Richtsnoer Veilige digitale toetsafname

Utrecht, 12 september 2013
Versienummer: 1.0
Kenmerk: (van versie 1.0) 19.735

Inhoudsopgave

1. Inleiding

Aanleiding

Een effectieve benutting van ICT in het hoger onderwijs en onderzoek kan leiden tot een scala aan voordelen, zoals bijvoorbeeld een efficiëntere bedrijfsvoering bij instellingen, verbetering van de studieresultaten en verlaging van de werkdruk van docenten.

Binnen dit algemene kader wordt ICT ook steeds meer ingezet als middel bij het afnemen van toetsen. Elk onderdeel van het toetsproces kan met ICT worden ondersteund:

- Toetsvragen maken (toetsconstructie): juist voor het samen met anderen, binnen of buiten de instelling, werken aan een set toetsvragen, kan ICT ondersteunend werken.
- Toetsen samenstellen: ICT kan helpen bij het samenstellen van een toets, zodat deze b.v. van de juiste moeilijkheid is, een juiste mix aan onderwerpen bevat, bewaking dat bepaalde vragen niet ongewenst hergebruikt worden, etc.
- Toetsafname: het is mogelijk voorgaande toetsstappen met ICT te ondersteunen, maar toetsafname op papier te doen. Ook is het mogelijk dat de toetsafname digitaal wordt gedaan.
- Toetsanalyse: ook voor beoordelen/scoren en/of analyseren kan ICT ondersteunend zijn.

Bij het inzetten van ICT voor toetsen is de vraag aan de orde: welke risico's gaan er spelen bij inzet van ICT? Welke maatregelen moet je overwegen? Dit document kan instellingen helpen bij het beantwoorden van die vragen.

Scope van dit document

Bij de totstandkoming van deze versie van dit document is discussie geweest over de scope. Daarbij speelde mee:

- Er moet aandacht worden besteed aan alle stappen in het toetsproces.
- Bij een eerste bijeenkomst met experts uit de instellingen bleek al veel tijd te gaan zitten in bespreken van risico's en maatregelen op gebied van digitale toets*afname.*
- Doordat (ook) de betrokken instellingen gebruik maakten van lokaal geïnstalleerde toetssoftware, was de ingebrachte expertise ook daarop gericht.
- In een tweede bijeenkomst is besproken welke gevolgen er zijn als delen van het toetsproces met IT in de cloud wordt ondersteund. De resultaten van die bijeenkomst zijn in bijlage 2 opgenomen.
- Bij digitaal toetsen wordt in veel gevallen gebruik gemaakt van standaard IT-middelen. We nemen in dit Richtsnoer aan dat elke instelling de standaard IT goed beveiligt, en dat er genoeg publicaties beschikbaar zijn waarin standaard maatregelen staan voor die beveiliging. Denk aan goede anti-virus-maatregelen, firewalls, ingericht capaciteitsbeheer, procedures voor hardenen van servers etc.
- Wat voor de ene lezer een open deur is, is voor de ander een welkome opfrisser.
- Er is een verschil voor beveiliging tussen formatief en summatief toetsen.
- De situatie is, door de vele technische en organisatorische mogelijkheden, in elke instelling anders. Aan de ene kant wil je met een publicatie als deze niet te globaal zijn, aan de andere kant wil je niet teveel in detail treden. Maar in bepaalde situaties is detail prettig, b.v. als voorbeeld.
- Moet er ook wat gezegd worden over het meenemen en gebruik van eigen apparatuur (Bring Your Own Device, BYOD)? BYOD stelt voor summatieve toetsen dusdanige eisen aan het beheer van die apparatuur dat het in de huidige praktijk moeilijk is hier een vertrouwde omgeving voor toetsen op te realiseren. In bepaalde omstandigheden kan BYOD voor specifieke toepassingen en in een kleine groep worden gebruikt, mits er deskundig toezicht

aanwezig is bij het afnemen van de toets. Denk bijvoorbeeld aan een blinde student die op zijn eigen laptop, voorzien van hulpmiddelen, een toets maakt.
- Voor in het voorjaar 2013 te starten experimenten was een 1ste versie van dit document gewenst: dat biedt de mogelijkheid dit document in de praktijk te beproeven en op basis van bevindingen te verbeteren.

Deze versie van het document beperkt zich alles afwegende tot:

1. De toetsafname
2. Lokale infrastructuur bij de instelling (‘on-premise’)
3. Gebruik van door de instelling beheerde apparatuur
4. *Summatief* toetsen

In latere versies van dit document zal de scope mogelijk worden verbreed.

Het gebruik van dit document

SURF wil instellingen die ICT inzetten voor hun toetsproces graag op weg helpen door het aanbieden van een Richtsnoer op gebied van beveiliging van digitaal toetsen. De term ‘Richtsnoer’ is overgenomen van het CBP (College Bescherming Persoonsgegevens).

Het document geeft praktische tips, en omdat elke situatie anders is moet de instelling zelf blijven nagaan in welke mate tips van toepassing zijn en welke aanvullende maatregelen nodig zijn voor een goede beveiliging.

Naast het Richtsnoer hebben we enkele praktijkvoorbeelden beschreven waaruit blijkt hoe enkele instellingen toetsen digitaal ondersteunen en welke maatregelen er zijn genomen om dat te beveiligen. Zie ‘*Praktijksituatie Veilige toetsafname in het Hoger Onderwijs en Onderzoek*’.

Dit ‘*Richtsnoer Veilige digitale toetsafname*’ kan gezien worden als aanvulling op de onderwijs- en examenregeling (OER). Overigens gaan de meeste onderwijs- en examenregelingen niet in op de wijze waarop tentamens worden afgenomen, de inrichting van het lokaal en de wijze waarop het toezicht is georganiseerd. Daarvoor hanteren faculteiten vaak een operationeel document met regels en richtlijnen van de examencommissie voor een bepaald type opleiding. Het kunnen aantonen dat voldaan is aan die regels en richtlijnen betekent dat het examen rechtmatig is verlopen.
Dit is de eerste versie van dit document. Alle lezers worden uitgenodigd hun opmerkingen, aanvullingen en suggesties te delen. Het streven is om begin 2014 een nieuwe versie te publiceren.

Totstandkoming

Dit richtsnoer is tot stand gekomen met inbreng van inhoudelijke experts uit instellingen. Er is een tweetal sessies georganiseerd:

1. In de eerste sessie is in kaart gebracht welke stappen er zijn in het toetsproces (zie bijlage 1). Vervolgens is ingezoomd op risico’s bij digitale toetsafname.
2. In de tweede sessie is gekeken naar de invloed van de cloud op digitaal toetsen, en is ook gekeken naar meer dan alleen digitale toetsafname.

De belangrijkste risico’s van digitale toetsafname zijn volgens de geraadpleegde experts:

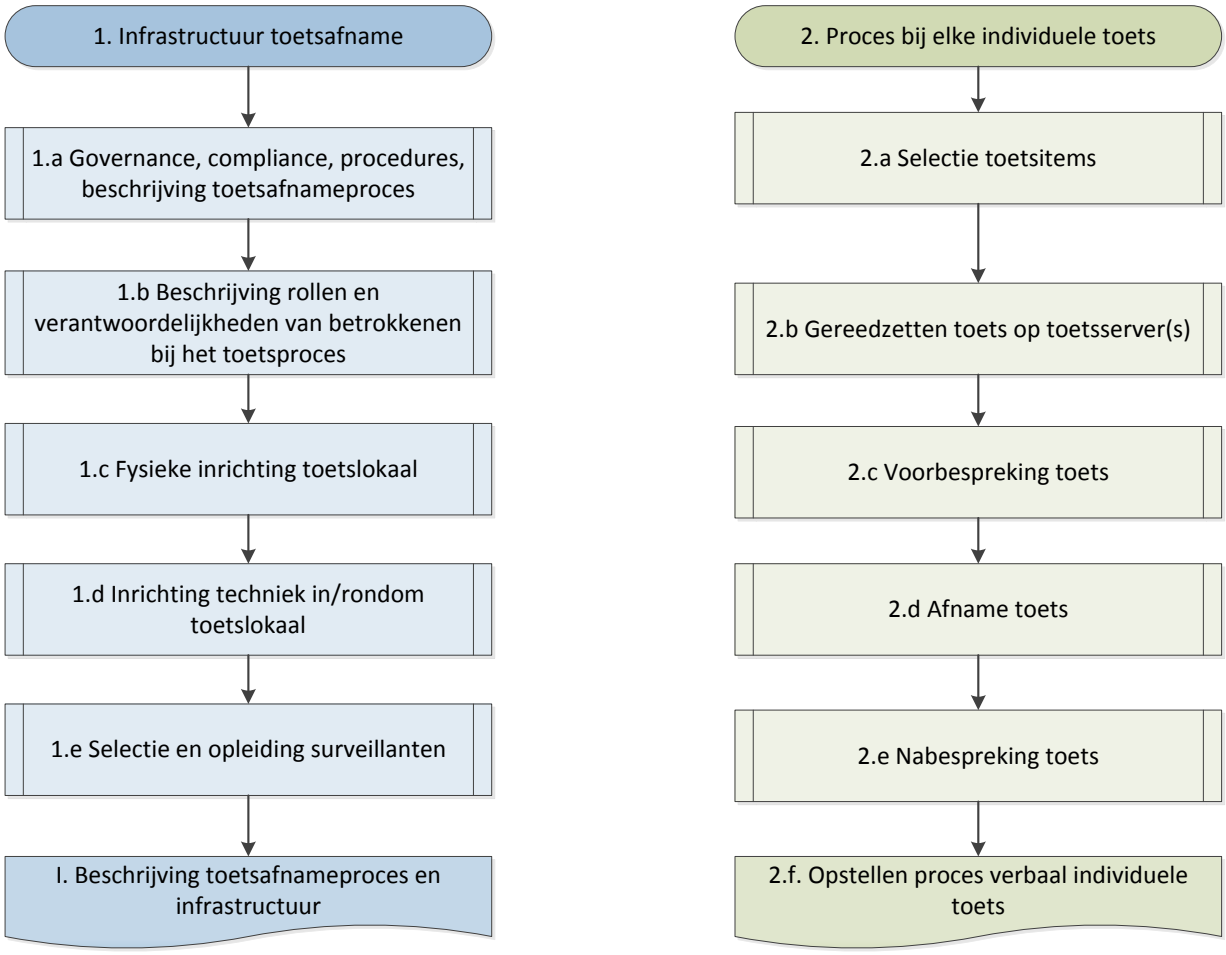
- Het niet kunnen aantonen dat de toets rechtmatig verlopen is.
- Onduidelijkheid over rollen en verantwoordelijkheden, waardoor bijvoorbeeld op ad hoc basis met incidenten en calamiteiten wordt omgegaan, met als gevolg dat toetsresultaten verloren kunnen gaan en imagoschade kan worden opgelopen.
- Technisch is het mogelijk om te frauderen, bijvoorbeeld door ongeoorloofd samen te werken of af te kijken.

2. Structuur: infrastructuur & individuele toets

We onderscheiden twee aspecten bij een veilige digitale toetsafname:

1. De benodigde infrastructuur, inclusief vastgestelde procedures, rollen en verantwoordelijkheden, technische voorzieningen en goed opgeleide surveillanten.
2. Daarnaast is er bij elke individuele toets een proces waarin de toetsafname wordt voorbereid, gehouden en geëvalueerd.

In onderstaande figuur is dit gevisualiseerd.



Als eerste behandelen we in dit document de aspecten governance en compliance (1.a: te volgen procedures, uitzonderingen en aantonen rechtmatigheid van de toets), vervolgens gaan we in op de gewenste rollen en verantwoordelijkheden bij een gecontroleerde toetsafname (1.b). Daarna volgen vereisten aan het toetslokaal (1.c), maatregelen in de techniek (1d), de kwaliteit en bevoegdheden van de surveillanten (1.e).

Bij de beschrijving van de toetsprocedure (1.a) wordt ook aandacht besteed aan het proces dat bij elke individuele toetsafname gevolgd dient te worden (2.a t/m 2.f).

3. Governance en compliance

Wanneer het proces van digitale toetsafname niet expliciet is beschreven, kan het voorkomen dat er op ad hoc-basis door verschillende betrokkenen omgegaan wordt met situaties die om een oplossing vragen. Het risico hierbij is dat de situatie kan ontstaan dat de instelling niet kan aantonen dat een toets rechtmatig is verlopen.

Het bestaande examenreglement moet worden aangevuld met zaken die van belang zijn voor digitale toetsafname. Voorbeelden:

- Welke rollen (LET OP: het gaat hier niet om *personen*, maar om *rollen*) en verantwoordelijkheden moeten belegd zijn, voor zover ze afwijken van papieren toetsafname?
- Wat moeten surveillanten weten van de techniek om hun werk adequaat uit te kunnen voeren?
- Wie roostert digitale toetsen in en in overleg met wie?
- Wie zet de toets gereed?
- Wie is verantwoordelijk voor de beveiliging van de infrastructuur en de werkplekken?
- Hoe voorkom je dat er te weinig server- en netwerkcapaciteit is?
- Hoe gaan we om met incidenten, calamiteiten en crises?

Voor dit onderdeel zijn de volgende risico's onderkend, en worden de genoemde maatregelen voorgesteld:

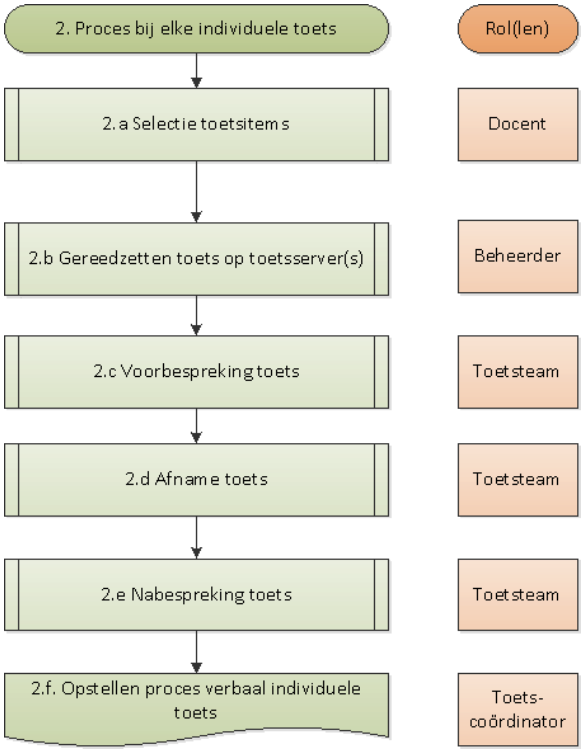
Risico	**Maatregel**
Geen duidelijkheid over de wijze van voorbereiden, afname en beoordeling van digitale toetsen, waardoor er van alles fout kan gaan: ongeoorloofd samenwerken, toetsen van te voren inzien, e.d.	Gc-1: beschrijving procedures bij digitaal toetsen
Geen ketenregie, waardoor taken niet adequaat worden uitgevoerd c.q. er geen coördinatie tussen taken is	Gc-2: beschrijving van de overdrachtsmomenten tussen betrokken rollen
Geen eenduidig beleid m.b.t. afwijkingen, incidenten, calamiteiten en crisis, waardoor in vergelijkbare situaties op verschillende manieren opgetreden wordt: willekeur	Gc-3: beschrijving van uitzonderingen en afwijkingen van procedures en overdrachtsmomenten
Slechte voorbereiding van de betrokkenen op incidenten, calamiteiten en crises, waardoor bijvoorbeeld gemaakte toetsen verloren gaan	Gc-4: periodiek testen van incident-, calamiteiten- en crisisplannen
Afwijkingen van beleid worden op ad hoc-basis genomen: willekeur Spieken en samenwerken is mogelijk	Gc-5: vooroverleg betrokkenen en bepalen bijzonderheden voorafgaand aan elke toetsafname
Tekort aan surveillanten Ondeskundige surveillanten	Gc-6: bepaling kwaliteit en kwantiteit in te zetten surveillanten
Niet kunnen aantonen dat de toets rechtmatig is verlopen	Gc-7: opstellen proces verbaal

Hieronder worden de maatregelen toegelicht:
Gc-1: beschrijving procedures
De gewenste gang van zaken bij digitale toetsen wordt beschreven en in procedures vastgelegd (klaarzetten van de toets, sleutelbeheer en uitleen, opleiding/training van surveillanten, omgaan met gestreste of zieke studenten, etc.).

De procedure veilige toetsafname beschrijft minimaal de volgende onderwerpen

- De wijze waarop de docent toetsitems kan selecteren
- Of en hoe de scheiding tussen de toetsitemvoorraad van de docenten en de toetsafnameserver tijdens alle deelprocessen gehandhaafd wordt
- Hoe de werkplekbeheerder / toetsondersteuner toetsitems gereed zet op de (dedicated) toetsafnameserver(s)
- Welke rollen en verantwoordelijkheden onderdeel zijn van het toets-team, bijvoorbeeld: toetscoördinator, beheerder en surveillance-coördinator, desgewenst aangevuld met incidentcoördinator en roosteraar
- Voor- en nabespreking per toetsperiode door het team
- Welke handelingen gelogd worden, bijvoorbeeld:
    - Wie op welk moment toegang krijgt tot de toetsitemvoorraad
    - Selectie van toetsitems
    - Wie op welk moment toegang krijgt tot de toetsafnameservers
    - Gereedzetten toets
    - Start en einde van elke individuele toetsafname
    - Vraag- en toetsanalyse + eventuele aanpassing cesuur
    - Inzage toetsresultaat
    - Aanpassen toetsuitslag na inzage
- Hoe de toegang tot het toetslokaal beveiligd is c.q. gecontroleerd wordt
- Hoe het toetslokaal ingericht behoort te zijn om samenwerken en afkijken tegen te gaan
- Welke technische maatregelen genomen dienen te worden om fraude te voorkomen
- Hoe een proces verbaal er uit dient te zien
- Beleid over uitzonderingen en afwijkingen en wie daarover besluiten neemt
- Wie verantwoordelijk is voor het opstellen, testen en onderhouden van incident-, calamiteiten- en crisisplannen
- Hoe het crisisteam functioneert in geval van calamiteiten gedurende een toetsafname.

Gc-2: overdrachtsmomenten tussen betrokkenen
In het proces van de individuele toetsafname zijn de volgende rollen betrokken.



Het proces is dus als volgt:

- Docent selecteert toetsitems en meldt aan de beheerder welke items op welke datum op de toetsafnameserver(s) gereed dienen te staan
- Beheerder rapporteert wanneer hij de items op de server heeft gezet en heeft getest of de items benaderbaar zijn
- Toetscoördinator formeert toetsteam, waarin minimaal de volgende rollen zijn vertegenwoordigd: toetscoördinator, beheerder, facilitair medewerker en surveillancecoördinator, desgewenst aangevuld met incidentcoördinator en roosteraar
- Toetsteam houdt voorbespreking: zie Gc-5, Gc-6
- Toetscoördinator maakt na evaluatie door toetsteam (2.e) proces verbaal op (Gc-7).

Gc-3: beleid voor uitzonderingen en afwijkingen
Ook uitzonderingen en afwijkingen van procedures en overdrachtsmomenten worden vastgelegd.

Voorbeelden:

- De beheerder maakt geen onderdeel uit van het toetsteam, omdat hij voorafgaand aan de toets zijn werk al gedaan heeft en er voor zorgt dat begin en einde van elke individuele toets gelogd wordt
- De facilitair medewerker maakt geen onderdeel uit van het toetsteam, omdat het enige dat hij doet is het sleutelbeheer van het toetslokaal
- Surveillantencoördinator delegeert zijn verantwoordelijkheid (kennis van procedures, uitzonderingen en calamiteitenplannen) tijdens de toetsafname aan de toetscoördinator.

Gc-4: testen van toetsomgeving en incident-, calamiteiten- en crisisplannen
Het regulier functioneren van de toetsomgeving wordt periodiek getest (testplan maken). Onderdeel van de procedures is het opstellen en periodiek testen van incident-, calamiteiten- en crisisplannen.

Oproep aan de lezers: kan iemand een voorbeeld van een testkalender leveren waarop de planning staat voor periodieke testen van de incident-, calamiteiten- en crisisplannen?

Gc-5: vooroverleg betrokkenen voor elke toetsafnameperiode
In de procedures is tevens vastgelegd dat voorafgaand aan elke toetsafnameperiode overleg plaatsvindt tussen de toetscoördinator, beheerder, facilitair manager, surveillancecoördinator en incidentencoördinator, aangevuld met docenten die in die periode digitale toetsen aanbieden. In dit overleg worden bijzonderheden besproken en vastgelegd, zoals bijvoorbeeld welke studenten extra tijd mogen gebruiken en voor welke studenten bijzondere voorzieningen gereed moeten zijn, bijvoorbeeld door medische omstandigheden, zoals bepaalde functiebeperkingen.

Gc-6: surveillanten
In het vooroverleg wordt tevens bepaald hoeveel surveillanten met welke kwaliteiten aanwezig dienen te zijn.

Voorbeelden:
- Er wordt vermoedelijk gewerkt met een standaard hoeveelheid aan surveillanten: 1 op x studenten. Indien in de voorbespreking duidelijk wordt dat bepaalde studenten extra hulp nodig hebben, bijvoorbeeld a.g.v. dyslexie , dan kan bepaald worden om een of meer extra surveillanten in te zetten
- In het geval dat een blinde student op een laptop met extra voorziening de toets zal afnemen kan er één surveillant gekozen worden die bekend is met die voorziening en eventueel assistentie kan verlenen.

Gc-7: proces verbaal
Van elke toets wordt bijgehouden hoe deze verlopen is. Na afloop worden de afwijkingen t.o.v. de procedures geëvalueerd en vastgelegd in een proces verbaal. In het proces verbaal worden de loggegevens van de tentamen-pc's opgenomen en indien nodig van commentaar voorzien. Het proces verbaal dient aan te tonen dat de toets rechtmatig verlopen is.

4. Rollen en verantwoordelijkheden

Wanneer rollen en verantwoordelijkheden bij digitaal toetsen niet zijn belegd is, de kans groter dat er fouten gemaakt worden, waardoor het risico op mislukte toetsen toeneemt. Betrokkenen horen te weten wat hun rol is en wat er van hen verwacht wordt.

We benadrukken hier nogmaals dat we spreken over rollen: een persoon kan soms meerdere rollen vervullen, waarbij wel moet worden gelet op voldoende functiescheiding.

Voor dit onderdeel zijn de volgende risico's onderkend, en worden de genoemde maatregelen voorgesteld:

Risico	**Maatregelen**
Het kan zijn dat de toets niet op tijd gereed staat, dat een verkeerde toets gereed staat, dat er veel te weinig surveillanten aanwezig zijn, dat de surveillanten niet weten hoe de toets-pc moet worden opgestart, e.d.	Beschrijven rollen en verantwoordelijkheden: • Toetscoördinator • Beheerder • Facilitair medewerker • Surveillancecoördinator • Incidentencoördinator • Examencommissie
Betrokkenen weten niet wat er van hen verwacht wordt in een bepaalde situatie, wachten op elkaar	
Onduidelijkheid m.b.t. omgang met incidenten en crisis, waardoor toetsresultaten verloren kunnen gaan of willekeurig wordt opgetreden	
Gebrek aan training en bewustwording bij betrokkenen Gebrek aan functiescheiding	

De volgende rollen en verantwoordelijkheden dienen beschreven en ingericht te zijn[1]:

- **Toetscoördinator**: is eindverantwoordelijk voor het gehele toetsproces, vanaf het klaarzetten van de toets (na overleg met de docent), de techniek, het lokaal, tot aan het optreden van de surveillanten. [N.B.: de beoordeling en eventuele inzage van de toetsen behoort tot de verantwoordelijkheid van de docent]. De toetscoördinator kan aantonen dat de toetsen rechtmatig zijn afgenomen en legt verantwoording af aan de examencommissie.
  N.B.: er zijn instellingen die werken met een toetsondersteuner, die de toetscoördinator kan ontlasten door eenvoudige werkzaamheden over te nemen.
- **Beheerder**: is verantwoordelijk voor de onder techniek vermelde zaken (beheer en onderhoud); rapporteert aan de toetscoördinator.
  N.B.: bij veel instellingen wordt onderscheid gemaakt tussen functioneel beheer en technisch beheer. In onderling overleg kunnen de aan de beheerder toebedachte taken tussen beide soorten beheerders worden verdeeld.
- **Facilitair medewerker**: is verantwoordelijk voor (toegang tot) de toetszalen, sleutelbeheer, de inrichting van het lokaal (niet de toets-pc's) en eventueel videobewaking. Is verantwoording verschuldigd aan de toetscoördinator.
  N.B.: er zijn instellingen waar de facilitair medewerker wordt ondersteund door een werkplekbeheerder, dan wel een zaal- of locatiebeheerder. Legt verantwoording af aan de toetscoördinator.

[1] Het zal voorkomen dat een instelling andere benamingen gebruikt. Waar het om gaat is dat alle bijbehorende taken belegd zijn. Het is niet de bedoeling dat dit allemaal aparte functionarissen moeten zijn; verschillende rollen kunnen aan één functie/functionaris worden toegewezen.

- **Surveillance-coördinator**: is verantwoordelijk voor de selectie, training, aanwezigheid en het functioneren van de surveillanten. Zorgt voor inroostering van surveillanten. Legt verantwoording af aan de toetscoördinator.
- **Incidentcoördinator**: verantwoordelijk voor afwijkingen, uitzonderingen, incidenten en crises. Legt verantwoording af aan de toetscoördinator.
- **Examencommissie**: heeft de finale eindverantwoordelijkheid.

De overdrachtsmomenten tussen genoemde rollen worden beschreven in de onderwijs- en examenregeling van de instelling (genoemd in 3, Governance en compliance).

5. Techniek

Toelichting

Technische maatregelen vormen naast governance het hart van dit richtsnoer. De techniek van digitale toetsafname moet werken (beschikbaarheid en capaciteitsmanagement) en dient ongeoorloofde handelingen te voorkomen, dan wel op te sporen.

Het is in het kader van dit Richtsnoer vrijwel onmogelijk om met alle technische mogelijkheden rekening te houden. De ene instelling heeft zijn toetsinfrastructuur ‘stand alone’ staan, terwijl de andere instelling het uit de cloud afneemt. We benoemen daarom een aantal aandachtspunten en verwijzen graag naar de praktijkvoorbeelden die separaat beschreven zijn.

Voor dit onderdeel zijn de volgende risico’s onderkend en worden de genoemde maatregelen voorgesteld:

Risico	**Maatregel**
Toetsvragen zijn tijdens het transport openbaar toegankelijk	T-1: versleuteld transport
Manipulatie van toetssoftware met mogelijk fraude als gevolg	T-2: eisen aan toetssoftware (het pakket)
Inzage bestanden en openbare kennis	T-3: blokkeren internet- en netwerktoegang
Student geeft zich voor een ander uit	T-4: opnemen student-ID in elke toetsapplicatie
Manipulatie van tentamen-pc’s en –servers voorafgaand aan een toetsafname	T-5: tentamen-pc’s dagelijks voorzien van nieuwe images
Manipulatie van tentamen-pc’s en –servers voorafgaand aan een toetsafname	T-6: perfect beheer van tentamen-pc’s en -servers
Manipulatie van toetsservers voorafgaand aan een toetsafname	T-7: hardening van servers
- Manipulatie van toetsinfrastructuur , waaronder toets–servers, voorafgaand aan een toetsafname - Stroomuitval, uitval servers	T-8:professioneel beheer van toetsomgeving, waaronder maandelijkse PENtest van servers
In geval van een calamiteit zijn servers niet beschikbaar of gemanipuleerd	T-9: up-date-plan voor servers
Beheerder manipuleert tentamen-pc’s	T-10: gelogde activiteiten beheerder beoordelen
Er wordt voorafgaand of na afloop van het tentamen toch aan de toets gewerkt	T-11: start en einde van elke individuele toets loggen
De pc is gemanipuleerd en de ‘dader’ kan niet meer achterhaald worden	T-12: loggen welke student op welke pc werkzaam is geweest
Ongeoorloofde samenwerking en/of raadplegen bestanden	T-13: meekijken op toets-pc’s tijdens de toetsafname
Beheerder is zich niet bewust van zijn rollen en verantwoordelijkheden	T-14: beheerder is verantwoordelijk voor de staat der techniek

Mogelijke maatregelen c.q. aandachtspunten

Hieronder worden de maatregelen toegelicht:

T-1: De opslag en het transport van toetsvragen en -antwoorden dienen altijd te worden beschermd door lichtpaden en/of versleuteling.

T-2: De gebruikte toetssoftware (het pakket) dient minimaal aan de volgende vereisten te voldoen
- De toetssoftware (of de configuratie van de ICT-voorzieningen van het toetslokaal) moet het mogelijk maken om af te dwingen dat de toets uitsluitend op het daarvoor bestemde moment en locatie gemaakt kan worden.
- De toetsapplicatie is onderzocht op gevoeligheid voor netwerkverstoringen. Op basis daarvan zijn fall-back-mechanismen ontworpen, geïnstalleerd en beheerd.

T-3: Bij summatieve toetsen wordt in de voorbespreking bepaald welke sites toegankelijk mogen zijn, omdat studenten daarvan gebruik mogen maken tijdens de toets. De rest van internet wordt geblokkeerd. Als de toegestane sites worden gewijzigd dient dit ook te worden getest in een zaalconfiguratie. Het inschakelen van andere dan de beoogde netwerkverbindingen dient gelogd te worden; een wired toets-pc heeft bijvoorbeeld geen Bluetooth, 3G of WiFi-dongle van de student nodig.
T-4: In elke toetsapplicatie wordt de ID van de desbetreffende student opgenomen, zodat de surveillant het fysieke ID kan vergelijken met die op het beeldscherm.
T-5: De tentamen-pc's dienen voorafgaand aan elke toets te worden voorzien van nieuwe images. Re-imagen moet zo eenvoudig en snel werken dat het bij een vermoeden van onregelmatigheden desnoods tussen twee toetsen in gedaan kan worden.
T-6: De tentamen-pc's dienen perfect beheerd te worden:
- Er moeten zodanige maatregelen genomen worden dat het de student onmogelijk gemaakt wordt om voorafgaand, tijdens of na de toets enige vorm van (ongeoorloofde) hard- en/of software te installeren en/of te gebruiken.
- Patches dienen up-to-date te zijn.
- Geen updates in de toetsperiode en goede test na elke update.
- Antivirus (en indien gebruikt mailfiltering) dient op orde te zijn.
- Local admin of rootrechten zijn uitgeschakeld.
- Waar mogelijk worden externe USB slots, firewire, etc. dichtgelijmd of anderszins onklaar gemaakt.

T-7: De gebruikte servers dienen te worden gehardend en gededicated:
- Hierbij moet de gehele (technische) keten worden bekeken; van server, via netwerk(componenten) t/m toetsafname-pc.

T-8: De digitale toetsomgeving wordt professioneel beheerd:
- Netwerk, server(s) en stroomvoorziening zijn redundant uitgevoerd.
- Incident-, change- en problem-procedures zijn beschreven en worden gevolgd.
- Onderdeel van de change-procedure is dat de toetsservers regelmatig gePENtest worden. Alternatief kan zijn dat er een apart toets-image wordt gebouwd, dat voorafgaand aan de toetsperiode wordt geïnstalleerd (zie ook T5) en dagelijks ververst. Dat toets-image wordt uitsluitend gebruikt bij een digitale toetsafname.

T-9: Er is een update-plan voor de servers beschikbaar.
T-10: De vooraf afgesproken relevante activiteiten van de beheerder worden gelogd en elke 3 maanden *steekproefsgewijs* bezien door de toetscoördinator. De bevindingen worden gedocumenteerd en –indien nodig- gerapporteerd aan de examencommissie.
T-11: De start en het einde van elke individuele toets wordt gelogd.
T-12: Er wordt gelogd welke student op welke toets-pc werkzaam is geweest.
T-13: Er is software geïnstalleerd, waarmee gedurende de toetsafname remote op alle toets-pc's meegekeken kan worden, teneinde te kunnen beoordelen of er ongeoorloofd wordt samengewerkt of bestanden geraadpleegd.
T-14: De beheerder is verantwoording schuldig over 'de staat der techniek' aan de toets-coördinator.

6. Toetslokaal

Toelichting

Vaak wordt een lokaal met bestaande werkplekken voor studenten tijdelijk ingericht voor een toetsafname. Dan dienen wel extra maatregelen genomen te worden voorafgaand aan de toetsperiode om onbevoegde toegang tot toets-pc's en bijvoorbeeld het plaatsen van bijvoorbeeld key-loggers te voorkomen. Maar ook als er een permanente ruimte voor digitale toetsafname beschikbaar is dienen dit soort zaken geregeld te zijn.

Om te voorkomen dat tijdens de toets wordt samengewerkt of afgekeken dienen maatregelen genomen te worden. Om te voorkomen dat voorafgaand aan een toets apparatuur gemanipuleerd wordt dient de toegang tot het lokaal gedurende de toetsperiode gereguleerd te zijn. Onderstaand enkele voorbeelden van mogelijke maatregelen. Voor beide typen maatregelen zijn diverse alternatieve maatregelen te bedenken. We presenteren enkele voorbeelden.

Voor dit onderdeel zijn de volgende risico's onderkend, en worden de genoemde maatregelen voorgesteld:

Risico	**Maatregel**
Onbevoegde toegang tot toets-pc's	Tl-1: sleutelbeheer
Onbevoegde toegang tot toets-pc's	Tl-2: videobewaking toegangsdeur toetslokaal
Afkijken en samenwerken	Tl-3: opstelling werkplekken en afscherming beeldschermen
M.b.v. bijv. hardware-matige key-loggers kan worden afgekeken	Tl-4: zichtbaarheid aansluitingen
M.b.v. bijv. hardware-matige key-loggers kan worden afgekeken	Tl-5: dagelijkse inspectie van alle aansluitingen
Inzien meegebrachte 'hulpmiddelen'	Tl-6: geen eigen spullen meenemen in het toetslokaal

Mogelijke maatregelen c.q. aandachtspunten

Hieronder worden de maatregelen toegelicht:

Tl-1: De facilitair manager beheert gedurende de periode dat de toetslokalen 'in control' moeten zijn de sleutels ervan. Alternatief: er wordt gewerkt met elektronische toegang: alleen personen met de juiste pas kunnen naar binnen
Tl-2: In een situatie waarin het toegangsbeheer niet adequaat geregeld kan worden dient gedurende de toetsperiode videobewaking van de toegangsdeur te worden aangebracht
Tl-3: Afhankelijk van hoe random de toetsvragen worden aangeboden aan de individuele studenten (krijgen ze wel of niet de vragen in dezelfde volgorde voorgeschoteld) worden regels gesteld aan:

- De afstand tussen de tafels
- De afscherming van beeldschermen: dat kan bijvoorbeeld door het werken met één-persoons tafels met pc, toetsenbord en muis, of laptop

Tl-4: De wijze waarop toets-pc's zijn aangesloten is zichtbaar, waardoor het eenvoudig visueel is te beoordelen of er bijvoorbeeld hardware-matige key-loggers zijn aangebracht
Tl-5: De werkplekbeheerder inspecteert in de toets-periode voorafgaand aan elke toets alle aansluitingen, om te controleren of er geen hardware-matige key-loggers zijn aangebracht
Tl-6: Het is niet toegestaan eigen spullen mee te nemen in het toetslokaal. Denk aan jassen, rugzakken, telefoons, laptops, e.d. Zorg dus voor kluisjes, kapstokken of een bemande garderobe buiten het toetslokaal.

7. Surveillanten

Toelichting

Toezicht tijdens examens is noodzakelijk. In iedere onderwijs- en examenregeling is daar ongetwijfeld aandacht aan besteed. Instellingen dienen na te gaan of er in het geval van digitale toetsafname aanvullende of afwijkende toezichtsmaatregelen genomen dienen te worden.

Om het toetsafnameproces zo vlot mogelijk te kunnen laten verlopen zullen surveillanten over bepaalde vaardigheden moeten beschikken (geen digibeten) en weten hoe met incidenten omgegaan dient te worden.

Voor dit onderdeel zijn de volgende risico's onderkend, en worden de genoemde maatregelen voorgesteld:

Risico	**Maatregel**
Ondeskundige surveillanten	S-1: opleidings- en trainingsplannen
Geen hulp kunnen bieden aan studenten	S-2: basiskennis van pc's en inlogprocedures
Geen snelle eerste hulp kunnen bieden in geval van afwijkingen, uitzonderingen en incidenten	S-3: basiskennis van afwijkingen, uitzonderingen en crisisplannen
Niemand kent de procedures m.b.t. afwijkingen, uitzonderingen en incidenten precies	S-4: aanwezige hoofdsurveillant kent afwijkingen, uitzonderingen en crisisplannen
Student geeft zich voor een ander uit	S-5: check ID-kaart met beeldscherm-ID
Ondeskundige en onprofessionele surveillanten	S-6: Surveillanten weten wat er mis kan gaan en hoe ze dan moeten optreden

Mogelijke maatregelen c.q. aandachtspunten

Hieronder worden de maatregelen toegelicht:

S-1: De surveillancecoördinator beschikt over een opleidings- en trainingsplan voor surveillanten.
S-2: Surveillanten beschikken minimaal over basiskennis van de bediening van pc's, laptops, het gebruikte netwerk en de te hanteren inlogprocedures. Zij herkennen ook nieuwe technologieën. Voor het idee: denk bijvoorbeeld eens wat mogelijk zou zijn met zaken als smart watches (slimme horloges), heel kleine USB-sticks en (binnenkort) technologie als Google Glass (en soortgelijke 'brillen' van andere leveranciers).
S-3: Surveillanten zijn globaal op de hoogte van de toe te passen procedures, uitzonderingen en afwijkingen daarbij en incident- en calamiteitenplannen.
S-4: Bij elke toets is in het toetslokaal één hoofdsurveillant aanwezig die exact op de hoogte is van de procedures, uitzonderingen en calamiteitenplannen. Deze is verantwoordelijk voor de correcte toepassing daarvan, notuleert afwijkingen t.b.v. het proces verbaal en is verantwoording verschuldigd aan de surveillancecoördinator, die verantwoording verschuldigd is aan de toetscoördinator.
S-5: De surveillanten controleren tijdens de toetsafname of het (fysieke) ID van de student overeenkomt met de ID die in het toetsprogramma gebruikt wordt en zichtbaar is op het beeldscherm.
S-6: Surveillanten zien toe op een ordelijk verloop van de toets en zijn zich bewust van wat er fout kan gaan, zowel technisch als sociaal. De hoofdsurveillant beschikt over de telefoonnummers van de leden van het crisisteam (in geval van calamiteiten tijdens de toetsafname)

8. De toetsafname

Toelichting

Om te voorkomen dat studenten zelf bepalen op welke (mogelijk vooraf gemanipuleerde) pc ze hun toets gaan afnemen worden enkele maatregelen voorgesteld. Ook de identificatie van studenten door vergelijking van hun papieren ID met het getoonde ID op het beeldscherm valt onder deze paragraaf.

Voor dit onderdeel zijn de volgende risico's onderkend, en worden de genoemde maatregelen voorgesteld:

Risico	**Maatregel**
Meedoen zonder jezelf op te geven	Ta-1: niet opgegeven = niet meedoen
Installeren software teneinde ongeoorloofd samen te werken of te spieken	Ta-2: toets-pc blijft tot het laatste moment onbekend
Student kan zich voor iemand anders uitgeven	Ta-3: aparte inlogcode voor de toets en daarna inloggen met eigen account
Onnodige discussies over bevoegdheden surveillanten	Ta-4: bekendheid met rol surveillanten

Mogelijke maatregelen c.q. aandachtspunten

Afwijkende regels met betrekking tot laatkomers en vroeg-vertrekkers ten opzichte van een papieren toetsafname lijken niet nodig.

Hieronder worden de maatregelen toegelicht:

Ta-1: Studenten die zich niet hebben opgegeven voor de toets worden in principe in het toetslokaal niet toegelaten, tenzij na goedkeuring van de studieadviseur.
Ta-2: Studenten bepalen niet zelf op welke toets-pc zij zullen werken; de werkstations worden willekeurig toegewezen en de student weet zijn PC niet vooraf. Er wordt geverifieerd of de juiste student op de juiste PC zit.
Ta-3: EVENTUEEL: studenten logt met zijn eigen ID in op de toets-pc en krijgt een specifiek wachtwoord per toets.
Ta-4: Studenten zijn op de hoogte van het onderwijs- en examenreglement en accepteren dat surveillanten naar hun ID vragen en op hun beeldscherm kijken. Het foto-ID van de student ligt voor de surveillant zichtbaar op tafel.

9. Inzage toetsresultaten

Toelichting

Het inzagerecht en nabespreking is wel geregeld in de onderwijs- en examenregeling. Het heeft betrekking op de termijn (bijvoorbeeld: tot 30 dagen na het tentamen), de wijze waarop de nabespreking plaatsvindt (individueel dan wel collectief) en de locatie. De laatste twee zaken worden bepaald door de examencommissie of de examinator, een rol die wij op dit moment niet hebben benoemd.

Het digitaal inzien van toetsresultaten zou op zich niet anders moeten dan het inzien van papieren toetsresultaten. Wanneer een toetsresultaat wordt aangepast dan dient herleidbaar te zijn wie welke wijziging heeft aangebracht en waarom. Het loggen van het wijzigingsproces kan in geval van verdenking bewijzen dat onbevoegden daarmee bezig zijn geweest.

De methode van inzage zal sterk afhangen van het gebruikte toetspakket. Het gaat er om dat dit zorgvuldig en integer kan worden uitgevoerd.

Voor dit onderdeel zijn de volgende risico's onderkend, en worden de genoemde maatregelen voorgesteld:

Risico	**Maatregel**
De student kan in een 1-op-1-situatie de docent bedreigen	Inz-1: aanwezigheid lid toetsteam tijdens toetsinzage
Docent wordt gedwongen ter plaatse de resultaten aan te passen	Inz-2: geen wijzigingen ter plaatse kunnen aanbrengen
Docent past zonder toezicht toetsresultaten aan	Inz-3: loggen van door docent aangebrachte wijzigingen

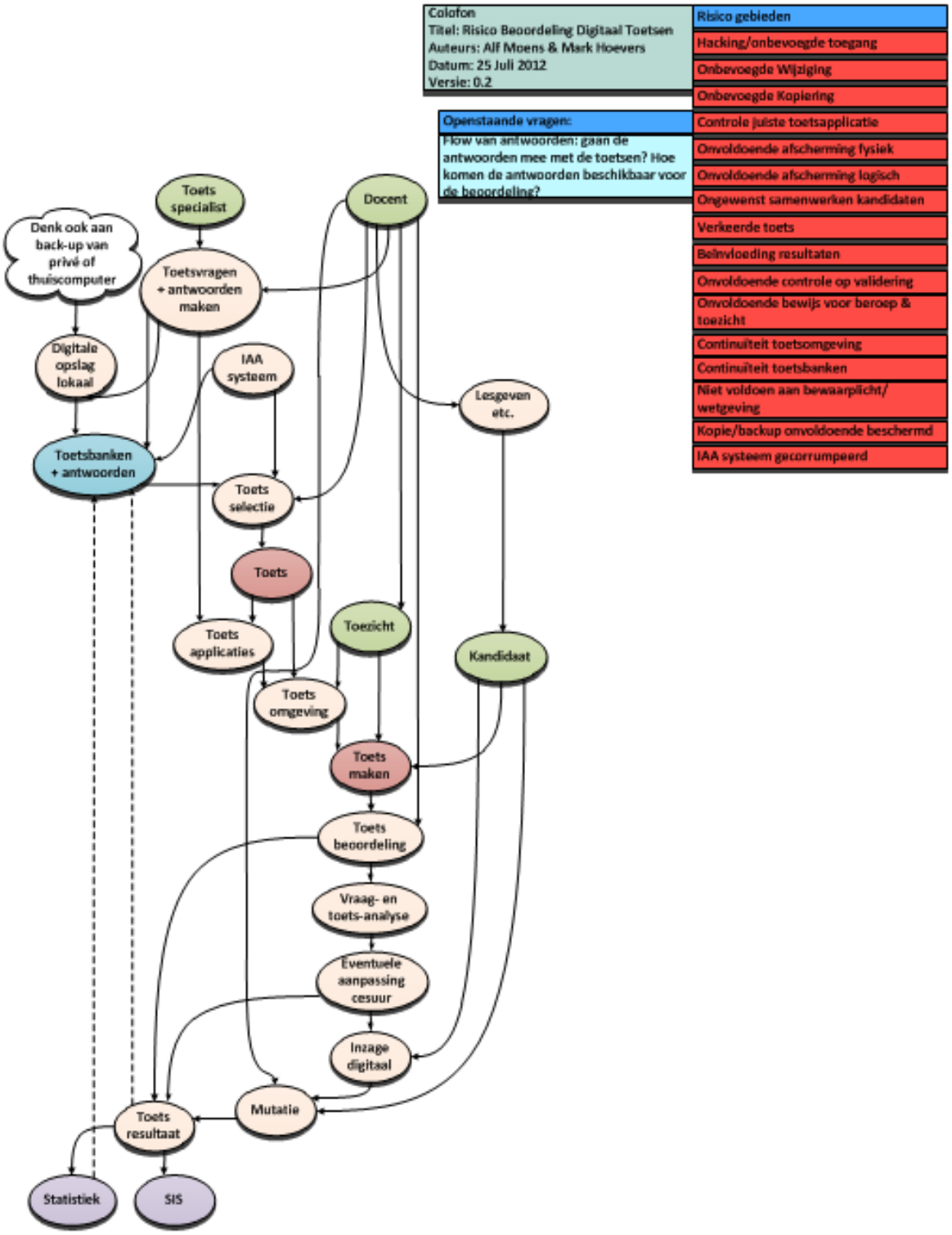
Mogelijke maatregelen c.q. aandachtspunten

De inzage van toetsresultaten is reeds onderdeel van het onderwijs- en examenreglement van de instelling. Voor zover er hieronder nog specifieke maatregelen worden genoemd voor inzage van digitaal afgenomen toetsen, worden zij toegevoegd aan dat reglement.

Hieronder worden de maatregelen toegelicht:

Inz-1: Bij de individuele inzage van een digitaal afgenomen toets zijn aanwezig: de betreffende student, de docent én een lid van het betreffende toetsteam.
Inz-2: Het is niet mogelijk om ter plaatse wijzigingen aan te brengen in de toetsresultaten.
Inz-3: Wanneer na inzage wordt besloten de beoordeling van het toetsresultaat aan te passen, dan dient herleidbaar te zijn dat er iets gewijzigd is en waarom. Het resultaat wordt binnen de in de OER gehanteerde termijn aangepast; dit wordt gelogd en aan het proces verbaal toegevoegd.

Bijlage 1: overzicht van het digitale toetsproces



Bijlage 2: Aandachtspunten voor toetsafname in de cloud

Dit document is tot stand gekomen met inbreng van experts uit enkele instellingen. Die zijn twee maal bijeen gekomen. In de tweede bijeenkomst is besproken welke gevolgen er zijn als delen van het toetsproces met IT in de cloud wordt ondersteund. Dit is opportuun omdat steeds meer leveranciers cloudversies van toetssoftware gaan aanbieden.

Veel van de door de experts genoemde risico's en maatregelen die gaan spelen als voor digitaal toetsen gebruik wordt gemaakt van services uit de cloud zijn generiek voor clouddiensten: denk aan vraagstukken op het gebied van privacy, beveiliging, beschikbaarheid, eigenaarschap, exit-strategie, e.d. Over deze generieke aspecten is inmiddels veel literatuur opgeleverd via het SURF-project '*Privacy en security in de cloud*'. Op http://www.surfsites.nl/cloud/wat-is-cloud/privacy-en-security-in-de-cloud/ treft u tips wanneer u delen van uw toetsproces wil uitvoeren in de cloud.

Naast generieke cloudrisico's, werden nog enkele specifieke zorgen/risico's benoemd voor digitaal toetsen in combinatie met de cloud:

- Risico: tekort aan licenties op toetsmoment.
  Toelichting: hoe bepaal je hoeveel licenties je nodig hebt? Op welke momenten wordt door hoeveel mensen (tegelijkertijd) getoetst? Dit zal afhangen van contracten van leveranciers: hoe bieden ze dit aan, hoe rekenen ze af. Hier moet je dus op letten.
- Risico: performance is onvoldoende op toetsmoment.
  Toelichting: als je vanuit de cloud gaat toetsen, dan moet de cloud op het toetsmoment wel goed performen. Hoe garandeer je dat? Wat als x partijen tegelijkertijd een toets afnemen, heb je dan last van andere gebruikers (capaciteit, afscherming)?
  Capaciteit: lokaal is anders dan internet: waar staat de server? Wanneer is welke bandbreedte nodig?
- Risico: vragensets worden hergebruikt.
  Toelichting: als je instellingsoverstijgend werkt, hoe coördineer je dan dat je voldoende afwisseling en roulatie hebt in je vragen? Zijn normale procedures om te voorkomen dat antwoorden bekend zijn, hier voldoende?
- Risico: versiebeheer niet goed verzorgd.
  Toelichting: bij gedeelde infrastructuur en applicaties moet op elke werkplek wel dezelfde toetsvragen aangeboden worden. Dit houdt in dat er eisen gesteld moeten worden aan het versiebeheer van vragensets (inclusief bijbehorende antwoorden).
- Risico: in de toetsapplicatie is onvoldoende functiescheiding toegepast, waardoor iemand die een toets afneemt op enige manier meer kan dan gewenst.

Bijlage 3: Casusbeschrijvingen

1. Inleiding

Deze beschrijving van enkele praktijksituaties met betrekking tot de afname van digitale toetsen in de sector Hoger Onderwijs en Onderzoek is als zelfstandig document leesbaar naast het Richtsnoer Veilige toetsafname. Omdat er nog geen sprake is van één best practice voor digitale toetsafname is:

a) het richtsnoer, waar het gaat om risico's en maatregelen daartegen, nog wat aan de globale kant, en
b) kan een beschrijving van de verschillende mogelijkheden behulpzaam zijn bij het maken van keuzes in concrete situaties.

Bij het beschrijven van enkele praktijkcases heeft SURF dankbaar gebruik gemaakt van de inventarisatie die in de SIG Digitaal Toetsen is opgesteld door de deelnemende instellingen.

De beschrijving van de praktijkcases is verder tot stand gekomen in een interview met de betreffende instelling.

2. TU Delft

Op 12-12-2012 heeft een interview met Meta Keijzer plaatsgevonden over de situatie met betrekking tot digitaal toetsen.

Digitaal toetsen is in Delft in 2008 als campusbreed **project** opgestart.

Infrastructuur

Er zijn drie aaneengesloten zalen met PC's (3 x 76), een zaal met 70 pc's en een zaal met 250 laptops . Inmiddels zijn er 18 servers, die het digitaal toetsen mogelijk maken. In het begin was loadbalancing nog problematisch, nu gaat dat goed.

Voorbereiding toetszalen

De zalen worden buiten de toetsperiode voor onderwijs gebruikt. Aan het begin van de toetsperiode wordt de specifieke toetssoftware geactiveerd (m.b.v. policies in Windows en PowerFuse). Het instellen van de policies heeft in het begin de nodige aandacht gekregen, omdat er 'lekken' te vinden waren en studenten toch 'naar buiten' konden.

De zaal met laptops moet worden omgebouwd: de laptops en bekabeling worden binnen een halve dag geplaatst. Dit betekent wel dat de digitale toetsen als blok ingeroosterd moeten worden: afwisselend papieren toetsen en digitale toetsen is te bewerkelijk. Tussen de toetsen zijn de zalen gesloten. Aan het einde van de toetsperiode worden de zalen weer vrijgegeven voor onderwijs (studentwerkplek).

Er wordt gewerkt met software van MapleTA en Windows. Voor de keuze voor MapleTA was vooral de functionaliteit doorslaggevend.

Toetsafname en identificatie

Bij binnenkomst nemen de studenten in volgorde van binnenkomst plaats. "Wij hanteren graag het 'pretpark-parkeer-systeem', waardoor de zaal op een systematische manier wordt gevuld. Als er dan een probleem-pc tussen zit, dan weten we dat dat 'gat' niet mag worden opgevuld door een andere student. Doordat vragen gerandomiseerd worden aangeboden is het niet nodig bepaalde lieden verder uit elkaar te zetten."

Studenten die zich niet hebben opgegeven voor een toets worden alleen toegelaten als er voldoende vrije plaatsen zijn. Als een trein vertraging heeft kan het voorkomen dat studenten die zich wel hebben opgegeven niet meer in de zaal kunnen. "We willen graag een experiment doen met toegangscontrole, waarbij alleen de studenten die zich hebben opgegeven na het scannen van hun collegekaart naar binnen mogen."

Op elke tafel ligt een instructiebriefje hoe de studenten dienen in te loggen. Eerst wordt op de computer ingelogd (beveiligde-omgeving) en vervolgens authentiseren ze zich met hun eigen netID, waarmee ze ook op Blackboard inloggen. Het komt voor dat studenten hun netID niet meer weten, omdat hun eigen laptop dat geautomatiseerd onthoudt; dit kan leiden tot oponthoud. Als het NetID niet in orde is moet de toets op papier afgenomen worden.

Vijftien minuten voor aanvang van de toets wordt deze op 'visible' gezet. Op de starttijd van het tentamen komt de link beschikbaar. De timer start zodra de student de 1^{e} vraag ziet.

In de toets staat studienummer en naam in grote letters bovenin het beeldscherm. Collegekaart moet op tafel liggen, zodat de surveillant deze kan vergelijken met het beeldscherm.

Er zijn geen kapstokken of kluisjes in of nabij de toetszalen. Jassen en rugzakken worden op de grond gelegd, wat voor surveillanten gevaarlijk kan zijn.

Surveillanten

"Wij werken met 50 studenten per surveillant. Naast de surveillanten is er ook minimaal één inhoudelijk betrokken persoon aanwezig, die kan assisteren als een opgave niet geheel duidelijk is."

In het begin waren sommige surveillanten onvoldoende computerwijs, waardoor ze studenten die foutief hadden ingelogd niet konden helpen. Inmiddels is een training ontwikkeld voor de surveillantenpool. Zij kunnen nu veel voorkomende vragen oplossen.

De surveillanten worden geworven via een uitzendbureau. Het is niet wenselijk om hiervoor student assistenten in te zetten i.v.m. fraudemogelijkheden.

Wordt er na afloop van elke toets een proces verbaal opgemaakt? "Op dit moment wordt gewerkt met een lijst met meldingen van 'incidenten'; dat moet opgeschaald worden naar een proces verbaal."

Inzage en bespreking van toetsresultaten

Zijn er aanvullende procedures voor het inzien van digitale toetsresultaten t.o.v. het onderwijs- en examen reglement (OER)? "Neen, dit recht is vastgelegd in de OER."

Hoe kan de student zijn toetsresultaten inzien? "De docent bepaalt in systeem wat studenten online kunnen zien. Toets is altijd samen met docent in te zien."

Zijn er naast de docent en de betreffende student nog andere personen aanwezig tijdens de bespreking van de toetsresultaten? "Neen."

Wie brengt eventuele wijzigingen aan in de toetsresultaten en hoe verloopt dat? "De docent kan de toetsresultaten in de betreffende module wijzigen, ook in het bijzijn van de student. Daarna moet de gewijzigde toetsuitslag nog doorgevoerd worden in het systeem waar de studieresultaten worden beheerd."

De meer technische zaken worden in de volgende tabel weergegeven.

Vraag	Antwoord
1. Welk OS wordt er gebruikt in de toetszalen en welke versie?	Windows 7 sp1
1.a Wordt er gebruik gemaakt van virtualisatie?	Neen
1.b Worden meerdere operating systemen ondersteund?	Neen
1.c Wordt gewerkt met vaste PC's, laptops (in eigen beheer, van studenten)?	We hebben 3 aaneengesloten zalen met PC's en 2 zalen met laptops (in eigen beheer)
2. Wordt er gebruik gemaakt van specifieke software om de toetszaal veilig te maken?	Ja
2.a Is dit gekochte software of zelf gebouwd?	Gekocht: PowerFuse en Citrix vormen een speciale beveiligingsschil
2.b Is er een koppeling met de centrale authenticatie database (LDAP / AD)?	Ja
2.c Hoe is dit ontstaan, vanuit organische groep of project?	Project
2.d Wordt de zaal voor het toetsen "schoon" ingericht?	Neen

Vraag	Antwoord
2.e Hoe worden specifieke bronnen uitgesloten of vrijgegeven?	Door het instellen van policies in Windows en de toepassing van PowerFuse.
2.f Kunnen meerdere verschillende toetsen naast elkaar worden gegeven?	Ja
3. Wat voor zaal wordt gebruikt?	
3.a Een specifieke toetszaal of een standaard onderwijs pc zaal?	Standaard
3.b Is deze zaal buiten toetstijden ook te gebruiken voor onderwijs?	Tussen de toetsen is de zaal op slot, na de laatste toets in de toetsperiode is de zaal beschikbaar voor onderwijs / studentwerkplek
3.c Wat voor capaciteit is beschikbaar in de za(a)l(en)?	3 * 76, 1 * 250 en 1 * 70
3.d Zijn er speciale voorzieningen voor controle, toegang en beheer (controleruimte, gescheiden ingang en uitgang)?	Neen
3.e Wordt de zaal ook gebruikt door derde partijen?	(nog) niet
4. Wat voor toetsen worden er afgenomen in de zaal?	
4.a Web gebaseerd? Met welke programma's?	Op dit moment alleen MapleTA en Windows calculator. Op termijn zal dit uitgebreid worden naar andere applicaties. Toetsen waarvoor andere software nodig is, kan ook, maar dan is de beveiliging anders geregeld (onze 'oude' situatie)
4.b Applicatie toetsen (Office, SAS/SPSS etc)?	Studenten hebben dan schrijfrechten op een directory. Werkplekservices verzamelt de bestanden voor de docent en geeft hem daar toegang toe
4.c Externe toetsen, dwz toetsen die commercieel worden betrokken (taaltoetsen, e.d.)?	Neen
4.d Papieren toetsen?	De zaal met capaciteit van 250 is ook een reguliere toets-zaal, maar het is niet zo dat er het ene moment een papieren toets en het andere moment een digitale toets is. De digitale toetsen worden zoveel mogelijk in een blok geroosterd.
4.e Combinaties van bovenstaande mogelijkheden?	Neen
5. Worden er tools gebruikt bij het surveilleren?	
5.a Classroom management (iTalc, NetControl, NetOp, AB Tutor, etc)	Neen
5.b Webcam controle van de afname pc?	Neen
5.c Cameratoezicht in de zaal?	Neen
5.d Maatregelen tegen afkijken	Inkijkhoek is redelijk klein, geen tussenschotten omdat dan het overzicht over de zaal voor de surveillanten slecht is. Husselen van antwoordopties, randomisatie van de tekst, plaatjes en/of getallen. De toets is alleen vanuit de tentamenzaal te maken (afscherming op IP-adres)
6. Problemen, oplossingen en discussiepunten	

Vraag	Antwoord
6.a Welke aspecten van de werkplektechniek ervaar je als meest problematisch?	Inlogprocedure is nog te complex, waardoor studenten regelmatig fouten maken. Updates van software geven soms onverwachte problemen
6.b Over welke aspecten ben je erg tevreden?	De functioneel beheerder kan de zaal van 250 zelf omzetten naar de digitale tentamenmodus
6.c Welke onderwerpen zou je graag bespreken tijdens de SIG DT-bijeenkomst?	Is er een toekomst voor BYOD Er is in Delft geëxperimenteerd met het afnemen van toetsen via een eigen laptop. Dat kon alleen met Windows. Bij een derde van de studenten werkte het niet.

3. Wageningen University

Op 26 februari 2013 is gesproken met Gerard Folkerts over de situatie m.b.t. veilig toetsen bij de WUR.

Digitaal toetsen is in Wageningen organisch gegroeid

Tien jaar terug werd begonnen met QMP, waarbij studenten niet met elkaar konden communiceren. Er werd een speciaal toets-image gemaakt. De universiteit beschikt over veel standaard onderwijs-pc-zalen, die ook gebruikt worden voor toetsafname. Er zijn geen dedicated digitale toetszalen.
Dit heeft 2 redenen:

1. Studenten komen van over de hele wereld (125 nationaliteiten) en hebben vaak geen eigen laptops
2. Alles staat klaar voor de docent; er is geen opstarttijd

Deze situatie blijft voorlopig gehandhaafd.

Zo'n 4 á 5 jaar geleden is voor digitaal toetsen een professionaliseringsslag gemaakt: van QM3 naar een verbeterde infrastructuur. Er werd een speciale dienst ingericht voor digitaal toetsen. Niet alleen de techniek werd geleverd, maar ook de ondersteuning voor de docenten: hoe maak je vragen, hoe zet je die klaar, hoe start je de zaal op, etc. De docent is verantwoordelijk voor zijn eigen toetsen, maar de ondersteuning zet de toets gereed en test eerst of deze naar behoren functioneert. Immers, je hebt een groot probleem als er tijdens de toets iets mis gaat.

Er bestaan drie toetsomgevingen:

1. Ontwikkelomgeving
2. Formatieve toetsomgeving, en
3. Summatieve toetsomgeving

Ondersteuners migreren items uit de ontwikkelomgeving naar de formatieve of summatieve toetsomgeving; niet de docenten.

Voorbereiding toetszalen

Van afstand (centraal) worden de pc's aangezet en afgegrendeld met behulp van 'windows group policies'. Dit neemt zo'n 15 minuten in beslag. Na afloop worden de pc's weer ingericht als standaard onderwijs-pc's.
Er worden geen fysieke controles uitgevoerd naar de aanwezigheid van bijv. key-loggers.

Omdat gewerkt wordt met de standaard onderwijszalen, die al gedimensioneerd zijn, is er geen sprake van capaciteitsproblemen in netwerken en servers tijdens de toetsafname.

Soms zijn de toetszalen helemaal vol en zitten de studenten relatief dicht bij elkaar. Het werken met tussenschotten heeft als nadeel dat het gebruik van een mobiele telefoon dan niet meer te controleren is. Het at random aanbieden van vragen is hiervoor een oplossing, maar niet elke docent heeft voldoende toetsen in de itembank staan om dat te realiseren.

De toetsafname

Er zijn twee typen toetsen:

- Web-based QM (summatieve toetsen)
- Software gebaseerde toetsen om vaardigheid te testen (de 'secure test en – environment' tools hiervan zijn beschikbaar gesteld via SURF)

De docent bepaalt of studenten aan een aan hem toegewezen pc komen te zitten, of dat de zaal o.b.v. volgorde van binnenkomst gevuld wordt.

Op elke werkplek ligt een A4 met een instructie en een te gebruiken account. Dit formulier dient afgetekend te worden en geldt daardoor tevens als aanwezigheidsformulier. Na het inloggen verschijn het ID in beeld en zal de surveillant dit kunnen vergelijken met de studenten-ID die op tafel ligt.
Bij verdenking kan later herleid worden welke student aan welke werkplek heeft gezeten.

Het komt voor dat er meer toets-pc's nodig zijn, dan aanwezig in het pand waar de toetsen altijd worden afgenomen. In zo'n geval kan uitgeweken worden naar een tweede pand.

De docent dient zelf zorg te dragen voor (voldoende) surveillanten. Dat zijn meestal AIO's, onderwijs assistenten en medewerkers van de betreffende leerstoelgroep. Onduidelijk is of er richtlijnen bestaan voor het maximum aantal studenten per surveillant.

Edu-support is aanwezig in de zaal tijdens het opstarten van de pc's, zodat eventuele calamiteiten tijdig verholpen kunnen worden. Ze blijven op afroep in de buurt.
De Edu-support-toets-coördinator checkt of alle stappen in het proces goed doorlopen worden (spreadsheet).
Voor de zekerheid zijn twee reserve accounts per 50 studenten aangemaakt, om incidenten op te kunnen vangen.

De gang van zaken tijdens de toetsafname is de verantwoordelijkheid van de docent. ICT tekent wel aan wat technisch fout ging.
Iemand uit het Edu-support-team is benoemd als incident-coördinator en legt verantwoordelijkheid af aan de examencommissie.
Niet overal zijn lockers aanwezig; soms worden jassen en rugzakken voorin de toetszaal gelegd.

Toetsinzage

Voor toetsinzage bestaan verschillende mogelijkheden:

- Direct na afloop van de toets wordt op de toets-pc feedback gegeven, waarbij reclameren mogelijk is (daarna niet meer)
- De toets wordt klassikaal besproken
- De toets wordt individueel besproken na een verzoek daartoe

De toetsresultaten zelf kunnen niet gewijzigd worden. Wel de spreadsheet die de docent uit het systeem krijgt aangeboden waarop alle toetsresultaten vermeld staan. Dat spreadsheet wordt verwerkt in het SIS. Er zijn geen regels gesteld m.b.t. het door de docent wijzigen van toetsresultaten; ook niet bij individuele inzage.

De meer technische zaken worden in de volgende tabel weergegeven.

Vraag	Antwoord
1. Welk OS wordt er gebruikt in de toetszalen en welke versie?	Windows 7
1.a Wordt er gebruik gemaakt van virtualisatie?	Neen
1.b Worden meerdere operating systemen ondersteund?	Neen
1.c Wordt gewerkt met vaste PC's, laptops (in eigen beheer, van studenten)?	Standaard pc onderwijszalen (eigen beheer)
1.d Hoeveel servers zijn nodig voor een ongestoorde toetsafname?	Er zijn 2 servers voor summatieve toetsen. Alles is redundant uitgevoerd
2. Wordt er gebruik gemaakt van specifieke software om de toetszaal veilig te maken?	Ja/Neen
2.a Is dit gekochte software of zelf gebouwd?	Zelfbouw
2.b Is er een koppeling met de centrale authenticatie database (LDAP / AD)?	Ja

Vraag	Antwoord
2.c Hoe is dit ontstaan, vanuit organische groep of project?	Groei
2.d Wordt de zaal voor het toetsen “schoon” ingericht?	Neen, de PC’s worden 15 minuten van te voren in de tentamenmodus gezet
2.e Hoe worden specifieke bronnen uitgesloten of vrijgegeven?	Door het instellen van policies in Windows
2.f Kunnen meerdere verschillende toetsen naast elkaar worden gegeven?	Ja
3. Wat voor zaal wordt gebruikt?	
3.a Een specifieke toetszaal of een standaard onderwijs pc zaal?	Standaard
3.b Is deze zaal buiten toetstijden ook te gebruiken voor onderwijs?	Ja
3.c Wat voor capaciteit is beschikbaar in de za(a)l(en)?	3 * 60 + overige pc-zalen (25 – 30 plaatsen)
3.d Zijn er speciale voorzieningen voor controle, toegang en beheer (controleruimte, gescheiden ingang en uitgang)?	Neen
3.e Wordt de zaal ook gebruikt door derde partijen?	Neen
3.f Zijn er kluisjes in of buiten de zaal aanwezig, zodat studenten hun jas, rugzak, mobiele telefoon, e.d. veilig kunnen opbergen? Dit kan ook behulpzaam zijn bij het voorkomen van spieken.	Dat verschilt per zaal (soms wel/soms niet).
	Soms worden de jassen en rugzakken voorin de zaal gelegd
4. Wat voor toetsen worden er afgenomen in de zaal?	
4.a Welke software?	QMP + andere software
	Tools: calculator en zoomit
4.b Applicatie toetsen?	De meeste software geïnstalleerd op de pc.
	Ingeleverd via eigen tool.
4.c Externe toetsen, dwz toetsen die commercieel worden betrokken (taaltoetsen, e.d.)?	Neen
4.d Papieren toetsen?	Andere zalen
4.e Combinaties van bovenstaande mogelijkheden?	Soms (uitzonderingen)
5. Worden er tools gebruikt bij het surveilleren?	
5.a Classroom management (iTalc, NetControl, NetOp, AB Tutor, etc)	Neen
5.b Webcam controle van de afname pc?	Neen
5.c Cameratoezicht in de zaal?	Neen
5.d Maatregelen tegen afkijken	Randomiseren, maximale fontgrootte
6. Problemen, oplossingen en discussiepunten	
6.a Welke aspecten van de werkplektechniek ervaar je als meest problematisch?	Veel ondersteuning nodig, zou minder moeten kunnen zijn.
6.b Over welke aspecten ben je erg tevreden?	Veel geautomatiseerd, docenten tevreden.
6.c Welke onderwerpen zou je graag bespreken tijdens de SIG DT-bijeenkomst?	-

4. Saxion

Op 4 maart 2013 is gesproken met Alvin Wullink (functioneel beheerder) over de situatie m.b.t. digitaal toetsen bij de Hogeschool Saxion.

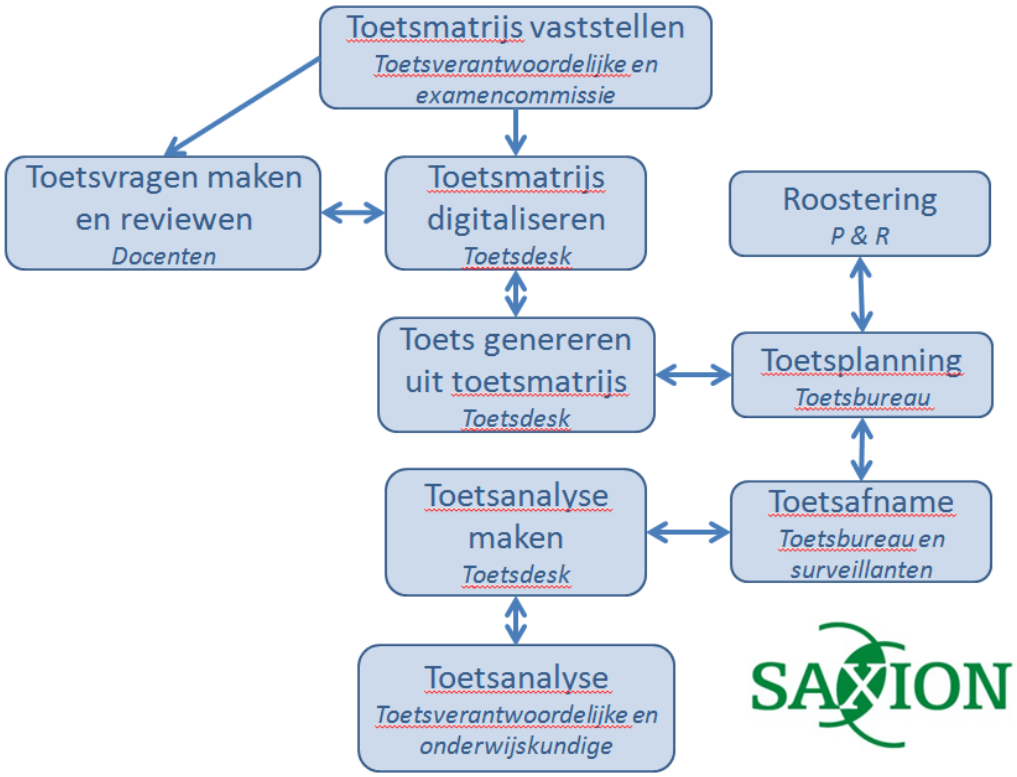
Algemeen

Er wordt sinds zeven jaar gewerkt met Testvision, dus zo lang wordt er al digitaal getoetst. Sinds 2010 is de digitale toetsomgeving bij ICT&Onderwijs in beheer. Het beheerteam bestaat uit 5 mensen. Zij ondersteunen 5 onderwijsapplicaties:

- Blackboard
- TestVision (straks: Surpass)
- Video: opnames, clips, promo's e.d.
- Een websurvey tool, en
- 360° Scorion feedback tool

Governance

De digitale toetsprocedure is beschreven (protocol) en ziet er op hoofdlijnen als volgt uit (pag. 12).



In het protocol zijn de volgende rollen met bijbehorende taken onderscheiden.

Rollen	Taak
Toetsverantwoordelijke	Aanspreekpunt voor validiteit, betrouwbaarheid en acceptatie van de toets: toets-matrijs Toets-analyse en vaststelling resultaten
Docent	Verantwoordelijk voor (deel van) de toets-vragen, review
Examencommissie	Borging van kwaliteit van de toets
Toets-desk	Toets-matrijs digitaliseren en genereren van de toetsen vanuit de toets-matrijs
Roostering en planning	Roostering van toets en locatie
Centraal toets-bureau	Coördinatie van uitvoering van de toetsen en inschrijving van deelnemers
Surveillant	Afname van de toets
Onderwijskundige	Uitleg van de analyse van de toets en toets-vragen
Informatiseringscentrum	Technisch beheer en ondersteuning infrastructuur
Functioneel beheer ICT&O	Beheer en ondersteuning van de applicatie

Toetszalen

Er zijn 2 officiële toetszalen die buiten de toetsperiodes ook voor onderwijs worden ingezet (samen voor 135 personen). Daarnaast zijn er nog 2 andere lokalen met 25 werkplekken elk. Het ultieme doel is om in alle onderwijszalen toetsen te kunnen afnemen. Daarvoor wordt gewerkt aan een *zaalcertificaat*, waarin de vereisten van een toetszaal zijn opgenomen. Denk daarbij aan afmetingen van de werkplekken, afstanden tussen de beeldschermen, wijze van afscherming, garderobe mogelijkheden, e.d.

Voorafgaand aan een toetsperiode wordt gecontroleerd of de techniek op alle toets-pc's goed werkt. De toetszalen worden dusdanig ingepland dat er altijd enkele reserve werkplekken zijn voor het geval een toets-pc het niet doet.
Bij de grote vakken kunnen de toetsvragen at random worden aangeboden; bij de kleinere vakken zijn daarvoor te weinig items.

De toets

Het centraal toetsbureau coördineert de uitvoering van de toetsen en de inschrijving van deelnemers. Als je niet bent ingeschreven mag je de toetszaal niet betreden. Degenen die zich wel hebben ingeschreven dienen zich te identificeren en een intekenlijst voor aanwezigheid af te tekenen. Studenten mogen gaan zitten waar ze willen. Er ligt een schriftelijke instructie op tafel met de te hanteren codes/ wachtwoorden. Na inloggen verschijnt de naam van de student op het beeldscherm; dit kan door de surveillant vergeleken worden met het fysieke ID. Er kan na afloop van een toets niet worden achterhaald welke student achter welke toets-pc heeft gezeten.

Surveillanten

Het centraal toetsbureau is verantwoordelijk voor de werving van surveillanten. Dit gebeurt via een uitzendbureau. Het gaat meestal om gepensioneerde mensen. De surveillanten krijgen een schriftelijke instructie mee en vullen een proces verbaal in wanneer er iets wordt geconstateerd. In geval er iets gebeurt dat ze niet kunnen oplossen bellen ze met het centraal toetsbureau, die instructies geeft of ICT&O belt.
In de toekomst zal er wat meer gelet worden of de surveillanten wel voldoende gekwalificeerd zijn: ICT-vaardigheid, stressbestendigheid, e.d. Op elke 30 studenten wordt één surveillant ingezet.

Toets-inzage

Elke academie verzorgt zijn eigen toetsinzage. Dat kan klassikaal voor meerdere toetsen. IT zet de toetsen dan klaar en de docent bespreekt (eventueel) de antwoorden. Mocht de docent de toetsuitslag

willen aanpassen, dan kan dat niet in de applicatie, maar gebeurt in het spreadsheet dat door de applicatie is vervaardigd. De informatie uit het spreadsheet wordt opgeslagen in het SIS.

Het beheer

De verschillende academies waren in het verleden zelf verantwoordelijk voor het beheer van toetsapplicaties. Nu is dat gecentraliseerd. Omdat er sprake is van veel verschillende toetsomgevingen (Blackboard, CITO, QMP, BOKS en, TestVision) is het beheer ervan complex. Er wordt naar gestreefd om elk van deze applicaties op alle toets-pc's af te kunnen nemen. Daarvoor is de Baseline + opgesteld, met extra eisen aan de toetsafname-pc's.

Op dit moment worden toetsen uitsluitend via het vaste netwerk afgenomen. Het WiFi-netwerk is nog niet toereikend. Derhalve op dit moment nog geen BYOD, maar dat is wel de ambitie.

De meer technische zaken worden in volgende tabel weergegeven.

Vraag	Antwoord
1. Welk OS wordt er gebruikt in de toetszalen en welke versie?	Windows 7 Enterprise 32 bits
1.a Wordt er gebruik gemaakt van virtualisatie?	Neen (wel servers)
1.b Worden meerdere operating systemen ondersteund?	Neen
1.c Wordt gewerkt met vaste PC's, laptops (in eigen beheer, van studenten)?	Vaste pc's
	Laptops voor studenten met beperkingen
2. Wordt er gebruik gemaakt van specifieke software om de toetszaal veilig te maken?	Ja
2.a Is dit gekochte software of zelf gebouwd?	SiteKiosk, is vrij te configureren
2.b Is er een koppeling met de centrale authenticatie database (LDAP / AD)?	Neen
2.c Hoe is dit ontstaan, vanuit organische groep of project?	Groei
2.d Wordt de zaal voor het toetsen "schoon" ingericht?	Met een speciale functietoets kunnen we de werkstations opnieuw voorzien van een schone installatie. Dit kan ook automatisch centraal worden ingegeven
2.e Hoe worden specifieke bronnen uitgesloten of vrijgegeven?	Via SiteKiosk
2.f Kunnen meerdere verschillende toetsen naast elkaar worden gegeven?	Ja binnen de toetsomgeving zijn meerdere toetsen simultaan af te nemen
3. Wat voor zaal wordt gebruikt?	
3.a Een specifieke toetszaal of een standaard onderwijs pc zaal?	Het zijn aparte lokalen die voor toetsdoeleinden zijn ingericht. Echter de werkstations hebben een standaard installatie en kunnen zodoende ook voor les ingezet worden
3.b Is deze zaal buiten toetstijden ook te gebruiken voor onderwijs?	Saxion heeft 2 officiële toetszalen die daarnaast ook voor onderwijs worden ingezet. Er wordt ook wel eens getoetst in zalen die ook voor onderwijs worden gebruikt. Saxion wil in principe in alle computerlokalen kunnen toetsen en daar een certificering voor afgeven
3.c Wat voor capaciteit is beschikbaar in de za(a)l(en)?	De officiële zalen in totaal voor 135 personen. De 2 andere lokalen in totaal 50 personen.

3.d Zijn er speciale voorzieningen voor controle, toegang en beheer (controleruimte, gescheiden ingang en uitgang)?	Ingang en uitgang zijn dezelfde. Controle gebeurt bij de ingang.
3.e Wordt de zaal ook gebruikt door derde partijen?	Neen
3.f Zijn er kluisjes in of buiten de zaal aanwezig, zodat studenten hun jas, rugzak, mobiele telefoon, e.d. veilig kunnen opbergen? Dit kan ook behulpzaam zijn bij het voorkomen van spieken.	In de officiële toetszalen zijn kapstokken voor tassen en jassen
4. Wat voor toetsen worden er afgenomen in de zaal?	
4.a Welke software?	Test Vision en voor de lerarenopleiding ook met CITO en QMP, voor gezondheidszorg met BOKS. De economische opleidingen en de hospitality business school maken gebruik van toetsen waar studenten iets moeten doen in Excel, MSWord of Access
4.b Applicatie toetsen?	Ja dus. Office, SPSS, zelfs de wens tot CadCam.
	Opgaven worden meestal op papier gegeven naast een gedeeltelijk ingevuld office document.
	Voor SPSS worden de vragen gesteld in de toetsapplicatie.
4.c Externe toetsen, dwz toetsen die commercieel worden betrokken (taaltoetsen, e.d.)?	Taaltoetsen van Academie Mens en Maatschappij
4.d Papieren toetsen?	In andere zalen
4.e Combinaties van bovenstaande mogelijkheden?	Neen
5. Worden er tools gebruikt bij het surveilleren?	
5.a Classroom management (iTalc, NetControl, NetOp, AB Tutor, etc)	Neen
5.b Webcam controle van de afname pc?	Neen
5.c Cameratoezicht in de zaal?	Neen
5.d Maatregelen tegen afkijken	Schotten tussen pc's/werkplekken en 1 surveillant per 30 studenten
6. Problemen, oplossingen en discussiepunten	
6.a Welke aspecten van de werkplektechniek ervaar je als meest problematisch?	Te weinig toetsplekken voor digitale afname
6.b Over welke aspecten ben je erg tevreden?	-

6.c Welke onderwerpen zou je graag bespreken tijdens de SIG DT-bijeenkomst?	Naar het idee van Functioneel- en Technisch beheer zijn we als instelling Saxion niet in staat om voor 5 verschillende applicaties (Blackboard, TestVision, CITO, QMP, Boks) organisatorisch en technisch de kwaliteit en veiligheid van het logistieke toetsproces voldoende te waarborgen zonder daar forse extra kosten (met name in termen van menskracht) voor te maken. Bij summatieve toetsen moet die borging wel, want als het summatieve toetsproces niet 100% gewaarborgd wordt, kunnen we in de krant komen. Er zijn 12 academies binnen Saxion. We hebben nu 2 academies, die ook eigen keuzes maken voor de tool waarin summatieve toetsen plaatsvinden, namelijk de APO is verplicht te toetsen in CITO en toetst ook nog in QMP, AGZ toetst ook met BOKS. Dit is een ontwikkeling die o.i. niet haalbaar is. Wij zijn benieuwd hoe andere instellingen hiermee omgaan.