Aanpak informatie- en kennisveiligheidincidenten

Informatietechnologie en facilitaire zaken

Open Universiteit

document	
identificatie	Aanpak informatie en kennisveiligheidincidenten v11.docx
status	Definitief
auteur(s)	[illegible] (ITF), [illegible] (ITF), [illegible] (AZ), [illegible] (AZ)
datum afdruk	16 januari 2023
opgeslagen	\\srv-hrl-03v\homedir$\MR1\Mijn Documenten_OU Bestanden\Security\Beleidsdocumenten\CyberIncident\Aanpak informatie en kennisveiligheidincidenten v11.docx

1 Inleiding

Dit document levert een bijdrage aan het vermogen van de Open Universiteit (OU) om in crisissituaties adequaat te handelen en daarmee de negatieve gevolgen voor studenten, medewerkers, de organisatie en de maatschappij te beperken. Voor fysieke incidenten beschikt de OU daartoe over het BHV crisisplan. Aanvullend daarop beschrijft dit document de aanpak bij informatie- en kennisveiligheidsincidenten. Daaronder verstaan wij incidenten die de beschikbaarheid, de integriteit of de vertrouwelijkheid van de bedrijfsinformatie van de OU in gevaar brengen.

Dit document beschrijft alleen de aanpak en de organisatie voor het beheersen en oplossen van informatie- en kennisveiligheidsincidenten. De maatregelen die de OU heeft getroffen voor bewustwording en preventie zijn elders beschreven. De operationele procedures en werkinstructies voor het uitvoeren van herstelmaatregelen in de ICT-infrastructuur zijn opgesteld en worden beheerd door de afdeling Operations (ITF-O).

2 Escalatie

Incidenten van allerlei aard worden op de OU gemeld bij de Servicedesk (servicedesk@ou.nl, t 045-576 2306) waar problemen meteen worden opgelost of belegd bij een specialist. Als de Servicedesk constateert dat een melding consequenties kan hebben voor onze informatieveiligheid dan informeren zij CERT OU via een e-mail aan CERT@OU.NL en (indien een incident urgent is) telefonisch aan het Hoofd Operations of de Chief Information Security Officer (CISO) op basis van eerste bereikbaarheid
Het Computer Emergency Response Team (CERT OU) is een virtueel team van technisch en juridisch specialisten dat in actie komt bij informatie- en kennisveiligheidsincident. Het CERT OU wordt gecoördineerd door de CISO.
CERT OU ontvangt niet alleen incidentmeldingen van onze eigen Servicedesk maar ook van partijen buiten de OU zoals van SURFcert en van individuen of organisaties die van mening zijn dat de systemen van de OU één of meerdere kwetsbaarheden bevatten.

bezoekadres: Valkenburgerweg 177 Heerlen
postadres: Postbus 2960 6401 DL Heerlen
T 045 - 576 22 22

Open Universiteit

Als handreiking voor het besluit of een informatieveiligheidsincident wordt behandeld als een informatieveiligheidscrisis gebruiken we:

Als de gevolgen van een incident of de gevolgen van de maatregelen die worden getroffen om het incident te beheersen, onze kritische:
- bedrijfsprocessen (inschrijving, tentaminering, onderwijs geven);
- bedrijfsgegevens (persoonsgegevens, onderzoeksdata, financiële gegevens);
- centrale ict-infrastructuur en netwerkverbindingen;

bedreigen, dan wordt het incident behandeld als een informatieveiligheidscrisis.

Zolang een informatieveiligheidsincident (nog) niet als een informatieveiligheidscrisis wordt behandeld, wordt het onder aansturing van CERT OU volgens de normale procedure afgehandeld. CERT OU administreert die meldingen en coördineert en bewaakt de afhandeling daarvan. In het algemeen worden de concrete maatregelen om (de gevolgen van) incidenten op te lossen aangestuurd met changes en uitgevoerd door medewerkers van ITF-O.

Zodra het CERT-lid dat een incident behandelt van mening is dat het betreffende informatieveiligheidsincident cf. bovenstaande handreiking een informatieveiligheidscrisis vormt, roept deze onmiddellijk de beschikbare CERT OU leden bijeen en overlegt met hen. Wanneer het een kennisveiligheidsincident betreft wordt ook de coördinator kennisveiligheid ingelicht. Waar nodig zal overlegd worden met het kennisveiligheidsteam.

Als CERT OU een informatieveiligheidscrisis vermoedt, adviseren zij de directeur ITF of diens vervanger om het Crisis Management Team Informatieveiligheid (CMTI) bijeen te roepen.

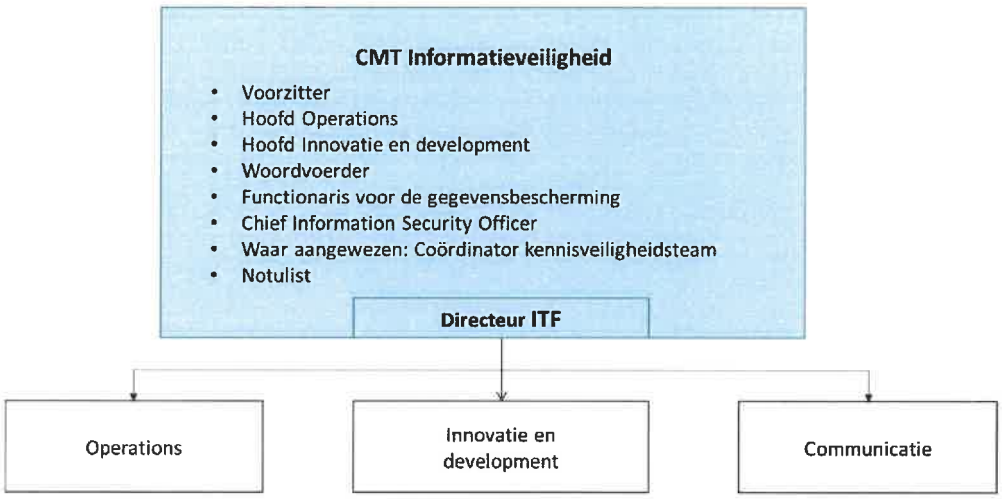
Bij de beoordeling of een informatieveiligheidscrisis wordt opgeschaald naar het College van bestuur neemt de directeur ITF de volgende criteria in aanmerking:

1. Is de persoonlijke of algemene (digitale) veiligheid van medewerkers en/of studenten (zoals bij afpersing) in gevaar?
2. Breidt het (dreigende) incident of de calamiteit zich ondanks de inzet van (universiteits)medewerkers en/of (hulp)diensten verder uit?
3. Is de (acute) inzet van externe hulpverlenende diensten of personen noodzakelijk of wenselijk?
4. Is de continuïteit van één of meerdere bedrijfsprocessen binnen de universiteit in gevaar?
5. Heeft het (dreigende) incident / de calamiteit gevolgen voor de reputatie, de financiën, de veiligheid of het normaal functioneren van (onderdelen van) de universiteit?
6. Heeft het (dreigende) incident/de calamiteit gevolgen voor de waardevolle kennisdomeinen of samenwerkingen met risicovolle landen die geformuleerd zijn in de checklist rode vlaggen risico kennisveiligheid (bijlage).
7. De universiteit wordt door 3de partijen onder druk gezet, zoals bij ransomware".
8. Genereert het (dreigende) incident/de calamiteit media-aandacht?

Zodra op één of meerdere van deze vragen het antwoord Ja is dan vindt opschaling naar het College plaats. Waar aangewezen zal het College van Bestuur ook de Raad van Toezicht informeren.

Open Universiteit

3 Structuur



3.1 Crisismanagementteam informatieveiligheid

In het Crisismanagementteam informatieveiligheid (CMTI) worden de navolgende rollen ingevuld:

3.1.1 Voorzitter

Taak: het aansturen van het CMT.

Bevoegdheid:

1. Aanwijzingen te geven aan OU-medewerkers i.v.m. het oplossen van de crisis, waaronder het oproepen van medewerkers buiten hun normale werktijden, medewerkers ontslaan van andere verplichtingen om hun inzet voor de crisisbeheersing mogelijk te maken.
2. Verplichtingen aan te gaan om op korte termijn maatregelen met financiële consequenties te kunnen treffen, bijvoorbeeld het inschakelen van externe specialisten.
3. Te beslissen over communicatie-uitingen van de OU over de crisis, zowel intern (naar het personeel) als extern naar studenten en de wereld.
4. Naar bevind van zaken andere deskundigen raadplegen en deze zo nodig tijdelijk tot lid van het CMT benoemen.

Verantwoordelijkheid: het managen van de crisis.

Tot het College deelneemt in het CMTI is de Directeur ITF voorzitter. Vanaf het moment dat het College deelneemt aan het crisismanagementteam dan is een collegelid de voorzitter.

Open Universiteit

3.1.2 Directeur Informatietechnologie en facilitaire zaken (ITF)

Taak:
1. Het inbrengen van IT-deskundigheid bij het analyseren en managen van de crisis.
2. Het doen uitvoeren van de besluiten die in het CMTI zijn genomen.

Bevoegdheid:

1. Het deprioriteren van andere taken van ITF t.b.v. het managen van de crisis.
2. Het aansturen van eventuele ingeschakelde externe partijen. Dit betreft het Incident Response Team vanuit Chubb (cyberverzekering).

Verantwoordelijkheid:

1. De kwaliteit van de analyses en adviezen.
2. De kwaliteit en de tijdige realisatie van de uitvoering van de besluiten uit het CMTI.

3.1.3 Hoofd operations (ITF-O)

Taak:

1. Het inbrengen van ITF-O-deskundigheid bij het analyseren en managen van de crisis.
2. Optreden als Change manager bij het realiseren van maatregelen.

Verantwoordelijkheid: de kwaliteit van de bijdrage van ITF-O aan het managen van de crisis.

3.1.4 Hoofd innovatie en development (ITF-IenD)

Taak: Het inbrengen van ITF-IenD-deskundigheid bij het analyseren en managen van de crisis.

Verantwoordelijkheid: de kwaliteit van de bijdrage van ITF–IenD aan het managen van de crisis.

3.1.5 Woordvoerder OU

Taak:
1. Adviseren van het CMTI m.b.t de communicatie over de crisis.
2. In opdracht van de voorzitter, namens de OU communiceren over de crisis, zowel intern (personeel) als extern (studenten en de wereld).

Bevoegdheid: gevraagd en ongevraagd adviseren van het CMTI, ondersteuning vragen (en krijgen) voor uitvoering van de communicatie (bijv. voor plaatsing/verspreiding van berichten).

Verantwoordelijkheid: de kwaliteit van de adviezen en de uitvoering van de afgesproken maatregelen.

Open Universiteit

3.1.6 Functionaris voor de gegevensbescherming

Taak: het behartigen van de belangen van eventuele personen wier privacy door het incident wordt bedreigd (de betrokkenen) bij het managen van de crisis, o.a. het adviseren over maatregelen die invloed hebben op die belangen.

Bevoegdheid (ook als er geen crisis is) het melden van datalekken aan de AP.

Verantwoordelijkheid:

1. De kwaliteit van de adviezen.
2. Beoordelen of persoonsgegevens onrechtmatig verwerkt zijn en of dat zodanige risico's voor de betrokkenen oplevert dat het incident als een datalek moet worden gemeld bij de Autoriteit Persoonsgegevens (AP).

3.1.7 Chief Information Security Officer

Taak: Het inbrengen van deskundigheid op het gebied van informatieveiligheid bij het analyseren en managen van de crisis.

Bevoegdheid: gevraagd en ongevraagd adviseren van het CMTI.

Verantwoordelijkheid:

1. De kwaliteit van de adviezen.
2. Borging dat de juiste aanpak en procedure gevolgd worden.

3.1.8 Coördinator kennisveiligheid

Taak:

1. Het inbrengen van kennisveiligheidsdeskundigheid bij het analyseren van de crisis.
2. Het doen uitvoeren van de besluiten die in het CMTI zijn genomen.

Bevoegdheid: gevraagd en ongevraagd adviseren van het CMTI.

3.1.9 Notulist

Taak: het zodanig notuleren van de CMTI-activiteiten dat relevante acties en besluiten naspeurbaar zijn.
Verantwoordelijkheid: de kwaliteit van de notulen.

De notulist wordt, afhankelijk van de situatie, door de voorzitter aangewezen.

Open Universiteit

3.2 Uitvoeringsorganisatie

3.2.1 Afdeling Operations

ITF-O analyseert de situatie, adviseert over mogelijke maatregelen en voert de in de CMTI besloten changes in de ICT-infrastructuur uit.

3.2.2 Afdeling Innovatie en Development

ITF-IenD analyseert de situatie, adviseert over mogelijke maatregelen en realiseert desgevraagd hulpmiddelen en wijzigingen in bestaande functionaliteit.

3.2.3 Afdeling Marketing en Communicatie

MenC realiseert – onder leiding van de woordvoerder – de in het CMTI vastgestelde communicatiestrategie.

4 Hulpmiddelen

4.1 Bereikbaarheid – intern

Hoofd operations heeft een Signal Appgroep "CMT OU" waarin alle bovengenoemde leden van het CMTI – initieel met uitzondering van het college – zijn opgenomen. Daarmee kan het CMTI worden opgeroepen en zijn de CMTI-leden voor elkaar bereikbaar. Tijdens een specifiek incident kunnen anderen tijdelijk in die Signal groep worden opgenomen.

Er zijn voorbereidende maatregelen getroffen om te waarborgen dat:

- Het CMTI en de door hen aangewezen personen (ook) buiten werktijd toegang hebben tot de gebouwen op de campus. Hoofd Operations initieert dat per geval.
- Bij de Servicedesk is een opgeladen GSM beschikbaar voor communicatie door en met het CMTI. Het nummer daarvan is: 06 11 91 58 16.

Open Universiteit

4.2 Bereikbaarheid – extern

4.2.1 Telefoon

De woordvoerder beheert een GSM waarvan het nummer bekend is bij de pers. Als informatie over een (vermeende) informatieveiligheidscrisis op de OU in de buitenwereld opduikt, zal de pers via dit nummer informatie zoeken. Het is van belang dat zij dan adequaat en deskundig te woord worden gestaan. Studenten zullen de OU telefonisch benaderen via Team Service en informatie. Zie onder § 4.2.2.

4.2.2 E-mail

De woordvoerder beheert het e-mailadres persvoorlichting@ou.nl dat bekend is bij de pers. Als informatie over een (vermeende) informatieveiligheidscrisis op de OU in de buitenwereld opduikt, zal de pers via dit e-mailadres informatie zoeken. Het is van belang dat zij dan adequaat en deskundig te woord worden gestaan.

Bij een informatieveiligheidscrisis kan ook het e-mailadres ou@ou.nl worden opengesteld voor informatie over de specifieke informatieveiligheidscrisis. Buiten die situaties moet dit e-mailadres antwoorden met een adequate doorverwijsboodschap.

Studenten zullen de OU middels e-mail benaderen via Team Service en informatie (SenI) op info@ou.nl. Bij een informatieveiligheidscrisis zullen de betreffende medewerkers SenI door de woordvoerder worden voorzien van Q&A betreffende de situatie. Bovendien kan worden overwogen om ook buiten de reguliere werktijden van SenI medewerkers in te zetten om studenten te woord te staan.

4.2.3 Internet

Bij een informatieveiligheidscrisis kan de OU informatie delen via onze corporate website www.ou.nl. Daartoe is er een crisiscommunicatie-app waarin alle webredacteuren zitten en ook de medewerkers van SenI die in Vraag en Antwoord teksten kunnen en mogen plaatsen. Dit proces wordt aangestuurd door de woordvoerder.

Ook als onze eigen ict-infrastructuur niet meer beschikbaar is, kan de OU informatie delen via de website http://oustatus.nl/. Hoofd Operations kan hier informatie plaatsen, onder aansturing van de woordvoerder.

4.3 Crisiscentrum - locatie, bereikbaarheid, gebruik

Zodra de voorzitter van het CMTI heeft vastgesteld dat er sprake is van een informatieveiligheidscrisis, wordt het crisiscentrum ingericht op de begane grond van gebouw Milton Keynes op de campus in Heerlen. Die keuze wordt gemaakt omdat die locatie goed bereikbaar is en de meeste mensen en apparatuur die bij de bestrijding een rol kunnen spelen, dan gemakkelijk beschikbaar zijn. Zo nodig worden die ruimten daartoe vrijgemaakt. Het Crisiscentrum wordt ingericht in de IOUnge. (MKE 0.87&0.82).

Uitwijklocatie: volgt. Voor een fysieke uitwijklocatie wordt een mogelijkheid bij Hs Zuyd onderzocht. Indien ICT voorziening Teams functioneert dan is een virtueel Team de uitwijkmogelijkheid.

Open Universiteit

Eenieder die geen lid is van het CMTI heeft slechts op uitnodiging toegang tot het crisiscentrum. Het overleg van het CMTI vindt plaats in het crisiscentrum. De leden van het CMTI kunnen hun werkzaamheden ook op andere plekken uitvoeren.

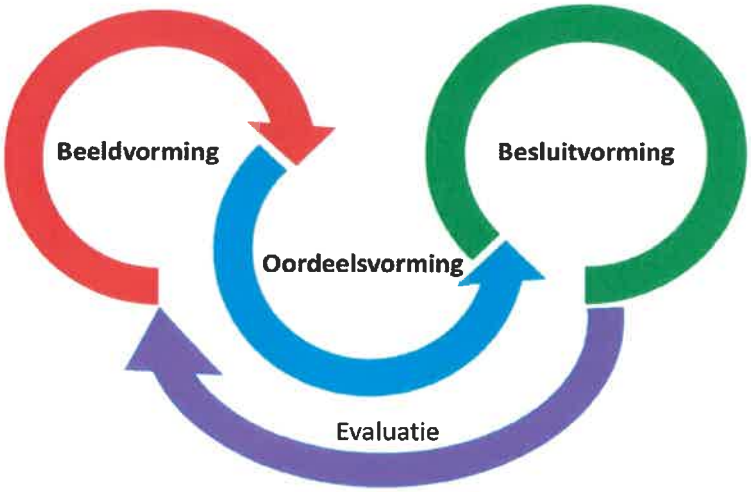
5 Contactinformatie – bereikbaarheidsgegevens

Rol	Telefoon	Gemandateerde	Telefoon
College van bestuur Portefeuillehouder		College van bestuur (Rector) Bestuurssecretaris	
Directeur ITF		Hoofd Operations	
Hoofd Operations		Systeem engineer	
Hoofd Innovatie en development		Enterprise architect	
Functionaris voor de gegevensbescherming (FG)		Er is geen gemandateerde FG. Bij afwezigheid van de FG kan voor juridisch advies een beroep worden gedaan op	
Woordvoerder OU		Communicatieadviseur	
Chief Information Security Officer		1e Hoofd Operations, 2e Systeem engineer,	
Coördinator kennisveiligheid		Secretaris Kennisveiligheid	
Notulist			
Te woord staan van betrokkenen (Service en Informatie)			
Incident Response Team Chubb (Via firma)		Via de " " app. Polisnummer:	

Open Universiteit

Bijlage: BOB procedure

Het BOB-model is in 1951 door Robert Bales en Fred Strodtbeck geïntroduceerd om tot weloverwogen besluiten te komen in een team. Bij iedere fase hieronder zijn de vragen van die fase beschreven, is de vergadermethodiek benoemd en is het beoogde resultaat opgeschreven.



Evaluatie
- Verandert de situatie?
- Lopen je scenario's nog zoals verwacht?
- Zijn er nieuwe opties of vallen er af?
- Wat betekent dat?
- Haal je dan het doel nog op tijd?
- Enzovoorts.

Tot het calamiteitenteam kan worden ontbonden.

Beeldvorming (1): Situatie-analyse

Vragen

- Wat weten we?
- Klopt alles wat we (denken te) weten?
- Wat weten we niet?
- Hebben we die informatie echt nodig om tot een goed besluit te komen?
- Hoe gaan we de ontbrekende informatie verzamelen?

Beeldvorming (2): Scenario-analyse

Vragen

- Waar gaat de crisis waarschijnlijk heen?
- Welke scenario's zijn er mogelijk nog meer te verwachten?
- Welk scenario moet absoluut voorkomen worden?

Scenario-analyse kan ertoe leiden dat je meerdere crises tegelijkertijd managet: de reële crisis zoals die zich nu al voordoet en de ongewenste crises die koste wat kost voorkomen moeten worden, hoe klein de kans ook is.

Open Universiteit

Vergadermethodiek

- Korte uitleg van de situatie door iedere deelnemer
- Brainstorm over de situatie
- Doorvragen ter verduidelijking
- Géén discussie

Resultaat

- Iedereen heeft hetzelfde beeld van de huidige situatie
- Vastgelegd gezamenlijk beeld van situatie en scenario's
- Actieplan om aan ontbrekende informatie te komen

Oordeelsvorming (1): Optie-analyse

Vragen

Optie-analyse: als de situatie en de scenario's duidelijk zijn, start de oordeelsvorming met het inventariseren van de opties.

- Wat is ons handelingsperspectief (wat kunnen we doen)?
- Wat zijn korte termijn opties en welke opties gelden voor een iets langere termijn?

Oordeelsvorming (2): Consequentie-analyse

- Wat betekent elke separate optie voor de veiligheid, continuïteit en reputatie van de organisatie / het vooruitzicht voor de student?

Vergadermethodiek

- Discussie
- Doorvragen naar achterliggende belangen en motivaties ('wat maakt dit besluit voor jou onaanvaardbaar' of 'wat moet er gebeuren om jouw bezwaren op te heffen')
- Dialoog
- Nieuwsgierig naar elkaars mening en belang

Resultaat

- Gezamenlijke belangen, criteria en voorwaarden in beeld

Besluitvorming

Vragen

Open Universiteit

- Wat besluiten we (concreet)?
- Weet iedereen welk besluit genomen is?
- Is iedereen het eens met het besluit?
- Wat gaan we doen (SMART acties)?

Vergadermethodiek

- Stemmen
- Consensus
- Compromis
- Rondje om te checken of de besluiten en acties klopt

Resultaat

- Besluitenlijst
- Actielijst

Open Universiteit

BIJLAGE: Basisagenda CMTI en Checklist voor de voorzitter

Basisagenda

1. Opening en controle aanwezigheid alle (extra) leden. Vastleggen in logboek
2. Mededelingen voorzitter. Prioriteiten in de agenda
3. Informatieronde. Mededelingen over stand van zaken en advies over acties op korte en middellange termijn. Zie het logboek vorige vergadering i.v.m. voortgang- en afdoeningscontrole
4. Opgave van nog uit te voeren acties door de individuele leden
5. Recapitulatie van de onderwerpen m.b.v. logboek
6. Afspraak tijdstip (en locatie) volgende vergadering
7. Sluiting

Checklist voor de voorzitter

- Waar komt het CMTI bijeen? Vraag dit zodra u gealarmeerd wordt. U kunt misschien niet naar de vaste locatie en moet er een alternatief gezocht worden.
- Roep bij afwezigheid van één of meer leden de plaatsvervangers of anderen op. Laat dit doen door bijvoorbeeld een van de eerst aanwezige leden van het CMTI. Ga vooral niet zelf telefoneren omdat u bereikbaar/beschikbaar moet blijven voor het voorzitterschap en coördinatie (leidinggeven aan) van de CMTI- werkzaamheden.
- Geef opdracht voor het oproepen van extra functionarissen of anderen die u noodzakelijk acht aanwezig te zijn naar aanleiding van de gebeurtenissen.
- Regel het afvangen van de telefoontjes, etc. die tijdens de vergaderingen kunnen binnenkomen en voor het CMTI of de individuele leden bedoeld zijn.
- Bellen en gebeld worden tijdens de vergaderingen is niet toestaan.
- Wees altijd bereikbaar en beschikbaar voor alle leden van het CMTI. Doe daarom niets zelf waardoor u zodanig in beslag genomen wordt dat u niet meer voor anderen beschikbaar bent.
- Bepaal het tijdstip waarop de eerste vergadering plaatsvindt. Wacht niet te lang met de eerste vergadering ook al zijn nog niet alle leden van het CMTI gearriveerd.
- Start elke vergadering met beeldvorming/situatiebeschrijving.
- Als er (nog) steeds leden van het CMTI of in het CMTI arriveren terwijl u al op gang bent gekomen, herhaal niet telkens weer de beeldvorming of wat er al besloten is. Praat hen bij (laat hen bijpraten) tijdens de eerstkomende schorsing zodat de anderen verder kunnen gaan met hun acties.
- Laat elk lid van de vergadering een bijdrage in die beeldvorming leveren. Houdt telkens een informatieronde en laat elk lid van de vergadering zelf (probleemeigenaren) toelichten aan welke onderwerpen wordt gewerkt of waaraan aandacht wordt besteed en stel dan controlevragen
- Voorkom dat u als enige aan het woord bent.
- Wijs altijd iemand aan die het onderwerp uitzoekt of moet laten uitvoeren als daar twijfel over bestaat (aanwijzen probleem- of activiteiteneigenaren).
- Zet (zonodig) alle acties en informaties op een rij (flip-over?) om zodoende overzicht te houden. Draag dit eventueel op aan de notulist van het CMTI.

Open Universiteit

- Stel prioriteiten van de onderwerpen die afgehandeld moeten worden en waarover in het CMTI verder gesproken moet worden.
- Vergader kort (bijv. 15 minuten) en geef in de schorsingen de gelegenheid om de afgesproken acties te kunnen uitzetten. Schorsingen kunnen langer duren dan de vergaderingen.
- Discussieer niet over onderwerpen die niet voor het CMTI overleg zijn bedoeld. Wijs de leden van het CMTI en externe adviseurs daar zo vroeg mogelijk op. Misschien dat veel door de CMTI leden zelf geregeld kan worden zonder alles eerst te noemen in het CMTI-overleg.
- Laat het logboek (korte notulen) bijhouden en maak hiervan gebruik. Laat het logboek tijdens de schorsingen printen en op de vergadertafel liggen ten behoeve van de volgende vergaderingen. Het logboek dient ook voor de voortgang- en afdoeningcontrole.
- Spreek met de leden af wanneer de volgende vergadering zal zijn.
- Spreek met de leden af hoe zij bereikbaar zijn tijdens de schorsingen voor eventueel tussentijds of spoedoverleg.
- Maak heldere afspraken over voorlichtingsactiviteiten (extern en intern).

Open Universiteit

Bijlage: Checklist rode vlaggen risico kennisveiligheid

- Wordt er onderzoek gedaan naar een van onderstaande waardevolle kennisdomeinen?
    - Digitale technologieën (kunstmatige intelligentie)
    - Engineering- en fabricagetechnologieën (3D printen, robotica)
    - Life science technologieën
- Vindt er een samenwerking plaats met een van de volgende landen?
    - China
    - Koeweit
    - Iran
    - Noord-Korea
    - Qatar
    - Rusland
    - Saoedi-Arabië
    - Turkije
    - Venezuela

Wanneer een of beide vragen van toepassing zijn dan betreft het mogelijk een risicovol onderzoek en wordt geadviseerd een melding te maken bij de secretaris of coördinator kennisveiligheid.