Marktconsultatie Content Management Systeem

Kansspelautoriteit (Ksa)
19-2-2025
Versie: 1.0

Inhoudsopgave

1. Algemeen

1.1 Kansspelautoriteit

Gokken is een spelvorm waar mensen zich in kunnen verliezen. De Kansspelautoriteit (Ksa) wil daarom dat mensen dit op een veilige en betrouwbare manier kunnen doen. Het maakt daarbij niet uit of dit op een website, via een app, in een casino of in een speelhal gebeurt.

Onze missie is: veilig spelen. Al onze medewerkers zetten zich hier elke dag voor in: toezien op betrouwbare kansspelen, transparante aanbieders die zich aan de regels houden en een goede bescherming van de speler.

Wij hebben de wettelijke taak om de markt te reguleren en toezicht te houden. Wij handhaven als het ergens misgaat, we geven voorlichting, helpen bij het zo goed mogelijk voorkomen en bestrijden van verslaving en we bieden de mogelijkheid een gokstop te nemen. Zo maken we veilig spelen mogelijk.

Toezichthouder kansspelen

De Kansspelautoriteit is de toezichthouder op de markt voor de kansspelen. Wij zijn een zelfstandig bestuursorgaan en voeren in opdracht van de minister voor Rechtsbescherming het Nederlandse kansspelbeleid uit. Bij het uitvoeren hiervan zijn wij onafhankelijk. Onze taken zijn onder andere vastgelegd in de Wet op de kansspelen.

Ons streven

Wij streven naar een wereld waarin kansspelen betrouwbaar zijn en aanbieders transparant. De speler wordt beschermd. Het spel is eerlijk en de winkansen zijn duidelijk. Er zijn geen gokverslaafden en geen illegale praktijken.

Wat wij doen

De Ksa heeft 3 doelstellingen en 7 wettelijke taken.

De 1e wettelijke taak is het **reguleren van de kansspelmarkt** door vergunningen te verlenen aan kansspelaanbieders. Om een vergunning te krijgen, moeten aanbieders voldoen aan voorwaarden. De Kansspelautoriteit controleert of dat het geval is.

De Kansspelautoriteit houdt **risicogestuurd toezicht**. Dat doen wij door vergunninghouders te controleren. Als de voorwaarden in de vergunning of wet- en regelgeving niet worden nageleefd, gaan wij over tot handhaving. Dat kan op verschillende manieren. Dit varieert van het voeren van een gesprek tot het opleggen van een boete of het intrekken van een vergunning. Toezicht is onze 2e wettelijke taak.

Handhaving is onze 3e wettelijke taak. De Kansspelautoriteit treedt op bij illegale activiteiten, bijvoorbeeld als een kansspel illegaal wordt aangeboden. Het gaat om zowel fysiek als online aangeboden kansspelen.

De 4e wettelijke taak is het **bevorderen van verslavingspreventie**. Dit doen wij door toe te zien op de vergunninghouders, die een zorgplicht hebben. Ook werken wij aan bewustwording van de risico's die er aan kansspelen kleven. Verder stimuleren wij dat organisaties samenwerken om te voorkomen dat consumenten kansspelverslaafd raken.

De 5e wettelijke taak is het geven van **voorlichting en informatie**. Dat is bijvoorbeeld het beantwoorden van vragen van gemeenten - medetoezichthouders - als er vragen zijn over kansspelen. Ook burgers hebben vragen, bijvoorbeeld wat ze kunnen doen als ze vinden dat een spel niet eerlijk is verlopen. Organisaties stellen eveneens vragen, bijvoorbeeld een voetbalvereniging die een loterij wil organiseren en met de opbrengst een nieuwe kantine wil bouwen.

De 6e wettelijke taak is het **tegengaan van gokgerelateerde matchfixing bij vergunninghouders**. Vergunninghouders van (online) sportweddenschappen en de totalisator moeten maatregelen treffen om matchfixing binnen hun wedaanbod te voorkomen en tegen te gaan. Zo moeten de vergunninghouders signalen die kunnen duiden op matchfixing detecteren en melden bij de juiste instanties.

Onze 7e wettelijke taak is het **beheren van het Centraal register uitsluiting kansspelen (Cruks)**. In de missie van de Ksa staat 'Veilig spelen' centraal. Cruks helpt de speler zichzelf te beschermen.

Spelers die zichzelf registreren in Cruks sluiten zich voor ten minste zes maanden uit van deelname aan risicovolle kansspelen bij alle in Nederland legale aanbieders, zowel online als landgebonden. Aanbieders van risicovolle kansspelen met een vergunning zijn verplicht Cruks te raadplegen voordat zij een speler toegang geven tot hun spelaanbod. Behalve vrijwillig is het ook mogelijk onvrijwillig in Cruks te worden geregistreerd. Hiervoor is het nodig dat een belanghebbende, bijvoorbeeld een partner, familielid of kansspelaanbieder, bij de Ksa een verzoek indient tot registratie. Na een zorgvuldige procedure bepaalt de Ksa of het verzoek wordt ingewilligd.

Advies Rechtsbescherming

Naast deze 7 taken adviseert de Kansspelautoriteit de minister voor Rechtsbescherming over het kansspelbeleid. Dat doen wij gevraagd en ongevraagd.

1.2 Inleiding

De Kansspelautoriteit is voor haar online communicatie afhankelijk van een goed werkend CMS-systeem waarop al haar sites kunnen draaien. Het huidige CMS is verouderd en voldoet niet meer aan de wensen en eisen van de organisatie. Het systeem (Iprox) dateert nog uit de tijd voordat de Ksa als zbo opgericht werd. Bij de oprichting van de Ksa in 2012 zijn de contractuele verplichtingen met Infoprojects, de aanbiedende partij van het huidige CMS, van JenV overgenomen. Sindsdien is het contract altijd stilzwijgend verlengd. Voorts is er geen service level agreement (SLA) met de aanbieder en verschillende features van het CMS zijn nu niet beschikbaar voor de Ksa en moeten dus elke keer apart ingekocht worden bij de aanbieder.

Bijkomend probleem is dat er voor verschillende sites van de Ksa verschillende CMS'en in gebruik zijn, andere hebben helemaal geen CMS.

1.3 Doel marktconsultatie

Ksa overweegt via een meervoudig onderhandse aanbestedingsprocedure een state of the art CMS te verkrijgen dat geschikt is voor de komende jaren. En waarbij alle benodigde features door de Ksa zelf zijn te gebruiken. Dit CMS moet de ruggengraat worden achter ons internet en intranet, maar ook achter sites als cruksregister.nl, gokstop.nl en het vernieuwde Loket Kansspel (is nog in ontwikkeling).

Naast het leveren en beheer en onderhoud is ook de migratie van content van de servers van de huidige aanbieder naar die van de nieuwe aanbieder of naar een plek die duurzaam voor de Ksa beschikbaar is en blijft. Deze migratie is onderdeel van deze aanbesteding.

Buiten de aanbesteding valt het design van de vernieuwde webomgeving waarop de Ksa overgaat na de afronding van dit traject. Hierbij geldt: het CMS biedt de structuur waarbinnen we gaan werken. Hoe de sites er visueel uit gaan zien, is dus iets wat wij zelf nader organiseren. Zo ontstaat er een drietrapsraket van inkoop van een nieuw CMS, design van de benodigde webomgevingen en tot slot het migreren van de content vanuit het oude CMS naar het nieuwe CMS.

Kortom: De Ksa wil zo snel mogelijk een nieuw CMS voor al haar online kanalen. Zo kan communicatie met aanbieders, spelers en stakeholders beter worden vormgegeven en kan de communicatie aansluiten op de veranderende situatie binnen de organisatie zelf. De afdeling C&S, die verantwoordelijk is voor de communicatie van de organisatie verandert van uitsluitend service verlenen naar strategisch adviseren en communiceren om de doelen en de missie van de Ksa kracht bij te zetten. Dit kan niet meer met het huidige CMS.

Deze aanbesteding moet dan ook een nieuw CMS opleveren dat voldoet aan alle eisen en wensen die op dit moment op communicatief vlak leven. Tevens moet het nieuwe CMS toekomstbestendig mee kunnen groeien met de veranderende wensen en eisen die de organisatie stelt aan haar communicatie.

Het doel van deze marktconsultatie is tweeledig:

- Duidelijkheid krijgen over de oplossingsrichting en inhoudelijke scope;
- Een indicatie krijgen van doorlooptijd en een grove totaal kosten indicatie.

2. Beoogde situatie

Ksa heeft de volgende rollen onderkent binnen het CMS:

- Redacteur
    - De redacteur houdt zich hoofdzakelijk bezig met het schrijven/plaatsen van content op de website
- Eindredacteur
    - De eindredacteur doet ook de taken van de redacteur, maar heeft daarnaast meer rechten en houdt zich ook bezig met de structuur van de content
- Beheerder
    - De beheerder in het CMS systeem kan rollen toewijzen, wijzigen en/of verwijderen van de gebruikers

Daarnaast verwacht Ksa dat het technische beheer van de onderliggende infrastructuur en technisch applicatiebeheer door de leverancier wordt opgepakt (SaaS dienstverlening met een duidelijke SLA).

Momenteel waardeert Ksa de volgende onderdelen in het huidige CMS:

- Het plaatsen van tekstcontent is “hufterproof”
- Het CMS systeem levert een vaste lay-out
- Het bestaan van de functie om content in te plannen
- Het systeem verwerkt een publicatie direct
- Het is makkelijk om interne links te plaatsen naar andere pagina’s binnen de website
- Het is makkelijk om content te verplaatsen
- Het bestaan van de voorvertoning optie en daarin het bewerken van de blokken
- Het is mogelijk om social content toe te voegen (blog/microblogs incl. reacties)
- Het systeem beschikt over een evenementenagenda
- De verschillende beheerde websites worden overzichtelijk weergegeven in het systeem
- De functie om pagina’s te testen voordat ze gepubliceerd worden
- Content en pagina’s worden automatisch gecheckt op webtoegankelijkheid voordat deze gepubliceerd wordt
- Het is mogelijk om fouten ongedaan te maken d.m.v. een ‘vorige versies’-functie

Het toekomstige systeem dient, naast intuïtiever, moderner en toekomstbestendiger, betere ondersteuning te geven bij:

- Uitgebreide mogelijkheden om zelf designkeuzes te maken
- In de huidige situatie moeten veel wijzigingen op de sites verlopen via de IT-leverancier, waardoor diverse wijzigingen via hen moet lopen. Dit zorgt voor tijdverlies wanneer er iets aangepast moet worden op de website
- In het CMS systeem moet duidelijk zijn wat welke content is of waar iets te vinden is
- Het plaatsen van multimedia op websites moet zo gemakkelijk mogelijk zijn. Video’s moeten direct in een bericht geüpload worden
- Met een zo beperkt mogelijk aantal klikken/handelingen moet je bij het deel van de site komen die je wilt bewerken
- De benaming van de blokken in de lay-out dient logisch te zijn en (zelfstandig) aangepast te kunnen worden
- Het toevoegen van applicaties moet op pagina’s mogelijk zijn ook in een later stadium
- De lay-out van een pagina is aanpasbaar
- Het is mogelijk om zelf monitoringtools en plugins te installeren (Google Ads/Piwik)
- Er kunnen zelfstandig formulieren toegevoegd/aangepast worden op de website
- Er is een nieuwsbriefmodule, waarin ook data verkregen kan worden over de nieuwsbrieven die worden uitgestuurd
- Het CMS systeem levert voor elke gebruiker zijn eigen werkomgeving, zodat deze alleen te zien krijgt waar hij/zij in hoort te werken. Dit voorkomt onnodig klikken om tot de juiste plek te komen in het systeem
- Uitgebreidere designmogelijkheden
- Een overzicht van ingeplande content

- Een goed georganiseerde bibliotheekfunctie
- Het systeem maakt geüploade PDF's automatisch webtoegankelijk
- Het systeem moet het mogelijk maken om meerdere sites te beheren via één systeem

3. Vragen

Ksa heeft een aantal vragen geformuleerd die zij graag wil voorleggen aan de markt in het kader van deze marktconsultatie. Deze vragen zijn opgenomen in Naast de elders in dit document en de bijbehorende bijlagen vermelde voorwaarden en bepalingen zijn op deze marktconsultatie ook de onderstaande voorwaarden en bepalingen van toepassing:

- De marktconsultatie is geen onderdeel van een mogelijke aanbesteding maar een consultatieronde.
- De Ksa behoudt zich het recht voor deze marktconsultatie tijdelijk of definitief te staken.
- De antwoorden zullen intern worden besproken en intern worden geadministreerd.
- Marktpartijen die niet meedoen aan de marktconsultatie zijn daarmee niet uitgesloten van deelname aan een mogelijke aanbesteding. Evenmin zijn marktpartijen die deelnemen aan de marktconsultatie op enige wijze bevoorrecht in een eventuele deelname aan een aanbesteding.
- De marktconsultatie is voor zowel alle deelnemers als de Ksa vrijblijvend.
- Partijen (inclusief partijen die niet deelnemen aan de marktconsultatie) kunnen aan deze marktconsultatie geen (wederzijdse) verplichtingen of rechten jegens de Ksa ontlenen.
- Deelname aan deze marktconsultatie biedt geen enkel recht op het verkrijgen van een opdracht.
- Eventuele kosten voor deelname aan deze marktconsultatie worden niet vergoed.
- Deelnemende marktpartijen stemmen ermee in dat door hen aangeleverde informatie verwerkt kan worden in het programma van eisen.
- De inbreng van deelnemende partijen zal zoveel mogelijk vertrouwelijk behandeld worden.
- Claims over het gebruik van informatie, vertrouwelijkheid of verzoeken om vergoeding in verband hiermee worden niet gehonoreerd.
- De Ksa is op geen enkele wijze gebonden aan de uitkomsten van de marktconsultatie of verplicht tot realisatie en/of aanbesteding van het project waarop de marktconsultatie betrekking heeft.
- Door deelname aan deze marktconsultatie geven partijen te kennen onvoorwaardelijk akkoord te gaan met de voorwaarden en bepalingen zoals vermeld in dit document.
- De voertaal tijdens deze marktconsultatie is Nederlands.

Bijlage 1 Kengetallen

Kenmerken	Nu
Aantal redactie gebruikers	ca. 10
Aantal intranet bezoekers	250
Aantal websites	5 tot 7
Aantal admin gebruikers	5
Aantal bezoekers websites	161.000 per maand (met 5% terugkerende bezoekers)
Nieuwsbrief abonnees	1500

Bovengenoemde kengetallen zijn indicatief. In de komende jaren wordt een toename verwacht in de hoeveelheid content, mede ook door opslag van meer beelden en video's.

4. Procedure marktconsulatie

Communicatie

Deze marktconsultatie wordt toezonden aan een aantal partijen die uit een eerste marktverkenning naar voren zijn gekomen.

Tijdens de marktconsultatie verloopt alle communicatie met betrekking tot dit onderwerp via de volgende contactpersoon Sander Grip; e-mailadres: sgrip@kansspelautoriteit.nl.

Planning

Hieronder is de planning voor de marktconsultatie opgenomen.

Activiteit	Planning
Verzenden marktconsultatie	20 februari
Mogelijkheid voor de marktpartijen tot het stellen van aanvullende vragen (middels bijlage 3)	27 februari
Beantwoording Ksa aanvullende vragen	4 maart
Inleveren antwoorden marktconsultatie	10 maart
Eventuele uitnodiging voor een gesprek	Uiterlijk 12 maart
Gesprekken met geselecteerde deelnemers	17-18 maart

Gesprekken marktconsultatie

Er worden uit alle reacties vanuit de marktconsultatie ongeveer 3-4 partijen uitgenodigd voor een gesprek en eventueel korte demo. Voor ieder gesprek is ca. 2 uur beschikbaar. Indien er meer dan 4 reacties uit de markt zijn teruggekomen, kan de Ksa ervoor kiezen een selectie te maken in uit te nodigen partijen. Selectie vindt plaats passend binnen de beschreven doelstellingen en gewenste situatie.

Per aanbieder mogen maximaal twee personen aanwezig zijn bij een eventueel gesprek. Tijdens het gesprek wordt er verder ingegaan op de gegeven antwoorden en kan de aanbieder een uitleg/demonstratie geven van de mogelijke oplossing. De aanbieder is vrij om te bepalen hoe hij deze uitleg/demonstratie vorm wil geven. De Ksa kan er in het kader van de marktconsultatie voor kiezen bepaalde vragen vanuit de aanbieder niet te beantwoorden. Dit om, indien de vraag van de Ksa in de markt wordt gezet, deze aanbieder geen voordeel te geven ten opzichte van de partijen die niet voor een gesprek zijn uitgenodigd.

De informatie uit de marktconsultatie wordt mogelijk gebruikt als input voor eventuele vervolgtrajecten. Bij een publicatie van een eventueel vervolgtraject, waarin de gegevens van de marktconsultatie worden gebruikt, hebben alle bedrijven die hierop inschrijven evenveel kans om voor gunning in aanmerking te komen. Dit is onafhankelijk van het wel of niet meedoen met deze marktconsultatie c.q. uitgenodigd worden voor een toelichtingsgesprek. In het kader van transparantie zal alle informatie uit de marktconsultatie met alle aangeschreven partijen worden gedeeld, of openbaar gemaakt.

In het kader van de marktconsultatie heeft u de mogelijkheid om via de eerder genoemde contactpersoon vragen te stellen aan de Ksa conform het gestelde in deze paragraaf en met gebruikmaking van het formulier dat is opgenomen in Bijlage 3 Vragenformulier voor het stellen van vragenDe beantwoording van de vragen wordt gedeeld aan alle deelnemende partijen. Alle volgens dit document op tijd en correct ingediende vragen zullen geanonimiseerd beantwoord worden.

5. Voorwaarden en bepalingen

Naast de elders in dit document en de bijbehorende bijlagen vermelde voorwaarden en bepalingen zijn op deze marktconsultatie ook de onderstaande voorwaarden en bepalingen van toepassing:

- De marktconsultatie is geen onderdeel van een mogelijke aanbesteding maar een consultatieronde.
- De Ksa behoudt zich het recht voor deze marktconsultatie tijdelijk of definitief te staken.
- De antwoorden zullen intern worden besproken en intern worden geadministreerd.
- Marktpartijen die niet meedoen aan de marktconsultatie zijn daarmee niet uitgesloten van deelname aan een mogelijke aanbesteding. Evenmin zijn marktpartijen die deelnemen aan de marktconsultatie op enige wijze bevoorrecht in een eventuele deelname aan een aanbesteding.
- De marktconsultatie is voor zowel alle deelnemers als de Ksa vrijblijvend.
- Partijen (inclusief partijen die niet deelnemen aan de marktconsultatie) kunnen aan deze marktconsultatie geen (wederzijdse) verplichtingen of rechten jegens de Ksa ontlenen.
- Deelname aan deze marktconsultatie biedt geen enkel recht op het verkrijgen van een opdracht.
- Eventuele kosten voor deelname aan deze marktconsultatie worden niet vergoed.
- Deelnemende marktpartijen stemmen ermee in dat door hen aangeleverde informatie verwerkt kan worden in het programma van eisen.
- De inbreng van deelnemende partijen zal zoveel mogelijk vertrouwelijk behandeld worden.
- Claims over het gebruik van informatie, vertrouwelijkheid of verzoeken om vergoeding in verband hiermee worden niet gehonoreerd.
- De Ksa is op geen enkele wijze gebonden aan de uitkomsten van de marktconsultatie of verplicht tot realisatie en/of aanbesteding van het project waarop de marktconsultatie betrekking heeft.
- Door deelname aan deze marktconsultatie geven partijen te kennen onvoorwaardelijk akkoord te gaan met de voorwaarden en bepalingen zoals vermeld in dit document.
- De voertaal tijdens deze marktconsultatie is Nederlands.

Bijlage 1 Kengetallen

Kenmerken	Nu
Aantal redactie gebruikers	ca. 10
Aantal intranet bezoekers	250
Aantal websites	5 tot 7
Aantal admin gebruikers	5
Aantal bezoekers websites	161.000 per maand (met 5% terugkerende bezoekers)
Nieuwsbrief abonnees	1500

Bovengenoemde kengetallen zijn indicatief. In de komende jaren wordt een toename verwacht in de hoeveelheid content, mede ook door opslag van meer beelden en video's.

Bijlage 2 Beantwoording vragen marktconsultatie

Het is **niet** noodzakelijk dat u op iedere vraag een (uitgebreid) antwoord geeft, mocht u een vraag willen overslaan dan is dit toegestaan.

Nr.	Vraag
Algemeen	
1	Kunt u uw oplossing voor een toekomstige situatie schetsen voor de Ksa? Wat maakt uw oplossing anders dan andere oplossingen in de markt?
Antwoord	
2	Welk CMS (of CMS-en) lijken op het eerste gezicht het beste passend voor Ksa? Kunt u ook aangeven waarom?
Antwoord	
3	Welke referenties per CMS kunt u noemen die het meeste lijken op Ksa
Antwoord	
4	Kunt u geheel zelfstandig de gevraagde werkzaamheden en/of functionaliteit verzorgen of werkt u samen met partners?
Antwoord	
5	Kunt u uw oplossing als SaaS – dienst aanbieden?
Antwoord	
6	Bestaat uw oplossing uit open source onderdelen?
Antwoord	
7	Is het logisch dat de Ksa de functionaliteit voor een (sociaal) intranet meeneemt in de scope van deze aanbesteding?
Antwoord	
8	Is het logisch dat Ksa de functionaliteit voor SEO meeneemt in de aanbesteding?
Antwoord	
9	Wat zijn de verschillen en voor- en nadelen van een traditioneel, headless of DXP CMS volgens u? Welke traditioneel, headless of DXP CMS kunt u leveren en ondersteunen?
Antwoord	
10	Beheert u bij een headless CMS ook de API’s?
Antwoord	
Implementatie	
11	Wat verwacht u tijdens de implementatie en migratie van de Ksa?
Antwoord	
12	Welke doorlooptijd verwacht u nodig te hebben tussen opdrachtverstrekking en ingebruikname (implementatie en migratie)?
Antwoord	
13	Welke kosten schat u voor het implementeren en migreren van nieuwe CMS-omgeving en migratie naar de nieuwe omgeving (een bandbreedte zou al voldoende zijn)?
Antwoord	

14	Zijn er onderdelen die de benodigde kosten sterk verhogen? Welke zijn dit en welk percentage van de kosten is dit dan ongeveer?
Antwoord	
Beheer en onderhoud	
15	Wat verwacht u tijdens het beheer van de Ksa?
Antwoord	
16	Welke standaard SLA met welke service levels hanteert u (beschikbaarheid, RTO-tijd, RPO-tijd etc.)?
Antwoord	
17	Welke kosten zijn gemoeid met voor het beheer van de omgeving (een bandbreedte op basis van een eerste calculatie op basis van aannames is voldoende)?
Antwoord	
18	Hoe worden de beheerkosten doorbelast, wat is uw afrekenmechanisme (bv. aantal GB content en/of aantal soort gebruikers (welke soorten gebruikers onderscheidt u)?
Antwoord	
19	In het CMS komt gevoelige informatie, hoe waarborgt u informatie beveiliging zodat Ksa kan voldoen aan de BIO BBN-2? Is uw oplossing een single tenant omgeving in een private cloud?
Antwoord	
20	Wat vindt u van de genoemde 31 beveiligingsaspecten in bijlage 4. Zijn deze voor een CMS redelijk en haalbaar?
Antwoord	
21	In het geval dat er strikte vertrouwelijke gegevens en/of (bijzondere) persoonsgegevens worden opgeslagen in uw CMS/ intranet heeft u , inclusief eventuele onderaannemers, dan adequate technische en organisatorische maatregelen genomen (bv opslag in de EER, ? Zo ja welke?
Antwoord	
22	Wat wilt u overigens nog kwijt ten behoeve van deze marktconsultatie?
Antwoord	

Ondertekening	
Onderneming	
Naam	
Functie	
Bereikbaarheidsgegevens (telefoonnummer, e-mail)	
Handtekening	
Plaats en datum	

Deze Bijlage is als separaat Word document toegevoegd.

Bijlage 3 Vragenformulier voor het stellen van vragen

Voor het indienen van vragen met betrekking tot de marktconsultatie dient gebruik gemaakt te worden van dit template.

Onderneming	
Naam en functie	
Bereikbaarheidsgegevens (telefoonnummer, e-mail)	

Nr	**Verwijzing (§, blz.)**	**Vraag**
1.		
Antwoord KSA		
2.		
Antwoord KSA		
3.		
Antwoord KSA		
4.		
Antwoord KSA		
5.		
Antwoord KSA		

Deze Bijlage is als separaat Word document toegevoegd

Bijlage 4 Aandachtspunten beveiliging

nr	Naam Eis	Samenvatting eis:	Mitigeert risico omschrijving:	Mitigeert risico omschrijving:	Mitigeert risico omschrijving:	Mitigeert risico omschrijving:	Mitigeert risico omschrijving:
1	Bedrijfscontinuïteit	De leverancier behoort processen, procedures en beheersmaatregelen te documenteren, te implementeren en te handhaven.	Onnodig lange uitval van bedrijfsactiviteiten na calamiteiten waardoor bedrijfsdoelstellingen niet worden gehaald.				
2	Sessiebeheer	Sessies behoren authentiek te zijn voor elke gebruiker en behoren ongeldig gemaakt te worden na een time-out of perioden van inactiviteit.	Misbruik van kwetsbaarheden in applicaties of hardware.	Onbevoegden maken via kwetsbaarheden gebruik van openstaande sessies en krijgen toegang krijgen tot gevoelige data. Het ontstaan van zwakheden als Cross-Site Request Forgery (CSRF) en Clickjacking.			
3	Gegevensopslag	Te beschermen gegevens worden veilig opgeslagen in databases of bestanden, waarbij zeer gevoelige gegevens worden versleuteld. Opslag vindt alleen plaats als noodzakelijk.	Misbruik van kwetsbaarheden in applicaties of hardware.	Opgeslagen gegevens worden ongeautoriseerd ingezien, aangepast of verwijderd door ontoereikende versleuteling.			
4	Communicatie	Het softwarepakket past versleuteling toe op de communicatie van gegevens die passend bij het classificatieniveau is van de gegevens en controleert hierop.	Misbruik van kwetsbaarheden in applicaties of hardware.	Misbruik van cryptografische sleutels en/of gebruik van zwakke algoritmen.	Onbevoegden krijgen toegang tot getransporteerde gegevens.		
5	Authenticatie	Softwarepakketten behoren de identiteiten van gebruikers vast te stellen met een mechanisme voor identificatie en authenticatie.	Misbruik van kwetsbaarheden in applicaties of hardware.	Misbruik van andermans identiteit.	Onterecht hebben van rechten.	Onbevoegde personen krijgen toegang tot de data in het softwarepakket.	
6	Toegangsautorisatie	Het softwarepakket behoort een autorisatiemechanisme te bieden.	Misbruik van kwetsbaarheden in applicaties of hardware.	Het toegang krijgen tot gegevens die niet noodzakelijk zijn voor het uitvoeren van de rol/functie.			
7	Autorisatiebeheer	De rechten die gebruikers hebben binnen een softwarepakket (inclusief beheerders) zijn zo ingericht dat autorisaties kunnen worden toegewezen aan organisatorische functies en scheiding van niet verenigbare autorisaties mogelijk is.	Misbruik van kwetsbaarheden in applicaties of hardware.	Misbruik van andermans identiteit.	Onterecht hebben van rechten.	Misbruik van gegevens in een softwarepakket.	
8	Logging	Het softwarepakket biedt signaleringsfuncties voor registratie en detectie die beveiligd zijn ingericht.	Incidenten worden niet tijdig opgepakt.	Informatie voor het aanpakken van incidenten ontbreekt.	Ketenafhankelijke data (-bestanden) input/output uit systemen	Afwijkingen van normaal gedrag binnen het softwarepakket zijn niet zichtbaar.	
9	Application Programming Interface (API)	Softwarepakketten behoren veilige API's te gebruiken voor import en export van gegevens.	Aanvallen via systemen die niet in eigen beheer zijn.	Misbruik van kwetsbaarheden in applicaties of hardware.	Ketenafhankelijke data (-bestanden) input/output uit systemen	Gegevens kunnen niet uitgewisseld worden.	
10	Malwareprotectie	Ter bescherming tegen malware behoren beheersmaatregelen voor preventie, detectie en herstel te worden geïmplementeerd, in combinatie met het stimuleren van een passend bewustzijn van gebruikers.	Toegang tot informatie wordt geblokkeerd.	Misbruik van kwetsbaarheden in applicaties of hardware.	Incidenten worden niet tijdig opgepakt.	Verificatie op corrupte data(-bestanden) uit de keten.	Malware wordt niet of te laat opgespoord en aangetroffen malware wordt niet of voldoende hersteld.
11	Hardenen server	Voor het beveiligen van een server worden overbodige functies en ongeoorloofde toegang uitgeschakeld.	Uitval van systemen door configuratiefouten.	Misbruik van kwetsbaarheden in applicaties of hardware.	Uitval van systemen door hardwarefouten.	Misbruik van overbodige en/of niet gebruikte functies, services en accounts.	

					Schade door het niet opmerkingen van fouten en/of onrechtmatighed en in het gebruik van waaronder ongeautoriseerde toegangspoginge n tot technische componenten.		
12	Logbestanden beheerders	Activiteiten van systeembeheerders en -operators behoren te worden vastgelegd en de logbestanden behoren te worden beschermd en regelmatig te worden beoordeeld.	Misbruik van speciale bevoegdheden.	Onterecht hebben van rechten.			
13	Logging	Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurte nissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.	Systemen worden niet gebruikt waarvoor ze bedoeld zijn.	Informatie voor het aanpakken van incidenten ontbreekt.	Foutieve informatie.	Ongeoorloofde acties op servers en besturingssyste men worden niet opgemerkt. Bij wel opmerken, is er geen bewijs voorhanden.	
14	Zonering en filtering	Groepen van informatiediensten, -gebruikers en -systemen behoren in netwerken te worden gescheiden (in domeinen).	Misbruik van speciale bevoegdheden.	Misbruiken van zwakheden in netwerkbeveiliging.	Toegang tot informatie wordt geblokkeerd.	Aanvallen via systemen die niet in eigen beheer zijn.	Verspreiding van aanvallen, indringers, ongewenste inhoud, virussen etc. in de organisatie.
15	Cryptografische services	Ter bescherming van de vertrouwelijkheid en integriteit van de getransporteerde informatie behoren passende cryptografische beheersmaatregelen te worden ontwikkeld, geïmplementeerd en ingezet.	Misbruik van cryptografische sleutels en/of gebruik van zwakke algoritmen.	Het openbaar worden van vertrouwelijke informatie en/of het corrumperen van informatie door kwaadwillenden.			
16	Logging en monitoring	Netwerken behoren te worden gemonitord op afwijkend gedrag en er behoren passende maatregelen te worden getroffen om potentiële informatiebeveiligingsincidente n te evalueren; logbestanden worden geregistreerd en bewaard.	Incidenten worden niet tijdig opgepakt.	Informatie voor het aanpakken van incidenten ontbreekt.	Herhaling van incidenten.	Afwijkingen van normaal gedrag zijn niet zichtbaar en niet te onderzoeken. Herstelacties kunnen niet tijdig worden genomen.	
17	Netwerk beveiligingsarch itectuur	De beveiligingsarchitectuur behoort de samenhang van het netwerk te beschrijven en structuur te bieden in de beveiligingsmaatregelen, gebaseerd op het vigerende bedrijfsbeleid, de leidende principes en de geldende normen en standaarden.	Misbruiken van zwakheden in netwerkbeveiliging.	Onvoldoende aandacht voor beveiliging bij uitbesteding van werkzaamheden.	Geen sturing hebben op de netwerkbeveiligin g.		
18	Inlogprocedure	Indien het beleid voor toegangsbeveiliging dit vereist, behoort toegang tot systemen en toepassingen te worden beheerst door een beveiligde inlogprocedure.	Misbruik van andermans identiteit.	Misbruik van speciale bevoegdheden.	Misbruik van kwetsbaarheden in applicaties of hardware.	Misbruiken van zwakheden in netwerkbeveiligi ng.	Er is misbruik en verlies van gevoelige gegevens en beïnvloeding van beschikbaarheid van informatiesyste men.
19	Wachtwoordenb eheer	De toewijzing en het beheer van authenticatie-informatie behoort te worden beheerst door middel van een beheerproces waarvan het adviseren van het personeel over de juiste manier van omgaan met authenticatie-informatie deel uitmaakt.	Slecht wachtwoordgebruik.	Bedrijfsbelangen lopen schade op.			
20	Fysieke toegangsbeveili ging	Beveiligde gebieden behoren te worden beschermd door passende toegangsbeveiliging.	Misbruik van andermans identiteit.	Misbruik van speciale bevoegdheden.	Misbruik van kwetsbaarheden in applicaties of hardware.	Misbruiken van zwakheden in netwerkbeveiligi ng.	Onbevoegden brengen schade toe aan en verstoringen in de computerruimte en aan informatie in de Huisvesting-IV-organisatie teweeg.

21	Transparantie	De CSP voorziet de CSC in een systeembeschrijving waarin de clouddiensten inzichtelijk en transparant worden gespecificeerd en waarin de jurisdictie, onderzoeksmogelijkheden en certificaten worden geadresseerd.	Gebrek aan sturing op informatiebeveiliging vanuit de directie.	Lijnmanagers nemen hun verantwoordelijkheid voor informatiebeveiliging niet.	Onvoldoende aandacht voor beveiliging binnen projecten.	Onduidelijkheid over classificatie en bevoegdheden.	Onvoldoende aandacht voor beveiliging bij uitbesteding van werkzaamheden.
22	Privacy en bescherming persoonsgegevens	De CSP behoort, ter bescherming van bedrijfs- en persoonlijke data, beveiligingsmaatregelen te hebben getroffen vanuit verschillende dimensies: beveiligingsaspecten en stadia, toegang en privacy, classificatie/labelen, eigenaarschap en locatie.	Onduidelijkheid over classificatie en bevoegdheden.	De bedrijfs- en persoonlijke data wordt onderbeveiligd.			
23	Clouddienstenarchitectuur	De CSP heeft een actuele architectuur vastgelegd die voorziet in een raamwerk voor de onderlinge samenhang en afhankelijkheden van de IT-functionaliteiten.	Toelaten van externen in het pand of op het netwerk.	Misbruik van andermans identiteit.	Misbruik van speciale bevoegdheden.	Onterecht hebben van rechten.	Onduidelijkheid over classificatie en bevoegdheden.
24	Herstelfunctie voor data en clouddiensten	De herstelfunctie van de data en clouddiensten, gericht op ondersteuning van bedrijfsprocessen, behoort te worden gefaciliteerd met infrastructuur en IT-diensten, die robuust zijn en periodiek worden getest.	Niet beschikbaar zijn van diensten van derden.	Informatie voor het aanpakken van incidenten ontbreekt.	Uitval van systemen door configuratiefouten.	Uitval van systemen door softwarefouten.	Fouten als gevolg van wijzigingen in andere systemen.
25	Dataprotectie	Data ('op transport', 'in verwerking' en 'in rust') met de classificatie BBN2 of hoger behoort te worden beschermd met cryptografische maatregelen en te voldoen aan Nederlandse wetgeving.	Wetgeving over het gebruik van cryptografie.	Data met de classificatie BBN2 of hoger is onvoldoende beveiligd			
26	Datascheiding	CSC-gegevens behoren tijdens transport, bewerking en opslag duurzaam geïsoleerd te zijn van beheerfuncties en data van en andere dienstverlening aan andere CSC's, die de CSP in beheer heeft.	Onveilig versturen van gevoelige informatie.	Versturen van gevoelige informatie naar onjuiste persoon.	Informatieverlies door verlopen van houdbaarheid van opslagwijze.	Foutieve informatie.	Misbruik van cryptografische sleutels en/of gebruik van zwakke algoritmen.
27	Scheiding dienstverlening	De cloud-infrastructuur is zodanig ingericht dat de dienstverlening aan gebruikers van informatiediensten zijn gescheiden.	Toegang tot informatie wordt geblokkeerd.	Aanvallen via systemen die niet in eigen beheer zijn.	Misbruiken van zwakheden in netwerkbeveiliging.	Beïnvloeding of communicatie van data.	
28	Malware-protectie	Ter bescherming tegen malware behoren beheersmaatregelen te worden geïmplementeerd voor detectie, preventie en herstel in combinatie met een passend bewustzijn van de gebruikers.	Toegang tot informatie wordt geblokkeerd.	Misbruik van kwetsbaarheden in applicaties of hardware.	Verificatie op corrupte data(-bestanden) uit de keten.	Malware wordt niet opgespoord en aangetroffen malware wordt niet of voldoende hersteld.	
29	Koppelvlakken	De onderlinge netwerkconnecties (koppelvlakken) in de keten van de CSC naar de CSP behoren te worden bewaakt en beheerst om de risico's van datalekken te beperken.	Misbruiken van zwakheden in netwerkbeveiliging.	Toegang tot informatie wordt geblokkeerd.	Aanvallen via systemen die niet in eigen beheer zijn.	Onveilig versturen van gevoelige informatie.	Versturen van gevoelige informatie naar onjuiste persoon.

30	Logging en monitoring	Logbestanden waarin gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiliging gebeurtenissen worden geregistreerd, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.	Incidenten worden niet tijdig opgepakt.	Informatie voor het aanpakken van incidenten ontbreekt.	Herhaling van incidenten.	Achteraf wordt niet de juiste actie ondernomen. Er wordt niet vastgesteld wie welke handelingen heeft uitgevoerd.	Afwijkingen van normaal gedrag zijn niet zichtbaar en niet te onderzoeken en herstelacties kunnen niet tijdig worden genomen.
31	Multi-tenantarchitectuur	Bij multi-tenancy wordt de CSC-data binnen clouddiensten, die door meerdere CSC's worden afgenomen, in rust versleuteld en gescheiden verwerkt op gehardende (virtuele) machines	Onveilig versturen van gevoelige informatie.	Misbruik van cryptografische sleutels en/of gebruik van zwakke algoritmen.	Geen of onvoldoende sturing hebben		