Samen aanjagen van vernieuwing

Bijlage B

User stories GRC-applicatie

Auteur(s): Projectgroep GRC-applicatie

Versie: 1.0
Datum: 22 juni 2023
Kenmerk: User stories GRC-applicatie

Inhoudsopgave

1 Opzet van de GRC-applicatie

In dit hoofdstuk is de beoogde opzet, het functioneel gebruik, van de GRC-applicatie beschreven.

1.1 Information Security Management System als proces

De borging van informatieveiligheid is gebaseerd op het uitvoeren van het (organisatorische) risicomanagementproces dat is gekoppeld aan beleid en duidelijk omschreven taken, bevoegdheden en verantwoordelijkheden. Voor het verbeteren van informatieveiligheid binnen mbo, ho en wo wordt op dit moment gebruik gemaakt van de standaard set aan beheersmaatregelen uit het NBA-LIO model voor volwassenheidsmodel voor Informatiebeveiliging van de Nederlandse Beroepsorganisatie voor Accountants (NBA-model), welke door SURF is vertaald in het SURFaudit Toetsingskader Informatiebeveiliging. Het SURFaudit Toetsingskader wordt gebruikt om de volwassenheid op het gebied van informatiebeveiliging voor een instelling te “meten”. De controle over de effectiviteit van de beheersmaatregelen is vervat in de plan-do-check-act cyclus waarmee de opzet, bestaan en werking van het risicomanagementproces wordt geborgd. Dit organisatieproces wordt aangeduid met het Informatie Security Management Systeem (ISMS) dat kan worden ondersteund met een Governance, Risk en Compliance-applicatie, kort GRC-applicatie. Het leveren van de GRC-applicatie is het onderwerp van deze uitvraag. Aanbieders wordt gevraagd een softwarematige oplossing (SAAS gebaseerde GRC-applicatie) te bieden waarmee besproken functionaliteit van de User Stories wordt ondersteund.

1.2 SURFaudit Toetsingskader voor Informatiebeveiliging

Binnen het mbo en het hoger onderwijs is een overstap gemaakt van een toetsingskader gebaseerd op de ISO 27002 norm naar het NBA-model (Nederlandse Beroepsorganisatie van Accountants), vertaald in het SURFaudit Toetsingskader Informatiebeveiliging. In het model is per onderwerp een opbouw aan beheersmaatregelen opgenomen waarmee het voor gebruikers duidelijker is hoe de groei in volwassenheid kan worden bereikt. Duidelijke prestatie-indicatoren per volwassenheidsniveau maken het meten van de volwassenheid door de instellingen eenvoudig en draagt bij aan een objectieve beoordeling.

Het SURFaudit Toetsingskader is te downloaden door de volgende URL die verwijst naar de SURFNET WIKI: https://wiki.surfnet.nl/display/SA/SURFaudit+Toetsingskader+2021

Volwassenheidsmeting in het SURFaudit Toetsingskader

Het SURFaudit Toetsingskader bestaat uit 69 beheersdoelstellingen. Elk van deze beheersdoelstellingen dekt een (inherent) risico af dat gekoppeld is aan de informatieveiligheid van de organisatie. Om het risico af te dekken kunnen -*per volwassenheidsniveau*- één of meerdere beheersmaatregelen worden genomen om het risico te mitigeren. In deze zin wijkt het SURFaudit Toetsingskader model af van bijvoorbeeld de ISO27002 norm voor informatieveiligheid die de volwassenheid bepaalt op basis van enkelvoudige beheersmaatregelen die worden gekoppeld aan de score volgens het CMM (Capability Maturity Model). Wanneer voor een statement in het SURFaudit Toetsingskader geldt dat voor volwassenheidniveau 3 moet worden voldaan aan 4 beheersmaatregelen, moeten al deze vier beheersmaatregelen ook daadwerkelijk zijn uitgevoerd alvorens het volwassenheidsniveau is bereikt. De GRC-oplossing dient te kunnen omgaan met deze alternatieve duiding van volwassenheid volgens het SURFaudit Toetsingskader.

1.3 SURFaudit Toetsingskader voor Privacy

Binnen het onderwijs wordt gebruik gemaakt van een toetsingskader privacy voor de borging van de privacy. Het bestaande kader uit 2020 wordt in SURF-verband bijgewerkt naar een nieuwe versie onder de naam SURFaudit Toetsingskader Privacy. Dit toetsingskader is net als andere frameworks uitgewerkt in hoofdthema's en beheersmaatregelen. Hierbij kan ook weer een mapping worden gemaakt naar andere normen en onderliggende wettelijke normen uit de AVG. Het plan is om ook de nieuwe versie van het toetsingskader Privacy op te nemen in de GRC-applicatie zodra deze beschikbaar komt voor het onderwijs.

1.4 SAAS-applicatie

SURF zoekt voor de aangesloten instellingen een GRC-applicatie gebaseerd op het SaaS-model. Als ICT-coöperatie van onderwijs en onderzoek sluit SURF met de leverancier een raamovereenkomst af en zal zorgdragen voor het contract- en leveranciersmanagement. Alle bij SURF aangesloten instellingen kunnen vervolgens, tegen vergoeding, via SURF gebruik maken van GRC-applicatie.
De onderwijskoepels moeten de mogelijkheid hebben om eigen kwaliteitsstandaarden (als het NBA-model) en specifieke documenten (bijvoorbeeld templates of best practices) binnen de eigen onderwijssector beschikbaar te stellen.

1.5 Onderwijsinstellingen zijn eigenaar

Instellingen zijn per definitie eigenaar van hun eigen gegevens. Gegevens over informatie-veiligheid en privacy zijn strikt vertrouwelijk per instelling en de veiligheid van gegevens moet zijn gegarandeerd. Om die reden moeten instellingen zelf kunnen kiezen welke informatie ze delen: met andere instellingen, de koepelorganisatie een externe auditor of SURF.
Een onderwijsinstelling kan zijn onderverdeeld in meerdere organisatorische eenheden, locaties, faculteiten; voor de instelling moet het mogelijk zijn om deze opdeling te maken binnen de GRC-applicatie. Daarbij moet door de instelling ook op geaggregeerd niveau gerapporteerd kunnen worden.
Met betrekking tot het beheer moet de onderwijsinstelling zelf in staat zijn om te bepalen wie toegang krijgen tot welke gegevens van de instelling. Dit geldt ook voor eventuele en tijdelijke beheer- of gebruiksrechten voor koepelorganisaties of SURF. Vanuit de aanbieder van de GRC-applicatie wordt dan ook gevraagd naar een visie over hoe de vertrouwelijkheid van de instellingsgegevens binnen de GRC-applicatie per instelling wordt gegarandeerd.

1.6 Rapportagebehoefte stakeholders

Onderwijsinstellingen hebben te maken met stakeholders waarmee informatie uit de GRC-applicatie moet worden gedeeld. Zo moeten de onderwijskoepels kunnen rapporteren over de ontwikkeling van de staat van informatieveiligheid van de aangesloten instellingen binnen hun eigen sector. Wanneer een koepel (zoals UNL, VH en MBO-Raad) een benchmark-meting uitschrijft, maakt deze afspraken met de aangesloten instellingen op welke manier de resultaten van hun instelling vanuit de GRC-applicatie worden gedeeld met de koepel en/of SURF.
Informatie zal veelal in de vorm van rapportages worden gedeeld waarbij de instelling zelf moet kunnen bepalen welke informatie (rapportage op basis van een selectie) wordt gedeeld met welke stakeholder (persoon of instelling) en met welke frequentie (bijvoorbeeld eenmalig, periodiek, op verzoek). Het is daarbij belangrijk dat geselecteerde parameters van rapportages kunnen worden opgeslagen zodat rapporten niet opnieuw samengesteld hoeven worden als eenzelfde rapportage of een variant met een kleine aanpassing in de parameters wordt gevraagd.

2 GRC-applicatie binnen de instellingen

Voor de beschrijving van de GRC-applicatie wordt uitgegaan van de user stories voor een drietal instellingen. Het verschil tussen de instellingen kan bestaan uit de complexiteit van de organisatiestructuur die bij universiteiten en hbo-instellingen vaak een grotere gelaagdheid kent ten opzichte van kleinere mbo-instellingen.

Voortbouwend op eerdere ervaring met GRC-applicaties binnen het onderwijs zijn de volgende aspecten belangrijk voor een goede gebruikersacceptatie:

- De GRC-applicatie moet overzichtelijk zijn in gebruik.
- Er zijn niet te veel muisbewerkingen (klikken) nodig om werkzaamheden uit te voeren.
- Er moet niet veel verplichte informatie / overhead worden ingevuld om bijvoorbeeld risico's aan te maken of taken toe te wijzen aan actiehouders.
- De getoonde functionaliteit is aanpasbaar naar de wensen van de instelling die soms minder functionaliteit (modules) wil gebruiken dan de applicatie kan bieden.

2.1 User story 1: Het Simpelveld College

Het Simpelveld College is een kleinere onderwijsinstelling. De ISO-rol is belegd bij de netwerkbeheerder. Door de veelheid van werkzaamheden komt zijn taak als ISO onder druk te staan. Hij doet wat hij kan.

Het Simpelveld College doet evenals alle andere onderwijsinstellingen mee aan de jaarlijkse SURF benchmark. In de eerste plaats omdat dat binnen SURF en met de koepels zo is afgesproken, maar de ISO ziet inmiddels ook voordelen voor zijn eigen werk: de benchmarkresultaten zijn een goede gesprekstarter over IB en P, bijvoorbeeld met zijn collega's IT, HR, Studentenzaken en halfjaarlijks zelfs het bestuur. Het CvB is met name geïnteresseerd hoe het Simpelveld College scoort ten opzichte van het landelijk gemiddelde; ze willen een goede middenmoter zijn. De volwassenheidsniveaus van de 69 statements uit het SURFaudit Toetsingskader Informatiebeveiliging houdt hij bij in een Excel bestand, waarin voor elk volwassenheidsniveau ook de prestatie-indicatoren uit het Toetsingskader zijn opgenomen. Veel statements zijn gescoord op niveau 2 en de ISO heeft voor komend jaar een selectie van statements gemaakt die naar niveau 3 zouden moeten. Deels omdat het quick wins zijn en deels omdat hij vanuit de SURF community heeft begrepen dat deze statements bovengemiddeld belangrijk zijn, omdat we in het algemeen op die gebieden hoge risico's lopen. Het Excel bestand helpt hem bij het bij het definiëren van maatregelen om naar niveau 3 te komen, en hij voegt zijn planning daaraan toe. Het Excel bestand wordt daarmee zijn roadmap, maar hij loopt wel tegen beperkingen van het werken in Excel aan. Om de volwassenheidniveaus te documenteren heeft hij namelijk veel documenten en procedures verzameld en hij wil deze koppelen aan de statements uit het Excel bestand. Daar loopt hij tegen technische beperkingen aan en daardoor hij heeft vaak moeite om de laatste versie van de documenten te kunnen vinden.

Hij was dan ook blij met het SURF-brede initiatief voor een GRC-applicatie. Hij heeft de trainingen gevolgd en had binnen weinig tijd zijn eigen omgeving opgezet. In tegenstelling tot zijn Excel-aanpak biedt de GRC-applicatie wel de mogelijkheden om bewijsmateriaal te koppelen aan de statements uit het toetsingskader. Verder zijn de mogelijkheden om zijn planning te bewaken veel uitgebreider. Hij bewaakt nu nog vooral zijn eigen taken, maar heeft ook al een taak uitgezet naar zijn collega IT, voor het beoordelen en verder uitwerken van het model back-up-beleid.

Hij heeft bij de training over het nieuwe GRC ook kennisgemaakt met een meer risico-gebaseerde aanpak, waarbij je belangrijke risico's kunt documenteren in het systeem en deze koppelt aan een of meerdere maatregelen. Je vult daarbij de weging van het risico aan in termen van kans en impact. Ook leg je de gewenste mitigerende maatregelen vast. Tot slot beoordeel je dan of het restrisico onder de afgesproken waarde voor de risicobereidheid voor het proces ligt. Deze aanpak heeft hij recent toegepast toen uit de SURF IV-metingen naar voren kwam dat de mailserver onvoldoende bescherming bood tegen phishing-mails. Hij begrijpt dat hij tot nu toe vooral bezig is geweest met compliance en is ervan doordrongen dat een meer risico gebaseerde aanpak de organisatie weerbaarder maakt. Met de nieuwe GRC-applicatie ziet hij dat wel zitten.

Omdat het Simpelveld college weinig functionaliteit gebruikt van de GRC-applicatie is het belangrijk dat niet gebruikte functionaliteit in de configuratie per instelling kan worden uitgeschakeld (v.b. incidentmanagement en assetmanagement) en daarmee worden verborgen voor de eindgebruikers. Op die manier kan de instelling met een simpele variant van de GRC-applicatie werken. Op het moment dat het Simpelveld college besluit meer functionaliteit te gebruiken kunnen zij de extra gewenste modules kunnen activeren in het configuratiescherm.

2.2 User story 2: Het Laaglanden College

In deze tweede user story is het Laaglanden College al verder in de ontwikkeling van het volwassenheidsniveau dan het Simpelveld College.

2.2.1 Bedrijfsvoering

Binnen de instelling van het Laaglanden College (Laaglanden) gaat nu ook de vmbo-afdeling meedraaien in het beveiligingsprogramma van de instelling. Voor de vmbo-afdeling is binnen de GRC-applicatie een aparte organisatie-eenheid aangemaakt. De lijnmanager van de vmbo-afdeling heeft in de afdelingsbespreking een aantal nieuwe risico's gesignaleerd en heeft daarbij in het overleg ook een aantal corrigerende maatregelen vastgesteld. Om de risico's te verwerken opent zij de GRC-applicatie en maakt de nieuwe risico's aan. Na overleg met de IBP-functionaris van de instelling weet ze de risico's te koppelen aan de juiste beheersmaatregelen van het SURFaudit Toetsingskader Informatiebeveiliging.

Voor het prioriteren van beheersmaatregelen kijkt de lijnmanager ook naar het huidige en gewenste volwassenheidsniveau van de instelling. Mede op basis van het SURF cyberdreigingsbeeld is door de IBP-manager voor elk van de statements uit het SURFaudit Toetsingskader instellingsbreed de streefvolwassenheid gedefinieerd. Na het uitvoeren van een self assessment voor de vmbo-afdeling wordt duidelijk waar de gap tussen de actuele volwassenheid en de streefvolwassenheid groot is: deze statements krijgen prioriteit en de daarbij behorende maatregelen zullen met voorrang worden uitgevoerd.

Bij het verwerken van gekozen maatregelen wijst ze de inrichting van de maatregelen als taken toe aan betrokken collega's van de instelling en voorziet deze van een deadline (datum). Voor vragen over het invullen van beheersmaatregelen verwijst ze naar de context gevoelige helpfunctie binnen de GRC-applicatie. Ook wijst ze de collega's in het commentaar bij de taak op de templates die zijn gekoppeld aan de beheersmaatregelen. Deze maken het schrijven van procedures eenvoudiger en de kwaliteit van de documenten beter. Betrokken collega's, aan wie taken zijn toegewezen, krijgen vervolgens individueel een berichtje dat ze een taak hebben om uit te voeren gekoppeld aan een deadline.

In het overzicht van mitigerende maatregelen in de GRC-applicatie kijkt de IBP-functionaris van Laaglanden wat de prioriteit en de status is van eerder uitgezette acties. Zichtbaar is dat nieuwe mitigerende maatregelen zijn gekoppeld aan acties en deze zijn met een deadline uitgezet in de organisatie bij medewerkers die verantwoordelijk zijn voor de uitvoering van de actie. Medewerkers waarvan de deadline bijna is verlopen krijgen automatisch een reminder toegestuurd.

Een collega heeft de status van zijn actie op gereed gezet en heeft ter controle een commentaar toegevoegd en beleidsdocument gekoppeld aan de maatregel. Na controle van de maatregel vraagt de IBP-functionaris nog een verandering toe te passen en maakt hiervoor een vervolgtaak aan.

2.2.2 Toevoeging privacy framework

In overleg met de FG is besloten om ook privacy risico's te gaan vastleggen in GRC-applicatie. Het idee is om ook het SURFaudit Toetsingskader Privacy in de GRC-applicatie te laden zodat daar bij privacy risico's naar kan worden verwezen. Daarna kan voor privacy gerelateerde risico's ook de prioritering worden bepaald op basis van kans en impact voor de betrokkene en de instelling.

2.2.3 Jaarlijkse benchmark

De jaarlijkse SURFaudit benchmark is dit jaar ook beschikbaar gesteld in GRC-applicatie. Voor het Laaglanden College betekent dit dat de IBP-functionaris een deel van de beheersmaatregelen nog wil bijwerken voor de deadline van deze benchmark. De benchmark-rapportage wordt na akkoord van de instelling door de GRC-applicatie gegenereerd op basis van de staat van betrokken beheersmaatregelen binnen de GRC-applicatie.

De uitkomst van de SURFaudit benchmark geeft de IBP-functionaris in ieder geval weer een handvat om het onderwerp op de agenda te krijgen voor meer middelen en uren. Zeker als uit de benchmark blijkt dat *Laaglanden College* relatief achterloopt in de ontwikkeling van de volwassenheid van informatieveiligheid binnen de sector.

2.2.4 Managementteamoverleg

Binnen de Laaglanden is de IBP-functionaris o.a. verantwoordelijk voor de beoordeling van het beleid en de procedures. Hij helpt de afdelingen met het invoeren van het GRC en risico-denken. Hiervoor moet veel voorlichtingswerk worden gedaan om afdelingen zelfstandig verantwoordelijk te maken voor het omgaan met risico's. Het kost nodige tijd van de IBP-functionaris maar de aanpak begint zijn vruchten af te werpen.

Deze week sluit de IBP-functionaris aan bij het managementteamoverleg om de status van de informatiebeveiliging binnen Laaglanden door te nemen. Daarbij is vorige week het nieuwe SURF-cyberdreigingsbeeld bekend geworden en deze is door SURF als risico-overzicht met beheersmaatregelen al in de GRC-applicatie geladen voor de instellingen. Hiermee kunnen de instellingen individueel rapporteren op welke gebieden beheersmaatregelen van het SURFaudit Toetsingskader meer aandacht nodig hebben. Het doel is om de resultaten van deze rapportage ook mee te nemen in het managementteamoverleg deze week.

Naast het overzicht van bestaande acties, draait hij een overzicht uit van beheersmaatregelen die nog niet goed zijn ingericht wanneer wordt gelet op het cyberdreigingsbeeld. Uit het dreigingsbeeld is bijvoorbeeld naar voren gekomen dat bewustzijn bij medewerkers op een hoger volwassenheids-niveau moet worden getild. Tot slot neemt hij een rapportage mee over

de stand van beheersmaatregelen rond de thema's op het gebied van governance (GO01 t/m GO07). Hier is afgesproken dat wordt gestart met volwassenheidsniveau 3 en een aantal maatregelen zijn nog niet voldoende ingevoerd. Het vorige niveau op dit thema was niveau 2. Eigenlijk wil hij laten zien dat ze nu voor wat betreft de voortgang op de helft van de taken zitten. Hij zou dit graag uitdrukken in een voortgangsindicator.

Om de voortgang over de beheersmaatregelen te rapporteren draait de IBP-functionaris de rapportage uit over de voortgang ten opzichte van de vorige bijeenkomst. Hiervoor selecteert hij in de datum van de vorige periode draait de actuele voortgangsrapportage uit. In de rapportage is het bestaande volwassenheidsniveau afgezet tegen de instellingsambitie en de landelijke ambitie van de sector.

2.2.5 Peer review

In overleg met de instellingen heeft SURF een lijst opgesteld met instellingen die op onderwerpen van het SURFaudit Toetsingskader vooruitlopen op de rest van de sector. Kennis van deze instellingen wordt door de instellingen gedeeld om een aantal samenwerkingspartners sneller vooruit te helpen op belangrijke domeinen binnen het Toetsingskader. Ook wordt deze samenwerking gebruikt om peer reviews uit te voeren. Deze aanpak sluit aan bij de tendens binnen het informatieveiligheidsveld om meer horizontaal toezicht binnen de eigen sector uit te voeren. Met het invoeren van horizontaal toezicht kan de druk van duur en ingrijpend verticaal toezicht worden verminderd.

Twee keer per jaar doet Laaglanden mee aan een peer review op het gebied van informatieveiligheid. Enerzijds kijkt Laaglanden mee in het GRC-systeem van een partner instelling in de regio: het Dijkland College. Anderzijds voert de IBP-functionaris van het Dijkland College een peer review uit op de opzet, bestaan en werking van het GRC van Laaglanden.
Om de peer review door het Dijkland College voor te bereiden maakt de IB-coördinator van Laaglanden een gastaccount aan om (uitsluitend) leesrechten te geven op de rapportage die voor dit doel is aangemaakt binnen de GRC-applicatie van Laaglanden.

Ter voorbereiding op de audit worden voor een aantal belangrijke maatregelen de bewijsstukken gecontroleerd die door de actiehouders zijn bijgewerkt in het systeem. Als de IBP-functionaris ziet dat alle bewijsstukken zijn aangeleverd bevriest hij de rapportage en geeft zijn collega van het Dijkland een seintje dat hij de audit kan uitvoeren. Hopelijk kan het nieuwe bewijsmateriaal hem overtuigen dat de beheersmaatregelen effectief werken.

Tijdens de peer review beoordeelt de auditor van het Dijkland College het bewijs dat is toegevoegd aan de beheersmaatregelen. Op plaatsen waar het bewijs aanvulling behoeft voegt hij aantekeningen toe aan het bewijs in een speciaal veld voor de auditor. Met deze opmerkingen kan Laaglanden de werkwijze aanpassen en nieuw bewijs aanmaken. Na een volgende review kan de auditor het bewijs goedkeuren.

2.2.6 Privacy framework

Laaglanden beslist zelfstandig dat zij ook de ISO27701 norm voor Privacy Informatie Management willen gaan hanteren binnen de instelling. Omdat deze norm nog niet bestaat binnen GRC-applicatie gaat Laaglanden deze norm zelf inlezen in haar eigen omgeving van GRC-applicatie en voegen daar nog enkele zelf vastgestelde maatregelen aan toe. Daarbij maken ze waar mogelijk en zinvol een mapping van de ISO27001 norm naar het SURFaudit Toetsingskader.

Door de mapping van de normen hoeven risicoanalyses en bijbehorende beheersmaatregelen maar een keer te worden aangemaakt en te worden geaudit.

2.2.7 SURFaudit

Jaarlijks wordt de SURFaudit uitgevoerd. Met de nieuwe GRC-applicatie kunnen gegevens eenvoudig worden gerapporteerd. Het SURFaudit Toetsingskader gaat immers uit van het opzet, bestaan en de werking van maatregelen. De status hiervan is vastgelegd in het GRC.

Na het afronden van de laatste controlemaatregelen kan de jaarlijkse benchmark rapportage worden opgesteld. Hiervoor draait de IBP-functionaris van Laaglanden de rapportage uit en stelt deze beschikbaar aan SURF. Ook MBO Digitaal, die als belangenbehartiger van het mbo, is aangesloten op de GRC-applicatie en vanuit haar rol als vertegenwoordiger van de mbo-sector rechten heeft om de benchmark rapportages van instellingen te lezen.

Nadat de koepel de rapportages van alle instellingen binnen de specifieke sector heeft verwerkt zal deze het landelijk beeld als landelijke benchmark laden in de GRC-applicatie. Hiermee kan de Laaglanden zijn eigen volwassenheid afzetten tegen het landelijk beeld. Deze rapportage wordt gebruik naar het CvB om de stand van informatieveiligheid van Laaglanden ten opzichte van het landelijk beeld te beoordelen.

2.3 User story 3: Het Hoogwerk College

Onze 3de instelling is een instelling die in basis hetzelfde werkt zoals beschreven bij het Laaglanden college, met een verschil in volwassenheid op het gebeid van toepassen van risicomanagement. Bij het Hoogwerk college is risicomanagement leidend in de activiteiten die worden uitgevoerd en ook leidend in de keuzes die gemaakt worden. Voor het Hoogwerk college is het dan ook zeer belangrijk dat de GRC-applicatie het proces van risicomanagement goed ondersteunt.

“Om de risico’s te verwerken opent zij de GRC-applicatie en maakt de nieuwe risico’s aan. Na overleg met de CISO van de instelling weet ze de risico’s te koppelen aan de juiste beheersmaatregelen van het SURFaudit Toetsingskader.”

In de toekomst is het de bedoeling om risico’s ook te kunnen identificeren en beoordelen per proces of per applicatie/kroonjuweel, zodat een risicoprofiel ervan inzichtelijk wordt. Bijvoorbeeld zo’n 40 van de 69 beheersmaatregelen uit het SURFaudit Toetsingskader hebben betrekking op applicaties/kroonjuwelen. Door de risico’s te identificeren en te beoordelen/analyseren die ten grondslag liggen aan de beheersmaatregelen, wordt inzicht verkregen in nut en noodzaak van de gegeven maatregelen. Zo kan per proces of applicatie/kroonjuweel de huidige status qua risico’s opgevraagd worden.

2.3.1 Risicoprofiel per applicatie of proces

Deze afzonderlijke risicoprofielen per applicatie/kroonjuweel of proces geven de CISO input om de volwassenheid per maatregel te bepalen. Om onderbouwd een bepaalde volwassenheid te claimen bijvoorbeeld ten aanzien van herstel van systeem en bestanden, zul je per systeem in beeld moeten hebben in hoeverre daartoe de noodzaak bestaat (al dan niet binnen de risicobereidheid van de organisatie) en zo ja, of processen in place zijn, backups worden veiliggesteld en dat deze worden getest op correcte werking. Een dergelijke maatregel per systeem zal op implementatie en uitvoering moeten worden getoetst (monitoring) of een en

ander daadwerkelijk op juiste wijze plaatsvindt. Dit om te voorkomen dat een risico op basis van de benodigde maatregel onterecht als binnen de risicobereidheid vallend wordt geclassificeerd.

2.3.2 Specifieke risicodefinitie

Een risicobeoordeling zal beginnen met een meer specifieke risicodefinitie, behorend bij de gegeven algemene beheersmaatregel uit het SURF Toestingskader. Met elkaar, zijnde tenminste de 1e lijns risico-eigenaar (proceseigenaar, applicatie-eigenaar, of anderszins), de 2e lijns informatiebeveiligings risico manager (CISO) en met een of meer subject matter experts (SME's) en andere belanghebbenden, wordt de in het toetsingskader gegeven risico omschrijving ontleed in oorzaak ("doordat…"), het risico zelf ("bestaat de kans dat…") en de impact ("met als gevolg dat…").

2.3.3 Risicomatrix

Vervolgens kunnen kans en impact worden gewogen op basis van de door het CvB vastgestelde risicomatrix. Deze matrix representeert de risicobereidheid van de organisatie. Eenvoudig gesteld; als de uitkomst van een weging (kans x impact) in een groen vak van de matrix valt, is geen risicobehandeling benodigd, althans wat het CvB betreft. De uitkomst van de weging geeft dan blijkbaar aan dat de organisatie bereid is om op voorhand de verwachte schade, afgezet tegen de ingeschatte kans van optreden, te dragen. Kostbare/ tijdrovende maatregelen zijn dan niet benodigd (proportionaliteit). Deze matrix is opgenomen in de GRC-applicatie, zodat de kansscores en impactscores kunnen worden ingegeven, op basis waarvan de uitkomst ervan in kleur wordt weergegeven (groen, geel, amber, rood). De matrix als zodanig is ook als pop-up aan te roepen tijdens wegingssessies (al dan niet online).

2.3.4 1e weging van het risico (bruto/inherent risico)

Dit specifieke risico wordt eerst beoordeeld op een situatie waarbij er geen beheersmaatregelen ingericht zijn, dus zonder reeds bestaande controls.

De uitkomst van deze 1e weging geeft bijvoorbeeld aan dat geen verdere risicobehandeling nodig is, hetgeen inhoudt dat heroverwogen moet worden of al bestaande maatregelen nog wel moeten worden uitgevoerd (moet je daar nog wel tijd en aandacht aan willen besteden)? De uitkomst wordt in de GRC-applicatie als 1e weging vastgelegd (bruto/inherent risico) en in het toelichtingenveld bij deze 1e weging wordt beschreven hoe men tot de uitkomst is gekomen en wat de conclusie is en mogelijke vervolg aanpak. Zo kan achteraf eenvoudig gereproduceerd worden hoe tot deze uitslag werd gekomen, wat daar wel/niet in werd betrokken en ook wie hierbij aanwezig was.

2.3.5 2e weging van het risico (netto/rest risico)

Als de uitkomst van deze 1e weging buiten de risicobereidheid valt (niet groen), dienen de al bestaande maatregelen in beeld gebracht te worden. Per maatregel is/wordt een maatregelplan opgesteld, gekoppeld aan dit risico. Op basis van de verwachte actuele effectiviteit van deze maatregelen bij elkaar, worden kans en impact van het beschreven risico opnieuw gewogen door de aanwezigen en op eenzelfde wijze vastgelegd als bij de 1e weging.

Als het restrisico buiten de risico bereidheid valt, dient aanvullende risicobehandeling plaats te hebben. Aanvullende maatregelen kunnen worden opgevoerd, bestaande kunnen worden gewijzigd, (een deel van) het restrisico kan worden geaccepteerd d.m.v. een formele risico-acceptatie.

2.3.6 3e weging van het risico (toekomstig netto/rest risico)

Deze 3e weging dient om op voorhand de verwachte effectiviteit te meten van de effectiviteit van alle maatregelen bij elkaar om zo vast te stellen of dit binnen de risicobereidheid zal gaan vallen, als daadwerkelijk geïmplementeerd. Vastlegging van de context vindt plaats op dezelfde wijze als bij de eerste 2 wegingen.

2.3.7 Aanpassing netto/rest risico na implementatie

Als een maatregel of een deel ervan is geïmplementeerd, kan de risico-eigenaar aan de 2e lijns risicomanager informatiebeveiliging (CISO) de weging van het netto/restrisico aanpassen op basis van de ingeschatte actuele effectiviteit van de maatregel.

2.3.8 Maatregeltemplate

In een dergelijke template is/wordt duidelijk omschreven of dit een bestaande of nieuwe maatregel betreft, aan welk risico deze gekoppeld is, waartoe de maatregel dient, wie de risico-eigenaar is, wie deze maatregel dient uit te voeren, de frequentie en data van uitvoering van de maatregel, alsook omschrijving van de evidence die gecreëerd dient te worden en waar deze bewaard wordt (audittrail). Als de maatregel nog geïmplementeerd dient te worden dan wordt een verwachte implementatiedatum ingevoerd, waarop gemonitord kan worden door zowel de 1e lijn (eigenaar van het risico) als door de 2e lijn risicomanager. De maatregel is gekoppeld aan het risico en daarmee aan de risico-eigenaar en proces of applicatie waar het risico op van toepassing is.

2.3.9 Monitoring maatregel

In de maatregeltemplate wordt vastgelegd door wie (rol binnen de 1e lijn), de frequentie en op welke wijze wordt gemonitord of de maatregel daadwerkelijk is uitgevoerd. Ook hiervoor wordt een taak aangemaakt voor de betreffende rol.

De effectiviteit van de maatregel wordt ook beoordeeld en door middel van een eenvoudige score (kleur Rood, Oranje of Groen (RAG-score)) wordt door de uitvoerder van de monitoring de effectiviteit in beeld gebracht). Per monitoring kan waar nodig een toelichtingenveld worden ingevuld/aangevuld. Zo monitort de 1e lijn op de door haar beoogde daadwerkelijk mitigerende werking van de maatregel.

De GRC-applicatie zal steeds, bijvoorbeeld een week voor afloop van een uit te voeren taak, per email een alert uitsturen naar de actiehouder van de taak. De actiehouder dient de uitgevoerde taak na uitvoering op ‘volbracht’ te melden d.m.v. invoer in de GRC-applicatie van een datum gereed. Een week later wordt eenzelfde alert uitgestuurd indien nog niet gereed is gemeld. Als een taak na 2 alerts niet als volbracht gemeld is, zal de risico-eigenaar en de manager van de uitvoerder hiervan een alert per mail ontvangen, zodat men op de hoogte is en actie kan ondernemen. Zolang de activiteit niet is gereed gemeld binnen 1 week na verloop van de actiedatum, krijgt de maatregel automatisch een Oranje RAG-status op ‘uitvoering maatregel’ en een Rode RAG-status als niet binnen 4 weken gereed gemeld.

Op het niet tijdig uitgevoerd zijn van taken en/of het niet effectief getest zijn van maatregelen kan een query gedraaid worden door zowel de 1e lijn zelf (monitoren op eigen uit te voeren maatregelen) als door de 2e lijn (steekproefsgewijs testen van maatregelen en ten behoeve van rapportages richting hoger management). Deze rapportages geven door de RAG-status geeft snel inzicht in het geheel.

2.3.10 Rapportage mogelijkheden

Ook rapportages kunnen naar eigen wens worden ingericht, gebaseerd op zelf samengestelde Query's. Zo kunnen bijvoorbeeld (doch niet beperkt tot) managementrapportages worden gerealiseerd, rapportages met betrekking tot het risicoregister, Heatmaps met betrekking tot de geïdentificeerde en geanalyseerde risico's kunnen worden opgenomen in de rapportages, rapportages met betrekking tot de controls (uitvoering en werking ervan) kunnen per proces of applicatie en/of per risico-eigenaar of uitvoerder worden gegenereerd.

3 GRC-applicatie binnen de sector

Dit hoofdstuk beschrijft het gebruik van de GRC-applicatie binnen de sector.

3.1 De rol van de koepelorganisaties

De koepelorganisaties treden op als de vertegenwoordigers van de belangen van de instellingen binnen de eigen onderwijs-sector voor mbo, hbo of wo. De koepel speelt een belangrijke rol in het bewaken van de voortgang van de informatieveiligheid binnen de sector.

Naast dat de koepels gebruik van een GRC-applicatie kan stimuleren kan de koepel de GRC-applicatie ook gebruiken voor:

- Het beschikbaar stellen en distribueren van templates en best practices.
- Het vertalen van dreigingsbeelden naar risico-overzichten met beheersmaatregelen.
- Het (na toestemming van de instelling) centraal uitvragen van de voortgang in de volwassenheid per instelling en de vertaling naar een landelijk beeld van alle instellingen.
- Het uitvragen van de SURFaudit benchmark.
- Het laden van de SURFaudit benchmark in de GRC-applicatie ter vergelijking van de instellingswaarde met de landelijke benchmark.
- Het eventueel centraal aanpassen van volwassenheidsmodellen wanneer er nieuwe versies uitkomen.
- Het beschikbaar stellen van andere frameworks rond informatiebeveiliging en privacy zoals bijvoorbeeld het SURFaudit Toetsingskader Privacy.
- Het onderling mappen van raamwerken zoals de mapping van NOREA controls naar SURFaudit Toetsingskader controls.

3.2 Landelijke benchmark informatieveiligheid

Jaarlijks op een vast moment wordt de Benchmark informatieveiligheid georganiseerd. Hiervoor leveren alle deelnemende instellingen via GRC-applicatie hun actuele NBA volwassenheids-rapportage aan. De koepels, die daarin geïnteresseerd zijn, verzamelen deze gegevens voor hun eigen sector en stellen hiervan een geanonimiseerd landelijk beeld op voor hun sector. Op de gegevens worden analyses gemaakt over bijvoorbeeld:

- De groei van de volwassenheid naar type of omvang van de instelling
- Relatie tussen de volwassenheid en nieuwe ontwikkelingen in het landelijke dreigingsbeeld.

Het landelijk beeld wordt kan per sector weer ingelezen in de GRC-applicatie waarmee instellingen in staat zijn om een vergelijking te maken van de landelijke benchmark met hun eigen situatie (GAP-analyse).

3.3 Stakeholders

Het Ministerie van Onderwijs, Cultuur en Wetenschap (OCW) is een belangrijke stakeholder binnen de onderwijssectoren. Vanuit OCW heeft ook behoefte aan informatie over de informatieveiligheid binnen de sectoren. Om die reden willen de koepels in staat zijn om geaggregeerde geanonimiseerde rapportages te genereren ten behoeve van de belangrijkste stakeholders. De individuele rapportage over instellingen zal te allen tijde aan de instellingen zelf voorbehouden zijn.

3.4 Regievoering vanuit de sectoren

Vanuit de regiefunctie vanuit de sectoren kan na verloop van tijd een nieuw volwassenheidsmodel wordt geïntroduceerd binnen om uit te rollen binnen de eigen sector. Een voorbeeld kan zijn dat het NOREA Privacy Control Framework voortaan jaarlijks in de benchmark wordt meegenomen.

Zodra deze keuze formeel wordt gemaakt volgt hieruit dat het framework moet worden ingelezen in GRC-applicatie en beschikbaar wordt gesteld aan alle instellingen. Als er instellingen zijn die zelf al een ander bekend framework hebben geïntroduceerd is het wellicht handig om de ook de mapping met deze norm op te nemen in GRC-applicatie. Zo zou een mapping van NOREA Privacy Control Framework naar ISO27701 norm voor Privacy Informatie Management centraal in het GRC opgenomen kunnen worden als ook de mapping naar het NBA framework. Dit voorkomt weer dubbel werk bij de jaarlijkse meting van de volwassenheid van informatiebeveiliging en privacy.

Ook kunnen bij nieuwe frameworks weer best practices en templates aan beheersmaatregelen worden toegevoegd, zodat niet iedere instelling zelf het wiel hoeft uit te vinden. Bovendien uniformeert het gebruik van templates en best practices de aanpak van informatieveiligheid en privacy binnen de sectoren.