Risicoregister

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

Datum: 11/5/2025

Risico’s – Risicoregister (PDCA, SMART, KPI/W-xx-kruisverband)

Doel en scope Dit risicoregister borgt dat Uno Automatiseringdiensten B.V. de SLA’s en must-haves van de raamovereenkomst naleeft: beschikbaarheid ≥ 99,8%, responstijd ≤ 1 uur, oplostijd ≤ 4 uur (kritisch), 24/7 monitoring, gebruik van Azure NL-datacenters en periodieke securityrapportage. We hanteren een 1–5 schaal voor Kans (K) en Impact (I); Score = K × I. Beheersmaatregelen zijn SMART en PDCA-gebaseerd, met directe koppeling naar KPI’s, Werkpakketten (W-xx) en Bewijs (B-xx).

KPI-overzicht (KPI-xx)

- KPI-01 Beschikbaarheid diensten ≥ 99,8% per maand.
- KPI-02 Responstijd P1-incident ≤ 1 uur (gemeten 24/7).
- KPI-03 Oplostijd P1-incident ≤ 4 uur.
- KPI-04 Beveiligingsincidenten: melding binnen 24 uur; maandrapportage 100% tijdig.
- KPI-05 Change-succesratio ≥ 95% per maand.
- KPI-06 Onderhoud: ≥ 2 geplande vensters/jaar; 100% ≥ 10 werkdagen vooraf gecommuniceerd.
- KPI-07 Monitoringdekking: 100% in-scope assets met actieve agents/alerts.
- KPI-08 Back-up succesrate ≥ 98%; kwartaal restore-test geslaagd.
- KPI-09 Patchcompliance: kritieke patches binnen 14 dagen ≥ 95%.
- KPI-10 Rapportage: maandrapportages uiterlijk werkdag 5, 100% compleet.
- KPI-11 Duurzaamheid: -10% CO2 per gebruiker/jaar (scope IT-infra), rapportage per kwartaal.
- KPI-12 Continuïteit: jaarlijkse DR-test geslaagd; RTO ≤ 4 uur, RPO ≤ 15 min.
- KPI-13 Klanttevredenheid (CSAT) ≥ 8,0 per kwartaal.

Werkpakketten (W-xx)

- W-01 Transitie & onboarding
- W-02 24/7 Monitoring & NOC
- W-03 Incident- & Major Incident Management
- W-04 Problem Management
- W-05 Change & Release Management
- W-06 Capaciteit- & Performance Management
- W-07 Security Operations (SOC/SIEM)
- W-08 Backup & Disaster Recovery
- W-09 Rapportage & Governance (SLA/EMVI)
- W-10 Vendor- & Azure Service Management
- W-11 Compliance & Audits (ISO 27001, VOG)
- W-12 Service Desk & Field Support
- W-13 Onderhoudsvensters & Communicatie
- W-14 Duurzaamheid & FinOps

Bewijsbronnen (B-xx)

- B-01 ISO 27001-certificaat en Verklaring van Toepasselijkheid
- B-02 VOG-overzicht personeel en screeningskalender
- B-03 Maandelijkse SLA/CSAT-rapportage (Power BI)
- B-04 Azure Monitor/Log Analytics dashboards + alertlogs
- B-05 Incident-/Major Incident-registraties (ITSM)
- B-06 Change-kalender en CAB-notulen
- B-07 Security-incidentenregister en SIEM-export
- B-08 Patch- en hardening-rapportages
- B-09 Backup-logs en kwartaal restore-testverslagen
- B-10 DR-testrapport, BIA/BCP
- B-11 Azure Service Health-exports en vendor-SLA’s
- B-12 Duurzaamheidsrapport (CO2/energie), FinOps-dashboards

Risicoregister (Kans/Impact 1–5; Score = K×I)

Risico	Kans	Impact	Score	Beheersmaatregel (SMART + PDCA)	Eigenaar	Status	Link KPI/W-xx	Residual Risk
1. Beschikbaarheid < 99,8% door configuratie- of platformfouten	3	5	15 (H)	Plan: Implementeren HA-referentiearchitectuur in Azure NL (AZ zones) voor alle kritieke workloads, deadline 30 dagen na start. Do: 24/7 monitoring op SLO's en auto-healing (week 2), change freeze tijdens piekevents. Check: Maandelijkse availability review op KPI-01. Act: Root cause in Problem backlog binnen 5 werkdagen en preventieve change binnen 15 werkdagen. Bewijs: B-04, B-03, B-06.	Technical Lead Azure	Actief	KPI-01; W-02, W-05, W-06; B-03, B-04	Wordt na maatregelen herbeoordeeld
2. Responstijd P1 > 1 uur	2	5	10 (M)	Plan: P1-paging via SIEM/NOC met escalatie binnen 5 min; dekkingsrooster 24/7 gereviewd wekelijks. Do: War-room procedure (bridge in 10 min). Check: Weekrapport P1-responstijden. Act: Opleiding en herroostering binnen 7 dagen bij afwijking. Bewijs: B-05, B-04.	NOC Lead	Actief	KPI-02; W-02, W-03; B-04, B-05	Wordt na maatregelen herbeoordeeld
3. Oplostijd P1 > 4 uur	3	4	12 (M)	Plan: Runbooks voor top-10 storingen gereed binnen 20 dagen; vendor re-escalatie binnen 30 min. Do: Swarm support met L2/L3 on-call. Check: Post-incident review binnen 48 uur. Act: Runbook-update binnen 5 dagen; training binnen 10 dagen. Bewijs: B-05, B-06.	Service Manager	Actief	KPI-03; W-03, W-04, W-10; B-05	Wordt na maatregelen herbeoordeeld
4. Capaciteitsproblemen tijdens piekbelasting (evenementen)	3	4	12 (M)	Plan: Capaciteitsmodel en auto-scaling policies opleveren binnen 30 dagen; piekkalender afstemmen maandelijks. Do: Load tests per kwartaal; tijdelijk schalen ≥ 24 uur vooraf. Check: KPI-01/06 vs. piekkalender. Act: Aanpassen thresholds binnen 5 dagen na incident. Bewijs: B-04, B-03.	Capacity Manager	Actief	KPI-01, KPI-06; W-06, W-13; B-04	Wordt na maatregelen herbeoordeeld
5. Ongepland onderhoud of conflict met bedrijfsvensters	2	4	8 (M)	Plan: Onderhoudskalender H1/H2 met 10 werkdagen aankondiging; minimaal 2 vensters/jaar. Do: Change met rollbackplan; communicatie via afgesproken kanalen. Check: Maandelijkse compliance op	Change Manager	Actief	KPI-06; W-05, W-13; B-06	Wordt na maatregelen herbeoordeeld

Risico	Kans	Impact	Score	Beheersmaatregel (SMART + PDCA)	Eigenaar	Status	Link KPI/W-xx	Residual Risk
				KPI-06. Act: Verbeterde planning/backup-window binnen 10 dagen bij afwijking. Bewijs: B-06, B-03.				
6. Security-incident (malware/phishing)	3	5	15 (H)	Plan: SOC use-cases top-20, MFA/Conditional Access verplicht; incidentmelding ≤ 24 uur. Do: EDR uitgerold 100% binnen 30 dagen; phishing-simulaties per kwartaal. Check: Maandrapport KPI-04, patch KPI-09. Act: Hardening-update binnen 10 dagen; awareness-training binnen 15 dagen. Bewijs: B-07, B-08, B-03.	CISO	Actief	KPI-04, KPI-09; W-07, W-11; B-07	Wordt na maatregelen herbeoordeeld
7. Dataresidentie/compliance (niet-NL datacenter)	2	5	10 (M)	Plan: Policy enforce “Region = NL” op alle resources; maandelijkse audit. Do: Azure Policy/Blueprints toepassen binnen 15 dagen. Check: Auditrapport; afwijkingen = 0. Act: Correctie binnen 24 uur bij afwijking; CAB-evaluatie. Bewijs: B-01, B-04.	Compliance Officer	Actief	KPI-10; W-10, W-11; B-01, B-04	Wordt na maatregelen herbeoordeeld
8. Backup/restore faalt	2	5	10 (M)	Plan: 3-2-1 back-up strategie; dagelijkse jobs; kwartaal restore-test. Do: Monitoring backup jobs en automatische retry. Check: KPI-08 maandelijks; DR-test jaarlijks. Act: Aanpassen retentie/vensters binnen 5 dagen na fout; extra test binnen 7 dagen. Bewijs: B-09, B-10.	DR & Backup Lead	Actief	KPI-08, KPI-12; W-08; B-09, B-10	Wordt na maatregelen herbeoordeeld
9. Rapportage niet tijdig/onvolledig	2	3	6 (L)	Plan: Rapportagesjablonen en datamapping gereed binnen 15 dagen; publicatie op werkdag 5. Do: Geautomatiseerde extracten uit ITSM/SIEM. Check: KPI-10 naleving maandelijks. Act: Datanaleving-correctie binnen 3 dagen; data-eigenaar aangewezen. Bewijs: B-03.	Governance Lead	Actief	KPI-10; W-09; B-03	Wordt na maatregelen herbeoordeeld
10. Wijzigingen veroorzaken verstoringen (lage change-succesratio)	3	4	12 (M)	Plan: Risk-based CAB, pre-prod tests verplicht; succesratio ≥ 95%. Do: Canary/blue-green waar mogelijk. Check: KPI-05; post-implementation review	Change Manager	Actief	KPI-05; W-05; B-06	Wordt na maatregelen herbeoordeeld

Risico	Kans	Impact	Score	Beheersmaatregel (SMART + PDCA)	Eigenaar	Status	Link KPI/W-xx	Residual Risk
				binnen 48 uur. Act: Releaseproces aanpassen binnen 10 dagen; extra testcases toevoegen. Bewijs: B-06.				
11. Derdepartij uitval (Azure-regio/SAAS)	2	5	10 (M)	Plan: Multi-AZ, alternatieve regio warm-standby voor kritieke apps; vendor-escalaties binnen 30 min. Do: Failover-oefening 2x/jaar. Check: KPI-01, KPI-12; vendor-SLA reviews. Act: Architectuuraanpassing binnen 20 dagen na major outage. Bewijs: B-11, B-10.	Vendor Manager	Actief	KPI-01, KPI-12; W-10, W-08; B-11	Wordt na maatregelen herbeoordeeld
12. Inzet medewerker zonder geldige VOG	1	5	5 (L)	Plan: VOG-check vóór inzet, register en alerts 30 dagen voor vervaldatum. Do: Toegangsbeheer gekoppeld aan VOG-status. Check: Maandelijkse audit; afwijking = 0. Act: Directe offboarding en vervanging binnen 24 uur. Bewijs: B-02.	HR & Security Officer	Actief	KPI-10; W-11; B-02	Wordt na maatregelen herbeoordeeld
13. Scope creep en ongeautoriseerde wijzigingen	3	3	9 (M)	Plan: Duidelijke RACI en Change type Standard/Normal/Emergency; autorisatie vereist. Do: Change templates inclusief impactanalyse en kosten. Check: Maandelijkse scope-review in governance. Act: Backlogherprioritering binnen 5 werkdagen; wijzigingsverzoek formaliseren. Bewijs: B-06, B-03.	Service Manager	Actief	KPI-05, KPI-10; W-05, W-09; B-06	Wordt na maatregelen herbeoordeeld
14. Duurzaamheidsdoelen niet gehaald	2	3	6 (L)	Plan: FinOps- en CO2-baseline binnen 30 dagen; reductiedoel -10% jaar 1. Do: Rightsizing/reserveringen; cold-tier storage; groene regions (NL). Check: Kwartaalrapport KPI-11. Act: Nieuwe optimalisaties binnen 30 dagen bij afwijking. Bewijs: B-12.	Sustainability Lead	Actief	KPI-11; W-14; B-12	Wordt na maatregelen herbeoordeeld

Toelichting PDCA en governancestructuur

- Plan: beleid, architectuur en processen vooraf vastgesteld en gedocumenteerd (W-01, W-05, W-11).
- Do: uitvoering via 24/7 NOC/SOC, ITSM-procedures en geautomatiseerde tooling (W-02, W-03, W-07).
- Check: dashboards, audits en rapportages per week/maand/kwartaal (KPI-01 t/m KPI-13; B-03 t/m B-12).
- Act: verbetermaatregelen met doorlooptijd en eigenaar, geborgd in Problem/Change backlog en CAB (W-04, W-05, W-09).

KO-compliance

- ISO 27001: geborgd via W-11; bewijs B-01 (geldig certificaat). Jaarlijkse interne audits, management review en externe audit.

- VOG: geborgd via W-11/HR-proces; bewijs B-02. Toegangsrechten zijn gekoppeld aan VOG-status.

Stakeholder- en escalatiemodel

- Operationele escalatie: NOC Lead (15 min), Service Manager (30 min), CISO/Technical Lead (60 min).
- Governance: maandelijkse SLA-review, kwartaal MT-review met verbeterplan.

Kruisverbanden samengevat

- W-xx → KPI's: elk werkpakket heeft minimaal één KPI (bijv. W-02 ↔ KPI-02/07; W-08 ↔ KPI-08/12).
- KPI's → Bewijs: iedere KPI heeft een vaste bewijsbron (bijv. KPI-01 ↔ B-04/B-11; KPI-10 ↔ B-03).
- Risico's → W/KPI/B: per risico vastgelegd in de tabel (laatste kolom en in de maatregel).

Continu verbeteren (SMART)

- Targets conform KPI's, meetfrequentie maandelijks/kwartaal.
- Afwijkingen > 5% op KPI-01/02/03 leiden tot een corrigerende maatregel binnen 10 werkdagen en herbeoordeling in CAB.
- Jaarlijkse herijking van risico's en KPI's met de opdrachtgever en verwerking in het Plan van Aanpak en Risicodossier.

Benodigde input: