Samen aanjagen van vernieuwing

# Handreiking

## Verantwoording over Cybersecurity in jaarverslagen

Auteur(s): Jeroen Schuuring, Albert Hankel
Versie: 1.0
Datum: 29 februari 2024
Kenmerk: ---

Deze handreiking wordt u aangeboden door de koepelorganisaties Vereniging Hogescholen (VH), Universiteiten van Nederland (UNL) en de MBO Raad in samenwerking met SURF. Deze handreiking is een resultaat van voorheen het programma Integrale Veiligheid Hoger Onderwijs, een platform van HO-instellingen die samenwerken om instrumenten te verzamelen of te ontwikkelen en kennis en ervaringen delen om grip te krijgen en te houden om goed voorbereid te zijn op incidenten en veiligheidsrisico's.

**Heeft u vragen?**
Mocht u vragen hebben of ondersteuning willen bij het implementeren of toepassen van de ontwikkelde instrumenten, dan kunt u een beroep doen op collega-instellingen, bijvoorbeeld de coördinatoren Integrale Veiligheid.

# Inhoudsopgave

# 1 Inleiding

Volgens de codes voor goed bestuur rapporteren de Raden van Toezicht/commissarissen over de werking van het risicomanagementsysteem in het jaarverslag. Binnen dat risicomanagementsysteem vormt cybersecurity een specifieke categorie.

Tussen de koepelorganisaties Vereniging Hogescholen (VH), Universiteiten van Nederland (UNL) en de MBO Raad en het Ministerie van OCW is afgesproken om in de verslaglegging aandacht te besteden aan cybersecurity. Tevens is afgesproken ter ondersteuning te komen met een handreiking Verantwoording cybersecurity in jaarverslagen.

Deze 'Handreiking Verantwoording cybersecurity in jaarverslagen' biedt handvatten aan instellingen bij de verslaglegging van de verantwoording omtrent cybersecurity in de risicoparagraaf in jaarverslagen. De handreiking voorziet in een minimale set aan vragen die inzicht geven in (de zelfevaluatie van) de cyberweerbaarheid van instellingen. Bij het opstellen van deze handreiking is er zoveel als mogelijk rekening gehouden met het vertrouwelijke karakter van de gevraagde informatie. De handreiking is niet voorschrijvend.

## 1.1 Achtergrond risicomanagement in jaarverslagen

Organisaties behoren in hun jaarverslag een beschrijving op te nemen van de voornaamste risico's en onzekerheden waarmee ze worden geconfronteerd. Het gaat daarbij niet om een uitputtende uiteenzetting van alle mogelijke risico's en onzekerheden, maar om een selectie en de weergaven van de belangrijkste risico's en onzekerheden waarvoor de organisatie zich geplaatst ziet. Hierbij kan aandacht worden besteed aan:

1. Risico's die in het afgelopen boekjaar een belangrijke impact hebben gehad;
2. De bereidheid om risico's en onzekerheden al dan niet af te dekken;
3. Getroffen maatregelen om risico's te beheersen, of een verklaring waarom er geen maatregelen zijn genomen om een groot risico te beheersen;
4. Verwachte impact van risico's op de resultaten of financiële positie;
5. Verbeteringen die in het systeem van risicomanagement zijn of worden aangebracht; en
6. Een toelichting op de verankering van het systeem van risicomanagement in de organisatie en de genomen maatregelen ter beïnvloeding van de cultuur, het gedrag en de motivatie van medewerkers.[1]

[1] Paragraaf overgenomen uit "Risicomanagement voor bestuurders en toezichthouders", Carla van der Weerdt-Norder, Alice Jansen-van den Tillaart en Frank van Egeraat.

## 1.2 Definitie verantwoording cybersecurity in jaarverslagen

De definitie van verantwoording van cybersecurity is als volgt:

> *"De verantwoording over de status van informatieveiligheid en verantwoording over hoe informatieveiligheid is opgenomen in de professionele en continue cyclus van integraal risicomanagement en governance."*

Cybersecurity is dan ook een onderdeel van de verantwoording over risico's in het algemeen. Daarmee kan voor dit deel van de verantwoording aangesloten worden bij de onderdelen die bovenstaand zijn genoemd.

## 1.3 Scope Handreiking verantwoording cybersecurity in jaarverslagen

De handreiking beperkt zich tot het formuleren van een aantal vragen die door de instellingen beantwoordt kunnen worden in de jaarverslagen. Hiermee geeft het richting op welke wijze de instelling kan rapporteren over cybersecurity en de bijbehorende risico's.

Met de handreiking worden instellingen geholpen om een praktische invulling te geven aan de eisen voor de risicorapportage uit de branchecodes voor goed bestuur. Het is aan instellingen zelf om te bepalen op welke wijze de verantwoording daadwerkelijk vormgegeven wordt.

# 2 Uitwerkingsvragen verantwoording cybersecurity in jaarverslagen

Om te kunnen voldoen aan de invulling van de gemaakte afspraken tussen de koepelorganisaties en het Ministerie van OCW voor de cyberverantwoording in jaarverslagen is ervoor gekozen een aantal vragen te formuleren die door de instellingen uitgewerkt kunnen worden. Het doel hiervan is overzichtelijkheid en eenduidigheid te creëren voor de verschillende belanghebbenden.

De cyberverantwoording wordt veelal gedaan in de risicoparagraaf in jaarverslagen. Een alternatief is het terug te laten komen als integraal deel van de beschrijving van andere onderdelen in het jaarverslag. Benoem in beide gevallen de cybersecurity risico's en maatregelen expliciet. De mate van diepgang en omvang van de verantwoording is ter beoordeling van de instellingen. Opgemerkt wordt dat in de beschrijving van de risico's vermeden moet worden om te specifieke informatie te geven waarmee een kwaadwillende (zoals cybercriminelen) inzicht krijgen in waar exact zwakke plekken in de organisatie zich bevinden. De organisatie dient telkens de balans te vinden tussen het geven tussen het gewenste inzicht voor de verantwoording versus ongewenst inzicht waar een kwaadwillende voordeel aan heeft.

Instellingen kunnen bij de verantwoording verwijzen naar initiatieven en/of jaarprogramma's/verbeterprogramma's die voorzien in de groei en ontwikkeling naar cybervolwassenheid, zonder daarbij details van de aanpak, invulling en het actuele niveau van cybervolwassenheid vrij te geven.

## 2.1 Handreiking te beantwoorden vragen

De volgende vragen kunnen als leidraad gebruikt worden voor het invullen van de risicoparagraaf voor cybersecurity:

1. Welke cybersecurityrisico's hebben zich het afgelopen jaar gemanifesteerd en/of hebben een belangrijke impact gehad?
2. Welke risicobereidheid heeft de organisatie ten aanzien van cybersecurity?
3. Welke maatregelen zijn het afgelopen jaar getroffen om cybersecurityrisico's te beheersen?
4. Wat is de verwachte impact als bepaalde cybersecurityrisico's zich manifesteren?
5. Welke verbeteringen zijn of worden in het systeem van risicomanagement aangebracht?
6. Op welke wijze zijn cybersecurityrisico's verankerd in het systeem van risicomanagement in de organisatie en welke maatregelen zijn genomen ter beïnvloeding van de cultuur, het gedrag en de motivatie van medewerkers?

## 2.2 Voorbeelden beantwoording vragen

Ter inspiratie worden enkele voorbeelden gegeven van (deel)antwoorden op de te beantwoorden vragen.

Ad 1: Welke cybersecurityrisico's hebben zich het afgelopen jaar gemanifesteerd en/of hebben een belangrijke impact gehad?

*In het afgelopen jaar hebben we een verhoogd aantal phishingaanvallen geconstateerd. Als gevolg hiervan zijn er inloggegevens buit gemaakt. Door een verplichte reset van wachtwoorden voor alle studenten en medewerkers lijkt de impact op de instelling beperkt: er is geen misbruik van de buitgemaakte inloggegevens geconstateerd en/of gemeld.*

Ad 2: Welke risicobereidheid heeft de organisatie ten aanzien van cybersecurity?

*Onze instellingen is een open instelling: wij verwelkomen dagelijks vele (gast)studenten en (gast)medewerkers. Het moet laagdrempelig zijn om geoorloofd gebruik te maken van onze infrastructuur. Deze openheid koesteren we en willen we behouden. Gevolg is dat we weten dat ook een kwaadwillende gebruik kan maken van deze open houding. We accepteren dat we daarom meer moeten doen in het detecteren van mogelijk misbruik en het daarop acteren. Ter bescherming van ons imago vinden wij het belangrijk om adequaat te reageren op dreigingen. Vandaar dat we bewust hebben geïnvesteerd in onze medewerkers, onder andere door meer vaste contracten aan te bieden en de formatie te vergroten. De financiële risico's die hieruit voort komen accepteren we bewust.*

Ad 3: Welke maatregelen zijn het afgelopen jaar getroffen om cybersecurityrisico's te beheersen?

*We hebben een projectteam ingericht om op alle controls door te ontwikkelen naar niveau 3 van het SURFaudit-toetsingskader. Hier zijn goede resultaten geboekt, wat tot een hogere positie in de benchmark heeft geleid. Daarnaast hebben we de capaciteit van het security operations center uitgebreid om meer aandacht aan monitoring en opvolging te kunnen geven. Tot slot heeft een rationalisatie van oude servers plaatsgevonden, waarmee kwetsbaarheden verminderd zijn.*

Ad 4: Wat is de verwachte impact als bepaalde cybersecurityrisico's zich manifesteren?

*Vanuit het cyberdreigingsbeeld zien we dat onze sector nog steeds onder vuur ligt van cybercriminelen die zich richten op ransomware. Een geslaagde aanval kan grote disruptieve gevolgen tot gevolg hebben waarbij ons primaire proces enige tijd stil kan liggen en er grote investeringen nodig zijn voor herstel.*

Ad 5: Welke verbeteringen zijn of worden in het systeem van risicomanagement aangebracht?

*Er is in het afgelopen jaar een interdisciplinair team ingericht dat regulier alle risico's naloopt en waar nodig aanvullende maatregelen bespreekt. Veel aandacht is besteed aan informatiebeveiliging en de bescherming van persoonsgegevens. Dit uitte zich onder meer in het borgen van 'privacy by design' bij (nieuwe) processen en het uitvoeren van een Data Protection Impact Assessment (DPIA) als onderdeel van het (her)inrichten van bedrijfsprocessen. Tevens is het register van verwerkingsactiviteiten geactualiseerd.*

Ad 6: Op welke wijze zijn cybersecurityrisico's verankert in het systeem van risicomanagement in de organisatie en welke maatregelen zijn genomen ter beïnvloeding van de cultuur, het gedrag en de motivatie van medewerkers

*Cybersecurity is opgenomen als een van de aandachtgebieden binnen de integrale risicomanagementaanpak die gehanteerd wordt. Hierbij wordt uitgegaan van het ISO 31000 Risk Management Framework. Daarbij hanteren wij het Three Lines model. Er wordt rechtstreeks gerapporteerd aan de CvB over de risico's en de genomen maatregelen. Er is een team dat actief reageert op incidenten. Ten minste éénmaal per jaar wordt meegedaan aan een grote oefening waar ook bestuurders aan deelnemen. Richting medewerkers is een anti-phishing campagne uitgevoerd en wordt aangestuurd op het rapporteren van verdachte zaken.*