In de UNL SBF vergadering van 16 april 2021 is afgesproken dat alle universiteiten elk jaar en hbo-instellingen eens per twee jaar een volwassenheidsmeting (zogeheten 'SURF audit') laten uitvoeren door een externe auditor. Om vergelijkbaarheid tussen instellingen te waarborgen en om ook volgende volwassenheidsmetingen ermee te kunnen vergelijken, hebben de CISO’s van de hogeronderwijsinstellingen een auditmethodiek opgesteld, te weten 'Auditmethodiek Informatieveiligheid WO' en 'Auditmethodiek Informatieveiligheid HBO'.

In de praktijk is gebleken dat de auditmethodiek op een aantal thema’s onvoldoende handvatten biedt, waardoor de SURF audit niet op een uniforme en vergelijkbare wijze wordt uitgevoerd en kwaliteit van de uitgevoerde externe onderzoeken verschilt. Deze thema’s betreffen onder meer:

* Scoping van systemen, normen en scoringsmethodiek
* Risicogebaseerd vs. Rule based beoordelen
* De wens om SURF audits efficiënter uit te kunnen voeren, zodat de ‘auditlast’ voor zowel auditor als audittee verminderd.
* Onduidelijkheid over informatielast per maatregel op basis van het toetsingskader

Dit memo betreft een aanvullende handreiking op de auditmethodiek zoals uitgebracht door SURF. Middels dit memo worden op de bovenstaande thema’s handvatten gegeven die auditor en auditee in staat kunnen stellen om op een meer uniforme en vergelijkbare wijze kwalitatief hoogwaardige SURF audits uit te (laten) voeren. Iedere SURF audit blijft echter maatwerk. Onderwijs- en onderzoeksinstellingen en externe auditpartijen zijn niet verplicht deze handreiking te hanteren.

# Scoping van systemen, normen en scoringsmethodiek

## Scoping van systemen en normen

In document [SURF - Audithandreiking scoping normen.xlsx] is een handreiking opgesteld om voor de systemen in scope handvatten te geven welke normen op welk niveau beoordeeld kunnen worden. In dit document staat in een advies beschreven:

* De handreiking van SURF inzake de selectie van systemen in scope op basis van relevantie
* Welke systeemlagen per type systeem in scope van het onderzoek op te nemen
* Welke normen per systeemlaag in scope van het onderzoek op te nemen

## Scoringsmethodiek

Voor het uniform toekennen van de scores gelden de uitgangspunten zoals beschreven in de auditmethodiek WO en HBO, te weten:

* Het volwassenheidsniveau wordt alleen toegekend indien aan alle eisen voor dat niveau aantoonbaar is voldaan. Indien dat niet het geval is wordt de score van het voorliggende volwassenheidsniveau toegekend. Er worden geen halve punten toegekend.
* Het eindcijfer per domein/cluster en het overall eindcijfer wordt afgerond op één tiende punt.
* Het gemiddelde eindcijfer wordt berekend door het optellen van alle resultaten van de individuele norm, gedeeld door het aantal normen in scope (dus niet door het optellen van de domein/cluster scores gedeeld door het aantal domeinen/clusters).

Deze uitgangspunten geven echter geen duidelijkheid over de scoringsmethodiek per systeem en systeemlaag. Voor het bieden van deze duidelijkheid is in document [SURF - Audithandreiking scoringsmethodiek.xlsx] een voorbeeld opgesteld hoe de scoringsmethodiek in de praktijk toegepast dient te worden.

# Richtlijnen voor het efficiënt uitvoeren van de SURF audit

Door de onderwijs- en onderzoeksinstellingen is in de evaluatie aangegeven dat de hoeveelheid aan informatie dat dient te worden aangeleverd als zeer omvangrijk wordt ervaren. Daarnaast maken steeds meer instellingen gebruik van een centrale (GRC) tool voor het uitvoeren en vastleggen van self-assessments, maar wordt hier tot op heden nog (te) weinig gebruik van gemaakt. Dit komt enerzijds door de onbekendheid van de externe auditor met de door de instelling gebruikte tooling. Anderzijds wordt door instellingen vaak minder gedocumenteerd en geregistreerd in de tool dan de externe auditor nodigt heeft om een bepaald volwassenheidsniveau vast te kunnen stellen.

Om de SURF audits efficiënter uit te voeren en de auditlast te verminderen kan de externe auditor in overleg met de te onderzoeken instelling de volgende richtlijnen hanteren:

* Na het afstemmen van de scope van systemen en normen voert de instelling een self-assessment uit. Dit self-assessment kan worden geregistreerd in een (GRC) tool van de betreffende instelling, of met behulp van een template aangeleverd door de externe auditor.
* Het is de verantwoordelijkheid van de te onderzoeken instelling om een kritische zelf-evaluatie uit te voeren en de benodigde informatie zorgvuldig vooraf te verzamelen en ter beschikking te stellen. Voor zover er overlap bestaat tussen de scope en reikwijdte van deze externe audit met andere uitgevoerde audits, mag de instelling in overleg met de externe auditor dezelfde auditinformatie ter beschikking stellen. Daarbij worden instellingen geadviseerd om expliciet te controleren of voor alle vereisten behorende bij het aangegeven volwassenheidsniveau informatie is aangeleverd om dit in opzet, bestaan en werking aan te kunnen tonen. Enkel het hebben van beleid is bijvoorbeeld niet toereikend voor volwassenheidsniveau 3.
* Als de instelling gebruik maakt van een (GRC) tool voor de vastlegging van informatie om het aangegeven volwassenheidsniveau aan te tonen, beoordeelt de externe auditor deze informatie op juistheid en volledigheid. Wanneer de in de (GRC) tool opgeslagen informatie ontoereikend is, communiceert de externe auditor met de instelling welke informatie nog mist om het betreffende volwassenheidsniveau vast te kunnen stelllen (zie volgende bullit).
* Op basis van het self-assessment en eventueel reeds ontvangen informatie via een (GRC) tool stelt de externe auditor een informatieverzoek op. Voor volwassenheidsniveau 1 is over het algemeen geen tot zeer beperkte informatie benodigd en voor volwassenheidsniveau 2 beperkte informatie. Voor volwassenheidsniveau 3 of hoger is vaak meer en diepgaandere informatie benodigd om aantoonbaar dit volwassenheidsniveau te kunnen behalen.
* Wanneer instellingen de auditlast als te veel ervaren en niet in staat zijn de gevraagde informatie tijdig op te leveren, kunnen zij in overleg met de externe auditor ervoor kiezen om de benodigde informatie met de auditor te verzamelen. Alhoewel dit vaak tijdsintensiever is voor de externe auditor, verhoogt dit de kwaliteit van de opgeleverde informatie (de auditor weet immers goed wat benodigd is) en verlaagt dit de doorlooptijd voor de instelling.
* Voor instellingen die eerder een externe audit hebben laten uitvoeren, kan met de volgende werkwijze efficiency worden behaald:
  + De instelling geeft op basis van de resultaten van vorig jaar middels een self-assessment aan voor welke normen verbeteringen zijn gerealiseerd en voor welke normen de situatie en het volwassenheidsniveau gelijk is aan het voorgaande jaar.
  + Voor alle normen met een maximum volwassenheidsniveau van 2 en waarvoor de instelling aangeeft geen verbeteringen te hebben gerealiseerd, hoeft geen nieuwe beoordeling uitgevoerd te worden. De externe auditor mag gebruik maken van de informatie van het voorgaande jaar.
  + Voor alle normen met een volwassenheidsscore van 3 of voor de normen waarvoor de instelling aangeeft verbeteringen te hebben gerealiseerd, wordt door de externe auditor een beoordeling uitgevoerd om vast te stellen dat aan het betreffende volwassenheidsniveau is voldaan.

# Risicogebaseerde aanpak bij het vaststellen van de volwassenheid

## Een toelichting op het door SURF gekozen volwassenheidsmodel

Het SURFaudit toetsingskader 2021 is gebaseerd op het door de NBA opgestelde volwassenheidsmodel Informatiebeveiliging v2.0. Dit model is ontwikkeld om bij te dragen aan de bewustwording over informatiebeveiliging en organisaties te helpen om het volwassenheidsniveau te realiseren dat past bij de betreffende organisatie.

Ten behoeve van een succesvolle toepassing van het volwassenheidsmodel dient een aantal (rand)voorwaarden in ogenschouw te worden genomen:

* Het vaststellen van het gewenste volwassenheidsniveau wordt met name bepaald door de aard van de activiteiten van de organisatie en haar processen, soort gegevens van de organisatie, de beschikbare applicaties en infrastructuur en dreigingen. Daarnaast zijn specifieke risico’s en is de risicobereidheid van de organisatie bepalend hoe hoog de lat voor de organisatie moeten liggen. Ondanks dat de onderwijssector met OCW heeft afgesproken een gemiddeld volwassenheidsniveau van 3 na te streven, blijft het de verantwoordelijkheid van iedere instelling om op basis van genoemde factoren het risico en bijbehorende niveau van maatregelen vast te stellen.
* Doordat veel organisaties delen van hun informatievoorziening en/of –verwerking hebben uitbesteed of afhankelijk zijn van derde partijen, dient er expliciet aandacht te worden besteed aan de afhankelijkheden van en samenwerking met business partners in de keten. Dit vergt ook een goede afstemming van de verschillende volwassenheidsniveaus binnen de keten.
* Per organisatie kan de van toepassing zijnde wet & regelgeving verschillend zijn. Het model wijst op de compliance met verplichte wet & regelgeving, echter deze zijn niet specifiek uitgewerkt en kunnen op onderdelen bepalend zijn voor de hoogte van de meetlat.

Om tot het (indicatief) gewenste volwassenheidsniveau te komen, moeten er vanuit de organisatie specifieke context (kansen en risico’s) onderbouwde keuzes worden gemaakt om bepaalde maatregelen wel of niet te treffen (“comply or explain”). Bij het uitvoeren van een dergelijke risico analyse dient rekening te worden gehouden met de organisatie, processen, systemen en data. Zo kent niet elk organisatieonderdeel of elk systeem dezelfde risico’s. Op basis van deze risico inschatting biedt het model te verwachten beheersingsmaatregelen per volwassenheidsniveau. In onderstaand schema is weergegeven hoe de inschatting van de risico’s kan worden gekoppeld aan het benodigde niveau van beheersmaatregelen.

|  |  |  |
| --- | --- | --- |
| Score | Risico-inschatting | Indicatie voor volwassenheidsniveau |
| N.V.T. | Niet van toepassing | Niet van toepassing |
| 1 | Nihil | Laag |
| 2 | Beperkt – ruim binnen risicobereidheid | Beperkt |
| 3 | Gemiddeld – net binnen / buiten risicobereidheid | Gemiddeld |
| 4 | Aanzienlijk – buiten risicobereidheid | Meer dan gemiddeld |
| 5 | Hoog – ruim buiten risicobereidheid | Hoog |

## De volwassenheidsniveaus en indicatieve criteria

Om een handreiking te geven bij de consistente toetsing van het actuele volwassenheidsniveau zijn vijf volwassenheidsniveaus gedefinieerd en nader uitgewerkt. Op basis van vijf beschrijvingen (van redelijkerwijs te verwachten beheersingsmaatregelen) kan worden bepaald welk volwassenheidsniveau per norm van toepassing is. Per norm zijn de vijf indicaties van volwassenheidsniveaus op basis van een aantal criteria nader uitgewerkt. De volgende vijf niveaus als mede de volgende bijbehorende leidende criteria zijn hierbij onderkend:

|  |  |  |  |
| --- | --- | --- | --- |
| Niveau | Naam | Omschrijving | Indicatieve criteria |
| 1 | Initieel | Beheersingsmaatregelen zijn niet of gedeeltelijk gedefinieerd en/of worden op inconsistente wijze uitgevoerd. Grote afhankelijkheid van individuen. | * Geen of beperkte controls geïmplementeerd. * Niet of ad-hoc uitgevoerd. * Niet /deels gedocumenteerd. * Wijze van uitvoering afhankelijk van individu. |
| 2 | Herhaalbaar | Beheersingsmaatregelen zijn aanwezig en worden op consistente en gestructureerde, maar op informele wijze uitgevoerd. | * Control is geïmplementeerd. * Uitvoering is consistent en standaard. * Informeel en grotendeels gedocumenteerd. |
| 3 | Gedefinieerd | Beheersingsmaatregelen zijn gedocumenteerd en worden op gestructureerde en geformaliseerde wijze uitgevoerd. De uitvoering is aantoonbaar en wordt getoetst. | * Control gedefinieerd o.b.v. risico assessment. * Gedocumenteerd en geformaliseerd. * Verantwoordelijkheden & taken toegewezen. * Aantoonbare effectieve werking. * Rapportage van uitvoering van beheersingsmaatregel aan management. * Effectieve werking van controls wordt periodiek getoetst. * De toetsing toont effectiviteit control aan. |
| 4 | Beheerst en meetbaar | De effectiviteit van de beheersingsmaatregelen wordt periodiek geëvalueerd. | * Periodieke (control) evaluatie en opvolging vindt plaats en evaluatie is gedocumenteerd. * Frequentie waarop wordt geëvalueerd is gebaseerd op het risicoprofiel van de onderneming en is minimaal jaarlijks. * Rapportage van evaluatie aan management. |
| 5 | Continu verbeteren | De beheersingsmaatregelen zijn verankerd in het integrale risicomanagement raamwerk, waarbij continu gezocht wordt naar verbetering. | * Continu evalueren van de maatregelen om de effectiviteit te verbeteren. Gebruik makend van resultaten uit Self-assessment, gap en root cause analyses. * De getroffen beheersingsmaatregelen worden gebenchmarkt en zijn ‘Best Practice’ in vergelijking met andere organisaties. * Real time monitoring. * Inzet automated tooling. |

De voorbeelden van maatregelen en volwassenheidsniveaus zijn niet statisch. Ontwikkelingen in ICT en beheersingsmaatregelen kunnen ertoe leiden dat voorbeelden die momenteel gezien worden als “best-practice”, op een later moment niet meer volstaan voor het betreffende volwassenheidsniveau. De voorbeelden van maatregelen zijn derhalve indicatief. Het is voor externe auditors aan te bevelen naast de gegeven voorbeelden in het SURF toetsingskader ook bovenstaande indicatieve criteria te hanteren voor het vaststellen van het volwassenheidsniveau. Wel geldt dat aan alle criteria dient te worden voldaan om aan het betreffende volwassenheidsniveau te voldoen. Enkel wanneer kan worden onderbouwd waarom een voorbeeldmaatregel of indicatief criterium niet bijdraagt aan het verlagen van het risico, hoeft niet aan het betreffende criterium te worden voldaan (comply or explain).