Rubicon
Consulting & Technology

Dienstbeschrijving

Azure Secure & Compliant managed cloud service

1 januari 2021

Versie 1.0

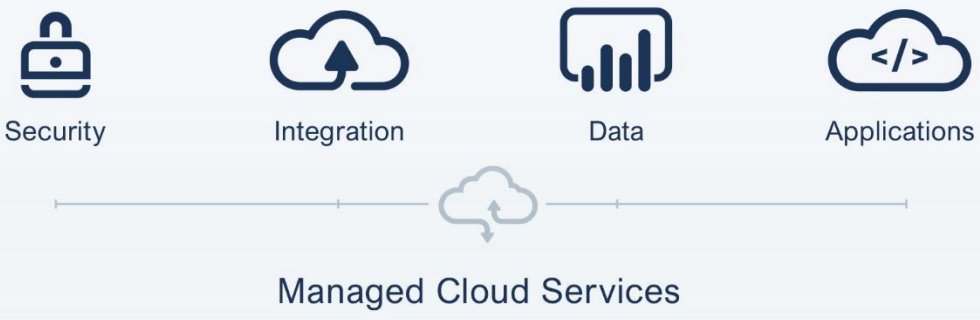
Gold
Microsoft Partner

Rubicon
Consulting & Technology

Uw partner voor cloud adoptie van Microsoft solutions en managed cloud diensten

Rubicon is dé expert binnen het Microsoft cloud diensten portfolio en levert consultancy, complete diensten en geavanceerde (maatwerk) oplossingen om digitale transformatie te laten slagen. Op basis van cloud oplossingen en managed cloud foundations realiseren we veilige, geïntegreerde en datagedreven klantorganisaties.

Met meer dan 200 senior consultants en een gedegen track record in de grootzakelijke markt en overheid garanderen wij schaalbaarheid, continuïteit en een resultaatgerichte aanpak. Door digitalisering van bedrijfsprocessen helpen wij onze opdrachtgevers met innovatie, productiviteitsverbetering, kostenbesparing en efficiënte samenwerking.



Gold
Microsoft Partner

Inhoudsopgave

Wijzigingshistorie

Versie	Datum	Auteur	Wijziging
1.0	24-11-20	Ed Feskens	Eerste versie

Rubicon Cloud Advisor

Rubicon levert sinds 1998 een compleet portfolio aan diensten die opdrachtgevers in staat stelt op innovatieve wijze invulling te geven aan digitalisering van bedrijfsprocessen, de wijze waarop medewerkers productiever samenwerken en klanten beter bediend worden. Sinds 2010 is Rubicon volledig gespecialiseerd in het Microsoft Cloud Platform en helpt organisaties naar deze nieuwe ICT-diensten te migreren en nieuwe cloud-native toepassingen te realiseren.

1. Azure Secure & Compliant

Met Azure Secure & Compliant biedt Rubicon een managed cloud dienst aan die organisaties in staat stelt om op een veilige en betrouwbare manier applicatie- en dataworkloads te hosten in Microsoft Azure.

Azure Secure & Compliant is dienstverlening die er voor zorgt dat uw Microsoft Azure platform goed en veilig wordt ingericht en altijd onderhouden blijft.

Azure is de verzamelnaam voor de Cloud datacenter diensten van Microsoft. Microsoft levert deze diensten vanuit haar eigen datacenters en zorgt natuurlijk voor beheer en onderhoud van die datacenters, servers, netwerk en opslag infrastructuur. Als u gebruik maakt van Azure krijgt u een eigen afgeschermd gedeelte daarvan toegewezen. Dit heet een tenant en kan het best worden vergeleken met een gewoon datacenter maar dan in de cloud van Microsoft.

Als u van Microsoft uw Azure tenant krijgt geleverd is deze allesbehalve gebruiksklaar. De Azure Secure & Compliant managed cloud dienst zorgt er voor dat alle noodzakelijke voorzieningen en beveiligingsmaatregelen voor het hosten van applicatie- en dataworkloads worden ingeregeld in uw Azure tenant en dat deze vervolgens ook wordt beheerd.

In dit document worden de verschillende elementen waaruit de dienst is opgebouwd beschreven:

2. Dienstverlening

De Azure Secure & Compliant managed cloud service dekt drie beheerdomeinen af te weten

- Operationeel beheer van de Azure tenant
- Security en compliance monitoring
- IT service management

De dienstverlening die Rubicon levert in het kader van Azure Secure & Compliant managed cloud services is voor ieder domein hieronder uitgewerkt.

2.1. Operationeel beheer van de Azure tenant

Het operationeel beheer dat door Rubicon wordt uitgevoerd heeft tot doel het in stand en gezond houden van de Azure tenant van de opdrachtgever inclusief de daarin geconfigureerde basisinrichting.

Item	Toelichting	Levering
Basisinrichting initieel	Als onderdeel van de dienst wordt de basisinrichting uitgerold en geconfigureerd in de Azure tenant van opdrachtgever. Deze basisinrichting is in het volgende hoofdstuk beschreven. Voorafgaand aan het uitrollen van de basisinrichting wordt deze met Opdrachtgever besproken. In deze bespreking kan Opdrachtgever aangeven op welke punten men wil afwijken van de basisinrichting, en welke aanvullingen wenselijk zijn.	Standaard onderdeel van de dienst.
Basisinrichting onderhoud	De basisinrichting inclusief specifieke configuraties ten behoeve van opdrachtgever worden ondergebracht in de GIT repository die bij de Azure tenant van de opdrachtgever hoort. Eventuele wijzigingen en aanvullingen op de basisinrichting die over de tijd worden doorgevoerd worden eveneens in deze GIT repository bijgehouden. Rubicon zorgt voor een back-up van deze GIT repository.	Standaard onderdeel van de dienst.
Basisinrichting herstel	In geval van een calamiteit kan opdrachtgever Rubicon verzoeken om de gehele basisconfiguratie te herstellen in de Azure tenant van opdrachtgever. Hiermee wordt de bestaande situatie volledig overschreven. Deze kan ook niet meer worden hersteld daarna.	Standaard onderdeel van de dienst.
Azure DevOps deployment pipeline	Rubicon beheert de Azure DevOps pipeline die wordt gebruikt voor het uitrollen en configureren van de basisinrichting.	Standaard onderdeel van de dienst.
GIT code repository	Rubicon beheert de GIT code repository die wordt gebruikt voor het onderbrengen en beheren van de templates, scripts en configuratiebestanden ten behoeve van de dienstverlening.	Standaard onderdeel van de dienst.
Monitoring	De gedefinieerde KPI's worden met behulp van Azure monitor en Log analytics continue gemonitord. Critical alerts worden automatisch verzonden naar de RCMC servicedesk en daar als incident geregistreerd en opgepakt. Afhandeling vindt plaats conform het afgesproken service level en incident management proces. Daarnaast vindt iedere werkdag een controle van de overige monitoring alerts plaats door een medewerker	Standaard onderdeel van de dienst.

Item	Toelichting	Levering
	van RCMC. Hiervoor wordt gebruik gemaakt van Azure Lighthouse als management tool.	
Health check	Een maandelijkse Azure health check maakt standaard onderdeel uit van de dienst. Op basis hiervan ontvangt de klant adviezen en verbetervoorstellen met betrekking tot beveiliging, gebruik van resources en life cycle management. De resultaten en verbetervoorstellen die voortkomen uit de health check worden tijdens het periodieke service management overleg met uw organisatie besproken. Verbetervoorstellen die door uw organisatie worden overgenomen worden door het RCMC als een wijzigingsverzoek behandeld conform het afgesproken service level en change proces.	Standaard onderdeel van de dienst
Drift detectie	Naast de maandelijkse health check wordt ook wekelijks de configuratie van de basisinrichting van de Azure tenant van opdrachtgever gecontroleerd op afwijkingen. Deze controle vindt plaats tegen de configuratie van de basisinrichting zoals die met opdrachtgever is besproken en afgesproken, startende vanaf de initiële uitrol in de transitiefase.	Standaard onderdeel van de dienst.

2.2. Security en compliance monitoring

Het security beheer zoals dat door het RCMC wordt uitgevoerd helpt u bij het bewaken van uw informatiebeveiliging in Azure, het tijdig signaleren van security risico's en mogelijke inbreuken en het nemen van preventieve maatregelen. In het geval er zich security incidenten voordoen, of er zich potentiële risico's voordoen zal het RCMC met uw organisatie in overleg treden en specifieke maatregelen adviseren. Daarbij zal ook de mogelijke impact worden aangegeven. ***U blijft echter zelf verantwoordelijk om te besluiten de adviezen van het RCMC ook op te (laten) volgen.*** Het RCMC neemt dan ook geen eindverantwoordelijkheid voor de veiligheid van systemen, applicaties en gegevens in uw Azure tenant.

Item	Toelichting	Levering
Security monitoring	Na oplevering van de Azure tenant in beheer wordt met behulp van Secure score en Security center pro-actief de security status van de tenant en de resources die zich daarin bevinden gemonitord.	Standaard onderdeel van de dienst.

Item	Toelichting	Levering
	Critical alerts die betrekking hebben op de tenant en de resources (voor zover die bij RCMC in beheer zijn), worden automatisch gemaild naar de RCMC servicedesk en daar als incident geregistreerd en opgepakt. Afhandeling vindt plaats conform het afgesproken service level en incident management proces. Daarnaast vindt iedere werkdag een controle van de overige Secure score alerts plaats door een medewerker van RCMC. De security alerts en aanbevelingen uit Secure score worden ook meegenomen in de maandelijkse Azure health check en besproken tijdens het periodieke service management overleg. Verbetervoorstellen die door uw organisatie worden overgenomen worden door het RCMC als een wijzigingsverzoek behandeld conform het afgesproken service level en change proces.	
Compliance monitoring	Compliance manager wordt gebruikt om compliance ten opzichte van de volgende standaarden te meten: • Microsoft Azure Foundations Benchmark • GDPR (AVG) • ISO 27001 Hierbij kijkt het RCMC ***uitsluitend*** naar de technische controls die onderdeel uitmaken van deze standaarden. Indien gewenst kan opdrachtgever Compliance manager zelf ook inzetten voor het managen van compliance ten opzichte van bovenstaande en aanvullende standaarden die door Compliance manager worden ondersteund. Opdrachtgever is dan zelf verantwoordelijk voor het inregelen van de niet-technische controls van de desbetreffende standaarden.	Standaard onderdeel van de dienst met uitzondering van het inregelen van niet-technische controls en aanvullende standaarden. Rubicon kan daarbij ondersteuning bieden als meerwerk.
Onderhoud van de security baseline	Rubicon houdt pro-actief alle wijzigingen en aanvullingen op de CIS Microsoft Azure security baseline bij en zorgt er voor dat deze ook in de tenant van opdrachtgever worden geïmplementeerd. De impact hiervan wordt vooraf met opdrachtgever besproken en afgestemd.	

N.B. Het is mogelijk om Security center aan te sluiten op Azure Sentinel, dan wel op een reeds bestaande SIEM voorziening van opdrachtgever. Dit maakt geen onderdeel uit van de standaard dienstverlening, maar Rubicon kan wel ondersteunen bij de inrichting hiervan.

2.3. IT Service management

IT Service management ondersteunt uw organisatie in het dagelijks gebruik en de operationele en tactische aansturing van de Azure Secure & Compliant managed cloud service. Tijdens de transitiefase worden de service management processen met uw organisatie besproken en worden afspraken gemaakt over de aansluiting op uw eigen service management processen. Deze afspraken worden vastgelegd in een Document Afspraken en Procedures (DAP).

Tegelijkertijd worden met uw organisatie ook de service niveaus besproken en vastgelegd in een Service Level Agreement (SLA).

Rubicon heeft de volgende service management processen ingericht:

Item	Toelichting	Levering
Incident management	Incidenten zijn verstoringen in de werking of beschikbaarheid van diensten of alerts die voortkomen uit de monitoringsystemen. Voor het afhandelen van incidenten hanteert het RCMC vaste service levels voor reactie- en oplostijden. Deze zijn afhankelijk van de prioriteitsklasse van het incident. Dit alles is vastgelegd in de SLA die met opdrachtgever is overeengekomen. Voor het afhandelen van incidenten hanteert het RCMC ook een vaste procedure. Deze procedure is vastgelegd in de DAP die met opdrachtgever is overeengekomen. Incidenten kunnen worden aangemeld bij de RCMC Service desk op volgende manieren: • Telefonisch tijdens openingstijden (zie SLA) • E-mail (24/7) • Serviceportaal (24/7)	Het afhandelen en oplossen van incidenten wordt altijd als meerwerk uitgevoerd.
Change management	Wijzigingen (ook wel RfC's) kunnen door opdrachtgever worden aangevraagd bij de servicedesk van het RCMC. Voor het afhandelen van wijzigingen hanteert het RCMC vaste service levels voor reactie- en verwerkingstijden. Dit alles is vastgelegd in de SLA die met opdrachtgever is overeengekomen.	Het behandelen en uitvoeren van wijzigingen wordt altijd als meerwerk uitgevoerd.

Item	Toelichting	Levering
	Voor het afhandelen van wijzigingen hanteert het RCMC ook een vaste procedure. Deze procedure is vastgelegd in de DAP die met opdrachtgever is overeengekomen. Wijzigingen kunnen worden aangemeld bij de RCMC Service desk op volgende manieren: • Telefonisch tijdens openingstijden (zie SLA) • E-mail (24/7) • Serviceportaal (24/7)	
Problem management	Op basis van de resultaten van de maandelijkse health check worden door het RCMC problemen (vaak voorkomende incidenten) gesignaleerd. Deze worden in het periodieke service management overleg met de organisatie van opdrachtgever besproken. Verbetervoorstellen die door uw organisatie worden overgenomen worden door het RCMC als een wijzigingsverzoek behandeld conform het afgesproken service level en change proces.	Standaard onderdeel van de dienst.
Service desk	Opdrachtgever krijgt toegang tot de RCMC Service desk. Deze is ingericht als een 2e lijns service desk met senior experts en biedt alleen ondersteuning aan functioneel en technisch beheerders binnen de organisatie van opdrachtgever. De RCMC Service desk is geopend op werkdagen van 8.30 tot 17.30. Buiten deze openstelling kan gebruik worden gemaakt van de bereikbaarheidsdienst. Hiervoor moet een aanvullende SLA worden afgesloten.	Standaard onderdeel van de dienst
Service coördinatie	Alle werkzaamheden met betrekking tot afhandelen van incidenten en wijzigingen worden gepland en met opdrachtgever afgestemd door de Service coördinator. De Service coördinator is ook verantwoordelijk voor het bewaken van en rapporteren over de voortgang richting de organisatie van opdrachtgever.	Standaard onderdeel van de dienst.
Service portaal	Opdrachtgever krijgt toegang tot het RCMC service portaal. Dit portaal is 24/7 bereikbaar voor het melden van incidenten en het aanvragen van wijzigingen. Ook kan hier inzicht worden verkregen in de actuele status van incidenten en wijzigingen.	Standaard onderdeel van de dienst.

Item	Toelichting	Levering
Service rapportage	Opdrachtgever krijgt maandelijks via een service management rapportage inzicht in de uitgevoerde werkzaamheden en de kosten die daaraan zijn gerelateerd. De service management rapportage omvat ook de score van het RCMC ten opzichte van de afgesproken SLA en de resultaten van het klanttevredenheidsonderzoek.	Standaard onderdeel van de dienst.
Azure verbruikskosten overzicht	Opdrachtgever krijgt maandelijks een overzicht van de geregistreerde Azure verbruikskosten (consumption). Deze is gegroepeerd naar de kostencodes die zijn toegekend aan de resources die in de tenant van opdrachtgever zijn uitgerold. Dit kostenoverzicht kan door opdrachtgever worden gebruikt voor de interne toewijzing van Azure verbruikskosten aan afdelingen of projecten. Voorwaarde voor het kunnen leveren van deze dienst is dat Rubicon ook optreedt als CSP voor opdrachtgever. Het kostenoverzicht is puur informatief en omvat geen aanbevelingen met betrekking tot kostenoptimalisatie. Het is ook geen vervanging van de factuur die opdrachtgever van Microsoft krijgt.	Standaard onderdeel van de dienst op voorwaarde dat Rubicon als CSP optreedt voor opdrachtgever.
Service management	Service management omvat het periodiek rapporteren over de geleverde dienstverlening aan opdrachtgever. Ook wordt met opdrachtgever periodiek een service management overleg gevoerd waarin deze rapportage samen met de resultaten van de maandelijkse health check worden besproken. In het service management overleg worden tevens de door opdrachtgever voorziene grote wijzigingen besproken en zo mogelijk ingepland.	

3. Basisinrichting

De Azure Secure & Compliant managed cloud service is gebaseerd op het uitrollen en configureren van een basisinrichting in uw Azure Tenant. Het uitrollen en configureren van deze basisinrichting gebeurt grotendeels geautomatiseerd. Hiervoor wordt door het RCMC een deployment pipeline ingericht in de Rubicon Azure DevOps omgeving. Deze deployment pipeline wordt vervolgens aangesloten op uw Azure tenant.

Alle templates, scripts en configuratiebestanden die nodig zijn voor het uitrollen en configureren van de basisinrichting in uw Azure tenant worden door het RCMC ondergebracht en beheerd in een GIT code repository die alleen voor uw organisatie wordt gebruikt.

De Azure Secure & Compliant basisinrichting omvat de volgende items:

Item	Toelichting	Levering
Azure DevOps deployment pipeline	Rubicon richt in haar eigen Azure DevOps omgeving een dedicated deployment voor opdrachtgever in. Deze deployment pipeline wordt aangesloten op de Azure tenant van opdrachtgever.	Standaard onderdeel van de dienst.
GIT code repository	Rubicon richt voor opdrachtgever een dedicated GIT code repository in. Hierin worden alle templates, scripts en configuratiebestand ten behoeve van deployments ondergebracht en beheerd.	Standaard onderdeel van de dienst.
Deployment van de basisinrichting	De basisinrichting wordt door Rubicon grotendeels geautomatiseerd uitgerold in de Azure tenant van opdrachtgever. Hierbij gelden de volgende uitgangspunten: • Rubicon heeft een user account met Global admin rechten nodig in de tenant van opdrachtgever. Dit account kan niet met MFA zijn geconfigureerd. Alle configuratie items worden vooraf met opdrachtgever doorgenomen en inhoudelijk afgestemd.	Standaard onderdeel van de dienst.
AD Connect Sync	AD Connect sync moet geconfigureerd en operationeel zijn in het eigen datacenter van opdrachtgever. Dit is een vereiste voor het kunnen inrichten van de Azure tenant van opdrachtgever. Als AD Connect sync nog niet is ingeregeld kan Rubicon helpen om AD Connect sync in te richten en te configureren. In de voorbespreking met Opdrachtgever wordt de configuratie doorgenomen en de inrichting getoetst aan de standaarden die voor onze managed service gelden. Desgewenst kan Rubicon adviseren over, en meehelpen met de uit te voeren aanpassingen.	Niet in standaard dienst. Ondersteuning door Rubicon is mogelijk als meerwerk.
AD Connect Health	AD Connect health moet geconfigureerd en operationeel zijn in het eigen datacenter van opdrachtgever. Als AD Connect Health nog niet beschikbaar is kan Rubicon helpen om dit juist in te richten en te configureren. In de voorbespreking met	Niet in standaard dienst.

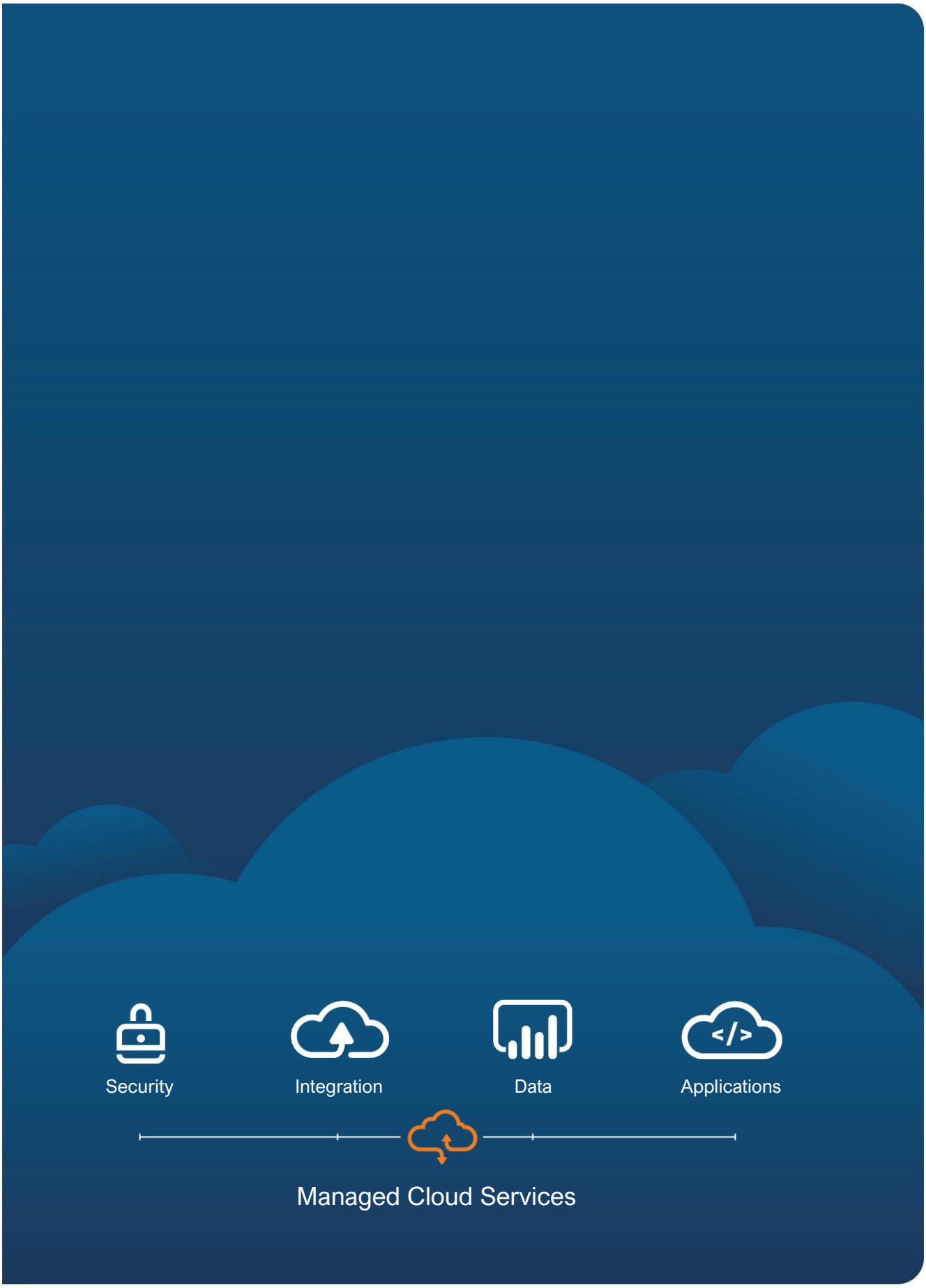
Item	Toelichting	Levering
	Opdrachtgever wordt de configuratie doorgenomen en de inrichting getoetst aan de standaarden die voor onze managed service gelden. Desgewenst kan Rubicon adviseren over, en meehelpen met de uit te voeren aanpassingen. Analyse van de AD Connect Health logs is onderdeel van de maandelijkse health check die door Rubicon wordt uitgevoerd als onderdeel van de dienst.	Ondersteuning door Rubicon is mogelijk als meerwerk.
Connectiviteit met het eigen datacenter van opdrachtgever	Het kan voor sommige applicatie of data workloads wenselijk zijn om een directe verbinding tussen het eigen datacenter en Azure te configureren. Het uitrollen configureren van een S2S VPN of ExpressRoute verbinding met het on premise datacenter maakt geen onderdeel uit van de basisinrichting omdat deze altijd specifiek is voor de situatie van opdrachtgever. Als ondersteuning vanuit Rubicon bij het configureren van een verbinding nodig is moet dit in de intake worden besproken en begroot.	Niet in standaard dienst. Ondersteuning door Rubicon is mogelijk als meerwerk.
Subscriptions	Ten behoeve van de basisinrichting moeten door opdrachtgever twee subscriptions in de Azure tenant van opdrachtgever beschikbaar worden gesteld: een OT subscription en een AP subscription. Op deze subscriptions wordt de basisinrichting uitgerold. Deze subscriptions worden vervolgens toegevoegd aan de managed service. Deze subscriptions kunnen worden gebruikt om de applicatie- en dataworkloads van opdrachtgever te hosten. Eventuele bestaande subscriptions worden ongemoeid gelaten en niet meegenomen in de beheer dienstverlening. Als opdrachtgever dat wenst kunnen bestaande workloads in subscriptions worden gemigreerd naar de managed subscriptions.	Standaard onderdeel van de dienst. Het migreren van bestaande workloads naar de managed subscriptions is meerwerk.
Workload autorisatie model	Voor het hosten van applicatie- en data workloads wordt een standaard autorisatie model uitgerold als onderdeel van de basisinrichting. Alle workloads worden altijd in dezelfde twee subscriptions (OT en AP) uitgerold en van elkaar geïsoleerd door middel van Resource groepen en Management groepen. Een gedetailleerde uitwerking van dit autorisatiemodel is beschikbaar en wordt gedeeld en besproken tijdens de intake.	Standaard onderdeel van de dienst.
RBAC autorisatie model	Voor het ontwikkelen, gebruiken en beheren van applicatie- en dataworkloads wordt een standaard RBAC autorisatiemodel uitgerold in Azure Active Directory.	Standaard onderdeel van de dienst.

Item	Toelichting	Levering
	Een gedetailleerde uitwerking van dit autorisatiemodel is beschikbaar en wordt gedeeld en besproken tijdens de intake.	
CIS security baseline	De CIS Microsoft Azure Foundations Benchmark wordt uitgerold en geconfigureerd als onderdeel van de basisinrichting. De verschillende onderdelen van deze baseline worden tijdens de intake besproken en eventuele aanvullingen of afwijkingen worden vastgelegd en meegenomen in de transitiefase.	Standaard onderdeel van de dienst met uitzondering van overeengekomen afwijkingen en aanvullingen. Deze worden als meerwerk uitgevoerd.
Secure score	Secure score wordt uitgerold en geconfigureerd als onderdeel van de basisinrichting. Alle aanbevelingen worden opgepakt in lijn met de CIS baseline controls tijdens de transitiefase.	Standaard onderdeel van de dienst.
Security center	Security center wordt uitgerold en geconfigureerd als onderdeel van de basisinrichting	Standaard onderdeel van de dienst
Compliance manager	Compliance manager wordt uitgerold en geconfigureerd als onderdeel van de basisinrichting	Standaard onderdeel van de dienst
Azure monitor	Azure monitor wordt uitgerold en geconfigureerd met de standaard KPI's als onderdeel van de basisinrichting. Standaard worden de volgende KPI's gemonitord: • CIS • AAD sync • GDPR (AVG) • ISO 27001 (technisch) Onderdeel van de uitrol is ook het aanmaken en configureren van de benodigde storage accounts.	Standaard onderdeel van de dienst
Tagging policies	Tagging policies worden ingericht in afstemming met de opdrachtgever voor het definiëren van resource locaties en naming conventies. De volgende tagging policies worden standaard uitgerold: Allowed storage account SKUs Allowed resource type Allowed locations Allowed virtual machine SKUs	Standaard onderdeel van de dienst.

Item	Toelichting	Levering
	"TagName": "#{company-affix}#AdminEmail", "TagValue": "user.techlead@mycompany.onmicrosoft.com" "TagName": "#{company-affix}#ApplicationName", "TagValue": "#{workload-name}#" "TagName": "#{company-affix}#CreatedDate", "TagValue": "#{date-time-now}#" "TagName": "#{company-affix}#ModifiedDate", "TagValue": "#{date-time-now}#" "TagName": "#{company-affix}#Environment", "TagValue": "#{environment}#" "TagName": "#{company-affix}#Version", "TagValue": "#{file-version}#"	
Kostencode tag	Als onderdeel van de tagging policies wordt ook een tagging van resources met een kostenplaats code verplicht. In de basis wordt hier de ApplicationName voor gebruikt. Welke kostenplaatsen worden gehanteerd wordt met de opdrachtgever tijdens de intake besproken. Tijdens de transitiefase worden deze kostenplaatsen geconfigureerd.	Standaard onderdeel van de dienst
KeyVault	KeyVault wordt uitgerold en ingericht ten behoeve van de geautomatiseerde deployment van de basisinrichting. Tevens kan de KeyVault worden gebruikt ten behoeve van specifieke applicatie- en dataworkloads. Dit vraagt echter aanvullende configuratie.	Standaard onderdeel van de dienst met uitzondering van de configuratie voor specifieke workloads. Deze worden als meerwerk uitgevoerd.
Core networking voor IaaS	Het inrichten van VNets en perimeter defense voor klanten met IaaS workloads maakt geen onderdeel uit van de basisinrichting. Als deze nodig is moet dit in de intake worden besproken en begroot als extra werk.	Meerwerk, te begroten op basis van de intake.
Storage accounts	Er worden storage accounts aangemaakt ten behoeve van de geautomatiseerde uitrol van de basisinrichting.	Standaard onderdeel van de dienst met

Item	Toelichting	Levering
	Als er voor specifieke applicatie- en dataworkloads storage accounts moeten worden aangemaakt dan is dat mogelijk als aanvullende configuratie. Dit wordt in de intake besproken en begroot als extra werk.	uitzondering van storage accounts voor specifieke workloads. Deze worden als meerwerk uitgevoerd.

Rubicon
Consulting & Technology



Lage Biezenweg 5 | 4131 LV Vianen
0347 35 88 00 | info@rubicon.nl | rubicon.nl

Gold
Microsoft Partner