

Resultaten Marktconsultatie Websites

Nederlands Instituut Publieke Veiligheid
Kemperbergerweg 783
6816 RW Arnhem
www.nipv.nl
info@nipv.nl
088 - 274 74 00

Colofon

Opdrachtgever:	Nederlands Instituut Publieke Veiligheid
Titel:	Resultaten marktconsultatie Websites
Datum:	25-02-2026
Status:	Definitief
Versie:	1.0

Het Nederlands Instituut Publieke Veiligheid is bij wet vastgelegd onder de naam Instituut Fysieke Veiligheid.

1 Resultaten

1.1 Concept programma van eisen (bijlage 1) NIPV.nl

1.	Kan uw organisatie de diensten conform de genoemde eisen leveren? Zo niet, waar ziet u uitdagingen en heeft u suggesties om dit te ondervangen?	Er hebben 7 partijen gereageerd die aangeven gevraagde dienstverlening te kunnen leveren, allen met (kleine) aanpassingen.
2.	Zijn er eisen opgenomen die naar uw inzicht overbodig zijn, omdat bijvoorbeeld de gevraagde functies ook op een andere manier haalbaar zijn? Zo ja, welke en hoe zijn deze haalbaar?	Eis 36: Escrow is overbodig bij een open source platform (een gedeelde GIT Repository volstaat) Eis 22 (archiefweb): Hiervoor worden geen werkzaamheden verwacht. Advies om eisen waar mogelijk functioneel te formuleren (wat moet het platform kunnen en welke kwaliteitseisen gelden), en de concrete invulling over te laten aan de opdrachtnemer binnen de kaders van WordPress. Dit vergroot de ruimte voor een onderhoudbare, veilig te beheren en toekomstbestendige inrichting, zonder dat het NIPV concessies hoeft te doen op de gewenste functionaliteit of kwaliteit.
3.	Kunt u op basis van het concept programma van eisen aangeven of: a. Er eisen gesteld worden die onnodig beperkend zijn? b. Er eisen gesteld worden die onnodig kostenverhogend zijn? c. Er eisen gesteld worden die onduidelijk zijn? d. Er eisen gesteld worden die om een andere reden niet wenselijk zijn? e. Er eisen gesteld worden die discriminerend zijn? f. Er eisen zijn die gemist worden? Indien ja, graag aangeven welke?	Beperkend: - Geschiktheidseisen, advies om ISO 22301, 14001 en 270127 als optioneel / nice to have op te nemen. ISO 22301 is al onderdeel van 27001 en dus onnodig. Alleen 27001 en evt 9001 (beide of vergelijkbaar) opnemen. - Eis 14 en 15: Specifieke ervaring met bestaande CMS keuze en commerciële plug-ins; in Nvl 2 aangegeven dat "ervaring met plug-ins die een vergelijkbaar doel vervullen" ook akkoord is. - As-is overname beperkt efficiency verbeteringen en heeft gevolgen. - Overweeg om kritieke (beveiligings)updates zonder vooraf overleg uit te laten voeren. Kostenverhogend: - 24/7 beschikbaarheid is kostbaar; geef hierin ook specifiek aan voor welke dienstverlening dit wordt verwacht.

		- De eis rondom jaarlijkse penetratietesten is kostenverhogend wanneer deze niet doelgericht wordt afgebakend. Advies om pentests primair te richten op de applicatie- en configuratielaag, zodat inspanning en risico's in balans zijn. - ESCROW regeling is onnodig. - SIEM praktisch onmogelijk zonder SOC. Andersom is een SOC zonder SIEM zonder waarde. Advies om uit te schrijven wat NIPV hierin verwacht. - De penetratietest zoals omschreven bij eis 34 is in de praktijk zeer kostenverhogend omdat dit zou kunnen betekenen dat er bij elke maandelijkse update een penetratietest uitgevoerd zou moeten worden. Advies om specifieker te beschrijven. Onduidelijk: - Eis 37: Cloud Security Privacy Control Framework van JenV; welke clouddiensten vallen hieronder? Concreet uitwerken. - Het is belangrijk dat in de aanbestedingsfase helder wordt afgebakend welke activiteiten onder de vaste SLA/DAP vallen en welke als implementatie, stabilisatie of doorontwikkeling worden beschouwd. Dit voorkomt misinterpretatie en scope creep. Niet wenselijk: - Niet alle geschiktheidseisen lijken relevant. - Advies om in de aanbestedingsstukken expliciet een overdrachts- en overgangsfase op te nemen, inclusief minimale overdrachtsdocumentatie en bij voorkeur een korte change freeze. Dit maakt de beheersnaam beter beheersbaar en verlaagt het risico op verstoringen. Discriminerend: - Veelheid aan geschiktheidseisen die eerder zijn genoemd. Gemist: - Het NIPV voldoet momenteel aan 28 van de 50 toegankelijkheidseisen (NvI 2 vraag 62). Wij adviseren deze informatie te delen met inschrijvers. Het verschil tussen 28/50 en 50/50 is een aanzienlijke hoeveelheid werk. Zonder dit inzicht moeten partijen een worst case scenario bepalen, wat leidt tot hogere en minder realistische aanbiedingen. - Wij adviseren om explicieter te maken welke minimale overdrachtsactiviteiten en documentatie van de huidige leverancier worden verwacht, zodat de nieuwe opdrachtnemer de omgeving aantoonbaar beheersbaar kan overnemen. - Toekomstvisie mist; hoe wordt samen doorontwikkeld.
--	--	---

		- Daarnaast adviseren wij om binnen de aanbesteding expliciet aandacht te besteden aan hoogwaardige (API-)koppelingen. Juist slimme integraties maken processen efficiënter en zorgen ervoor dat systemen écht met elkaar samenwerken. - Vul SLA eisen in SLA in in plaats van in het PvE. - Het document noemt functionaliteit en beheer, maar mist een concrete eis met betrekking tot minimale laadsnelheid of webperformance (bijv. Google PageSpeed Score), wat essentieel is voor de gebruiksvriendelijkheid en vindbaarheid van de publieke websites
4.	Ziet u knelpunten in het overnemen van de huidige websiteomgeving zonder dat er onderbreking plaatsvindt?	Een aantal partijen zien geen knelpunten Enkele wel; - Een korte change stop zou de migratie vereenvoudigen.) - Er moet aan een aantal voorwaarden worden voldaan en zijn aanvullende werkzaamheden nodig. - Kijk kritisch naar optimalisatie van aantal plug-ins
5.	Zijn er plug-ins in gebruik die volgens u een risico vormen als deze door u beheerd moeten worden? En zo ja: zijn er volgens u geschikte alternatieve plug-ins beschikbaar die vóór 15 november geïmplementeerd kunnen worden?	Van de maatwerk plug-ins dient meer informatie beschikbaar te worden gesteld om hierop eenduidig te kunnen antwoorden. Het hoeft geen risico te zijn maar hierover is op dit moment onvoldoende informatie beschikbaar.
6.	Ziet u uitdagingen in het voldoen aan 'één of meerdere van de gestelde eisen onder 'Service management (SLA) & Dossier Procedures en Afspraken (DAP) (PvE)', in combinatie met het gestelde maximumbedrag voor de SLA en DAP.	De meeste partijen zien geen uitdagingen, mits de scope van de SLA duidelijk wordt afgebakend. Specifiek wordt aandacht gevraagd rondom: • Prio-1 meldingstermijn en in welke situaties moet worden ingegrepen • 24/7 beschikbaarheid • Penetratietesten en of deze binnen of buiten de SLA worden uitgevoerd
7.	Wat is volgens u een geschikt maximumbedrag voor de implementatiekosten die gemaakt moeten worden om de huidige multi-site omgeving van het NIPV over te nemen?	Bedragen lopen uiteen van €5.000,- tot €85.000,- . Factoren die als implementatiekostenverhogend benoemd worden, zijn: • Comaxx plug-ins en de volledigheid en kwaliteit van de aanwezige documentatie. • Strengere beveiligingseisen • Verouderde plug-ins die bij implementatie beter vervangen kunnen worden. • Diverse integraties (API-koppelingen) met externe systemen • Mate van technische achterstand

		• Complexiteit overhevelen OTAP-omgeving (incl. Alle genoemde subsites)
--	--	---

1.2 Concept programma van eisen (bijlage 1) Brandweer.nl

8.	Kan uw organisatie de diensten conform de genoemde eisen leveren? Zo niet, waar ziet u uitdagingen en heeft u suggesties om dit te ondervangen?	De meeste partijen geven aan de diensten conform de eisen te kunnen leveren, maar benoemen een aantal kritieke randvoorwaarden: - Technische Complexiteit: De omvangrijke contentstructuur (CPT's, vacatures, kazernes) en integraties met HR-systemen worden als uitdagende aandachtspunten gezien. - Transitie en Overdracht: Een zorgvuldige overdracht, een korte change freeze tijdens de migratie en tijdige toegang tot alle documentatie en licenties zijn essentieel om risico's te beperken. - Scope-afbakening: Er is een sterke behoefte aan een heldere definitie van wat onder de vaste SLA/DAP valt en wat als (eenmalige) implementatie of doorontwikkeling wordt beschouwd. - Herbouw vs. Migratie: Sommige partijen adviseren om niet "as-is" te migreren, maar direct te herbouwen binnen een eigen framework om technische schuld en verouderde structuren kwijt te raken
9.	Geef een beschrijving aan welke eisen u niet kunt of wilt voldoen.	Er zijn enkele specifieke certificerings- en technische eisen waar partijen moeite mee hebben: - ISO-certificeringen: Meerdere partijen kunnen niet voldoen aan de eis voor ISO 22301 (Business Continuity) en ISO 14001 (Milieu) als dit een harde eis voor de opdrachtnemer zelf is, in plaats van de onderliggende cloudprovider. - Laadtijdgarantie: Een harde garantie op de laadtijd van de website is voor sommigen onmogelijk, omdat dit mede afhankelijk is van de content die de opdrachtgever zelf plaatst. - BIO-certificering: Hoewel de meeste partijen conform de principes werken (via ISO 27001), beschikken ze niet altijd over een formele BIO-certificering, aangezien dit vaker een in-control verklaring betreft

