

# **KPI / SLA Dashboard**

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

Datum: 11/19/2025

## KPI/SLA-dashboard – Raamovereenkomst ICT-beheer t.b.v. Gemeente Middenstad (Project 1380)

Doele en scope Dit KPI/SLA-dashboard borgt prestaties voor beheer, onderhoud, beveiliging en continuïteit van cloud- en infrastructuuroplossingen en Microsoft 365. Het dekt 24/7 incidentafhandeling, proactieve monitoring, EU-dataverwerking, ITIL-servicedesk en continuïteitsbeheer. Het document is PDCA-conform, SMART ingericht en kruist W-xx-eisen met KPI, risico en bewijs.

Definitie W-xx (verwijzingen naar aanbestedingseisen en deliverables)

- W-01: KO ISO 27001 gecertificeerd
- W-02: KO ISO 9001 gecertificeerd
- W-03: KO 24/7 bereikbaarheidsdienst
- W-04: Must P1 responstijd ≤ 30 minuten
- W-05: Must beschikbaarheid ≥ 99,8%/maand
- W-06: Must monitoring & patchmanagement geborgd
- W-07: Must ITIL-gebaseerde servicedeskprocessen
- W-08: Must alle data binnen EU verwerkt
- W-09: Must escalatieprocedure incidenten & changes
- W-10: Must continuïteitsplan (BCP) beschikbaar
- W-11: Must VOG indien vereist
- W-12: Must proactieve monitoring netwerk & endpoints
- W-13: Must ondersteuning Microsoft 365
- W-14: Deliverable Plan van Aanpak
- W-15: Deliverable Risicodossier
- W-16: Deliverable KPI-overzicht

### PDCA-sturingskader

- Plan
  - Service Blueprint (W-14): scope, CMDB-structuur, kritieke ketens, P1/P2-definities, onderhoudsvensters, escalatiepaden en RACI (Uno SDM ↔ Gemeente contractmanager). Oplevering binnen 20 werkdagen na start.
  - Risicodossier (W-15): top-20 risico's met eigenaar, kans/impact, beheersmaatregelen, KPI-koppeling en bewijs. Eerste versie binnen 20 werkdagen, kwartaalupdate.
- Do
  - 24/7 monitoring en incidentrespons (W-03, W-06, W-12).
  - ITIL-processen voor Incident, Request, Change, Problem en Knowledge (W-07).
  - Maandelijkse patchrondes, kwetsbaarhedenscans, back-up en restore-tests (W-06).
  - Microsoft 365 beheer en security-baselines (W-13).
- Check
  - Dagelijkse operationele checks; wekelijkse trendanalyse; maandelijkse SLA-rapportage (uiterlijk werkdag 5); kwartaal-QBR met verbeterplan en risicoherijking.
  - Audits: ISO 27001/9001 en EU-dataverwerking (W-01, W-02, W-08).
- Act
  - RCA met 5xWhy/Fishbone binnen 5 werkdagen na P1; probleemtickets met structurele maatregelen (change backlog).
  - Continual Improvement Register (CIR) met prioritering MoSCoW, realisatie via CAB (W-09).

KPI/SLA-tabel KPI/SLA | Target | Meetmethode | Frequentie | Escalatie | Verantwoordelijke | Link W-xx/criterium

1. Beschikbaarheid kritieke systemen |  $\geq 99,8\%$  per kalendermaand; gepland onderhoud uitgesloten (max. 4u/maand, 2 werkdagen vooraf aangekondigd) | Uptime-metingen via monitoringplatform; berekening per dienst en gewogen totaal | 24/7 monitoren; maandelijks rapport | Bij downtime > 60 min in lopende maand: P1 + escalatie naar Incident Manager (15 min), SDM (30 min), klant-Contractmanager (60 min) | Uno Technisch Lead; SDM | W-05, W-06, W-12; EMVI: Kwaliteit, Risicobeheersing
2. Responstijd P1-incidenten (24/7) |  $\leq 30$  min vanaf melding tot eerste contact en triage | ITSM-tijdstempels; call-opname | Per P1; wekelijks steekproef | > 20 min: Incident Manager; > 30 min: SDM + klant-Contractmanager; recurrent ( $\geq 2$ /mnd): CAP in QBR | Incident Manager | W-03, W-04, W-07, W-09; EMVI: Kwaliteit
3. Oplostijd P1-incidenten |  $\leq 4$  uur tot serviceherstel (workaround toegestaan) | ITSM, hersteltijd, klantbevestiging | Per P1; maandelijks | > 2 uur: War-room + leveranciers; > 3 uur: MT-escalatie; > 4 uur: formele major incident review binnen 2 werkdagen | Incident Manager; Problem Manager | W-07, W-09, W-10; EMVI: Risicobeheersing
4. Responstijd P2-incidenten (kantoortijd) |  $\leq 4$  uur (ma-vr 08:00-18:00 CET) | ITSM-tijdstempels | Per P2; maandelijks | > 3 uur: SDM; overschrijding: rapport + verbeteractie | Servicedesk Lead | W-07, W-09; EMVI: Kwaliteit
5. Oplostijd P2-incidenten |  $\leq 2$  werkdagen | ITSM doorlooptijd | Per P2; maandelijks | Dag 1 reminder; dag 2 SDM; dag 3 CAB-prioritering | Problem Manager | W-07; EMVI: Kwaliteit
6. Patch compliance endpoints/servers | Kritiek:  $\geq 95\%$  binnen 7 dagen; Hoog:  $\geq 95\%$  binnen 14 dagen; Overig OS/firmware:  $\geq 95\%$  binnen 30 dagen | Patchmanagement-rapportages; agent compliance | Wekelijks; maandelijks rapport | < target 2 weken op rij: Change naar versnelde patch; 4 weken: SDM + klant | Technical Lead Security | W-06, W-12; EMVI: Risicobeheersing
7. Back-up succes en herstel | Back-up jobs succesvol  $\geq 99\%$  per week; restore test 1x/maand per dienst; RPO  $\leq 24$ u; RTO  $\leq 4$ u (kritiek) | Backupconsole; restore-tests met testrapport | Dagelijks; maandelijks test | 2 opeenvolgende failures: SDM; restore test fail: binnen 5 werkdagen hertest + RCA | Backup Owner | W-10; EMVI: Risicobeheersing
8. Security incident TTD/MTTC | TTD  $\leq 15$  min; MTTC  $\leq 60$  min (containment) | SIEM/EDR alerts; incidentlog | 24/7; maandelijks | TTD > 15 min of MTTC > 60 min: Security Officer + SDM + klant binnen 2 uur; RCA binnen 5 werkdagen | Security Officer | W-06, W-12; EMVI: Risicobeheersing
9. Kwetsbaarheden remediatie | Kritiek (CVSS  $\geq 9$ ):  $\leq 7$  dagen; Hoog (7-8.9):  $\leq 30$  dagen; Acceptatie via risicotraject met eigenaar en einddatum | Vulnerability scans; change evidence | Tweewekelijks; maandelijks | Overschrijding: CAB-escalatie; bij herhaling: directie-escalatie | Security Officer; Change Manager | W-06, W-15; EMVI: Risicobeheersing
10. EU-dataverwerking compliance | 100% opslag en verwerking binnen EU; 0% datalekken door datalokatie | DPIA/ISO-logs; verwerksovereenkomsten; locatorrapport | Kwartaal; bij wijziging direct | Afwijking: direct stoppen verwerking, DPO-melding, plan herstel binnen 24u | Compliance Officer | W-08, W-01; EMVI: Kwaliteit, Risicobeheersing
11. Servicedesk First Contact Resolution |  $\geq 70\%$  FCR voor eindgebruikers-incidenten | ITSM-categorie FCR; QA-steekproef | Maandelijks | < 70% gedurende 2 maanden: kennisbank-actie + training; rapport in QBR | Servicedesk Lead | W-07; EMVI: Kwaliteit, Prijs
12. Klanttevredenheid (CSAT) | Gemiddeld  $\geq 8,2/10$ ; respons  $\geq 30\%$  van gesloten tickets | Post-ticket survey; trendanalyse | Doorlopend; maandelijks | < 8,2 of respons < 30%: verbeterplan + 2 weken acties; escalatie SDM → klant | SDM | W-02; EMVI: Kwaliteit
13. Change succes en communicatie | Succesrate  $\geq 98\%$  (geen rollback); klantimpact changes  $\geq 5$  werkdagen vooraf aangekondigd; Emergency Change PIR  $\leq 2$  werkdagen | ITSM-change logs; CAB-notulen | Wekelijks CAB; maandelijks | Succesrate < 98%: CAB herzien; communicatiebreuk: SDM-escalatie | Change Manager | W-09, W-07; EMVI: Kwaliteit, Risicobeheersing

14. Monitoring- en EDR-dekking | ≥ 99% assets met actieve monitoring; EDR/AV up-to-date ≥ 98% | CMDB vs agents; EDR-console | Dagelijks; wekelijks | Gap > 1% > 24u: P2; > 3 dagen: SDM-escalatie | Technical Lead Monitoring | W-06, W-12; EMVI: Risicobeheersing
15. Microsoft 365 beheer SLA | Standaard provisioning/verwijderen accounts ≤ 1 werkdag; licentiecompliance 100%; herstel mailbox/site ≤ 4u | ITSM; M365 auditlogs; licentie-rapport | Dagelijks; maandelijks | Overschrijding: SDM + M365 Lead; structureel: CAB-automatisering | M365 Lead | W-13; EMVI: Kwaliteit
16. BCP/DR-oefening | 1x per jaar integrale test per kritieke dienst; 100% testdoelen gehaald of verbeterplan binnen 10 werkdagen | Testplan, testrapport, RCA | Jaarlijks; QBR review | Testdoel niet gehaald: directie-escalatie en herhaling binnen 30 dagen | SDM; Business Continuity Manager | W-10; EMVI: Risicobeheersing
17. VOG- en toegangscompliance | 100% medewerkers on-site met geldige VOG; toegangsmatrix jaarlijks herzien | HR-dossiers; access reviews | Kwartaal | Afwijking: medewerker van site, melding klant, herstel binnen 24u | HR Manager | W-11; EMVI: Risicobeheersing
18. Duurzame hosting en operatie | 100% datacenterstroom hernieuwbaar; -10% kWh per VM/jr t.o.v. nulmeting via right-sizing | Energiebewijs/GoO; resource-rapportage | Halfjaar; QBR | Afwijking: plan van aanpak binnen 30 dagen; alternatieve provider-advies | SDM; Sustainability Lead | EMVI: Duurzaamheid

#### Kruismatrix KPI ↔ Risico ↔ Bewijs (selectie)

- KPI 1 (Beschikbaarheid) ↔ Risico: Onbeschikbaarheid primaire dienstverlening ↔ Bewijs: Uptime-rapporten, incidentlogs, onderhoudsberichten ↔ W-05/W-06/W-12.
- KPI 2–5 (Response/Resolutie P1/P2) ↔ Risico: Verlengde verstoringen en reputatieschade ↔ Bewijs: ITSM-exports, war-room notulen ↔ W-03/W-04/W-07/W-09.
- KPI 6 (Patch) ↔ Risico: Exploit van bekende kwetsbaarheden ↔ Bewijs: Patchcompliance-overzichten, CAB-besluiten ↔ W-06/W-12.
- KPI 7 (Back-up/Herstel) ↔ Risico: Dataverlies ↔ Bewijs: Backup- en restore-rapporten, testprotocollen ↔ W-10.
- KPI 8–9 (Security/VA) ↔ Risico: Security-incidenten en datalek ↔ Bewijs: SIEM/EDR-alerts, VA-rapporten, waivers ↔ W-06/W-12/W-01.
- KPI 10 (EU-data) ↔ Risico: Schending AVG en datalocatie-eis ↔ Bewijs: Verwerksovereenkomsten, datalocator, DPIA ↔ W-08.
- KPI 11–12 (FCR/CSAT) ↔ Risico: Inefficiënte operatie en lage tevredenheid ↔ Bewijs: ITSM KPI exports, surveyresultaten ↔ W-07/W-02.
- KPI 13 (Change) ↔ Risico: Wijzigingsfalen en uitval ↔ Bewijs: Change logs, PIR's, CAB-notulen ↔ W-09/W-07.
- KPI 14 (Monitoring/EDR) ↔ Risico: Onopgemerkte storingen en malware ↔ Bewijs: Agent health-rapporten, CMDB-exports ↔ W-06/W-12.
- KPI 15 (M365) ↔ Risico: Toegangs- en complianceproblemen ↔ Bewijs: M365 auditlogs, licentie-overzichten ↔ W-13.
- KPI 16 (BCP/DR) ↔ Risico: Onvoldoende herstelvermogen ↔ Bewijs: Testrapporten, RCA's ↔ W-10.
- KPI 17 (VOG) ↔ Risico: Ongearriveerde toegang op locatie ↔ Bewijs: HR/VOG-dossiers, access reviews ↔ W-11.
- KPI 18 (Duurzaamheid) ↔ Risico: Niet behalen duurzaamheidsdoelen ↔ Bewijs: GvO certificaten, energie- en right-sizing rapporten ↔ EMVI: Duurzaamheid.

#### Escalatie- en communicatiekanalen

- P1: Direct telefonisch en via ITSM push naar Incident Manager (binnen 15 min), SDM (binnen 30 min) en Contractmanager Gemeente (binnen 60 min). War-room met leveranciers waar relevant.
- P2: ITSM-notificatie naar Servicedesk Lead; escalatie naar SDM bij dreigende overschrijding.
- Governance: MBR (maandelijks operationeel), QBR (strategisch, inclusief risico's, verbeteracties, KPI-trends), ad-hoc Security Council bij high/critical kwetsbaarheden.

#### Audit en bewijsvoering

- Alle KPI's zijn herleidbaar via ITSM-exports (CSV/PDF), monitoring-/SIEM-rapportages, CAB-notulen, back-up/logboeken, M365 auditlogs, HR/VOG-dossiers en verwerkersovereenkomsten. Bewijs wordt minimaal 24 maanden bewaard ten behoeve van audits (ISO 27001/9001) en opdrachtgever-controles.

#### Benodigde input:

- Lijst kritieke systemen/ketens en gewenste weging voor beschikbaarheid.
- Definitie P1/P2/P3 per dienst en gewenste onderhoudsvensters.
- Contact- en escalatielijst (Contractmanager, Technisch aanspreekpunt, Security officer).
- Acceptatie van meetlocaties/metingen (monitoring end-to-end vs. component).
- Overzicht datalocaties/geo-voorkeuren en verwerkers (voor EU-dataverwerking).
- Goedkeuring RTO/RPO per dienst en back-up retentiebeleid.
- Toegang tot relevante tenant/omgevingen en licentieoverzichten (Microsoft 365).
- Locaties en functies waarvoor VOG vereist is; proces voor badge/toegang.
- Duurzaamheidsdoelstellingen van Gemeente (eventuele aanvullende KPI's).
- Afstemming survey-template CSAT en minimale steekproefgrootte.

#### Benodigde input: