch na 10 minuten. Verder zijn de docenten geïnstrueerd altijd hun scherm te blokkeren als zij hun werkplek verlaten en het management ziet hierop toe.

TOETSEN VOORBEREIDEN

De docenten hebben 80 toetsvragen definitief gemaakt. Zij gaan een tentamen met 40 vragen digitaal afnemen. Voor een aantal uitzonderingsgevallen moet ook een papieren versie van het tentamen beschikbaar zijn.

Onveilige praktijk

Voor de papieren toets hebben ze afgesproken dat één van hen 40 vragen selecteert en deze op een USB-stick zet. De USB-stick leggen ze in hun postvak in de docentenkamer. De andere docent haalt de stick daar op en zet de vragen in de toetstemplate. Hij gebruikt hiervoor zijn privé-tablet omdat hij dat gemakkelijker vindt. Hij stuurt de toets via e-mail naar een externe repro, omdat de interne repro die week geen tijd heeft.

Veilige praktijk

Voor de papieren toets hebben ze afgesproken dat één van hen 40 vragen selecteert, en deze in de beveiligde omgeving zet. De andere docent zet deze in de juiste toetstemplate en zal de prints via de repro regelen, omdat zij niet zelf vanuit de veilige toetsomgeving kunnen printen. De repro print uitsluitend toetsen die worden aangeleverd via de beveiligde toetsomgeving. De docenten leveren hun toets via de beveiligde omgeving aan, vergezeld van een formulier met aantallen en andere gegevens. Inmiddels is ook het toetsbureau op de hoogte van de aankomende toets.

PAPIEREN TOETS BIJ DE REPRO

De repro print de gevraagde papieren toetsen.

Onveilige praktijk

De repro print de papieren toetsen en informeert het onderwijsbureau, dat de toetsen klaarliggen en kunnen worden afgehaald. Een medewerker van het onderwijsbureau krijgt de tentamens mee in een verzegelde enveloppe en geeft deze aan de docent die het tentamen gaat afnemen. Omdat het tentamen pas over een week plaatsvindt, ligt de enveloppe tot die tijd op het bureau van de docent.

Veilige praktijk

De repro print de papieren versies van de toets niet eerder dan drie dagen voor het tentamen. Direct na het printen worden de toetsen in een verzegelde enveloppe bewaard in de afsluitbare en met camera bewaakte bergruimte naast de repro. De instelling heeft als regel dat de repro de toetsen just-in-time aflevert bij het toetsbureau. Het toetsbureau draagt zorg voor veilige bewaring in een afgesloten ruimte waarvoor een strikt toegangsbeleid geldt. Pas een uur vóór de toets kan de docent of de surveillant de toets daar ophalen.

NAKIJKEN VAN DE TOETS

De toets is gemaakt. Een dag na de toetsafname staan de resultaten van de digitaal afgenomen toets klaar in de toetsapplicatie. De docenten hebben de gemaakte papieren tentamens opgehaald bij het onderwijsbureau. Een docent doet de eerste correctie, vervolgens bekijkt de tweede docent de toetsen die rond de 6 uitkomen.

Onveilige praktijk

De papieren tentamens liggen de rest van de dag op het bureau van de docent, terwijl deze voor de klas staat. Er zijn 6 twijfelgevallen die de tweede corrector nog een keer nakijkt. Deze schrijft op de papieren tentamens zijn eigen beoordeling en overschrijft in de cijferlijst in Excel het eerder gegeven cijfer. De docent stuurt deze file dan via e-mail naar de administratie.

Veilige praktijk

De docent staat de rest van de dag voor de klas en legt de tentamens in zijn kluisje totdat hij tijd heeft om deze na te kijken.

Om in te loggen in de beveiligde omgeving is een extra toegangscode nodig. De docent kiest ervoor de code via SMS te ontvangen. Er zijn 6 twijfelgevallen die de tweede corrector nog een keer nakijkt. Deze schrijft op de papieren tentamens zijn eigen beoordeling. Een typefout in de digitale cijferlijst (die in de beveiligde omgeving staat) is snel gemaakt. Daarom laat de docent zowel op de papieren versie als in de digitale totaallijst de beoordeling door de eerste corrector staan. Hij voegt zijn eigen beoordeling in een aparte kolom toe zodat de historie vastligt.

INZAGE TENTAMEN STUDENTEN

De studenten kunnen op een bepaald moment hun gemaakte toets digitaal of op papier inkijken in een toetslokaal.

Onveilige praktijk

De studenten bekijken in het toetslokaal hun resultaat in de digitale toetsomgeving, maar de docent is vergeten dit moment door te geven aan het toetsbureau; de medewerkers daar zorgen dat de studenten alleen leesrechten hebben en niet bij andere applicaties kunnen. Nu hebben zij zowel lees- als schrijfrechten en kunnen ze bij andere internet applicaties. De docent vertrouwt zijn studenten wel, ze zullen de toetsvragen niet zo gauw via e-mail wereldkundig maken. Degene die hun toets op papier hebben gemaakt kunnen deze inzien in de kamer van de docent. De docent gelooft er niet in dat studenten de antwoorden stiekem zullen wijzigen. Zo'n vaart zal het allemaal niet lopen. Hij ontvangt soms meer dan 6 studenten tegelijk in zijn kamer.

Als een student het niet eens is met zijn cijfer bespreekt hij dit met de docent. De docent wijzigt het cijfer ook ter plekke in het systeem.

Veilige praktijk

De studenten kunnen op een bepaald moment hun gemaakte toets digitaal inkijken in een toetslokaal binnen de beveiligde toetsomgeving, waarbij ze geen toegang hebben tot bijvoorbeeld e-mail. Zij hebben alleen leesrechten. Als ze vragen hebben kunnen ze dit ter plekke aangeven bij de aanwezige docent. Degene die hun toets op papier hebben gemaakt, kunnen deze inzien in de docentkamer. Zij worden per tweetal naar binnen geroepen. De docent blijft erbij aanwezig. Mobiele telefoons zijn niet toegestaan en de tassen van de studenten staan bij de docent. De docent zorgt er op deze manier altijd voor dat studenten geen toegang hebben of kunnen krijgen tot zaken die niet voor hen bestemd zijn. Zijn bureau is altijd leeg. Ook is het verboden om papieren tentamens in eigen kasten te bewaren.

Als een student het niet eens is met zijn cijfer bespreekt hij dit met de aanwezige docent. De docent maakt hiervan een notitie en zal na afloop de wijzigingen doorvoeren in de beveiligde omgeving waar hij altijd door middel van dubbele authenticatie moet inloggen.

BEHEREN VAN TOETSEN

Als alle cijfers definitief zijn, worden de toets en de toetsresultaten van zowel de digitale als de papieren versies gearchiveerd.

Onveilige praktijk

De docent markeert de digitale toets en de resultaten als 'afgehandeld' in de toetsapplicatie.

De docent neemt het stapeltje papieren toetsen mee naar zijn kantoor. Hij legt het onderin zijn kast bij de andere gemaakte papieren toetsen. Hij moet de toetsen 2 jaar bewaren. Omdat hij een chronisch tekort aan kastruimte heeft, gooit hij een 'oudere' stapel met toetsen weg in zijn prullenbak. De sleutel van de kast is hij kwijt.

Veilige praktijk

De docent markeert de digitale toets en de resultaten als 'afgehandeld' in de beveiligde omgeving. Om in te loggen heeft hij een extra toegangscode nodig die hij via SMS ontvangt.

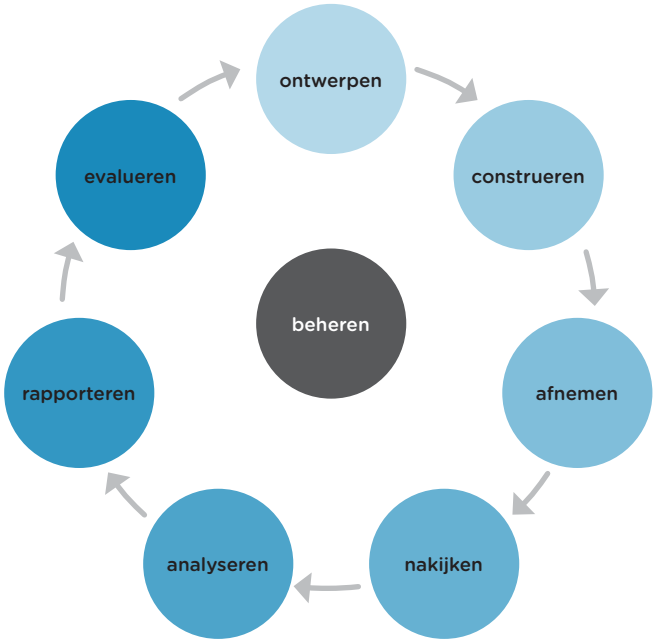
De docent brengt het stapeltje met papieren toetsen naar de kluis die speciaal hiervoor aanwezig is op de instelling. Hij tekent de toegangslijst voordat hij naar binnen gaat, zodat er altijd getraceerd kan worden wie er binnen is geweest. Een beperkt aantal medewerkers binnen de instelling heeft toegang tot deze ruimte.

Na het verstrijken van de overeengekomen bewaartermijn van twee jaar worden de toetsen op een veilige manier afgevoerd door een gespecialiseerd bedrijf.

2 VEILIGHEIDSRISICO'S IN HET TOETSPROCES

In dit hoofdstuk lees je waar de risico's in het toetsproces zitten. Het biedt je handvatten om een risicoanalyse van je eigen instelling uit te voeren en om de daaruit volgende maatregelen goed te kunnen uitvoeren. Ook vind je in dit hoofdstuk een overzicht van succesfactoren die kunnen bijdragen aan het realiseren van een veilig toetsproces.

De toetscyclus (zie figuur 1) is het uitgangspunt van de risicoanalyse. Op basis van ervaring van de vijf instellingen hebben we de risicoanalyse uitgevoerd op hoofdlijnen van de zeven stappen van de toetscyclus, zie hiervoor tabel 2.



Figuur 1. Toetscyclus (uit het Begrippenkader digitaal toetsen)

2.1. Risicoanalyse

In tabel 2 geven we per deelproces van de toetscyclus een overzicht van de belangrijkste veiligheidsrisico's, de geschatte kans dat deze optreden en de impact hiervan op de aspecten beschikbaarheid, integriteit en vertrouwelijkheid. Deze analyse is opgesteld in samenspraak met experts uit de instellingen. Ons advies is om deze analyse als uitgangspunt te nemen, te toetsen aan de praktijk in je eigen instelling en waar nodig bij te stellen of aan te vullen.

De invulling van hoog/midden/laag is gebaseerd op ervaringen uit de praktijk en kan per situatie verschillen. De tabel laat zien waar het grootste risico bij toetsing zich bevindt: bij de afname. In de praktijk worden daar dan ook heel veel maatregelen genomen om risico's te verkleinen. Tegelijkertijd laat de tabel zien dat ook bij veel andere processtappen behoorlijk grote risico's liggen. Dit werkboek geeft daarom een overzicht van maatregelen om veiligheidsrisico's op alle processtappen te beperken.

Het is goed om te realiseren dat een risicoanalyse een momentopname is: er kunnen altijd nieuwe risico's ontstaan. Daarom is het zinvol de risicoanalyse periodiek te herhalen.

DEELPROCES	KANS	IMPACT			HIGHLIGHTS PER DEELPROCES
		B	I	V	
Ontwerpen	L	L	L	L	Het deelproces *ontwerpen* bevat geen veiligheid-kritische aspecten. De toetsmatrijs is niet geheim. Hierdoor is de kans dat de veiligheid in gevaar komt klein. Procesbeheersing richt zich vooral op inhoudelijke kwaliteit.
Construeren	M	M	H	H	Docenten *construeren* toetsvragen, doen dat meestal op hun pc (laptop, tablet), bewaren concepten 'ergens' (harde schijf, Dropbox, USB-stick etc.) en sturen deze per e-mail naar collega's voor review. Dit is allemaal weinig veilig, tenzij maatregelen worden genomen. Als toetsmateriaal vroegtijdig uitlekt is de schade groot.
Afnemen	H	H	H	H	Tijdens de *toetsafname* kan er veel misgaan: spieken, ongeoorloofd manipuleren van digitale toetsen, verloren raken of kwijtmaken van resultaten, etc.
Nakijken	M	M	H	H	In het *nakijkproces* is het denkbaar dat er (digitale) manipulatie van resultaten plaatsvindt, toetsen kwijtraken of anderszins gecorrumpeerd raken.
Analyseren	L	M	H	M	Bij de *analyse* ligt het risico vooral in manipulatie van de resultaten en de cesuur (normenset).
Rapporteren	M	M	H	H	*Inzage* is, zeker op papier, een belangrijk fraude-gevoelig moment. Denk aan het wijzigen van antwoorden of het ongeoorloofd kopiëren van toetsvragen. Daarnaast zijn gerapporteerde uitslagen vertrouwelijk.
Evalueren	L	L	M	M	Bij *evaluaties* zijn examenprogramma's, toetsmaterialen en toetsresultaten betrokken. Hoewel integriteit (examenprogramma's) en vertrouwelijkheid (materialen en resultaten) belangrijke aspecten zijn, is dat altijd na afloop van een periode en niet herleidbaar naar individu. Aangezien tussen evaluatie en hergebruik een periode van herziening en eventueel herstel beschikbaar is, geldt in het deelproces evaluatie geen verhoogd risico.
Beheren	M	M	H	H	Als er in de *opslag* van toetsvragen, toetsen en/of toetsresultaten ongeoorloofde manipulaties plaatsvinden of materiaal verloren gaat, dan is dit van invloed op de aantoonbaarheid en/of rechtmatigheid van toetsen.

Tabel 2 Veiligheidsaspecten per deelproces van de toetscyclus.
B=beschikbaarheid; **I**=integriteit; **V**=vertrouwelijkheid; **L**=laag; **M**=midden; **H**=hoog.

In dit werkboek hanteren we de volgende uitgangspunten:

a. Als het risico *laag* is, dan is het niet nodig om aanvullende maatregelen te nemen
b. Daar waar het risico *midden* is, mag je er van uitgaan dat dit in voldoende mate is afgedekt als *het Normenkader informatiebeveiliging Hoger Onderwijs* (zie kader op pagina 12) correct is geïmplementeerd.
c. Als het risico *hoog* is, zijn aanvullende maatregelen noodzakelijk.

Normenkader Informatiebeveiliging Hoger Onderwijs

De instellingen in het hoger onderwijs hebben in de SURF Community voor Informatiebeveiliging en Privacy (SCIPR) met elkaar een normenkader op het gebied van informatiebeveiliging opgesteld: het Normenkader Informatiebeveiliging Hoger Onderwijs. Als de instelling hieraan voldoet, betekent dit dat de informatiebeveiliging aan een binnen het hoger onderwijs geaccepteerd basisniveau voldoet. De volledige implementatie van dit normenkader in de instelling geeft een generieke informatiebeveiliging op niveau midden. Het normenkader is gebaseerd op ISO 27002:2013, een internationaal gangbare normenset.

In het normenkader staan onder andere zaken als virusbescherming, gebruik van wachtwoorden en de toepassing van firewalls en een aantal procesgerichte aspecten. Het totale normenkader is een heel uitgebreid document, waar we in dit werkboek niet nader op ingaan.

Kader Toelichting op het normenkader informatiebeveiliging

2.2. Succesfactoren voor een veilige oplossing

De betrokken instellingen geven duidelijk aan dat het veilig maken van de toetsketen een complex traject is met een stevige ‘menskant’ in combinatie met een technische aanpak. We benoemen een aantal succesfactoren die een belangrijke bijdrage kunnen leveren aan de haalbaarheid van een veilig toetsproces:

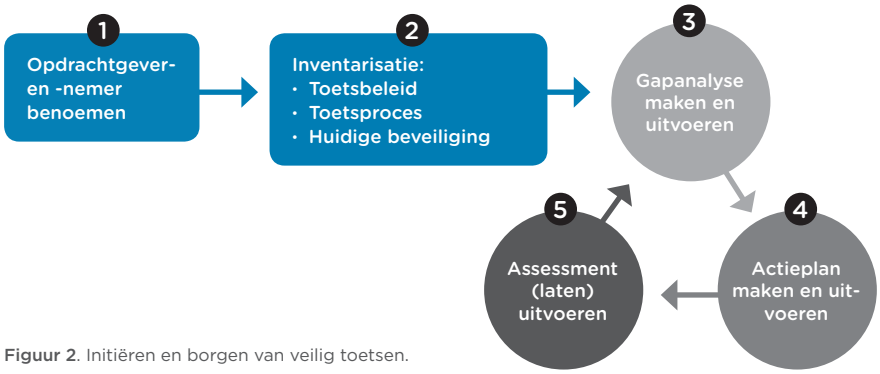
- Uniformiteit in het toetsproces bevordert de voorspelbaarheid ervan en daarmee de beheersbaarheid; beheersbaarheid is een voorwaarde om *in control* te kunnen zijn en snel te kunnen anticiperen op eventuele incidenten.
- *Keep it simple*. Hiermee bereik je dat veilig werken goed uit te leggen is en uitvoerbaar blijft. Hiermee voorkom je dat mensen binnen de instelling naar alternatieven gaan zoeken of shortcuts gaan nemen.
- Sluit zoveel mogelijk aan bij wat je toch al aan beveiliging doet binnen de instelling en besteed veel aandacht aan gebruiksgemak. Als een werkwijze te ingewikkeld is, gaan mensen deze omzeilen.
- Veilige organisatie (mensen) en techniek zijn beide belangrijk.
- Veiligheid is mensenwerk, dat betekent dat bewustwording cruciaal is. Maak veiligheid op regelmatige basis bespreekbaar, zodat je kunt aansluiten op houding en gedrag binnen de organisatie.
- Realiseer je dat het vrijwel onmogelijk is om te voorkomen dat toetsvragen na afloop van de toets bekend worden: studenten zijn heel vindingrijk in het (ongeoorloofd) kopiëren of onthouden van toetsvragen, die in de praktijk snel gaan circuleren bijvoorbeeld op Facebook of op www.studeersnel.nl.

3 NAAR EEN VEILIG TOETSPROCES

In dit hoofdstuk lees je welke stappen je als instelling moet zetten om tot een veilig toetsproces te komen.

3.1. Overzicht stappen

Welke stappen moet een instelling zetten om te komen tot een veilig toetsproces? En hoe wordt toetsveiligheid geborgd in de lijn? Sterk vereenvoudigd is dit weergegeven in figuur 2. In de volgende paragrafen lichten we de afzonderlijke stappen toe.



Figuur 2. Initiëren en borgen van veilig toetsen.

3.2. Stap 1: opdracht en eigenaarschap

Het is belangrijk om onderscheid te maken tussen een initiële activiteit om het toetsproces (beter) te beveiligen enerzijds en het onderhoud hiervan anderzijds. Afhankelijk hiervan kan het beveiligen van het toetsproces in de lijn worden belegd of projectmatig worden aangepakt. Dit laatste is aan te raden als je verwacht dat een grote inhaalslag nodig is.

Een vraag die je altijd moet stellen en beantwoorden is: wie is of wordt de opdrachtgever en vervolgens eigenaar van ‘veilig toetsen’? Uiteraard hangt dit sterk samen met de vraag, wie mandaat heeft (of krijgt) om door de gehele keten heen te kunnen sturen. Deze rol kan bijvoorbeeld worden vervuld door de manager Planning & Control, een directeur Onderwijs. Een benadering om deze rol meer gewicht te geven is door deze formeel als ‘Ketenregisseur toetsen’ te benoemen.

Een ketenregisseur toetsen (ook wel ‘proceseigenaar toetsen’) is binnen de instelling specifiek verantwoordelijk voor het gehele toetsproces en heeft de bevoegdheid om daarin in te grijpen, als hij/zij dat noodzakelijk acht. Daarom moet de ketenregisseur kennis van het toetsproces hebben én voldoende mandaat krijgen. Dit laatste betekent al snel dat de rol van ketenregisseur het best door een directeur of manager wordt ingevuld.

In praktijk is het meestal niet eenvoudig om de eigenaar van veilig toetsen te vinden en benoemd te krijgen. Soms kan het helpen om dan eerst aan de slag te gaan met processtap 2 – dan wordt mogelijk wel duidelijk wie de aangewezen persoon kan zijn.

3.3. Stap 2: inventarisatie

De voorbereiding richt zich op de analyse van de huidige situatie op drie aspecten: het toetsbeleid in relatie tot toetsveiligheid, de uitwerking van het toetsproces en het informatiebeveiligingsbeleid van de instelling.

a. Bespreek met een aantal betrokkenen tabel 2 uit dit werkboek om na te gaan, of de hier voorgestelde risico's overeenkomen met de situatie in je eigen instelling.
b. Ga na wat in het toetsbeleid van de instelling is vastgelegd over toetsveiligheid. In de meeste gevallen gaat het toetsbeleid in elk geval in op een aantal aspecten van fraude. De benadering van toetsveiligheid moet hiermee in lijn zijn (of het toetsbeleid moet worden aangepast).
c. Breng het toetsproces binnen de instelling in kaart; gebruik hierbij desgewenst de gedetailleerde voorbeeldUitwerking die in bijlage 1 van dit werkboek is opgenomen.
d. Ga na welke reguliere informatiebeveiligingsmaatregelen er binnen de instelling zijn; wij adviseren je hierbij samen te werken met de information security of- ficer van je instelling. Als de maatregelen voldoen aan het normenkader informatiebeveiliging HO, dan is in elk geval een solide basis aanwezig die voor toetsen voldoet op het niveau 'midden'. Dat betekent dat waar een beveiligingsni- veau 'hoog' is aanvullende maatregelen nodig zijn. Een hulpmiddel hierbij vind je in bijlage 2.

3.4. Stap 3: gapanalyse

e. Als de huidige situatie in kaart is gebracht, kun je een gapanalyse uitvoeren. Omdat je hier tot in detail naar de beveiliging van het gehele toetsproces kijkt, zal dit een omvangrijke klus zijn. In bijlage 3 is hiervoor een uitvoerig hulpmiddel beschikbaar, dat je als leidraad of checklist kunt gebruiken. Zo nodig kun je eerst de processtappen uit het werkboeken aanpassen op je eigen situatie. Vervolgens beoordeel je per stap of de maatregelen in je eigen situatie voldoende zijn in relatie tot het risico. Daar waar de maatregelen onvoldoende zijn, is sprake van een 'gap'. De verzamelde gaps vormen de basis voor de volgende stap: het opstellen van het actieplan.

3.5. Stap 4: actieplan toetsveiligheid

f. Maak een actieplan: bepaal gezamenlijk prioriteiten en de aanpak van de realisatie van maatregelen. Maak hierbij gebruik van de voorbeeldmaatregelen in bijlage 3.
g. Voer het actieplan uit. Breng prioritering aan als blijkt dat er veel acties zijn. De prioritering richt je op de grootste risico's met de grootste kans en/of op maatregelen die een groot effect hebben omdat ze veel risico's in één keer verkleinen. De acties zullen zowel gericht zijn op veilig handelen door de betrokken actoren (awareness), als op technische maatregelen.

3.6. Stap 5: assessment

h. Doe vervolgens een self-assessment of laat een externe assessment doen op het beter beveiligde toetsproces. Hiervoor biedt bijlage 4 een kapstok. Deze stap is van belang voor de validering van de genomen maatregelen en daarmee de borging van de beoogde veiligheid van het toetsproces.

3.7. Toekomstbestendigheid van toetsveiligheid

Als de toetsveiligheid het gewenste niveau heeft, is het zaak de continuïteit hiervan te borgen. Dat vraagt om:

- een eigenaar van het veilige toetsproces, zoals de eerder genoemde keten-regisseur of proceseigenaar toetsen.
- periodieke monitoring van de status van de toetsveiligheid en zo nodig de implementatie van aanvullende maatregelen – in feite herhaling van de deelstappen c tot en met g zoals hierboven genoemd.
- regelmatige aandacht voor awareness onder alle actoren in de toetsketen.

4 TOT SLOT

Het goed en structureel veilig maken van het gehele toetsproces is geen sinecure. Echter, gelet op het belang van de rechtmatigheid van toetsing in het hoger onderwijs, is het in onze ogen een noodzakelijke exercitie.

Dit werkboek is dankzij de inspanningen van velen tot stand gekomen. Wij zijn hen daarvoor zeer dankbaar. Ook bedanken we iedereen die feedback heeft gegeven op versie 1, waardoor deze versie 2 sterk verbeterd is. Reacties blijven welkom. Dat kan door een e-mail te sturen naar Annette Peet, projectmanager Digitaal toetsen bij SURFnet, annette.peet@surfnet.nl.

BIJLAGEN

BIJLAGE 1
Voorbeelduitwerking van het toetsproces

BIJLAGE 2
Toetsveiligheid op basis van de baseline informatiebeveiliging

BIJLAGE 3
Beveiligingsmaatregelen per deelproces

BIJLAGE 4
Assessment veilig toetsen

BIJLAGE 5
HORA objecten vallend binnen het toetsproces

BIJLAGE 6
Gebruikt bronmateriaal

BIJLAGE 1

VOORBEELD-UITWERKING VAN HET TOETSPROCES

Inleiding

Om tot een veilig toetsproces te komen beschrijft het werkboek in hoofdstuk 3 een aantal stappen. De eerste stap is het in kaart brengen van het toetsproces van de instelling (*zie ook stap 2 in paragraaf 3.3 op pagina 14*). De gedetailleerde voorbeelduitwerking in deze bijlage kan als voorbeeld gebruikt worden. Je kunt deze als leidraad gebruiken om het toetsproces van de instelling uit te werken of deze hieraan toetsen.

Deze voorbeelduitwerking is ontstaan uit de analyse van het toetsproces van de vijf instellingen die hebben meegewerkt aan het schrijven van dit werkboek. Het is daarmee een 'gemene deler' van de vijf instellingen als voorbeeld, en in elke instelling kan het proces afwijkend zijn. Je kunt het model gebruiken als volledigheidscheck.

Het is belangrijk dat de rollen en verantwoordelijkheden binnen de instelling eenduidig belegd zijn en beheerd worden. Onder het toetsproces verstaan we alle stappen van de toetscyclus plus het beheer van toetsen (*zie figuur 1 op pagina 10*). We beschrijven het hoofdproces en vervolgens de deelprocessen aan de hand van de toetscyclus. Ieder deelproces is vervolgens uitgewerkt in activiteiten en rollen, de activiteiten zijn geclassificeerd en deze vormen de input voor de risicomatrix (*bijlage 3*).

Het proces gaat uit van een digitale werkwijze; ook bij het afnemen van papieren toetsen is immers veelvuldig sprake van een digitale voorbereiding waarbij een tekstverwerkingsprogramma, e-mail en digitale opslag aan de orde zijn.

Opbouw van deze bijlage

We geven een gedetailleerde beschrijving per deelproces. Deze detaillering maakt het mogelijk te komen tot concrete interventies om het toetsproces stap voor stap veiliger te maken. Het format van de beschrijving per deelproces is:

1. tabel met hoofdkenmerken van het deelproces;
2. procesflow;
3. activiteitbeschrijving.

Volgend op de beschrijving van de deelprocessen omschrijven we alle rollen en is een RACI[7]-tabel opgenomen.

[7] RACI is een veelgebruikte methodiek om rollen en bevoegdheden in te delen naar Responsible (verantwoordelijk), Accountable (eindverantwoordelijk), Consulted (geraadpleegd) en Informed (geïnformeerd).

Indeling van deze bijlage

Legenda symbolen

ACTIVITEIT 	Een activiteit bestaat uit een aantal handelingen die een enkele 'actor' (persoon, systeem of afdeling) in één ononderbroken tijdsinterval kan uitvoeren.
KEUZE- OF BESLISMOMENT 	Tijdens de uitvoering van een proces zijn altijd momenten dat er keuzes gemaakt moeten worden of dat omstandigheden of situaties leiden tot meerdere mogelijkheden.
DOCUMENT OF BESTAND 	Binnen een proces worden documenten of bestanden gemaakt, verplaatst, uitgewisseld of gemuteerd. Nevenstaand symbool staat zowel voor documenten als digitale bestanden. De benaming is in schema en in procesbeschrijving blauw en vetgedrukt.
COMMUNICATIE 	In tegenstelling tot de 'dichte' pijl (⟶) die de proces-flow weergeeft, is de onderbroken lijn bedoeld om communicatie te tonen. Communicatie in de vorm van overleg, informeren etc., maar ook het versturen van mail, document of bestand.
ANDER PROCES 	Met dit symbool wordt aangegeven dat er een inkomende verbinding (input) of uitgaande verbinding (output) van/naar een ander (deel)proces loopt.
DATAOPSLAG 	Dataopslag, bijvoorbeeld hard disk

VEILIGE TOETSCYCLUS
VOORBEELDPROCES

HOOFDKENMERKEN

Proceseigenaar
Opleidingsmanager

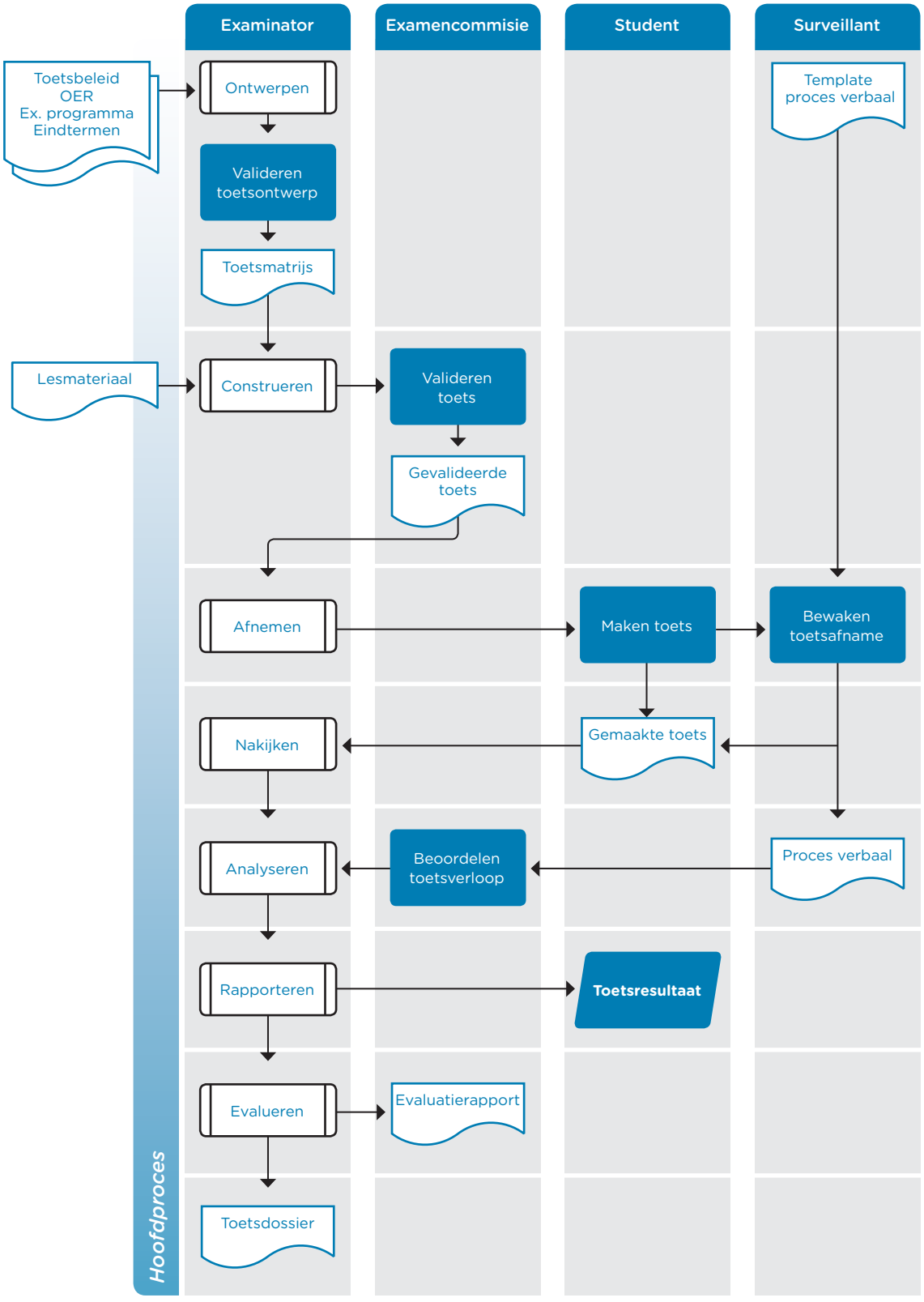
Procesomschrijving
Het totale proces van ontwerpen t/m evalueren inclusief beheren van toetsen.

Procesdoel
Vaststellen of de student de juiste kennis en/of vaardigheden bezit.

Procesvoorwaarden(n)
Het proces is betrouwbaar (beschikbaar, integer, vertrouwelijk) en controleerbaar.

Input
Op examenprogramma gebaseerde toetsbare eenheid.

Output
Terecht toegekende studiepunten en toetsdossier.



DEELPROCES 1 ONTWERPEN

HOOFDKENMERKEN

Proceseigenaar
Examinator

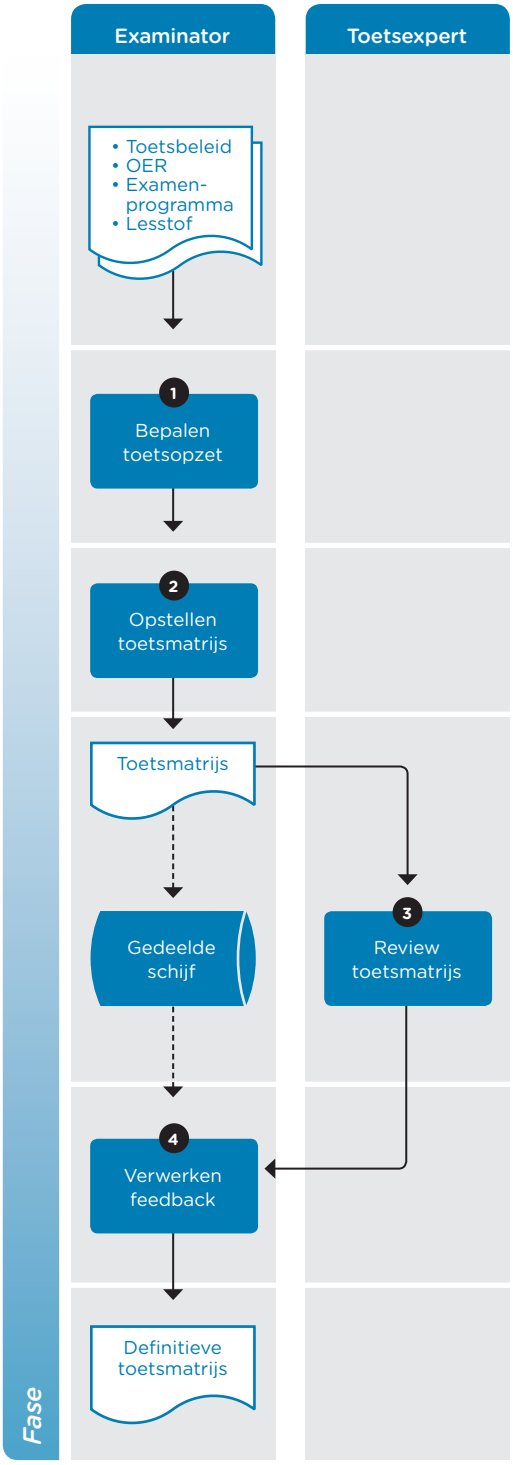
Procesomschrijving
Gedurende het jaar krijgen studenten lesstof te verwerken. Op goede wijze toetsen vereist een doordachte opzet van de toets.

Procesdoel
Het ontwerpen (specificeren) van een toets.

Procesvoorwaarden(n)
Proces is betrouwbaar (beschikbaar, integer, vertrouwelijk) en controleerbaar.

Input
Het geldende toetsbeleid, het OER, het examenprogramma met de eindcriteria, de te toetsen lesstof en de opvattingen van de examinator over datgene wat belangrijk is om in welke vorm getoetst moet worden.

Output
Definitieve toetsmatrijs



ACTIVITEITEN IN DEELPROCES 1: ONTWERPEN

	Activiteit	Hoe (procedurebeschrijving)	Wanneer	Wie
1	BEPALEN TOETSOPZET	De examinator bepaalt de opzet van de toets. Deze raadpleegt hiervoor verschillende bronnen.	Hele jaar	Examinator
2	OPSTELLEN TOETSMATRIJS	De examinator vertaalt de toetsopzet in een toetsspecificatie (toetsmatrijs) en legt deze vast in een document. Hij slaat dit document lokaal op de pc of op een netwerklocatie en mailt het naar een toetsexpert. Ook is opslag in een learning management-, toets- of generiek samenwerkings-systeem mogelijk, waartoe peers en toetsexperts toegang hebben.		Examinator
3	REVIEW TOETSMATRIJS	Op verzoek van de examinator reviewen één of meer experts de door de examinator ontwikkelde toetsspecificatie. Zij voorzien de examinator van onderwijskundige feedback zodat de examinator een optimale toetsmatrijs kan vaststellen.		Toetsexpert
4	VERWERKEN FEEDBACK	De examinator verwerkt de feedback van de reviewers tot een definitieve toetsspecificatie.		Examinator

DEELPROCES 2 CONSTRUEREN

HOOFDKENMERKEN

Proceseigenaar
Examinator

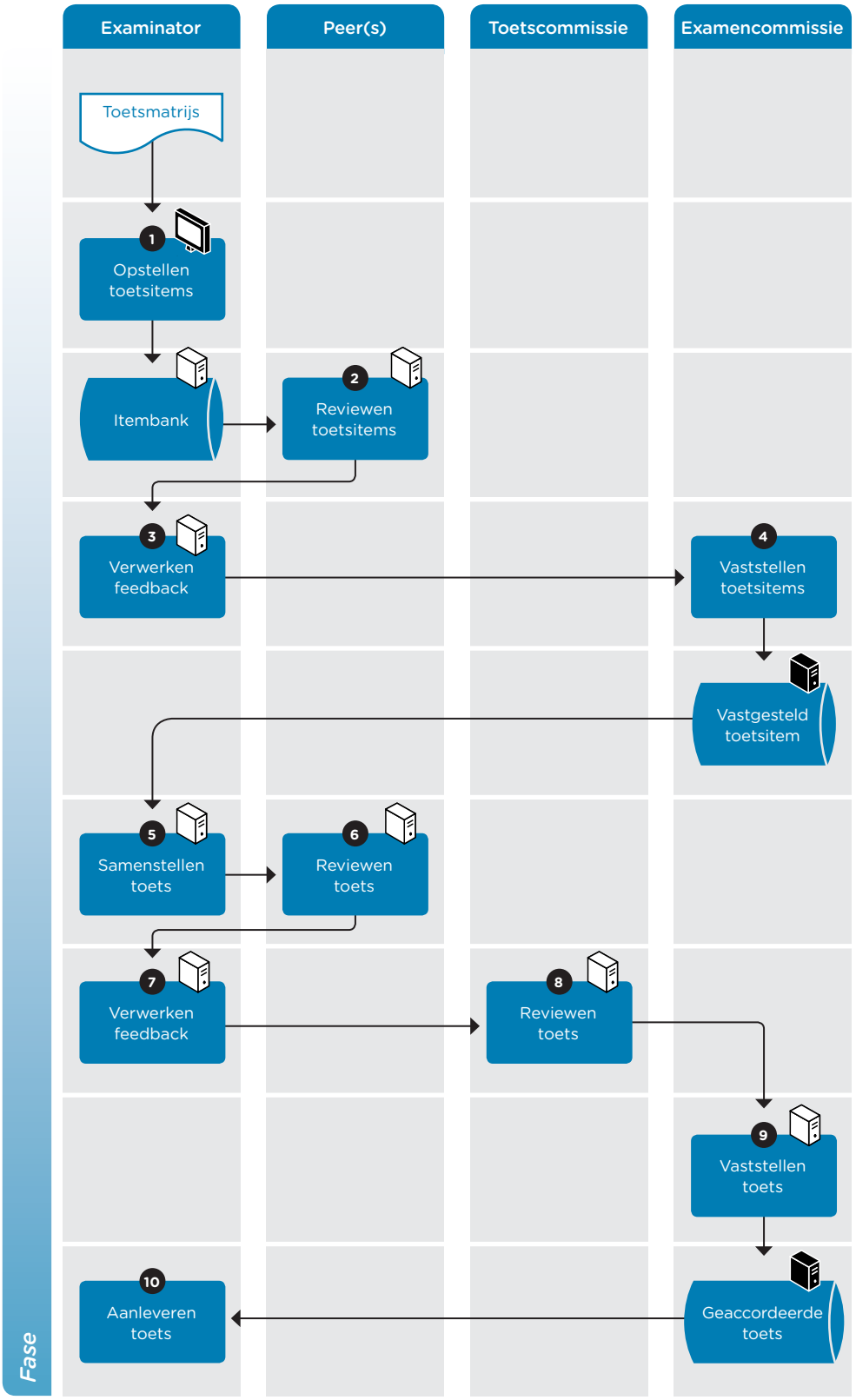
Procesomschrijving
Op goede wijze toetsen vereist een doordachte uitwerking van de toets. In het deelproces Construeren wordt de toets gebouwd.

Procesdoel
Goede toetsen/toetsitems

Procesvoorwaarden(n)
Proces is betrouwbaar (beschikbaar, integer, vertrouwelijk) en controleerbaar.

Input
Toetsmatrijs, te toetsen lesmateriaal

Output
Geaccordeerde toetsitems en toets



Itembank
Itembank
Auteursomgeving

ACTIVITEITEN IN DEELPROCES 2: CONSTRUEREN

	Activiteit	Hoe (procedurebeschrijving)	Wanneer	Wie
1	OPSTELLEN TOETSITEMS	De examinator maakt op basis van de toetsmatrijs de toetsitems. Deze worden lokaal op een pc, tablet of op een netwerk- of cloudlocatie opgeslagen en aangeboden aan een toetsexpert. Ook is opslag in een learning management-, toets- of generiek samenwerkingssysteem mogelijk waartoe peers en toetsexperts toegang hebben. Soms ook betreft het documenten op een USB-stick.	Hele jaar	Examinator
2	REVIEWEN TOETSITEMS	Op verzoek van de examinator reviewen één of meer collega's de door de examinator ontworpen toetsitems. Zij voorzien de examinator van (onderwijskundige) feedback zodat de examinator optimale toetsitems kan opstellen.		Peers
3	VERWERKEN FEEDBACK	De examinator verwerkt de feedback van de reviewers tot definitieve toetsitems.		Examinator
4	VASTSTELLEN TOETSITEMS	De examencommissie stelt de toetsitems vast en geeft ze daarmee vrij voor gebruik in toetsen.		Toetscommissie
5	SAMENSTELLEN TOETS	De examinator stelt op basis van de toetsmatrijs en de toetsitems de toets samen. Deze wordt lokaal op een pc, tablet of op een netwerk- of cloudlocatie opgeslagen en aangeboden aan een toetsexpert. Ook is opslag in een learning management-, toets- of generiek samenwerkingssysteem mogelijk waartoe peers en toetsexperts toegang hebben. Soms ook betreft het documenten op een USB-stick.	Twee weken voor toets	Examinator
6	REVIEWEN TOETS	Op verzoek van de examinator reviewen één of meer collega's de door de examinator ontworpen toets. Zij voorzien de examinator van (onderwijskundige) feedback zodat de examinator optimale toets kan opstellen.		Peers, eventueel ook toetscommissie
7	VERWERKEN FEEDBACK	De examinator verwerkt de feedback van de reviewers tot definitieve toetsen.		Examinator
8	REVIEWEN TOETS	De toetscommissie reviewt de door de examinator ontworpen toetsen voordat deze vastgesteld worden.		Toetscommissie
9	VASTSTELLEN TOETS	De examinator verwerkt de feedback tot de definitieve toets.	Een week voor toets	Examinator
10	AANLEVEREN TOETS	De examinator levert een digitale of papieren toets aan voor afname.	(Vlak) voor tentamen- / toetsweken	Examinator

DEELPROCES 3a
AFNEMEN - DIGITAAL

HOOFDKENMERKEN

Proceseigenaar
Examinator

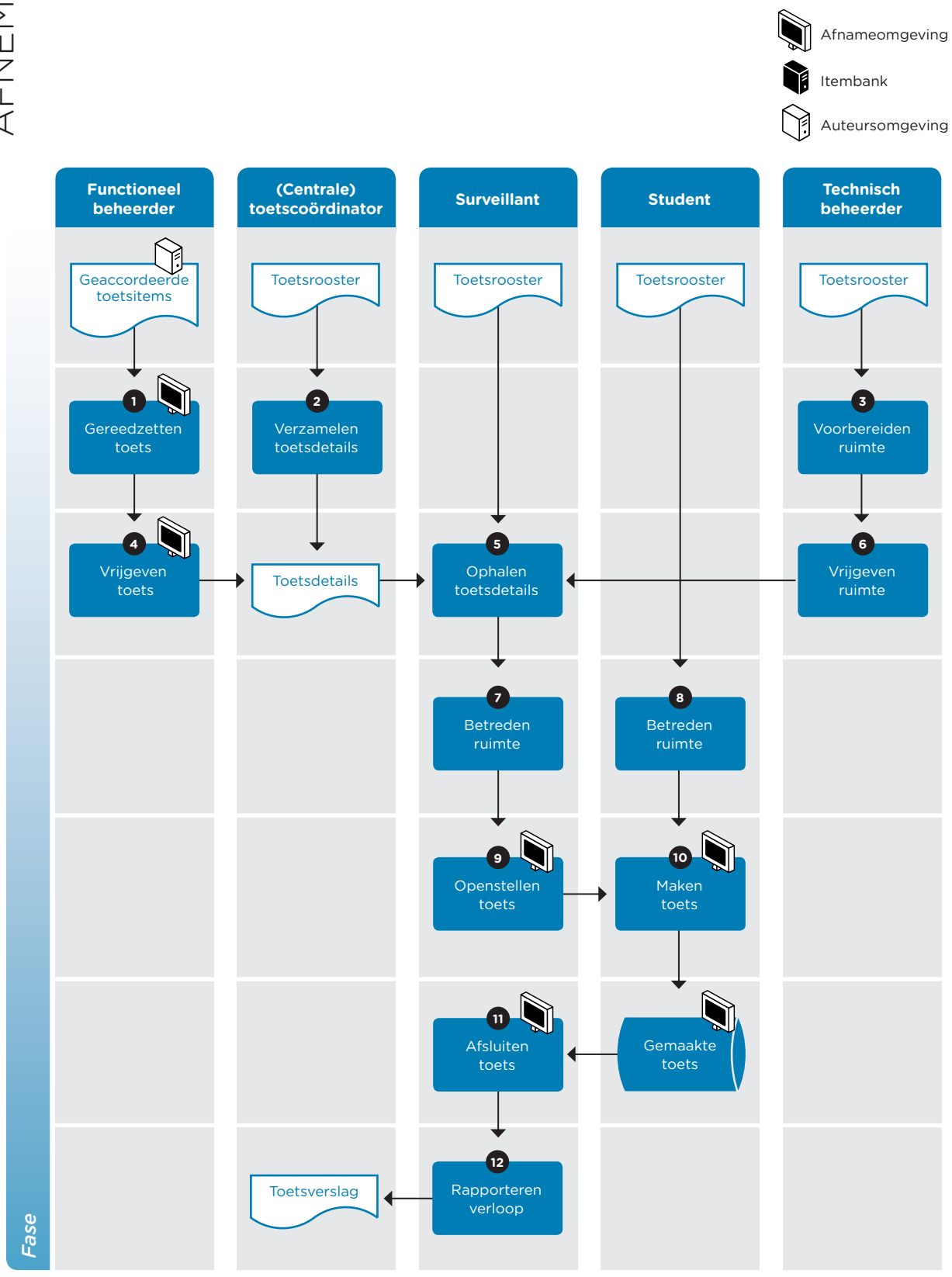
Procesomschrijving
Afnemen van toetsen

Procesdoel
Studenten op betrouwbare en controleerbare wijze toetsen afnemen.

Procesvoorwaarden(n)
Proces is betrouwbaar (beschikbaar, integer, vertrouwelijk) en controleerbaar.

Input
Geaccordeerde toetsitems, toetsrooster

Output
Gemaakte toetsen, toetsverslag (protocol)



ACTIVITEITEN IN DEELPROCES 3a: AFNEMEN - DIGITAAL

	Activiteit	Hoe (procedurebeschrijving)	Wanneer	Wie
1	GEREEDZETTEN TOETS	De functioneel beheerder krijgt de complete toets aangeleverd en zet deze klaar in de afname-omgeving van het toetssysteem.	Tot dag voor toets	Functioneel beheerder
2	VERZAMELEN TOETSDETAILS	De toetscoördinator verzamelt alle informatie met betrekking tot de toets.	Tot uur voor toets	Toetscoördinator
3	VOORBEREIDEN RUIMTE	De ruimte wordt gereedgemaakt voor de toetsafname. Deze voorbereiding kunnen werkzaamheden bevatten als het in de juiste opstelling zetten van tafels, het installeren van afscherming, het klaarmaken van afname-pc's of het verzorgen van voorzieningen voor studenten met een functiebeperking.	Tot uur voor toets	Zaalbeheerder
4	VRIJGEVEN TOETS	Voorafgaand aan het feitelijke toetsmoment wordt de toets in het toetssysteem voor afname vrijgegeven. Als er deelnemers zijn die de toets op papier maken, bijvoorbeeld vanwege functiebeperkingen, drukt de toetscoördinator de toetsitems af op papier en bewaart tot de surveillant de toetsdetails komt afhalen.	Tot uur voor toets	Functioneel beheerder
5	OPHALEN TOETSDETAILS	De surveillant haalt alle benodigdheden voor een goede toetsafname af bij de toetscoördinator. De toetsdetails omvatten ten minste het volgende: • Contactgegevens beheer; • Deelnemerslijst; • Bijzonderheden voor deze toetsafname (begin- en eindtijd, speciale voorzieningen, open/gesloten boek etc.); • Eventuele bijzonderheden in afwijking op het toetsreglement; • Inlogcodes toetsafnamesysteem; • Model toetsverslag en -protocol; • Eventueel geprinte toetsen.	Een uur voor toets	Surveillant
6	VRIJGEVEN RUIMTE	Zodra de ruimte gereed is voor de toetsafname is de sleutel van de ruimte beschikbaar voor de surveillant.	Een uur voor toets	Technisch beheerder
7	BETREDEN RUIMTE	De surveillant opent de ruimte en verifieert dat de ruimte zich bevindt in toestand conform toetsdetails.	Half uur voor toets	Surveillant
8	BETREDEN RUIMTE	In de tijd voorafgaand aan de start van de toets (zoals opgenomen in de toetsdetails) worden de studenten die opgenomen zijn op de deelnemerslijst, toegelaten tot de ruimte.	Kwartier voor toets	Student
9	OPENSTELLEN TOETS	Conform tijd in de toetsdetails stelt de surveillant het starten van de toets beschikbaar voor de deelnemers of deelt papieren toetsen uit.	Vijf minuten voor start toets	Surveillant
10	MAKEN TOETS	De deelnemer maakt de toets. De deelnemers die gereed zijn melden zich af in het afnamesysteem of leveren de gemaakte toets in bij de surveillant. Tijdelijk verlaten van de toetsruimte is toegestaan als dat volgens de toetsdetails toegestaan is, de voorwaarden staan dan eveneens in de toetsdetails.		Student
11	AFSLUITEN TOETS	Als niet vooraf ingesteld sluit de surveillant aan het eind van de toetsperiode de toets in het toetssysteem. Na afsluiting is muteren in de afname-omgeving niet meer mogelijk.	Aan het eind van toetstijd	Surveillant
12	RAPPORTEREN VERLOOP	Na afloop van de toets vult de surveillant het proces verbaal (PV) in. Het PV heeft een vast format waarin het verloop van de toets inclusief alle bijzonderheden systematisch opgenomen kunnen worden. Urgente bijzonderheden tijdens de toets stemt de surveillant telefonisch met de toetscoördinator en/of beheerders af.	Binnen een uur na toets	Surveillant

