Samen aanjagen van vernieuwing

Bijlage C

Programma van Eisen

Auteur(s): Projectgroep GRC-applicatie

Versie: 1.0
Datum: 19 juni 2023
Kenmerk: Programma van Eisen

Inhoudsopgave

Inleiding

In deze bijlage worden de Eisen beschreven voor het leveren, onderhouden en ondersteunen van een Governance, Risk & Compliance (GRC) applicatie.

Dit betreft minimumeisen. Indien een Inschrijving niet onvoorwaardelijk aan alle in het Programma van Eisen gestelde eisen voldoet, dan sluit de aanbestedende dienst deze Inschrijving direct uit van verdere deelname aan de aanbestedingsprocedure. Voor alle eisen geldt dat Inschrijver hieraan moet voldoen op het moment van het indienen van de Inschrijving, tenzij bij de betreffende eis of elders in de aanbestedingsstukken door de aanbestedende dienst uitdrukkelijk is aangegeven dat dit op een later tijdstip plaats mag vinden.

H1: Algemene Eisen

ID	Omschrijving van de Minimumeis	Inschrijver voldoet wel/niet aan deze minimumeis	
		Wel	Niet
ALG1	Facturatie: Op de (digitale) factuur staat minimaal vermeld: - Onderdeel of bestelnummer - Omschrijving geleverde diensten - Referentienummer of activiteitencode SURF/Instelling/Koepel - Naam Instelling - Naam van de contactpersoon of afdeling van SURF/Instelling/Koepel - Orderdatum - Nettoprijs per stuk exclusief BTW - Netto totaalprijs per orderregel - Door SURF/Instelling/Koepel aan te leveren bestelordernummer of werkordernummer - Bij functioneel beheer het aantal uren en het netto uurtarief exclusief BTW.	☐	☐

H2: Eisen t.a.v. authenticatie

ID	Omschrijving van de Minimumeis	Inschrijver voldoet wel/niet aan deze minimumeis	
		Wel	Niet
AUT1	De toepassing biedt een authorisatiemechanisme waarmee de volgende rollen onderscheiden kunnen worden: - Beheerder: kan andere gebruikers rechten geven tot specifieke onderdelen van de toepassing - Hoofdgebruiker: kan frameworks aanpassen en functionaliteiten toevoegen/weglaten en kan de GRC-applicatie zelf gebruiken - Taakgebruiker: kan voor een specifieke taak input geven - Auditor/peerreview: kan specifieke controls bekijken en daar een oordeel bij geven.	☐	☐
AUT2	Toegang tot de toepassing is gebaseerd op role based access per aangesloten instelling of organisatie.	☐	☐
AUT3	Elke gebruiker mag enkel die gegevens/data zien waartoe ze zelf geautoriseerd zijn.	☐	☐
AUT4	De toepassing ondersteunt het delen van bepaalde data met Koepels en/of andere Instellingen. Hierbij kan de Instelling zelf aangeven welke ontvanger exact welke gegevens krijgt (voorbeeld: het delen van scores voor een benchmark, waarbij de instelling tevens kan kiezen of ook bewijsstukken meegestuurd worden).	☐	☐

H3: Eisen t.a.v. dienstverlening

ID	Omschrijving van de Minimumeis	Inschrijver voldoet wel/niet aan deze minimumeis	
		Wel	Niet
DIE1	Inschrijver biedt op verzoek van een Instelling functioneel beheer. Vergoeding hiervoor gaat conform de in het prijzenblad op te geven prijs.	☐	☐
DIE2	Inschrijver ondersteunt Instelling(en) bij het importeren van data uit andere ISMS- en GRC-toepassingen.	☐	☐
DIE3	Inschrijver levert op verzoek van Opdrachtgever ondersteuning bij het inlezen van frameworks voor landelijke uitrol.	☐	☐

H4: Eisen t.a.v. Exit

ID	Omschrijving van de Minimumeis	Inschrijver voldoet wel/niet aan deze minimumeis	
		Wel	Niet
EXI1	Inschrijver zal na het beëindigen van de overeenkomst en het teruggeven van de data aan de instellingen, de data van de systemen onder beheer van Inschrijver verwijderen nadat de opdrachtgever hiertoe akkoord heeft gegeven. Voor het verwijderen van de data zullen geen additionele kosten in rekening worden gebracht.	☐	☐
EXI2	Bij beëindiging van de overeenkomst wordt alle gestructureerde data en documenten opgeslagen is de GRC-applicatie teruggegeven aan betrokken instellingen. Gestructureerde data worden in gedenormaliseerde vorm met CSV-bestanden aan de instellingen ter beschikking gesteld. Gekoppelde documenten in hun originele formaat. Voor het beschikbaar stellen van de data zullen geen additionele kosten in rekening worden gebracht.	☐	☐
EXI3	Inschrijver blijft tijdens de exit periode de dienstverlening leveren conform de gemaakte vereisten en afspraken.	☐	☐
EXI4	Inschrijver waarschuwt en adviseert in de bespreking over of de voorbereiding van de exit tijdig over noodzakelijke werkzaamheden en maatregelen voor de exit.	☐	☐

H5: Eisen t.a.v. functionaliteit

ID	Omschrijving van de Minimumeis	Inschrijver voldoet wel/niet aan deze minimumeis	
		Wel	Niet
FUN1	De GRC-applicatie dient bruikbaar te zijn voor ten minste de drie genoemde user-stories zoals opgenomen in de betreffende bijlage bij de aanbestedingsstukken. Hierbij moet het mogelijk zijn voor een Instelling om over te gaan naar een meer en/of minder volwassen scenario.	☐	☐
FUN2	De toepassing ondersteunt verschillende frameworks, waaronder maar niet beperkt tot, frameworks voor:- Privacy control, inclusief ISO27701 en het Norea privacy control framework- Informatiebeveiliging, inclusief ISO27002- Toetsingskaders, inclusief SURFaudit toetsingskader.	☐	☐

ID	Omschrijving van de Minimumeis	Inschrijver voldoet wel/niet aan deze minimumeis	
		Wel	Niet
FUN3	De toepassing ondersteunt de registratie van bedrijfsmiddelen (toepassingen, systemen) door 1) invoer vanuit de toepassing, 2) import vanuit een csv of MS-Excel, en 3) koppeling met Topdesk.	□	□
FUN4	De toepassing moet beschikken over import- en exportmogelijkheden (van en naar MS-Excel of CSV) van modellen.	□	□
FUN5	De toepassing moet beschikken over zoekmogelijkheid waarbij een gebruiker enkel resultaten ziet waar die gebruiker toe geautoriseerd is.	□	□
FUN6	De toepassing moet beschikken over contextgevoelige helpfunctie waarbij bij het oproepen van de helpfunctie direct informatie wordt getoond die relevant is voor de module en het onderdeel waaraan wordt gewerkt.	□	□
FUN7	Het moet mogelijk zijn om bij beheersmaatregelen bewijs en/of toelichting toe te voegen in de vorm van een tekstveld en in de vorm van documenten.	□	□
FUN8	Het moet mogelijk zijn om activiteiten binnen de PDCA-cyclus te plannen. Per activiteit moet de voortgang aangegeven kunnen worden als percentage of completion.	□	□
FUN9	Auditors moeten rechten hebben om beheersmaatregelen of het bewijs voor het bestaan of de werking van beheersmaatregelen goed te keuren of af te keuren. Beheersmaatregelen moeten door de auditor voorzien kunnen worden van commentaar in een specifiek veld voor de auditor.	□	□
FUN10	De toepassing moet het mogelijk maken om een self assessment uit te voeren voor geselecteerde frameworks en om (externe) audits uit te voeren voor geselecteerde frameworks. De toepassing ondersteunt dat hiertoe specifieke rechten gegeven kunnen worden.	□	□
FUN11	Het moet mogelijk zijn om beheersmaatregelen(sets) in frameworks aan te passen of niet van toepassing te verklaren.	□	□
FUN12	De toepassing moet in staat zijn een mapping aan te maken van controls/beheersmaatregelen over frameworks heen. Deze mapping moet ervoor zorgen dat identieke beheersmaatregelen uit verschillende frameworks, maar één keer hoeven te beantwoorden met acties, documentatie, bewijs, en commentaar.	□	□
FUN13	Verschillende frameworks moeten in de toepassing geladen kunnen worden en naast elkaar gebruikt kunnen worden.	□	□
FUN14	Bij een nieuwe versie van een framework dient informatie betreffende een bepaalde maatregel of onderdeel van het framework, zoals al bestaande documentatie, bewijs,	□	□

ID	Omschrijving van de Minimumeis	Inschrijver voldoet wel/niet aan deze minimumeis	
		Wel	Niet
	commentaar en acties, behouden blijven en beschikbaar zijn in de nieuwe versie.		
FUN15	Het moet mogelijk zijn om de resultaten van de landelijke benchmark informatieveiligheid (gebaseerd op het SURFaudit toetsingskader informatiebeveiliging) in te lezen in de GRC-applicatie en de eigen score hieraan te relateren.	□	□
FUN16	Het moet binnen de applicatie mogelijk zijn om een landelijke ambitie voor het volwassenheidsniveau per beheersmaatregel op te nemen.	□	□
FUN17	Het moet mogelijk zijn een instellingsgerelateerde ambitie aan te geven voor het volwassenheidsniveau per beheersmaatregel.	□	□
FUN18	De toepassing dient frameworks met verschillende diepgang of opbouw te kunnen verwerken, waaronder maar niet beperkt tot bijvoorbeeld domeinen, hoofdnormen, subnormen, maatregelen en/of submaatregelen.	□	□
FUN19	Binnen de toepassing dient het mogelijk te zijn om bij beheersmaatregelen zowel handreikingen op te nemen, als opmerkingen toe te kunnen voegen in een tekstveld.	□	□
FUN20	Per maatregel moet aangegeven worden met welke maatregelen de organisatie een volgend hoger volwassenheidsniveau kan bereiken ten opzichte van de gemeten volwassenheid op de maatregel.	□	□
FUN21	Binnen de toepassing is het mogelijk om statements van bepaalde frameworks te vertalen naar alternatieve indelingen in categorieën en alternatieve groeperingen, welke vervolgens gebruikt kunnen worden en waarvan rapportages kunnen worden gemaakt.	□	□
FUN22	Een Instelling dient voor de benchmark op basis van het SURFaudit toetsingskader gebruik te kunnen maken van de reeds ingevulde beheersmaatregelen. Hierbij is het dus niet nodig om voor de benchmark handmatig antwoorden in te geven indien deze antwoorden al beschikbaar zijn.	□	□
FUN23	De toepassing moet een operationeel risico managementsysteem systeem bevatten waarmee risico's ten minste kunnen worden gekoppeld aan: - een organisatieonderdeel, - een (bedrijfs-)proces, - een bedrijfsmiddel - een incident - een of meerdere beheersmaatregelen, - een of meerdere acties.	□	□

ID	Omschrijving van de Minimumeis	Inschrijver voldoet wel/niet aan deze minimumeis	
		Wel	Niet
FUN24	De toepassing moet in staat zijn om per organisatieonderdeel (faculteit) risicoregisters te genereren, inclusief risico's en beheersmaatregelen.	□	□
FUN25	Binnen de toepassing dient het mogelijk te zijn om bij risico's in het risicoregister documenten toe te voegen, waaronder maar niet beperkt tot risicoanalyses en beschrijvingen van maatregelen.	□	□
FUN26	Het moet mogelijk zijn om het jaarlijkse dreigingsbeeld met bijbehorende risico's beheersingsmaatregelen vanuit een bestand (CSV-formaat) te importeren in het risicoregister van de GRC-applicatie.	□	□
FUN27	Binnen de toepassing dient het mogelijk te zijn om van elk afzonderlijk risico een risicoscore te berekenen door de kans op het optreden van het risico te vermenigvuldigen met de impact van het risico.	□	□
FUN28	Risico’s moeten herbeoordeeld kunnen worden om het risico-overzicht te actualiseren.	□	□
FUN29	Binnen de toepassing dient het mogelijk te zijn om risico's aan meerdere normen te koppelen en om meerdere beheersmaatregelen aan een risico te koppelen.	□	□
FUN30	Binnen de toepassing dient het mogelijk te zijn voor geautoriseerde gebruikers om een prioriteit aan een taak te geven en te wijzigen. De toepassing heeft ten minste de mogelijkheid de prioriteiten laag, midden en hoog toe te kunnen kennen.	□	□
FUN31	Het moet mogelijk zijn om een of meerdere taken per risico toe te wijzen.	□	□
FUN32	Binnen de toepassing dient het mogelijk te zijn om de voortgangsinformatie van de uitvoering van taken te monitoren.	□	□
FUN33	De toepassing dient bij het risicomanagement de mogelijkheid te hebben om aan te geven wat het restrisico is dat overblijft na de genomen beheersmaatregelen (zie ook user story 3 voor de beschrijving van het restrisico en de gevraagde functionaliteiten hieromtrent).	□	□
FUN34	De toepassing dient het mogelijk te maken om in formulieren en rapportages te kunnen filteren op wat getoond wordt en wat niet getoond wordt.	□	□
FUN35	Het moet mogelijk zijn om taken aan te maken en toe te wijzen aan actiehouders.	□	□
FUN36	Taken moeten via workflow uitgezet kunnen worden. Hierbij moeten notificaties en rappels via e-mail verstuurd kunnen worden en moet het mogelijk zijn om een taak aan een ander te delegeren.	□	□

ID	Omschrijving van de Minimumeis	Inschrijver voldoet wel/niet aan deze minimumeis	
		Wel	Niet
FUN37	Bij taken dient een einddatum geselecteerd te kunnen worden.	☐	☐
FUN38	De toepassing dient GAP-analyses te ondersteunen, bijvoorbeeld bij het rapporteren over het SURFaudit toetsingskader waarbij de GAP tussen de behaalde score en de gewenste score gegeven moet kunnen worden en waarbij de GAP gegeven moet worden welke beheersmaatregelen nog niet geheel zijn afgerond.	☐	☐
FUN39	De toepassing moet voor asset management het mogelijk maken om per asset de BIV-classificatie (beschikbaarheid, integriteit, vertrouwelijkheid) vast te leggen.	☐	☐
FUN40	Het GRC-systeem moet ondersteuning bieden voor verschillende risicobehandelingsopties, zoals accepteren, overdragen, vermijden en verminderen	☐	☐
FUN41	Beheersmaatregelen moeten per organisatieonderdeel kunnen worden getoond, met daarbij de aanduiding voor het voldoen aan de opzet (beschreven), het bestaan (geïmplementeerd) en de werking (effectiviteit) van de beheersmaatregel.	☐	☐
FUN42	De oplossing dient een incidentenregister te ondersteunen, waarbij incidenten via een import en via handmatige vastlegging ondersteund wordt.	☐	☐
FUN43	Incidenten moeten kunnen worden gekoppeld aan risico's.	☐	☐
FUN44	De GRC-applicatie moet de mogelijkheid bieden om risico's en maatregelen te koppelen aan verschillende organisatieonderdelen (zie ook de functionele beschrijving in de bijlage User stories).	☐	☐
FUN45	De oplossing dient leveranciersmanagement te ondersteunen, waarbij per leverancier meerdere contracten en SLA's vastgelegd kunnen worden waarbij SLA's aan assets gekoppeld kunnen worden.	☐	☐
FUN46	De oplossing dient leveranciersbeoordelingen, servicelevel rapportages, incident analyses etc. te kunnen koppelen aan de betreffende leverancier en SLA.	☐	☐
FUN47	De oplossing dient risico’s te kunnen koppelen aan bepaalde leveranciers en de bijbehorende SLA('s).	☐	☐
FUN48	De oplossing dient bij opgenomen SLA's te ondersteunen dat aangegeven kan worden of de SLA voldoet aan de interne eisen van een Instelling ten aanzien van beschikbaarheid, integriteit en vertrouwen.	☐	☐

H6: Eisen t.a.v. implementatie

ID	Omschrijving van de Minimumeis	Inschrijver voldoet wel/niet aan deze minimumeis	
		Wel	Niet
IMP1	De GRC-applicatie dient de migratie naar de GRC-applicatie te ondersteunen. Dit geldt voor: - het importeren van frameworks - importeren van een risico register.	□	□
IMP2	Inschrijver dient trainingen in het gebruik van de applicatie te kunnen geven. De trainingen dienen toegespitst te zijn op het type gebruiker.	□	□
IMP3	Inschrijver informeert gebruikers proactief ten aanzien van nieuwe releases.	□	□
IMP4	Inschrijver ondersteunt onboarding van Instellingen waarbij gedifferentieerd wordt naar het door de Instelling gekozen scenario c.q. gewenste gebruik (onder meer ten aanzien van de volwassenheid zoals beschreven in de drie user stories).	□	□
IMP5	De oplossing ondersteunt standaard gebruiksprofielen die zich onderling onderscheiden in aangeboden functionaliteit, waaronder ten minste, maar niet beperkt tot, de drie user stories zoals opgenomen bij de Aanbesteding. Inschrijver biedt de standaard gebruiksprofielen aan Instellingen aan bij de implementatie. Instellingen dienen op basis van de standaard gebruiksprofielen zelf de eigen inrichting nader te kunnen instellen.	□	□
IMP6	Inschrijver kan trainingen verzorgen indien een Instelling gebruik wenst te maken van meer functionaliteiten, bijvoorbeeld in geval Instelling naar een meer volwassen niveau groeit en daartoe meer functionaliteiten vanuit de oplossing wenst te gebruiken.	□	□

H7: Eisen t.a.v. rapportage

ID	Omschrijving van de Minimumeis	Inschrijver voldoet wel/niet aan deze minimumeis	
		Wel	Niet
RAP1	Een Instelling dient ten minste de volgende rapportages te kunnen maken: - Volwassenheidsrapportage per framework - Meerjaarsontwikkeling in de volwassenheid - Eigen situatie ten opzichte van de landelijke benchmark - Eigen situatie ten opzichte van de eigen ambitie - Eigen situatie ten opzichte van de landelijke ambitie - Risico rapportages - Historische rapportages te genereren over de staat van de informatieveiligheid en privacy en risico's (van tot datum interval) - Rapportages per organisatieonderdeel - Rapportages per domein - Rapportages per beheersmaatregel - Risicomanagement rapportages inclusief informatie over openstaande risico's, beheersmaatregelen, actiehouders, vervaldata en restrisico's - Heatmap rapportages voor risico's (met horizontaal de kans en verticaal de impact) - Rapportage van openstaande taken en percentage van taken die uitgevoerd zijn - Rapportage van openstaande bevindingen - Rapportage van afgeronde maatregelen om tot een bepaald ambitieniveau te komen - Rapportage van de voortgang t.a.v. de PDCA-cyclus - Trendrapportages.	☐	☐
RAP2	Een Koepel dient ten minste de volgende rapportages te kunnen maken: - Geaggregeerd rapportages over de actuele staat van de informatieveiligheid en privacy en risico's van meerdere Instellingen	☐	☐

ID	Omschrijving van de Minimumeis	Inschrijver voldoet wel/niet aan deze minimumeis	
		Wel	Niet
	- Benchmarks van verschillende frameworks op basis van de informatie die Instellingen beschikbaar stellen - De geaggregeerde landelijke score ten opzichte van het landelijk ambitieniveau - Volwassenheid rapportage per framework - Meerjaarsontwikkeling in de volwassenheid - Risico overzicht - Geaggregeerd landelijk historische rapportages te genereren over de staat van de informatieveiligheid en privacy en risico's (Van - tot datum interval) - Beheersmaatregelen die de grootste risico's met zich meebrengen - Trendrapportages.		
RAP3	Van elk gebruikt framework dient het mogelijk te zijn om vanuit de oplossing een rapportage te genereren.	☐	☐
RAP4	Het moet mogelijk zijn om meerjaarsrapportages te genereren waarbij de ontwikkeling in volwassenheid wordt weergegeven (trend). Zowel op Instellingsniveau door een Instelling zelf als door de Koepel(s) over de sector heen. Daarnaast moet SURF kunnen rapporteren over het landelijk beeld van alle aangesloten instellingen (mbo, hbo, wo en overigen).	☐	☐
RAP5	Het moet mogelijk zijn om een bepaalde rapportage als format op te slaan. Deze opgeslagen formats dienen op een later moment weer gebruikt, en waar nodig aangepast, te kunnen worden.	☐	☐
RAP6	Het moet mogelijk zijn bepaalde rapportages op te slaan. Vervolgens dienen de opgeslagen rapportages gebruikt te kunnen worden om te vergelijken met de huidige stand van zaken, zodat de voortgang inzichtelijk wordt.	☐	☐
RAP7	Binnen rapportages moet het mogelijk zijn te filteren, onder meer maar niet gelimiteerd tot: - periode (van datum - tot en met datum), - status van de indiende meting (voorlopig of definitief) - organisatieonderdeel, - domein, - maatregel, - status (beheersmaatregelen, risico's), - volwassenheid.	☐	☐
RAP8	Instellingen en Koepels dienen rapportages zelf aan te kunnen passen. Rapportages dienen verschillende grafische weergaven, zoals maar niet beperkt tot verschillende typen diagrammen (cirkel- en staafdiagrammen).	☐	☐

ID	Omschrijving van de Minimumeis	Inschrijver voldoet wel/niet aan deze minimumeis	
		Wel	Niet
RAP9	De GRC-applicatie moet rapportages kunnen exporteren in pdf-, MS-Word formaten.	☐	☐
RAP10	De uitvoeringsstatus van een taak moet kunnen worden aangeduid met een RAG-score (Rood, Oranje, Groen), waarbij de overschrijdingstermijn instelbaar zijn door de beheerder (zie ook de functionele beschrijving in de bijlage User stories).	☐	☐
RAP11	Instellingen dienen te kunnen bepalen welke gegevens doorgestuurd worden naar de Koepel(s). Hierbij wordt de identiteit van de instelling meegestuurd.	☐	☐

H8: Eisen t.a.v. SaaS

ID	Omschrijving van de Minimumeis	Inschrijver voldoet wel/niet aan deze minimumeis	
		Wel	Niet
SAA1	De GRC-applicatie wordt volledig als een online (SaaS) dienst aangeboden. De gebruiker benadert de software over het internet bij de aanbieder van de dienst.	☐	☐
SAA2	De GRC-applicatie werkt vanuit de meest gebruikte, gangbare browsers, waaronder maar niet beperkt tot Safari, Firefox en Explorer.	☐	☐
SAA3	De GRC-applicatie werkt in de browser zonder add-ons, plug-ins of andere extra software aan de kant van de gebruiker.	☐	☐
SAA4	De aanbieder verzorgt onder meer het technisch beheer, het maken van back-ups, het onderhoud en de installatie van nieuwe versies en updates.	☐	☐
SAA5	De GRC-applicatie wordt aangeboden in het Nederlands en Engels, waarbij een gebruiker de gewenste taal kan selecteren.	☐	☐
SAA6	Inschrijver verleent medewerking indien Opdrachtgever een pentest laat uitvoeren. Genoemde pentest kan jaarlijks uitgevoerd worden en is op kosten van Opdrachtgever.	☐	☐
SAA7	De data van verschillende aangesloten Instellingen en Koepels is gescheiden van elkaar en van andere klanten.	☐	☐
SAA8	De GRC-applicatie moet een veilige audittrail logging bevatten met daarin minimaal: - Wie heeft een activiteit uitgevoerd - Welke activiteit is uitgevoerd (create, update, delete). - In welke onderdeel is de activiteit uitgevoerd - Wanneer is de activiteit uitgevoerd.	☐	☐

ID	Omschrijving van de Minimumeis	Inschrijver voldoet wel/niet aan deze minimumeis	
		Wel	Niet
SAA9	Data is tijdens transport en in opslag beveiligd via encryptie.	☐	☐
SAA10	De oplossing dient inloggen via MFA te ondersteunen. Inschrijver toont tijdens de POC aan dat de MFA-functionaliteit via SURFsecureID en SURFconext werkt [zie https://wiki.surfnet.nl/display/SURFtoolbox/SURFsecureID voor meer informatie].	☐	☐
SAA11	De GRC-applicatie moet SAML 2.0 of OpenID connect ondersteunen zoals geïmplementeerd door SURFconext. De specificaties van SURFconext zijn beschreven op de site van SURF.nl via de url: https://www.surf.nl/surfconext-overal-veilige-toegang-met-1-set-credentials	☐	☐
SAA12	Inschrijver heeft een geldige en toepasselijke certificering ISO27001 of ISAE 3000 type 2 of vergelijkbaar.	☐	☐
SAA13	De GRC-applicatie dient inloggen via de Azure AD van een Instelling te ondersteunen.	☐	☐
SAA14	Inschrijver zorgt dat gegevens, ook in geval van bijvoorbeeld een incident, niet verloren gaan, dan wel dat ze met maximaal 1 dag verlies hersteld kunnen worden.	☐	☐
SAA15	Inschrijver ondersteunt individueel aangesloten Instellingen en Koepels in het geval ze voor de betreffende organisatie een restore willen doen van eerdere data, bijvoorbeeld door, maar niet beperkt tot, het terugzetten van data uit een back-up van de betreffende organisatie.	☐	☐
SAA16	De inschrijver voert jaarlijks een restore test om te controleren of de back-up en restore van de GRC-applicatie betrouwbaar en volledig is en deelt de resultaten hiervan met Opdrachtgever.	☐	☐
SAA17	Privacy en security by design is toegepast bij ontwerp en (door)ontwikkeling van de oplossing.	☐	☐
SAA18	Alle gegevens worden opgeslagen binnen de grenzen van de Europees Economische Ruimte (EER).	☐	☐
SAA19	Alle intellectuele eigendomsrechten op ingevoerde data en documentatie blijven te allen tijde eigendom van betrokken instellingen.	☐	☐
SAA20	Beschikbaarheid van de toepassing moet minimaal gelijk zijn aan 99% per kalendermaand binnen het afgesproken service window. Hierbij wordt de beschikbaarheid berekend met de volgende formule: (([de som van de minuten binnen het service window per kalendermaand] minus [de som van de minuten van niet-beschikbaarheid binnen het service windows per	☐	☐

ID	Omschrijving van de Minimumeis	Inschrijver voldoet wel/niet aan deze minimumeis	
		Wel	Niet
	kalendermaand]) gedeeld door ([de som van de minuten binnen het service window per kalendermaand])) x 100%.		
SAA21	Page load time maximaal 7 seconden (pagina performance).	☐	☐
SAA22	Inschrijver heeft een helpdesk voor ondersteuning voor alle gebruikers van de toepassing in zowel de Nederlandse als de Engelse taal. De helpdeskondersteuning is bereikbaar van maandag tot en met vrijdag van 08.00 tot en met 17.00 CET (Central European Time), met uitzondering van de in Nederland algemeen erkende feestdagen.	☐	☐
SAA23	Onderhoudswerkzaamheden aan de toepassing door de leverancier die leiden tot een beperking in de beschikbaarheid van de toepassing vinden buiten het Service Window plaats.	☐	☐
SAA24	Geplande uitval van de toepassing wordt minimaal twee werkdagen vooraf aan de uitval gemeld aan de gebruikers van de toepassing.	☐	☐
SAA25	Inschrijver maakt een roadmap voor de (door)ontwikkeling van de applicatie en bespreekt deze ten minste twee keer per jaar met Opdrachtgever.	☐	☐
SAA26	Inschrijver rapporteert maandelijks over de behaalde servicelevels.	☐	☐

Naam Inschrijver	
Naam ondertekenaar	
Functie	
Datum	