10.	Geef een beschrijving van de eisen die naar uw inzicht overbodig zijn, omdat bijvoorbeeld de gevraagde functies ook op een andere manier haalbaar zijn.	Marktpartijen wijzen op overlap en verouderde technische voorschriften: - Specifieke Plug-ins: Het voorschrijven van specifieke (soms verouderde of leveranciersgebonden) plug-ins wordt als overbodig en risicovol gezien. Geadviseerd wordt om eisen functioneel te formuleren (bijv. "voorzien in SEO-analyse") in plaats van specifieke productnamen te noemen. - Cumulatie van Certificeringen: De stapeling van ISO 27017, SOC 2 en ISAE 3402 voor de opdrachtnemer zelf wordt als disproportioneel en onnodig kostenverhogend ervaren voor een contract van deze omvang. - Algemene 24/7 Support: Een generieke 24/7 verplichting wordt voor een websiteomgeving niet altijd proportioneel geacht; een risicogedreven benadering (alleen voor kritieke verstoringen) geniet de voorkeur.
11.	Kunt u op basis van het concept programma van eisen aangeven of: - Er eisen gesteld worden die onnodig beperkend zijn? - Er eisen gesteld worden die onnodig kostenverhogend zijn? - Er eisen gesteld worden die onduidelijk zijn? - Er eisen gesteld worden die om een andere reden niet wenselijk zijn? - Er eisen gesteld worden die discriminerend zijn? - Er eisen zijn die gemist worden? Indien ja, graag aangeven welke?	a. Onnodig beperkend: De verplichting tot volledige as-is overname inclusief de technische stack beperkt de ruimte voor optimalisatie en technische sanering voorafgaand aan de migratie. b. Onnodig kostenverhogend: De combinatie van 24/7-dienstverlening, structurele security-monitoring, jaarlijkse penetratietesten en maandelijks release-management binnen een vast maximumbedrag wordt als zeer kritisch gezien. c. Onduidelijk: De exacte scope van het Cloud Security Privacy Control Framework van JenV is voor veel partijen onduidelijk. Ook de verantwoordelijkheidsverdeling tussen technisch beheer en contentbeheer behoeft scherpere definities. d. Om andere reden niet wenselijk: Het opnemen van online marketing in een primair technische uitvraag wordt afgeraden, omdat dit een wezenlijk ander specialisme is. e. Discriminerend: Geen partijen geven dit aan. f. Gemiste eisen: Partijen missen expliciete eisen rondom back-upretentie, recovery-testfrequenties en de minimale overdrachtsdocumentatie die de huidige leverancier moet aanleveren

1.3 Dienstverlening

12.	Beschrijf in het kort hoe u de inbeheername, migratie en de implementatie van de beheerprocessen ter hand neemt. (servicemanagement)	Alle partijen hebben een uitgebreid en gestructureerd migratie en implementatieproces aangeleverd. De nadruk lag op een veilige migratie met minimaal dataverlies en minimale tot geen downtime. Elementen die o.a. werden benoemd: • Kick-off en governance-inrichting • Technische-, risico- en afhankelijkheidsanalyse (due dilligence) • Opstellen transitieplan • Inrichting OTAP omgevingen en servicemanagementtool • Formaliseren beheerafspraken • Formele overdracht
13.	Kunt u aangeven wat volgens u een realistische implementatietermijn is vanaf het moment van gunning tot volledige overname van de dienstverlening van de website, inclusief eventuele fasering? Welke factoren beïnvloeden deze termijn en welke afhankelijkheden ziet u?	4-16 weken
14.	Kunt u een grove inschatting geven van de te verwachten implementatiekosten?	De schattingen lopen erg uiteen met een gemiddelde van 18k voor NIPV.nl en 17k voor brandweer.nl, dit gemiddelde wordt omhoog gebracht door een enkele grote uitschieter naar boven.
15.	Wat zijn naar uw mening de grootste risico's voor de inbeheername van de beoogde websiteomgevingen.	Er worden geen onbeheersbare risico's benoemd. Risico's die wel benoemd worden, maar beheersbaar blijven mits hier vooraf duidelijke afspraken over zijn gemaakt zijn o.a.: • Technische complexiteit en technische schuld • (Financiële) onhaalbaarheid compliance eisen • Verouderde techniek / plugins en ontbrekende documentatie • Onzekere scope en SLA • Externe integraties/API-koppelingen • Onvolledige overdracht • Communicatiesnelheid en beschikbaarheid van alle betrokken partijen • Prioritering NIPV en Brandweer
16.	Welke passende sancties of maatregelen acht u geschikt	De markt is hierover verdeeld. Enerzijds wordt aangegeven dat het stellen van sancties geen goed idee

	wanneer de in eis 48 genoemde responstijden herhaaldelijk niet worden behaald?	is en dat deze kosten uiteindelijk (verdekt) doorberekend worden aan de klant. Ook heeft dit invloed op de samenwerking. Anderzijds geeft de markt aan dat er gewerkt kan worden met (korting op) een strippenkaart, of een korting op het SLA-maandbedrag,
17.	Beschrijf of en waarom naar uw mening een eventuele opdracht zou moeten worden gesplitst in aparte percelen voor NIPV en Brandweer.nl	Beide kan; Geen percelen: De opdracht is goed behapbaar voor alle partijen en vanuit efficiency, continuïteit, uniformiteit en kennisbundeling is het logisch om als 1 opdracht in de markt te zetten. Andere voordelen; end-to-end verantwoordelijkheid, security governance, uniform servicemanagement. Wel percelen: Ivm verschillende doelgroepen, verschillende functionele aspecten. Marktwerving vergroten en migratierisico's per omgeving beheersbaar houden. Andere voordelen; beperking onderlinge afhankelijkheden, heldere verantwoordelijkheidsafbakening, flexibelere contractstructuur, minder impact wijzigingen tussen omgevingen.
18.	Wat zijn volgens u de noodzakelijke randvoorwaarden om één of beide websiteomgevingen in beheer te nemen.	De marktpartijen geven vergelijkbare randvoorwaarden, zoals: • Volledige toegang tot alle noodzakelijke gegevens en bestanden, inclusief documentatie • Heldere afbakening scope en SLA en vooraf vastgestelde incidentclassificatie. • Overzicht van integraties en API-koppelingen met externe systemen • ISO27001 certificering • Gesprek met de huidige websiteleverancier indien nodig • Read-only toegang tot de acceptatieomgeving of een gedocumenteerde technische walkthrough
19.	Welke suggesties heeft u waarmee het NIPV haar voordeel zou kunnen doen t.b.v. deze aanbesteding?	- Voeg duidelijke KPI's toe aan het PvE / SLA met betrekking tot oa. web performance, zoals minimale laadsnelheid of maximale reactietijden. - Aanscherpen exit-scenario's en overdrachtdocumentatie (ook bij aanvang). - Geef ruimte voor herstructurering. - Overweeg andere overdraagbare architectuur. - Vraag concreet migratieplan om zonder downtime over te nemen. - Overweeg om online marketing los te koppelen. - Faseer het project. Overweeg hierin een tijdelijke change freeze. - Formuleer eisen functioneel.

		- Specificeer "vergelijkbaar". - Afbakening scope binnen DAP/SLA en tussen technisch beheer en contentbeheer. - Vastleggen van documentatie eisen. - Concretisering meetmethodiek en acceptatiecriteria. - Geef meer informatie over de huidige staat. - Realistische 24/7 eisen en sancties. - Maak onderscheid in inschrijfprijs tussen implementatie (eenmalige) en periodieke kosten tijdens de contractperiode.
--	--	--

1.4 Innovaties / ontwikkelingen

20.	Welke innovaties zijn recentelijk doorgevoerd en door u aan te bevelen?	Er zijn ontwikkelingen genoemd rondom: - Security (oa Security by design) - Functionele integratiestrategie - Professionalisering WordPress multisite beheer - Data gedreven doorontwikkeling - AI - Zoekoptimalisaties - Geautomatiseerde updates - Continue toegankelijkheidsmonitoring / geavanceerder monitoring - Back up-architectuur - Performance optimalisatie - Cookie-loze tracking en privacy - Kwaliteitsborging / continue verbetering
-----	---	--

1.5 Marktsituatie

21.	Op welke vlakken zit uw onderscheidend vermogen met betrekking tot deze opdracht?	De resultaten hiervan worden op verzoek niet bekend gemaakt.
22.	Bent u voornemens om in te schrijven op de aanbesteding voor beheer en hosting van onze websites? Zo ja, welke factoren zijn voor u bepalend om daadwerkelijk een inschrijving te doen?	Alle marktpartijen geven aan voornemens zijn in te schrijven, al dan niet na aanpassing van enkele (geschikheids)eisen.