

Nvl marktconsultatie Back-up

Ref. nr.	Fase	Onderwerp	Vraag	Antwoord
1	Inschrijffase	gebruik van tape	Is er in de nieuwe situatie nog steeds behoefte om data op tape op te slaan of mag dit ook op disk met een zogeheten aircap?	Nee
2	Inschrijffase	gebruik van cloud	Dient alle hardware in het DC van VRU geplaatst te worden of is cloud ook toegestaan?	Niet in de cloud
3	Inschrijffase	Meerdere locaties	Is er een mogelijkheid om back-up data op twee locaties op te slaan binnen het netwerk van VRU?	Ja dit is mogelijk
4	Inschrijffase	algemeen	Waarom is opdrachtgever alleen voornemens de hardware te vervangen onder de Veeam software? Nieuwe technieken en bijbehorende innovatie zoals bijv. ransomware en sensitive data detectie en preventie in combinatie met een veel hoger niveau van security worden juist in de software laag opgelost. Door het alleen vervangen van de hardware ontvangt opdrachtgever straks niets anders dan een volgende generatie commodity hardware.	Wij hebben nog een contract voor de Veeam software en deze valt daarmee buiten de scope van deze aanbesteding.
5	Inschrijffase	Long term back-up	Is er een voorkeur om long-term back-up on premises op te slaan of in de Cloud? Mogen we hier vrijblijvend advies op geven?	On Premise, advies mag
6	Inschrijffase	Totale netto data	Is de genoemde back-up data van 37,8 TB de totale netto data die in 5 jaar voorzien moet worden van een retentie?	Deze hoeveelheid is inclusief berekening datagroei genomen over 5 jaar
7	Inschrijffase	Organisatie	Waar worstelt uw organisatie momenteel vooral mee?	Niet van toepassing
8	Inschrijffase	Support back-up	Hoe is de support op dit moment geregeld aangaande de back-up? Heeft U voor storingen of support aangaande hard en software 1 contact? Of heeft u voor wat betreft de hardware en voor wat betreft de software 2 separate contact mogelijkheden?	Software support is apart belegd. De scope van deze aanbesteding is alleen hardware incl. support voor de hardware
9	Inschrijffase	Containers	Maakt U gebruik van containers die gebackuppeld moeten worden?	Nee
10	Inschrijffase	Insider attack	Is het nu mogelijk bij U in de organisatie om intern door een backup administrator de back-up data te verwijderen? Een zogenaamde "insider attack"? Indien dit het geval is, zou u hiervoor bescherming willen?	Dit valt niet binnen de scope van deze aanbesteding
11	Inschrijffase	Data	Uw totale hoeveelheid te back-uppen data is ongeveer 37.8 TB. Als u deze moet categoriseren in de volgende data-typen: VM-filesystem & VM-database; Kunt u aangeven wat de verdeling is tussen deze twee? Bv. 70% VM-filesystem, 30% VM-database.	75% VM-filesystem, 25% VM-database
12	Inschrijffase	Disaster Recovery en Cyber Recovery	Disaster Recovery en Cyber Recovery verschillen van elkaar. Bij een Cyber aanval kan het zijn dat uw complete productie omgeving is geraakt en dus ook uw DR oplossing (storage/back-up replicatie). Zou de oplossing die u uitvraagt moeten kunnen herstellen vanuit zo'n situatie met een schone back-up kopie?	Maakt dit onderdeel uit van de hardware oplossing ?
13	Inschrijffase	Cyber Resiliency	In het kader van Cyber Resiliency (Weerbaarheid tegen Cyber aanvallen), kunt u uw doelstellingen omschrijven als het gaat om het veiligstellen van uw data?	Maakt dit onderdeel uit van de hardware oplossing ?
14	Inschrijffase	Back-ups	Buiten de VM image back-up, maakt u nog andere applicatie consistente back-ups? Welke applicaties?	Wij backuppen VM's en Office 365 cloud data
15	Inschrijffase	VMs	Heeft u bepaalde VMs waarbij het maken van een snapshot een probleem geeft op de applicatie? (Applicatie die zeer gevoelig is voor latency)	Nee
16	Inschrijffase	Back-ups	Maakt u gebruik van VM image gebaseerde back-ups?	Ja
17	Inschrijffase	Hyper-visor	In uw plaatje laat u zien dat u gebruik maakt van een virtuele omgeving (virtuele servers). Welke hyper-visor gebruikt u hiervoor? VMware, Hyper-V of een andere smaak?	Vmware
18	Inschrijffase	Recover Point Objective	Heeft u specifieke RPO (Recover Point Objective) eisen? Met andere woorden, wat is uw maximaal toelaatbare hoeveelheid dataverlies na een disaster?	Maakt dit onderdeel uit van de hardware oplossing ?
19	Inschrijffase	Recover Point Objective	Bij het uitvallen van componenten in uw datacenter (stroom, mogelijke overstrooming etc..) en u moet terugvallen op uw back-up om 10TB te herstellen, hoe lang mag deze recovery duren? Met andere woorden, wat zijn uw RTO (Recover Point Objective) waardes?	Wij kunnen hier op dit moment geen inschatting over maken.
20	Inschrijffase	Back-up naar tape	U schrijft een back-up naar Tape te maken. Is dit iets wat in de toekomstige oplossing terug moet komen?	Ja
21	Inschrijffase	Compatibiliteit met Veeam	U schrijft dat de hardware compatible moet zijn met Veeam en tegelijkertijd voorgelicht wil worden over nieuwe technieken en mogelijkheden in de markt. Er zijn veel mogelijkheden die met Veeam te werken maar ook andere oplossingen t.b.v. visie en strategie v.w.b. Data Protectie / Cyber Recovery. Staan jullie ervoor open om deze harde eis te laten vallen?	Wij kunnen deze eis i.v.m. bestaand softwarecontract niet laten vallen.
22	Inschrijffase	SaaS back-up oplossing	Er is een EU SaaS back-up oplossing waarbij geen upload en download kosten (ingress/egress) gerekend worden, en waarbij de back-up data achter een Air Gap is geplaatst, 3x wordt opgeslagen waarvan 1x immutable, en gescanned wordt op ransomware. Gezien de toepassingen van M365 en de aangegeven hoeveelheid TB in het DC zou dit een perfecte oplossing zijn voor VRU (geen hardware meer, geen software/licenties, onderhoud, tapes, technische beheer/updates/updates etc) , zou de VRU openstaan voor een scenario waarin alle data via SaaS wordt opgeslagen?	Nee, niet op dit moment
23	Inschrijffase	Ransomware scanning	Een moderne back-up oplossing voorziet in een Air Gap. Echter, als de data achter de Air Gap is geïnfecteerd, is het onbruikbaar na een cyberaanval. Is VRU geïnteresseerd om ransomware scanning toe te passen op de offline data in het eigen datacenter?	Dit maakt geen onderdeel uit van deze aanbesteding.

24	Inschrijffase		Welke mogelijke dreigingen wenst VRU te mitigeren met de (toekomstige) back-up oplossing?	De VRU probeert zich tegen zoveel mogelijk dreigingen te beschermen.
25	Inschrijffase		Uit wat voor type(s) data/workloads bestaat hetgeen in de back-ups meegenomen zal worden?	Kunnen we op dit moment geen antwoord op geven
26	Inschrijffase		Maakt VRU momenteel gebruik van data-encryptie technieken? Zo ja, welke? Zo niet, wat is hier de reden voor?	Kunnen we op dit moment geen antwoord op geven
27	Inschrijffase		Welke mate van granulariteit verwacht VRU van eventuele restores?	Zo hoog mogelijk (de laatste back-up)
28	Inschrijffase		Tot in hoeverre wenst VRU de back-up naar tape te behouden of te vernieuwen?	10 jaar of onbeperkt?
29	Inschrijffase		Hoe wordt op dit moment de beheerlast ervaren?	Niet relevant voor deze aanbesteding.
30	Inschrijffase		Tot in hoeverre verwacht men een hogere mate van automatisering/orchestratie t.o.v. de huidige situatie?	Op dit moment geen idee.
31	Inschrijffase		In welke mate zijn audits en/of rapportages over de back-ups voor VRU van belang?	Niet relevant voor deze aanbesteding