DEELPROCES 3b
AFNEMEN - PAPIER

HOOFDKENMERKEN

Proceseigenaar
Examinator

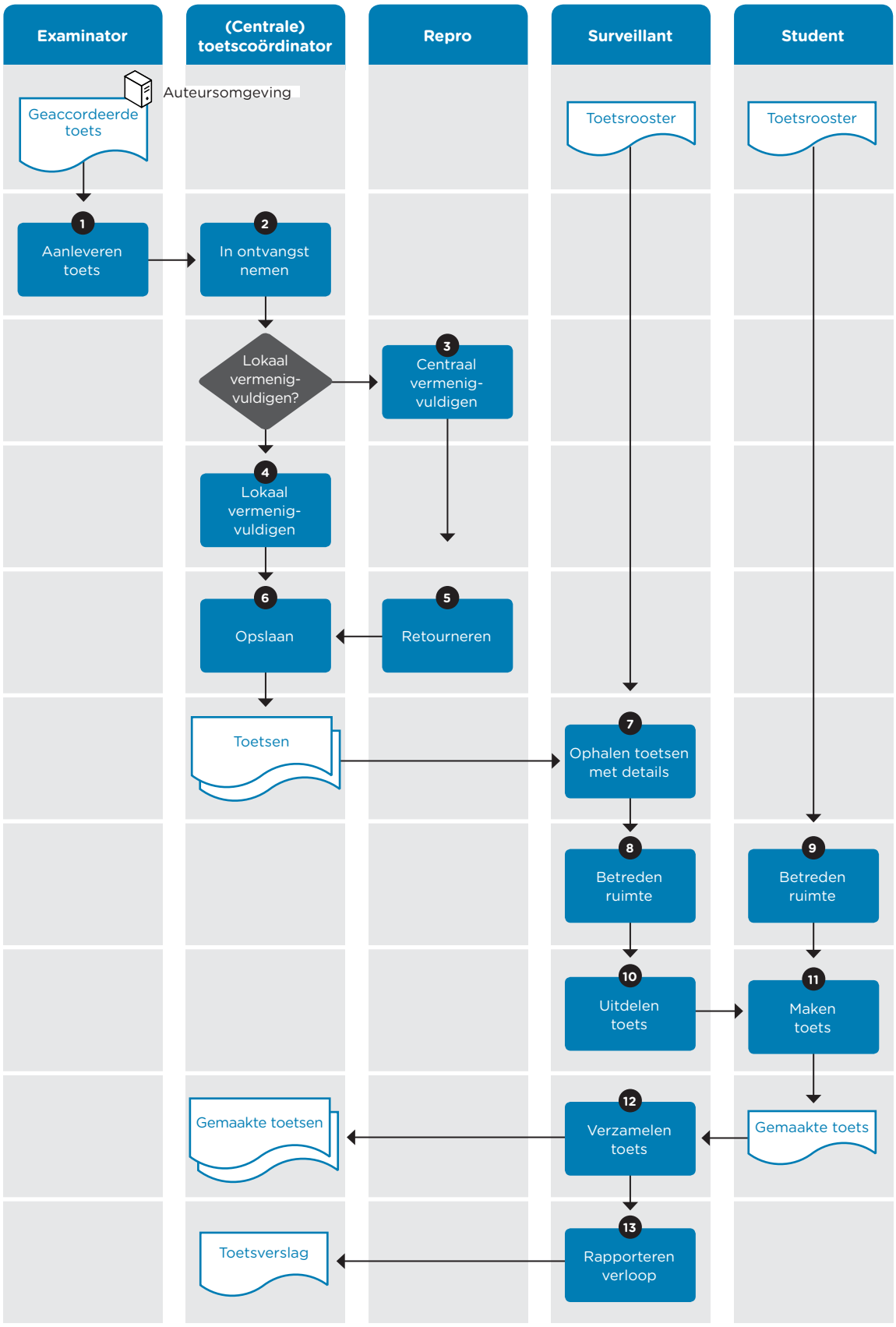
Procesomschrijving
Afnemen van toetsen

Procesdoel
Studenten op betrouwbare en controleerbare wijze toetsen afnemen.

Procesvoorwaarden(n)
Proces is betrouwbaar (beschikbaar, integer, vertrouwelijk) en controleerbaar.

Input
Geaccordeerde toetsitems, toetsrooster

Output
Gemaakte toetsen, toetsverslag (protocol)



ACTIVITEITEN IN DEELPROCES 3b: AFNEMEN - PAPIER

	Activiteit	Hoe (procedurebeschrijving)	Wanneer	Wie
1	AANLEVEREN TOETS	De examinator levert de voorbereide toets aan ter voorbereiding voor de afname. Doorgaans vindt aanlevering digitaal plaats.	Tot week voor toets	Examinator
2	IN ONTVANGST NEMEN	De toetscoördinator neemt het origineel van de toets in ontvangst en bewaart deze tot reproductie start.	Tot week voor toets	Toetscoördinator
3	CENTRAAL VER-MENIGVULDIGEN	Het origineel van de toets wordt aangeboden aan de reproafdeling.	Een dag voor toets	Toetscoördinator
4	LOKAAL VERMENIG-VULDIGEN	De toetscoördinator regelt zelf het benodigde aantal kopieën van de originele toets.	Een dag voor toets	Toetscoördinator
5	RETOURNEREN	Repro brengt de gekopieerde toets bij de toetscoördinator	Een dag voor toets	Repro
6	OPSLAAN	De gekopieerde toets wordt opgeslagen tot deze in de toetsruimte benodigd is.		Toetscoördinator
7	OPHALEN TOETSEN MET DETAILS	De surveillant haalt alle benodigdheden voor een goede toetsafname af bij de toetscoördinator. De toetsdetails omvatten ten minste het volgende: • Contactgegevens beheer; • Deelnemerslijst; • Bijzonderheden voor deze toetsafname (begin- en eindtijd, speciale voorzieningen, open/gesloten boek etc.); • Eventuele bijzonderheden in afwijking op het toetsreglement; • Model toetsverslag en -protocol; • Geprinte toetsen.	Een uur voor toets	Surveillant
8	BETREDEN RUIMTE	De surveillant opent de ruimte en verifieert dat de ruimte zich bevindt in toestand conform toetsdetails.	Half uur voor toets	Surveillant
9	BETREDEN RUIMTE	De in toetsdetails opgenomen tijd voorafgaand aan de start van de toets worden de studenten die opgenomen zijn op de deelnemerslijst (door de surveillant) toegelaten tot de ruimte.	Half uur voor toets	Student
10	UITDELEN TOETS	Conform tijd in de toetsdetails wordt de toets uitgedeeld aan de studenten die aan de toelatingseisen voldoen.	Kwartier voor toets	Surveillant
11	MAKEN TOETS	De deelnemer maakt de toets. De deelnemers die gereed zijn leveren de gemaakte toets in bij de surveillant. Tijdelijk verlaten van de toetsruimte is toegestaan indien dat volgens de toetsdetails toegestaan is, de voorwaarden staan dan even-eens in de toetsdetails.		Student
12	VERZAMELEN TOETSEN	Aan het einde van de toetstijd vraagt de surveillant het maken van de toets te beëindigen en de toetsen in te leveren.		Surveillant
13	RAPPORTEREN VERLOOP	Na afloop van de toets vult de surveillant het proces verbaal (PV) in. Het PV heeft een vast format waarin het verloop van de toets inclusief alle bijzonderheden systematisch opgenomen kunnen worden. Urgente bijzonderheden tijdens de toets stemt de surveillant telefonisch met de toetscoördinator en/of beheerders af.	Binnen een uur na toets	Surveillant

DEELPROCES 4 NAKIJKEN

HOOFDKENMERKEN

Proceseigenaar
Examinator

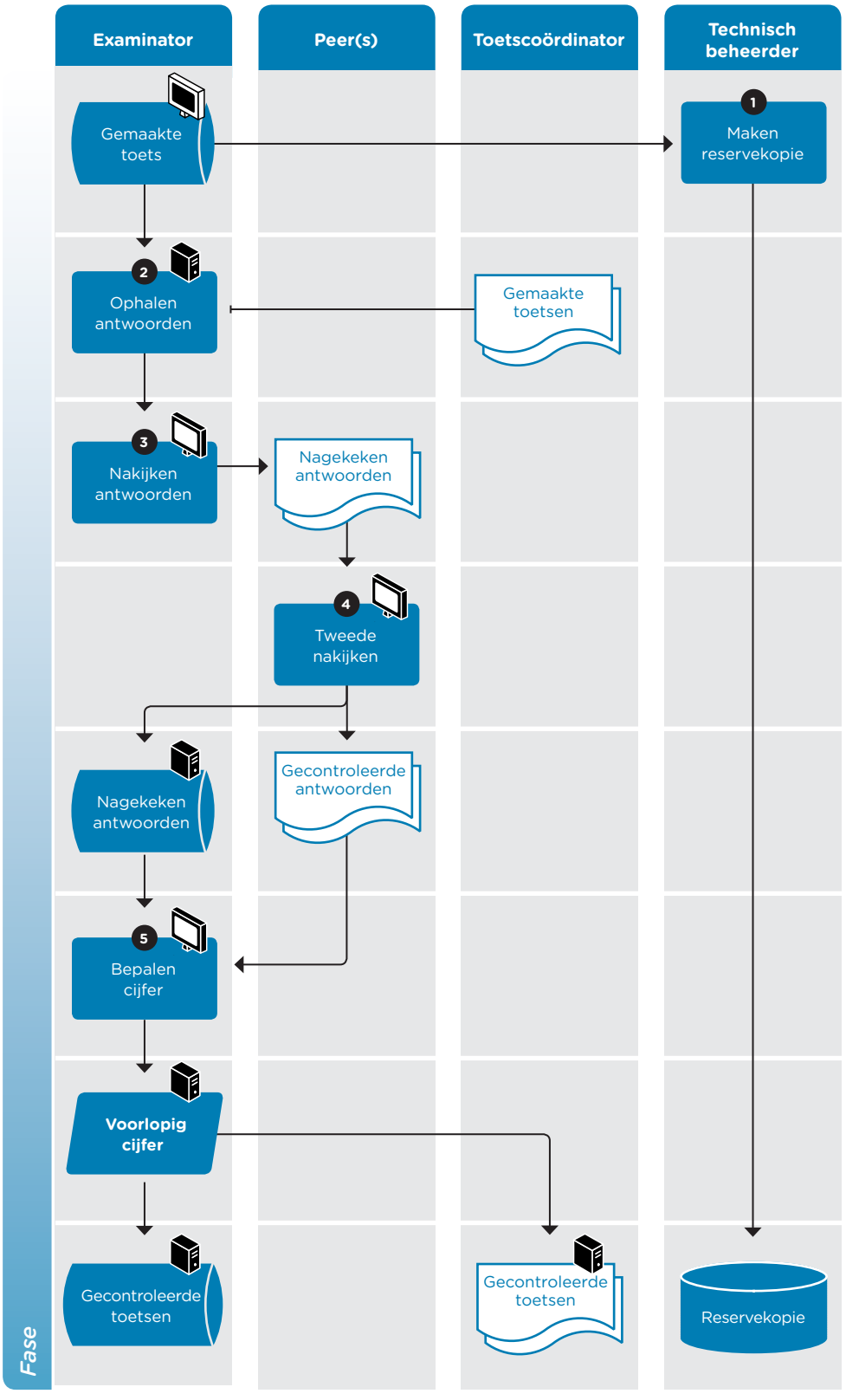
Procesomschrijving
Nakijken van de gemaakte vragen en aan de antwoorden een voorlopige waarde toekennen conform de normering.

Procesdoel
Gemaakte toetsen op correcte wijze van een oordeel voorzien

Procesvoorwaarden(n)
Proces is betrouwbaar (beschikbaar, integer, vertrouwelijk) en controleerbaar.

Input
(Model)Antwoorden op de toetsvragen, normering (bijv. rubric)

Output
Gewaardeerde toetsen (voorlopige uitslagen), gecontroleerde normering



Itembank

Itembank

Afnameomgeving

ACTIVITEITEN IN DEELPROCES 4: NAKIJKEN

	Activiteit	Hoe (procedurebeschrijving)	Wanneer	Wie
1	MAKEN BACK-UP	Direct na afloop van een digitale toetsafname wordt een reservekopie van ingevulde toetsen gemaakt.	Binnen een uur na toets	Functioneel Beheerder
2	OPHALEN ANTWOORDEN	De examinator haalt de gemaakte toetsen op. Voor digitaal afgenomen meerkeuzetoetsen kan dat zijn het ophalen van een CSV-bestand met antwoorden, het toegang verkrijgen tot de item-bank waarin de gemaakte toetsen aanwezig zijn of het ophalen van een set uitwerkingen op papier.		Examinator
3	NAKIJKEN ANTWOORDEN	Vergelijken van de antwoorden met de norm-antwoorden. Dit wordt ofwel volledig door de examinator gedaan, ofwel ondersteund door de toetsprogrammatuur als het een deels of volledig digitale toetsafname betrof.		Toetscoördinator
4	TWEEDE NAKIJKEN	Als het reglement of het toetsdetail dit aangeeft wordt de toets nagekeken door een 2e corrector.		Peer(s)
5	BEPALEN CIJFER	De examinator kent een voorlopig cijfer toe aan het gemaakte werk.	Binnen een week na toets	Examinator

DEELPROCES 5 ANALYSEREN

HOOFDKENMERKEN

Proceseigenaar
Examinator

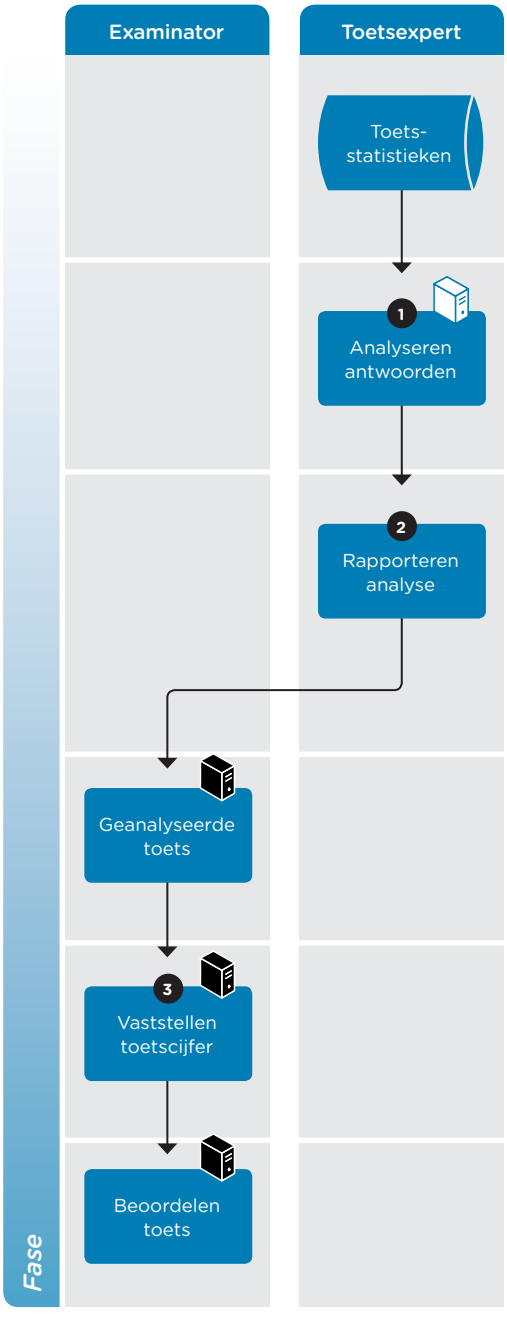
Procesomschrijving
Opsporen van items die van onvoldoende kwaliteit zijn, bijvoorbeeld omdat ze te gemakkelijk, te moeilijk of ambigu blijken te zijn. Deze items worden doorgaans buiten beschouwing gelaten bij het vaststellen van het cijfer.

Procesdoel
Corrigeren van de normering om de betrouwbaarheid van toets en waardering van de antwoorden te vergroten.

Procesvoorwaarden(n)
Proces is betrouwbaar (beschikbaar, integer, vertrouwelijk) en controleerbaar.

Input
Antwoorden op de toetsvragen, normering

Output
Gecontroleerde vragen en normering



Itembank

Analyseomgeving

ACTIVITEITEN IN DEELPROCES 5: ANALYSEREN

	Activiteit	Hoe (procedurebeschrijving)	Wanneer	Wie
1	ANALYSEREN ANTWOORDEN	De toetsexpert onderzoekt de betrouwbaarheid van de toets op basis van statistieken in de item-bank en/of (bv.) Excel-sheets uit het toetspakket.	Na het nakijken	Toetsexpert
2	RAPPORTEREN ANALYSE	De toetsexpert rapporteert de bevindingen aan de examinator. Een advies zou kunnen zijn vragen te verwijderen en/of de cesuur te herzien.	Binnen SMART afspraak	Toetsexpert
3	VASTSTELLEN CIJFER	Op basis van de gecontroleerde toetsen (papier of digitaal) en de definitief vastgestelde cesuur stelt de examinator het cijfer vast.	Binnen periode volgens OER	Examinator

DEELPROCES 6
RAPPORTEREN

HOOFDKENMERKEN

Proceseigenaar
Examinator

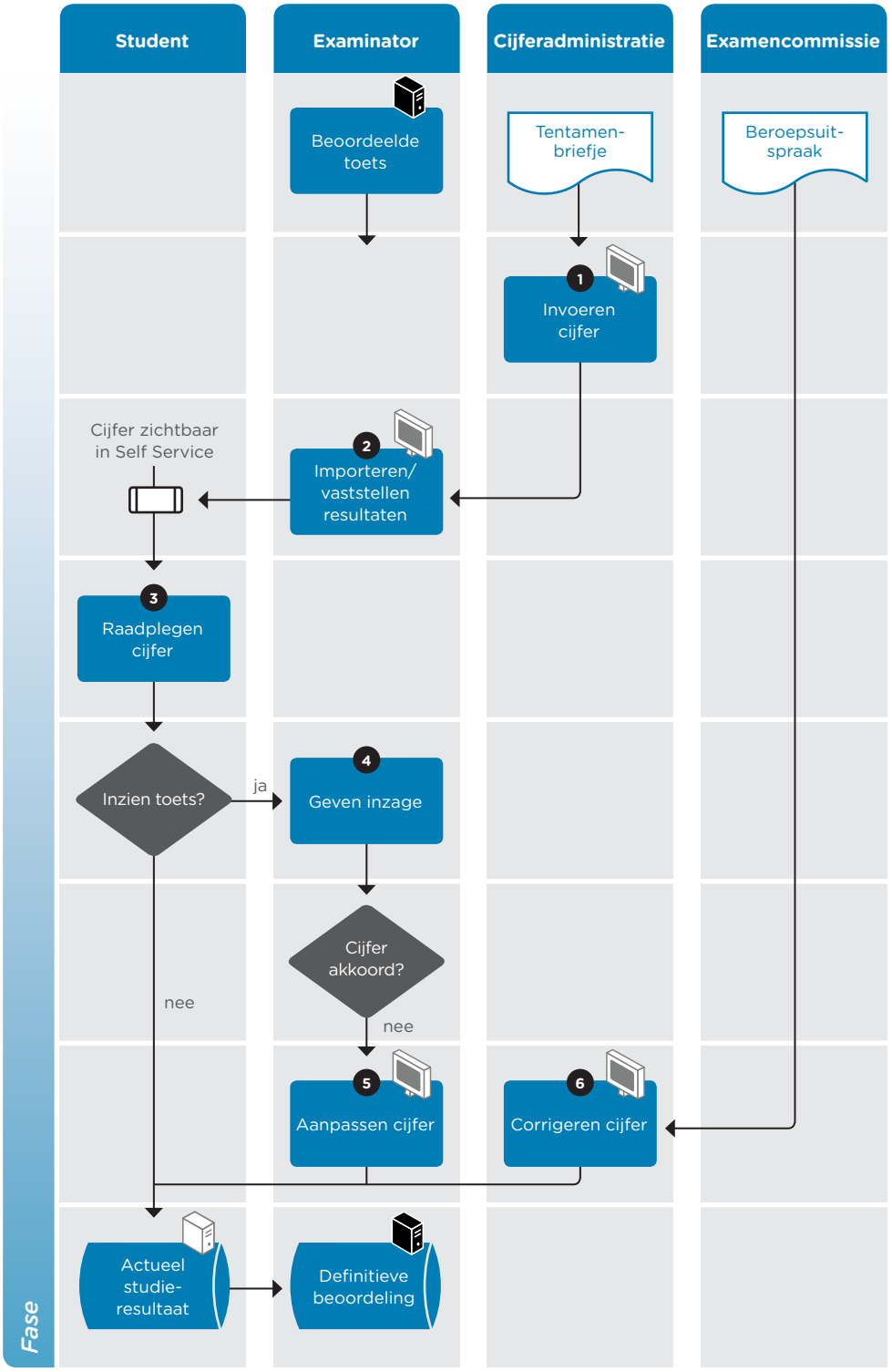
Procesomschrijving
Terugkoppelen van toetsresultaten

Procesdoel
Studenten op betrouwbare en controleerbare wijze hun resultaten meedelen en inzagemogelijkheid bieden.

Procesvoorwaarden(n)
Proces is betrouwbaar (beschikbaar, integer, vertrouwelijk) en controleerbaar.

Input
Beoordeelde toetsen

Output
Gecommuniceerd resultaat



SIS
Itembank
SIS
Ander proces

ACTIVITEITEN IN DEELPROCES 6: RAPPORTEREN

	Activiteit	Hoe (procedurebeschrijving)	Wanneer	Wie
1	INVOEREN CIJFERS	Optioneel wordt gewerkt met tentamenbriefjes (al dan niet digitaal). De examinator levert deze in bij de cijferadministratie. De cijferadministratie legt vervolgens de resultaten in het ELO en/of SIS vast.	Binnen 1 dag na ontvangst	Cijfer-administratie
2	IMPORTEREN/ VASTSTELLEN RESULTATEN	De examinator is verantwoordelijk voor de cijfers. Deze geeft de resultaten daarom vrij aan studenten. Dat kan via drie paden: • cijfers komen via een koppeling met het toetssysteem als concept in het SIS, examinator controleert en geeft vrij; • administratie heeft cijfers ingevoerd, examinator hoeft slechts nog te controleren en vrijgeven; • examinator voert cijfers zelf in en geeft vrij.	Binnen 1 dag na invoer	Examinator
3	RAADPLEGEN CIJFER	Zodra vrijgegeven door de examinator kan de student de cijfers raadplegen in ELO en/of SIS.	Binnen periode volgens OER	Student
4	GEVEN INZAGE	Toetsen zijn beschikbaar voor inzage. Tijdens de inzage kunnen toetsdeelnemers antwoorden en normering van het gemaakte werk bespreken.	Binnen periode volgens OER	Examinator
5	AANPASSEN CIJFER	De examinator heeft de mogelijkheid cijfers te wijzigen gedurende een in het OER vastgestelde periode na toetsafname.	Binnen periode volgens OER	Examinator
6	CORRIGEREN CIJFER	Op last van een beroepsuitspraak kan de cijfer-administratie het geldende resultaat aanpassen.		Cijfer-administratie

DEELPROCES 7 EVALUEREN

HOOFDKENMERKEN

Proceseigenaar
Examinator

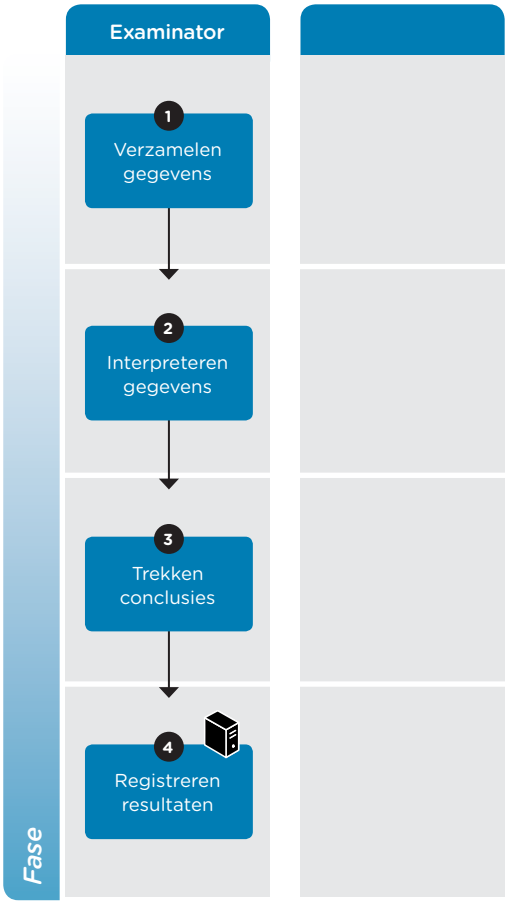
Procesomschrijving
Gebruikte toetsen (antwoorden op gemaakte toetsen) zijn een waardevolle bron om op basis van de praktijk de kwaliteit van een toets te bepalen. In het deelproces Evalueren wordt op basis van de gemaakte/afgelegde toetsen de kwaliteit van de afzonderlijke items en de toets als geheel beoordeeld met als doel te komen tot betere toets, toetsitems en/of toetsmatrijs.

Procesdoel
Construeren van toetsen die optimaal aansluiten bij het doel van de toets.

Procesvoorwaarden(n)
Proces is betrouwbaar (beschikbaar, integer, vertrouwelijk) en controleerbaar.

Input
Toetsmatrijs, gemaakte toetsen, eventueel feedback van studenten.

Output
Verbeterde toetsmatrijs en/of toets(items); verbeterde itembank.



Itembank

ACTIVITEITEN IN DEELPROCES 7: EVALUEREN

	Activiteit	Hoe (procedurebeschrijving)	Wanneer	Wie
1	VERZAMELEN GEGEVENS	Alle informatie die nodig is, of verwacht wordt nodig te zijn, wordt verzameld.	Na afloop van een enkele of een serie toetsen	Examinator
2	INTERPRETEREN INFORMATIE	Gelet op het doel van de toets beoordelen of de validiteit en betrouwbaarheid (en mogelijk ook de rechtvaardigheid en bruikbaarheid) van de toets passend is.		Examinator
3	TREKKEN CONCLUSIES	Het nemen van besluiten over de kwaliteit van de onderzochte toets.		Examinator
4	REGISTREREN RESULTATEN	Vastleggen van de resultaten zodat peers hier kennis van kunnen nemen en/of de itembank aan waarde toeneemt.		Examinator

DEELPROCES 8 BEHEREN

HOOFDKENMERKEN

Proceseigenaar
Beheerder

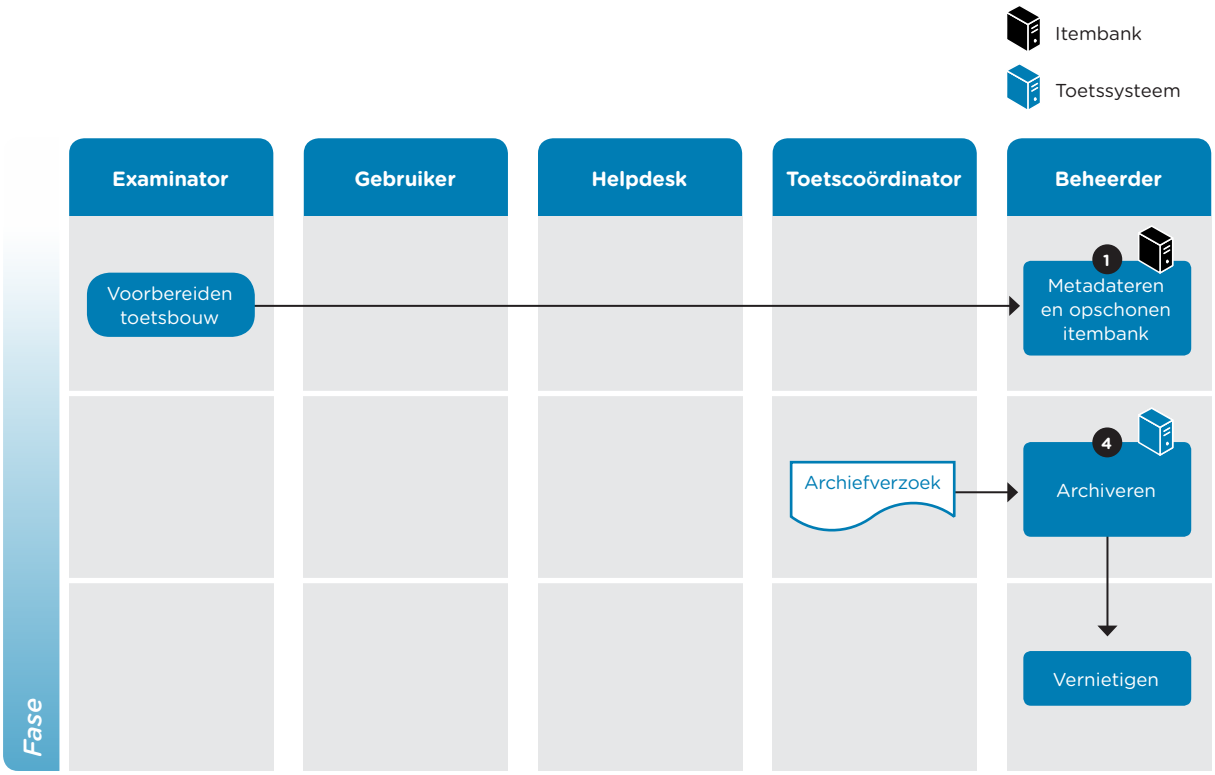
Procesomschrijving
Zowel technisch, functioneel en inhoudelijk In beheer nemen, in stand houden en afstoten van de bedrijfsmiddelen die bij het toetsproces ingezet worden.

Procesdoel
Het in stand houden van de toetsomgeving inclusief database/itembank zodat deze geschikt blijft voor het doel waarvoor deze in gebruik genomen is en het betrouwbaar archiveren van toetsen en toetsresultaten.

Procesvoorwaarden(n)
Proces is betrouwbaar, efficiënt en effectief.

Input
Te beheren objecten, beheerafspraken, wijzigingsverzoeken en storingsmeldingen.

Output
Een toetsomgeving die op de overeengekomen momenten gebruiksklaar is.



ACTIVITEITEN IN DEELPROCES 8: BEHEREN

	Activiteit	Hoe (procedurebeschrijving)	Wanneer	Wie
1	METADATEREN EN OPSCHONEN ITEMBANK	Periodiek (zoals per blok of per jaar) of op afroep schoont de (gegevens)beheerder de data in de itembank op. Hiermee bereik je dat geleerd wordt van gebruikte items, metadata aan nieuwe items worden toegevoegd en verouderde items uit de itembank verwijderd worden.	Gedurende het jaar	Beheerder
2	ARCHIVEREN	De toetsresultaten worden bewaard conform de afspraken. Dat houdt ook in dat (meestal na één of twee jaar) de resultaten moeten worden geanonimiseerd, zodat deze niet meer tot individuele studenten te herleiden zijn.		Beheerder

RACI VOOR HET GEHELE TOETSPROCES

Deze tabel omschrijft de rollen en verantwoordelijkheden van alle betrokkenen bij het toetsproces.

Een verklaring van de gebruikte codes:

- **R**esponsible: De persoon of afdeling waar de activiteit wordt uitgevoerd.
- **A**ccountable: De persoon aan wie R moet rapporteren of die zorgt dat de juiste beslissing wordt genomen. *Een persoon kan overigens ook zowel R als A zijn als de specifieke taak binnen de functierol valt en die persoon niet direct verantwoording hoeft af te leggen.*
- **C**onsulted: De persoon die tijdens de uitvoering van de taak geconsulteerd wordt.
- **I**nformed: De persoon of het systeem die/dat 'geïnformeerd' wordt nadat de taak is uitgevoerd.

Rol	Hoofdtaak/-verantwoordelijkheid
APPLICATIEBEHEERDER	Verantwoordelijk voor het (meer technisch georiënteerde) applicatiebeheer van het toetssysteem.
CIJFERADMINISTRATIE	Invoeren of corrigeren van cijfers (in het SIS).
EXAMENCOMMISSIE	Verantwoordelijk voor de borging van het toetsproces.
EXAMINATOR (DOCENT/PEER):	Verantwoordelijk voor het toetsen van de kennis en vaardigheden van deelnemers. In dit proces concreet: het maken van goede toetsen en het beoordelen van de antwoorden. *NB: In een aantal instellingen is de examinator verantwoordelijk voor het goede verloop van de toets.*
FACILITAIR MEDEWERKER	Verantwoordelijk voor (toegang tot) de toetszalen, sleutelbeheer, de inrichting van het lokaal (niet de toets-pc's) en eventueel videobewaking. *NB: Er zijn instellingen waar de facilitair medewerker wordt ondersteund door een werkplekbeheerder of een zaal- of locatiebeheerder. De facilitair medewerker legt verantwoording af aan de toetscoördinator.*
FUNCTIONEEL BEHEERDER	Verantwoordelijk voor het functionele beheer van het toetssysteem en rapporteert aan de toetscoördinator. Is tussenpersoon tussen gebruikersorganisatie en applicatiebeheer/leverancier.
OPLEIDINGSMANAGER	Heeft de eindverantwoordelijkheid over het toetsproces binnen zijn/haar opleiding.
REPRO	Verantwoordelijk voor het kopiëren van toetsen in de gevraagde hoeveelheid.
STUDENT	Neemt als onderdeel van het leerproces deel aan toetsen waarmee de kwaliteit van competenties gemeten wordt.
SURVEILLANT	Bewaakt dat de toetsafname reglementair verloopt.
TECHNISCH BEHEERDER	Verantwoordelijk voor het technische beheer van servers en/of werkplekken.
TOETSCOMMISSIE	Ziet toe op de onderwijskundige kwaliteit van de toetsen.
TOETSCOÖRDINATOR	Eindverantwoordelijk voor het toetsafnameproces, vanaf het klaarzetten van de toets (na overleg met de docent), de techniek, het lokaal, tot en met het optreden van de surveillanten. De toetscoördinator kan aantonen dat de toetsen rechtmatig zijn afgenomen. *NB: De toetscoördinator kan zijn werkzaamheden delegeren aan een operationeel team.*
TOETSEXPERT	Adviseert over omtrent de kwaliteit van toetsen, van constructie t/m evaluatie.

Nr.	Activiteit	Toetscoördinator	Examinator	Technisch beheerder	Functioneel beheerder	Facilitair medewerker	Surveillant	Toetscommissie	Examencommissie	Student	Cijferadministratie	OLD
1	**Ontwerpen**											
1	Bepalen toetsopzet		R					A				
2	Opstellen toetsmatrijs		R					A				
3	Review		R					C	A			
4	Verwerken feedback		R					A				
2	**Construeren**											
1	Opstellen toetsitems		R					A				
2	Reviewen toetsitems		R					C	A			
3	Verwerken feedback		RA					A				
4	Vaststellen toetsitems		C						RA			A
5	Samenstellen toets		RA									
6	Reviewen toets		RA									
7	Verwerken feedback		R					A				
8	Reviewen toets		A					R				
9	Vaststellen toets		I						R			A
10	Aanleveren toets		R						A			A
3A	**Afnemen - digitaal**											
1	Gereedzetten toets	A			R							
2	Verzamelen toetsdetails	RA										
3	Voorbereiden ruimte	A		R		R						
4	Vrijgeven toets	A			R							
5	Ophalen toetsdetails	A					R					
6	Vrijgeven ruimte	A		R		R						

Nr.	Activiteit	Toetscoördinator	Examinator	Technisch beheerder	Functioneel beheerder	Facilitair medewerker	Surveillant	Toetscommissie	Examencommissie	Student	Cijferadministratie	OLD
7	Betreden ruimte	A					R					
8	Betreden ruimte	A								R		
9	Openstellen toets	A					R					
10	Maken toets									RA		
11	Afsluiten toets	A					R					
12	Rapporteren verloop	A					R					
3B	**Afnemen - papier**											
1	Aanleveren toets	A	R									
2	In ontvangst nemen	RA										
3	Centraal vermenig-vuldigen					R						
4	Lokaal vermenig-vuldigen	A				R						
5	Retourneren	A				R						
6	Opslaan	A				R						
7	Ophalen toets met details	A					R					
8	Betreden ruimte	A					R					
9	Betreden ruimte									RA		
10	Uitdelen toets	A					R					
11	Maken toets									RA		
12	Verzamelen toets	A					R					
13	Rapporteren verloop	A					R					
4	**Nakijken**											
1	Maken reservekopie	A		R								
2	Ophalen antwoorden	RA										
3	Nakijken antwoorden		R					A				
4	Tweede nakijken		R					A				

Nr.	Activiteit	Toetscoördinator	Examinator	Technisch beheerder	Functioneel beheerder	Facilitair medewerker	Surveillant	Toetscommissie	Examencommissie	Student	Cijferadministratie	OLD
5	Bepalen voorlopig cijfer		R						A			
5	**Analyseren**											
1	Analyseren antwoorden		R						A			
2	Rapporteren analyse		R						A			
3	Vaststellen toetscijfer		R						A			
6	**Rapporteren**											
1	Invoeren cijfer		R								R	A
2	Importeren / vaststellen resultaten		R						A			A
3	Raadplegen cijfer									RA		
4	Geven inzage		RA							C		
5	Aanpassen cijfer		RA							I		
6	Corrigeren cijfer								A	I	R	
7	**Evalueren**											
1	Verzamelen gegevens		R									
2	Interpreteren gegevens		R									
2	Trekken conclusies		R									
3	Registreren resultaten		R									
8	**Beheren**											
1	Metadateren en opschonen itembank		R									
2	Archiveren			R	R							

BIJLAGE 2

TOETSVEILIGHEID OP BASIS VAN HET NORMENKADER INFORMATIEBEVEILIGING

Hogeronderwijsinstellingen hebben in de SURF Community voor Informatiebeveiliging en PRivacy (SCIPR) met elkaar een normenkader op het gebied van informatiebeveiliging opgesteld: het Normenkader Informatiebeveiliging Hoger Onderwijs. De volledig implementatie van dit normenkader in de instelling geeft een generieke informatiebeveiliging op niveau midden. Het normenkader is gebaseerd op ISO 27002:2013, een internationaal gangbare normenset.

In onderstaande tabel is een zeer beperkt aantal normen opgenomen met voorbeeldmaatregelen die specifiek van toepassing zijn op het toetsproces. Het volledige basisniveau bevat veel meer normen die generiek zijn en ook bijdragen aan beveiliging van het toetsproces op het niveau midden. De security officer van de instelling kan je hierover meer vertellen. We benadrukken dat het toetsproces alleen optimaal beveiligd kan worden als de baseline op orde is, dat wil zeggen dat alle maatregelen die vereist zijn om het niveau midden te bereiken daadwerkelijk geïmplementeerd zijn.

De genoemde maatregelen in de tabel zijn zogenaamde ‘voorbeeldmaatregelen’. Dat wil zeggen dat zo’n maatregel een mogelijke aanpak is om het gewenste veiligheidsniveau te bereiken. Er kunnen ook wellicht andere maatregelen worden toegepast om hetzelfde te bereiken – wij raden aan om de voorbeeldmaatregelen steeds kritisch te beoordelen op hun bruikbaarheid in de specifieke context van de eigen instelling.

ISO NORM	TEKST VAN DE BEVEILIGINGSEIS (ISO 27002:2013)	VOORBEELDMAATREGELEN TOETSPROCES
6.2.1.1	**Beleid voor mobiele apparatuur:** Beleid en ondersteunende beveiligingsmaatregelen zijn vastgesteld om de risico’s te beheren die het gebruik van mobiele apparatuur met zich meebrengt.	• De locaties waarop aan het toetsproces gewerkt mag worden, zijn bepaald (bijvoorbeeld alleen in speciale ruimtes binnen de instelling, alleen binnen de gebouwen van de instelling of ‘overal’). • Er is een afspraak met welke middelen (laptop, tablet en/of smartphone, eigen of alleen instellingsapparatuur, etc.) aan het toetsproces mag worden gewerkt. • Veilige toegang tot toetsgegevens wordt technisch (onafhankelijk van de locatie) afgedwongen door toepassing van netwerk- en applicatiebeveiliging.
7.2.2	**Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging:** Alle medewerkers van de organisatie en, voor zover relevant, contractanten, krijgen een passende bewustzijnsopleiding en -training en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie.	• Awareness-acties (nieuwsbrieven/flyers) worden vanuit een jaarprogramma uitgevoerd. • Toetsveiligheid wordt periodiek besproken.

ISO NORM	TEKST VAN DE BEVEILIGINGSEIS (ISO 27002:2013)	VOORBEELDMAATREGELEN TOETSPROCES
9.1.1	**Beleid voor toegangsbeveiliging:** Een beleid voor toegangsbeveiliging is vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen.	Applicaties en (mobiele) gebruikers krijgen niet meer rechten dan noodzakelijk om de toetsgerelateerde taken uit te voeren.
9.2.1	**Registratie en afmelden van gebruikers:** Een formele registratie- en afmeldingsprocedure is geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.	Toewijzing van toegangsrechten tot toetssoftware en -gegevens vindt plaats via een formele procedure, waar mogelijk geautomatiseerd via provisioning.
9.2.6	**Toegangsrechten intrekken of aanpassen:** De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatieverwerkende faciliteiten worden bij beëindiging van hun dienstverband, contract of overeenkomst verwijderd, en bij wijzigingen aangepast.	In de toetsketen heeft iedereen alleen de noodzakelijke rechten (“least privilege”).
10.1.1.1	**Beleid bij het gebruik van cryptografische beheersmaatregelen:** Ter bescherming van informatie is een beleid voor het gebruik van cryptografische beheersmaatregelen ontwikkeld en geïmplementeerd.	Tools om het beleid rond het veilige toetsproces af te dwingen, zoals veilige apps en policies, zijn instellingsbreed aanwezig.
13.2.1	**Beleid en procedures voor informatietransport:** Ter bescherming van het informatietransport, dat via alle soorten communicatiefaciliteiten verloopt, zijn formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht.	• Toepassing van herkenbare en verzegelde enveloppen bij transport van toetsen en toetsresultaten. • Vervoer tentamenenveloppen alleen door vertrouwde personen. • Tracking & tracing bij overdracht en vervoer van tentamenenveloppen.

BIJLAGE 3

BEVEILIGINGSMAAT-REGELEN PER DEELPROCES

In de volgende tabellen zijn maatregelen benoemd die bijdragen aan een veilig toetsproces. Deze maatregelen kun je treffen bovenop de maatregelen van het normenkader informatiebeveiliging. Het zijn aanbevolen maatregelen om een hoger beveiligingsniveau dan 'midden' te bereiken; daarom zijn vooral die aspecten uitgewerkt, waar het risico hoog is. Ook hier geldt dat de genoemde maatregelen steeds kritisch moeten worden bekeken in de context van de eigen instelling, en dat er wellicht ook andere maatregelen mogelijk zijn om hetzelfde doel te bereiken. Ook is het mogelijk dat in je eigen context sommige risico's anders uitpakken.

In de tabellen wordt veelvuldig gesproken over het 'werkstation' van bijvoorbeeld de examinator. Hiermee wordt bedoeld de pc, laptop, tablet of andere device die wordt gebruikt om bijvoorbeeld toetsvragen te construeren. Dit kan een apparaat zijn dat door de instelling is verstrekt en wordt beheerd, maar ook een apparaat in eigendom van de betrokken medewerker – en niet zelden zal het voorkomen dat een medewerker zowel instellings- als eigen apparatuur door elkaar gebruikt.

1.1. Ontwerpen

Net als vele andere bedrijfsprocessen is het ontwerpen van toetsen is in de loop van de jaren gedigitaliseerd. Het ontwerpen van toetsen is met de komst van digitale toetsafname niet essentieel gewijzigd. Het ontwerp speelt zich grotendeels af onder directe invloed van de examinator, binnen de eigen organisatie-eenheid.

Activiteit	Risico's integriteit en vertrouwelijkheid						Beheersmaatregelen			
		Kans	Impact				systeeminrichting	autorisaties (functiescheiding)	rapportages	gebruikerscontroles
			B	I	V					
1. Bepalen toetsopzet		–	–	–	–					
2. Opstellen toetsmatrijs	Ongeoorloofde toegang tot werkstation van de examinator	M	L	L	L					
	Onderschepping van de toetsmatrijs bij transport tussen werkstations van betrokkenen	L	L	L	L					
	Ongeoorloofde toegang tot gedeelde omgeving	M	L	L	L					
3. Review toetsmatrijs	Ongeoorloofde toegang tot werkstation van de toetsexpert	M	L	M	L					
4. Verwerken feedback op toetsmatrijs	Feedback niet ontvangen	M	L	H	L		Automatische ophoging versie	Alleen aangewezen personen hebben wijzigrechten		Melding door examinator aan peer dat feedback is verwerkt
	Feedback niet verwerkt	L	L	H	L				Toegangsverslag Mutatieverslag	Periodieke toegangs- en versiecontrole door toetscoördinator

1.2. Construeren

Tijdens de toetsconstructie worden de toetsvragen (toetsitems) ontwikkeld. Omdat toetsvragen voor summatieve toetsing doorgaans niet vooraf bekend mogen zijn bij de studenten geldt hier een hoog risico. De tabel laat dit in detail zien. In dit deel van het toetsproces komt een aantal risico's meerdere malen voor. Echter, omdat er per geval soms gedeeltelijk andere beheersmaatregelen bij horen, zijn ze niet per definitie in één keer op te lossen voor verschillende activiteiten.

Activiteit	Risico's integriteit en vertrouwelijkheid						Beheersmaatregelen			
		Kans	Impact				systeeminrichting	autorisaties (functiescheiding)	rapportages	gebruikerscontroles
			B	I	V					
1. Opstellen toetsitems	Ongeoorloofde toegang tot werkstation van de examinator	M	M	L	H		Lokale opslag alleen versleuteld of opslag in de (private) cloud	Toegang tot pc alleen met persoonsgebonden account	Na upload audit trail met gebruiker en datum/tijd	Periodieke controle loggings
	Ongeoorloofde toegang tot auteursomgeving (software, gegevens)	M	M	L	H		Met 2-factor authenticatie en versleutelde verbinding	• Need-to-know toegang inregelen • Persoonlijke inlog	Audit trail met gebruiker en datum/tijd	Periodieke controle loggings
2. Reviewen toetsitems	Onderschepping toetsitems bij transport van werkstation examinator naar gedeelde omgeving	L	M	M	H		Versleutelde verzending van gegevens	• Alleen aangewezen personen krijgen lees- en schrijfrechten • Eerdere versies kunnen niet worden overschreven.	Track changes, vorige versie(s) bewaren	Notificatie van veranderingen aan betrokkenen
3. Verwerken feedback	Ongeoorloofde toegang tot werkstation van de examinator	M	M	M	H		Lokale opslag alleen versleuteld of opslag in de (private) cloud	Alleen toetseigenaar (examinator) heeft rechten om track changes te accepteren.	• Track changes zijn zichtbaar • Reactie op review wordt vastgelegd	Notificatie wanneer track changes zijn verwerkt

Activiteit	Risico's integriteit en vertrouwelijkheid						Beheersmaatregelen			
		Kans	Impact				systeeminrichting	autorisaties (functiescheiding)	rapportages	gebruikerscontroles
			B	I	V					
4. Review toetsitems	Ongeoorloofde toegang tot werkstation van de toetsexpert	M	M	M	H		• Lokale opslag alleen versleuteld of opslag in de (private) cloud • Opmerkingen kunnen alleen in de vorm van comments of track changes	• Alleen aangewezen personen krijgen lees- en schrijfrechten • Eerdere versies kunnen niet worden overschreven	Commentaar/ wijzigings-voorstellen zijn zichtbaar	
	Onderschepping van toets of toetsitems bij transport tussen werkstations van betrokkenen	H	M	M	H		Met 2-factor authenticatie en versleutelde verbinding naar digitale toetsomgeving	Alleen aangewezen personen krijgen lees- en schrijfrechten	Logging van activiteiten in digitale toetsomgeving	Overzicht van inlogmomenten, pogingen en gekoppelde IP-adressen en gebruikers
5. Vaststellen toetsitems	Ongeoorloofde toegang tot werkstation van de examinator	M	M	H	H		Lokale opslag alleen versleuteld of opslag in de (private) cloud	Toegang tot pc alleen met per-soonsgebonden account	Logging van activiteiten in digitale toetsomgeving	Wijzigingen en loggings worden gecontroleerd
6. Samenstellen toets	Ongeoorloofde toegang tot werkstation van de examinator	L	M	M	H		• Lokale opslag alleen versleuteld of opslag in de (private) cloud • Opmerkingen kunnen alleen in de vorm van comments (geen track changes)	• Alleen aangewezen personen krijgen lees- en schrijfrechten • Eerdere versies kunnen niet worden overschreven	Commentaar/ wijzigings-voorstellen zijn zichtbaar	Status toetsitems wordt weergegeven
	Ongeoorloofde toegang tot auteursomgeving	M	M	M	H		Met 2-factor authenticatie en versleutelde verbinding naar digitale toetsomgeving	Toegang tot pc alleen met persoonsgebonden account	Commentaar/ wijzigings-voorstellen zijn zichtbaar	
7. Review toets	Ongeoorloofde toegang tot werkstation van de reviewer	M	M	M	H		• Lokale opslag alleen versleuteld of opslag in de (private) cloud • Opmerkingen kunnen alleen in de vorm van comments of track changes	• Alleen aangewezen personen hebben lees- en schrijfrechten • Eerdere versies kunnen niet worden overschreven	Commentaar/ wijzigingsvoor-stellen zijn zichtbaar.	Aantal comments wordt weergegeven
	Onderschepping toetsitems bij transport van werkstation examinator naar gedeelde omgeving	M	M	M	H		Met 2-factor authenticatie en versleutelde verbinding naar digitale toetsomgeving	Alleen aangewezen personen krijgen lees- en schrijfrechten	Logging van activiteiten in digitale toetsomgeving	Overzicht van inlogmomenten, pogingen en gekoppelde IP-adressen
8. Verwerken feedback	Ongeoorloofde toegang tot werkstation van de examinator	M	M	H	H		Lokale opslag alleen versleuteld of opslag in de (private) cloud	Alleen toetseigenaar (exami-nator) heeft recht om track changes te accepteren	Track changes zijn zichtbaar	Notificatie wanneer track changes zijn verwerkt
9. Review toets	Ongeoorloofde toegang tot werkstation van de reviewer	M	M	H	H		• Lokale opslag alleen versleuteld of opslag in de (private) cloud • Opmerkingen kunnen alleen in de vorm van comments of track changes	• Alleen aangewezen personen hebben lees- en schrijfrechten • Eerdere versies kunnen niet worden overschreven	Commentaar/ wijzigings-voorstellen zijn zichtbaar	Aantal comments wordt weergegeven
	Onderschepping toetsitems bij transport van werkstation examinator naar gedeelde omgeving	M	M	M	H		Met 2-factor authenticatie en versleutelde verbinding naar digitale toetsomgeving	Alleen aangewezen personen krijgen lees- en schrijfrechten	Logging van activiteiten in digitale toetsomgeving	Overzicht van inlogmomenten, pogingen en gekoppelde IP-adressen
10. Vaststellen toets	Ongeoorloofde toegang tot werkstation van de examinator	M	M	H	H		Uitsluitend werken op beveiligde gedeelde omgeving	Alleen aangewezen personen krijgen lees- en schrijfrechten	Logging van activiteiten in digitale toetsomgeving	Overzicht van inlogmomenten, pogingen en gekoppelde IP-adressen
11a. Digitaal aanleveren toets	Onderschepping toetsitems bij transport van werkstation examinator naar gedeelde omgeving	H	M	H	H		Met 2-factor authenticatie en versleutelde verbinding naar digitale toets-omgeving	Alleen aangewezen personen krijgen lees- en schrijfrechten	Logging van activiteiten in digitale toetsomgeving	Overzicht van inlogmomenten, pogingen en gekoppelde IP-adressen
11b. Aanleveren toets op papier/ In ontvangst nemen toets	Ongeoorloofde inzage in vragen of normering dan wel ongeoor-loofde wijziging van normering.	H	M	M	H		• Printen alleen in gecontroleer-de ruimte, dan wel beveiligd printen • Verwerken prints (sorteren/ inpakken/opslag etc.) alleen in gecontroleerde ruimte	Enveloppen worden door verzender verzegeld	Overdrachtsmomenten vastleggen (Track & Trace)	Examinator kan inzien in welk stadium van het vermenigvuldigings-/trans-portproces de toetsen zich bevinden

1.3. Afnemen

De omgeving waarin summatief getoetst wordt, loopt relatief veel risico. Op dit aspect nemen de instellingen doorgaans al veel maatregelen die van oudsher noodzakelijk zijn bij elke toetsafname (denk aan controle op spiekbriefjes, regels rondom toiletbezoek, een verbod op het meenemen van mobiele telefoon, etc.). De punten in de tabel zijn daarom vooral gericht op digitale afname, een relatief nieuwe 'tak van sport'.

De eerste tabel gaat in op vier risico's die niet specifiek gekoppeld zijn aan een processtap, maar waar bij digitaal toetsen wel goed op gelet moet worden. De tweede tabel behandelt alle gedetailleerde processtappen.

Risico's integriteit en vertrouwelijkheid						Beheersmaatregelen			
	Kans	Impact				systeeminrichting	autorisaties (functiescheiding)	rapportages	gebruikerscontroles
		B	I	V					
Manipulatie van toetssoftware met mogelijk fraude als gevolg	M		H	H		Beveiliging toetssoftware door: • Tijdsbeperking openstelling • Locatiebeperking openstelling	• Alleen toegang indien expliciet toegestaan • Toegang met minimale rechten	Logging van toegang tot server en applicatie	• Tijdige installatie van updates en patches • Periodieke audit op beveiliging • Controle logging na afname • Hardening servers en netwerkcomponenten • Signalen vanuit studenten serieus nemen
Manipulatie van tentamens-pc's voorafgaand aan een toetsafname	M		H	H		• Tentamenzalen met speciale sloten zodat onderscheid met standaardsloten duidelijk is • Tentamen-pc's automatisch dagelijks voorzien van authentieke programmatuur (images) • Ingangspoorten als USB onklaar of afwezig • Pc's in toetszalen fysiek afgesloten op tafel monteren		Logging imageprocedure	• Extra beveiligde sleutelafgifte • Dagelijkse controle afloop imagingproces
Voorafgaand / na afloop van toets wordt er toch aan toets gewerkt	M		H	H		• Start en einde van elke toets loggen • Opstarten toets éénmalig mogelijk (noodprocedure beschikbaar voor uitzonderingen)			Controle logging na afloop toets
Tentamen-pc is gemanipuleerd en dader niet te achterhalen	L		H	H		• Loggen welke student op welke pc werkzaam is geweest • Per student een pc toewijzen		Gebruikslog	• Controle gebruikerslijst • Controle video surveillancebeelden

De risico's en maatregelen per activiteit:

Activiteit	Risico's integriteit en vertrouwelijkheid						Beheersmaatregelen			
		Kans	Impact				systeeminrichting	autorisaties (functiescheiding)	rapportages	gebruikerscontroles
			B	I	V					
1. Gereedzetten toets	Toets wordt te vroeg (of te laat) opengesteld in de afnameomgeving	M	H	L	M		Gereedzetten verloopt via voorgeprogrammeerde stappen	• Alleen toegang indien expliciet toegang gegeven • Toegang met minimale rechten		Gereedzetten alleen na geautoriseerd verzoek en vier-ogenprincipe hanteren
2. Verzamelen toetsdetails	Ongeoorloofde toegang tot werkstation van de toetscoördinator	L	H	H	H		Zie deelproces Ontwerpen			
3. Voorbereiden ruimte	Manipulatie van de werkstations in de toetsruimte, zoals door hardwarematige key-loggers	H	H	H	H		Ruimten altijd op slot buiten afnametijdvak	Buiten toetsperiode alleen toegang door aangewezen zaalbeheerders		• Bewaking toegang tot de ruimte middels camera's, registraties en strikt toegangsbeheer via sleutel of pas • Fysieke controle aansluitingen en componenten door zaalbeheer

Activiteit	Risico's integriteit en vertrouwelijkheid						Beheersmaatregelen			
		Kans	Impact				systeeminrichting	autorisaties (functiescheiding)	rapportages	gebruikerscontroles
			B	I	V					
4. Vrijgeven toets	Te vroege kennisname van de toetsvragen	L	H	H	H		Splitsing tussen vrijgave toets en vrijgave voor deelnemers	Alleen vrijgave door Functioneel beheer-rol		Alleen vrijgeven na geautoriseerd verzoek
5. Ophalen toetsdetails	Onderschepping van de details bij transport tussen werkstations of werkplek van surveillant en toetscoördinator	M	H	M	M		Zie deelproces Ontwerpen			
	Manipulatie van de toetsdetails (vooral: naam toevoegen aan deelnemerslijst)	M	H	M	M					Toetsdetails in verzegelde envelop transporteren
6. Vrijgeven ruimte	Ruimte wordt te vroeg vrijgegeven waardoor ruimte gemanipuleerd kan worden	L	N.v.t.	M	L			Sleutel wordt alleen afgegeven aan vooraf aangewezen begeleiders van de toets	Noteren sleutelafgifte in log	Sleutel ruimte is vanaf een uur voor het tentamen beschikbaar
7. Betreden ruimte (surveillant)	N.v.t.	N.v.t.	N.v.t.	N.v.t.	N.v.t.				Tijd betreding vastleggen in proces verbaal	
8. Betreden ruimte (student)	N.v.t.	N.v.t.	N.v.t.	N.v.t.	N.v.t.			Betreden door alleen voor toets ingeschreven studenten toegestaan (bijvoorbeeld na scan collegekaart)		Betreden vanaf 15 minuten voor aanvang, toelating door surveillant
9. Openstellen toets	Te vroege kennisname van de toetsvragen	M	H	L	H		Openstellen niet eerder dan 10 minuten voor start mogelijk		Tijd openstelling vastleggen in proces verbaal	
10. Maken toets	Niet de student zelf maar een vervanger neemt deel aan de toets.	H	N.v.t.	H	H		In toetssysteem aanwezige foto van deelnemer op beeldscherm			Controle identiteit door surveillant
	Meedoen zonder te zijn aangemeld voor de toets	H	N.v.t.	H	H		Starten toets alleen mogelijk indien account geactiveerd			Controle aanmelding door surveillant
	Inzage bestanden en openbare kennis tijdens de toets	H	N.v.t.	H	H		Blokkeren internet- en netwerktoegang (zoals door lock-down browser), ook bij gebruik studentenlaptop (beveiligde BYOD oplossing)			Surveillant stelt vast dat geen eigen spullen in het toetslokaal aanwezig zijn
	Ongeoorloofde samenwerking en/of raadplegen bestanden	H	N.v.t.	H	H		• Veilige opstelling werkplekken (afstand) en afscherming beeldschermen (schotten, anti-afkijkfolie) • Randomizing van de vragen			• Toezicht tijdens afname door surveillant • Signalen van studenten en surveillanten (tijdens en na tentamen) over fraudes serieus nemen
	De toets kan per student meer dan eens gestart worden waardoor student antwoorden kan corrigeren etc.	M	N.v.t.	H	H		Vooraf programmeren hoe vaak de toets gemaakt kan worden per student			
	Gebruik van spiekbriefjes e.d.	H	N.v.t.	H	H					Toezicht tijdens afname door surveillant
	Toiletbezoek	H	N.v.t.	H	H		• Toiletblokken alleen tijdens de toets toegankelijk maken • Toiletblokken voor tentamen controleren			Begeleiding toiletbezoek door surveillant
11. Afsluiten toets	Toets te lang open waardoor deelnemer te lang inzage heeft	M	N.v.t.	H	M		Toets wordt automatisch afgesloten		Tijd afsluiten vastleggen in proces verbaal	
12. Rapporteren verloop	Tijdens rapportage toetsmateriaal onbeheerd	M	N.v.t.	H	H					Opbergen documenten in verzegelde enveloppe, doos etc.

1.4. Nakijken

Het deelproces nakijken betreft papieren en digitale toetsen. Voor beide varianten is onderstaande tabel ingevuld.

Activiteit	Risico's integriteit en vertrouwelijkheid						Beheersmaatregelen			
		Kans	Impact				systeeminrichting	autorisaties (functiescheiding)	rapportages	gebruikerscontroles
			B	I	V					
1a. Maken back-up	Back-up is incompleet of on-bruikbaar	M	H	H	H		• Automatische melding bij technische fouten • Inrichten automatische back-up	Volledige leesrechten voor back-up account	Statusverslag	• Initiële test op juiste werking • Periodieke controle bruikbaarheid back-up
1b. Digitaliseren op papier gemaakte toets	Niet alle pagina's gedaan	H	H	M	L		• Automatische metagegevens • Opslag in beveiligde omgeving	Digitaliseren alleen door geautoriseerd persoon	Digitaliseringsverslag	Alle toetsen en pagina's digitaal aanwezig en leesbaar.
2. Ophalen antwoorden	Niet alle antwoorden (gemaakte toetsen) worden opgehaald	M	N.v.t.	H	L		Alle gemaakte toetsen worden bij elkaar (één enveloppe en/of map) opge-slagen. Bij digitale toetsen gebeurt opslag read-only.			Controle op aansluiting aanwezigheidslijst met namen op toetsen
	Onbevoegde haalt antwoorden op of muteert antwoorden	M	N.v.t.	H	H		• Digitaal: 2-factor authenticatie bij inloggen • Papier: identificatie bij ophalen	Alleen aan toets toegewezen personen kunnen toetsen ophalen	Noteren (loggen) door wie en wanneer toets is opgehaald	Controle identiteit ophaler
3. Nakijken antwoorden	Ongeoorloofde toegang tot workstation examinator	M	M	H	H		Lokale opslag alleen versleuteld of nakijken in de (private) cloud Digitaal: 2-factor authenticatie	Op digitaal gemaakt werk alleen leesrechten	Correcties zichtbaar als comments (digitaal) of met andere kleur pen (papier)	
4. Tweede nakijken	Ongeoorloofde toegang tot workstation examinator (2e corrector)	M	M	H	H		Als bovenstaand			
5. Bepalen cijfer	Gebruik onjuiste cesuur (nor-menset)	L	M	H	L		Versiebeheer op normenset		Mutatieverslag normenset	Narekenen door peer

1.5. Analyseren

De analyse spoort items op die van onvoldoende kwaliteit zijn, bijvoorbeeld omdat ze te gemakkelijk, te moeilijk of ambigu blijken te zijn. Hiervoor worden de antwoorden overgehaald naar de analyseomgeving, bij voorbeeld een statistisch programma. De analyse kan leiden tot herziening van de normering en daarmee tot aanpassing van de cijfers.

Activiteit	Risico's integriteit en vertrouwelijkheid						Beheersmaatregelen			
		Kans	Impact				systeeminrichting	autorisaties (functiescheiding)	rapportages	gebruikerscontroles
			B	I	V					
1. Analyseren antwoorden	Ongeoorloofde toegang tot werkstation van de toetsexpert	M	M	H	H		• Lokale opslag alleen versleuteld of analyse in de (private) cloud • Toegang tot de antwoorden via 2-factor authenticatie	Antwoorden niet te wijzigen, door alleen leesmogelijkheid		
	Ongeoorloofde toegang tot analyseomgeving	L	N.v.t.	H	H		Toegang tot de analyseomge-ving via 2-factor authenticatie	Antwoorden niet te wijzigen, door alleen leesmogelijkheid		
2. Rapporteren analyse	Manipuleren cijfers onderweg van itembank/afnameomgeving naar analyseomgeving dan wel analysetool	M	M	H	H		Automatische versleutelde ver-zending door toepassing van servercertificaat			Bij webbased toegang is beveiliging zichtbaar aan een groen slotje in de adresbalk van de browser
3. Vaststellen cijfer	Ongeoorloofde toegang tot werkstation van de examinator	M	M	H	H		Toegang tot de cijfers in de itembank alleen via 2-factor authenticatie	Toegang tot werkstation alleen met persoonsgebonden account	Logging van activiteiten in itembank	Eindcontrole op de audit trail: herziening alleen door bevoegde gebruiker(s)

1.6. Rapporteren

Bij rapportage gaat het om het publiceren van cijfers, inzage en het vastleggen van cijfers in bijvoorbeeld het studentinformatiesysteem (SIS). In dit proces zijn verschillende risico's te identificeren, zoals het ongeoorloofd muteren van cijfers.

Activiteit	Risico's integriteit en vertrouwelijkheid						Beheersmaatregelen			
		Kans	Impact				systeeminrichting	autorisaties (functiescheiding)	rapportages	gebruikerscontroles
			B	I	V					
1. Invoeren cijfers	Manipuleren tentamenbriefjes	L	M	H	M		Digitaliseren tentamenbriefjes			• Persoonlijk afgeven • Beveiligde opslag
	Foutief intypen	M	M	H	M		• Controle op toegestane cijferformats • Controle of toets actief is	Invoer alleen door examinator en administratie (in opdracht van examinator)	Periodieke controle mutatieoverzicht	Vrijgave cijfers door examinator/derde
2. Importeren / vaststellen resultaten	Onjuist inlezen	M	M	H	M		• Inleesprogramma vooraf getest • Controles tijdens inlezen zoals: cursuscode op brief en bestand gelijk	Rechten volgens autorisatiematrix	Transactieverslag	• Vergelijken aangeboden versus ingelezen cijfers • Transactieverslag zonder uitval
	Onjuist vaststellen	M	M	H	L			Vaststellen alleen beschikbaar voor examinator	Transactieverslag	Vergelijken invoer met oorspronkelijk document
	Manipuleren cijfers onderweg van examinator naar SIS (digitaal, via netwerk)	L	M	H	H		Uitslagen versleuteld versturen			
3. Raadplegen cijfer (student)	Raadplegen door ander dan student	M	N.v.t.	L	M		• Alleen toegang tot eigen resultaten • Overige toegang conform autorisatiematrix		Autorisatierapport	Periodieke controle toegekende autorisaties t.o.v. autorisatiematrix
	Raadplegen ongeldige cijfers	M	N.v.t.	L	M		Alleen vrijgegeven cijfers opvraagbaar	Vrijgeven door examinator		
4. Geven inzage	Ongeoorloofde toegang tot ingeleverd werk	M	M	H	H			Alleen inzage eigen materiaal	Vastleggen toegang (wie, wanneer)	Buiten inzagemoment veilige opslag
	Ongeoorloofd aanpassen ingeleverd werk	M	N.v.t.	H	H		Digitale inzage: alleen leesrechten			Inzage onder toezicht
5. Aanpassen cijfer	Onder druk zetten examinator	L	N.v.t.	H	H		Aanpassen alleen via 2-factor authenticatie	Aanpassen alleen door administratie, na goedkeuring examencommissie of examinator	Mutatieverslag inclusief reden van aanpassen	
	Ongeoorloofde aanpassingen via werkstation van de examinator	M	N.v.t.	H	H				Mutatieverslag	Wekelijkse controle mutatieverslag
		N.v.t.	N.v.t.	N.v.t.	N.v.t.					Terugmelden aanpassing
6. Corrigeren cijfer	Ongeoorloofde toegang tot werkstation van de cijferadministratie	M	M	H	H			Aanpassen alleen door administratie	Mutatieverslag	Wekelijkse controle mutatieverslag
	Manipuleren beroepsuitspraken	L	N.v.t.	H	H		Digitale ondertekening uitspraken			Terugmelden aanpassing
	Manipuleren cijfers in het SIS	M	N.v.t.	H	H		Verzwaarde beveiliging SIS		Was-wordt rapportage	Maandelijkse controle wijzigingsmomenten

1.7. Evalueren

In het deelproces evalueren wordt op basis van de gemaakte/afgelegde toetsen, de kwaliteit van de afzonderlijke items en de toets als geheel beoordeeld met als doel te komen tot betere toets, toetsitems en/of toetsmatrijs. Aangezien tussen evaluatie en hergebruik een periode van herziening en eventueel herstel beschikbaar is, geldt in deelproces evalueren geen verhoogd risico.

Activiteit	Risico's integriteit en vertrouwelijkheid						Beheersmaatregelen			
		Kans	Impact				systeeminrichting	autorisaties (functiescheiding)	rapportages	gebruikerscontroles
			B	I	V					
1. Verzamelen gegevens		M	L	M	M			Alleen bij de evaluatie betrokkenen hebben leesrechten op de gegevens		
2. Interpreteren informatie	Onbevoegde toegang tot informatie	M	L	M	M					
3. Trekken conclusies		M	L	M	M					
4. Registreren resultaten	Onbevoegde toegang tot de itembank	M	M	M	M		Toegang tot de cijfers in de itembank alleen via 2-factor authenticatie	Toegang tot itembank alleen met persoonsgebonden account en alleen tot relevant onderdeel	Logging van activiteiten in itembank	Eindcontrole op de audit trail: toegang alleen door bevoegde gebruiker(s)

1.8. Beheren

Het beheer van toetsen en toetsresultaten is doorgaans gericht op het achteraf kunnen verantwoorden van resultaten en het mogelijke hergebruik van toetsitems en toetsen. Herschrijven is gericht op beheer van de toets in plaats van de toetsapplicatie.

Activiteit	Risico's integriteit en vertrouwelijkheid						Beheersmaatregelen			
		Kans	Impact				systeeminrichting	autorisaties (functiescheiding)	rapportages	gebruikerscontroles
			B	I	V					
1. Metadateren en opschonen itembank	Metadata worden onjuist toegevoegd	M	M	M	L		• Geprogrammeerde invoercontroles • Gebruik vaste keuzelijsten	Metadateren door opgeleide expert	Wijzigingsrapportage	Kwaliteitscontrole door peer
	Verkeerde items worden gewist	M	M	M	L		Logging van verwijderde items	Expert heeft alleen toegang tot eigen items	Wijzigingsrapportage	Kwaliteitscontrole door peer
	Items raken verminkt	M	M	M	L		Logging van oude en nieuwe items	Expert heeft alleen toegang tot eigen items	Wijzigingsrapportage	Kwaliteitscontrole door peer
2. Archiveren	Accountbeheer wordt misbruikt	L	M	H	H		Baseline plus 2-factor authenticatie			Periodieke controle wijzigingen
	Archief is incompleet	M	L	H	L			Volledige leesrechten voor archiefaccount	Statusverslag	Controle door archiefbeheerder
	Archief is niet bruikbaar	M	L	H	L		Automatische melding bij technische fouten			Periodieke controle op toegankelijkheid door uitlezen archief
	Ongeautoriseerde toegang tot archief	M	L	L	H		• Toegangscontrole • Versleuteling van archief	Alleen archiefmedewerkers hebben toegang	Toegangslijst	• Controle sleutels • Maandelijkse logcontrole
	Persoonsgegevens worden niet tijdig / correct vernietigd	N.v.t.	M	M	H		• Automatische procedure inregelen	Alleen archiefmedewerkers hebben toegang	Vernietigingsverslag	Periodieke controle vernietigingen

BIJLAGE 4

ASSESSMENT VEILIG TOETSEN

De internationale ISO 27002:2013 norm beschrijft in de hoofdstukken vijf tot en met achttien die aspecten rond informatiebeveiliging die als good practice ingevuld dienen te zijn. Alle security officers in het hoger onderwijs hanteren deze good practice binnen de instelling. Het is daarom goed werkbaar deze norm ook binnen het toetsproces toe te passen.

Onderstaande matrix toont de hoofdstukken met de bijbehorende eisen, ingevuld voor het toetsproces. Het advies is deze matrix te hanteren bij de initiële en vervolgens jaarlijks te herhalen inschatting van het niveau van beveiliging. We bevelen aan hierbij samen te werken met de security officer van je instelling. Op basis van deze matrix kan beoordeeld worden of het toetsproces voldoende beveiligd is. Hiervoor kun je een externe audit laten uitvoeren of een self-assessment doen. NB: deze tabel strekt verder dan alleen de maatregelen die specifiek op het toetsproces zijn gericht, zoals benoemd in hoofdstuk 2 van dit werkboek.

Hfst	Uitwerking / selectie relevante eisen van ISO norm
5.	**Toetsbeleid:** 1. Instelling heeft toetsbeleid opgesteld met ten minste een doelstelling, verantwoordelijkheden en (periodieke) controle op naleving. 2. Het toetsbeleid is beschikbaar voor belanghebbenden, o.a. in OER en vertaald naar praktische instructies en wordt periodiek onder de aandacht gebracht.
6.	**Organiseren van een veilig toetsproces:** 1. De rollen binnen de toetsketen zijn helder uitgewerkt en gecommuniceerd. 2. De locaties waarop uitvoeren van activiteiten binnen het toetsproces is toegestaan (thuis, lokaal, BYOD) zijn concreet en helder uitgewerkt.
7.	**Veilig personeel (zoals docenten, IT-beheerders, surveillanten en assistenten):** 1. Uitgewerkt is wie onder welke voorwaarden ingezet mag worden in het toetsproces. 2. Uitgewerkt is welke kennis/ervaring een betrokkene dient te hebben. 3. Training of trainingsmateriaal is beschikbaar. 4. Actuele geheimhoudingsverklaring (o.i.d.) is getekend.
8.	**Beheer van bedrijfsmiddelen:** 1. Uitgewerkt is welke middelen ingezet worden binnen het toetsproces, inclusief wie daarvan eigenaar en beheerder is. 2. Duidelijk is wat de vertrouwelijkheid van toetsonderdelen (vragen, cesuur, formatief, summatief etc.) is. 3. Uitgewerkt is hoe met verwijderbare media (cd's, USB-sticks, papier) omgegaan wordt.
9.	**Toegangsbeveiliging:** 1. Uitgewerkt is wie wanneer en waar toegang tot toetsmateriaal heeft. 2. Op alle momenten in het gehele toetsproces vindt toegang tot netwerk en applicatie(s) veilig plaats. 3. Toegangsrechten van alle typen gebruikers zijn uitgewerkt (accounts, geldigheid, mogelijkheden binnen accounts). 4. In het bijzonder de speciale toegangsrechten van beheerders, coördinatoren zijn juist uitgewerkt. 5. Toegangsrechten worden periodiek beoordeeld en waar nodig aangepast/ingetrokken. 6. Gebruikers zijn bekend met de wijze waarop zij met wachtwoorden en dergelijke dienen om te gaan. 7. Wachtwoorden worden degelijk beheerd. 8. Waar nodig zijn beveiligde inlogprocedures van toepassing (dubbel inloggen, sterke authenticatie, zoals via SURFconext). 9. Toegang tot broncode (zoals van toetsprogramma's) is deugdelijk ingeregeld.

10.	**Cryptografie:** 1. Uitgewerkt is op welke onderdelen van het toetsproces cryptografie ingezet wordt. 2. Het beheer van de cryptografische sleutels is deugdelijk ingericht.
11.	**Fysieke beveiliging en beveiliging van de omgeving:** 1. Uitgewerkt is welke gebieden (ruimten) rondom het toetsproces beveiligd zijn. 2. Uitgewerkt is hoe de fysieke beveiliging is ingericht. 3. Uitgewerkt is hoe toegang (en registratie daarvan) tot beveiligde ruimten ingericht is. 4. Uitgewerkt is hoe te gebruiken apparatuur in de beveiligde ruimten geplaatst (ruimte tussen toets-pc's, schotten) en ingericht (zoals anti-meeleesfolie e.a.) is. 5. Uitgewerkt is wie onderhoud mag uitvoeren en hoe/waarmee. 6. Uitgewerkt is wie middelen (papier, apparatuur) uit beveiligde ruimten mag meenemen.
12.	**Veiligheid bedrijfsvoering:** 1. Uitgewerkt is hoe binnen het toetsproces gebruikte middelen bediend mogen worden. 2. Uitgewerkt is hoe middelen (toetsen, antwoorden, applicaties, systemen) gewijzigd mogen worden. 3. Uitgewerkt is hoe zeker gesteld wordt dat middelen voldoende capaciteit bieden. 4. Scheiding van ontwikkel-, test- en productieomgevingen is ingericht. 5. Omgevingen en middelen zijn tegen malware beschermd. 6. Van toetsmaterialen en -resultaten worden back-ups gemaakt. 7. Relevante toetsactiviteiten worden gelogd. 8. Ook logs zijn afdoende beschermd. 9. Tijden in de verschillende logs (systemen) zijn gesynchroniseerd. 10. De integriteit van systemen binnen het toetsproces is gewaarborgd. 11. Benutting van technische kwetsbaarheden wordt voorkomen (hardening, virusscanners).
13.	**Communicatiebeveiliging in toetsproces:** 1. Netwerk en netwerkdiensten worden beheerd. 2. Netwerk en netwerkdiensten zijn beveiligd, bijvoorbeeld door netwerkscheiding. 3. Berichten worden voldoende beveiligd uitgewisseld.
14.	**Acquisitie, ontwikkeling en onderhoud van applicaties:** 1. Eisen aan systemen en applicaties (zowel tijdens ontwikkeling als beheer) zijn vastgelegd. 2. Met leveranciers (intern/extern) is over eisen afgestemd. 3. Controle op naleving van de afgesproken eisen vindt plaats. 4. Test van (nieuwe, gewijzigde) toepassingen voorafgaand aan ingebruikname vindt plaats.
15.	**Leveranciersrelaties:** 1. Veilige toegang door leveranciers is geregeld, formeel en in de praktijk. 2. Daar waar sprake is van een leverancierskeken, is toegang binnen de keten geregeld. 3. Naleving van afspraken met leveranciers wordt bewaakt.
16.	**Beheer van incidenten:** 1. Uitgewerkt is welke verantwoordelijkheden en rollen actueel zijn met betrekking tot toetsincidenten. 2. Incidenten worden gerapporteerd. 3. Melding van mogelijke zwakke plekken in de beveiliging van het toetsproces is ingericht. 4. Incidenten worden beoordeeld en correct afgehandeld. 5. Van incidenten wordt geleerd. 6. In geval van incidenten vindt verzamelen van bewijsmateriaal gestructureerd plaats.
17.	**Toetscontinuïteit:** 1. Continuïteitsplannen zijn aanwezig, actueel en periodiek getest. 2. Waar nodig zijn redundante componenten beschikbaar.
18.	**Naleving:** 1. Wettelijke, contractuele en beleidsmatige eisen worden nageleefd. Dit is inclusief eisen rond archivering en intellectuele eigendom. 2. Bescherming van privacy van betrokkenen (met name toetsdeelnemers) is deugdelijk ingeregeld. 3. Naleving van de eisen rond de veilige toetsproces is door onafhankelijke controle geborgd.

BIJLAGE 5

HORA OBJECTEN VALLEND BINNEN HET TOETSPROCES

De Hoger Onderwijs Referentie Architectuur (HORA) benoemt een groot aantal bedrijfsobjecten[8]. Dat zijn elementen die vanuit het bedrijfsperspectief relevant zijn. Het HORA architectuurteam heeft voor deze bedrijfsobjecten een classificatievoorstel gedaan over het vereiste kwaliteitsniveau voor beschikbaarheid, integriteit en vertrouwelijkheid. De bedrijfsobjecten die een rol spelen binnen het toetsproces zijn hieronder weergegeven. Deze classificatie is ook gebruikt om de classificatie binnen de deelprocessen te bepalen in onder andere de risicomatrix in hoofdstuk 2 en de beveiligingsmaatregelen in bijlage 3.

BETROKKEN HORA OBJECTEN IN HET TOETSPROCES

Object	Beschikbaarheid	Integriteit	Vertrouwelijkheid
Opleiding	Midden	Hoog	Openbaar
Onderwijsprogramma	Midden	Hoog	Laag
Examenprogramma	Midden	Hoog	Laag
Toetsresultaat	Laag	Hoog	Midden
Onderwijseenheidresultaat	Laag	Hoog	Midden
Onderwijsovereenkomst	Laag	Midden	Laag
Deelnemer	Midden	Hoog	Hoog
Waardedocument	Laag	Hoog	Laag
Lesgroep	Midden	Midden	Laag
Leergroep	Laag	Midden	Laag
Competentie	Laag	Laag	Openbaar
Onderwijsactiviteit	Midden	Midden	Laag
Deelnemeractiviteit	Midden	Midden	Hoog
Beoordeling	Laag	Hoog	Midden
Rooster	Hoog	Midden	Laag
Toetsmateriaal	Hoog	Hoog	Hoog

[8] http://www.wikixl.nl/wiki/hora/index.php/Categorie:Bedrijfsobjecten

BIJLAGE 6

GEBRUIKT BRONMATERIAAL

- Begrippenkader voor digitaal toetsen (SURF/Michiel van Geloven, 2013) https://www.surf.nl/kennisbank/2013/begrippenkader-voor-digitaal-toetsen.html
- Richtsnoer Veilige digitale toetsafname (SURF, v2.0 mei 2014 kenmerk 19.735, 2014) https://www.surf.nl/kennisbank/2013/richtsnoer-veilige-digitale-toetsafname.html
- Procesbeschrijving Toetsing en Beoordeling door hogeschool VHL, mede gebaseerd op procesbeschrijving van Saxion. (intern document)
- Geslaagd! Handreiking examencommissies (HBO raad vereniging van hogescholen, februari 2011)
- Model beveiligingsbeleid uit het Framework Informatiebeveiliging Hoger Onderwijs (SCIPR, mei 2015) https://www.surf.nl/binaries/content/assets/surf/nl/2015/informatiebeveiligingsbeleid-xx-v20-2015.pdf
- HO Baseline informatiebeveiliging v1.0 (SCIPR, 1 mei 2015) https://www.surf.nl/binaries/content/assets/surf/nl/2015/baseline-informatiebeveiliging-ho-2015.pdf
- Normenkader informatiebeveiliging HO v. 1.4 https://www.surf.nl/binaries/content/assets/surf/nl/2015/normenkader-informatiebeveiliging-ho-2015-v1.3.pdf

COLOFON

Projectleiding en samenstelling inhoud
Jenny de Werk, *SURFnet*
Michiel van Geloven, *SURFnet*
Martin Romijn, *SURFnet*

Kerngroep veilig toetsen
Monica Buijinck, *Saxion*
Roger Deimann, *Hogeschool/Universiteit van Amsterdam*
Louwarnoud van der Duim, *Rijksuniversiteit Groningen*
Ludo van Meeuwen, *Technische Universiteit Eindhoven*
Lud Overkamp, *Saxion*
Nils Siemens, *Hogeschool/Universiteit van Amsterdam*
Hans van der Wal, *Saxion*
Dorinde Winkelaar, *De Haagse Hogeschool*
Alwin Wullink, *Saxion*

Klankbordgroep security officers
(SURF community voor informatiebeveiliging en privacy, SCIPR)
Bart van den Heuvel, *Maastricht University*
Elma Middel, *Hanzehogeschool*
Martijn Plijnaer, *Inholland*
Anita Polderdijk-Rijntjes, *Windesheim*
Alf Moens, *SURFnet*

Klankbordgroep toetsexperts
Joost Dijkstra, *Maastricht University*
Meta Keijzer-de Ruijter, *Technische Universiteit Delft*

Vormgeving
Vrije Stijl, Utrecht

Foto omslag
Flickr - www.flickr.com/photos/yusamoilov/13334048894

November 2017

SURFnet

Moreelsepark 48
3511 EP Utrecht

Postbus 19035
3501 DA Utrecht

088 – 787 30 00
www.surf.nl/surfnet