Richtsnoer Veilige digitale toetsafname

Utrecht, mei 2014
Versienummer: 2.0
Kenmerk: 19.735

Inhoudsopgave

Versiebeheer

Versie	Datum	Door	Wijziging
…			
1.0	17-04-2013	Michiel van Geloven	Eerste definitieve versie
1.01	02-05-2013	Michiel van Geloven	Afwerking voor verspreiding
1.02	01-09-2013	Raoul Teeuwen	Diverse redactionele aanpassingen
1.03	19-09-2013	Brenda van der Laan	Publiceerbare versie
1.04	08-10-2013	Raoul Teeuwen	Extra casus (CHE) toegevoegd
1.05	10-01-2014	Brenda van der Laan	Redactionele aanpassingen casussen
2.0	15-05-2014	Raoul Teeuwen / Michiel van Geloven	Aanvulling na uitkomsten ethical hacks / redactionele aanpassingen

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 werken met anderen, binnen of buiten de instelling, aan een set toetsvragen, kan ICT ondersteunend werken.
- Toetsen samenstellen: ICT kan helpen bij het samenstellen van een toets, zodat deze bijvoorbeeld van het juiste moeilijkheidsniveau is, een juiste mix aan onderwerpen bevat of om te bewaken 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 de toets digitaal af te nemen.
- Toetsanalyse: ook voor beoordelen/scoren en/of analyseren kan ICT ondersteunend zijn.

Bij het inzetten van ICT voor toetsen speelt de vraag: 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 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 het bespreken van risico's en maatregelen op het gebied van digitale toets*afname.*
- Doordat 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 ICT 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 ICT-middelen. We nemen in dit richtsnoer aan dat elke instelling de standaard ICT goed beveiligt, en dat er genoeg publicaties beschikbaar zijn waarin standaard maatregelen staan voor die beveiliging. Denk aan goede anti-virusmaatregelen, 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 groot 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 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 summatief 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.

Dit document beperkt zich tot:

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

In dit document zijn de bevindingen van beveiligingstests (ethical hacks) verwerkt die eind 2013 en begin 2014 zijn uitgevoerd op twee digitale toetsomgevingen op vijf instellingen voor hoger onderwijs.

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 (zie bijlage) beschreven waaruit blijkt hoe enkele instellingen toetsen digitaal ondersteunen en welke maatregelen er zijn genomen om dat te beveiligen.

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.

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:

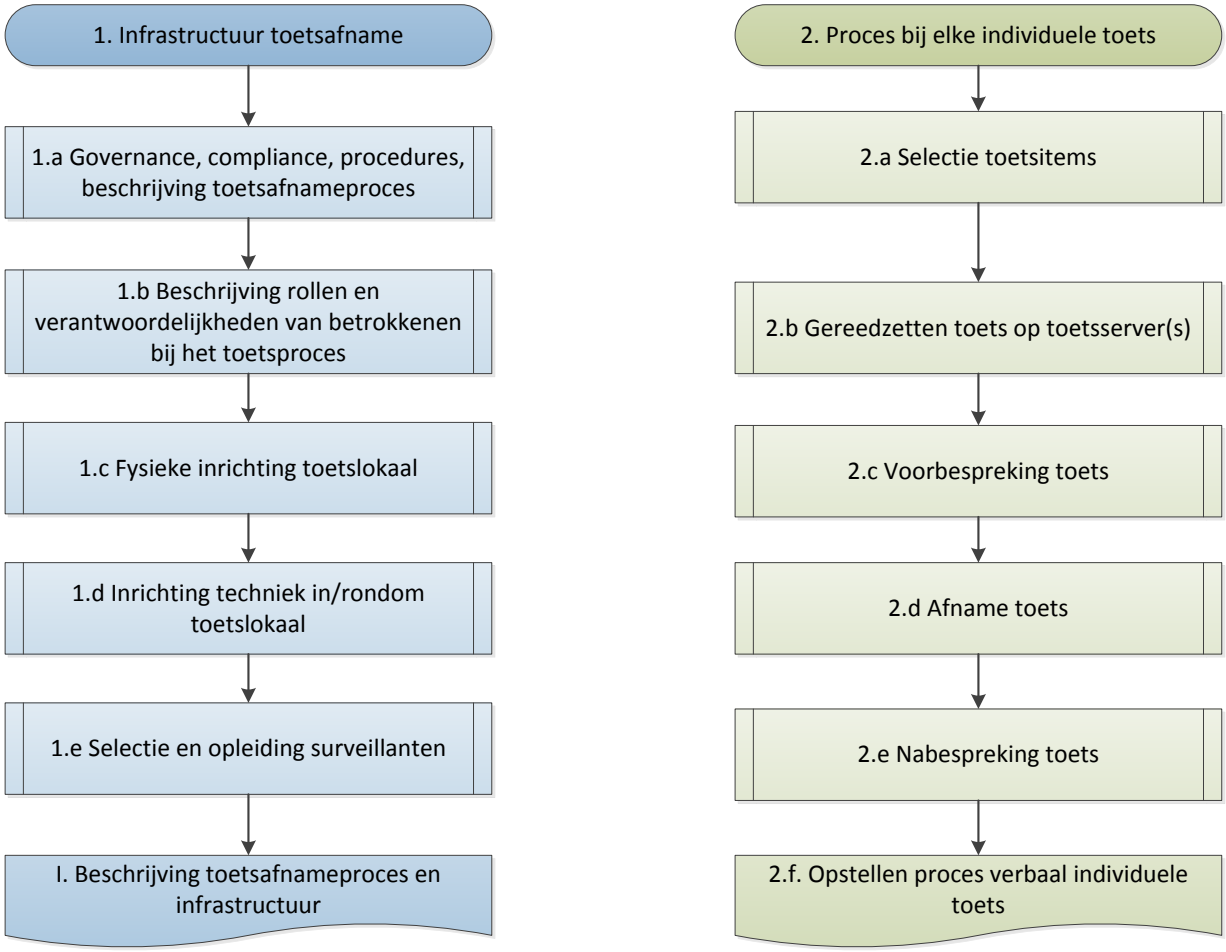
- Het niet kunnen aantonen dat de toets rechtmatig verlopen is.
- Onduidelijkheid over rollen en verantwoordelijkheden, waardoor bijvoorbeeld op ad-hocbasis met incidenten en calamiteiten wordt omgegaan. Met als gevolg dat toetsresultaten verloren kunnen gaan en de instelling imagoschade kan oplopen.
- 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 (1.d), 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-hocbasis 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 zorg je dat er voldoende server- en netwerkcapaciteit is?
- Hoe ga je 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 voor 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

Hierna worden de maatregelen toegelicht:

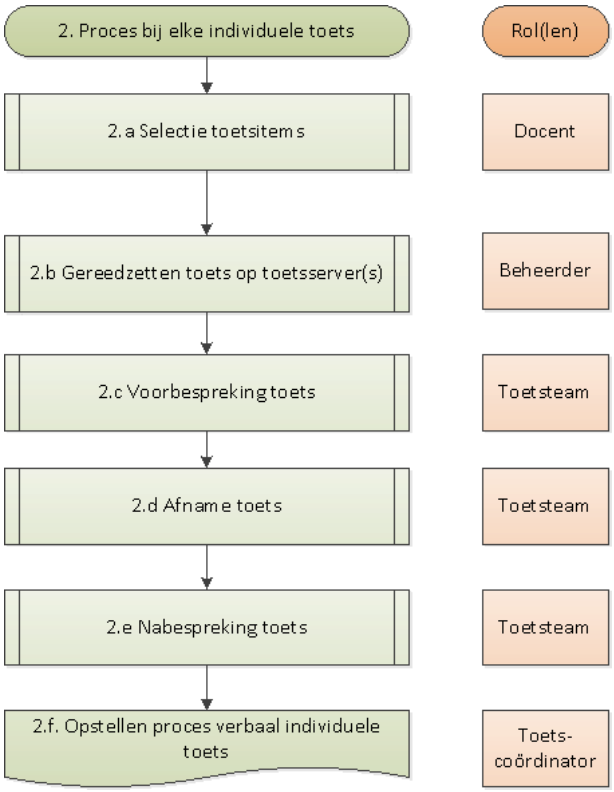
Gc-1: beschrijving procedures
De gewenste gang van zaken bij digitale toetsen wordt beschreven en in procedures vastgelegd (klaarzetten van de toets, sleutelbeheer en uitleen, opleiding/training van surveillanten, omgaan met gestreste of zieke studenten, etc.).

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 toetsteam, 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 en 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 eruit 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 ervoor zorgt dat begin en einde van elke individuele toets gelogd wordt.
- De facilitair medewerker maakt geen onderdeel uit van het toetsteam, omdat hij alleen het sleutelbeheer van het toetslokaal doet.
- De 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.

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 doorgaans gewerkt met een standaard aantal surveillanten: 1 op x studenten. Indien in de voorbespreking duidelijk wordt dat bepaalde studenten extra hulp nodig hebben, bijvoorbeeld wegens 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 eventuele afwijkingen 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 om 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 verschillende 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 te weinig surveillanten aanwezig zijn, dat de surveillanten niet weten hoe de toets-pc moet worden opgestart, etc.	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 over 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) en rapporteert aan de toetscoördinator.
  N.B.: Veel instellingen maken onderscheid 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 of een zaal- of locatiebeheerder. Legt verantwoording af aan de toetscoördinator.
- **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).

[1] Het zal voorkomen dat een instelling andere benamingen gebruikt. Waar het om gaat, is dat alle bijbehorende taken belegd zijn. Verschillende rollen kunnen aan één functie/functionaris worden toegewezen.

5. Techniek

Toelichting

Technische maatregelen vormen naast governance het hart van dit richtsnoer. De techniek van digitale toetsafname moet goed functioneren (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 haar toetsinfrastructuur lokaal draaien, terwijl de andere instelling het uit de cloud afneemt. We benoemen daarom een aantal aandachtspunten en verwijzen graag naar de praktijkvoorbeelden die in de bijlage 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 tijdens de toets	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 toetsservers, voorafgaand aan een toetsafname Stroomuitval, uitval servers	T-8:professioneel beheer van toetsomgeving, waaronder maandelijkse PENtest van servers
Als gevolg van een calamiteit zijn servers niet beschikbaar of gemanipuleerd	T-9: uitwijkplan
Beheerder manipuleert tentamen-pc's	T-10: gelogde activiteiten beheerder beoordelen
Er wordt voorafgaand aan, 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
De toets kan per student meer dan eens gestart worden waardoor een student antwoorden ongewenst kan corrigeren etc.	T-15: aantal malen dat de toets gemaakt kan worden per student beperken tot één

Mogelijke maatregelen en aandachtspunten

Hieronder worden de maatregelen toegelicht:

T-1: De opslag en het transport van toetsvragen en -antwoorden moeten altijd beschermd worden 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 in het toetslokaal) moet het mogelijk maken om af te dwingen dat de toets uitsluitend op het daarvoor bestemde moment en locatie gemaakt kan worden.
  - Tijdsbeperking: de toetsomgeving moet dus zo kort mogelijk open staan. In veel toetsomgevingen kan ingesteld worden in welke periode een toets gemaakt kan worden.
  - Locatiebeperking: dit gaat zover dat studenten de toets niet vanaf apparaten (laptops, pc's etc.) kunnen maken die niet formeel aan de toets mee mogen doen. Mogelijke maatregel daarvoor is ervoor zorgen dat de toetsomgeving alleen vanaf een apart VLAN/aparte IP-range benaderd kan worden.
- De toetsapplicatie is onderzocht op gevoeligheid voor netwerkverstoringen. Op basis daarvan zijn fall-backmechanismen ontworpen, geïnstalleerd en beheerd.

T-3: Bij summatieve toetsen wordt in de voorbespreking bepaald welke sites en/of software toegankelijk mogen zijn en waar studenten gebruik van mogen maken tijdens de toets. De rest wordt geblokkeerd (dit principe heet 'white listing'). Als er meer/minder toegestaan wordt, moet dit 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.

Veel van deze zaken zijn te regelen via zogenaamde 'secure browsers' (andere namen voor dit soort software zijn lockdown-browsers en kiosk-software). De ethical hacks die SURF eind 2013 en begin 2014 liet uitvoeren laten zien dat dit soort browsers, mits correct geconfigureerd, goed kunnen helpen bij het beveiligen van de digitale toetswerkplek. Maar het bleek ook dat dit slechts een deel van de beveiliging is. Bekende voorbeelden zijn SiteKiosk en de Respondus Lock-down browser. Onder meer Question Mark Perception en Surpass hebben een eigen secure browser. Sommige oplossingen, zoals de Secure Test Environment die gratis via SURF beschikbaar is, maken het mogelijk zowel websites als lokale software zoals Excel/SPSS etc te gebruiken.

T-4: In elke toetsapplicatie worden de ID's van studenten opgenomen, zodat de surveillant de fysieke ID's (bijvoorbeeld een studentenkaart) 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 moeten perfect beheerd 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.
- In de toetsperiodes mogen geen updates plaatsvinden en een goede test na elke update is noodzakelijk.
- Antivirusprogramma's (en indien gebruikt mailfiltering) dienen 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 plan voor als de servers onbeschikbaar zijn. Dat kan betekenen dat er snel vervangende servers beschikbaar gemaakt worden. Maar het kan ook betekenen dat wordt teruggevallen op papieren examens of, als dat niet anders kan, het examen later opnieuw afgenomen wordt. Alhoewel de servers belangrijk kunnen zijn, dient voor elk onderdeel van ‘de keten’ nagedacht te worden over wat er moet gebeuren als een onderdeel niet goed werkt.

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, om te kunnen beoordelen of er ongeoorloofd wordt samengewerkt of bestanden worden geraadpleegd.

T-14: De beheerder is verantwoording schuldig over ‘de staat der techniek’ aan de toetscoördinator.

T-15: Er is ingesteld dat elke toets per student maar 1 maal gestart mag worden en elke student maar 1 maal ingelogd mag zijn op de toets. Er zijn procedures die zorgen dat een student opnieuw bij de toets kan als een toetswerkplek bijvoorbeeld crasht waardoor de student opnieuw moet inloggen op de toets.

6. Toetslokaal

Toelichting

Vaak wordt een lokaal met bestaande werkplekken voor studenten tijdelijk ingericht/gebruikt voor een toetsafname. Dan moeten extra maatregelen genomen worden voorafgaand aan de toetsperiode om onbevoegde toegang tot toets-pc's en bijvoorbeeld het plaatsen van 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, moet de toegang tot het lokaal gedurende de toetsperiode gereguleerd te zijn. Hieronder staan enkele voorbeelden van mogelijke maatregelen.

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

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

Mogelijke maatregelen en aandachtspunten

Hieronder worden de maatregelen toegelicht:

TI-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.
TI-2: In een situatie waarin het toegangsbeheer niet adequaat geregeld kan worden, dient gedurende de toetsperiode videobewaking van de toegangsdeur te worden aangebracht.
TI-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-persoonstafels met pc, toetsenbord en muis, of laptop.
- Als de werkplekken erg dicht bij elkaar staan, is aan te raden om 'schotten' te plaatsen.
- Eventueel kan worden gewerkt met 'anti-afkijkfolie', waardoor het beeld alleen te zien is als je recht voor het beeldscherm zit.

TI-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
TI-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
TI-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 bij 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 en 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 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 voor 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 de (fysieke) ID's van de studenten. overeenkomt met de ID's dat in het toetsprogramma gebruikt worden en zichtbaar zijn op de beeldschermen.
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 en 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 of examencommissie.
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: optioneel: Student 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 de nabespreking is 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.

Het digitaal inzien van toetsresultaten zou niet anders moeten zijn dan het inzien van papieren toetsresultaten. Wordt een toetsresultaat aangepast, dan moet herleidbaar 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 hangt sterk af van het gebruikte toetspakket. Het gaat erom 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
De docent wordt onder druk gezet om 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

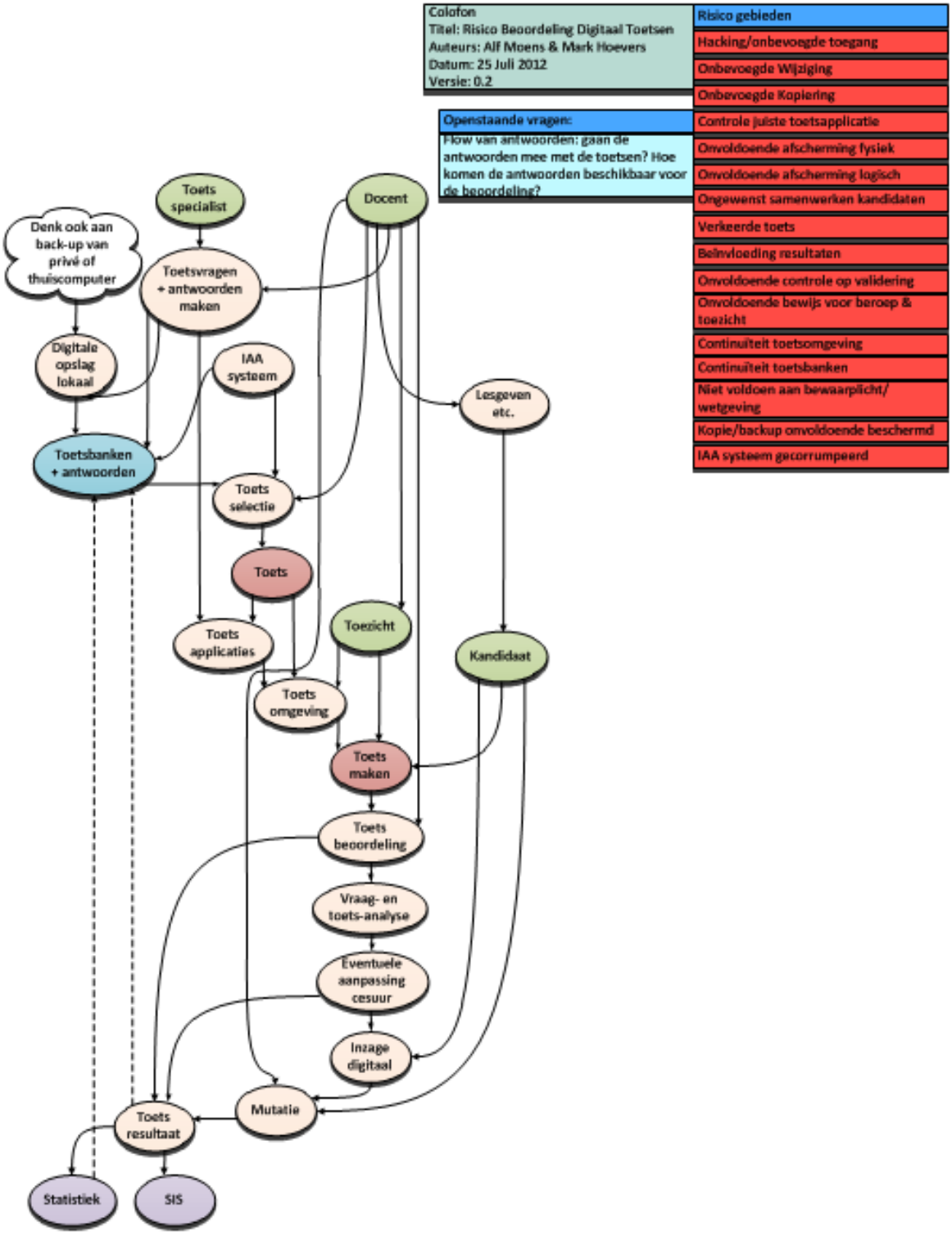
Mogelijke maatregelen en aandachtspunten

De inzage van toetsresultaten is reeds onderdeel van het onderwijs- en examenreglement (OER) van de instelling. Specifieke maatregelen voor inzage van digitaal afgenomen toetsen moeten worden 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: Wordt na inzage besloten de beoordeling van het toetsresultaat aan te passen, dan moet herleidbaar 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 tweemaal bijeengekomen. In de tweede bijeenkomst is besproken welke gevolgen er zijn als delen van het toetsproces met ICT in de cloud wordt ondersteund. Dit is opportuun omdat steeds meer leveranciers cloudversies van toetssoftware aanbieden.

Veel van de door de experts genoemde risico's en maatregelen zijn generiek voor clouddiensten: denk aan vraagstukken op het gebied van privacy, beveiliging, beschikbaarheid, eigenaarschap en exit-strategie. Over deze generieke aspecten is inmiddels veel literatuur opgeleverd via het SURF-project 'Privacy en security in de cloud'. Op de website van SURF vind je bij privacy en security in de cloud tips wanneer je delen van het toetsproces wilt 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?
- Risico: performance is onvoldoende op toetsmoment of de clouddienst is niet bereikbaar.
  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? Is er een alternatieve route mogelijk om de clouddienst te bereiken?
- 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: 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 digitale 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.

Casusbeschrijving: digitale toetsafname bij TU Delft

De TU Delft bouwt onderwijszalen tijdens toetsperiodes om tot toetszalen. "Digitaal toetsen is in Delft in 2008 als campusbreed project opgestart. We gebruiken momenteel Windows 7 en software van MapleTA. Studenten authentiseren zich met hun netID waarmee ze ook inloggen op Blackboard. De surveillanten werven we via een uitzendbureau. Tijdens de toetsafname zijn er per surveillant 50 studenten", vertelt Meta Keijzer, consultant IT in Education.

Toetszalen
TU Delft heeft 3 aaneengesloten zalen met elk 76 pc's en 1 zaal met 250 laptops. Buiten de toetsperiode worden de zalen voor onderwijs gebruikt. De zaal met laptops moet voor het digitaal toetsen worden omgebouwd: het plaatsen van de laptops en de bekabeling neemt een halve dag in beslag. "Dit betekent 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."

Toetssoftware
TU Delft gebruikt de toetssoftware van MapleTA. Voor de keuze voor MapleTA was vooral de functionaliteit doorslaggevend. Aan het begin van de toetsperiode wordt de toetssoftware geactiveerd met behulp van 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." Er zijn 18 servers die het digitaal toetsen mogelijk maken. "In het begin was de loadbalancing nog problematisch, nu gaat dat goed."

Vijftien minuten voor aanvang wordt de toets op 'visible' gezet. Op de starttijd van het tentamen komt de link beschikbaar. De timer start zodra de student de eerste vraag ziet.

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

Studenten die zich niet hebben opgegeven voor een toets worden alleen toegelaten als er voldoende vrije plaatsen zijn. Studenten die te laat zijn, kunnen niet meer in de zaal. "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 waarin staat hoe de studenten moeten inloggen. Eerst loggen ze in op de computer in een beveiligde omgeving. Vervolgens authentiseren ze zich met hun eigen NetID, waarmee ze ook op Blackboard inloggen. In de toets staat het studienummer en de naam van de student in grote letters bovenin het beeldscherm. De collegekaart moet op tafel liggen, zodat de surveillant deze kan vergelijken met het beeldscherm. "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 student de toets op papier maken."

Surveillanten
TU Delft werkt met 50 studenten per surveillant. De surveillanten worden geworven via een uitzendbureau. In verband met fraudemogelijkheden zet de universiteit geen studentassistenten in. 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. Hierdoor konden ze studenten die foutief hadden ingelogd niet helpen. Inmiddels is een training ontwikkeld voor de surveillantenpool. Zij kunnen nu veel voorkomende vragen oplossen. Na afloop van elke toets wordt een lijst met meldingen van 'incidenten' opgesteld. Dat moet opgeschaald worden naar een proces verbaal."

De zalen hebben geen tussenschotten, omdat het overzicht over de zaal voor de surveillanten dan slecht is. “Maatregelen tegen afkijken zijn: het husselen van antwoordopties en randomisatie van de tekst, plaatjes en/of getallen. De toets is alleen vanuit de tentamenzaal te maken. We maken gebruik van afscherming op IP-adres.”

Inzage en bespreking van toetsresultaten
TU Delft heeft geen aanvullende procedures voor het inzien van digitale toetsresultaten naast het onderwijs- en examenreglement (OER). “De docent bepaalt in het toetssysteem wat studenten online kunnen zien. Daarnaast is de toets altijd samen met docent in te zien. Er zijn naast de docent en de student geen andere personen aanwezig tijdens de bespreking van de toetsresultaten. 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 technische aspecten van de digitale toetsafname in een overzicht:

Vraag	Antwoord
1. Welk operating system (OS) wordt er gebruikt in de toetszalen en welke versie?	Windows 7 SP 1
1.a Wordt er gebruik gemaakt van virtualisatie?	Nee
1.b Worden meerdere operating systemen ondersteund?	Nee
1.c Wordt gewerkt met vaste pc’s, laptops (in eigen beheer, van studenten)?	We hebben 3 aaneengesloten zalen met pc’s en 1 zaal 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 authenticatiedatabase (LDAP / AD)?	Ja
2.c Hoe is dit ontstaan, vanuit organische groep of project?	Project
2.d Worden de toets-pc’s/laptops voor het toetsen ‘schoon’ ingericht?	Nee
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 onderwijszaal met pc’s?	Standaard onderwijszaal
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 zalen met 76 pc’s, 1 zaal met 250 laptops en 1 zaal met 70 pc’s
3.d Zijn er speciale voorzieningen voor controle, toegang en beheer (controleruimte, gescheiden ingang en uitgang)?	Nee
3.e Wordt de zaal ook gebruikt door derde partijen?	(Nog) niet
3.f Zijn er kluisjes in of buiten de zaal aanwezig, zodat studenten hun jas, rugzak, mobiele telefoon, e.d. veilig kunnen opbergen?	Geen kapstokken of kluisjes in of nabij toetszalen. Jassen en rugzakken worden op de grond gelegd. Kan gevaarlijk zijn voor surveillanten.

Vraag	Antwoord
4. Wat voor toetsen worden er afgenomen in de zaal?	
4.a Webgebaseerd? 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 (de 'oude' situatie).
4.b Applicatie toetsen (Office, SAS/SPSS etc)?	Studenten hebben schrijfrechten op een directory. Werkplekservices verzamelt de bestanden voor de docent en geeft hem daar toegang toe.
4.c Externe toetsen: toetsen die commercieel worden betrokken (taaltoetsen, e.d.)?	Nee
4.d Papieren toetsen?	De zaal met capaciteit van 250 is ook een reguliere toetszaal. Het is echter 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?	Nee
5. Worden er tools gebruikt bij het surveilleren?	
5.a Classroom management (iTalc, NetControl, NetOp, AB Tutor, etc)	Nee
5.b Webcamcontrole van de afname-pc?	Nee
5.c Cameratoezicht in de zaal?	Nee
5.d Maatregelen tegen afkijken	De inkijkhoek is redelijk klein. Er zijn geen tussenschotten, omdat het overzicht over de zaal voor de surveillanten dan slecht is. Maatregelen zijn: 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	
6.a Welke aspecten van de werkplektechniek ervaar je als meest problematisch?	De 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 met 250 pc's zelf omzetten naar de digitale tentamenmodus.

Het interview met Meta Keijzer vond plaats op 12 december 2012.

Casusbeschrijving: digitale toetsafname bij Wageningen University

Digitaal toetsen is bij Wageningen University organisch gegroeid. De universiteit gebruikt de standaard onderwijszalen met pc's voor digitale toetsafname. "We hebben drie toetsomgevingen: een ontwikkelomgeving en een formatieve en summatieve toetsomgeving. De pc's worden op afstand aangezet en afgegrendeld met Windows group policies. Een speciale dient voor digitaal toetsen zorgt voor de techniek en ondersteuning aan docenten", aldus Gerard Folkerts, ICT-consultant.

Toetszalen
Wageningen University beschikt over veel standaard onderwijszalen met pc's die ook gebruikt worden voor toetsafname. Er zijn geen speciale zalen voor digitaal toetsen. Deze situatie blijft voorlopig gehandhaafd.

Toetsomgevingen
Tien jaar terug begon de universiteit met Question Mark Perception (QMP) waarbij studenten niet met elkaar konden communiceren. Er werd een speciaal 'toets-image' gemaakt. Zo'n 4 tot 5 jaar geleden maakt Wageningen University voor digitaal toetsen een professionaliseringsslag: van QM3 naar een verbeterde infrastructuur. Op dit moment bestaan er drie toetsomgevingen:

1. ontwikkelomgeving
2. formatieve toetsomgeving
3. summatieve toetsomgeving

"We hebben een speciale dienst ingericht voor digitaal toetsen. Niet alleen voor levering van de techniek, maar ook voor 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. Ondersteuners migreren items uit de ontwikkelomgeving naar de formatieve of summatieve toetsomgeving. Zij zetten de toets klaar en testen eerst of alles naar behoren functioneert. Want je hebt een groot probleem als er tijdens de toets iets mis gaat."

Wageningen University maakt gebruik van twee typen toetsen: webbased Question Mark Perception voor summatieve toetsen en softwaregebaseerde toetsen om vaardigheid te testen. De universiteit beveiligt de omgeving met de Secure Test Environment (STE, beschikbaar via SURF).

Voorbereiding toetszalen
Tijdens de voorbereiding van de toetsafname worden de pc's op afstand (centraal) 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. We voeren geen fysieke controles uit naar de aanwezigheid van bijvoorbeeld. key-loggers."

De standaard onderwijszalen zijn gedimensioneerd, dus er is geen sprake van capaciteitsproblemen in netwerken en servers tijdens de toetsafname. "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 kunnen we uitwijken naar een tweede pand."

Toetsafname en identificatie
De docent bepaalt vooraf of de studenten aan toegewezen pc's komen te zitten of dat de zaal gevuld wordt op basis van volgorde van binnenkomst. Op elke werkplek ligt een A4 met een instructie en een te gebruiken account. De student tekent dit formulier en dat geldt daardoor als aanwezigheidsformulier. Na het inloggen verschijn het ID in beeld. De surveillant kan dit vergelijken met de studenten-ID die op tafel ligt. Bij verdenking van fraude kan later herleid worden welke student aan welke werkplek heeft gezeten.

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

Surveillanten en support
De docent moet zorgen voor (voldoende) surveillanten. Dat zijn meestal aio’s, onderwijsassistenten en medewerkers van de leerstoelgroep. Edu-support is aanwezig in de zaal tijdens het opstarten van de pc’s voor het verhelpen van eventuele calamiteiten. Ze blijven op afroep in de buurt. De toetscoördinator van Edu-support checkt of alle stappen in het proces goed doorlopen worden aan de hand van een spreadsheet. Per 50 studenten zijn er twee reserveaccounts om incidenten op te kunnen vangen.

De verantwoordelijkheden van alle betrokken zijn duidelijk afgesproken. “De gang van zaken tijdens de toetsafname is de verantwoordelijkheid van de docent. ICT registreert welke technische aspecten fout gingen. Iemand uit het Edu-supportteam is benoemd als incident-coördinator en legt verantwoordelijkheid af aan de examencommissie.”

Inzage en bespreking van toetsresultaten
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). Ook kan de toets klassikaal worden besproken. Na een verzoek van een student kan de docent de toets ook individueel met de student bespreken.

De toetsresultaten in het systeem zelf kunnen niet gewijzigd worden. Wel kan de docent de spreadsheet met alle toetsresultaten die hij uit het systeem krijgt aanpassen. Die gegevens worden verwerkt in het studentinformatiesysteem. Wageningen University heeft geen regels gesteld voor docenten rondom het wijzigen van toetsresultaten, ook niet bij individuele inzage.

De technische aspecten van de digitale toetsafname in een overzicht:

Vraag	Antwoord
1. Welk operating system (OS) wordt er gebruikt in de toetszalen en welke versie?	Windows 7
1.a Wordt er gebruik gemaakt van virtualisatie?	Nee
1.b Worden meerdere operating systemen ondersteund?	Nee
1.c Wordt er gewerkt met vaste pc’s, laptops (in eigen beheer, van studenten)?	Standaard onderwijszalen met pc’s (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 authenticatiedatabase (LDAP / AD)?	Ja
2.c Hoe is dit ontstaan, vanuit organische groep of project?	Groei
2.d Worden de toets-pc’s/laptops 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?	

Vraag	Antwoord
3.a Een specifieke toetszaal of een standaard onderwijszaal met pc's?	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 zalen met 60 pc's + 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?	Dat verschilt per zaal. 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: 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 Webcamcontrole 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.

Het interview met Gerard Folkerts vond plaats op 26 februari 2013.

Casusbeschrijving: digitale toetsafname bij Saxion

Saxion heeft twee officiële toetszalen die buiten de toetsperiodes voor onderwijs worden ingezet. Ook gebruikt de hogeschool onderwijszalen met pc's voor digitale toetsen. "We werken met veel verschillende toetssoftware: Testvision, CITO, Question Mark Perception (QMP), Body of Skills and Knowledge (BoKS) en MS Office. Het beheer is gecentraliseerd en de digitale toetsprocedure is beschreven in een protocol met rollen en taken", vertelt functioneel beheerder Alvin Wullink.

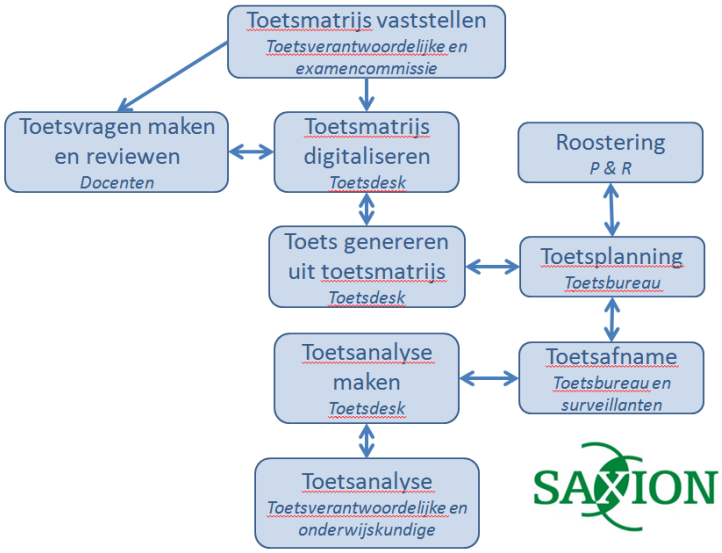
Toetszalen
Saxion heeft twee 2 officiële toetszalen die buiten de toetsperiodes ook voor onderwijs worden ingezet. Samen bieden deze zalen ruimte aan 135 personen. Daarnaast zijn er twee andere lokalen met elk 25 werkplekken waar ook wel eens getoetst wordt. "Ons ultieme doel is om in alle computerzalen te kunnen toetsen. Daarvoor werken we 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 etc."

Op dit moment neemt Saxion alle toetsen uitsluitend af via het vaste netwerk van de hogeschool. Het wifi-netwerk is nog niet toereikend. "Daarom werken wen op dit moment nog niet volgens BYOD (bring your own device), maar hebben wel die ambitie."

Toetssoftware
De hogeschool werkt sinds 2006 jaar met Testvision, dus er wordt al zeven jaar digitaal getoetst. Voor de lerarenopleiding werkt Saxion ook met CITO en Question Mark Perception (QMP) en voor de gezondheidszorg met Body of Skills and Knowledge (BoKS). De economische opleidingen en de hospitality business school maken gebruik van toetsen waar studenten moeten werken in Excel, MSWord of Access.

De verschillende academies waren in het verleden zelf verantwoordelijk voor het beheer van toetsapplicaties. Nu is dat gecentraliseerd. Het beheer ligt bij ICT&Onderwijs. De vele verschillende toetsomgevingen maakt het beheer complex. "We streven ernaar om alle applicaties op alle toets-pc's af te kunnen nemen."

Governance
De digitale toetsprocedure is beschreven in een protocol en ziet er op hoofdlijnen als volgt uit:



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

Rollen	Taak
Toetsverantwoordelijke	• Aanspreekpunt voor validiteit, betrouwbaarheid en acceptatie van de toets: toetsmatrijs • Toetsanalyse en vaststelling resultaten
Docent	• Verantwoordelijk voor (deel van) de toetsvragen en review
Examencommissie	• Borgen van kwaliteit van de toets
Toetsdesk	• Toetsmatrijs digitaliseren en genereren van de toetsen vanuit de toetsmatrijs
Roostering en planning	• Roosteren van toets en locatie
Centraal toetsbureau	• Coördinatie van uitvoering van de toetsen en inschrijving van deelnemers
Surveillant	• Afname van de toets
Onderwijskundige	• Uitleg van de analyse van de toets en toetsvragen
Informatiseringscentrum	• Technisch beheer en ondersteuning infrastructuur
Functioneel beheer ICT&O	• Beheer en ondersteuning van de applicatie

Voorbereiding toetszalen
Het centraal toetsbureau coördineert de uitvoering van de toetsen en de inschrijving van deelnemers. 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 reservewerkplekken zijn voor het geval een toets-pc het niet doet.

Toetsafname en identificatie
Studenten die zich hebben ingeschreven, moeten zich identificeren en een aanwezigheidslijst tekenen. Zonder inschrijving mogen studenten de toetszaal niet betreden. "De studenten mogen gaan zitten waar ze willen. Er ligt een schriftelijke instructie op tafel met de te hanteren codes en wachtwoorden. Na inloggen verschijnt de naam van de student op het beeldscherm. De surveillant kan dit vergelijken met het fysieke ID. Na afloop van een toets kunnen we niet achterhalen welke student achter welke toets-pc heeft gezeten."

Bij de grote vakken kunnen opleidingen van Saxion de toetsvragen at random aanbieden. Bij de kleinere vakken zijn daarvoor te weinig items. Als andere maatregel tegen afkijken heeft Saxion schotten tussen de pc's en werkplekken en 1 surveillant per 30 studenten.

Surveillanten
Het centraal toetsbureau is verantwoordelijk voor de werving van surveillanten. Dit gebeurt via een uitzendbureau. Het gaat meestal om gepensioneerde mensen. Op elke dertig studenten wordt één surveillant ingezet. De surveillanten krijgen een schriftelijke instructie mee en vullen een proces verbaal in wanneer ze iets constateren. "Als er iets gebeurt dat ze niet kunnen oplossen, bellen ze met het centraal toetsbureau. Het bureau geeft dan instructies of belt ICT&O. In de toekomst zullen we meer opletten of de surveillanten voldoende gekwalificeerd zijn qua ICT-vaardigheid, stressbestendigheid, etc."

Inzage en bespreking van toetsresultaten
Elke academie van Saxion verzorgt haar 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. Dat kan in de spreadsheet die door de applicatie is vervaardigd. De informatie uit het spreadsheet wordt opgeslagen in het studentinformatiesysteem."

De technische aspecten van de digitale toetsafname in een overzicht:

Vraag	Antwoord
1. Welk operating system (OS) wordt er gebruikt in de toetszalen en welke versie?	Windows 7 Enterprise 32 bits
1.a Wordt er gebruik gemaakt van virtualisatie?	Nee (wel servers)
1.b Worden meerdere operating systemen ondersteund?	Nee
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 authenticatiedatabase (LDAP / AD)?	Nee
2.c Hoe is dit ontstaan, vanuit organische groep of project?	Groei
2.d Worden de toets-pc's/laptops 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 onderwijszaal met pc's?	Aparte lokalen die voor toetsdoeleinden zijn ingericht. 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.
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?	Nee
3.f Zijn er kluisjes in of buiten de zaal aanwezig, zodat studenten hun jas, rugzak, mobiele telefoon, e.d. veilig kunnen opbergen?	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, CITO, QMP, BoKS, Excel, MSWord, Access
4.b Applicatie toetsen?	Ja. 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: 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?	Nee
5. Worden er tools gebruikt bij het surveilleren?	
5.a Classroom management (iTalc, NetControl, NetOp, AB Tutor, etc)	Nee
5.b Webcamcontrole van de afname-pc?	Nee
5.c Cameratoezicht in de zaal?	Nee
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. Het waarborgen van de kwaliteit en veiligheid van het logistieke toetsproces voor 5 verschillende applicaties zonder forse extra kosten. Academies die ook eigen keuzes maken voor de tool waarin summatieve toetsen plaatsvinden.
6.b Over welke aspecten ben je erg tevreden?	-

Het interview met Alvin Wullink vond plaats op 4 maart 2013.

Casusbeschrijving: digitale toetsafname bij Christelijke Hogeschool Ede

Digitaal toetsen is bij de Christelijke Hogeschool Ede (CHE) in 2004 als hogeschoolbreed project opgestart. De CHE heeft momenteel vijf onderwijszalen met pc's voor toetsafname. "We gebruiken voornamelijk Question Mark Perception (QMP) en hebben drie toetsomgevingen: een ontwikkelomgeving, een formatieve omgeving en een summatieve omgeving. Fraude proberen we te voorkomen door surveillantentrainingen, anti-spiekschermen en randomisatie van vragen", aldus Jan Bootsman (ICT) en Ilse Zwering (Toetsbureau).

Toetsinfrastructuur
De CHE heeft vijf computerlokalen met verschillende aantallen pc's (van 12 tot 37 pc's). De lokalen zijn standaard onderwijszalen/studentwerkplekken. "We plannen altijd maximaal 110 studenten per digitaal moment. We bouwen een marge in van 10%. Zo zorgen we er bijvoorbeeld voor een student bij incidenten kan uitwijken naar een andere computer. Er is één server die het digitaal toetsen mogelijk maakt. Een tweede server verzorgt de toegang voor de proeftoetsen."

Toetssoftware
Het Toetsbureau werkt met drie verschillende omgevingen binnen Question Mark Perception (QMP): de ontwikkelomgeving, de formatieve omgeving en de summatieve omgeving. "Tot voor kort had alleen het Toetsbureau toegang tot deze omgevingen, maar sinds schooljaar 2013-2014 is een aantal docenten verantwoordelijk voor hun eigen vragen. Zij hebben toegang tot de ontwikkelomgeving. Het creëren van de toetsen en de toegang tot de summatieve omgeving blijft in beheer van het Toetsbureau." Ook neemt CHE toetsen of met toetssoftware van Cito.

Voorbereiding toetslokalen
De toetsen worden uiterlijk twee werkdagen voor aanvang van de toets in de planning van QMP gezet. Daarna controleert het Toetsbureau of alles goed is ingevoerd. Op de starttijd van het tentamen komt de link naar de toets beschikbaar.

Toetsafname en identificatie
De regel is dat studenten (ruim) 5 minuten voor aanvang van de toets in het lokaal aanwezig moeten zijn. Na de starttijd van de toets mag een student niet meer deelnemen aan de toets. Student worden alleen toegelaten met een geldig legitimatiebewijs en een CHE-schoolpas/bewijs van inschrijving. Heeft de student deze pasjes niet bij zich, dan hij door de surveillant naar het Toetsbureau gestuurd voor een briefje vervanging van de pasjes.

In de toets staat het studentnummer van de student bovenin het beeldscherm. Het legitimatiebewijs en de CHE-schoolpas moeten op de hoek van de tafel liggen, zodat de surveillant deze kan vergelijken met het studentnummer op het beeldscherm. De studenten moeten altijd de presentielijst tekenen, de surveillant gaat met deze lijst rond.

Op de starttijd van de toets maakt de surveillant het speciaal voor de toets aangemaakt account bekend en kunnen de studenten inloggen op de computer. "Vervolgens loggen ze met hun eigen studentenaccount in op QMP. De studenten krijgen dan een introductiepagina te zien waarin de knoppen van de toets worden uitgelegd en de toets start op."

Beveiliging
Het Toetsbureau van de CHE probeert fraude zoveel mogelijk te voorkomen. "Zo zijn er getrainde surveillanten die ongeveer een jaar geleden een training hebben gehad over fraude. We hebben toen zoveel mogelijk verschillende manieren van frauderen met ze doorgenomen. Daarnaast staat op ieder computerscherm een anti-spiekscherm dat ervoor zorgt dat studenten niet bij elkaar op het scherm kunnen kijken vanaf de zijkant. Mocht het lokaal niet helemaal vol zitten, dan zorgt de surveillant ervoor dat de studenten zoveel mogelijk verspreid door het lokaal zitten."

De toets is alleen vanuit de computerlokalen te maken. De vragen zijn gerandomiseerd, zodat studenten nooit dezelfde vragen op het scherm krijgen. Ook staat QM Secure op alle computers geïnstalleerd. Dat programma voor zorgt dat alleen de toets opgestart kan worden, maar bijvoorbeeld geen Word, Excel, Outlook en Explorer.

Surveillanten
Het Toetsbureau regelt de surveillance voor de toetsmomenten. Er zijn nu ongeveer 29 surveillanten werkzaam bij de CHE, dit zijn veelal gepensioneerden. De surveillanten worden geworven door het Toetsbureau. De betalingen lopen wel via een uitzendbureau. “De surveillanten hebben trainingen gehad over fraude en over digitaal toetsen. Nu houden wij hen op de hoogte via een enquête (ook in de digitale omgeving) en nieuwsbrief die twee keer in het jaar uitgegeven wordt. Daarnaast staat er het hele jaar een oefentoets voor ze klaar waarmee ze kunnen oefenen.”

Mocht er toch iets fout gaan in het lokaal, dan nemen de surveillanten via de telefoon contact op met het Toetsbureau. “Een medewerker van het Toetsbureau komt dan naar het lokaal om te assisteren, maar over het algemeen gaat het erg goed en weten de surveillanten wat ze moeten doen om veel voorkomende problemen te verhelpen. Aan het eind van de toets vullen zij een protocol in over hoe het toetsmoment is verlopen. Hierop kunnen zij ook incidenten melden. Deze worden vervolgens opgenomen in het klachtenoverzicht en meegenomen naar de Academie of andere betreffende diensten.”

Inzage en bespreking van toetsresultaten
Studenten kunnen direct aan het einde van de toets de fout beantwoorde vragen bekijken. Sommige docenten hebben feedback gekoppeld aan foutieve antwoordmogelijkheden. Bij een enkele opleiding wordt deze feedback via de mail naar studenten gestuurd. Na afloop van de toets worden de resultaten uitgelezen door het Toetsbureau en verstuurd naar de academies. “De docent vraagt een coachingreport op bij het Toetsbureau en gaat altijd samen met de student of klas de toets inzien. Het coachingreport moet na inzage ingenomen en vernietigd worden. Afhankelijk van de afspraken bij de academie zelf kunnen studenten zich inschrijven op een klassikaal of individueel inzagemoment of dit aanvragen bij de betreffende docent.”

De technische aspecten van de digitale toetsafname in een overzicht:

Vraag	Antwoord
1. Welk OS wordt er gebruikt in de toetszalen en welke versie?	Windows 7 SP 1
1.a Wordt er gebruik gemaakt van virtualisatie?	Nee
1.b Worden meerdere operating systemen ondersteund?	Nee
1.c Wordt gewerkt met vaste pc’s, laptops (in eigen beheer, van studenten)?	We hebben 5 computerlokalen met pc’s, deze zijn in eigen beheer. Laptop wordt soms ingezet voor een student met een beperking.
2. Wordt er gebruik gemaakt van specifieke software om de toetszaal veilig te maken?	Nee
2.a Is dit gekochte software of zelf gebouwd?	N.v.t.
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 Worden de toets-pc’s/laptops voor het toetsen ‘schoon’ ingericht?	Nee
2.e Hoe worden specifieke bronnen uitgesloten of vrijgegeven?	Door het instellen van policies in Windows m.b.v. SCCM.
2.f Kunnen meerdere verschillende toetsen naast elkaar worden gegeven?	Ja

Vraag	Antwoord
3. Wat voor zaal wordt gebruikt?	
3.a Een specifieke toetszaal of een standaard onderwijszaal met pc's?	Standaard
3.b Is deze zaal buiten toetstijden ook te gebruiken voor onderwijs?	Ja, de zaal is beschikbaar voor onderwijs / studentwerkplek. Soms is het lokaal tussen toetsen door gesloten i.v.m. de anti-spiekschermen.
3.c Wat voor capaciteit is beschikbaar in de za(a)l(en)?	Lokaal 1.078 met 33 pc's, lokaal 1.082 met 37 pc's, lokaal 1.084 met 33 pc's, lokaal 1.093 met 12 pc's en lokaal 1.097 met 13 pc's.
3.d Zijn er speciale voorzieningen voor controle, toegang en beheer (controleruimte, gescheiden ingang en uitgang)?	Nee
3.e Wordt de zaal ook gebruikt door derde partijen?	Ja
3.f Zijn er kluisjes in of buiten de zaal aanwezig, zodat studenten hun jas, rugzak, mobiele telefoon, e.d. veilig kunnen opbergen?	Op de begaande grond is een garderobe en zijn er kluisjes die studenten kunnen huren. Tijdens een toetsmoment worden de jassen en tassen voorin het lokaal op de grond gelegd.
4. Wat voor toetsen worden er afgenomen in de zaal?	
4.a Web gebaseerd? Met welke programma's?	QMP en Cito
4.b Applicatie toetsen (Office, SAS/SPSS etc)?	Nee
4.c Externe toetsen: toetsen die commercieel worden betrokken (taaltoetsen, e.d.)?	Nee
4.d Papieren toetsen?	Nee, deze worden in andere lokalen afgenomen.
4.e Combinaties van bovenstaande mogelijkheden?	Soms, maar dit betreft dan een uitzondering.
5. Worden er tools gebruikt bij het surveilleren?	
5.a Classroom management (iTalc, NetControl, NetOp, AB Tutor, etc)	Nee
5.b Webcamcontrole van de afname-pc?	Nee
5.c Cameratoezicht in de zaal?	Nee
5.d Maatregelen tegen afkijken	Husselen van antwoordopties, randomisatie van de tekst, plaatjes en/of getallen. De toets is alleen vanuit de computerlokalen te maken. Anti-spiekschermen geplaatst op de computerschermen.
6. Problemen, oplossingen en discussiepunten	
6.a Welke aspecten van de werkplektechniek ervaar je als meest problematisch?	Te weinig computerwerkplekken voor de digitale afname.
6.b Over welke aspecten ben je erg tevreden?	Gaat over het algemeen erg goed, weinig grote problemen.

Jan Bootsman (ICT) en Ilse Zwering (Toetsbureau) hebben de situatie beschreven op 23 september 2013.