Risicoregister

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

Datum: 11/19/2025

Risico’s – Risicoregister Uno Automatiseringsdiensten B.V. voor Raamovereenkomst Catering- en Horecadiensten voor Gemeente Middenstad (Project 1380)

Scoringsmethodiek:

- Kans: 1 (zeer laag) – 5 (zeer hoog)
- Impact: 1 (beperkt) – 5 (kritiek op dienstverlening/continuïteit)
- Score = Kans x Impact. Risico’s met score ≥12 krijgen versnelde opvolging via de maandelijkse PDCA-review.

KPI-overzicht (sturing en bewijs):

- KPI-01 Beschikbaarheid kritieke systemen ≥ 99,8% per maand (SLA)
- KPI-02 Responstijd P1 < 30 min (SLA)
- KPI-03 Oplostijd P1 < 4 uur (SLA)
- KPI-04 Patch compliance kritisch ≥ 95% binnen 14 dagen
- KPI-05 Back-up succesratio ≥ 99%, hersteltests per kwartaal
- KPI-06 Aantal security-incidenten met dataverlies = 0
- KPI-07 Changesucces ≥ 98% zonder ongeplande downtime
- KPI-08 Monitoring coverage = 100% van in-scope assets
- KPI-09 EU data residency = 100%
- KPI-10 CSAT ≥ 8,0/10
- KPI-11 SLA-rapportage tijdig 100% (uiterlijk 5e werkdag maand)
- KPI-12 Kritieke kwetsbaarheden verholpen binnen 7 dagen ≥ 95%

Werkpakketten (W-xx) voor uitvoering:

- W-01 24/7 NOC & monitoring
- W-02 Incidentmanagement (ITIL) P1–P3
- W-03 Patch- en changemanagement
- W-04 Continuïteit/BCP & DR-oefeningen
- W-05 Security & compliance (ISO 27001)
- W-06 Data residency EU-borging
- W-07 Servicedesk & escalaties (ITIL)
- W-08 Vendor- en contractmanagement
- W-09 Capaciteit- & performancemanagement
- W-10 Onboarding & kennisborging
- W-11 Governance & rapportage (SLA/CSAT)
- W-12 Microsoft 365 beheer & security
- W-13 Endpoint/EDR beheer
- W-14 Documentatie & bewijsvorming

Bewijsbronnen (controleerbaar):

- SLA- en KPI-rapportages (W-11), changekalender en CAB-notulen (W-03), monitoring- en incidentlogs (W-01/W-02), BCP/DR-testverslagen (W-04), ISO 27001/9001 certificaten (W-05), verwerkersovereenkomst + DPIA’s (W-06), patch- en vulnerability-rapportages (W-03), back-up en restore-rapporten (W-04), CSAT-enquêtes (W-11), VOG-register en toegangsmatrix (W-05).

Risicoregister

Risico	Kans	Impact	Score	Beheersmaatregel (SMART, PDCA + Bewijs)	Eigenaar	Status	Link KPI/W-xx	Residual Risk
1. Onvoldoende beschikbaarheid (<99,8%) door storingen	3	5	15	Plan: definieer kritieke services en HA-architectuur met RTO≤4u/RPO≤1u voor scope, gereed 30 dagen na start. Do: 24/7 monitoring, auto-remediation, failoverprocedures; implementatie binnen 45 dagen. Check: maandelijkse beschikbaarheidsrapporten; drempel alert bij 99,9%→ root cause. Act: binnen 10 werkdagen na incident: PIR	Service Delivery Manager	Actief	KPI-01, KPI-11 / W-01, W-04, W-11	Wordt na maatregelen herbeoordeeld

Risico	Kans	Impact	Score	Beheersmaatregel (SMART, PDCA + Bewijs)	Eigenaar	Status	Link KPI/W-xx	Residual Risk
				en structurele maatregel. Bewijs: SLA-rapport, PIR, monitoringlogs.				
2. Responstijd P1 > 30 min	2	5	10	Plan: definieer P1-triggers en paging-schema 24/7; hard in SLA-tool, gereed binnen 14 dagen. Do: war room-protocol en first-call ownership. Check: wekelijkse steekproef 10 P1/P2 tickets. Act: hertraining binnen 5 werkdagen bij afwijking; escalatielijst bijgewerkt binnen 24u. Bewijs: incidentlog, on-call rooster.	Teamlead Servicedesk	Onder controle	KPI-02 / W-02, W-07	Wordt na maatregelen herbeoordeeld
3. Oplostijd P1 > 4 uur	3	4	12	Plan: runbooks voor top-10 P1-scenario's, vendor-EAs met 1u response, afgerond binnen 30 dagen. Do: swarming model, parallel vendor-escalatie. Check: maandelijkse TTR-analyse. Act: bij TTR>4u: probleemrecord en change binnen 15 werkdagen. Bewijs: TTR-rapport, CAB-notulen.	Incident Manager	Actief	KPI-03, KPI-07 / W-02, W-03, W-08	Wordt na maatregelen herbeoordeeld
4. Patchachterstand en kwetsbaarheden	3	5	15	Plan: patchbeleid: kritisch ≤14 dagen; VA-scan 2-wekelijks; gereed dag 10. Do: change windows 2x per maand; emergency patching binnen 48u. Check: patch compliance-rapport wekelijks. Act: non-compliance >5% → escalatie naar CAB binnen 5 werkdagen. Bewijs: VA-rapporten, patchdashboard.	Change Manager	Actief	KPI-04, KPI-12 / W-03	Wordt na maatregelen herbeoordeeld
5. Data buiten EU verwerkt	2	5	10	Plan: datastromenkaart en leveranciersreview; EU-only contractclausules binnen 30 dagen. Do: geo-locking en DLP in M365; logging op data-export. Check: kwartaalreview verwerkersovereenkomsten. Act: afwijking → binnen 24u blokkeren, DPIA-update binnen 5 werkdagen. Bewijs: verwerkersovereenkomst, DPIA, configuratie-screens.	Security Officer (CISO)	Onder controle	KPI-09, KPI-06 / W-05, W-06, W-12	Wordt na maatregelen herbeoordeeld
6. Onvoldoende monitoring coverage (blinde vlekken)	3	4	12	Plan: CMDB-baseline + auto-discovery; 100% asset coverage binnen 30 dagen. Do: healthchecks en synthetic probes; alert-	NOC Lead	In uitvoering	KPI-08 / W-01, W-14	Wordt na maatregelen herbeoordeeld

Risico	Kans	Impact	Score	Beheersmaatregel (SMART, PDCA + Bewijs)	Eigenaar	Status	Link KPI/W-xx	Residual Risk
				tuning binnen 7 dagen per nieuwe asset. Check: maandelijkse gap-analyse CMDB vs. monitor. Act: gaps >0 → binnen 5 werkdagen ingeregeld. Bewijs: CMDB-export, monitoringcoverage-rapport.				
7. Capaciteitsproblemen (CPU/RAM/storage/netwerk)	3	4	12	Plan: drempelwaarden (80% early, 90% critical) en capaciteitsrapportage maandelijks. Do: trendanalyse en scaling-changes per kwartaal. Check: maandelijkse review met opdrachtgever. Act: capacity breach → binnen 10 werkdagen mitigatieplan. Bewijs: performancedashboards, capacity reports.	Capacity Manager	Actief	KPI-01 / W-09, W-03, W-11	Wordt na maatregelen herbeoordeeld
8. Ongecontroleerde changes veroorzaken verstoringen	2	5	10	Plan: CAB-kalender 2-wekelijks, risicobeoordeling; no change window voor piekperiodes van opdrachtgever. Do: standaard changes geautomatiseerd; non-std via CAB. Check: changesucces-rate maandelijks. Act: <98% succes → herzien build/runbook binnen 10 werkdagen. Bewijs: CAB-notulen, changelog.	Change Manager	Onder controle	KPI-07, KPI-11 / W-03, W-11	Wordt na maatregelen herbeoordeeld
9. Continuïteit/BCP faalt; herstel niet tijdig	2	5	10	Plan: BIA en BCP afgestemd met gemeente; RTO/RPO per systeem, afgerond binnen 45 dagen. Do: DR-test 2x per jaar, back-up daily, restore test per kwartaal. Check: testverslagen en afwijkingen. Act: tekortkomingen opgelost binnen 20 werkdagen. Bewijs: BCP, DR-testverslag, backup logs.	Continuity Manager	Actief	KPI-05, KPI-01 / W-04	Wordt na maatregelen herbeoordeeld
10. Endpointbeveiliging tekort (EDR), ransomware	3	5	15	Plan: EDR op 100% endpoints; policy “isolate on detect” binnen 30 dagen. Do: 24/7 SOC-triage, phishing-simulaties per kwartaal. Check: maandelijks EDR coverage en MTTD/MTTR. Act: incident → containment <1u, volledige eradication	Security Officer (CISO)	Actief	KPI-06, KPI-08, KPI-12 / W-13, W-05	Wordt na maatregelen herbeoordeeld

Risico	Kans	Impact	Score	Beheersmaatregel (SMART, PDCA + Bewijs)	Eigenaar	Status	Link KPI/W-xx	Residual Risk
				binnen 24u; lessons learned binnen 10 werkdagen. Bewijs: EDR-rapporten, incident-PIR.				
11. Leveranciers leveren niet conform (ketenrisico)	3	4	12	Plan: underpinning contracts met SLA's; escalatieniveaus vastgelegd binnen 30 dagen. Do: vendor QBR's per kwartaal, performance tracking. Check: contract-KPI's maandelijks. Act: bij non-performance: service credit of exit-plan binnen 20 werkdagen. Bewijs: contracten, QBR-notulen.	Vendor Manager	Actief	KPI-03, KPI-01 / W-08, W-11	Wordt na maatregelen herbeoordeeld
12. Escalaties en communicatie niet tijdig/duidelijk	2	4	8	Plan: RACI, escalatiematrix en communicatiesjablonen binnen 14 dagen. Do: war room-communicatie met update-cadans (bij P1: elke 30 min). Check: CSAT en post-incident survey. Act: communicatieklachten → aanpassing sjabloon en training binnen 10 werkdagen. Bewijs: escalatielijst, updates in ticket.	Service Delivery Manager	Onder controle	KPI-02, KPI-10, KPI-11 / W-07, W-11	Wordt na maatregelen herbeoordeeld
13. Privacy-incident/datalek of VOG-non-compliance	2	5	10	Plan: DPIA's en dataclassificatie binnen 45 dagen; VOG-controle vooraf toegang. Do: meldprocedure AVG (≤72u); rechtenbeheer per functie. Check: kwartaal-audit toegang en VOG-register. Act: afwijking → direct toegang intrekken, datalek melden binnen 24u en oorzaken oplossen binnen 10 werkdagen. Bewijs: VOG-register, auditrapporten.	Privacy Officer (FG)	Actief	KPI-06, KPI-09 / W-05, W-06	Wordt na maatregelen herbeoordeeld
14. Onboarding onvolledig → vertraging en fouten	3	3	9	Plan: 30-60-90 dagen onboardingsplan incl. CMDB-vulling, klaar dag 7. Do: kennisoverdracht-sessies en documentatie W-14. Check: wekelijkse voortgang en acceptatiecriteria. Act: achterstand >10% → resourcebijsturing binnen 5 werkdagen. Bewijs: onboarding-checklist, CMDB-status.	Projectmanager Onboarding	In uitvoering	KPI-08, KPI-11 / W-10, W-14	Wordt na maatregelen herbeoordeeld
15. M365-misconfiguraties (phishing/uitval)	3	4	12	Plan: M365 baseline (MFA, CA, DKIM/DMARC, Safe	M365 Lead	Actief	KPI-06,	Wordt na maatregelen

Risico	Kans	Impact	Score	Beheersmaatregel (SMART, PDCA + Bewijs)	Eigenaar	Status	Link KPI/W-xx	Residual Risk
				Links/Attachments) binnen 30 dagen. Do: hardening en secure score ≥ 80 binnen 60 dagen. Check: maandelijkse Secure Score en auditlogs. Act: afwijking → policy-fix binnen 5 werkdagen; awarenesscampagnes per kwartaal. Bewijs: Secure Score-rapporten, auditlogs.			KPI-12, KPI-10 / W-12, W-05	herbeoordeeld

Toelichting op knock-outs en musts (kruisverbanden):

- ISO 27001/9001 (KO) en ITIL-processen (must) zijn geborgd via W-05 en W-07; bewijs via certificaten en procesaudits. Deze mitigeren risico's 4, 5, 8, 13 en 12.
- 24/7 bereikbaarheidsdienst (KO) en P1-responstijd 30 min (must) zijn geborgd via W-01/W-02; mitigeren risico's 2 en 3; bewijs via incidentlogs en on-call roosters.
- Beschikbaarheid 99,8% (must) via W-01/W-04/W-09; mitigeren risico's 1 en 7; bewijs via SLA-rapporten.
- Monitoring & patchmanagement (must) via W-01/W-03/W-14; mitigeren risico's 4 en 6; bewijs via dashboards en changelog.
- EU-dataverwerking (must) via W-06; mitigeren risico 5; bewijs verwerkersovereenkomsten/DPIA's.
- Escalatieprocedure en BCP (must) via W-07/W-04; mitigeren risico's 3, 9 en 12; bewijs via escalatiematrix, BCP en DR-testverslagen.
- VOG (must) via W-05; mitigeren risico 13; bewijs VOG-register.
- Proactieve monitoring endpoints en M365-support (must) via W-13/W-12; mitigeren risico's 10 en 15; bewijs EDR- en Secure Score-rapporten.

PDCA-borging (procesniveau):

- Plan: jaarlijkse strategie- en risicoreview met Gemeente Middenstad in Q4; KPI-doelen bevestigd in SLA addendum.
- Do: uitvoering W-01 t/m W-14 met vaste cadence (dagelijks/wekelijkse operationele ritmes; maandelijkse rapportage).
- Check: maandelijkse SLA-review (KPI-rapport, PIR's, auditbevindingen) en kwartaal-QBR met verbeterportfolio.
- Act: verbeteringen met eigenaar, budget en deadline (standaard ≤ 30 werkdagen) opgenomen in verbeterlog; opvolging via CAB/QBR.

Benodigde input:

- Definitieve lijst kritieke systemen en scope (incl. locaties en openingstijden).
- Escalatielijst met contactpersonen en autorisaties (24/7).
- Changevensters en blackout-perioden van Gemeente Middenstad.
- Huidige leveranciers, contracten en contactpunten voor ketenafhankelijkheden.
- Bestaande BCP/BIA, prioritaire processen en RTO/RPO-wensen.
- M365 tenantinformatie en benodigde adminconsents.
- Data residency voorkeuren (EU-regio's) en bestaande verwerkersovereenkomsten.
- Securitybeleid, DPIA's en eisen t.a.v. logging/bewaring.
- Vereisten rond VOG-proces en toegang tot locaties.
- Gewenst format en ontvangers voor SLA-rapportage (deadline: 5e werkdag).

Benodigde input: