

Risicoregister

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

Datum: 11/26/2025

Risicoregister – Raamovereenkomst Catering- en Horecadiensten voor Gemeente Middenstad (Project 1380) Opdrachtnemer: Uno Automatiseringsdiensten B.V. (ISO 9001 en ISO 27001) Doel en methodiek:

- Doel: actieve beheersing van kwaliteits-, continuïteits- en securityrisico's conform ISO 27001/9001 en ITIL, gericht op het halen van alle SLA/KPI's.
- Scoring: Kans en Impact op schaal 1 (laag) – 5 (zeer hoog). Score = Kans x Impact. Drempel: Score ≥ 12 = hoog; 8–11 = midden; ≤ 7 = laag.
- PDCA-borging per risico met SMART-maatregelen en aantoonbaar bewijs.

KPI-codes (selectie, incl. SLA's):

- KPI-A1 Beschikbaarheid kritieke systemen $\geq 99,8\%$ per maand (SLA)
- KPI-I1 Responstijd P1 < 30 min (SLA)
- KPI-I2 Oplostijd P1 < 4 uur (SLA)
- KPI-P1 Patch compliance: $\geq 95\%$ kritieke patches ≤ 14 dagen; $100\% \leq 30$ dagen
- KPI-M1 Monitoringdekking: 100% servers/endpoints gemonitord
- KPI-S1 EDR/AV-dekking: 100% endpoints met actuele agent; 0 kritieke alerts > 24 uur open
- KPI-B1 Back-up succesratio $\geq 99\%$; kwartaal hersteltest geslaagd
- KPI-C1 Change-succesratio $\geq 98\%$; 100% changes met back-out plan
- KPI-D1 Data residency: 100% verwerking binnen EU; 0 ongeautoriseerde transfers
- KPI-H1 24/7 bezetting: min. 2 medewerkers per dienst; rooster 8 weken vooruit
- KPI-R1 SLA-rapportage: binnen 5 werkdagen na maandsluiting gepubliceerd

Werkpakketten (W-xx): W-01 Monitoring & Alerting, W-02 Patch & Vulnerability, W-03 Incidentmanagement, W-04 Escalatie & Major Incident, W-05 Continuïteit/BCP-DR, W-06 EU Data & Privacy, W-07 Microsoft 365 Beheer, W-08 Endpoint Security (EDR/AV), W-09 Back-up & Restore, W-10 Change & Release, W-11 Capaciteit & Performance, W-12 Vendor & Contract, W-13 Rapportage & SLA, W-14 HR/VOG & 24/7 Roostering.

Bewijsbronnen (E-xx): E-01 ISO 27001/9001 certificaten; E-02 NOC/monitoring exports; E-03 Ticketing- en SLA-rapporten; E-04 SIEM/EDR-logs; E-05 BCP/DR-testverslagen; E-06 DPA/verwerkersregister; E-07 M365 Secure Score; E-08 Back-uprapporten; E-09 Change/CAB notulen; E-10 24/7 rooster- en bereikbaarheidslog.

Risicotabel

Risico	Kans	Impact	Score	Beheersmaatregel (PDCA, SMART)	Eigenaar	Status	Link KPI/W-xx	Residual Risk
1. SLA-breuk: beschikbaarheid < 99,8%	2 (20%)	5	10	P: Definieer kritieke services en failover binnen 10 werkdagen na start (CMDB en runbooks). D: Configureer actieve monitoring op alle kritieke componenten met automatische failover waar mogelijk voor 100% van scope binnen 30 dagen. C: Weekelijks availability-review; maandelijkse SLA-rapportage. A: Bij <99,8% twee maanden op rij, binnen 5 werkdagen CAPA en binnen 30 dagen implementatie. Bewijs: E-02, E-03, E-05.	Service Manager	Beheerst	KPI-A1; W-01, W-05, W-11	Wordt na maatregelen herbeoordeeld

Risico	Kans	Impact	Score	Beheersmaatregel (PDCA, SMART)	Eigenaar	Status	Link KPI/W-xx	Residual Risk
2. Te late P1-responstijd (>30 min)	3 (30%)	4	12	P: 24/7 escalatieschema en MIM-proces binnen 5 werkdagen gepubliceerd. D: NOC-auto-paging, parallelle alarmering (SMS/Teams/Phone) live binnen 10 dagen; target: 100% P1 alerting in 2 min. C: Maandelijkse audit van 10 P1-cases op responstijd. A: Bij overschrijding >2x/maand, hertraining en roosteraanpassing binnen 7 dagen. Bewijs: E-03, E-10.	Major Incident Manager	In uitvoering	KPI-I1; W-03, W-04, W-14	Wordt na maatregelen herbeoordeeld
3. P1 niet opgelost binnen 4 uur	2 (20%)	4	8	P: War-room procedure en technische swatlist binnen 10 dagen. D: Voor kritieke systemen 24/7 escalatie naar L3 en leveranciers binnen 15 min; back-out/rollback in runbooks. C: MTTR-trendrapport per maand. A: Bij MTTR > doel 2 maanden, root cause workshop binnen 5 werkdagen; implementatie binnen 20 werkdagen. Bewijs: E-03, E-09.	Incident Manager	Beheerst	KPI-I2; W-03, W-04, W-10	Wordt na maatregelen herbeoordeeld

Risico	Kans	Impact	Score	Beheersmaatregel (PDCA, SMART)	Eigenaar	Status	Link KPI/W-xx	Residual Risk
4. Patch backlog en kwetsbaarheden	3 (30%)	4	12	P: Maandelijke patchkalender en risicogestuurde prioritering (CVSS ≥ 7 binnen 14 dagen) vastgesteld. D: Uitrol naar $\geq 95\%$ binnen 14 dagen en 100% binnen 30 dagen; uitzonderingen via CAB. C: Weekelijkse compliance-rapportage; maandelijke vuln-scan. A: Bij $< 95\%$, binnen 5 werkdagen inhaalplan; blokkeren changes zonder patchstatus. Bewijs: E-02, E-04.	Lead Patchmanagement	In uitvoering	KPI-P1; W-02, W-10	Wordt na maatregelen herbeoordeeld
5. Security-incident (malware/ransomware)	2 (20%)	5	10	P: 100% EDR-dekking en hardening-baselines binnen 30 dagen; phishing-simulaties kwartaal. D: 24/7 detect & respond; containment < 30 min, forensics gestart < 2 uur. C: Maandelijks SOC-kpi's en incidentpostmortems. A: Bij SEV1-incident, binnen 72 uur verbeterplan en binnen 30 dagen maatregelen doorgevoerd. Bewijs: E-04, E-03.	CISO	Beheerst	KPI-S1, KPI-I2; W-08, W-03	Wordt na maatregelen herbeoordeeld
6. Data buiten EU verwerkt (non-compliance)	1 (10%)	5	5	P: Verwerkersregister en datastromenmapping binnen 15 werkdagen afgerond; DPA's gevalideerd. D: Geofencing en datalocatiepolitie in M365/Azure en back-up. C: Kwartaalreview verwerkers; steekproeven logs. A: Onregelmatigheid \rightarrow binnen 24 uur containment en DPIA-update binnen 10 dagen. Bewijs: E-06, E-07.	Privacy Officer	Beheerst	KPI-D1; W-06, W-07, W-09	Wordt na maatregelen herbeoordeeld

Risico	Kans	Impact	Score	Beheersmaatregel (PDCA, SMART)	Eigenaar	Status	Link KPI/W-xx	Residual Risk
7. Monitoringdekking/false negatives	3 (30%)	4	12	P: Monitoring-SOP en device-onboarding checklijst binnen 5 dagen. D: 100% assets in CMDB met monitoring binnen 30 dagen; alert-tuning om ruis ≤ 15% te houden. C: Wekelijkse missende-sensoren scan; maandelijkse alert-kwaliteitsreview. A: Gaps >0% → herstel binnen 48 uur; structureel → tool/regel update binnen 10 dagen. Bewijs: E-02.	NOC Lead	In uitvoering	KPI-M1; W-01, W-11	Wordt na maatregelen herbeoordeeld
8. Onsuccesvolle change met verstoring	2 (20%)	4	8	P: CAB-kalender en risicoclassificatie; 100% changes met test- en back-out plan. D: Pilots en onderhoudsvensters; change freeze tijdens piekuren. C: Maandelijkse change-succesratio en back-out analyse. A: Succesratio <98% → binnen 5 dagen extra QA-gates en kennisupdate; herbeoordeling na 30 dagen. Bewijs: E-09, E-03.	Change Manager	Beheerst	KPI-C1; W-10	Wordt na maatregelen herbeoordeeld
9. Onvoldoende 24/7 bezetting (ziekte/uitval)	3 (30%)	4	12	P: Rooster 8 weken vooruit met min. 2 FTE per dienst; pool met 20% overcapaciteit. D: Cross-train op P1-runbooks; standby-contracten. C: Weekelijkse roostercontrole; maandelijks uitvalrapport. A: Bij gaten → binnen 24 uur herdubbeling; binnen 14 dagen aanvulling pool. Bewijs: E-10.	HR & Operations Lead	In uitvoering	KPI-H1; W-14	Wordt na maatregelen herbeoordeeld
10. Derdepartijenstoring (ISP/Microsoft)	3 (30%)	4	12	P: Leveranciers-SLA's vastgelegd; multi-provider waar zinvol. D: Actieve	Vendor Manager	Beheerst	KPI-A1, KPI-I2;	Wordt na maatregelen herbeoordeeld

Risico	Kans	Impact	Score	Beheersmaatregel (PDCA, SMART)	Eigenaar	Status	Link KPI/W-xx	Residual Risk
				synthetische tests en failover; escalatiepaden en creditsbewaking. C: Maandelijks vendor review; kwartaal service review met opdrachtgever. A: Meervoudige SLA-schending → binnen 10 dagen mitigatieplan of contractswitch-case. Bewijs: E-12-analoge logs via E-03/E-09.			W-12, W-01	
11. BCP/DR faalt of niet getest	2 (20%)	5	10	P: BCP/DR-scenario's en RTO/RPO per dienst vastgesteld binnen 20 dagen. D: Jaarlijkse volledige DR-test en kwartaal tabletop; kritieke backups 3-2-1. C: Testresultaten en gap-lijst per kwartaal. A: Failures → binnen 10 dagen CAPA; binnen 45 dagen her-test. Bewijs: E-05, E-08.	BCP Manager	In uitvoering	KPI-B1, KPI-A1; W-05, W-09	Wordt na maatregelen herbeoordeeld
12. M365-misconfiguratie (security/continuïteit)	2 (20%)	4	8	P: Baselines (CIS/Microsoft) en Secure Score ≥ 75 binnen 30 dagen. D: Conditional Access en DLP policies; change via CAB. C: Maandelijks Secure Score-rapportage; kwartaalconfig-audit. A: Score < 75 → maatregelen binnen 10 dagen; kritieke bevinding → patch binnen 72 uur. Bewijs: E-07, E-09.	M365 Lead	Beheerst	KPI-D1, KPI-S1; W-07, W-10	Wordt na maatregelen herbeoordeeld
13. Escalatieprocedure niet gevolgd	2 (20%)	3	6	P: MIM-runsheets en RACI gedeeld binnen 5 dagen. D: Kwartaaltraining; escalatie-simulatietest 2x per jaar. C: Post-incident review op escalatiepaden. A: Afwijking → coaching binnen 5 werkdagen; her-simulatie binnen	Major Incident Manager	Beheerst	KPI-I1, KPI-I2; W-04	Wordt na maatregelen herbeoordeeld

Risico	Kans	Impact	Score	Beheersmaatregel (PDCA, SMART)	Eigenaar	Status	Link KPI/W-xx	Residual Risk
				14 dagen. Bewijs: E-03.				
14. Onvolledige of late SLA-rapportage	2 (20%)	3	6	P: Rapportagesjabloon en databronnen vastgelegd; automatisering dashboards. D: Publicatie binnen 5 werkdagen na maandsluiting. C: Interne QA op 100% rapporten. A: Te laat/onvolledig → binnen 3 werkdagen correctie; structureel → procesupdate binnen 10 dagen. Bewijs: E-03.	Service Manager	Beheerst	KPI-R1; W-13	Wordt na maatregelen herbeoordeeld
15. VOG/HR-compliance niet op orde	2 (20%)	3	6	P: VOG-verplichting in onboarding-checklist; register bijgehouden. D: 100% medewerkers met VOG vóór toegang; jaarlijkse hercontrole. C: Kwartaal-audit personeelstoegang. A: Non-compliance → toegang binnen 24 uur ingetrokken; VOG binnen 10 werkdagen geregeld. Bewijs: E-01, E-10.	HR & Compliance Lead	Beheerst	KPI-H1; W-14	Wordt na maatregelen herbeoordeeld
16. On-site netwerkproblemen bij opdrachtgever	3 (30%)	4	12	P: Site assessment en minimale netwerkeisen binnen 15 dagen vastgesteld. D: Proactieve monitoring WAN/LAN; 4G/5G-fallback voor kritieke locaties. C: Maandelijkse capacity-trends; incidentcorrelatie met netwerk. A: Structurele issues → advies en verbeterplan binnen 10 werkdagen; hercontrole na 30 dagen. Bewijs: E-02, E-03.	Capaciteitsmanager	In uitvoering	KPI-A1, KPI-I2; W-11, W-12	Wordt na maatregelen herbeoordeeld

Toelichting kruisverbanden W-xx ↔ KPI ↔ Risico ↔ Bewijs:

- Voorbeeld: Risico 4 (patch backlog) ↔ W-02 Patchmanagement ↔ KPI-P1 (patch compliance) ↔ Bewijs E-02/E-04 (monitoring/vuln/EDR-logs).
- Voorbeeld: Risico 1 (beschikbaarheid) ↔ W-01 Monitoring & W-05 BCP ↔ KPI-A1 ↔ Bewijs E-02/E-05.
- Voorbeeld: Risico 6 (EU-data) ↔ W-06 & W-07 ↔ KPI-D1 ↔ Bewijs E-06/E-07.

PDCA-borging:

- Plan: beleid, baselines, planning en RACI vastgesteld met doorlooptijden (5–30 dagen na start).
- Do: uitvoering met concrete targets (bijv. 100% monitoringdekking, 95% patches ≤ 14 dagen).
- Check: vaste reviewcycli (wekelijks/maandelijks/kwartaal) en KPI-rapportage.
- Act: drempels en termijnen voor CAPA (correctieve/preventieve acties) en her-test.

Benodigde input: