



Projectstartarchitectuur

Bijlage 7.2 (bij Selectieleidraad)

Datum: 12 december 2023

Versie: 1.0

Status: Definitief

Opdrachtgever: Richard Lohuis

Projectmanager: Dik van Roon

Opsteller: Danny Thakoer

Classificatie: Openbaar

Vol energie naar morgen

Inhoudsopgave

1	Versiebeheer	2
2	Introductie	3
3	Strategie en uitgangspunten	4
4	Business Architectuur	5
4.1	Algemene Kaders & Principes	5
5	Applicatie Architectuur	6
5.1	Algemene Kaders & Principes	6
5.2	Huidig high level applicatielandschap	7
5.3	Integratie	10
6	Data Architectuur	11
6.1	Algemene Kaders & Principes	11
6.2	Orkestratie	12
7	Security Architectuur	14
7.1	Algemene Kaders & Principes	14
8	Non-functionals	24
8.1	Berekening Beschikbaarheid	25
8.2	Applicatie responsetijd	27
8.3	Service Window	27
8.4	Prioriteit	28
8.5	Reactie- en hersteltijd	29
8.6	Oplossen van incidenten	30
8.7	Back-up en herstel	31
8.8	Update en upgrades	31
8.9	Rapportage	32

1 Versiebeheer

Versie	
1.0	Definitief voor selectiefase
[1.1]	Bevindingen Nota van Inlichtingen, fase 1, toegevoegd
[1.2]	Update PSA t.b.v. inlichtingenfase
[1.3]	Update PSA n.a.v. inlichtingenfase t.b.v. Definitief Beschrijvend Document

Dit document zal in verschillende fasen verder worden uitgediept en meer in detail uitgewerkt. Versie 1.0 is bedoeld om in de selectiefase van het project een beeld bij belangstellende aanbieders ('Gegadigden') te geven van de gewenste oplossing.

In de nog te verschijnen versie 1.1 worden, indien dit naar de mening van Aanbestedende dienst nodig is, de aanvullingen naar aanleiding van de Nota van Inlichtingen, fase 1, aan de hoofdstukken/paragrafen toegevoegd.

In de nog te verschijnen versie 1.2 wordt een inhoudelijke verdieping aangebracht bij de verschillende onderwerpen bedoeld als startpunt voor de consultatiefase. Het doel van dit document is een leidraad te verkrijgen om inhoudelijke te discussiëren over, door de Inschrijver, aangeboden oplossing.

In de nog te verschijnen versie 1.3 is de gewenste oplossing uitgewerkt bedoeld als startpunt voor de aanbestedingsfase samen met het definitief beschrijvend document. In deze versie heeft Cogas zoveel mogelijk haar definitieve kaders en richtlijnen opgenomen waaraan de aangeboden integrale Bedrijfsvoeringsoplossing dient te voldoen.

2 Introductie

De Cogas-groep wenst haar deels verouderde en te veel versnipperde (bedrijfsvoerings-) applicatielandschap ter ondersteuning van onderstaande primaire en ondersteunende processen primaire en ondersteunende processen te vervangen door een geïntegreerd samenstel van geconfigureerde applicaties dat op veilige wijze via het internet bij de Cogas-groep wordt aangeboden en beheerd: de Bedrijfsvoeringsoplossing.

Leeswijzer

Dit document bevat de projectstartarchitectuur (PSA) van het project ATLAS. Onder architectuur wordt verstaan de samenhangende structuur van de informatievoorziening, de daarmee te ondersteunen bedrijfsomgeving en de benodigde technische componenten. De PSA is het contract tussen opdrachtgever, projectmanager en architect(en). Het heeft de volgende functies:

- het verduidelijken van de scope van het project ATLAS;
- het inzichtelijk maken van de gevolgen van het project ATLAS voor Cogas;
- het aangeven van het kader waarbinnen het project ATLAS moet werken. De PSA biedt een uitgangspunt voor ontwerp- en bouwactiviteiten.

3 Strategie en uitgangspunten

Op basis van de door het Cogas directieteam geadopteerde Sourcing Strategie heeft de Cogas-groep de transitie ingezet van een on-premises systeemlandschap en bijbehorende beheer- en ontwikkelorganisatie naar een op SaaS oplossingen gebaseerde regieorganisatie.

Hieruit volgen de volgende uitgangspunten:

- De Cogas-groep kiest voor standaard, bij voorkeur, ‘commercial of the shelf’ oplossingen op basis van cloudoplossingen (SaaS). Dat maakt dat een keuze wordt gemaakt uit oplossingen en leveranciers die er ook daadwerkelijk zijn. In beginsel wordt geen ‘specifiek’ maatwerk toegepast. Specifiek maatwerk onderscheidt zich van generiek maatwerk doordat specifiek maatwerk uitsluitend voor een opdrachtgever wordt gemaakt. Generiek maatwerk wordt in het releasebeleid van de Leverancier meegenomen en om die reden ook aan andere klanten ter beschikking gesteld en is daarmee toegestaan.
- De Cogas-groep kiest voor een integrale Bedrijfsvoeringsoplossing die naar keuze van de Inschrijver/Leverancier kan bestaan uit één of meerdere ‘best of breed’ softwarecomponenten/-diensten. Inschrijver/Leverancier is daarbij uitdrukkelijk verantwoordelijk voor adequate integratie van eventuele (eveneens door of onder verantwoordelijkheid van Inschrijver/Leverancier op basis van Gebruiksrechten ter beschikking te stellen) ‘losse’ softwarecomponenten en/of -diensten die onderdeel uitmaken van de integrale Bedrijfsvoeringsoplossing.
- De registerfunctie en de basiseisen ten aanzien van beschikbaarheid, integriteit en vertrouwelijkheid moeten hierbij zijn geborgd, zowel voor het eigen aandachtsgebied (de informatievoorziening voor de onderscheiden processen) als voor de gehele keten binnen de integrale Bedrijfsvoeringsoplossing. In het bijzonder zijn de doelmatigheidsdoelstellingen hierbij leidend, evenals het verbeteren of consolideren van de noodzakelijke borging van de continuïteit in de bedrijfsvoering.

4 Business Architectuur

4.1 Algemene Kaders & Principes

Principe	Uitleg
Een open Cogas, in een open samenleving	Cogas laat duidelijk zien wat zij doet en hoe zij dat doet, aan medewerkers, (partner)organisaties en klanten.
Een betrouwbare partner	Cogas komt afspraken na, zonder dat er een gouden laagje om een product of dienst zit.
Een duurzame bedrijfsvoering	De continuïteit van de Cogas dienstverlening staat centraal.
Actief werken aan hoge kwaliteit	Cogas streeft naar hoogwaardige dienstverlening en effectieve samenwerkingen.
'Nooit af': wendbaarheid en aanpassingsvermogen	Om het juiste niveau te kunnen bieden, blijft Cogas haar producten en diensten continu verbeteren.

4.1.1 Uitgangspunten

Uit deze algemene kaders en principes volgen de volgende uitgangspunten:

- De Cogas groep kent een negental juridische entiteiten met specifieke taken en (wettelijke) verantwoordelijkheden. Het is voor de medewerkers, afnemers, klanten en overige stakeholders duidelijk met welke van de juridische entiteiten ze te maken hebben.
- De inhoud van het contact of de communicatie is begrijpelijk en eenduidig. De inhoud van een individueel contact of individuele communicatie is voor alle kanalen gelijk.
- De interactie met de verschillende stakeholders vindt bij voorkeur digitaal plaats, waarbij geïdentificeerde en geautoriseerde belanghebbenden eigen relevante informatie kunnen benaderen via een portal.
- Binnen de Cogas groep worden de commerciële en persoonsgegevens van Coteq Netbeheer B.V. en Cogas Duurzaam B.V. gescheiden om invulling te geven aan de beperkingen die voortvloeien uit respectievelijk de Gaswet, Elektriciteitswet 1998 en Energiewet voor Coteq Netbeheer B.V. en de Warmtewet voor Cogas Duurzaam B.V.
- De verschillende juridische entiteiten maken gebruik van de industrie standaarden die van toepassing zijn binnen de sector waarin zij opereren. Dit is met name van toepassing op Coteq Netbeheer B.V. in relatie tot het MFF BAS en de bijbehorende ontwikkeling als gevolg van wijzigingen op bedrijfsprocessen.
- Uitval in applicaties of in de integratie tussen applicaties is near real time inzichtelijk en snel en simpel op te lossen.

5 Applicatie Architectuur

5.1 Algemene Kaders & Principes

Principe	Uitleg
Ontkoppel waar mogelijk	Applicatie(funcitie)s kunnen zoveel mogelijk onafhankelijk van elkaar opereren.
Werk in de actualiteit	Applicaties worden ontworpen om snel te reageren op nieuwe gebeurtenissen (<i>event driven</i>).
Altijd aan	Applicaties worden standaard ontwikkeld met hoge beschikbaarheidseisen.
Streef naar eenvoud	We streven naar een zo eenvoudig mogelijk applicatielandschap

5.1.1 Uitgangspunten

Uit deze algemene kaders en principes volgen de volgende uitgangspunten:

- De dienstverlening binnen juridische entiteiten binnen de Cogas-groep vereist een hoge beschikbaarheid van zowel de functionaliteit als de gegevens binnen de integrale Bedrijfsvoeringsoplossing.
- Foutmeldingen in applicaties of in de integratie tussen applicaties is near real time inzichtelijk en snel en simpel op te lossen.
- Foutmeldingen in applicaties of in de integratie tussen applicaties is near real time moet beperkt blijven tot de component waarin de uitval is opgetreden en mag geen onnodig negatief effect hebben op aangrenzende componenten en processen.
- De impact van het technisch falen van een component in de integrale Bedrijfsvoeringsoplossing moet beperkt blijven tot de component waarin de uitval is opgetreden en mag geen negatief effect hebben op aangrenzende componenten en processen.
- Verantwoordelijk medewerkers of afdelingen krijgen near real time informatie als er sprake is van relevante wijzigingen in de relevante processen.
- Gegevens moeten ontsloten worden ten behoeve van de Cogas standaard BI voorziening.

5.2 Huidig high level applicatielandschap

In onderstaande tabel zijn de applicaties opgenomen die interactie hebben met de integrale Bedrijfsvoeringsoplossing voor het uitvoeren van de processen binnen het domein financieel, magazijn of marktfacilitering uit de LBD.

Bedrijfsvoering applicatie	Toelichting	Impact
Ultimo	Betreft de Enterprise Asset Management (EAM) tool, waarmee Cogas alle onderhoudstaken aan de gas-, elektriciteits- en warmtenetten uitvoert. Dit systeem bevat dan ook alle onderhoudsdata.	Bron voor gegevens als er sprake is van verhaalbare schade en er een factuur gemaakt dient te worden. Zie LBD financieel domein paragraaf 3.4.4.2 Factureren overige
CoNEKT	CoNEKT betreft een systeem waarmee Cogas aangesloten is op mijnaansluiting.nl en het DSP. Via dit systeem worden de technische gereed meldingen en tekeningen van het werk binnen de infrastructuur van aannemers ontvangen.	Start voor projecten in het Aansluitdomein en Meetdomein. Zie LDB financieel domein hoofdstuk 3.4.4 Projectkostenbeheersing
ZeroFriction	Dit systeem wordt ingezet voor verbruiksbepaling en facturatie van aangeslotenen op het warmtenet.	Levert relevante journaalposten op aan de integrale Bedrijfsvoeringsoplossing.
Beaufort	Binnen Beaufort wordt de salarisadministratie uitgevoerd.	Levert relevante journaalposten op aan de integrale bedrijfsvoeringsoplossing zie 3.3.2 Inrichting financiële administratie
DTG	De DTG applicatie betreft een applicatie waarmee monteurs de administratie van het plaatsen, verwijderen of wijzigen van een gas- of elektriciteitsmeter kunnen doorgeven aan Coteq Netbeheer BV.	Levert relevante gegevens op ten behoeve van Marktfacilitering zie paragraaf 5.2.3 Beheren meters
SOA MMP	Dit betreft een orkestratie van het metermutatieproces (MMP) die binnen de SOA omgeving van de OFM (Oracle Fusion Middleware) is ontwikkeld.	Levert relevante gegevens op ten behoeve van Marktfacilitering zie paragraaf 5.2.3 Beheren meters

In onderstaande tabel zijn de applicaties opgenomen die interactie hebben met de integrale Bedrijfsvoeringsoplossing aangezien deze de basis vormen voor de generieke kantoorautomatisering en BI binnen de Cogas-groep.

Generieke Applicatie	Toelichting
Matillion	Deze applicatie wordt gebruikt voor de ontsluiting van databronnen.
Snowflake	De data vanuit Matillion wordt in de database van de applicatie Snowflake opgeslagen.
Power BI	De gebruikersinterface waarmee rapportages opgesteld en gebruikt kunnen worden van de data binnen Snowflake.
Office 365	Binnen de Cogas-groep wordt veelvuldig gebruik gemaakt van Microsoft tooling (o.a. Teams, SharePoint, Excel, Word).

Ook zijn er nog een aantal **externe applicaties** die voor de Cogas-groep van groot belang zijn.

Externe Applicatie	Toelichting	Impact
LIP (mijnaansluiting.nl)	Dit betreft het portaal waarop potentiële klanten en aangeslotenen aanvragen in kunnen dienen voor nieuwe aansluitingen of wijzigingen en verwijderingen van bestaande aansluitingen.	Huidige integratie via CoNEKT zie tabel bedrijfsvoeringsapplicaties, hoofdstuk 3.2
DSP	Het digitale samenwerkingsplatform betreft een systeem waarmee werk binnen de infrastructuur bij aannemers belegd kan worden. Dit platform zorgt voor de uitwisseling van relevante informatie tussen de partijen.	Huidige integratie via CoNEKT zie tabel bedrijfsvoeringsapplicaties, hoofdstuk 3.2
C-AR	Het Centrale Aansluitingen Register bevat alle informatie die nodig is om de marktwerking binnen de gas- en elektriciteitsmarkt te ondersteunen.	Zie LBD marktfacilitering domein
C-ARM	Het Centrale Allocatie, Reconciliatie en Meetdata systeem betreft het systeem waarbinnen alle meetdata van de gas- en elektriciteitsaansluitingen wordt bijgehouden en waar de allocatie en reconciliatie plaats vindt.	Zie LBD marktfacilitering domein paragraaf 5.4 Beheren stamgegevens en paragraaf 5.5 Beheren meters Huidige integratie via OiC
CERES	CERES betreft het systeem waarop eigenaren hun opwekinstallaties dienen aan te melden. Deze informatie wordt door de netbeheerder onder andere gebruikt voor het uitvoeren van netberekeningen.	Zie LBD marktfacilitering domein paragraaf 5.4 Beheren stamgegevens Huidige integratie via OiC
ADC	Alle aangeslotenen in het kleinverbruik segment hebben een contract met de netbeheerder via de energieleverancier.	Zie LBD financieel domein paragraaf 3.4.4.3 Verwerken ADC

	De energieleverancier brengt kosten voor de netbeheerder in rekening bij haar klanten. Het AfDrachtControle systeem regelt de uitwisseling van deze opbrengsten voor de netbeheerder tussen de energieleverancier en netbeheerder.	Huidige integratie via OiC
PUD	Het Portaal Uitwissel Diensten regelt het uitwisselen van data die niet in C-AR is vastgelegd, maar wel nodig is voor het ondersteunen van de marktwerving.	Zie LBD marktfacilitering domein paragraaf 5.4 Beheren stamgegevens en paragraaf 5.5 Beheren meters Huidige integratie via OiC
Connexo	Dit betreft het systeem waarmee de slimme meters van de Cogas-groep worden beheerd. Dit systeem wordt door Enexis beheerd en wordt gevoed vanuit het C-AR van de Cogas-groep.	Zie LBD marktfacilitering domein paragraaf 5.4 Beheren meters Huidige integratie via OiC

5.3 Integratie

- De integratie van de componenten binnen de integrale Bedrijfsvoeringsoplossing valt onder de volledige verantwoordelijkheid van de Leverancier.
- Integratie met applicaties uit de tabel externe applicaties of cloud oplossingen in de tabel Bedrijfsvoeringsapplicaties is toegestaan mits dit conform de geldende industrie standaarden mogelijk is.
- Voorziet de integrale Bedrijfsvoeringsoplossing niet in een directe integratie dan wordt de integratie via het OiC iPaaS platform van Cogas ingericht.
- Point-to-point (tight coupling) oplossingen tussen applicaties zijn niet toegestaan tenzij:
 - De (derde partij)toepassing dit afdwingt. Voorbeeld: een streaming van log- of video- of monitoringdata.
 - Een tijdelijke point to point oplossing aantoonbaar kosten en/of mankracht bespaart.

6 Data Architectuur

6.1 Algemene Kaders & Principes

Principe	Uitleg
Datasets zijn onze key assets	Onze data speelt een sleutelrol en wordt daarom behandeld als key assets.
Adequate toegang voor medewerkers en 3 ^e partijen	Elke medewerker en 3 ^e partijen van Cogas heeft toegang tot de data die hij/zij nodig heeft, ongeacht de plek waar die data staat.
Duidelijke data provenance	De bron, status en kwaliteit van de door Cogas gebruikte of geleverde data is voor iedereen duidelijk.
Data gedistribueerd beschikbaar stellen	Wie data genereert, is ook verantwoordelijk voor het beschikbaar maken van die data aan derden (intern en extern).
Bronregistraties zijn leidend	Dit impliceert onder andere dat data niet redundant wordt opgeslagen en in onze situatie er koppelingen noodzakelijk zijn met bronnen zoals het C-AR en C-ARM.

6.1.1 Uitgangspunten

Uit deze algemene kaders en principes volgen de volgende uitgangspunten:

- Het eigenaarschap van data is belegd.
- Data kent maar één waarheid. Deze is gebaseerd op de mutatedatum en/of de tijdsgeldigheid van het data item.
- Data kent maar één bron. Deze bron bevat de bovenstaande waarheid.
- Vastlegging van data buiten deze bron, ook vluchtig, is geautoriseerd en gedocumenteerd.
- Cogas data is BIV geclassificeerd.

6.2 Orkestratie

Binnen het marktfacilitering domein (LBD paragraaf 5.3 Beheren stamgegevens en paragraaf 5.4 Beheren meters) is er veel procesinteractie en dus applicatie-interactie.

Vanuit de fysieke wereld ontstaat gegevens die in de administratieve wereld geregistreerd en gedeeld moet worden.

Fysiek	Toelichting	Impact
DTG	De DTG applicatie betreft een applicatie waarmee monteurs de administratie van het plaatsen, verwijderen of wijzigen van een gas- of elektriciteitsmeter kunnen doorgeven aan Coteq Netbeheer.	Levert relevante gegevens op ten behoeve van Marktfacilitering zie paragraaf 5.4 Beheren meters

Administratief	Toelichting	Impact
ADC	Alle aangeslotenen in het kleinverbruik segment hebben een contract met de netbeheerder via de energieleverancier. De energieleverancier brengt de kosten voor de netbeheerder in rekening bij hun klanten. Het AfDrachtControle systeem regelt de uitwisseling van deze opbrengsten voor netbeheerder tussen de energieleverancier en netbeheerder.	
C-AR	Het Centrale Aansluit Register bevat alle gegevens die nodig is om de marktwerking binnen de gas- en elektriciteitsmarkt te ondersteunen.	Zie LBD marktfacilitering domein
C-ARM	Het Centrale Allocatie, Reconciliatie en Meetdata systeem betreft het systeem waarbinnen alle meetgegevens van de gas- en elektriciteitsaansluitingen wordt bijgehouden en waar de allocatie en reconciliatie plaats vindt.	Zie LBD marktfacilitering domein paragraaf 5.3 Beheren stamgegevens en paragraaf 5.4 Beheren meters Huidige integratie via OiC
SOA MMP	Dit betreft een orkestratie van het metermutatieproces (MMP) die binnen de SOA omgeving van de OFM (Oracle Fusion Middleware) is ontwikkeld.	Zie LBD proces meterbeheer.

CoNEKT	CoNEKT betreft de applicatie waarmee Cogas aangesloten is op het LIP en DSP. Via deze applicatie wordt het DSP gevoed en worden bijvoorbeeld de technische gereedmeldingen en tekeningen van het werk binnen de infrastructuur van aannemers ontvangen.
---------------	---

Om verschillende informatiestromen volledig, correct en tijdig in de verschillende systemen te verwerken is orkestratie vereist. Op dit moment is dit onderdeel van de OIC iPaaS en on-premises OFM. Het heeft de voorkeur om deze orkestratie onder te brengen in de integrale Bedrijfsvoeringsoplossing.

7 Security Architectuur

7.1 Algemene Kaders & Principes

Dit hoofdstuk beschrijft de Security Architectuur en stelt een set aan principes, standaarden en controles vast. Dit vormt de basis bij het implementeren, wijzigen, migreren en verwijderen van gegevens en informatiesystemen. Dit heeft als doel een baseline beveiligingsniveau te creëren en de vertrouwelijkheid, integriteit en beschikbaarheid van gegevens te kunnen borgen. Het biedt de operatie handvatten om gecontroleerd en gestructureerd invulling te geven aan de IT-dienstverlening.

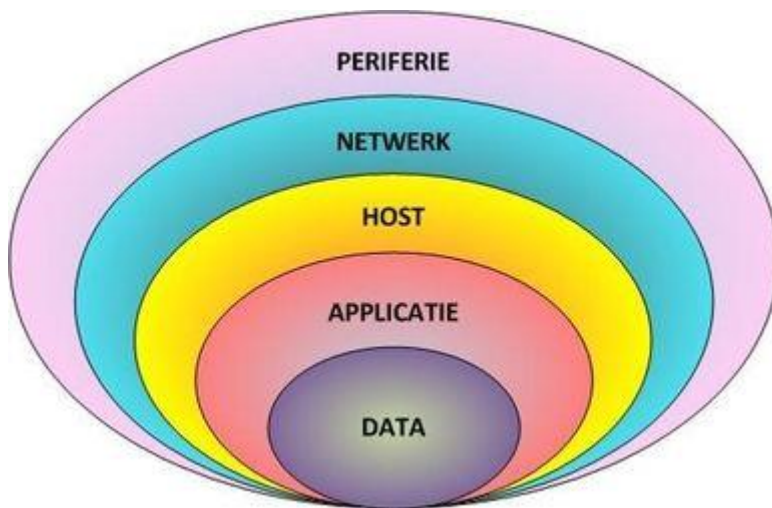
De beschreven principes en richtlijnen dienen toegepast te worden bij de implementatie van nieuwe informatiesystemen binnen het IT-landschap van Cogas, bij het uitwisselen van informatie met derden zoals leveranciers en partners en gedurende de designfase van nieuwe omgevingen. Deze richtlijnen en principes gelden voor geheel Cogas.



Figuur 1 BIV-triade

SP01. Zorg voor balans tussen veiligheid en nut	
Omschrijving	De mate van beveiliging dient in overeenstemming te zijn met het risicoprofiel. Beveilig vitale systemen met de hoogste prioriteit gevolgd door minder vitale systemen. Automatiseer waar mogelijk, om menselijke fouten te beperken.
Rationale	Securitymaatregelen dienen in verhouding te staan tot de risico's. Risico's worden bepaald door het uitvoeren van een risicoanalyse. Buitenproportionele maatregelen zorgen voor onnodige complexiteit en kosten.
Implicatie	Data dient geclassificeerd te zijn door de dataeigenaar op basis van: Vertrouwelijkheid, Integriteit en Beschikbaarheid . Maatregelen dienen genomen te worden in overeenstemming met de dataclassificatie. Een risico analyse dient uitgevoerd te worden om zo kostenefficiënt mogelijk veiligheidsmaatregelen te treffen.

SP02. Security by Design	
Omschrijving	Veiligheidsmechanismen om de Vertrouwelijkheid, Integriteit en Beschikbaarheid te borgen dienen vanaf de initiatiefase meegenomen te worden en niet achteraf. Dit geldt ook voor de business processen.
Rationale	Controles ten behoeve van vertrouwelijkheid, beschikbaarheid en integriteit in informatie en informatiesystemen zijn duurder om te implementeren aan het einde van een project en vaak minder efficiënt en geïntegreerd, dan wanneer het in het oorspronkelijke ontwerp van het project meegenomen wordt.
Implicatie	Beveiliging is een integraal onderdeel van de systeemarchitectuur. De beveiliging moet op alle lagen van de architectuur meegenomen worden en schaalbaar zijn. Alle oplossingen moeten op veiligheid getest worden. Daarbij kan gedacht worden aan, maar niet beperkt tot de volgende controlegebieden: fysieke beveiliging, logische toegangscontrole, functiescheiding, informatie-uitwisseling, eventregistratie, beheer van technische kwetsbaarheden, wet- en regelgeving, mogelijkheid tot het uitvoeren van audits op informatiesystemen.
SP03. Security als Proces	
Omschrijving	Security dient als een proces ingericht te zijn. Door <u>continu</u> te monitoren is de veiligheid geborgd en kan bijgesteld worden indien nodig.
Rationale	Dreigingen veranderen continu en daarmee ook de bijbehorende risico's. Risicoanalyses dienen daarom regelmatig uitgevoerd/herijkt te worden om hierop aan te sluiten en risico's te kunnen mitigeren.
Implicatie	Risicoprofielen worden continu beoordeeld en indien nodig aangepast. Dit geldt voor (technische) oplossingen die hieraan ten grondslag liggen alsook de organisatorische aspecten.
SP04. Defense in Depth	
Omschrijving	Op elk niveau van het proces en keten moeten gepaste maatregelen getroffen worden om deze adequaat te beveiligen.
Rationale	Een gelaagde verdedigingsaanpak met oplossingen op elk niveau die elkaar aanvullen verlaagt de kans op het compromitteren van de data.
Implicatie	Vertrouw niet op maatregelen van functies die elders getroffen zijn en houd rekening met worst case scenario's. Implementeer meerdere verdedigingsmechanismen zoals: data-encryptie, firewalling, encryptie van transport, signing van data en hardening van het onderliggende besturingssysteem (zie figuur). Als één laag van het mechanisme faalt, dan wordt de bedreiging opgevangen door de volgende laag. Stel veilige grenzen, houd informatiestromen gescheiden en documenteer alle lagen van verdediging.



Figuur 2 Lagen van beveiliging

SP05. Verleen toegang tot informatiesystemen op basis van rollen	
Omschrijving	Verleen toegang tot informatie en informatiesystemen op basis van RBAC-rollen in plaats van gebruikers- en systeemaccounts.
Rationale	Autorisaties moeten toegekend worden op basis van rollen in plaats van gebruikers en/of systeemaccounts. Een gebruiker- of systeemaccount wordt op basis van functie en verantwoordelijkheden aan een of meerdere rollen toegekend. Elke rol moet beschreven zijn in een autorisatiematrix waarin per rol duidelijk aangegeven wordt wat de rechten zijn om die werkzaamheden uit te kunnen voeren. Hier moet het <i>Least Privileges Principle</i> toegepast worden.
Implicatie	Per functie en proces moet duidelijk zijn wat de rollen en bijbehorende autorisatieniveaus zijn. Hiervoor moeten de proceseigenaren geraadpleegd worden. Authenticatie en autorisatie moeten adequaat ingericht zijn. Autorisatie na authenticatie.

SP06. Least Privilege Principle – Need to know principle	
Omschrijving	Pas het principe toe van minimale rechten (least privileges)
Rationale	Pas minimale rechten toe aan personen, applicaties en systemen, die noodzakelijk zijn voor het uitvoeren van taken en niet meer. Het doel is, om het risico te beperken door het aantal personen te beperken met toegang tot kritieke systemen en controles. Hierbij kan gedacht worden aan het toekennen van (meer) rechten aan gebruikers, controle houden over wie wel en niet bepaalde security functies van een systeem mag/kan aanpassen.
Implicatie	Zorg voor meerdere beheerders met beperkte toegang i.p.v. één persoon met super user rechten. Rechten worden toegekend op basis van functie en/of rol(len). Toegekende rechten moeten gewijzigd worden als gevolg van functiewijziging en/of het vertrek bij Cogas/Coteq. Niet gebruikte services worden uitgeschakeld.

SP07. Houd Rekening met Incidenten	
Omschrijving	Houdt rekening dat incidenten zich voordoen.
Rationale	Incidenten doen zich voor, hoe goed de getroffen maatregelen ook zijn, om exploitatie te voorkomen.
Implicatie	Er moet een goede backup procedure zijn ingericht en deze moet periodiek getoetst worden op effectiviteit. Daarnaast moet een incident response procedure aanwezig zijn om de impact van een security breach tot een minimum te beperken.

SP08. Logging en Monitoring	
Omschrijving	Log en monitor alle gebeurtenissen.
Rationale	Alle gebeurtenissen en acties met betrekking tot gebruikers, processen en systemen moeten gelogd en gemonitord worden. Hierdoor kan continu en op elk moment controle en inzicht verkregen worden over de omgeving en te allen tijde een traceback gedaan worden in geval er een ongeautoriseerde actie uitgevoerd moet worden en/of systemen niet beschikbaar zijn.
Implicatie	Systemen, applicaties en diensten moeten ingesteld worden om alle (belangrijke) acties te loggen en naar een centraal loggingsysteem te sturen. Logfiles moeten centraal opgeslagen worden, voorzien zijn van een timestamp en een hash om manipulatie aantoonbaar te maken.

SP09. Test en Scan Regelmatig	
Omschrijving	Maatregelen en systemen moeten periodiek getest en gescand worden.
Rationale	Computers en omgevingen waarin we werken zijn dynamisch. De technologie, gebruikers, informatie in de systemen, risico's en beveiligingseisen veranderen continu. Om vast te stellen dat genomen maatregelen aansluiten bij de risico's en dreigingsniveaus moeten regelmatig security testen uitgevoerd worden. Door systemen en componenten periodiek te testen en te scannen op kwetsbaarheden kan de tijd tussen het optreden van een kwetsbaarheid en de uitbuiting hiervan tot een minimum worden beperkt.
Implicatie	Een assessmentproces moet ingericht worden die voorziet in het periodiek uitvoeren van security audits en pentesten om maatregelen en het beleid te toetsen op effectiviteit.

SP10. Eigenaarschap	
Omschrijving	Elk bedrijfsmiddel dient een eigenaar te hebben.
Rationale	Elke set aan data kent een eigenaar die eindverantwoordelijk is voor het laten uitvoeren van een risicoanalyse en bepaling van de classificatie van de data.

Implicatie	Een lijst moet opgesteld worden, waarin alle diensten en systemen opgenomen zijn met één eigenaar en niet een groep van eigenaren. Deze lijst moet periodiek gecontroleerd en herzien worden. De eigenaren moeten zich bewust zijn van zijn/haar verantwoordelijkheden en zorgdragen dat taken op de juiste wijze zijn gedelegeerd.
SP11. Zonering en Segmentering	
Omschrijving	Zorg voor een goede zonering en segmentering van data en infrastructuur.
Rationale	Op basis van dataclassificatie wordt informatie en informatiesystemen in de daarvoor bestemde zone toegewezen. Dit vindt plaats op basis van vertrouwensniveaus (zogenaamde trust levels). Hierin worden 4 niveaus gehanteerd: <i>Onvertrouwd</i> , <i>Semi-Vertrouwd</i> , <i>Vertrouwd</i> en <i>Zeer Vertrouwd</i> .
Implicatie	Classificatie van informatie(systemen) op basis van vertrouwelijkheid en integriteit moet aanwezig zijn. Het classificatiesysteem moet periodiek gecontroleerd en gevalideerd worden. Systemen moeten logisch ingedeeld en geïsoleerd worden door gebruik te maken van fysieke componenten en/of security controles (bvb firewalls, ACLs, VLANs en NSGs). Zorg dat informatiestromen met verschillende risicoprofielen van elkaar gescheiden zijn. Verschillende stadia van systemen (Ontwikkel, Test, Acceptatie en Productie) en functie (logging, monitoring, auditing) moeten gescheiden zijn.

SP12. Gelijke Minimale Beveiliging	
Omschrijving	Gelijke minimale beveiliging.
Rationale	Indien meerdere paden naar een object (informatie/informatiesysteem) leiden, waarbij verschillende security maatregelen getroffen zijn, dan moeten deze een minimale gelijke beveiliging hebben.
Implicatie	Het toepassen van dit principe leidt er toe dat het niet mogelijk is om sterk beveiligingsmechanisme te omzeilen via een minder veilige route naar informatie en/of informatiesystemen.
SP13. KISS (Keep It Simple, Stupid)	
Omschrijving	Houd het simpel.
Rationale	Veiligheid is het meest effectief als diegene die ermee werken ook begrijpen hoe het werkt. Door het simpel en veilig te houden is de kans op het compromitteren van informatie en informatiesystemen laag. Complexiteit verhoogt de kans op fouten en kan een averechts effect hebben op security.
Implicatie	Bij het implementeren van een nieuwe techniek moet rekening gehouden worden met de gebruiker. Zorg dat de kennis belegd is bij meerdere medewerkers en begrepen wordt. Dat voorkomt afhankelijkheid. Het moet makkelijk op te zetten, te onderhouden en beheersbaar zijn.

SP14. Audit	
Omschrijving	Zorg voor volledige en beveiligde audit trails.
Rationale	Om een goed en volledig inzicht te hebben wie toegang heeft tot welke diensten en welke data, is het van belang dat alle acties die uitgevoerd worden, worden gemonitord. Oneigenlijk gebruik en het adequaat blijven functioneren van het systeem wordt hiermee geborgd.
Implicatie	Implementeer auditmechanismen om ongeautoriseerde toegang en gebruik van informatie en informatiesystemen te detecteren en onderzoek naar incidenten te ondersteunen. Hierbij moet rekening worden gehouden met de retentie, opslag en archivering van audit data.
SP15. Pas-Toe of Leg-Uit (Comply or Explain)	
Omschrijving	Werk volgens architectuur en vastgestelde standaarden.
Rationale	Door gestandaardiseerd en op een uniforme, controleerbare en reproduceerbare manier te werken, wordt veiligheid en privacy van data en diensten geborgd. Afwijken van architectuurprincipes verhoogt de kans op de introductie van fouten. Hierdoor neemt het risico toe op het compromitteren van data. Afwijken van architectuurprincipes is alleen toegestaan indien er zwaarwegende redenen zijn, die gemotiveerd kunnen worden en betrekking hebben op specifieke situaties. Algemene afwijkingsgronden worden als onvoldoende beschouwd.
Implicatie	Procedures moeten opgesteld, afgestemd en gevolgd worden. De architectuurprincipes bepalen de uitgangspunten en de te volgen werkwijze. Procedures moeten tollgates bevatten die het toepassen van architectuur principes en standaarden toetsen en borgen.
SP16. Gebruik Altijd Veilige Protocollen	
Omschrijving	Maak alleen gebruik van veilige protocollen die security intrinsiek ingebouwd hebben.
Rationale	Het gebruik van onveilige protocollen introduceert veiligheidsrisico's die gemakkelijk voorkomen kunnen worden.
Implicatie	Het gebruik van onveilige protocollen is alleen toegestaan als interactie met een niet-vertrouwde omgeving essentieel is. Protocollen moeten gevalideerd worden tegen de applicatie.
SP17. Beveilig Data in Transit	
Omschrijving	Bescherm data die in transit is.

Rationale	Data wat zich door één of meerdere netwerken heen beweegt moet adequaat beveiligd worden tegen manipulatie en af luisteren door het gebruik van netwerkbeveiliging en encryptie.
Implicatie	Het niet implementeren van dit architectuurprincipe kan leiden tot het compromitteren van de integriteit en betrouwbaarheid van de data in transit.

SP18. Beveilig Data in Rust

Omschrijving	Bescherm data die in rust verkeert.
Rationale	Data die zich in rust bevindt (zoals in databases en fileshares) moet adequaat beveiligd worden tegen manipulatie en/of exfiltratie door het gebruik van encryptie en/of afscherming.
Implicatie	Het niet implementeren van dit architectuurprincipe leidt tot het compromitteren van de integriteit en betrouwbaarheid van deze data.

SP19. Authenticatie

Omschrijving	Authentiseer gebruikers en processen om zorg te dragen dat adequate toegangscontrole mechanismen zijn toegepast binnen en tussen domeinen.
Rationale	Authenticatie is het proces waarin een systeem vaststelt of het opzetten van een verbinding of het verkrijgen van toegang valide is of niet. Het is essentieel dat voldoende authenticatie wordt gerealiseerd om het beveiligingsbeleid te implementeren en te borgen.
Implicatie	Er is een service nodig om gebruikers en processen te authenticeren.

SP20. Autorisatie

Omschrijving	Autoriseer gebruikers en processen nadat deze geauthentiseerd zijn.
Rationale	Autorisatie moet uitgevoerd worden als een expliciete controle nadat de gebruiker of het proces geauthentiseerd is. Autorisatie is niet alleen afhankelijk van de rechten die zijn gekoppeld aan een geverifieerde gebruiker, maar ook van de context van het verzoek. Afhankelijk van het systeem, de applicatie en het proces dient het tijdstip van het autorisatieverzoek en de locatie van de aanvrager mogelijk in overweging worden genomen.
Implicatie	Indien het een gevoelige bewerking betreft, dan moet er opnieuw geauthentiseerd worden.

SP21. Need-to-know principe	
Omschrijving	Autoriseer gebruikers en processen om zorg te dragen dat adequate toegangscontrole mechanismen zijn toegepast binnen en tussen domeinen.
Rationale	Autorisatie is het proces waarin een systeem vaststelt of het opzetten van een verbinding of het verkrijgen van toegang valide is of niet. Het is essentieel dat voldoende authenticatie wordt gerealiseerd om het beveiligingsbeleid te implementeren en te borgen.
Implicatie	Er is een service nodig om gebruikers en processen te autoriseren.

7.1.1 Uitgangspunten

Uit deze algemene kaders en principes volgen de volgende uitgangspunten:

7.1.1.1 IAM gebruikers

- De Leverancier maakt gebruik van de Azure Active Directory van Cogas
- Bij het ontwerp van ieder nieuw systeem of iedere nieuwe applicatie moet een Role Based Access-matrix worden gedefinieerd en dienovereenkomstig worden geïmplementeerd. Alle ontwerpen moeten beoordeeld worden en goedgekeurd door de systeemeigenaar.
- Iedere gebruiker die werkt met systemen, gegevens en bronnen van Cogas moet een uniek identificeerbare identiteit hebben.
- Een standaard naamgevingsconventie moet gedocumenteerd en consistent worden toegepast op gebruikersaccounts, serviceaccounts, beveiligingsgroepen, bronnen, systemen en apparaten met het oog op een unieke identificatie.
- Standaard procedures moeten beschreven zijn voor inhuur/indiensttreding, wijziging van rol en/of functie en uitdiensttreding van personeel van de Leverancier of namens de Leverancier toegang heeft tot de integrale Bedrijfsvoeringsoplossing. Dit moet worden gedocumenteerd en afgestemd met belanghebbenden voor het beschikbaar stellen en vrijgeven van accounts en rechten.
- Het aanmaken van gebruikersaccounts en verlenen van toegangsverzoeken, inclusief speciale accounts en rechten, moeten formeel worden gedocumenteerd en goedgekeurd door de juiste manager en/of systeemeigenaar.
- Waar mogelijk moeten gebruikersaccounts ingesteld worden om automatisch te verlopen op een vooraf gedefinieerde datum.
- Accounts toegewezen aan contractanten en tijdelijk personeel moeten ingesteld worden, om te vervallen volgens de vervaldatum van het contract.
- Gebruikersaccounts van intern personeel en aannemers moeten uitgeschakeld worden na 90 dagen van inactiviteit.
- Externe gebruikersaccounts moeten uitgeschakeld worden na 30 dagen inactiviteit.
- Toegangsrechten moeten onmiddellijk gedeactiveerd of verwijderd worden wanneer een werknemerscontract wordt beëindigd of wanneer een gebruiker geen legitieme reden meer heeft om toegang te krijgen tot de systemen of gegevens van Cogas.

Gedeactiveerde gebruikersaccounts en data moeten na 90 dagen worden verwijderd, tenzij er een door het management goedgekeurde reden is om het account en de bijbehorende gegevens te bewaren.

- Gastaccount toegang moet strikt worden beperkt tot de bijbehorende systemen en bronnen en moet ingesteld worden, om te verlopen wanneer geen toegang meer nodig is.
- Het gebruik en het wijzigen van gebruikers-, gedeelde- en serviceaccounts moet gecontroleerd en ge-audit worden, inclusief het tijdstip van authenticatie en gebeurtenissen. Auditlogs moeten veilig bewaard worden gedurende ten minste één jaar voor kritieke systemen en 90 dagen voor niet-kritieke systemen.
- Alle gebruikersaccounts en toegangsrechten moeten ten minste om de 6 maanden door systeemeigenaren worden gecontroleerd om slapende accounts en accounts met buitensporige rechten te detecteren.
- De identiteit van een gebruiker moet positief geverifieerd worden, voordat een nieuw wachtwoord wordt toegekend en een account wordt ontgrendeld
- Need-to-Know: Gebruikers of bronnen krijgen toegang tot systemen die noodzakelijk zijn om hun taken uit te voeren.
- Least Privilege: Gebruikers krijgen minimale rechten die nodig zijn om hun taken uit te voeren.
- Externe en openbare toegang tot de integrale Bedrijfsvoeringoplossing moet gebruikmaken van multi-factor authenticatie.

7.1.1.2 IAM applicaties

- Waar mogelijk moeten alle interne en externe systemen worden geïntegreerd met Azure Single Sign On (SSO) voor het opslaan en leveren van identiteiten en authenticatie.
- Een standaard naamgevingsconventie moet gedocumenteerd worden en consistent worden toegepast op gebruikersaccounts, serviceaccounts, beveiligingsgroepen, bronnen, systemen en apparaten met het oog op een unieke identificatie.
- Bij het ontwerp van ieder nieuw systeem of iedere nieuwe applicatie moet een Role Based Access-matrix gedefinieerd worden en dienovereenkomstig worden geïmplementeerd. Alle ontwerpen moeten beoordeeld worden en goedgekeurd door de systeemeigenaar.
- Systeem- en serviceaccounts mogen alleen gebruikt worden door systeemcomponenten die authenticatie vereisen en krijgen geen interactieve inlogrechten; toegang tot inloggegevens moet beperkt worden tot geautoriseerde IT-beheerders.
- Het gebruik en het wijzigen van gebruikers-, gedeelde- en serviceaccounts moet gecontroleerd en ge-audit worden, inclusief het tijdstip van authenticatie en gebeurtenissen. Auditlogs moeten veilig bewaard worden gedurende ten minste één jaar voor kritieke systemen en 90 dagen voor niet-kritieke systemen.
- Need-to-Know: Gebruikers of bronnen krijgen toegang tot systemen die noodzakelijk zijn om hun taken uit te voeren.
- Least Privilege: Gebruikers zullen minimale rechten krijgen die nodig zijn om hun taken uit te voeren.
- Externe en openbare toegang tot de integrale Bedrijfsvoeringoplossing moet gebruikmaken van multi-factor authenticatie.

- Application Programming Interfaces (API's) moeten een uniek token gebruiken voor authenticatie van elke API-aanroep. Uitzonderingen moeten gedocumenteerd worden en vereisen beoordeling en goedkeuring van de Security Officer.
- Alleen goedgekeurde authenticatieprotocollen die gebruik maken van cryptografisch beveiligde authenticatiemechanismen kunnen worden gebruikt voor interne en externe systemen en applicaties.

7.1.1.3 IAM generiek

- Gedeelde identiteiten zijn niet toegestaan tenzij goedgekeurd en gedocumenteerd door systeemeigenaren en de Security Officer. Er moet een gegronde reden zijn om af te wijken waarbij aantoonbaar gemaakt moet worden dat een identiteit gedeeld moet worden.
- In het geval van een incident of gebeurtenis met een hoog risico, heeft de Security Officer de bevoegdheid om onmiddellijk passende maatregelen te nemen (d.w.z. het uitschakelen van gebruikerstoegang) om het risico te beheersen en te beperken.
- Systeem- en applicatiesessies moeten automatisch vergrendeld of afgemeld worden, na minimaal 15 minuten van inactiviteit. Alle uitzonderingen moeten goedgekeurd worden door de Security Officer of een persoon verantwoordelijk voor informatiebeveiliging voordat deze ingesteld wordt.
- Application Programming Interfaces (API's) moeten een uniek token gebruiken voor authenticatie van elke API-aanroep. Uitzonderingen moeten gedocumenteerd worden en vereisen beoordeling en goedkeuring van de Security Officer.
- Waar mogelijk moeten detectie- en preventieve controles ingesteld worden tegen brute-force-aanvallen, meerdere inlogfouten en onmogelijke aanmeldingen op basis van tijds- en geografische afstandsbeperkingen.
- Waar mogelijk moet minimaal IP-whitelisting toegepast worden, voor toegang tot systemen en applicaties.
- Geoblocking van toegang uit "ongewone" landen moet overwogen worden.

8 Non-functionals

1.	De integrale Bedrijfsvoeringsoplossing is locatie- en tijdonafhankelijk benaderbaar vanuit verschillende (mobiele) devices via een internetverbinding door middel van een webbrowser of app. De dienst beschikt over een webbased userinterface die zonder beperking van functionaliteit, benaderbaar is met de twee laatste versies van de meest gangbare browsers zoals Microsoft Edge, Google Chrome, Apple Safari, Opera en Mozilla Firefox zonder gebruik te maken van plug-ins (zoals Flash, Silverlight, ActiveX, etc.). Cogas gebruikt op dit moment Microsoft Edge.																								
2.	De data in de integrale Bedrijfsvoeringsoplossing blijft eigendom van Cogas.																								
3.	De integrale Bedrijfsvoeringsoplossing moet naadloos samenwerken met huidige en toekomstige samenwerkingsplatformen, dataopslag en –deling, Cogas gebruikt op dit moment Microsoft Office 365 waarbij gebruik wordt gemaakt van o.a. Word, Excel, OneNote, Teams, Outlook, SharePoint, OneDrive, Jira en Confluence.																								
4.	De Leverancier en de mogelijke onderaannemers moeten beschikken over en voldoen aan de vigerende versie van de norm: NEN/ISO/IEC 27001, NEN/ISO/IEC 27001:2013 Managementsysteem voor informatiebeveiliging, met Verklaring van Toepasselijkheid.																								
5.	Cogas wenst dat de integrale Bedrijfsvoeringsoplossing werkt op basis van Open Standaarden en bewezen technologieën met als achterliggende doel, de bevordering van de interoperabiliteit en de vergroting van de leveranciersonafhankelijkheid. Mocht de Inschrijver een ‘gelijkwaardige’ standaard aanbieden, dan dient deze aan te tonen dat dit alternatief de interoperabiliteit en leveranciersonafhankelijkheid in voldoende mate waarborgt. <table><tr><td>• NEN/ISO/IEC 27034</td><td>NEN/ISO/IEC 27034:2011+</td><td>Richtlijnen voor applicatiebeveiliging</td></tr><tr><td>• OpenAPI Specification</td><td>3</td><td>Beschrijven van REST APIs</td></tr><tr><td>• OAuth</td><td>2.0</td><td>Authorisatie</td></tr><tr><td>• OpenID Connect</td><td>1.0 of SAML 2.0</td><td>Authenticatie en autorisatie</td></tr><tr><td>• HTTPS en HSTS</td><td>1.2</td><td>Beveiligde websiteverbinding</td></tr><tr><td>• TLS 1.3 en 1.2</td><td></td><td>Beveiligde internetverbinding</td></tr><tr><td>• SCIM</td><td>RFC 7642, 7643 en 7644</td><td>Uitwisseling identiteitsinformatie</td></tr><tr><td>• SOAP/XML</td><td>C-AR en C-ARM</td><td></td></tr></table>	• NEN/ISO/IEC 27034	NEN/ISO/IEC 27034:2011+	Richtlijnen voor applicatiebeveiliging	• OpenAPI Specification	3	Beschrijven van REST APIs	• OAuth	2.0	Authorisatie	• OpenID Connect	1.0 of SAML 2.0	Authenticatie en autorisatie	• HTTPS en HSTS	1.2	Beveiligde websiteverbinding	• TLS 1.3 en 1.2		Beveiligde internetverbinding	• SCIM	RFC 7642, 7643 en 7644	Uitwisseling identiteitsinformatie	• SOAP/XML	C-AR en C-ARM	
• NEN/ISO/IEC 27034	NEN/ISO/IEC 27034:2011+	Richtlijnen voor applicatiebeveiliging																							
• OpenAPI Specification	3	Beschrijven van REST APIs																							
• OAuth	2.0	Authorisatie																							
• OpenID Connect	1.0 of SAML 2.0	Authenticatie en autorisatie																							
• HTTPS en HSTS	1.2	Beveiligde websiteverbinding																							
• TLS 1.3 en 1.2		Beveiligde internetverbinding																							
• SCIM	RFC 7642, 7643 en 7644	Uitwisseling identiteitsinformatie																							
• SOAP/XML	C-AR en C-ARM																								
6.	De integrale Bedrijfsvoeringsoplossing kan (stam)bestanden importeren en exporteren. Hierbij moet minimaal de formaten csv, xml, xls en JSON worden ondersteund.																								
7.	Persoonsgegevens, zoals bedoeld in de AVG, moeten overeenkomstig de daarvoor geldende wettelijke eisen en Nederlandse richtlijnen verwerkt en beveiligd worden.																								
8.	De gegevens van (en met betrekking tot) Cogas worden uitsluitend opgeslagen op een locatie binnen de Europese Economische Ruimte.																								
9.	De integrale Bedrijfsvoeringsoplossing ondersteunt Role Based Acces Control.																								

10.	De integrale Bedrijfsvoeringsoplossing ondersteunt ontsluiting via een Identity and Access Control Management mechanisme. Voor Cogas is dat op dit moment Azure Active Directory. De integrale Bedrijfsvoeringsoplossing moet mee kunnen bewegen met eventuele toekomstige ontwikkelingen.
11.	De integrale Bedrijfsvoeringsoplossing ondersteunt single-sign-on. Cogas beschikt op dit moment over één (1) active directory. De integrale Bedrijfsvoeringsoplossing moet mee kunnen bewegen met eventuele toekomstige veranderingen.
12.	Gebruikers en autorisaties moeten door medewerkers van Cogas-groep aangemaakt kunnen worden.
13.	De Leverancier levert gebruikers- en applicatiebeheerdocumentatie voor de aangeboden integrale Bedrijfsvoeringsoplossing.
14.	De gebruikersdocumentatie is beschikbaar in het Nederlands.
15.	De algehele voertaal tijdens de looptijd van de Dienstverleningsovereenkomst in woord en geschrift is Nederlands.
16.	De Leverancier voorziet in integratiemogelijkheden op basis van gangbare standaarden in het algemeen en voor de Cogas-groep geldende industrie standaarden in het bijzonder.
17.	De Leverancier garandeert een Beschikbaarheid van minimaal 99,5% per maand bij een gebruikersvenster van 7*24 uur. Buiten afgestemd gepland onderhoud.
18.	De maximale toelaatbare tijd waarin de integrale Bedrijfsvoeringsoplossing reageert na een gebruikersactie (de responsetijd) bedraagt maximaal 2 seconden.
19.	De integrale Bedrijfsvoeringsoplossing moet berichten met een elektronische, rechtmatige handtekening kunnen versturen en ontvangen.
20.	De Leverancier biedt de mogelijkheid om op een door Cogas te bepalen moment over te gaan op een nieuwe versie van de integrale Bedrijfsvoeringsoplossing.
21.	Naast de productieomgeving wordt ook een acceptatieomgeving beschikbaar gesteld aan Cogas.
22.	De leverancier van de integrale Bedrijfsvoeringsoplossing heeft effectief de eisen van ISO/IEC 27018:2019 of een gelijkwaardige standaard geïmplementeerd.
23.	Systeem- en applicatiesessies moeten automatisch vergrendeld worden of afgemeld na minimaal 15 minuten van inactiviteit.
24.	Leverancier levert iedere 2 jaar een SOC2 Type 2 rapport op.
25.	Opdrachtgever mag in samenspraak een PEN-test uit laten voeren.

8.1 Berekening Beschikbaarheid

Indien gebruik van de integrale Bedrijfsvoeringsoplossing een internetverbinding vereist, voor de eindgebruiker, dan draagt Cogas zelf zorg voor de Beschikbaarheid hiervan vanaf de demarcatie naar het internet. Dit kan de officiële internetverbinding zijn vanaf kantoor of een verbinding elders.

De Beschikbaarheid wordt over een tijdsperiode van een kalendermaand als volgt berekend:

$$\text{beschikbaarheid} = \frac{\text{daadwerkelijke beschikbaarheid van de service in minuten}}{\text{totaal aantal minuten} - \text{aantal minuten gepland onderhoud}} \times 100\%$$

**) Gepland onderhoud wordt niet meegenomen in de beschikbaarheidsberekening, mits deze vooraf is afgestemd met Cogas en er sprake is van onderhoud met onderbreking. In dit geval wordt vooraf afgestemd welke werkzaamheden, wanneer en met welke onderbrekingsduur gerekend wordt.*

Leverancier garandeert een minimale Beschikbaarheid zoals hierboven staat omschreven van 99,5 %.

Gepland onderhoud met onderbreking per kalendermaand betreft maximaal 4 uur.

Gepland onderhoud zonder onderbreking kent geen limiet zolang dit onderhoud op geen enkele wijze invloed heeft voor de eindgebruiker en/of voor de te leveren dienst.

8.2 Applicatie responsetijd

De integrale Bedrijfsvoeringsoplossing reageert na een gebruikersactie (de responsetijd) near real time. Er geldt een maximum van twee seconden.

De Leverancier moet, met onderbouwing, aangeven wanneer bepaalde functionaliteiten hier niet aan kunnen voldoen. Hierover moeten afspraken worden gemaakt.

Gebruikersacties mogen geen negatieve invloed hebben op de dienst in al zijn volledigheid voor wat betreft performance en beschikbaarheid.

8.3 Service Window

De service windows van de dienstverlening zijn als volgt:

Soort	Wanneer
Integrale Bedrijfsvoeringsoplossing, beschikbaarheid	7 dagen per week, van 00:00 tot 24:00 uur
Service desk Leverancier, beschikbaarheid applicatie inhoudelijke (functioneel) support	Op alle werkdagen: ma t/m vr, 07:30 tot 17:00 uur
Service desk Leverancier, storingsdienst (bij prio 1 problemen)	7 dagen per week, van: 00:00 tot 24:00 uur
Onderhoud, uitvoering (met behoud van beschikbaarheid van de dienst)	Mogelijk op elke dag, van: 00:00 tot 06:00
Back-up (met behoud van beschikbaarheid van de dienst)	7 dagen per week, van: 00:00 tot 24:00 uur
Onderhoud infrastructuur, uitvoering (met behoud van beschikbaarheid van de dienst)	Mogelijk op elke dag, van: 00:00 tot 06:00
Voor onderhoud bij voorkeur op basis van een onderhoudskalender	Onderhoud met onderbreking in het weekend, max 1 x per 2 weken. Spoedonderhoud in afstemming met de opdrachtgever
Software updates, uitvoering	Binnen één maand na een release. Security patches worden zo spoedig mogelijk volgens een patchmanagement proces doorgevoerd. Updates vinden plaats buiten reguliere kantoortijden

*) Uitgezonderd officiële Nederlandse feestdagen die vanuit de overheid als vrije dag worden aangemerkt. Opdrachtgever kan besluiten een officiële feestdag te benoemen als werkdag en Leverancier dient die dag dan ook als zodanig te zien.

8.4 Prioriteit

De hierna genoemde prioriteiten zijn van toepassing bij verstoringen (incidenten en problemen) en door de melder te bepalen.

Prioriteit	Betekenis
1	Business impact Kritisch
2	Business impact Hoog
3	Business impact Medium
4	Business impact Laag

Deze prioriteiten worden door de melder bepaald door middel van onderstaande matrix

Prioriteit		Impact			
		Uitgebreid Volledige bedrijf	Groot Afdeling	Beperkt Klein aantal gebruikers	Minimaal Eén gebruiker
Urgentie	Kritisch Geen enkele functie binnen de service kan worden uitgevoerd	1 - Kritisch	1 – Kritisch	2 - Hoog	2 - Hoog
	Hoog Primaire functies binnen de service kunnen niet langer uitgevoerd worden	1 - Kritisch	2 - Hoog	2 - Hoog	3 - Medium
	Medium Functies binnen de service hebben een verminderde werking	2 - Hoog	3 - Medium	3 - Medium	3 - Medium
	Laag De functie kan door middel van een workaround worden uitgevoerd, maar verdient verbetering	4 - Laag	4 - Laag	4 - Laag	4 – Laag
	Impact	De mate van invloed van een Incident op de businessprocessen. De invloed is een vermindering van de			

		beschikbaarheid in aantallen gebruikers, diensten of bedrijfsprocessen die er hinder van hebben ("hoe ernstig is het")
	Urgentie	De mate van hoelang het duurt totdat een Incident een significante impact heeft op de business en daarmee op de snelheid waarop het Incident, Probleem opgelost en de wijziging doorgevoerd moet worden.

8.5 Reactie- en hersteltijd

Opdrachtnemer hanteert de volgende reactie- en oplostijden tijdens klokuren (0:00-24:00):

Omschrijving	Reactietijd (maximum)	Norm	Oplostijd (maximum)	Norm
Prio 1 incident	1 uur	99%	4 uur	99%
Prio 2 incident	2 uur	96%	8 uur	96%

Opdrachtnemer hanteert de volgende reactie- en hersteltijden binnen service window:

Omschrijving	Reactietijd (maximum)	Norm	Oplostijd (maximum)	Norm
Prio 3 incident	4 uur	97%	24 uur	97%
Prio 4 incident	8 uur	97%	80 uur	97%

8.6 Oplossen van incidenten

De helpdesk is zowel via telefoon als e-mail bereikbaar.

Leverancier doorloopt tenminste de volgende stappen met betrekking tot de incidentmelding:

- Het bevestigen naar Cogas van ontvangst van de incidentmelding met vermelding van de door Cogas bepaalde prioriteit. Verschil van inzicht ten aanzien van prioriteit kunnen partijenachteraf bespreken.
- Het op de hoogte houden van de Cogas op gezette tijden betreffende de voortgang (in het Nederlands). Bij prioriteit 1 en prioriteit 2 minimaal 1x per uur informeren van de Service Manager van Cogas.
- Het oplossen van het incident.
- Door Cogas laten bepalen of de geboden oplossing kwalitatief voldoende is.
- Het afmelden van het incident, inclusief rapportage.

Verder zoekt Leverancier contact met Cogas om de oplossingsrichting te bepalen, de oplossing voor te leggen, in samenspraak met Cogas te testen en op te leveren.

Een incident wordt in overleg met de melder afgesloten bij daadwerkelijk aantoonbaar functieherstel. De afmelding wordt voorzien van rapport, waarin vermeld wordt:

- Oorzaak incident met een root-cause analyse voor prio 1 en prio 2 incidenten.
- Gekozen oplossing van het incident.
- Voorgestelde wijziging/verbetering om herhaling te voorkomen

8.7 Back-up en herstel

De Leverancier maakt dagelijks meerdere, juiste en volledige back-ups van de gegevens en test deze regelmatig (halfjaarlijks) op foutloosheid, bijvoorbeeld door deze te herstellen in een niet-productie omgeving. Back-ups worden separaat van andere klanten, versleuteld opgeslagen op een voor dat doel adequaat beveiligde locatie die zich op een zodanige afstand van de bron bevindt dat geen schade wordt aangericht als zich een calamiteit voordoet op een hoofdlocatie.

Dagelijkse back-up bestanden moeten een week bewaard worden.

Een wekelijks back-up bestand moet minimaal 3 maanden bewaard worden.

Een maandelijks back-up bestand moet minimaal 1 jaar bewaard worden.

De back-up bestanden worden op eerste vordering van Cogas door Leverancier aan Cogas verstrekt, met bijbehorende applicatie ter ontsluiting.

8.8 Update en upgrades

Het is aan Leverancier om zorg te dragen dat de integrale Bedrijfsvoeringsoplossing te allen tijde up to date is en service- en security patches zo bij voorkeur binnen 3 dagen mogelijk geïnstalleerd worden. Regulier onderhoud, waaronder updates met uitzondering van service- en security patches, worden tenminste 1 maand voor uitvoering doorgegeven aan Cogas.

Service- en securitypatches worden zo spoedig mogelijk gemeld aan Cogas.

In overleg met Cogas wordt gepland onderhoud uitgevoerd, bij voorkeur op basis van een onderhoudskalender. Daarnaast wordt Cogas geïnformeerd over aanvang en beëindiging, uitloop en eventuele afgelasting van het onderhoud.

8.9 Rapportage

Leverancier rapporteert, dan wel stelt via een applicatie beschikbaar een maandelijks leesbare rapportage met daarin tenminste opgenomen:

- De overall beschikbaarheid van de integrale Bedrijfsvoeringoplossing 24/7 van de voorgaande kalendermaand.
- De overall beschikbaarheid van de integrale Bedrijfsvoeringsoplossing binnen het afgesproken service window van de voorgaande kalendermaand.
- De beschikbaarheid van de servicedesk.
- De responsetijd van de servicedesk (telefonisch, mail, tooling/portaal).
- Het aantal meldingen:
 - Incidenten;
 - Verzoeken;
 - Changes;
 - Nieuw aangemeld;
 - Afgehandeld;
 - KPI rapportage.
- De responstijd op meldingen.
- De hersteltijd van meldingen.
- De responstijd van de applicatie.
- Tekstuele toelichting op de cijfers.
- Duur van gepland onderhoud versus daadwerkelijk uitgevoerd onderhoud.
- Prognose komende maand (bijvoorbeeld wijzigingen).
- Lessons learned afgelopen maand.
- Financiële rapportage, waaronder licentiebeheer