EMVI / Plan van Aanpak

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

Datum: 11/5/2025

EMVI / Plan van Aanpak — Raamovereenkomst Cloud- en Infrastructuurbeheer voor Opdrachtgever (NVAO/Gemeente Middenstad)

1. Samenvatting Wij, Uno Automatiseringdiensten B.V. (KVK 27172538, ISO 9001 en ISO 27001 gecertificeerd), bieden een PDCA-gestuurde, 24/7 beheerdienst voor cloud- en infrastructuuroplossingen in Microsoft Azure (West Europe, Nederland). We garanderen minimaal 99,8% beschikbaarheid (maandelijks), responstijd ≤ 1 uur en oplostijd ≤ 4 uur voor kritieke incidenten. We leveren 24/7 monitoring, 2 geplande onderhoudsmomenten per jaar (wij leveren 4x per jaar patching/onderhoud om risico's verder te reduceren), en periodieke beveiligingsrapportages (maandelijks, en binnen 24 uur bij incidenten). We borgen informatiebeveiliging conform ISO 27001, met VOG voor medewerkers met toegang. Duurzaamheid realiseren we via Azure-efficiency (auto-scaling, right-sizing), reductie van compute-waste, en kwartaalrapportage over CO2-footprint in de cloud.

Onze aanpak is SMART: we definiëren KPI's met meetmethode, frequentie en normen; we rapporteren maandelijks; we voeren kwartaal-verbetersprints door via CAB/steering committee. We koppelen elk Programma van Wensen (W-xx) aan KPI's, risico's (R-xx) en bewijsstukken, zodat u aantoonbare grip heeft op kwaliteit, security, continuïteit en duurzaamheid.

2. Begrip van de opdracht en scope-afbakening

- Doel: Continu, veilig en duurzaam beheer, onderhoud en beveiliging van Azure-gebaseerde infrastructuur en cloud-diensten voor de opdrachtgever, met hoge beschikbaarheid en aantoonbare compliance (ISO 27001).
- Scope:
  - Proactief en reactief beheer (24/7).
  - Incident-, probleem-, change- en release-management (ITIL v4-principes).
  - Monitoring, back-up/restore, patching, capacity management.
  - Security operations (logverzameling, SIEM/Sentinel, vulnerability management, rapportages).
  - Rapportage en governance (SLA/KPI, risico's, verbeterinitiatieven).
  - Gebruik van Azure West Europe (NL) met Availability Zones; datalokalisatie NL.
- In scope deliverables: Plan van Aanpak (dit document), Risicodossier (R-xx), KPI-overzicht met SLA.
- Niet in scope (behoudens separate opdracht): Applicatieontwikkeling; hardwareleveringen buiten Annex IX; functionele applicatiebeheeractiviteiten.
- Knock-outs: ISO 27001 geldig; VOG voor betrokken personeel — wij voldoen hieraan; bewijs op verzoek beschikbaar.

3. Aanpak (PDCA) 3.1 Plan – Transitie en Nulmeting (T0–T+90 dagen)

- T0–T+10 dagen: Kick-off, overdracht contactpersonen, vaststelling ketenkaart en crisisnummers.
- T+10–T+30 dagen: Nulmeting (assets, workloads, netwerk, IAM, back-ups), security-baseline (CIS/Microsoft benchmark), risicoanalyse R-xx en CMDB-vulling.
- T+30–T+60 dagen: Implementatie monitoring (Azure Monitor, Log Analytics), SIEM-koppeling (Microsoft Sentinel), patchkalender, back-upbeleid (Azure Backup), runbooks.
- T+60–T+90 dagen: Proefdraaien (war room), failover-test, acceptatie, Go-Live.
- Output: Baseline-rapport (configuratie, kwetsbaarheden, capaciteit, CO2-verbruik), Risicodossier v1, KPI-dashboard v1.

3.2 Do – Beheer en Operatie (continu)

- 24/7 NOC/SOC: Bewaking met detectie van P1 binnen 5 minuten (KPI K-02), automatische alerts en runbooks.
- Incidentmanagement: Prioritering P1–P4, responstijd P1 ≤ 1 uur, oplostijd P1 ≤ 4 uur of workaround ≤ 2 uur, root cause analyse binnen 3 werkdagen.
- Probleembeheer: Trendanalyse maandelijks, structurele oplossingen in CAB, probleemsluiting met verificatie.
- Change- & releasemanagement: CAB maandelijks; standaard changes binnen 2 werkdagen; normale changes binnen 5 werkdagen; spoedchange binnen 2 uur besluitvorming.
- Patching & onderhoud: 4 onderhoudsvensters per jaar (buiten kantooruren), vooraf 14 dagen communicatie en impactanalyse. Minimaal 2 per jaar is must; wij leveren 4, waarmee risico's op kwetsbaarheden afnemen (R-03).
- Capaciteits- en kostenoptimalisatie: Maandelijks right-sizing, auto-scaling waar mogelijk, reservecapaciteit voor kritische ketens.
- Back-up & herstel: Dagelijkse back-ups van kritische systemen; retentie 30/180 dagen (operational/archief). Hersteltest per kwartaal; RTO P1 ≤ 4 uur; RPO P1 ≤ 15 minuten waar gebruik van Azure services dat ondersteunt (bijv. geo/zone-redundant storage en SQL PITR).
- Security Operations:
    - Kwetsbaarheidsscan maandelijks; patch binnen 14 dagen bij high/critical CVE.
    - MFA, Conditional Access en Just-In-Time admin-roles standaard.
    - Sentinel use cases (privilege escalation, data exfiltration, brute force, anomalous logins) met playbooks.
    - Beveiligingsincidenten: meldplicht binnen 24 uur (W-07) en eindrapport binnen 5 werkdagen.

3.3 Check – Rapportage en Audits

- Maandelijks SLA/KPI-rapport: beschikbaarheid, incidenten, oplostijden, changes, beveiligingsmeldingen, CO2-metrics.
- Kwartaalreview (QBR): PDCA-verbeterplan, roadmap, kostenoptimalisaties, security posture score, auditbevindingen.
- Jaarlijkse audit readiness: ISO 27001 controle op relevante controls, testrapport DR/BCP, lessons learned.

3.4 Act – Continu Verbeteren

- Kwartaal-verbetersprint met maximaal 5 verbeteracties (SMART) per kwartaal, inclusief eigenaar, target en beoogde risicoreductie.
- Post-incident reviews (≥ P1, binnen 10 werkdagen): structurele maatregelen, update risico/draaiboeken.
- Jaarlijkse strategische update: afstemming op Azure-roadmap, lifecycle (EoL/EoS), en duurzaamheid.

4. Borging (kwaliteit, veiligheid, continuïteit)

- Kwaliteit: ISO 9001-gestuurde processen, RACI-matrix, CMDB, gestructureerde overdracht en documentatie.
- Informatiebeveiliging: ISO 27001 ISMS; toegang op need-to-know; VOG-vereiste voorafgaand aan toegang; logretentie 180 dagen operationeel, 365 dagen forensisch.
- Continuïteit: Redundantie via Azure Availability Zones; DR runbooks; jaarlijkse failover-test (KPI K-09 100% testdekking).
- Datalokalisatie: Data geborgd in Azure West Europe (Nederland); geen replicatie buiten NL zonder schriftelijke toestemming.

- Privacy: DPIA-ondersteuning op verzoek; verwerkersovereenkomst conform AVG; dataclassificatie en lifecyclebeleid.
- Crisismanagement: 24/7 bereikbaarheidsregeling; escalatie in 3 niveaus; communicatie-sjablonen en stakeholdermapping.

5. Duurzaamheid (20% gunningscriterium)

- Cloud-efficiency:
  - Right-sizing en auto-scaling: maandelijkse besparingsscan; doel ≥ 15% compute-waste reductie in jaar 1 (KPI K-12).
  - Stoppolicy non-productie buiten kantooruren; target ≥ 70% van non-prod workloads auto-shutdown binnen 6 maanden.
- Azure-duurzaamheid: Gebruik energie-efficiënte datacenters in NL; Microsoft's commitment aan 100% hernieuwbare energie-inkoop richting 2025 en CO2-negatief in 2030; wij rapporteren kwartaal CO2-equivalent verbruik op basis van Azure-rapportages en gebruiksprofielen.
- Dataverkeer en opslag:
  - Lifecycle policies: cold storage waar passend; reductie hot storage ≥ 10% in jaar 1 zonder performanceverlies.
  - Compressie en caching waar veilig; traffic-optimalisatie om netwerkenergie te verlagen.
- Circulariteit en mobiliteit:
  - Remote-first samenwerking; doel 90% remote interventies.
  - Duurzame vervanging hardware alleen wanneer strikt noodzakelijk (exclusie hardwareleveringen behoudens Annex IX).
- Maatschappelijke waarde:
  - 1 BBL/BBI-plek per jaar op de servicedesk.
  - 2 kennisdelingssessies per jaar voor opdrachtgever (cloud security en kostenoptimalisatie).
- Borging:
  - Kwartaal CO2-rapportage (KPI K-13), maatregelen en realisatie.
  - Opname duurzaamheidsacties in CAB en QBR.

6. Risico's en mitigerende maatregelen Toprisico's (selectie, volledige lijst in Risicodossier R-xx):

- R-01 Onvoldoende zicht op legacy-configuraties → Maatregel: Nulmeting + CMDB binnen 30 dagen (W-01, K-01/K-05). Rest-risico: Medium.
- R-02 Late detectie van P1-storingen → Maatregel: 24/7 monitoring, detectie ≤ 5 min (W-03, K-02). Rest-risico: Low.
- R-03 Security-kwetsbaarheden door achterstallige patches → Maatregel: 4x/jaar onderhoud + high/critical patch < 14 dagen (W-05, K-06). Rest-risico: Low.
- R-04 Datalek of ongeautoriseerde toegang → Maatregel: MFA, CA, JIT, Sentinel use-cases; meldplicht 24 uur (W-07, K-07/K-08). Rest-risico: Low/Medium.
- R-05 Onvoldoende beschikbaarheid < 99,8% → Maatregel: AZ, health checks, runbooks; root cause analyse (W-02, K-01/K-03). Rest-risico: Low.
- R-06 Onvoldoende herstel na incident → Maatregel: Back-up/draaitest, RTO ≤ 4 uur, RPO ≤ 15 min op kritieke diensten (W-08, K-09). Rest-risico: Low.
- R-07 Kostenoverschrijding cloud → Maatregel: FinOps-rapportage en right-sizing (W-11, K-12/K-13). Rest-risico: Medium.
- R-08 Niet-conforme medewerkers (geen VOG) → Maatregel: VOG-check voor toegang; HR-controle (W-14, K-11). Rest-risico: Low.
- R-09 Change veroorzaakt verstoring → Maatregel: CAB, change-vensters, back-out plan (W-05, K-10). Rest-risico: Low.

- R-10 Dataverkeer buiten NL → Maatregel: Datalokalisatiebeleid en policy enforcement (W-06, K-05). Rest-risico: Low.

Risicomatrix (samenvatting) | Risico | Kans | Impact | Initieel | Maatregel | Rest | | R-01 | Medium | Medium | Hoog | CMDB+Nulmeting 30d | Medium | | R-02 | Medium | Hoog | Hoog | 24/7 monitor, detect ≤5m | Low | | R-03 | Medium | Hoog | Hoog | 4x patch, ≤14d CVE | Low | | R-04 | Low | Hoog | Medium | MFA/CA/JIT, Sentinel | Low/Med | | R-05 | Low | Hoog | Medium | AZ, runbooks, RCA | Low | | R-06 | Low | Hoog | Medium | DR-test, RTO/RPO | Low | | R-07 | Medium | Medium | Medium | FinOps/Right-sizing | Medium | | R-08 | Low | Medium | Low | VOG-check | Low | | R-09 | Medium | Medium | Medium | CAB/back-out | Low | | R-10 | Low | Hoog | Medium | NL-only policy | Low |

7. Organisatie en governance

- Team:
  - Service Manager (eindverantwoordelijke SLA en QBR).
  - Lead Architect Azure (design, security baseline).
  - NOC/SOC Engineers 24/7 (incident/monitoring).
  - Change Coordinator (CAB, releases).
  - Security Officer (ISMS, incidentcoördinatie AVG).
- Bereikbaarheid: 24/7 via servicedeskportaal en noodnummer P1.
- Escalatie:
  - Niveau 1: Service Manager (reactie ≤ 1 uur P1).
  - Niveau 2: Technisch Directeur (binnen 2 uur).
  - Niveau 3: Directie (binnen 4 uur).
- Overleggen:
  - Wekelijks operationeel (tickets, changes).
  - Maandelijks CAB en SLA-rapport.
  - Per kwartaal Steerco/QBR.
- Documentatie:
  - CMDB en kennisbank actueel binnen 5 werkdagen na wijziging.
  - Post-incident rapportage P1: binnen 5 werkdagen.

8. Programma van Wensen – Invulling en Kruiskoppelingen | W-xx | Wens opdrachtgever | Onze invulling (SMART) | KPI-koppeling | Risico-koppeling | Bewijs | | W-01 | SLA-responstijd < 1 uur | P1/P2 respons ≤ 1u/2u 24/7; P3 ≤ 1 werkdag; meet via ticketing (tijdstempel) | K-03, K-04 | R-02 | Maandrapport tickets, systeemtimestamps | | W-02 | ≥ 99,8% beschikbaarheid | Maandelijkse beschikbaarheid ≥ 99,8%; doelstelling 99,85% voor kernsystemen; AZ inzet; RCA binnen 3 werkdagen bij breach | K-01 | R-05 | Uptime-rapport Azure Monitor, RCA-rapporten | | W-03 | 24/7 monitoring/support | NOC/SOC 24/7; detectie P1 ≤ 5 min; alerting via Sentinel/Monitor | K-02 | R-02 | Alertlogboeken, on-call rooster | | W-04 | Oplostijd ≤ 4 uur P1 | P1 opgelost ≤ 4u of workaround ≤ 2u; escalatie binnen 30 min | K-04 | R-06 | Ticketdata, escalatielog | | W-05 | Min. 2 onderhoud p/jaar | 4 onderhoudsvensters/jaar; communicatie ≥ 14 dagen; change-succesratio ≥ 98% | K-10 | R-03, R-09 | Changekalender, succesratio-rapport | | W-06 | Azure NL datacenters | Datalokalisatie: Azure West Europe (NL) AZ; policy die egress naar non-NL blokkeert | K-05 | R-10 | Azure Policy compliance, region settings | | W-07 | Periodieke security rapportage | Maandelijks SIEM-rapport; incidentmelding binnen 24u; high/critical patch ≤ 14 dagen | K-06, K-07, K-08 | R-03, R-04 | SIEM-rapporten, patch-compliance | | W-08 | Continuïteit getest | Jaarlijkse DR-test 100% scope; RTO ≤ 4u P1; RPO ≤ 15m voor kritieke services | K-09 | R-06 | Testrapporten, testplannen | | W-09 | AVG en privacy | DPIA-ondersteuning; logging 365d forensisch; toegangsreviews per kwartaal | K-08 | R-04 | Toegangsreviewverslagen, DPIA-notulen | | W-10 | Snelle onboarding | Onboarding binnen 30 dagen tot productierijp; trainingssessie 2 uur | K-05 | R-01 |

Onboardingchecklist, opleverdocument | | W-11 | Duurzaam gebruik cloud | Kwartaal CO2-rapport; ≥ 15% compute-waste reductie in jaar 1; ≥ 70% non-prod auto-shutdown | K-12, K-13 | R-07 | CO2-rapport, FinOps-rapport | | W-12 | Kennisoverdracht | 2 kennissessies/jaar; 1 runbook per kritieke keten; acceptatie door opdrachtgever | K-05 | R-01, R-05 | Presentielijsten, runbooks | | W-13 | Exit & reversibility | Exitplan binnen 60 dagen; data-export binnen 5 werkdagen op verzoek | K-05 | R-05 | Exitplan document, exportlogs | | W-14 | VOG personeel | VOG vereist en geregistreerd vóór toegang; jaarlijkse controle | K-11 | R-08 | HR-registraties, auditverslag |

9. KPI/SLA-samenvatting | KPI | Omschrijving | Norm | Meetmethode | Frequentie | Rapportage | Service credits | | K-01 | Beschikbaarheid (maandelijks) | ≥ 99,8% | Azure Monitor/SLM | Maandelijks | SLA-rapport | <99,8%: 5% credit; <99,5%: 10% | | K-02 | Detectietijd P1 | ≤ 5 min | Alertlogs | Maandelijks | SLA-rapport | >5 min in maand: 2% | | K-03 | Responstijd P1 | ≤ 1 uur | Tickets | Maandelijks | SLA-rapport | >1 uur: 3% | | K-04 | Oplostijd P1 | ≤ 4 uur (of workaround ≤ 2 uur) | Tickets | Maandelijks | SLA-rapport | >4 uur: 3% | | K-05 | Documentatie/CMDB en governance | 100% kritieke config in CMDB; 1x/mnd operationeel overleg | Checklists/notulen | Maandelijks | Notulen | Niet gehaald: verbeteractie verplicht | | K-06 | Patch-compliance high/critical | ≤ 14 dagen | Patchrapport | Maandelijks | Security-rapport | Overschrijding: 2% | | K-07 | Incidentmelding security | ≤ 24 uur | Incidentlog | Per incident | Incidentrapport | Overschrijding: 3% | | K-08 | Toegangsreviews | 100% kwartaalreview | Reviewrapport | Per kwartaal | QBR | Niet gehaald: 2% | | K-09 | DR/BCP-test | 100% jaarlijkstest; RTO/RPO gehaald | Testrapport | Jaarlijks | QBR | Niet gehaald: 5% | | K-10 | Change-succesratio | ≥ 98% | Change-logs | Maandelijks | SLA-rapport | <98%: 2% | | K-11 | VOG-compliance | 100% | HR-audit | Halfjaarlijks | QBR | Niet gehaald: 3% | | K-12 | Compute-waste reductie | ≥ 15% in jaar 1 | FinOps-rapport | Per kwartaal | QBR | Informerend; sturing in CAB | | K-13 | CO2-rapportage cloud | 100% per kwartaal | Azure/FinOps | Per kwartaal | QBR | Informerend; sturing in CAB |

Toelichting service credits: Service credits worden als percentage verrekend op de maandelijkse dienstvergoeding voor de beheerdienst, cumulatief gemaximeerd op 10% per maand, en gelden als prikkel tot continue verbetering (zonder afbreuk aan overige rechten van de opdrachtgever).

10. Transitieplanning (eenvoudige Gantt, T0=contractstart) | Fase | Week 1-2 | Week 3-4 | Week 5-6 | Week 7-8 | Week 9-10 | Week 11-12 | | Kick-off & toegang | X | | | | | | Nulmeting & CMDB | X | X | | | | | Monitoring & SIEM | | X | X | | | | Patching/back-up beleid | | X | X | | | | Proefdraaien & WAR-room | | | X | X | | | DR-test & acceptatie | | | | X | X | | Go-Live & overdracht | | | | | X | X |

11. PDCA-borging per cyclus

- Plan: Maandelijks verbetervoorstellen (max. 5) in CAB op basis van KPI’s en incidenttrends; kwartaaldoelen vastgesteld (S.M.A.R.T.).
- Do: Implementatie door toegewezen eigenaren met start/einddatum; communicatie naar stakeholders ≥ 5 werkdagen vooraf.
- Check: Maandelijkse KPI-review; QBR met trendanalyse (3 maanden) en auditbevindingen.
- Act: Herprioritering backlog; update runbooks/CMDB binnen 5 werkdagen; kennisdeling in eerstvolgende operationeel overleg.

12. Compliance en bewijsvoering

- ISO 27001 en ISO 9001 certificeringen: geldig; scope dekt cloud- en infrastructuurbeheer. Statement of Applicability en certificaten beschikbaar voor inzage.
- VOG: Verplicht vóór toegang; registratie in HR-systeem; halfjaarlijkse steekproefcontrole.
- Registraties: Tickets, changes, alerts, patchrapporten, DR-testen en QBR-notulen worden minimaal 24 maanden bewaard.

- AVG: Verwerkersovereenkomst conform template opdrachtgever; DPIA-ondersteuning en datalekprocedure met 24-uurs meldplicht.

13. Innovatie en meerwaarde

- Zero Trust principes: MFA, CA, JIT, en segmentatie als default.
- Sentinel use-case library: Geprioriteerd op dreigingen in onderwijs/overheid (o.a. account takeover, privilege abuse).
- FinOps: Transparante dashboards; advies over reserved instances/savings plans, zonder lock-in buiten contractuele kaders.
- Security awareness: 1 sessie/jaar voor key users (60 minuten), phish-simulatie optioneel na akkoord.

14. Conclusie Onze aanpak combineert bewezen beheerprocessen, strikte security en continuïteit met meetbare prestaties en duurzame optimalisatie. We voldoen aan alle knock-out eisen (ISO 27001, VOG) en overtreffen must-haves met extra onderhoud (4x/jaar), strakkere detectietijden en een volwassen FinOps- en duurzaamheidskader. Door de PDCA-cyclus, transparante KPI’s en heldere governance minimaliseren we risico’s en maximaliseren we beschikbaarheid, veiligheid en kostenbeheersing.

Bijlage: Compact Risicodossier en KPI-overzicht zijn geïntegreerd in dit EMVI-plan; nadere detaillering leveren wij bij gunning binnen 10 werkdagen.

Benodigde input:

- Overzicht van alle huidige systemen/workloads, netwerkdiagrammen en afhankelijkheden (actueel).
- Toegang tot Azure-subscripties/tenant (delegatie/privileged access) en bestaande monitoring/logging.
- Aangewezen contactpersonen voor CAB, security/FG en operationeel overleg.
- Beschikbare beleidstukken (security, privacy, datalokalisatie), change-freeze kalender en onderhoudsvensters.
- Lijst met medewerkers met toegangsbehoefte (voor VOG-verificatie) en autorisatiematrix.

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: