Risicoanalyse informatiebeveiliging

Schuldenknooppunt

Classificatie:	**Vertrouwelijk**
Auteur:	B. Tel (Axxemble)
Versie:	1.1
Datum:	31-08-2022

axxemble

Inleiding

Dit document beschrijft de risicoanalyse m.b.t. informatiebeveiliging zoals uitgevoerd t.a.v. het Schuldenknooppunt. Allereerst wordt de aanpak voor de risicoanalyse beschreven waarna de scope van de risicoanalyse wordt beschreven. Tot slot volgende de risico's zoals geïdentificeerd en het voorgestelde behandelplan ter mitigatie van deze risico's.

Inhoud

Managementsamenvatting

Met betrekking tot de gehele scope van het Schuldenknooppunt is een risicoanalyse uitgevoerd met medewerking van leden van het projectteam, het bestuur (portfoliohouder), deelnemers, de belangrijkste leverancier (Innovadis) en adviseurs / specialisten m.b.t. privacy en informatiebeveiliging.

Gekeken is naar zowel organisatorische alsook technische aspecten in de opzet en de werking van het Schuldenknooppunt en het risico op incidenten die impact hebben op de beschikbaarheid, integriteit en vertrouwelijkheid van de gegevens.

Uit de risicoanalyse zijn 19 risico's geïdentificeerd die met een risiconiveau 'laag' of 'normaal' zijn geclassificeerd[1]. Er zijn geen grote of kritische risico's vastgesteld. De verschillende risico's hebben vooral betrekking op het menselijk handelen, ongeautoriseerde toegang en bedrijfscontinuïteit, zie onderstaand dreigingsprofiel.

Voor de risico's zijn maatregelen benoemd die kunnen worden samengevat als:

- Verbetering van documentatie / procedures en mogelijke vervanging van sleutelpersonen
- Aanpassing van backup-strategie / retentie
- Veiligstellen van kritische broninformatie / kennis / contracten en het opstellen van een calamiteitenplan
- Vaststellen van rollen en verantwoordelijkheden en gerelateerd daaraan het verbeteren van het toegangsbeheer door leverancier

Het betreft geen dwingende maatregelen die op korte termijn gerealiseerd dienen te worden maar uiteraard wel aandacht behoeven in de verdere ontwikkeling van het Schuldenknooppunt.

[1] De gebruikte classificatie is bepaald in het hoofdstuk 'Aanpak risicobeheersing' en is vastgesteld door het management.

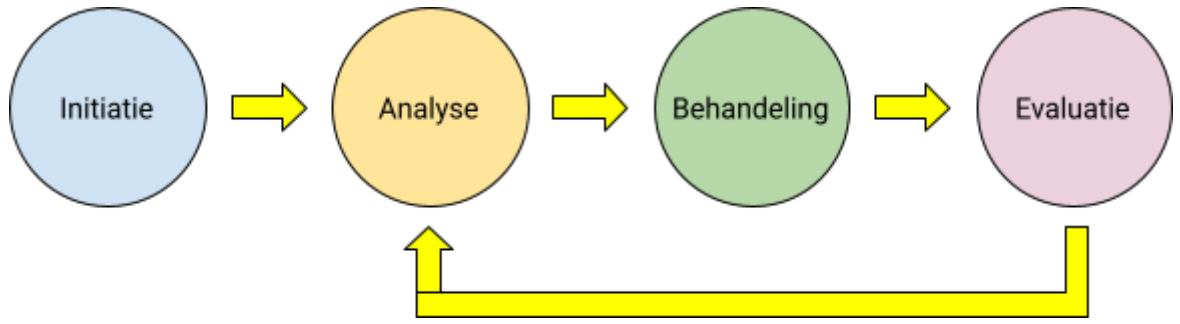
Aanpak risicobeheersing

Dit hoofdstuk beschrijft het algemene proces van risicobeheersing zoals deze wordt gehanteerd binnen de organisatie.

Risicobeheersing beoogt de risico's op het gebied van de informatiebeveiliging te reduceren tot voor de organisatie en zijn stakeholders acceptabele niveaus door het nemen van passende en effectieve maatregelen.

De risicobeheersing doorloopt de volgende stappen:

- Initiatie
- Risicoanalyse
- Behandelplan
- Evaluatie



Initiatie

Bij de volgende criteria wordt een risicoanalyse geïnitieerd:

1. Een significante verandering binnen de organisatie met een effect op de informatiebeveiliging (te beoordelen door de security officer);
2. Een nieuw - of vervanging van een - belangrijk informatiesysteem;
3. Naar aanleiding van één of meerdere beveiligingsincidenten (op initiatief van een proces- of systeem-eigenaar en/of security officer);
4. Na een periode van maximaal 3 jaar.

Wordt de risicoanalyse gestart dan is de eerste stap die genomen moet worden voordat men kan beginnen het bepalen van de scope en de vereiste deelnemers.

Scope

Het bepalen van de scope is een belangrijk onderdeel voor de risicobeheersing. Gezien de aard en opzet van de organisatie zal dit vrijwel altijd de volledige dienst alsook de bijbehorende organisatie rondom het Schuldenknooppunt betreffen.

Deelnemers

Nadat de scope is bepaald dient bepaald te worden met wie de risicoanalyse wordt uitgevoerd. Het is belangrijk om te beseffen dat kennis over risico's niet kan voortkomen uit het hulpmiddel of het proces zelf, maar slechts uit de personen die aanwezig zijn bij de risicoanalyse. Zij zijn namelijk degene die weten wat er speelt. Deelnemers zijn dus die personen die goed zicht hebben op wat echt belangrijk is voor de organisatie, maar daarbij nog voldoende zicht hebben op wat er speelt op de werkvloer.
Selectiecriteria zijn:

- personen die verantwoordelijkheid hebben voor de processen, systemen etc.;
- personen die nadelen ondervinden van problemen (incidenten);
- personen die kennis hebben van de processen, systemen etc..

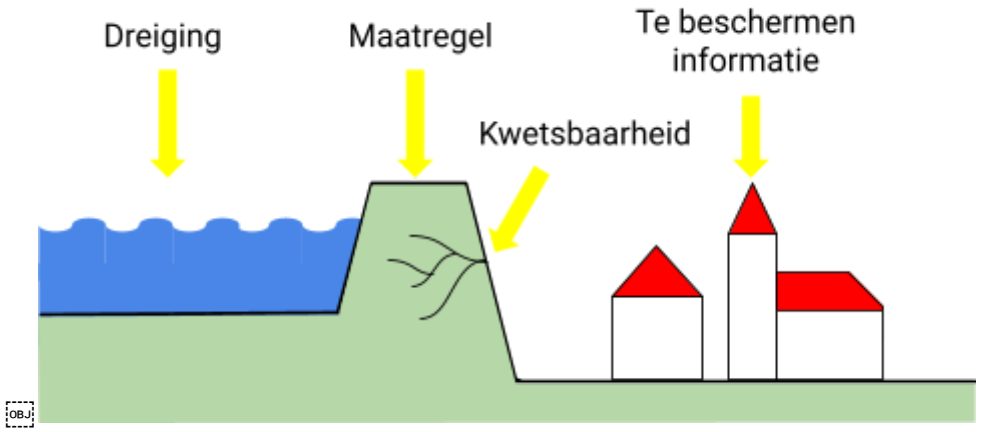
Het strategisch/tactische niveau wordt ingevuld door het bestuur (portefeuillehouder), eventueel aangevuld met de belangrijkste stakeholders. Het operationeel niveau wordt doorgaans uitgevoerd door overige stakeholders, specialisten en sleutelpersonen.

De deelnemers dienen van te voren van het proces rondom de risicoanalyse op de hoogte te zijn. Een beknopte handleiding voor deelnemers is beschikbaar. Verder dienen zij op de hoogte te zijn van de scope voor de risicoanalyse (uitkomst eerdere stap).

Voor het uitvoeren van de risicoanalyse wordt voldoende tijd gereserveerd. Deze ligt typisch in de buurt van een dagdeel (4 uur) maar is vanzelfsprekend sterk afhankelijk van de scope.

Risicoanalyse

Tijdens de risicoanalyse wordt getracht voor de betreffende scope de risico's te identificeren uitgaande van dreigingen, bestaande maatregelen en mogelijke kwetsbaarheden. Om een volledige dekking te garanderen wordt gebruik gemaakt van een gestandaardiseerde lijst, overgenomen van RAVIB. Binnen de PDCA-cyclus van het managementsysteem wordt jaarlijks getoetst of deze lijst actueel en volledig is.



Figuur 1. Algemene scope van een risico

Per dreiging wordt bekeken welke bestaande maatregelen er reeds zijn en welke kwetsbaarheden mogelijk zijn. De combinatie van dreiging, kwetsbaarheid en gevolgen worden beschreven als het risicoscenario en wordt als zodanig vastgelegd.

Per risico wordt de kans en de impact ingeschat volgens onderstaande 5-punts verdelingen.

Kans betreft de inschatting van de frequentie dat het risicoscenario met schadelijke gevolgen voor zal komen.

Kans	**Factor**	**Toelichting**
Onwaarschijnlijk	1	Vrijwel niet of hooguit eens elke 10 jaar
Zelden	2	Minder dan eens per twee jaar
Mogelijk	3	Eens per één of twee jaar
Waarschijnlijk	5	Eens per jaar of vaker
Vrijwel zeker	7	Meerdere keren per jaar, komt regelmatig voor

Impact betreft de schadelijke gevolgen op beschikbaarheid, integriteit en/of de vertrouwelijkheid en de daarmee gepaard gaande financiële gevolgen voor alsmede imago van de organisatie.

Impact	**Factor**	**Toelichting**
Niet merkbaar	1	Financieel: < 1.000 / Imago: individueel / Publiciteit: intern
Klein	3	Financieel: 1.000 - 10.000 / Imago: eigen medewerkers / Publiciteit: lokaal
Gemiddeld	7	Financieel: 10.000 - 250.000 / Imago: beperkt aantal deelnemers / Publiciteit: regionaal
Groot	11	Financieel: 250.000 - 1.000.000 / Imago: alle deelnemers / Publiciteit: landelijk
Desastreus	19	Financieel: > 1.000.000 / Imago: publiekelijk / Publiciteit: landelijk en politiek

Door vermenigvuldiging van de kans- en impactfactoren wordt de risicofactor bepaald.

Risicofactor			Impact				
			Niet merkbaar	Klein	Gemiddeld	Groot	Desastreus
			1	*3*	*7*	*11*	*19*
Kans	Vrijwel zeker	*7*	7	21	49	77	133
	Waarschijnlijk	*5*	5	15	35	55	95
	Mogelijk	*3*	3	9	21	33	57
	Zelden	*2*	2	6	14	22	38
	Onwaarschijnlijk	*1*	1	3	7	11	19

De risicofactor wordt via bovenstaande risicomatrix vertaald in een risicoklasse.

Risicoklasse	Min	Max	Toelichting
Laag	1	6	Deze risico's mogen geaccepteerd worden maar maatregelen kunnen overwogen worden (quick wins).
Gemiddeld	7	15	Deze risico's mogen bij uitzondering tijdelijk geaccepteerd worden maar er dienen direct of op middellange termijn passende maatregelen genomen te worden. Tijdelijke acceptatie van het risico dient door het bestuur (portefeuillehouder) bekrachtigd te worden.
Hoog	16	49	Voor deze risico's dienen direct passende maatregelen genomen te worden, een tijdelijke maatregel kan om organisatorische redenen overwogen worden. Het bestuur (portefeuillehouder) dient hierover geïnformeerd te worden.
Kritiek	50	133	Voor deze risico's dienen direct passende maatregelen genomen te worden. Realisatie van de maatregelen dient de hoogste prioriteit te hebben en het bestuur (portefeuillehouder) dient geïnformeerd en betrokken te zijn totdat het risico teruggebracht is tot hoog/gemiddeld/laag.

Voor de aanpak van het risico kan worden gekozen uit de onderstaande strategieën.

Strategie	Toelichting
Beheersen	Hierbij worden maatregelen getroffen vanuit de eigen organisatie om het risico terug te dringen (denk aan backup, redundantie etc.)
Overdragen	Hierbij wordt het risico en/of de te nemen maatregelen overgedragen aan een externe partij (denk aan verzekeren, uitbesteden etc.).
Ontwijken	Hierbij wordt de dreiging weggenomen door de context te veranderen (denk aan het verhuizen naar een veiligere locatie).
Accepteren	Hierbij wordt het bestaande risico / restrisico geaccepteerd zonder verdere maatregelen te nemen. Deze aanpak is alleen toegestaan voor een lage risicoklasse of tijdelijk voor een gemiddelde risicoklasse.

In de meeste gevallen zal getracht worden het risico te beheersen door het nemen van maatregelen die de kans en/of de impact terugdringen. Bekeken moet worden of na toepassing van de maatregelen het restrisico acceptabel is.

Voor de te nemen maatregelen kan bekeken worden welke maatregelen in Bijlage A van de ISO-27001:2017 relevant zijn voor de betreffende dreiging.

Op basis van de risicoanalyse is er inzicht in de maatregelen die getroffen moeten worden.

Het geheel vormt een volledige lijst met relevant en passende maatregelen op basis waarvan het behandelingsplan (realisatie van de maatregelen) opgesteld kan worden.

Behandelplan

Op basis van de uitkomsten van de risicoanalyse is er een volledige lijst van maatregelen die het risico dient terug te dringen tot een acceptabel niveau (restrisico).

De risico-eigenaar is verantwoordelijk voor het (laten) uitvoeren van eventuele wijzigingen/aanvullingen conform de beoogde maatregelen. De security officer maakt met de risico-eigenaar afspraken wat er gedaan moet worden en wanneer dit gebeurt en ziet daarop toe. Maatregelen / wijzigingen die een risico-eigenaar niet kan of wenst door te voeren, maar die vanuit de risicoanalyse wel als belangrijk of noodzakelijke worden gezien, dienen aan het bestuur (portefeuillehouder) voor een beslissing te worden voorgelegd.

Alle maatregelen, beoogde wijzigingen, benodigde investeringen, verantwoordelijken en planning tezamen resulteert in het behandelplan. De security officer ziet toe op de uitvoering er van.

Evaluatie

Na realisatie van de beoogde maatregelen conform het behandelplan dient opnieuw bepaald te worden of het restrisico acceptabel is. Dit kan gedaan worden door een hernieuwde risicoanalyse en/of door het beoordelen van de effectiviteit van de maatregelen.

Scopebeschrijving risicoanalyse

De scope voor deze risicoanalyse betreft het Schuldenknooppunt. Het Schuldenknooppunt is een centrale, digitale voorziening ter facilitering van de gegevensuitwisseling in het schuldendomein in Nederland.

Door het Schuldenknooppunt wordt het schuldhulpverleningsproces versneld, (maatschappelijke) kosten gereduceerd en de kwaliteit van dienstverlening verbeterd. Dit is in het belang van mensen met schulden en de maatschappij als geheel.

1. Het Schuldenknooppunt ontzorgt de informatie-uitwisseling tussen schuldhulpverleners en schuldeisers door standaardafspraken te maken over
    - berichten;
    - deelnemende partijen;
    - proces.
2. Het Schuldenknooppunt zorgt voor procesoptimalisatie:
    - gegevensuitwisseling vindt gestandaardiseerd plaats;
    - via een centraal beheerd digitaal platform;
    - waarop schuldhulpverleners en schuldeisers eenvoudig kunnen aansluiten;
    - dat voldoet aan de vereisten vanuit de AVG;
    - kwaliteit verbeterd door minder menselijke handelen;
    - snellere doorlooptijden, waardoor schuldhulpverleners meer tijd overhouden voor begeleiding en meer mensen met schulden kunnen helpen.
3. Het Schuldenknooppunt heeft geen commercieel oogmerk, het dient het maatschappelijk belang van betrokken partijen in de schuldenketen.

De reikwijdte van de risicoanalyse betreft het Schuldenknooppunt, bestaande uit de communicatiestromen tussen schuldhulpverleners en schuldeisers, inclusief de daarvoor benodigde ondersteunende processen alsook de organisatie en haar leveranciers.

De risicoanalyse richt zich specifiek op de architectuur, de techniek, het proces en de governance van de huidige productieversie.

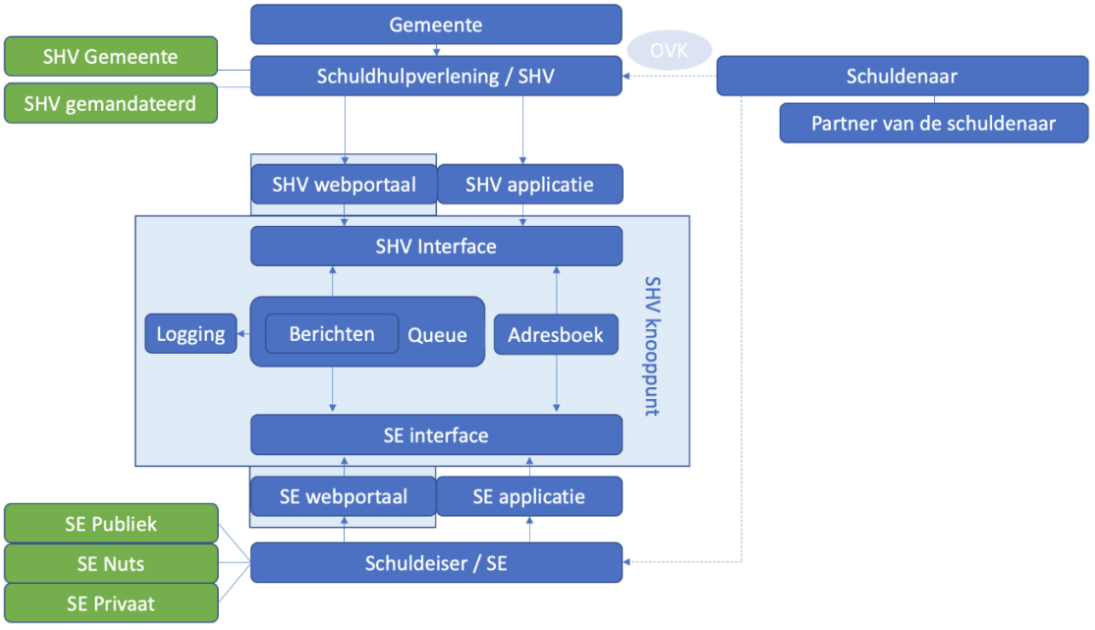
Het schuldhulpverleningsproces zelf valt buiten de risicoanalyse. Verder zijn privacy-gerelateerde risico's eveneens buiten beschouwing aangezien deze reeds middels een DPIA in kaart zijn gebracht.

De hieronder volgende beschrijving van het Schuldenknooppunt is overgenomen van de eerder uitgevoerde DPIA met kleine aanpassingen.

Overzicht

Het Schuldenknooppunt bestaat uit de onderstaande componenten.

- Een interface naar de schuldhulpverlener en een interface naar de schuldeiser.
    - Het knooppunt is vooral gericht op een zogeheten system-to-system implementatie. Daarvoor is er een (Soap/XML) interface naar de applicatie waarmee de schuldhulpverlener zijn klanten bedient c.q. de applicatie waarmee de schuldeiser zijn debiteuren beheert.
    - Niet elke schuldeiser en schuldhulpverlener heeft echter de mogelijkheid om, al dan niet op korte termijn, een system-to-system koppeling te realiseren. Daarom is er voor zowel schuldeisers als schuldhulpverleners ook een uitwisseling op bestandsniveau, via een webportaal.
- Berichtenverkeer tussen schuldhulpverleners en schuldeisers. De berichten worden door de zender via een buffer in een berichten-postbus geplaatst en daar vervolgens door de ontvanger uitgehaald of automatisch verwijderd indien deze niet tijdig is opgehaald. Het betreft gestandaardiseerde berichten. De berichten zijn versleuteld, waarbij iedere aangesloten partij een eigen versleuteling heeft. Binnen het knooppunt wordt hersleuteld naar de sleutel van de ontvangende partij.
- Een adresboek met contactgegevens van alle op het knooppunt aangesloten partijen. Een zender kiest via het adresboek de geadresseerde waar het bericht heen moet.
- Een loggingfunctie op het gebruik van het knooppunt.

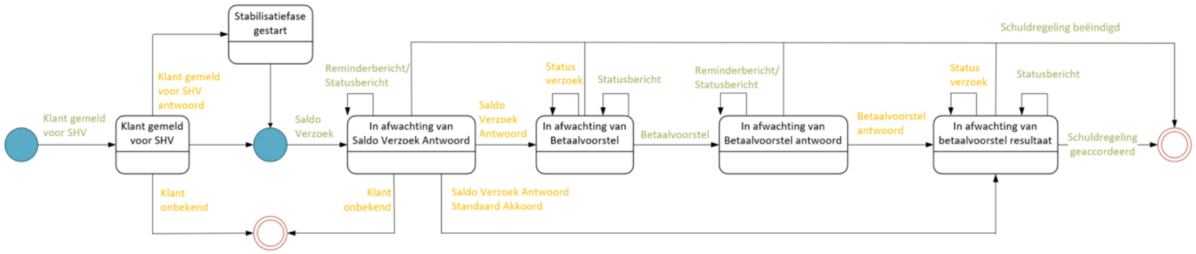


Figuur 2. Overzicht Schuldenknooppunt[2]

[2] SHV staat voor “schuldhulpverlener” en SE voor “schuldeiser.

Berichtenstromen

In onderstaande figuur zijn de berichtenstromen van het Schuldenknooppunt schematisch weergegeven.



Figuur 3. Berichtenstromen

Het Schuldenknooppunt faciliteert de onderstaande gegevensstromen.

1. Klant gemeld voor schuldhulpverlening (optioneel)
    - De schuldhulpverlener meldt aan de schuldeiser dat er schuldhulpverlening is gestart voor de klant
    - De schuldeiser kan de schuldhulpverlener laten weten dat hij de klant kent en het juiste klantnummer of factuurnummer teruggeven. De schuldeiser kan ook laten weten dat hij de klant niet kent.
2. Saldoverzoek
    - De schuldhulpverlener vraagt bij de schuldeiser op wat de schuldpositie is van de klant
        - De schuldeiser laat de schuldhulpverlener weten wat bij hem de schuldpositie is van de klant
            - ➢ *door naar stap 3*
        - De schuldeiser laat weten standaard akkoord te gaan met de schuldregeling
            - ➢ *door naar stap 4*
        - De schuldeiser laat weten dat hij de klant niet kent
            - ➢ *einde van het proces voor deze schuldeiser*
3. Betaalvoorstel
    - De schuldhulpverlener doet de schuldeiser een voorstel voor schuldregeling
        - De schuldeiser laat de schuldhulpverlener weten of hij al dan niet akkoord gaat met het voorstel
4. Uitkomst
    - De schuldhulpverlener laat de schuldeiser weten wat de uitkomst van de schuldregeling is

In aanvulling hierop worden er status- en herinneringsberichten verstuurd. Ook kan de schuldhulpverlener op elk moment laten weten dat het traject tussentijds beëindigd is.

Procesbeschrijving

Hieronder volgt een beschrijving van de verschillende processtappen in het proces ‘schuldregeling’.

Start schuldhulpverleningsproces (buiten het knooppunt)

Een schuldenaar meldt zich aan voor schuldhulpverlening. Eerst wordt dan zijn situatie gestabiliseerd. De schuldenaar geeft aan de schuldhulpverlener door welke schuldeisers vorderingen op hem hebben.

Daarna wordt, indien mogelijk, een schuldregelingstraject aangeboden. Daartoe wordt een schuldhulpovereenkomst gesloten tussen de schuldenaar en de schuldhulpverlener.

Afhankelijk van het soort schulden kan het zijn dat ook de partner van de schuldenaar partij dient te worden betrokken bij de overeenkomst. Het is mogelijk dat de schuldhulpverlener ernaar streeft om separate regelingen voor beide partners te treffen. Dan zijn er dus ook twee overeenkomsten.

Start schuldregeling

De schuldhulpverlener laat de door de schuldenaar opgegeven schuldeisers weten dat er een schuldregelingstraject is gestart. De inhoud van dit bericht is gelijk aan die van het bericht saldoverzoek.

Saldoverzoek

De schuldhulpverlener benadert de door de schuldenaar opgegeven schuldeisers. Hij gebruikt daarbij het adresboek van het knooppunt, zodat de berichten op de juiste plek aankomen. De geadresseerde schuldeisers ontvangen een saldoverzoek.

Het algemene saldoverzoek bevat in de kern de volgende gegevens:

- wie de schuldenaar is ;
- wie de partner van de schuldenaar is (uitsluitend indien de vordering verhaalbaar is op zowel de schuldenaar als degene die in de BRP als diens partner te boek staat) ;
- welke schuldhulpverleningsorganisatie dit verzoek doet.

Vervolgens sturen de schuldeisers een reactie aan de schuldhulpverlener. Er zijn drie soorten reacties mogelijk:

1. Saldo-opgave: De schuldeiser geeft aan wie aan zijn zijde de behandelaar is, en wat de hoogte en status van de schuld zijn.
2. Standaard akkoord: De schuldeiser geeft aan bij voorbaat akkoord te gaan met de te treffen schuldregeling.
3. De schuldeiser geeft aan dat de klant bij hem niet bekend is (einde traject voor deze schuldeiser).

Opstellen van een betaalvoorstel (buiten het knooppunt)

Na ontvangst van de verschillende saldo-opgaven (dan wel berichten “standaard akkoord”) van de schuldeisers van de klant, stelt de schuldhulpverlener een betaalvoorstel op. Hiervoor wordt ook een berekening gemaakt om vast te stellen wat het vrij te laten bedrag (vtlb) is.18

Betaalvoorstel

De schuldhulpverlener stuurt een betaalvoorstel aan iedere schuldeiser van de klant die niet heeft aangegeven standaard akkoord te gaan.

Vervolgens stuurt de schuldeiser een reactie op dit betaalvoorstel aan de schuldhulpverlener. Dat bericht kan een instemming zijn of een afwijzing.

Uitkomst schuldregeling

Een minnelijke regeling gaat in nadat alle betrokken schuldeisers akkoord hebben gegeven. Daarom stuurt de schuldhulpverlener als alle schuldeisers akkoord zijn een bericht aan de schuldeisers dat het minnelijke traject start. Ook wanneer het traject wordt beëindigd – wat gedurende het hele traject mogelijk is – stuurt de schuldhulpverlener een bericht hierover aan de schuldeisers; dit bericht vermeldt de reden van de beëindiging.

Statusberichten

De verzender van een bericht kan via statusberichten zien of het bericht goed is aangekomen:

- de verzender ontvangt een bevestiging wanneer het verzonden bericht succesvol is opgeslagen in de buffer van het knooppunt
- de verzender ontvangt een bevestiging wanneer de geadresseerde het verzonden bericht heeft opgehaald
- de verzender ontvangt een bericht wanneer de geadresseerde het verzonden bericht niet binnen de afgesproken termijn heeft opgehaald, met de mededeling dat het verzonden bericht uit de buffer is verwijderd

Afronden proces ‘schuldregelen’ (buiten het knooppunt)

Bij akkoord van alle schuldeisers zorgt de schuldhulpverlener ervoor dat het resultaat van de minnelijke regeling bekrachtigd wordt. Bij niet akkoord heeft de schuldhulpverlener de mogelijkheid tot rappel.

Techniek

Tot slot wordt een beschrijving van de technische opzet van het Schuldenknooppunt gegeven.

Hosting

Het Schuldenknooppunt wordt gehost op het Microsoft Azure-platform. De gekozen locatie is West Europe. Dit betekent dat de gegevensverwerking hoofdzakelijk in Nederland plaatsvindt. Om technische redenen kunnen de gegevens in sommige gevallen ook elders binnen de Europese Unie verwerkt worden.

Versleuteling en buffer

De berichten tussen de schuldhulpverlener en de schuldeiser worden versleuteld. Er is geen end-to-end versleuteling, omdat in die situatie een sleutel met alle aangesloten partijen zou moeten worden gedeeld en beheerd. De versleuteling betreft het pad van de schuldhulpverlener tot aan het knooppunt en het pad van het knooppunt tot aan de schuldeiser, en omgekeerd.

Per aangesloten partij wordt door het Schuldenknooppunt een sleutel beheerd. De verzonden berichten worden binnen het Schuldenknooppunt hersleuteld naar de sleutel van de ontvangende partij. De berichten bevinden zich op geen enkel moment in onversleutelde staat in het Schuldenknooppunt, behalve om technische redenen heel kort tijdens het proces van hersleutelen en tijdens verwerking in het webportaal. De versleuteling vindt plaats met de Advanced Encryption Standard (AES) 256-bit. De netwerkverbindingen worden beveiligd op basis van certificaten (https-protocol).

Het adresboek en de monitorgegevens zijn niet versleuteld. Het adresboek kan alleen bevraagd worden door aangesloten partijen, de verbinding van en naar het adresboek is versleuteld middels two-way authenticatie. Monitorgegevens zijn opvraagbaar via het beheerportaal; alleen geautoriseerde gebruikers hebben hier toegang toe. Het transport van de gegevens wordt versleuteld middels een SSL-certificaat.

Buffer (queue)

Het knooppunt maakt gebruik van een zogenaamde queue of buffer. De zender plaatst een bericht in deze buffer. In deze buffer wordt het bericht bewaard gedurende een nog nader te bepalen termijn (bijvoorbeeld twee dagen, dit kan verschillen per berichttype). Een persoon die (via zijn werkgever) is aangesloten op het knooppunt kan op verschillende manieren (zie hieronder) zien of er berichten voor hem klaarstaan en die vervolgens ophalen. De zender ontvangt in dat geval een statusbericht dat de geadresseerde het bericht heeft opgehaald. Mocht de geadresseerde het bericht niet binnen de daarvoor gestelde termijn ophalen, dan wordt het bericht uit de buffer verwijderd en ontvangt de zender hierover een statusbericht.

System-to-system koppeling met SHV-applicatie of SE-applicatie

Een schuldhulpverlener gebruikt een applicatie bij de dienstverlening naar zijn klanten. Een schuldeiser heeft een applicatie waarmee hij het beheer van debiteuren uitvoert. Alle schuldhulpverleners en een aantal schuldeisers werken (uitsluitend) via een system-to-system koppeling met het Schuldenknooppunt. Het versturen en ontvangen van berichten vindt dan plaats vanuit die applicaties (via een SOAP webservice), en is daarmee eenvoudiger geïntegreerd in de werkwijze van de schuldhulpverlener c.q. de schuldeiser. Het berichtenverkeer tussen het knooppunt en de applicaties verloopt via een beveiligde verbinding (two-way SSL op basis van PKIOverheid-certificaten).

Webportaal

(Medewerkers van) schuldeisers of schuldhulpverleners die geen gebruik maken van de system-to-system koppeling kunnen via de gebruikersinterface van het webportaal berichten versturen en ophalen. Een ontvanger kan via het webportaal middels een csv-interface alle aan hem gerichte berichten in één keer downloaden. Evenzo kan een verzender alle berichten die hij op een bepaald moment wil versturen in één keer verzenden.

Het webportaal is vanuit de kerndienstverlening van het Schuldenknooppunt gezien een endpoint. Dat wil zeggen dat er onversleutelde berichten verwerkt kunnen worden. Versleutelde ontvangen berichten uit de berichtenpostbus worden in het webportaal ontsleuteld en in een csv-bestand gezet. En gebruikers uploaden te verzenden berichten via een csv-bestand naar het webportaal, dat ze versleutelt en naar het knooppunt stuurt ter opname in de berichtenpostbus.

Authenticatie voor het webportaal verloopt via e-Herkenning niveau EH3.

De productieversie van het webportaal wordt automatisch gescand op de OWASP Top 10 kwetsbaarheden.

Logging

Het berichtenverkeer over het knooppunt wordt gelogd. Bij de logging worden in de productieversie geen persoonsgegevens gebruikt. Wat wordt gelogd zijn het tijdstip, de betrokken organisaties, en wat er met het bericht is gebeurd (achtergelaten op het knooppunt, opgehaald bij het knooppunt, verwijderd). Op de bewaartermijn van de logginggegevens is in de productieversie een limiet van drie jaar gesteld. Alleen geautoriseerde medewerkers van het knooppunt hebben toegang tot de logginggegevens.

Voor deelnemers is een logboekservice beschikbaar, waarmee zij de logs van hun berichtenverkeer kunnen doorzoeken. Deze kan gebruikt worden als bijvoorbeeld een bericht niet tijdig is opgehaald of bij de ontvanger intern is zoekgeraakt. Via de logboekservice kan dit opgespoord worden, waarna de ontvanger verzocht kan worden om het bericht opnieuw te verzenden.

Adresboek

Het adresboek bevat de contactgegevens van alle aangesloten partijen. Een zender selecteert één ontvanger waar een bericht naar toe gestuurd moet worden. Het is ook mogelijk om de adresgegevens uit het knooppunt op te halen, en deze op te slaan in de eigen administratie. Aangesloten organisaties die gebruik maken van de system-to-system interface kunnen voor het versturen van berichten gebruik maken van de adresreferentie die aanwezig is in het knooppunt.

Als blijkt dat een aangesloten partij zich niet houdt aan de aansluitvoorwaarden voor het gebruik van het knooppunt, dan kan deze partij in het adresboek geblokkeerd of verwijderd worden. De partij is daardoor uitgesloten van het gebruik van het Schuldenknooppunt.

Rol in berichtenverkeer

Een partij is binnen het knooppunt ofwel schuldhulpverlener, ofwel schuldeiser. Is een partij beide, dan worden hiervoor in het knooppunt twee verschillende entiteiten aangemaakt. Een schuldhulpverlener kan alleen schuldhulpverlenersberichten versturen, en een schuldeiser alleen schuldeisersberichten. Zenders kunnen geen berichten versturen aan geblokkeerde ontvangers.

Geïdentificeerde risico's

Tijdens de risicoanalyse zijn de volgende risico's vastgesteld.

Nr	Risico	Kans	Impact	x	Risiconiveau	Maatregelen / behandelplan
1	**Verstoring van de dienstverlening als gevolg van wegvallen van sleutelpersonen** Door het wegvallen van belangrijke personen - met name Bart van de Ven en Marianne Oostrik - wordt de dienstverlening mogelijk verstoord. ● Operationeel zal het SKP blijven draaien ● Kennis is breder beschikbaar maar niet altijd en in voldoende mate gedocumenteerd ● Het activeren van nieuwe deelnemers (nu alleen door Bart mogelijk) wordt vertraagd, zie ook risico #7 *Categorie*: Bedrijfscontinuïteit	Zelden	Significant	12	Normaal	*Bestaande maatregelen*: - Documentatie van kennis en procedures *Nieuw te nemen maatregelen*: - Uitbreiding documentatie - Vervanging regelen *ISO 27001 beheersmaatregelen*: - A.12.1.1 - A.17.1.2

Nr	Risico	Kans	Impact	x	Risiconiveau	Maatregelen / behandelplan
2	**Registratie van foutieve / malafide deelnemers als gevolg van onvoldoende controle op authenticiteit van nieuwe aanmeldingen** De controle op de betrouwbaarheid van deelnemers is niet beschreven en wordt ad-hoc uitgevoerd op basis van eigen kennis (netwerk) en mogelijk (indien onbekend) zoekopdrachten op het internet. Uitkomsten zijn dus sterk afhankelijk van de persoon die dit uitvoert en de diepgang van het onderzoek. Hierdoor kunnen mogelijk malafide deelnemers geregistreerd worden. Kans en impact worden beperkt door het gebruik van certificaten (eHerkenning / PKI) waar de deelnemer over moet beschikken en de communicatie vanuit schuldhulpverleners gestart moet worden. Risico is dus wel groter indien de malafide deelnemer zich als schuldhulpverlener weet te registreren. *Categorie*: Menselijk handelen	Zelden	Significant	12	Normaal	*Bestaande maatregelen*: - *Nieuw te nemen maatregelen*: - Documentatie van procedure / checklist op controle van nieuwe aanmeldingen en deze toepassen in de aanmeldprocedure *ISO 27001 beheersmaatregelen*: - A.12.1.1

Nr	Risico	Kans	Impact	x	Risiconiveau	Maatregelen / behandelplan
3	**Geen doorontwikkeling van de dienstverlening als gevolg van financiële problemen bij de organisatie** Door problemen in de financiële continuïteit wordt de dienstverlening op termijn verstoord, met name wat betreft de doorontwikkeling en het onderhoud van de software en beveiligingsaspecten. • Operationeel (korte termijn) zal het SKP blijven draaien *Categorie*: Bedrijfscontinuïteit	Onwaarschijnlijk	Significant	6	Laag	*Bestaande maatregelen*: - Bestaande afspraken met leverancier *Nieuw te nemen maatregelen*: - *ISO 27001 beheersmaatregelen*: - A.17.1.1 - A.17.1.2 - A.17.1.3

Nr	Risico	Kans	Impact	x	Risiconiveau	Maatregelen / behandelplan
4	**Misbruik van het Schuldenknooppunt als gevolg van malafide medewerkers bij de deelnemers** Malafide medewerkers bij de deelnemers (zowel schuldhulpverleners als schuldeisers) kunnen misbruik maken van de dienst doordat zij berichten met de verkeerde intentie plaatsen. Het Schuldenknooppunt maakt dit vanwege de relatieve anonimiteit makkelijker / moeilijker verifieerbaar. Reden voor misbruik kan zijn vanwege een deal met schuldenaar (deel van de mogelijk kwijtgescholden schuld wordt 'verdiend' door de medewerker), gebruik van de schuldinformatie voor afpersing / misbruik van de schuldenaar of anderszins. Ook kunnen medewerkers schuldinformatie opvragen en deze informatie doorverkopen aan derden (hoewel hier een signaalfunctie op mogelijk is). Zie ook risico #5. De verantwoordelijkheid voor dit risico ligt niet direct bij het Schuldenknooppunt	Onwaarschijnlijk	Klein	3	Laag	*Bestaande maatregelen*: - Afspraken (algemene voorwaarden) met deelnemers *Nieuw te nemen maatregelen*: - *ISO 27001 beheersmaatregelen*: - A.15.1.1 (m.b.t. deelnemers) - A.15.1.2 (m.b.t. deelnemers) - A.15.2.1 (m.b.t. deelnemers)

Nr	Risico	Kans	Impact	x	Risiconiveau	Maatregelen / behandelplan
	maar bij de betreffende deelnemer maar het kan de positie en berichtgeving (reputatie) van het Schuldenknooppunt wel raken. *Categorie*: Menselijk handelen					

Nr	Risico	Kans	Impact	x	Risiconiveau	Maatregelen / behandelplan
5	**Misbruik van het Schuldenknooppunt als gevolg van misbruik van de identiteit van gebruikers** Hoewel de gebruikersaccounts op het Schuldenknooppunt in principe persoonsgebonden zijn kan hier in het geval van een system-to-system koppeling een andere invulling aan zijn gegeven of kiest een organisatie er bewust voor om een bepaald account te delen met meerdere medewerkers. Ook binnen de organisatie van de deelnemer kan er sprake zijn van identiteitsdiefstal, bijv. door het onbeheerd achterlaten van een werkplek. Via dit scenario is misbruik van het Schuldenknooppunt mogelijk met dezelfde doelstelling en gevolgen als bij risico #4. De verantwoordelijkheid voor dit risico ligt niet direct bij het Schuldenknooppunt maar bij de betreffende deelnemer maar het kan de positie en reputatie van het Schuldenknooppunt wel raken. *Categorie*: Ongeautoriseerde toegang	Onwaarschijnlijk	Klein	3	Laag	*Bestaande maatregelen*: - Afspraken (algemene voorwaarden) met deelnemers *Nieuw te nemen maatregelen*: - *ISO 27001 beheersmaatregelen*: - A.7.2.2 - A.9.4.2 - A.11.2.8 - A.11.2.9 - A.15.1.2 (m.b.t. deelnemers)

Nr	Risico	Kans	Impact	x	Risiconiveau	Maatregelen / behandelplan
6	**Meldingen (incidenten) worden niet tijdig / correct afgehandeld als gevolg van het ontbreken van een gestructureerde aanpak** De organisatie heeft een SLA t.a.v. de afhandeling van meldingen en incidenten maar hiervoor geen gestructureerde aanpak ingericht. Hierdoor worden deze meldingen mogelijk niet tijdig / correct afgehandeld. Er is een voornemen om met een ticketsysteem (Zendesk) te gaan werken. Verder zijn er ook SLA afspraken met de leverancier (Innovadis) zodat opvolging door de leverancier wel geregeld is. In de praktijk worden meldingen op dit moment goed opgepakt en afgehandeld. Qua beschikbaarheid wordt gestreefd naar een hoge beschikbaarheid maar geldt ook dat de dienst zelf geen grote impact hoeft te hebben voor de deelnemers bij (beperkte) beschikbaarheidsproblemen. *Categorie*: Incidentafhandeling	Zelden	Klein	6	Laag	*Bestaande maatregelen*: - *Nieuw te nemen maatregelen*: - Inrichten ticketsysteem - Toewijzen rollen en verantwoordelijkheden - Documentatie van incidentafhandeling *ISO 27001 beheersmaatregelen*: - A.16.1.1 - A.16.1.4 - A.16.1.5

Nr	Risico	Kans	Impact	x	Risiconiveau	Maatregelen / behandelplan
7	**Nieuwe deelnemers kunnen niet (tijdig) geactiveerd worden als gevolg van onbeschikbaarheid van Bart van de Ven** Nieuwe deelnemers kunnen niet (tijdig) geactiveerd worden - dat wil zeggen toegevoegd in het adresboek van het Schuldenknooppunt - wanneer Bart van de Ven onbeschikbaar is. Deze functie wordt uitsluitend door Bart uitgevoerd. Technisch gezien ook door Innovadis maar zij doen dit in principe niet voor de productieomgeving. Bij langere onbeschikbaarheid zou Marianne Oostrik deze taak wel kunnen overnemen of opdracht geven aan Innovadis. *Categorie*: Bedrijfscontinuïteit	Onwaarschijnlijk	Niet merkbaar	1	Laag	*Bestaande maatregelen*: - *Nieuw te nemen maatregelen*: - Vervanging regelen *ISO 27001 beheersmaatregelen*: - A.6.1.1 - A.12.1.1

Nr	Risico	Kans	Impact	x	Risiconiveau	Maatregelen / behandelplan
8	**Fouten in de administratie of verstoring in de communicatie als gevolg van het ontbreken van het gestructureerd doorvoeren van wijzigingen in de deelnemersadministratie** Bij wijzigingen t.a.v. deelnemers, bijvoorbeeld als gevolg van reorganisaties / opheffing / fusies etc. worden deze wijzigingen nu ad-hoc doorgevoerd. De mogelijkheid bestaat dat hierdoor fouten ontstaan of dat de communicatie over schulden vast loopt. *Categorie*: Menselijk handelen	Zelden	Klein	6	Laag	*Bestaande maatregelen*: - *Nieuw te nemen maatregelen*: - Documentatie en verificatie van wijzigingsprocedure *ISO 27001 beheersmaatregelen*: - A.12.1.1 - A.12.1.2

Nr	Risico	Kans	Impact	x	Risiconiveau	Maatregelen / behandelplan
9	**Communicatie loopt vast als gevolg van het niet ophalen van berichten door deelnemers** Wanneer deelnemers berichten niet (tijdig) ophalen loopt de communicatie over een schuldenregeling vast. Hoewel hier technisch gezien geen problemen ontstaan (het wordt bijvoorbeeld gemeld aan de andere deelnemer(s)), kan het wel leiden tot workarounds door medewerkers om om het Schuldenknooppunt heen te werken wat uiteindelijk de basis onder het Schuldenknooppunt ondermijnt. Het niet ophalen van berichten wordt wel inzichtelijk gemaakt maar hierop is geen structurele monitoring / bewaking. *Categorie*: Betrouwbaarheid van systemen	Onwaarschijnlijk	Klein	3	Laag	*Bestaande maatregelen*: - Analyseren van oorzaak n.a.v. meldingen / problemen *Nieuw te nemen maatregelen*: - Actief monitoren / notificaties bij niet ophalen van berichten *ISO 27001 beheersmaatregelen*: - A.12.4.1

Nr	Risico	Kans	Impact	x	Risiconiveau	Maatregelen / behandelplan
10	**Imagoschade als gevolg van een langdurige opstartfase van de organisatie** De organisatie, Stichting Schuldenknooppunt, al lange tijd als projectorganisatie en benoemt dat zelf als: “nog in de opstartfase”. Dit geeft een verkeerd beeld en kan deelnemers afschrikken wat uiteindelijk kan leiden tot staking van de dienstverlening bij uitblijvend succes. *Categorie*: Menselijk handelen	Zelden	Significant	12	Normaal	*Bestaande maatregelen*: - *Nieuw te nemen maatregelen*: - Afronden migratie naar ‘staande organisatie’ *ISO 27001 beheersmaatregelen*: - A.6.1.1

Nr	Risico	Kans	Impact	x	Risiconiveau	Maatregelen / behandelplan
11	**Bewaartermijn van managementinformatie (metadata) langer dan wenselijk als gevolg van het ontbreken van een archivering hiervan** Managementinformatie (metadata van het berichtenverkeer) wordt momenteel niet actief gearchiveerd / verwijderd en blijft dus langer beschikbaar dan wenselijk / vereist. De verwachting is dat dit maximaal 3 jaar zou moeten zijn (na afronden van de conversatie). Dit vergroot de impact van risico #12. Momenteel is dit risico nog niet aanwezig aangezien de beoogde bewaartermijn van 3 jaar nog niet van verstreken is voor de eerste gegevens. Op termijn wordt dit wel een relevant risico. *Categorie*: Wet- en regelgeving	Zelden	Klein	6	Laag	*Bestaande maatregelen*: - *Nieuw te nemen maatregelen*: - Op termijn: verwijderen van verouderde managementinformatie *ISO 27001 beheersmaatregelen*: - A.18.1.1 - A.18.1.4

Nr	Risico	Kans	Impact	x	Risiconiveau	Maatregelen / behandelplan
12	**Negatieve publieke beeldvorming over deelnemers als gevolg van het lekken van managementinformatie (metadata) over de schuldhulpverlening** Op basis van managementinformatie (metadata van het berichtenverkeer) kan een beeld worden opgesteld van de 'prestaties' van deelnemers t.a.v. de schuldsanering / hulpverlening. Een deelnemer kan bijvoorbeeld relatief vaak een schuldsanering afwijzen wat tot negatieve beeldvorming leidt als deze gegevens openbaar worden. Hoewel de berichten zelf niet meer te herleiden zijn bevat de metadata op dit moment wel informatie over het wel of niet akkoord zijn met het betalingsvoorstel door deelnemers (schuldeisers). Zie ook risico #11. *Categorie*: Menselijk handelen	Zelden	Significant	12	Normaal	*Bestaande maatregelen*: - *Nieuw te nemen maatregelen*: - Op termijn: verwijderen van verouderde managementinformatie *ISO 27001 beheersmaatregelen*: - A.18.1.1

Nr	Risico	Kans	Impact	x	Risiconiveau	Maatregelen / behandelplan
13	**Verstoring van de dienstverlening als gevolg van continuïteitsproblemen bij de leverancier (Innovadis)** De dienstverlening kan verstoord worden indien de leverancier in problemen komt, bijvoorbeeld door een faillissement. Er zijn enkele 'waarborgen' om als Stichting Schuldenknooppunt de dienst op een andere manier te organiseren in deze situatie maar hier zijn mogelijke complicaties bij geïdentificeerd: ● Het contract van Azure staat op naam van Innovadis ● Broncode is weliswaar eigendom van het Schuldenknooppunt maar de organisatie heeft hier op dit moment geen toegang toe (bijvoorbeeld leestoegang tot de code repository) *Categorie*: Bedrijfscontinuïteit	Onwaarschijnlijk	Groot	11	Normaal	*Bestaande maatregelen*: - Bestaande afspraken met leverancier *Nieuw te nemen maatregelen*: - Azure contract overnemen - Beschikbaarheid van source code (ESCROW of soortgelijk) - Calamiteitenplan vaststellen en verifiëren *ISO 27001 beheersmaatregelen*: - A.15.1.1 - A.15.1.2 - A.15.2.1 - A.15.2.2 - A.17.1.1 - A.17.1.2 - A.17.1.3

Nr	Risico	Kans	Impact	x	Risiconiveau	Maatregelen / behandelplan
14	**Langere bewaartermijn (en kwetsbaarheid) van berichten als gevolg van lange retentie van backups** Er worden momenteel dagelijks, wekelijks, maandelijks backups alsook een jaar-backup bewaard. Deze backups bevatten de (versleutelde) inhoud van berichten. Hiermee is de bewaartermijn van (een deel van) de berichten dus langer dan 4 dagen zoals in het algemeen wordt gecommuniceerd. De lange bewaartermijn lijkt daarmee niet in overeenstemming met de doelstelling en de meerwaarde is er ook in praktische zin niet aangezien deelnemers ook een eigen administratie hebben van de communicatie (conversaties) die na verloop van tijd te veel verschillen om een bruikbare backup van het Schuldenknooppunt mogelijk te maken. Zie ook risico #18. *Categorie*: Wet- en regelgeving	Vrijwel zeker	Niet merkbaar	7	Normaal	*Bestaande maatregelen*: - *Nieuw te nemen maatregelen*: - Beperken van backup retentie - Beperken van backup data (uitsluiten van berichten in backup) *ISO 27001 beheersmaatregelen*: - A.12.3.1 - A.18.1.1

Nr	Risico	Kans	Impact	x	Risiconiveau	Maatregelen / behandelplan
15	**Inconsistenties tussen administraties van deelnemers en het Schuldenknooppunt als gevolg van het terugplaatsen van een backup** Aangezien het Schuldenknooppunt een administratie bijhoudt van de conversaties (berichtenverkeer t.a.v. een betalingsregeling voor een schuldenaar) en hierbij een status hanteert die (in meer en mindere mate) in overeenstemming moet zijn met de administratie van deelnemers t.a.v. diezelfde betalingsregeling kan dit bij het terugplaatsen van een backup tot consistentie-problemen leiden en dus fouten in de communicatie. Zie ook risico #19. *Categorie*: Betrouwbaarheid van systemen	Onwaarschijnlijk	Klein	3	Laag	*Bestaande maatregelen*: - *Nieuw te nemen maatregelen*: - Beschrijven van restore procedure / beperkingen *ISO 27001 beheersmaatregelen*: - A.12.1.2 - A.12.3.1

Nr	Risico	Kans	Impact	x	Risiconiveau	Maatregelen / behandelplan
16	**Ontbrekende updates en patches op middleware als gevolg van onduidelijkheid in verantwoordelijkheden t.a.v. het beveiligingsonderhoud** Het is niet duidelijk geworden welke partij het beveiligingsonderhoud uitvoert op de middleware en waar deze grens precies ligt. Er wordt gebruik gemaakt van web apps / services maar hoe deze zich verhouden tot het beveiligingsonderhoud is niet duidelijk en mogelijk blijven hiermee kwetsbaarheden langer bestaan dan wenselijk is. *Categorie*: Ongeautoriseerde toegang	Zelden	Significant	12	Normaal	*Bestaande maatregelen*: - Regulier onderhoud door Azure / leverancier *Nieuw te nemen maatregelen*: - Vaststellen juiste rollen en verantwoordelijkheden *ISO 27001 beheersmaatregelen*: - A.6.1.1 - A.12.6.1

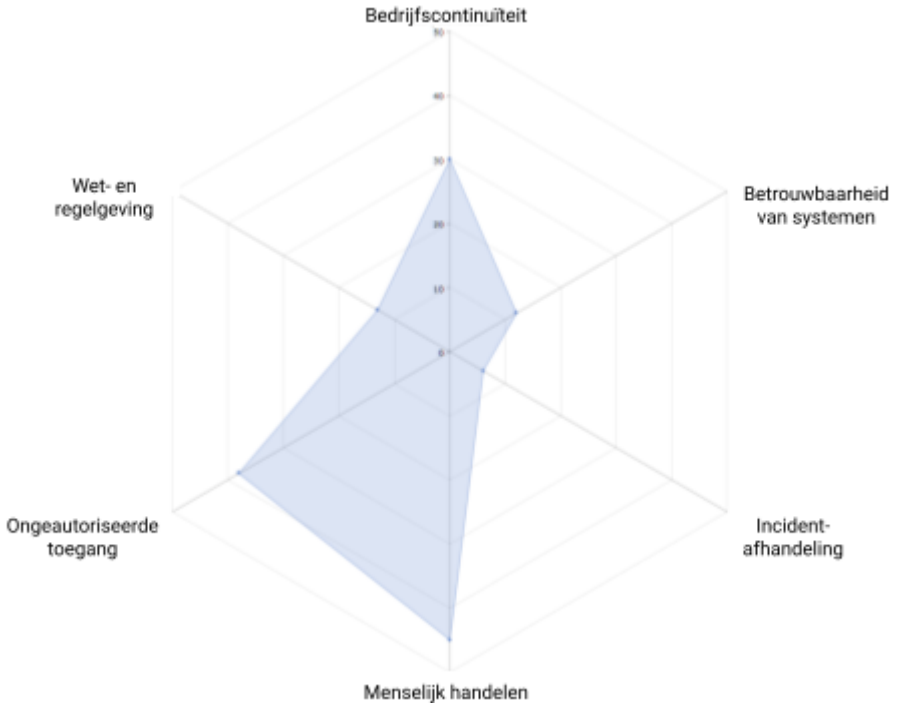
Nr	Risico	Kans	Impact	x	Risiconiveau	Maatregelen / behandelplan
17	**Ongeautoriseerde toegang tot de productieomgeving door de leverancier als gevolg van grofmazige autorisaties binnen de Azure-omgeving** Binnen de Azure-omgeving wordt momenteel met een zogeheten resourcegroep gewerkt voor toegang tot de (productie-)omgeving van het Schuldenknooppunt. Hierdoor hebben naast de projectbeheerders ook een aantal ontwikkelaars toegang. De toegang zelf wordt weer geregeld door beheerders binnen Innovadis. De toegang wordt regelmatig gecontroleerd door de security officer van Innovadis. In een toekomstige update wil men de toewijzing fijnmaziger inrichten zodat bijvoorbeeld de ontwikkelaars - die feitelijk hiermee ongeautoriseerde toegang hebben - geen toegang meer hebben tot de productieomgeving en alleen geselecteerde beheerders. *Categorie*: Ongeautoriseerde toegang	Zelden	Significant	12	Normaal	*Bestaande maatregelen*: - Grofmazige autorisaties - Autorisatiecontroles *Nieuw te nemen maatregelen*: - Fijnmazige autorisaties *ISO 27001 beheersmaatregelen*: - A.9.1.1 - A.9.1.2 - A.9.2.2 - A.9.2.3 - A.9.2.5 - A.9.4.1 - A.9.4.2

Nr	Risico	Kans	Impact	x	Risiconiveau	Maatregelen / behandelplan
18	**Berichten worden inzichtelijk voor ongeautoriseerden als gevolg van kwetsbaarheden in de opslag en toegang van de backup data** Aangezien de backup data een veelheid aan berichten bevat over een langere periode is ongeautoriseerde toegang / hack op de backup data een relevant risico. Zie ook risico #14. *Categorie*: Ongeautoriseerde toegang	Onwaarschijnlijk	Groot	11	Normaal	*Bestaande maatregelen*: - Beperkte toegang / afscherming van backup data *Nieuw te nemen maatregelen*: - Beperken van backup retentie - Beperken van backup data - Controle op mogelijke kwetsbaarheden *ISO 27001 beheersmaatregelen*: - A.12.3.1 - A.12.6.1

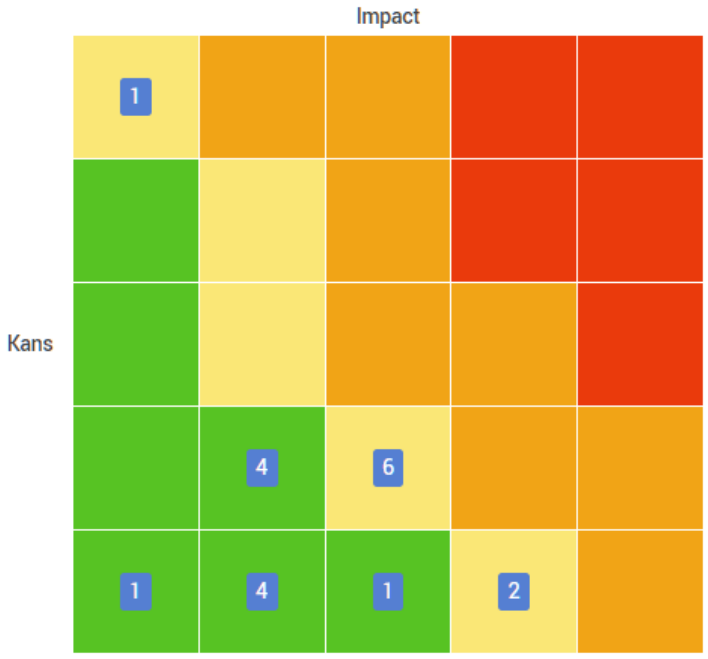
Nr	Risico	Kans	Impact	x	Risiconiveau	Maatregelen / behandelplan
19	**Verstoring van de dienstverlening door het niet kunnen terugplaatsen van een backup ouder dan ~1 uur** Terugplaatsen van een oudere backup (zeg >1 uur oud) levert meer problemen op en kan eigenlijk niet, in plaats daarvan lijkt het verstandiger om eventuele problemen rechtstreeks met betrokken deelnemers op te lossen. Dit beïnvloedt met name de waarschijnlijkheid van het probleem maar levert ook een nieuw risico op. Zie ook risico #15. *Categorie*: Betrouwbaarheid van systemen	Zelden	Klein	6	Laag	*Bestaande maatregelen*: - *Nieuw te nemen maatregelen*: - Beschrijven van restore procedure / beperkingen *ISO 27001 beheersmaatregelen*: - A.12.1.2 - A.12.3.1

Overzichten

Risicoprofiel



Risicomatrix



axxemble

houdt informatie veilig

www.axxemble.nl
info@axxemble.nl
+31(0)85 30 38 429