

# **EMVI / Plan van Aanpak**

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

Datum: 11/19/2025

EMVI / Plan van Aanpak — Project 1380 Raamovereenkomst Catering- en Horecadiensten voor Gemeente Middenstad (feitelijke scope: ICT-beheer, cloud- en infrastructuurdiensten) — Uno Automatiseringsdiensten B.V.

1. Managementsamenvatting Doel Wij leveren onder de raamovereenkomst aantoonbaar veilige, betrouwbare en continu beschikbare beheer- en supportdiensten voor de ICT-omgeving van Gemeente Middenstad, met:

- Beschikbaarheid kritieke systemen  $\geq 99,8\%$  per maand
- Responstijd  $P1 \leq 30$  minuten, oplostijd  $P1 \leq 4$  uur
- Volledige EU-dataverwerking, ISO 27001 en ISO 9001 geborgd
- 24/7 bereikbaarheidsdienst (NOC/SOC), ITIL-processen en proactieve monitoring

EMVI-waarde in één oogopslag

- Kwaliteit (40%): ITIL v4-gedreven operatie, PDCA-cyclus met maandelijkse service reviews en kwartaalverbeterplannen; bewezen onboarding in  $\leq 90$  dagen met nul-onderbrekingsmigratie.
- Duurzaamheid (20%): 100% EU-datacenters op groene stroom;  $PUE \leq 1,3$ ; CO2 per ticket max. 0,5 kg door remote-first; circulaire hardware-adviezen; meetbaar rapporteren per kwartaal.
- Risicobeheersing (20%): Risicodossier met 12 kernrisico's, preventieve drempelwaarden (bijv. CVSS  $\geq 9$ : patch  $\leq 48$  uur), crisisrunbooks, geo-redundantie en RTO/RPO per dienstlaag.
- Prijs (20%): Efficiëntie door automatisering (Intune/Autopilot, scripted remediation), shift-left servicedesk, volumekortingen op patching en monitoring; voorspelbaar maandtarief per device/gebruiker, met optionele modules.

Kernresultaten (SMART)

- Uptime  $\geq 99,8\%$  op kritieke systemen, gemeten via synthetics en server-side probes, maandelijks gerapporteerd; bij afwijking  $> 0,1\%$ : root cause binnen 5 werkdagen + corrigerende maatregel binnen 10 werkdagen (PDCA).
- P1-respons  $\leq 30$  min voor 95% van de P1's per maand; P1-oplossing  $\leq 4$  uur in  $\geq 90\%$  van de gevallen.
- Patchcompliance: kritieke patches (CVSS  $\geq 9$ ) binnen 48 uur  $\geq 95\%$ , hoog (CVSS 7-8,9) binnen 7 dagen  $\geq 95\%$ .
- EU-data: 100% van data en back-ups binnen EU; jaarlijkse DPIA/TSF-updates en leveranciersstatement updates.
- Klanttevredenheid (CSAT)  $\geq 8,2$  gemiddeld per kwartaal, response rate  $\geq 25\%$ .

Knock-out eisen (voldaan)

- KO: ISO 27001 gecertificeerd — bewijs B-01
- KO: ISO 9001 gecertificeerd — bewijs B-02
- KO: 24/7 bereikbaarheidsdienst — bewijs B-03 (NOC/SOC-piket en roosters)

2. Begrip van de opdracht Context en scope

- Ondanks de tenderbenaming betreft de feitelijke scope ICT-beheer- en beveiligingsdiensten (conform Must-eisen en SLA's). Wij richten ons op beheer, onderhoud en security van cloud- en infrastructuuroplossingen, inclusief Microsoft 365, endpoints, netwerken en kritieke applicaties.
- Doelstelling opdrachtgever: continuïteit en beschikbaarheid van gemeentelijke diensten, veilig datagebruik conform AVG en BIO, voorspelbare dienstverlening met korte responstijden.

Functionele scope

- 24/7 monitoring en incidentafhandeling; ITIL-gebaseerde servicedesk.
- Proactief patchmanagement, change- en releasemanagement.
- Microsoft 365-ondersteuning (Exchange Online, SharePoint, OneDrive, Teams, Entra ID, Intune).
- Netwerk- en endpointbewaking, kwetsbaarheidsscans, hardening (CIS-benchmarks).
- Continuïteit (BCP/DR): RTO/RPO per systeemklasse, testfrequentie halfjaarlijks.

#### Randvoorwaarden en aannames

- Alle data en back-ups blijven in de EU (NL/DE).
- Opdrachtgever levert tijdig benodigde toegangen en informatie aan; locaties toegankelijk tijdens kantooruren.
- Besluitvorming binnen afgesproken termijnen; rechtmatige licenties (M365, overige).
- Uitsluitingen: levering/beheer onsite hardware, third-party SaaS-support buiten onze regie, projectmatig meerwerk buiten vaste fee; adoptie/training op verzoek.

#### Compliance

- AVG/BIO, NEN 7510-principes waar relevant, logging en bewaartermijnen conform beleid.
- VOG voor personeel indien vereist; register en controles ingericht (bewijs B-08).

#### 3. Aanpak (Plan van Aanpak — PDCA) 3.1 Transitie en onboarding (0–90 dagen)

- Doel: in 90 kalenderdagen naar gestabiliseerd beheer met nul verstoring van kritieke diensten (max. 30 min venster per change, buiten kantooruren).
- Deliverables: As-is CMDB, transitieplan, risico-overnamematrix, meetplan, runbooks, noodprocedures.

#### Eindresultaten en mijlpalen:

- D+10: Kick-off, governance-inrichting, intake security- en privacy-eisen.
- D+20: Tooling live (monitoring agents, SIEM-connectors, Intune), eerste basismetrics.
- D+45: Compleet servicecatalogus, CMDB v1, kritieke afhankelijkheden in kaart, eerste patchwindow uitgevoerd.
- D+75: Runbooks incident/major incident, changekalender + freeze-policy, DR-testplan v1.
- D+90: Go-live steady state, eerste MBR (maandreview), PDCA-backlog Q1.

#### 3.2 Beheer en operatie (steady state) Incident- en requestmanagement (ITIL)

- Intakekanalen: portaal en telefoon (24/7); prioritering P1–P4 conform impact/urgentie-matrix.
- P1: responstijd ≤ 30 min, oplostijd ≤ 4 uur; P2: resp. ≤ 1 uur, oplos ≤ 8 uur; P3: resp. ≤ 4 uur, oplos ≤ 3 werkdagen.
- Major Incident Manager inzet binnen 15 min na P1-classificatie; communicatie elke 30 min tot herstel.

#### Probleem- en changemanagement

- Problem reviews wekelijks; Known Error Database met workarounds binnen 5 werkdagen na herhaal-P1/P2.
- Changes: CAB wekelijks; standaard changes vooraf gedefinieerd en geautomatiseerd waar mogelijk; no-go windows tijdens kantooruren; noodchanges via e-CAB binnen 2 uur.

#### Patch- en releasemanagement

- Kritiek (CVSS ≥ 9): uitrol ≤ 48 uur; Hoog: ≤ 7 dagen; Overig: binnen 30 dagen.
- M365 release rings: pilot (5%), broad (45%), enterprise (50%); rollbackplan per update.
- Patchvensters: woensdag 20:00–02:00 en zaterdag 22:00–04:00; afwijkingen in overleg.

## Monitoring, detectie en response

- 24/7 NOC/SOC met drempelwaarden: CPU > 85% > 15 min, disk < 15% vrij, latentie > 120 ms, packet loss > 2%.
- SIEM-regels voor MFA-bypass, mass-login, privilege escalations; triage < 15 min, containment binnen 2 uur voor confirmed high severity.

## Security & compliance

- CIS-hardened baseline voor servers en endpoints; baseline review per kwartaal.
- Kwetsbaarheidsscans maandelijks; remediation binnen SLA's; phishing-simulaties per kwartaal.
- AVG: DPIA's op relevante verwerkingen; verwerkersovereenkomst; DLP en retentie policies M365.

## Continuïteit (BCP/DR)

- RTO/RPO: Kritiek RTO ≤ 4 uur, RPO ≤ 15 min; Hoog RTO ≤ 8 uur, RPO ≤ 1 uur; Overig RTO ≤ 24 uur, RPO ≤ 24 uur.
- Back-up: dagelijkse volledige en logback-ups; succesratio ≥ 99%; restore-tests per kwartaal.
- DR-test halfjaarlijks met rapport en verbeterplan binnen 10 werkdagen.

## Rapportage en PDCA

- MBR: maandelijks SLA-rapport, risico-update, capaciteitsanalyse, security-findings, actie- en verbeterpunten.
- QBR: per kwartaal roadmap, trendanalyse, ketenrapportage, duurzaamheidsrapportage en KPI's.
- Continual Improvement Register: max. 10 open verbeteracties tegelijk, meetbaar en eigenaar toegewezen.

## 3.3 Eenvoudige Gantt (transitie 0–90 dagen)

Fase | Week 1–2 | 3–4 | 5–6 | 7–8 | 9–10 | 11–12 | 13 Inventarisatie & Kick-off | ■■■■ | Tooling & Monitoring live | ■■■■ | CMDB v1 & Servicecatalogus | ■■■■ | Patch & Changekalender | ■■■■ | Runbooks & DR-testplan v1 | ■■■■ | Go-live steady state & MBR1 | ■■■■ | ■■■■

## 4. Borging (Kwaliteit en continu verbeteren)

- ISO 9001 QMS: processen gedocumenteerd, jaarlijkse externe audit; interne audits per halfjaar.
- KPI-guardrails: automatisch gemonitord, afwijkingen triggeren problem review binnen 5 werkdagen.
- KTO/CSAT: per ticket; kwartaal-rapport; verbeteractie bij CSAT < 8,2.
- Gedragslijnen: 4-ogenprincipe voor changes, segregatie van taken (admin vs. reviewer).
- Kennisborging: up-to-date runbooks, KEDB, technische notities; training en certificering (Microsoft, ITIL, security).
- Contract- en leveranciersmanagement: DAP (Data Processing Agreement), subverwerkerslijst, jaarlijkse due diligence.

## 5. Duurzaamheid en maatschappelijke waarde

- Datacenters: EU-locaties met 100% groene stroom; PUE ≤ 1,3; rapportage per QBR.
- Energie-reductie: power policies endpoints (10% verbruiksreductie in 6 maanden), server right-sizing (doel: 15% minder idle).
- Reisbewegingen: remote-first; max. 1 onsite-dag per maand per locatie voor regulier beheer; bundeling bezoeken.
- E-waste & circulariteit: gecertificeerde refurb/recycle partners; datavernietiging met bewijs; lifecycleadvies en M365 Cloud PC waar passend.

- KPI's duurzaamheid: CO2/incident  $\leq 0,5$  kg; km/maand  $\leq 150$ ; % groene stroom 100%; e-waste 100% gecertificeerd verwerkt.

## 6. Risico's (register en beheersing)

ID | Risico | Kans | Impact | Maatregelen | KPI-koppeling | W-koppeling | Rest-risico R-01 | Onvolledige CMDDB → gemiste afhankelijkheden | M | H | Discovery tooling, validatie door proceseigenaren, CMDDB-review maandelijks | KPI-09 CMDDB-dekking  $\geq 95\%$  | W-02 | Laag R-02 | P1-storm (kettingincidenten) | M | H | Problem mgmt, auto-scaling, MIM-proces, call-trees | KPI-02 P1-oplossing, KPI-03 FCR | W-04 | Middel R-03 | Security breach via endpoint | M | H | CIS baseline, EDR, patching 48u, phishing-tests | KPI-05 Patchcompliance, KPI-11 Security incidenten | W-06 | Laag R-04 | Leveranciersstoring (cloud) | M | H | Multi-AZ, failover, runbooks, statusmonitoring | KPI-01 Uptime | W-03 | Middel R-05 | Datalocatie-breach (non-EU) | L | H | Contractuele borging, geofencing, CASB/DLP | KPI-12 EU-dataverwerking 100% | W-07 | Laag R-06 | Change-failure | M | M | CAB, test, back-out, ringed releases | KPI-07 Change-succes  $\geq 98\%$  | W-05 | Laag R-07 | Niet-tijdige escalatie | L | H | Escalatieprocedure, wallboards, 2e-lijn piket | KPI-02, KPI-04 Escalaties tijdig | W-08 | Laag R-08 | Capaciteitstekort | M | M | Capaciteitsplanning maand, trendanalyse | KPI-10 Capaciteit | W-10 | Middel R-09 | Back-up mislukt | L | H | 2-locaties, immutability, monitoring, test | KPI-08 Back-up succes  $\geq 99\%$  | W-09 | Laag R-10 | Kennisafhankelijkheid key-person | M | M | Documentatie, rotaties, shadowing | KPI-13 Kennisdekking | W-11 | Laag R-11 | AVG-naleving (retenties) | M | M | DLP/retentie, DPIA, awareness | KPI-14 AVG-audits zonder major | W-07 | Laag R-12 | Onvoorziene legacy | M | M | Isolatie, containerization, tijdelijke workarounds | KPI-06 Vulnerability backlog | W-12 | Middel

## 7. Organisatie en governance Rollen en bezetting (indicatief)

- Service Owner/Governance: Service Manager (0,2 fte) — aanspreekpunt, MBR/QBR, PDCA.
- Technisch Lead Cloud/Infra (0,1 fte) — architectuur, changes, escalaties.
- NOC/SOC 24/7 pool — 1e/2e lijn, monitoring, triage, herstel.
- M365 Specialist — tenant, compliance, adoption-advies op verzoek.
- Security Officer — SIEM-rules, audits, pentestcoördinatie.
- Onsite Engineer (optioneel) — geplande werkzaamheden, hardware-handelingen. Escalatie (tijdens P1)
- 0–15 min: Incident Manager; 15–30 min: Technisch Lead; 30–60 min: Service Manager en leverancier-escalatie; >60 min: opdrachtgever-CIO/contractmanager geïnformeerd. Overlegstructuur
- Dagelijks: stand-up (intern).
- Wekelijks: operationeel overleg (tickets, changes, capaciteit).
- Maandelijks: MBR met opdrachtgever (SLA's, risico's, acties).
- Per kwartaal: QBR (roadmap, duurzaamheid, security, contract KPI's). Communicatie
- Real-time statuspagina/portal met P1-updates; postmortem binnen 5 werkdagen; wijzigingen via changekalender.

## 8. Programma van Wensen (W-xx) Tabel: Wens, invulling, KPI, risico, bewijs

### W-01 KO: ISO 27001

- Invulling: Gecertificeerd ISMS; jurisdictie NL/EU; jaarlijkse audits.
- KPI: KPI-14 (AVG/ISMS audit zonder major).
- Risico: R-11.
- Bewijs: B-01 ISO 27001 certificaat (kopie bijgevoegd).

### W-02 KO: ISO 9001

- Invulling: QMS met interne/extern audits; PDCA.
- KPI: KPI-15 (Interne audit-actiefloop 100% binnen 60 dagen).

- Risico: R-10.
- Bewijs: B-02 ISO 9001 certificaat.

#### W-03 KO: 24/7 bereikbaarheidsdienst

- Invulling: NOC/SOC-roosters, MIM-proces, call trees.
- KPI: KPI-02 (P1-responstijd).
- Risico: R-02.
- Bewijs: B-03 Piketrooster + MIM-runbook.

#### W-04 Must: Maximale responstijd P1 30 min

- Invulling: SLA-wallboards, prioritering, auto-paging.
- KPI: KPI-02  $\leq$  30 min (95%).
- Risico: R-07.
- Bewijs: B-04 SLA-rapport voorbeeld.

#### W-05 Must: Beschikbaarheid 99,8%/maand

- Invulling: redundantie, health checks, synthetics, failover-tests.
- KPI: KPI-01  $\geq$  99,8%.
- Risico: R-04.
- Bewijs: B-05 Monitoringrapport voorbeeld.

#### W-06 Must: Monitoring & patchmanagement

- Invulling: 24/7 monitoring; kritieke patches  $\leq$  48u; maandelijks patchrapport.
- KPI: KPI-05 Patchcompliance.
- Risico: R-03, R-12.
- Bewijs: B-06 Patchpolicy + rapport.

#### W-07 Must: ITIL-servicedesk

- Invulling: Incident/Request/Problem/Change; CAB; KEDB.
- KPI: KPI-03 FCR; KPI-07 Change-succes.
- Risico: R-06.
- Bewijs: B-07 ITIL-procesbeschrijvingen.

#### W-08 Must: EU-dataverwerking

- Invulling: EU-only datacenters; geofencing; subverwerkerslijst.
- KPI: KPI-12 100% EU.
- Risico: R-05.
- Bewijs: B-09 Verwerkersovereenkomst + subverwerkerslijst.

#### W-09 Must: Escalatieprocedure incidenten & changes

- Invulling: e-CAB, escalatieladder, communicatiecadans 30 min.
- KPI: KPI-04 Tijdige escalatie.
- Risico: R-07.
- Bewijs: B-03, B-10 Escalatieschema.

#### W-10 Must: Continuïteitsplan (BCP)

- Invulling: RTO/RPO, DR-test 2x/jaar, back-up immutability.

- KPI: KPI-08 Back-up succes; KPI-16 DR-test geslaagd.
- Risico: R-09.
- Bewijs: B-11 BCP/DR-plan + testrapport.

#### W-11 Must: VOG-personeel

- Invulling: VOG-register; onboarding-checklist; jaarlijkse hercontrole steekproefsgewijs.
- KPI: KPI-17 100% VOG indien vereist.
- Risico: R-10.
- Bewijs: B-08 VOG-proces.

#### W-12 Must: Proactieve monitoring netwerk & endpoints

- Invulling: NTA/EDR, SNMP/Flow, anomaliedetectie.
- KPI: KPI-11 Security-incidenten tijd tot detectie  $\leq 15$  min.
- Risico: R-03.
- Bewijs: B-12 Use-cases SIEM/EDR.

#### W-13 Must: Ondersteuning Microsoft 365

- Invulling: Tenant hardening, DLP/retentie, release rings, Teams/SharePoint governance.
- KPI: KPI-07 Change-succes; KPI-06 Vulnerability backlog.
- Risico: R-12.
- Bewijs: B-13 M365 governance-notitie.

#### W-14 Extra: Duurzaamheidsrapportage

- Invulling: CO2/incident, PUE, km/maand, e-waste 100% verwerkt; kwartaalrapport.
- KPI: KPI-18 Duurzaamheids-KPI's gehaald.
- Risico: R-08 (capaciteit).
- Bewijs: B-14 Duurzaamheidsrapport sjabloon.

#### W-15 Extra: Security awareness

- Invulling: 2x per jaar phishing-simulatie + microtraining; rapportage.
- KPI: KPI-19 Phish fail-rate  $\leq 5\%$  binnen 12 maanden.
- Risico: R-03.
- Bewijs: B-15 Voorbeeldrapport simulatie.

#### W-16 Extra: Ketenmonitoring

- Invulling: synthetics voor kritieke e-dienstverlening; SLO's per keten.
- KPI: KPI-01 Uptime; KPI-10 Capaciteitstrends.
- Risico: R-04.
- Bewijs: B-05 Synthetics-sjabloon.

9. KPI/SLA-samenvatting ID | KPI | Target | Meting | Frequentie | Escalatie | W/R-koppeling KPI-01 | Uptime kritieke systemen |  $\geq 99,8\%$  p/mnd | Synthetics + server probes | Maandelijks |  $<99,8\%$ : MIM RCA + verbeterplan 10 wd | W-05, R-04 KPI-02 | P1-responstijd |  $\leq 30$  min ( $\geq 95\%$ ) | ITSM-timestamps | Maandelijks |  $<95\%$ : staffing/herroostering binnen 2 wk | W-04, R-07 KPI-03 | First Contact Resolution |  $\geq 70\%$  (P3/P4) | ITSM | Maandelijks |  $<70\%$ : kennisbank update + training | W-07, R-02 KPI-04 | Tijdige escalatie | 100% volgens ladder | ITSM/MIM-log | Per P1 | Afwijking: postmortem + procesupdate | W-09, R-07 KPI-05 | Patchcompliance kritisch |  $\geq 95\% \leq 48u$  | Vulnerability mgmt | Wekelijks/maandelijks |  $<95\%$ : noodwindow + CAB | W-06, R-03 KPI-06 | Vulnerability backlog (High) |



0 > 30 dagen | Scanner/CMDB | Wekelijks | Overschrijding: escalatie CAB | W-06, R-12 KPI-07 | Change-succesrate |  $\geq 98\%$  | ITSM/CAB | Maandelijks |  $<98\%$ : QA-gate aanscherpen | W-07, R-06 KPI-08 | Back-up succes |  $\geq 99\%$  | Backup logs | Wekelijks/maand |  $<99\%$ : hersteltests + tuning | W-10, R-09 KPI-09 | CMDB-dekking |  $\geq 95\%$  juist/volledig | CMDB audit | Maandelijks |  $<95\%$ : discovery sweep + owners | W-02, R-01 KPI-10 | Capaciteitsmarges |  $\geq 15\%$  vrij | Monitoring | Maandelijks |  $<15\%$ : scaling plan | W-10, R-08 KPI-11 | TTD security alerts (High) |  $\leq 15$  min | SIEM | Maandelijks |  $>15$  min: rule tuning + staffing | W-12, R-03 KPI-12 | EU-dataverwerking | 100% | Contract/logs | Kwartaal | Afwijking: exit/subprocessor swap | W-08, R-05 KPI-13 | Kennisdekking |  $\geq 2$  engineers/runbook | HR/KB | Kwartaal |  $<2$ : training/rotatie | W-02, R-10 KPI-14 | ISMS/AVG major non-conformities | 0 | Audit | Jaarlijks | Bevinding: CAPA  $\leq 30$  dgn | W-01, W-07, R-11 KPI-15 | QMS acties afgesloten | 100%  $\leq 60$  dgn | QMS | Kwartaal | Overschrijding: MT-escalatie | W-02, R-10 KPI-16 | DR-test geslaagd | 2/jaar, 100% | DR-rapport | Halfjaar | Faal: extra test  $\leq 30$  dgn | W-10, R-09 KPI-17 | VOG op orde | 100% indien vereist | HR-check | Halfjaar | Tekort: offboarding/opschorting toegang | W-11, R-10 KPI-18 | Duurzaamheids-KPI's |  $\geq 3/3$  gehaald | Rapport | Kwartaal | Miss: verbeterplan  $\leq 30$  dgn | W-14, R-08 KPI-19 | Phish fail-rate |  $\leq 5\%$  in 12 mnd | Simulaties | Kwartaal |  $>5\%$ : extra training | W-15, R-03

#### SLA-credit en sancties (kwaliteitsborging)

- Bij niet halen KPI-01 of KPI-02 in een maand: 2% service credit per KPI (max. 10%) op maandfee.
- Bij herhaald falen ( $>2$  maanden in kwartaal): verscherpt verbeterplan en QBR-escalatie.

#### 10. Bewijsstukken (B-xx)

- B-01: Kopie actueel ISO/IEC 27001-certificaat Uno Automatiseringsdiensten B.V. (uitgegeven door geaccrediteerde certificerende instelling).
- B-02: Kopie actueel ISO 9001-certificaat.
- B-03: 24/7 bereikbaarheidsplan incl. piketroosters en Major Incident-proces.
- B-04: Voorbeeld maandelijks SLA-rapport (geanonimiseerd).
- B-05: Voorbeeld monitoringdashboard/synthetics-rapport (geanonimiseerd).
- B-06: Patch- en kwetsbaarhedenbeleid + voorbeeldrapportage.
- B-07: ITIL-procesbeschrijvingen (Incident/Change/Problem).
- B-08: VOG-procedure en registerformat (persoonsgegevens geanonimiseerd).
- B-09: Verwerkersovereenkomst + subverwerkerslijst met EU-datalocaties.
- B-10: Escalatieschema en communicatiecadans (P1).
- B-11: BCP/DR-plan + voorbeeld DR-testrapport (geanonimiseerd).
- B-12: SIEM/EDR use-case catalogus (overview).
- B-13: Microsoft 365 governance-notitie (rings, DLP, retentie).
- B-14: Duurzaamheidsrapport sjabloon (CO2, PUE, reisbewegingen, e-waste).

#### 11. Prijs- en factureringsmodel (overzicht)

- Basismodel: per gebruiker/device maandfee voor servicedesk, monitoring, patching en M365-ondersteuning; optionele modules (24/7 SOC, on-site, advanced SIEM).
- Facturatie: maandelijks achteraf op basis van CMDB/portal-tellingen; prijsaanpassingen na wijziging volume  $> 10\%$ .
- Kostentransparantie: maandelijks kostenrapportage; geen verborgen toeslagen; meerwerk via vooraf geaccordeerde change/wijzigingsopdracht.
- Garantie: 12 maanden op projectdeliverables binnen transitie; daarna reguliere SLA's.

#### 12. Conclusie Met deze aanpak leveren wij aantoonbaar veilige, beschikbare en duurzame ICT-diensten conform de eisen van Gemeente Middenstad. Onze ISO-gecertificeerde PDCA-werkwijze, 24/7



operatie en strakke SLA/KPI-sturing borgen continuïteit en compliance. De voorgestelde KPI-set, risicobeheersing en governance zorgen voor voorspelbare resultaten en transparante samenwerking. Wij staan klaar om binnen 90 dagen gecontroleerd over te nemen en de dienstverlening aantoonbaar te verbeteren.

Benodigde input:

- Overzicht systemen/diensten (CMDB/export), classificatie (kritiek/hoog/overig) en afhankelijkheden.
- Huidige SLA's, changekalender en maintenance windows; lijst van lopende changes.
- Toegang tot huidige monitoring/ITSM-tools of API's; gewenste integraties.
- Overzicht van locaties, netwerktopologie en contactpersonen (functioneel/technisch).
- Security- en privacybeleid (AVG/BIO), bestaande DPIA's en verwerkersovereenkomsten.
- M365-tenantdetails (enrollment, policies), licentie-overzicht en security baselines.
- Back-up- en DR-architectuur (RTO/RPO), laatste testrapporten.
- Lijst van subverwerkers/leveranciers en contractuele afspraken (SLA's).
- Beveiligingseisen voor personeel (VOG-procedure, onboarding).
- Governancevoorkeuren: overlegfrequenties, rapportageformat, escalatielijst.

## 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: