EMVI / Plan van Aanpak

Uno Automatiseringdiensten B.V. — Raamovereenkomst Catering- en Horecadiensten voor Gemeente Middenstad

Datum: 11/26/2025

EMVI / Plan van Aanpak — Raamovereenkomst Catering- en Horecadiensten voor Gemeente Middenstad (Project 1380) — Uno Automatiseringdiensten B.V.

Samenvatting

- Positie en duiding: Hoewel de titel van de aanbesteding op catering/horeca duidt, blijkt uit de eisen (ISO 27001/9001, ITIL, 24/7, Microsoft 365, EU-data) dat het gaat om een raamovereenkomst voor ICT-beheer- en securitydiensten. Deze EMVI-inschrijving adresseert integraal de gevraagde ICT-diensten onder EMVI-criteria Kwaliteit (40%), Duurzaamheid (20%), Risicobeheersing (20%) en Prijs (20%).
- KO-conformiteit: Uno Automatiseringdiensten B.V. voldoet aan alle knock-outs: ISO 27001 gecertificeerd; ISO 9001 gecertificeerd; 24/7 bereikbaarheidsdienst operationeel.
- SMART-doelstellingen (kern):
  - Beschikbaarheid kritieke systemen: ≥ 99,8% per kalendermaand (KPI-01).
  - Responstijd P1: < 30 minuten, 24/7 (KPI-02).
  - Oplostijd P1: < 4 uur, 24/7 (KPI-03).
  - Patch-compliance: 100% kritieke patches servers ≤ 14 dagen; endpoints ≤ 21 dagen (KPI-04).
  - Back-up succesratio: ≥ 99,5% dagelijks (KPI-05).
  - CSAT: ≥ 8,2/10 met ≥ 25% response (KPI-07).
  - EU-dataverwerking: 100% binnen EU (KPI-09).
- PDCA-cyclus: Maandelijks KPI-rapport (Check), kwartaal-CSI-sessies (Act), jaarplan met verbeterinitiatieven (Plan), iteratieve implementatie (Do). Governance: maandelijks operationeel overleg, kwartaal stuurgroep met opdrachtgever.
- Duurzaamheid: 100% EU-datacenters met groene stroom, reductie energieverbruik endpoint door policies (–10% idle power in 12 maanden), levensduurverlenging hardware met 12 maanden gemiddeld via OS-optimalisatie en monitoring. Jaarlijks CO2-dashboard per dienst.
- Risico’s: Uitval bij ketenafhankelijkheden, onvolledige inventarisatie, security-incidenten, shadow IT en wetgeving (NIS2). Beheersing: Zero Trust, EDR, discovery-scans, heldere scope- en changecontrole, jaarlijkse BCP-test.
- Waarde: Bewezen 24/7 operatie in onderwijs- en overheidsomgevingen, ISO-gecertificeerde processen, security-first, meetbare resultaten, lage verstoringsgraad en voorspelbare oplevering.

Begrip van de opdracht

- Doel: Continu en veilig beheer, onderhoud en beveiliging van de ICT-omgeving van Gemeente Middenstad onder een raamovereenkomst, met focus op hoge beschikbaarheid, snelle respons, proactieve monitoring, EU-data, ITIL-gestuurd service management en ondersteuning van Microsoft 365.
- Omvang:
  - Servicedesk (ITIL) en 24/7 P1/P2-storingsdienst.
  - Proactieve monitoring netwerk, servers, endpoints en M365-tenant; patchmanagement; vulnerability management; back-up & restore.
  - Security: EDR, hardening, logging, incident response, identity & access governance.
  - Changes: gestandaardiseerde CAB, no-regret changes buiten kantoortijd waar nodig.
  - Rapportage & governance: maandrapporten, real-time dashboard, kwartaalreview met verbeterprogramma.
- Raamovereenkomst-exploitatie:
  - Call-offs conform werkpakketten (beheer, projecten, changes).
  - Duidelijke scheiding tussen vast beheer (SLA) en projectmatig werk (afroep), conform uitsluitingen extra projecten buiten beheer.
- Randvoorwaarden: Alle data binnen EU, VOG voor personeel indien vereist, continuïteitsplan (BCP), escalatieprocedure, licenties rechtmatig en internetverbindingen voldoen aan minimumeisen.

Aanpak (Plan-Do-Check-Act) Plan – Onboarding en transitie (0–12 weken)

- Week 1–2: Kick-off, afstemming SLA/KPI, aanstelling regieteam, techniek- en security-due-diligence; toegang inregelen; assessment op EU-datalocatie; inventarisatie en CMDB-bouw.
- Week 2–4: Monitoring livezetten (Azure Monitor, Microsoft Defender for Endpoint, Intune); back-upstrategie borgen (M365 en on-prem waar van toepassing); baseline security hardening (CIS/L1-profiles).
- Week 3–6: Patchmanagement inrichten (Intune/WSUS); changeproces (CAB, RACI); incidentclassificatie P1–P4; communicatie- en escalatierichtlijnen publiceren.
- Week 4–8: Proefrestore en BCP-tabeltest (RTO/RPO validatie); EDR 100% coverage endpoints en servers; SSO/Conditional Access voor beheerders.
- Week 6–10: Kennisoverdracht en runbooks; rapportage- en dashboarding (Power BI) per KPI; eerste maandrapport en verbetervoorstellen.
- Week 10–12: Exit-readiness check (dataportabiliteit), security awareness kick-off voor key users, ondertekening operationele DAP’s per systeem.

Do – Operationeel beheer

- Servicedesk: ITIL-v4, KPI-sturing; prioritering met duidelijke P1-criteria (dienstonderbreking > 20% of cruciale ketencomponent).
- Incidentrespons:
  - P1: triage binnen 15 min, remote interventie binnen 30 min, resolver group geactiveerd, war room 24/7; resolutie < 4 uur of workaround < 2 uur + root cause binnen 2 werkdagen.
  - P2: respons < 1 uur; resolutie < 8 uur.
- Changes: CAB wekelijks; standaard changes via templates; noodchanges met post-implementation review binnen 2 werkdagen.
- Patch- en vulnerability management:
  - Kritieke patches: servers ≤ 14 dagen; endpoints ≤ 21 dagen; uitzonderingen alleen via CAB.
  - Maandelijkse vulnerability-scan; risicoscoretrend gerapporteerd; 0 bekende kritieke CVE’s > 30 dagen (KPI-04).
- Monitoring & back-up:
  - 24/7 monitoring; alerting op beschikbaarheid, performance, security events; back-up succesratio ≥ 99,5% (KPI-05); proefrestore per kwartaal.
- Microsoft 365:
  - Tenant-beveiliging (MFA, Conditional Access), dataclassificatie labels, DLP-policies, secure score > 75% binnen 6 maanden.
- Documentatie & CMDB:
  - CMDB actueel (≤ 5 werkdagen na wijziging); audittrail changes en incidenten.

Check – Meten en rapporteren

- Maandelijks: KPI-rapport vóór werkdag 5; security-rapportage (events, trends); patch- en kwetsbaarhedenstatus; CSAT; lessons learned.
- Kwartaal: Stuurgroep; SLA-evaluatie; risico-review; compliance-check EU-data; roadmap-update.
- Audit: Interne ISO 9001/27001 audits halfjaarlijks; externe audits jaarlijks.

Act – Continu verbeteren

- CSI-backlog met prioriteit en businesscase; minimaal 3 verbeteracties per kwartaal doorvoeren.
- Root cause elimination: voor elke P1 een probleemrecord met structurele maatregel binnen 10 werkdagen.
- Roadmap: per halfjaar aanpassen op basis van KPI’s, wetgeving (NIS2), dreigingslandschap.

Eenvoudige Gantt (Onboarding 12 weken)

Fase	Wk1	Wk2	Wk3	Wk4	Wk5	Wk6	Wk7	Wk8	Wk9	Wk10	Wk11	Wk12
Kick-off & due-diligence	X	X										
Infrastructuur inventarisatie	X	X	X	X								
Monitoring & back-up		X	X	X	X							
Patch/EDR uitrol			X	X	X	X	X					
ITIL/CAB processen				X	X	X	X	X				
BCP test & proefrestore						X	X	X				
Rapportage & dashboard					X	X	X	X	X	X		
Exit-readiness check										X	X	X

Borging van kwaliteit, security en continuïteit

- Certificeringen: ISO 9001 (kwaliteitsmanagement) en ISO 27001 (informatiebeveiliging); procesmatige borging van alle W-xx via ISMS/QMS.
- ITIL-v4 processen: Incident, Request, Problem, Change, Knowledge; CAB; servicecatalogus en SLA-matrix.
- Continuïteit:
  - BCP met jaarlijkse test; RTO kritieke diensten ≤ 4 uur; RPO M365-data ≤ 1 uur via policy-gebaseerde recovery en geo-redundantie waar beschikbaar.
  - Personele continuïteit: 24/7-rooster, minimaal 3 opgeleide engineers per kerntechnologie; vervangingspool.
- Security-by-design:
  - Zero Trust-principes; least privilege; Just-in-Time admin; EDR op 100% endpoints/servers; phishing-simulaties 2x per jaar.
- Data-soevereiniteit: 100% EU-dataverwerking, contractueel en technisch geborgd; leveranciersbeoordeling en DPIA-ondersteuning.

Duurzaamheid (20%)

- Energie en cloud-efficiëntie:
  - Rightsizing en autoscaling waar van toepassing; doel: –15% compute idle time binnen 9 maanden.
  - Endpoint power policies: –10% idle power binnen 12 maanden.
- Levensduurverlenging:
  - Performance-tuning en monitoring verhogen bruikbare levensduur endpoints/servers gemiddeld met 12 maanden; rapportage per kwartaal.
- Circulariteit:

    - E-waste-proces met gecertificeerde verwerkers; 100% datadragervernietiging met certificaat; hergebruik prioriteren bij vervanging.
- Mobiliteit:
    - Remote-first support; > 85% incidenten remote oplosbaar; doel: –20% autokilometers in jaar 1 vs. baseline.
- Transparantie:
    - Jaarlijks CO2-dashboard per dienst en reductieplan; leveranciersscorekaart op duurzaamheid.

Risico’s en beheersing (selectie)

Risico (R-xx)	Kans	Impact	Beheersmaatregel (SMART)	W-xx	KPI-link	Bewijs	Eigenaar
R-01 Onvolledige inventarisatie	M	H	Discovery-scan en CMDB compleet ≤ 20 werkdagen; validatie door CAB	W-06	KPI-10, KPI-08	CMDB-export; CAB-notulen	Service Manager
R-02 Security-incident	M	H	EDR 100% coverage ≤ 8 weken; MTTR P1 < 4 uur; RCA binnen 10 werkdagen	W-06	KPI-02, KPI-03	EDR-rapport; RCA-document	Security Lead
R-03 EU-data non-compliance bij leverancier	L	H	Leverancierscheck 100%; contract EU-only; kwartaal-audit	W-09	KPI-09	Vendor-assessments; auditlog	Compliance Officer
R-04 Patchachterstand kritieke systemen	M	H	Servers ≤ 14 dagen; endpoints ≤ 21 dagen; afwijking alleen via CAB	W-07	KPI-04	Patch-rapport; CAB-besluiten	Patch Manager
R-05 Shadow IT	M	M	Maandelijkse software-inventaris; blokkade ongeautoriseerde apps binnen 5 werkdagen	W-06	KPI-12, KPI-04	Intune-compliance; rapport	Endpoint Lead
R-06 Scope creep	M	M	RfC-proces; duidelijke servicecatalogus; stuurgroepbesluit bij grensgevallen	W-08	KPI-10, KPI-08	RfC-logs; stuurgroepnotulen	Service Manager
R-07 Personele uitval	L	H	24/7-rooster; 3-voudige kennisdekking; onboarding vervanging ≤ 10 werkdagen	W-03	KPI-02, KPI-03	Roosters; skills-matrix	Operations Lead
R-08 Wet- en regelgeving	M	M	Kwartaal compliance-review;	W-16	KPI-10	Reviewdocument; roadmap	Compliance Officer

Risico (R-xx)	Kans	Impact	Beheersmaatregel (SMART)	W-xx	KPI-link	Bewijs	Eigenaar
(NIS2)			maatregelen opgenomen in CSI-roadmap				
R-09 Dataverlies bij restore	L	H	Kwartaal-proefrestore; RPO ≤ 1 uur M365; herstelprocedures getest	W-11	KPI-05	Proefrestore-rapporten	Backup Lead

Organisatie, rollen en governance

- Leverancier: Uno Automatiseringdiensten B.V., KVK 27172538, BTW NL8070.79.266.B01, Einsteinlaan 14, 2719 ER Zoetermeer. Contact: Eric van de Vreugdenhil, +31 703300502.
- Key-rollen:
  - Service Manager (SPOC, KPI's, rapportage).
  - Security Lead (ISMS, incident response, EDR).
  - Operations Lead (24/7 operatie, roosters).
  - Patch Manager (patch/vulnerability).
  - Backup Lead (back-up & herstel).
  - Compliance Officer (ISO, EU-data, audits).
- 24/7-structuur:
  - Piketdienst met escalatie 1e/2e/3e lijn; maximum wachttijd 15 min tot engineer.
  - Escalatie naar management binnen 60 min bij P1.
- Overlegstructuur:
  - Operationeel overleg: maandelijks (60 min), acties ≤ 10 werkdagen.
  - Stuurgroep: per kwartaal (90 min), besluitvorming met notulen binnen 5 werkdagen.
- Kennisborging:
  - Runbooks; KEDB; kennisartikelen; opleidingsplan per rol (min. 2 trainingen p.j.).

Programma van Wensen (W-xx) met KPI- en risicokoppeling

W-xx	Omschrijving	Acceptatiecriterium (SMART)	KPI-koppeling	Risico-koppeling	Bewijs
W-01	KO: ISO 27001 gecertificeerd	Geldig ISO 27001-certificaat; scope omvat beheerdiensten	KPI-10	R-08	ISO 27001-certificaat; auditrapport
W-02	KO: ISO 9001 gecertificeerd	Geldig ISO 9001-certificaat; jaarlijkse audit	KPI-10	R-06	ISO 9001-certificaat; auditrapport
W-03	KO: 24/7 bereikbaarheidsdienst	Piket 24/7; max aanneemtijd 30 min; escalatie ≤ 60 min	KPI-02, KPI-03	R-07	Roosters; test-logs
W-04	Responstijd P1 < 30 min	95e percentiel < 30 min; 100% P1's gelogd met stempel	KPI-02	R-02, R-05	Ticketlog; maandrapport

W-xx	Omschrijving	Acceptatiecriterium (SMART)	KPI-koppeling	Risico-koppeling	Bewijs
W-05	Beschikbaarheid 99,8%	≥ 99,8%/maand; berekening excl. gepland onderhoud	KPI-01	R-05	Uptime-rapport; monitoring-logs
W-06	Proactieve monitoring netwerk & endpoints	100% endpoints/servers in monitoring; alerting 24/7	KPI-01, KPI-12	R-01, R-02, R-05	Monitoring-inventaris; alert-rapportage
W-07	Monitoring & patchmanagement volledig geborgd	Kritieke patches servers ≤ 14 d; endpoints ≤ 21 d; rapportage maandelijks	KPI-04	R-04	Patchcompliance-rapport; CAB-notulen
W-08	ITIL-gebaseerde servicedeskprocessen	Incident/Change/Problem actief; CAB wekelijks; CSAT ≥ 8,2	KPI-07, KPI-08	R-06	Processdocs; CAB-notulen; CSAT-rapport
W-09	Alle data wordt binnen de EU verwerkt	100% dataverwerking EU; kwartaalcontrole	KPI-09	R-03	Leveranciersbeoordelingen; DPIA-notities
W-10	Escalatieprocedure voor incidenten & changes	Gedocumenteerd; getest 2x/jaar	KPI-10	R-05, R-07	Escalatieplan; testrapporten
W-11	Continuïteitsplan (BCP) beschikbaar	BCP gepubliceerd ≤ week 6; jaarlijkse test; RTO ≤ 4 uur	KPI-05, KPI-10	R-09	BCP; testverslag; proefrestore-rapport
W-12	Personeel beschikt over VOG indien vereist	VOG op dossier voor alle ingeplande medewerkers ≤ 10 werkdagen na start	KPI-10	R-07	VOG-registratie
W-13	Ondersteuning Microsoft 365 omgeving	Secure Score > 75% in 6 mnd; DLP/MFA/CA actief binnen 8 weken	KPI-10, KPI-06	R-02	Secure Score-rapport; policy-overzicht
W-14	Realtime SLA/KPI-dashboard	Live dashboard dag 30; maandrapport dag 5	KPI-10	R-06	Dashboard-screens; rapportarchief
W-15	Security awareness en phishingtests	2x per jaar; clickrate < 8% in 12 mnd	KPI-06	R-02	Testverslagen; deelname-overzicht
W-16	Continu verbeterprogramma (CSI)	Min. 3 verbeteracties per kwartaal; effect gemeten binnen 90 dagen	KPI-08, KPI-10	R-06, R-08	CSI-backlog; effectmeting
W-17	Dataclassificatie en DLP in M365	Labels en DLP actief binnen 12 weken; 0 kritieke exfiltraties ≥ 30 dagen	KPI-06, KPI-09	R-02, R-03	DLP-policy; incidentrapportage

W-xx	Omschrijving	Acceptatiecriterium (SMART)	KPI-koppeling	Risico-koppeling	Bewijs
W-18	Privacy by design (DPIA-ondersteuning)	DPIA-adviestraject ≤ 20 werkdagen per nieuw dataproces	KPI-10, KPI-09	R-03	DPIA-templates; adviesrapporten
W-19	NIS2-ready beheerprocessen	Kwartaal gap-assessment; top 5 maatregelen doorgevoerd binnen 90 dagen	KPI-10	R-08	Gap-rapport; actie-overzicht
W-20	Exit- en dataportabiliteit	Exit-draaiboek dag 60; volledige data-overdracht ≤ 10 werkdagen op verzoek	KPI-10, KPI-09	R-06	Exitplan; overdrachtrapport

KPI/SLA-samenvatting

KPI-ID	KPI-naam	Definitie/Meetmethode	Target	Frequentie	Correctieve maatregel (Act)
KPI-01	Beschikbaarheid kritieke systemen	Uptime monitoring excl. gepland onderhoud	≥ 99,8%/maand	Maandelijks	Root cause + maatregel binnen 10 wd; verbeteractie
KPI-02	Responstijd P1	Tijdsduur melding tot start triage	< 30 min (95p), 24/7	Maandelijks	Escalatie en capaciteitbijsturing
KPI-03	Oplostijd P1	Tijdsduur melding tot herstel	< 4 uur (90p), 24/7	Maandelijks	RCA verplicht; extra piketcapaciteit
KPI-04	Patch-compliance	% systemen met kritieke patches binnen termijn	Servers ≤ 14d; Endpoints ≤ 21d	Maandelijks	CAB-interventie; change window uitbreiding
KPI-05	Back-up succesratio	% geslaagde jobs per dag	≥ 99,5%	Maandelijks	Proefrestore; tuning backup-venster
KPI-06	Security-event beheersing	Detectie/containment high/critical via EDR/Defender	Containment ≤ 15 min	Maandelijks	Regelupdate; use case-tuning
KPI-07	Klanttevredenheid (CSAT)	Score na ticketafsluiting	≥ 8,2/10; ≥ 25% response	Maandelijks	Verbeterworkshops; knowledge-update
KPI-08	Change-succesratio	% changes zonder terugval/rollback	> 98%	Maandelijks	PIR; standaardisatie template
KPI-09	EU-dataresidentie	% dataverwerking binnen EU	100%	Kwartaal	Leveranciersreset; migratie naar EU
KPI-10	Rapportage & governance	Tijdigheid maandrapport en stuurgroep	100% (dag 5; per kwartaal)	Maand/Kw	Escalatie naar directie;

KPI-ID	KPI-naam	Definitie/Meetmethode	Target	Frequentie	Correctieve maatregel (Act)
					procesaanpassing
KPI-11	BCP-test en RTO/RPO	Jaarlijkse test; RTO/RPO conforme norm	1x/jaar; RTO ≤ 4h; RPO ≤ 1h	Jaarlijks	Herzien BCP; extra redundantie
KPI-12	Endpoint security coverage	% endpoints/servers met EDR en compliance	100% coverage	Maandelijks	Remediatie binnen 5 wd; blokkade niet-conform

Borging PDCA per KPI

- Plan: SLA's/KPI's contractueel vastleggen en procesontwerpen in ISMS/QMS.
- Do: Operationele uitvoering en tooling (Intune/Defender/Azure Monitor).
- Check: Meet, rapporteer en review in overlegstructuur.
- Act: PIR/RCA/CSI-acties met deadlines en eigenaarschap.

Compliance en bewijsvoering

- ISO 27001/9001 certificaten en auditrapporten.
- CMDB-export, monitoring- en patchrapporten, back-uplogs, proefrestoreverslagen.
- CAB-notulen, escalatietests, BCP-testverslagen.
- EU-data onderbouwing: leveranciersbeoordelingen, DPIA-notities.
- Security-rapportages, Secure Score-rapporten.

Assumpties (transparant)

- Opdrachtgever levert tijdig benodigde toegangen en informatie aan.
- Locaties toegankelijk binnen kantoortijden; internet/netwerk voldoen aan minimumeisen.
- Besluitvorming door opdrachtgever binnen afgesproken termijnen.
- Licenties voor Microsoft 365 en overige pakketten zijn rechtmatig verkregen.

Uitsluitingen

- Levering en beheer van onsite hardware buiten scope tenzij expliciet overeengekomen.
- Third-party SaaS/applicatiesupport buiten directe verantwoordelijkheid.
- Projecten buiten regulier beheer niet onder vast maandtarief.
- Onvoorziene meerwerkzaamheden apart geoffreerd.
- Adoptie- en trainingsprogramma's voor eindgebruikers uitsluitend op verzoek.

Governance en rapportage

- Maandrapport (dag 5): SLA/KPI, incidenten, changes, vulnerabilities, patchstatus, CSAT, verbeteracties.
- Kwartaal stuurgroep: voortgang, risico's, compliance (EU-data, ISO), roadmap, duurzaamheid.
- Dashboards: realtime status KPI-01 t/m KPI-12 met drill-down.

Toegevoegde waarde richting EMVI-criteria

- Kwaliteit (40%): Hoge beschikbaarheid, bewezen ITIL-procesvolwassenheid, 24/7-respons, uitgebreide automatisering en meetbaarheid.
- Duurzaamheid (20%): Concreet CO2- en energiereductieplan met meetbare doelen, e-waste governance, remote-first.
- Risicobeheersing (20%): Volledig risicoregister met maatregelen, Zero Trust, BCP, exit-readiness.

- Prijs (20%): PDCA-gestuurde efficiëntie verlaagt TCO (minder incidenten, minder kilometers, langere levensduur hardware).

Conclusie Uno Automatiseringdiensten B.V. levert een volledig ISO-geborgd, security-first en PDCA-gestuurd beheerplatform met 24/7-beschikbaarheid, aantoonbare EU-dataresidentie en hoge servicekwaliteit. Met SMART KPI's, strakke governance, duurzaamheid met meetbare reducties en een uitgewerkt risicodossier borgen wij continuïteit en betrouwbaarheid voor Gemeente Middenstad. Wij voldoen aan alle KO-eisen en overtreffen de must-haves met extra waarde (awareness, NIS2-readiness, exit-plan, realtime dashboards). Deze EMVI biedt voorspelbare resultaten, maximale transparantie en aantoonbare verbeterkracht gedurende de looptijd van de raamovereenkomst.

Conclusie / Meerwaarde

Onze aanpak borgt meetbare prestaties via PDCA, een sluitende KPI/SLA-set en aantoonbare risicoreductie. We koppelen ieder W-xx aan KPI's en beheersmaatregelen, leveren bewijslast per bijlage en rapporteren transparant op frequenties die aansluiten bij de opdrachtgever. Daarmee maximaliseren we BPKV-scores, reduceren faalkosten en versnellen oplevering.

Benodigde input: