Risicoregister

Digital Ease B.V. — Raamovereenkomst Catering- en Horecadiensten voor Gemeente Middenstad

Datum: 12/8/2025

Risicoregister – Raamovereenkomst Catering- en Horecadiensten voor Gemeente Middenstad (referentie: GV-IT-2026-001) – Digital Ease B.V.

Toelichting en aanpak

- Doel: het structureel beheersen van contract- en uitvoeringsrisico's die de beschikbaarheid (99,8%), responstijden (<30 min) en oplostijden (<4 uur) kunnen beïnvloeden, conform EMVI-criterium Risicobeheersing.
- Scope: 24/7 beheer-, monitoring- en supportdiensten voor kritieke systemen en Microsoft 365, inclusief security en continuïteit, met dataverwerking binnen de EU.
- Werkwijze: elk risico is voorzien van SMART-maatregelen in PDCA-cyclus, gekoppeld aan KPI's en onderliggende werkpakketten (W-xx), met expliciete bewijsvoering.

Werkpakketten (W-xx) voor kruisverwijzing

- W-01 Intake & Onboarding
- W-02 Proactieve Monitoring & Alerting
- W-03 Patch- & Vulnerability Management
- W-04 Incident- & Major Incident Management (ITIL)
- W-05 Change & Release Management
- W-06 Continuïteitsmanagement (BCP/DR)
- W-07 Servicedesk 24/7 & Escalatie
- W-08 Security Operations (EDR/MFA/Logging)
- W-09 Configuratie- & Assetmanagement (CMDB)
- W-10 Rapportage & SLA/KPI Management
- W-11 Compliance & Datalocatie (EU)
- W-12 Microsoft 365 Beheer & Hardening
- W-13 Vendor & Third-Party Management
- W-14 Capaciteits- & Performancebeheer
- W-15 Kennisborging & Personele Continuïteit (incl. VOG)

KPI's (SLA-definities en aanvullend)

- KPI-1 Beschikbaarheid kritieke systemen: 99,8% per maand
- KPI-2 Responstijd P1-incidenten: < 30 minuten
- KPI-3 Oplostijd P1-incidenten: < 4 uur
- KPI-4 (intern) Patch compliance: ≥ 95% binnen 14 dagen kritieke updates
- KPI-5 (intern) Change-succesratio: ≥ 98% per maand

Risicoregister

Risico	Kans	Impact	Score	Beheersmaatregel (SMART + PDCA)	Eigenaar	Status	Link KPI/W-xx	Residua
1. Niet halen 99,8% beschikbaarheid door storingen in kritieke componenten	3 (Middel)	5 (Zeer hoog)	15	Plan: definieer per 01-02-2026 een top-10 kritieke systeemlijst met single points of failure en onderhoudsvensters (W-14). Do: implementeer actieve/actieve opzet en synthetische checks binnen 30 dagen (W-02). Check: maandelijkse beschikbaarheidsrapportage met root cause analyse (W-10). Act: binnen 10 werkdagen na afwijking wijzigingsvoorstel (W-05). SMART: ≥99,8% uptime per maand; max. 50 min downtime. Bewijs: maandrapportages, monitoring-export.	Service Delivery Manager	Actief	KPI-1; W-02, W-14, W-10, W-05. Bewijs: ISO 9001-procesrapportage.	Wordt na maatrege herbeoor
2. Overschrijden responstijd P1 (>30 min) bij 24/7 meldingen	2 (Laag)	5 (Zeer hoog)	10	Plan: definieer P1-triggers, escalatiematrix en wachtdienstrooster 24/7 per 15-01-2026 (W-07). Do: automatische paging via SMS/Teams/telefonie, 3-minuten bevestigingsplicht (W-02). Check: wekelijkse responstijd-audit; QBR-trend (W-10). Act: bij >1 afwijking/maand: rooster herzien en back-up engineer toevoegen binnen 7 dagen. SMART: mediaan P1-responstijd ≤10 min; 95e	NOC Lead	Actief	KPI-2; W-07, W-02, W-10. Bewijs: wachtdienstlogboeken.	Wordt na maatrege herbeoor

Risico	Kans	Impact	Score	Beheersmaatregel (SMART + PDCA)	Eigenaar	Status	Link KPI/W-xx	Residua
				percentiel ≤20 min. Bewijs: pager logs.				
3. Te late P1-oplossing (>4 uur) door onvoldoende major incident-proces	3 (Middel)	4 (Hoog)	12	Plan: MIM-runbook en war room-protocol per 20-01-2026 (W-04). Do: standby MI-manager, 15-min update-cadans naar stakeholders (W-07). Check: post-mortem binnen 48 uur (W-10). Act: problem record en structurele maatregel binnen 10 werkdagen (W-04/W-05). SMART: ≥90% P1 opgelost <4 uur, rest met workaround <2 uur. Bewijs: MIM-dossiers, post-mortems.	Major Incident Manager	Actief	KPI-3; W-04, W-07, W-10. Bewijs: ITIL-procesdocumenten.	Wordt na maatrege herbeoor
4. Patch-achterstand verhoogt dreiging exploit of verstoring	3 (Middel)	4 (Hoog)	12	Plan: CVSS≥7 binnen 14 dagen; overige binnen 30 dagen (policy per 01-02-2026) (W-03). Do: geautomatiseerde patching en maintenance windows (W-05). Check: wekelijkse compliance-rapportage (W-10). Act: bij <95% compliance: change freeze voor niet-urgent werk tot herstel binnen 5 werkdagen. SMART: ≥95% binnen 14 dagen; 100% binnen 30 dagen. Bewijs: patchrapporten.	Tech Lead Infrastructure	Actief	KPI-4; W-03, W-05, W-10. Bewijs: scanresultaten (Nessus/Defender).	Wordt na maatrege herbeoor
5. Onvoldoende monitoring/alerting leidt tot late detectie	2 (Laag)	4 (Hoog)	8	Plan: 100% dekking kritieke assets in monitoring-CMDB per 01-02-2026 (W-02, W-09). Do: drempels, synthetics en logcorrelatie activeren (W-08). Check: maandelijkse gap-scan vs CMDB (W-10). Act: ontbrekende sensoren binnen 3 werkdagen toevoegen. SMART: ≥99% kritieke assets gemonitord; false positives <5%/maand. Bewijs: monitoring-inventaris.	Monitoring Lead	In uitvoering	KPI-1; W-02, W-09, W-08, W-10. Bewijs: CMDB-exports.	Wordt na maatrege herbeoor
6. Datalocatie buiten EU of onduidelijkheid daarover	2 (Laag)	5 (Zeer hoog)	10	Plan: datalocatie-matrix en verwerkerslijst per 15-02-2026 (W-11). Do: blokkeren niet-EU regio's in tenants, DLP en geo-fencing (W-12/W-08). Check: kwartaalreview verwerkers en tenant-instellingen (W-10). Act: afwijking binnen 48 uur corrigeren en DPIA-update binnen 5 dagen. SMART: 0 datastromen buiten EU. Bewijs: verwerkersoverzicht, tenant-config.	CISO	Actief	W-11, W-12, W-08, KPI-1 (indirect). Bewijs: ISO 27001 scopeverklaring.	Wordt na maatrege herbeoor
7. Escalatie faalt door onvolledige contactketen opdrachtgever/leveranciers	3 (Middel)	3 (Middel)	9	Plan: escalatiediagram met contactgegevens opdrachtgever en leveranciers per 20-01-2026 (W-07, W-13). Do: gezamenlijke P1-oefening binnen 30 dagen na start	Service Delivery Manager	In uitvoering	KPI-2/KPI-3; W-07, W-13, W-04, W-10.	Wordt na maatrege herbeoor

Risico	Kans	Impact	Score	Beheersmaatregel (SMART + PDCA)	Eigenaar	Status	Link KPI/W-xx	Residua
				(W-04). Check: halfjaarlijkse call tree-test (W-10). Act: binnen 3 dagen na test alle verouderde contacten actualiseren. SMART: ≥95% bereikbaarheid in call tree-tests. Bewijs: testrapporten.				
8. Onvoldoende getest BCP/DR leidt tot lange uitval	2 (Laag)	5 (Zeer hoog)	10	Plan: BCP/DR-scenario's en RTO/RPO per 01-03-2026 (W-06). Do: jaarlijkse DR-test en halfjaarlijkse tabletop (W-06). Check: testresultaten vs RTO≤4 uur voor P1-systemen (W-10). Act: herstelplan met investeringsvoorstel binnen 15 werkdagen. SMART: ≥1 volledige DR-test/jaar; ≥90% doelstellingen gehaald. Bewijs: testrapporten, BCP.	Continuïteitsmanager	Gecontroleerd	KPI-1/KPI-3; W-06, W-10.	Wordt na maatrege herbeoor
9. Change-falen veroorzaakt downtime of terugval	3 (Middel)	4 (Hoog)	12	Plan: CAB-kalender en risicoscore >7 vereist back-outplan per 01-02-2026 (W-05). Do: standard changes met sjablonen; black-out windows (W-05). Check: maandelijkse change-succes KPI (W-10). Act: bij succesratio <98% root cause en aanpassing sjablonen binnen 10 werkdagen. SMART: ≥98% succesvolle changes/maand. Bewijs: CAB-notulen.	Change Manager	Actief	KPI-1/KPI-5; W-05, W-10.	Wordt na maatrege herbeoor
10. Security-incident (bijv. ransomware) door EDR/MFA-gaps	2 (Laag)	5 (Zeer hoog)	10	Plan: EDR op 100% endpoints en MFA op alle admins per 01-02-2026 (W-08, W-12). Do: 24/7 SOC-alerting, isolatie binnen 15 minuten (W-08). Check: maandelijkse EDR-coverage en phishing-simulaties (W-10). Act: coverage <100% binnen 48 uur herstellen; lessons learned in hardening guide binnen 7 dagen. SMART: 0 kritieke security-incidenten/kwartaal. Bewijs: EDR-rapporten, MFA-policy.	Security Lead	Actief	KPI-1/KPI-3; W-08, W-12, W-10.	Wordt na maatrege herbeoor
11. Capaciteitsknelpunten (CPU/RAM/storage) leiden tot vertraging of uitval	3 (Middel)	3 (Middel)	9	Plan: drempels 75/85/95% met automatische tickets per 01-02-2026 (W-14). Do: maandelijks capacity review en voorspelling 90 dagen (W-10). Check: rapportage met trends en aanbevelingen (W-14). Act: binnen 10 werkdagen change voor uitbreiding of optimalisatie (W-05). SMART: 0 P1's door resource-uitputting. Bewijs: capacity-rapporten.	Performance Engineer	Actief	KPI-1; W-14, W-10, W-05.	Wordt na maatrege herbeoor
12. Onjuiste/onj complete CMDB leidt tot foutieve impactanalyse	3 (Middel)	3 (Middel)	9	Plan: datamodel en owners per CI per 31-01-2026 (W-09). Do: auto-discovery + handmatige validatie per maand (W-02/W-09).	Configuration Manager	In uitvoering	KPI-1/KPI-5; W-09, W-02, W-10.	Wordt na maatrege herbeoor

Risico	Kans	Impact	Score	Beheersmaatregel (SMART + PDCA)	Eigenaar	Status	Link KPI/W-xx	Residua
				Check: maandelijkse audit; afwijking >5% is non-conform (W-10). Act: datakwaliteitsplan binnen 7 dagen bij afwijking. SMART: ≥95% CI-accuracy; 100% kritieke CIs geverifieerd/maand. Bewijs: auditlog CMDB.				
13. Vertraging onboarding door ontbrekende toegangen/info opdrachtgever	3 (Middel)	2 (Beperkt)	6	Plan: RACI en onboarding-checklist met harde afhankelijkheden per 20-01-2026 (W-01). Do: wekelijkse voortgangsstand-ups met opdrachtgever tot go-live (W-01). Check: burn-down tegen mijlpalen (W-10). Act: blokkades >5 werkdagen escaleren naar stuurgroep; workaround voorstellen binnen 2 werkdagen. SMART: 100% mijlpalen op tijd ±5 werkdagen. Bewijs: onboarding-bord, actielijsten.	Projectmanager	In uitvoering	W-01, W-10; KPI-2/KPI-3 (indirect).	Wordt na maatrege herbeoor
14. Personele uitval/ontoereikende vervanging (24/7 borging)	2 (Laag)	4 (Hoog)	8	Plan: skills-matrix, 2-deep coverage op kritieke rollen per 15-02-2026 (W-15). Do: kennisoverdracht en runbooks; VOG geborgd (W-15). Check: kwartaalreview bezetting vs rooster (W-07/W-10). Act: binnen 2 weken bijschakelen via partners SecureOps NL/IT Infra Group. SMART: 0 gemiste shifts; 100% VOG op dossier. Bewijs: skills-matrix, VOG-register.	HR & Operations Manager	Actief	KPI-2/KPI-3; W-15, W-07, W-10.	Wordt na maatrege herbeoor
15. Leveranciersfalen (SaaS/connectiviteit) beïnvloedt SLA	3 (Middel)	4 (Hoog)	12	Plan: onderaannemers-SLA's alignen op 99,9% en P1 <30/<4 per 01-02-2026 (W-13). Do: contractuele credits en prioritaire escalatiepaden (W-13). Check: maandelijkse vendor scorecards (W-10). Act: bij 2 maanden op rij non-conform: verbeterplan of exit binnen 30 dagen. SMART: ≥95% vendor-SLA-compliance/kwartaal. Bewijs: scorecards, contracten.	Vendor Manager	Actief	KPI-1/KPI-2/KPI-3; W-13, W-10.	Wordt na maatrege herbeoor
16. M365-misconfiguraties (conditional access, sharing) leiden tot risico's	2 (Laag)	4 (Hoog)	8	Plan: M365 baseline (CIS/MS) per 01-02-2026; change-guardrails (W-12). Do: policy enforcement, least privilege, secure score ≥80 (W-12/W-08). Check: maandelijkse secure score review (W-10). Act: afwijkingen >5 punten herstellen binnen 5 dagen. SMART: Secure Score ≥80 blijvend. Bewijs: Secure Score-rapporten.	M365 Architect	Actief	KPI-1/KPI-3; W-12, W-08, W-10.	Wordt na maatrege herbeoor

Toelichting koppeling Risico ↔ KPI ↔ W-xx ↔ Bewijs

- Voor elk risico is minimaal één primaire KPI benoemd (KPI-1/2/3) en het onderliggende werkpakket (W-xx) dat het resultaat levert.

- Bewijsvoering is geborgd via: ISO 27001/ISO 9001 (Digital Ease B.V., KvK 88392011), NEN 7510, Microsoft Secure Score-rapporten, monitoring-exports, post-mortems, CAB-notulen, BCP/DR-testverslagen, CMDB-audits, wachtdienstlogboeken en vendor scorecards.
- PDCA-cycli zijn aantoonbaar via maandrapportages (W-10), change-records (W-05), problem records (W-04), auditlogs (W-09) en management reviews (ISO).

PDCA-borging en escalatie

- Plan: beleid, runbooks, RACI, KPI-definities en onderhoudsvensters worden per werkpakket vastgesteld en formeel geaccordeerd met de opdrachtgever in de opstartfase (voor 01-03-2026).
- Do: uitvoering via 24/7 servicedesk, NOC/SOC, geautomatiseerde monitoring/patching, MIM-procedures en CAB.
- Check: maandelijkse SLA/KPI-rapportage en kwartaal QBR met trendanalyses, inclusief beschikbaarheid, responstijden, oplostijden, patch compliance, change-succes en security-coverage.
- Act: verbetermaatregelen met eigenaar, deadline en verificatiecriteria; bij KPI-onderprestatie wordt binnen 10 werkdagen een corrigerend actieplan doorgevoerd en hergetest.

Afhankelijkheden en randvoorwaarden (conform aannames)

- Tijdige aanlevering van noodzakelijke toegangen, informatie en besluitvorming door de opdrachtgever (impact op W-01/W-07).
- Lokale netwerkinfrastructuur voldoet aan minimale eisen; licenties (Microsoft 365 e.a.) zijn rechtmatig en actief.
- Onsite hardware valt buiten scope tenzij expliciet overeengekomen; third-party SaaS support via W-13.

Continuïteit en security

- Certificeringen: ISO 27001, ISO 9001, NEN 7510 geborgd in onze managementsystemen; Microsoft Solutions Partner – Modern Work; Fortinet NSE4-capaciteit aanwezig.
- Personeel en VOG: W-15 borgt 2-deep bezetting, VOG en kennisoverdracht; partners SecureOps NL en IT Infra Group zijn vooraf gecontracteerd voor piek/uitval.

Rapportage en sturing

- KPI-rapportage: maandrapporten binnen 5 werkdagen na maandultimo; QBR met trendgrafieken en RCA-overzichten.
- Escalatie: P1 binnen 30 min respons en escalatie volgens call tree; opdrachtgever ontvangt statusupdates elke 15 minuten tot mitigatie.

Benodigde input: