|  |
| --- |
| Procedure RisicobeheerTemplate |

|  |  |
| --- | --- |
| Auteur(s): |  |
| Versie: |  |
| Datum: | Kies of typ een datum |
| Kenmerk: |  |
|  |  |
|  |  |

**Documentinformatie**

Dit document maakt onderdeel uit van een complete set (beleidspiramide) met formeel vastgestelde documenten op strategisch, tactisch en operationeel niveau. Dit document heeft betrekking op de laag Procedure in de beleidspiramide.



**Versiebeheer**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Datum** | **Auteur** | **Verwerking** |
|  |  |  |  |
|  |  |  |  |

**Distributielijst**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Datum** | **Ontvanger** | **Doel** |
|  |  |  |  |
|  |  |  |  |

**Vaststelling**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Datum** | **Vastgesteld door** | **Vastgesteld op** |
|  |  |  |  |
|  |  |  |  |

**Samenhang met andere documenten**

|  |  |  |  |
| --- | --- | --- | --- |
| **Naam** | **Bovenliggend** | **Gelijk niveau** | **Onderliggend** |
| [INFORMATIEBEVEILIGINGSBELEID] | x |  |  |
| [BELEID RISICOBEHEER] | x |  |  |
| [BIJLAGE BIJ PROCEDURE] |  |  | x |
| [DIVERSE HULPMIDDELEN] |  |  | x |
|  |  |  |  |

**Verwijzingen naar SURFaudit Toetsingskader en ISO27001**

|  |  |
| --- | --- |
| **Kader** | **Verwijzing (tags)** |
| SURFaudit Toetsingskader | RM.01, RM.02, RM.03 |
| ISO 27001 | 6.1, A.12, A.16 |
| ISO 27005 | 7, 8, 8.2, 8.3, 8.4, 9, 10 |
| ISO 31000 | 5.4, 6.1, 6.4, 6.6, 6.7 |

**Creative Commons**

Dit template is een product van het SURF Security Expertise Centrum en beschikbaar onder de licentie Creative Commons Naamsvermelding 4.0 Internationaal. <https://creativecommons.org/licenses/by/4.0/deed.nl>

Inhoudsopgave

|  |
| --- |
| [Samenvatting 4](#_Toc192747603)[1 Inleiding 5](#_Toc192747604)[1.1 Doel 5](#_Toc192747605)[1.2 Toepassingsgebied en Reikwijdte 5](#_Toc192747606)[2 Procedure Risicobeheer 6](#_Toc192747607)[2.1 Reikwijdte, Context en Criteria 6](#_Toc192747608)[2.2 Risicobeoordeling 7](#_Toc192747609)[2.2.1 Risico-identificatie 7](#_Toc192747610)[2.2.2 Risicoanalyse 8](#_Toc192747611)[2.2.3 Risico-evaluatie 9](#_Toc192747612)[2.3 Risicobehandeling 9](#_Toc192747613)[2.4 Monitoren en beoordelen 10](#_Toc192747614)[2.5 Communicatie en advies 11](#_Toc192747615)[2.6 Registratie en rapportage 11](#_Toc192747616)[2.7 Planning en Control Cyclus 11](#_Toc192747617)[3 Vaststelling 13](#_Toc192747618)[Bijlage 1 Verklarende woordenlijst 14](#_Toc192747619) |

Samenvatting

Hier komt een samenvatting, op zichzelf leesbaar, van de inhoud van dit document in max. 1 A4.

# Inleiding

Deze procedure beschrijft de uitvoering van het risicobeheer binnen onze instelling. Risicobeheer is een integraal onderdeel van de organisatie en ondersteunt bij het identificeren, beoordelen, behandelen, monitoren en rapporteren van risico’s die onze strategische en operationele doelstellingen kunnen beïnvloeden.

Deze procedure is opgesteld in overeenstemming met de relevante normen en richtlijnen, waaronder ISO 31000, ISO 27001 en ISO 27005, en is onderliggend aan op ons bredere Risicobeheer Beleid.

## Doel

Het doel van deze procedure is het vastleggen van een systematische en gestructureerde aanpak voor risicobeheer, zodat risico’s tijdig worden onderkend, geanalyseerd en beheerst. Dit draagt bij aan:

* Het beschermen van de beschikbaarheid, integriteit en vertrouwelijkheid van informatie.
* Het ondersteunen van strategische en operationele besluitvorming.
* Het naleven van wet- en regelgeving en sectorale richtlijnen.
* Het bevorderen van een risicobewuste cultuur binnen de instelling.

## Toepassingsgebied en Reikwijdte

Deze procedure is van toepassing op alle afdelingen, processen, systemen en diensten binnen de instelling waarin risico’s geïdentificeerd, geanalyseerd en beheerst moeten worden. Dit betreft onder andere:

* Informatiebeveiligingsrisico’s die voortvloeien uit dreigingen en kwetsbaarheden.
* Strategische, operationele en compliance-risico’s.
* Alle medewerkers, externe partijen en stakeholders die betrokken zijn bij risicobeheer.
* De implementatie van risicobeheer binnen de gehele beleidspiramide, waarbij het beleid, de processen en de operationele uitvoering op elkaar aansluiten.

# Procedure Risicobeheer

Het risicobeheer bestaat uit een reeks gestructureerde stappen die helpen bij het identificeren, analyseren, behandelen en bewaken van risico’s. Onze instelling hanteert ISO 31000:2018 als leidraad voor het risicobeheer, en NEN-ISO 27005:2022 als leidraad voor risicobeheer informatiebeveiliging.

|  |  |
| --- | --- |
| ***Reikwijdte, context en criteria*** *(zie 2.1)* | *Afbeelding met tekst, schermopname, diagram, Lettertype  Automatisch gegenereerde beschrijving**Figuur 1 – Risicobeheer Informatiebeveiliging* |
| ***Risicobeoordeling (2.2)*** |
|  *Risico-identificatie (2.2.1)* |
|  *Risicoanalyse (2.2.2)* |
|  *Risico-evaluatie (2.2.3)* |
| ***Risicobehandeling (2.3)*** |
| ***Monitoring en beoordelen (2.4)*** |
| ***Communicatie en advies (2.5)*** |
| ***Registratie en rapportage (2.6)*** |

## Reikwijdte, Context en Criteria

De eerste stap in het risicobeheer is het bepalen van de reikwijdte en het vaststellen van de context en criteria. Dit zorgt ervoor dat risico’s binnen de juiste kaders worden geïdentificeerd en beoordeeld.

**Reikwijdte**

De reikwijdte van risicobeheer omvat alle processen, systemen, informatie en activiteiten binnen onze instelling die risico’s kunnen beïnvloeden. Dit kan variëren van operationele activiteiten tot strategische en compliance-gerelateerde processen. De instelling hanteert een integrale benadering waarbij zowel interne als externe factoren worden meegenomen in de risicoanalyse.

**Contextanalyse**

Het bepalen van de context houdt in dat alle relevante interne en externe factoren die van invloed kunnen zijn op risico’s worden geanalyseerd. Dit omvat o.a.:

* De missie, visie en strategische doelstellingen van onze instelling.
* De wettelijke en regelgevende vereisten waaraan onze instelling moet voldoen.
* Interne factoren zoals de organisatiestructuur, beleid en beschikbare middelen.
* Externe factoren zoals economische ontwikkelingen, technologische veranderingen en dreigingen uit de sector (bijvoorbeeld cybersecuritydreigingen[[1]](#footnote-1)).

**Criteria**

Om risico’s op een consistente en objectieve manier te beoordelen, worden vaste criteria gehanteerd:

* **Kans:** De waarschijnlijkheid dat een risico zich voordoet, gebaseerd op historische gegevens en trends.
* **Impact:** De potentiële gevolgen van een risico voor de organisatie, ingedeeld op basis van ernst en schaal (financieel, operationeel, reputatieschade, juridische consequenties).
* **Acceptatiedrempel**: De mate waarin een risico acceptabel is binnen de vastgestelde risicobereidheid. Risico’s die de acceptatiedrempel overschrijden, vereisen actie of escalatie naar het management.

Risico’s worden in een risicoregister bijgehouden waarbij eventueel gebruik gemaakt kan worden van een Governance, Risk, Compliance (GRC)-applicatie.

## Risicobeoordeling

Volgende stap in het risicobeheer is risicobeoordeling. Dit omvat het systematisch identificeren, analyseren en evalueren van risico’s. Dit proces helpt onze instelling te bepalen welke risico’s de grootste impact kunnen hebben en welke beheersmaatregelen nodig zijn om deze risico’s te mitigeren of te accepteren.

De risicobeoordeling bestaat uit drie stappen:

* **Risico-identificatie**: Het in kaart brengen van potentiële risico’s en kwetsbaarheden.
* **Risicoanalyse**: Het beoordelen van de ernst van de risico’s door kans en impact in te schatten.
* **Risico-evaluatie**: Het vergelijken van risico’s met vastgestelde criteria om te bepalen welke risico’s beheerst moeten worden en welke geaccepteerd kunnen worden.

### Risico-identificatie

Risico-identificatie is de eerste stap in het proces van risicobeoordeling. Hierbij worden alle mogelijke risico’s binnen de organisatie in kaart gebracht. Het doel is om een volledig overzicht te krijgen van dreigingen en kwetsbaarheden die impact kunnen hebben op de strategische, operationele en compliance-doelstellingen van onze instelling.

**Methoden voor risico-identificatie**

Voor het identificeren van risico’szijn meerdere methoden mogelijk die naast elkaar of afzonderlijk inzetbaar zijn.

* **Top-down benadering**

Elke eigenaar van een proces of applicatie organiseert, met de IB-risicomanager, periodiek (minimaal 1 keer per jaar) een risicobeoordeling voor zijn/haar processen en/of applicaties. Dit kan plaatsvinden op verschillende niveaus in de organisatie (strategisch, tactisch, operationeel).

Risico-identificaties vinden plaats in interdisciplinaire samenwerking, waarbij experts met kennis van proces, systeem, gebruikers, wet- en regelgeving, architectuur etc. kunnen worden uitgenodigd.

Onze instelling maakt hierbij gebruik van verschillende methoden, zoals workshops, interviews, procesanalyses, risico-dialoog etc. Bronnen die geraadpleegd kunnen worden zijn o.a.:

* + Het Cyberdreigingsbeeld van SURF, NCSC.
	+ De op kernprocessen en -applicaties uitgevoerde DPIA’s[[2]](#footnote-2).
	+ Decentrale risico-assessments (in de eerste lijn, door domein-, proces- en/of systeemeigenaren, IB (-risico) functionarissen).
	+ Overige assessments, bijvoorbeeld als onderdeel van audits of eigen onderzoeken naar specifieke dreigingen of kwetsbaarheden.
	+ Overige externe informatiebronnen.
* **Bottom-up benadering**

Operationele risico’s geïdentificeerd door meldingen van medewerkers, functioneel beheerders, privacy-officers, ISO’s, studenten, onderzoekers etc.

Alle geïdentificeerde risico’s worden vastgelegd in het centrale risicoregister en voorzien van een eerste inschatting van kans en impact.

### Risicoanalyse

Na de identificatie van risico’s volgt de risicoanalyse. Dit proces beoordeelt de ernst van de risico’s door de kans van optreden en de impact ervan te kwantificeren. De analyse helpt bij het prioriteren van risico’s, zodat onze instelling effectieve beheersmaatregelen kan nemen.

**Classificatie van risico’s**

De risico’s worden ingedeeld in de volgende categorieën:

* **Laag**: De impact is beperkt en de kans van optreden is gering. Monitoring volstaat.
* **Gemiddeld**: Er is enige impact en kans van optreden. Aanvullende beheersmaatregelen kunnen nodig zijn.
* **Hoog**: De impact is aanzienlijk en de kans op optreden is reëel. Specifieke beheersmaatregelen zijn vereist.
* **Kritiek**: De impact is zeer ernstig en/of de kans op optreden is hoog. Directe actie is noodzakelijk.

**Methoden voor risicoanalyse**

Bij het uitvoeren van een risicoanalyse worden risico’s in detail onderzocht naar directe en indirecte dreigingen, oorzaken en gevolgen. Hierbij kunnen de volgende methoden worden toegepast:

* **Kwalitatieve analyse**: Beoordeling op basis van expertise en scenario-analyses.
* **Kwantitatieve analyse**: Gebruik van numerieke modellen en statistische berekeningen.
* **Scenario-analyses**: Het doorlopen van mogelijke scenario’s om de impact en gevolgen van risico’s beter te begrijpen.
* **Heatmaps**: Visuele weergave van de ernst en prioriteit van risico’s binnen een gestructureerd framework.

De resultaten van de risicoanalyse worden vastgelegd in het risicoregister en gebruikt voor verdere besluitvorming.

In het document ‘Bijlage bij Procedure Risicobeheer’ zijn verschillende voorbeelden opgenomen waarmee kans en impact van risico’s in te schatten of te bepalen zijn en een voorbeeld van een risico-heatmap, en effectiviteitswaardering rond maatregelen.

### Risico-evaluatie

De laatste stap in de risicobeoordeling is de risico-evaluatie. Hierbij worden de geanalyseerde risico’s vergeleken met vastgestelde risicocriteria om te bepalen welke acties nodig zijn.

**Stappen binnen risico-evaluatie**

* **Vergelijking met acceptatiedrempels**: Elk risico wordt afgezet tegen de risicobereidheid en acceptatiedrempels van de instelling.
* **Besluitvorming over risicobehandeling**: Op basis van de evaluatie wordt bepaald of het risico geaccepteerd, gemitigeerd, overgedragen of geëlimineerd moet worden.
* **Escalatieprocedure**: Risico’s die de vastgestelde drempels overschrijden, worden geëscaleerd naar het management of het College van Bestuur.

De uitkomsten van de risico-evaluatie worden vastgelegd in het risicoregister en dienen als basis voor het opstellen van een risicobehandelplan.

## Risicobehandeling

Na de risico-evaluatie wordt bepaald welke maatregelen nodig zijn om de geïdentificeerde risico’s te beheersen. De noodzaak voor risicobehandeling kan ook voortkomen uit het monitoren van risico’s, incidenten, nieuwe ontwikkelingen, inzichten of beheersmaatregelen.

Risicobehandeling omvat het kiezen van een geschikte strategie en het implementeren van maatregelen om risico’s te verminderen tot een acceptabel niveau.

De keuze voor een specifieke behandelstrategie is afhankelijk van factoren zoals de risicotolerantie van de instelling, de kosten en effectiviteit van beheersmaatregelen en de mate waarin risico’s kunnen worden gedeeld of overgedragen. Er zijn vier primaire behandelopties:

* **Elimineren**: Het volledig verwijderen van de oorzaak van het risico. Bijvoorbeeld door de betreffende activiteiten niet meer te doen.
* **Mitigeren**: Het nemen van maatregelen om de kans of impact van een risico te verlagen. De risico-eigenaar bepaalt in overleg met stakeholders de planning van de verbeteracties. Deze worden vastgelegd in het risico-register (zie 2.6).
Na mitigatie kunnen restrisico’s blijven bestaan. Deze restrisico’s worden alsnog gemitigeerd of onderworpen aan het risico-acceptatieproces.
* **Overdragen**: Het risico (gedeeltelijk) overdragen aan of samenwerking met andere partijen (collega-instellingen of derden) die beter en/of goedkoper in staat zijn de tegenmaatregelen te treffen. Denk ook aan het afsluiten van een verzekering of outsourcing.
* **Accepteren**: Het risico bewust accepteren als de kosten van beheersmaatregelen niet opwegen tegen de verwachte schade. Dit gebeurt meestal bij evaluatie van risico’s die al in het risicoregister zijn opgenomen. In dit geval wordt de risicobehandelingsstap overgeslagen. Risico’s worden expliciet geaccepteerd door de risico-eigenaar.

Voor risico’s ‘gemiddeld’ of hoger die niet worden geaccepteerd wordt een termijn afgesproken waarbinnen deze moet worden geëlimineerd, gemitigeerd of overgedragen (zie het document ‘Bijlage bij Procedure Risicobeheer’).

Voor elk risico waarvoor beheersmaatregelen nodig zijn, wordt een risicobehandelplan opgesteld. Dit plan bevat de geplande maatregelen, de verantwoordelijke personen en de tijdslijnen voor implementatie en evaluatie.

## Monitoren en beoordelen

Risicobehandeling is een continu proces, waarbij regelmatig wordt geëvalueerd of de genomen maatregelen effectief zijn en of de risicoclassificatie moet worden bijgesteld. Monitoring en beoordeling zorgen ervoor dat risicobeheer dynamisch blijft en aansluit op veranderende omstandigheden.

**Rollen en verantwoordelijkheden**

* **Risicomanager(s)** bewaken de implementatie en effectiviteit van risicobeheersmaatregelen, houden toezicht op restrisico’s en voeren periodieke revisies uit.
* **IB (risico-) functionaris** monitort de status van risico’s in het risicoregister en de voortgang van verbeteracties. De risico-eigenaar dient hierbij als bron.
* **CISO** rapporteert structureel en ad hoc aan de portefeuillehouder in het College van Bestuur over openstaande en geaccepteerde risico’s die aandacht behoeven.
* **Actiehouders** zijn verantwoordelijk voor het uitvoeren van maatregelen binnen de gestelde termijnen. Bij non-compliance of onvoldoende voortgang gaat de IB-functionaris eerst in gesprek met de actiehouder. Indien nodig wordt dit geëscaleerd naar de risico-eigenaar en CISO.

**Evaluatie en audits**

De evaluatie van risico’s, die zijn opgenomen in het risicoregister (zie 2.6), vindt plaats op basis van vastgestelde herzieningstermijnen:

* Kritieke risico’s: evaluatie elke drie (3) maanden.
* Hoge risico’s: evaluatie elke zes (6) maanden.
* Gemiddelde risico’s: jaarlijkse evaluatie.

Gemitigeerde risico’s worden opnieuw geëvalueerd bij relevante veranderingen in processen, IT-systemen, dreigingen en kwetsbaarheden en wet- en regelgeving.

Behandelde risico’s zijn minimaal een (1) keer per jaar door de eigenaar geëvalueerd omdat de hoogte van risico’s kan veranderen door ontwikkelingen buiten de onderwijsinstelling, bijvoorbeeld, nieuwe aanvalstechnieken kunnen de kans van een risico sterk verhogen.

Bij de evaluatie wordt ook gekeken naar de effectiviteit van de geïmplementeerde maatregelen (zie het document ‘Bijlage bij Procedure Risicobeheer’).

Geaccepteerde risico’s worden periodiek geëvalueerd.

[Daarnaast worden periodieke audits en controles uitgevoerd door de interne auditafdeling en externe auditoren. De resultaten van deze beoordelingen worden teruggekoppeld aan het management en, indien nodig, wordt de risicobehandelstrategie aangepast.]

## Communicatie en advies

Effectieve communicatie is een belang onderdeel van risicomanagement. Transparantie over risico’s en beheersmaatregelen zorgt ervoor dat alle belanghebbenden binnen de organisatie goed geïnformeerd zijn en dat risico’s tijdig en adequaat worden aangepakt.

In alle fasen vindt overleg plaats tussen betrokkenen en andere belanghebbenden, en met eventuele externe partijen, over de uitgevoerde analyses en dergelijke. Het gaat hierbij zowel over interne rapportages (zoals planning & control cyclus) als over externe rapportages aan stakeholders en breder publiek (bijvoorbeeld via het jaarverslag).

De CISO, de ISO’s en BSO’s ondersteunen belanghebbenden bij het begrijpen van risico's, de basis waarop beslissingen worden genomen en de redenen waarom specifieke acties nodig (of juist overbodig) zijn. De risico-eigenaar stelt besluitvormers en andere belanghebbenden op de hoogte van zowel geaccepteerde risico's alsook de aard en de omvang van het resterende risico na de risicobehandeling.

## Registratie en rapportage

Een gestructureerde registratie en rapportage van risico’s is noodzakelijk om grip te houden op het risicomanagementproces en verantwoording af te kunnen leggen aan toezichthouders en andere belanghebbenden. Onderdeel hiervan zijn:

* **Centraal risicoregister**: Alle geïdentificeerde risico’s (met ten minste de informatie-, privacy- en IT-gerelateerde risico's) worden vastgelegd met bijbehorende classificaties, beheersmaatregelen en evaluatiemomenten.
* **Formele rapportagestructuren**: Risicorapportages worden opgenomen in de planning- en controlcyclus en periodiek besproken op managementniveau.
* **Risicobehandelplannen**: met per risico de uit te voeren verbeteracties met bijbehorend benodigde budgetten, besluiten etc., in beheer bij de risico-eigenaar.
* **Integratie met ISMS**: Risico’s en maatregelen die betrekking hebben op informatiebeveiliging worden opgenomen in het Information Security Management System (ISMS) om consistentie en naleving van ISO 27001 te waarborgen.
* **Continue verbetering**: Op basis van registraties en rapportages wordt het risicomanagementproces periodiek geëvalueerd en waar nodig aangepast.

De CISO rapporteert via zijn Management Rapportage (MARAP) op strategisch niveau aan het CvB over het risicoprofiel van de onderwijsinstelling, de werking van beheersmaatregelen en status van verbeteracties;

De CISO rapporteer drie (3) keer per jaar, synchroon met overige bestuurlijke rapportage cycli aan het CvB en zo nodig ad hoc indien het risico dit naar mening van de CISO vereist.

## Planning en Control Cyclus

Risicomanagement is een integraal onderdeel van de bestuurlijke en operationele aansturing van de instelling. Het is nauw verweven met de planning- en controlcyclus en maakt deel uit van het Information Security Management System (ISMS). Dit waarborgt een continue evaluatie en verbetering van het risicomanagementproces volgens de Plan-Do-Check-Act (PDCA)-cyclus.

**Periodieke evaluatie en review**

* Het risicoregister wordt periodiek beoordeeld door de CISO en GRC-officer. Hierbij worden niet alleen openstaande risico’s geanalyseerd, maar worden ook eerder geaccepteerde risico’s herzien in het licht van nieuwe ontwikkelingen, zoals veranderende dreigingen, technologische innovaties en aanpassingen in wet- en regelgeving.
* Minimaal eens per jaar worden strategische risico’s en bijbehorende scenario’s besproken. Hierbij wordt ook geëvalueerd hoe tactische en operationele risico’s worden beheerst en welke maatregelen nodig zijn om risico’s effectief te mitigeren.

**Bestuurlijke informatievoorziening**

* Het College van Bestuur (CvB) ontvangt minimaal eens per vier (4) maanden een update over de tactische en operationele risico’s binnen de instelling.
* De strategische risico’s die de doelstellingen en continuïteit van de instelling kunnen beïnvloeden, worden regelmatig besproken in het CvB en de Raad van Toezicht.
* Tactische rapportages over informatiebeveiliging worden opgenomen in de verantwoordingsgesprekken van faculteits- en instituutsdirecteuren met het CvB, zodat risico’s tijdig worden gesignaleerd en beheerst.

# Vaststelling

Dit document is aldus vastgesteld.

[PLAATS], [DATUM].

[College van Bestuur]

<Na (her)vaststelling, ook de tabel op p.2 bijwerken>

1. Verklarende woordenlijst

|  |  |
| --- | --- |
| Actiehouder | Door de risico-eigenaar aangewezen persoon verantwoordelijk voor de uitvoering van acties om risico’s te behandelen. |
| Monitoren en beoordelen | Het omvat het plannen, verzamelen en analyseren van informatie, het vastleggen van uitkomsten/resultaten en het geven van feedback. |
| Registratie en Rapportage | De registratie en de rapportage (en de controle hiervan) moeten in alle fasen van het risicoproces plaatsvinden. Rapportage is een integraal onderdeel en moet de kwaliteit van de dialoog met belanghebbenden verbeteren en het bestuur ondersteunen bij het nakomen van de aan hen toegeschreven verantwoordelijkheden. |
| Risicoanalyse | Het achtereenvolgens begrijpen van de aard, de kenmerken en het niveau van verschillende (typen) risico’s. Het omvat een gedetailleerde afweging van onzekerheden, risicobronnen, gevolgen, waarschijnlijkheden, gebeurtenissen, scenario's, controles en de effectiviteit ervan. |
| Risicobehandeling | Het selecteren en implementeren van opties voor het aanpakken van risico's. De opties zijn: elimineren (vermijden), reduceren (mitigeren), verleggen (overdragen) en accepteren. |
| Risicobeoordeling | Het totale proces van risico-identificatie, risicoanalyse en risico-evaluatie. |
| Risicobereidheid | Andere benaming: Risk appetite. De hoeveelheid risico die de onderwijsinstelling als aanvaardbaar beschouwt. Risico’s onder deze waarde kunnen zondermeer geaccepteerd worden (tenzij er sprake van stapeling is). |
| Risicoclassificatie | Een methode voor het wegen van risico’s op basis van hun waarschijnlijkheid en potentiële impact. |
| Risico-eigenaar | De functionaris binnen de onderwijsinstelling die verantwoordelijk is voor het behandelen van een risico. Veelal zal de eigenaar van een IT-omgeving of proces ook de risico-eigenaar zijn van de risico’s binnen deze omgeving. De risico-eigenaar is vaak iemand in de business. |
| Risico-evaluatie | Betreft het ondersteunen van beslissingen aan de hand van het vergelijken van de resultaten van de risicoanalyse met de vastgestelde risicocriteria. Op basis van deze vergelijkingen kunnen waar nodig aanvullende maatregelen worden getroffen of al bestaande maatregelen worden aangepast. |
| Risico-houding | Wat vind je van die risico’s (die uit de risico-perceptie komen). |
| Risico-identificatie | Het vinden, herkennen en beschrijven van risico's die kunnen voorkomen dat een organisatie haar doelstellingen bereikt. |
| Risico-stapeling | Risico-stapeling vindt plaats wanneer een al geïdentificeerd risico een versterkend effect heeft op het risico dat de risico-eigenaar aan het beoordelen is. Hierdoor wordt de eventuele impact en/of kans van het risico verhoogd en is een ander risiconiveau wellicht passender. |
| Risico-perceptie | Welke risico’s zien we? |
| Risicotolerantie | Risico’s boven de risicobereidheid die de instelling onder bepaalde omstandigheden is bereid te accepteren. Alles boven de tolerantie dient aangepakt te worden. |
| Risk appetite | Zie Risicobereidheid.  Zien we als de resultante van de risico-perceptie (welke risico’s zie je?) en de risicohouding (wat vind je van die risico’s?).Hoe hoger het risico is hoe minder de organisatie dat risico zal aanvaarden, en hoe lager de risk appetite. Bij een Kritiek risico zal de organisatie het risico direct willen oplossen. Aan de andere kant: bij een Laag risico is het oplossen optioneel of laat men het as-is (hoge risk appetite). |

1. <https://sec.surf.nl/cyberdreigingsbeeld-2024-lessen-en-actiepunten-na-tien-jaar-cyberdreigingen-in-onderwijs-en-onderzoek/> [↑](#footnote-ref-1)
2. <https://pec.surf.nl/het-uitvoeren-van-een-dpia-hoe-doe-je-dat/> [↑](#footnote-ref-2)