Risicoregister

Digital Ease B.V. — Raamovereenkomst Managed IT Services 2026–2030

Datum: 12/24/2025

Risico’s

1. Strategisch risicoregister Managed IT Services 2026–2030

Onderstaand risicoregister is opgesteld voor de raamovereenkomst Managed IT Services 2026–2030 voor Digital Ease B.V. De maatregelen zijn SMART geformuleerd en ingericht volgens de PDCA-cyclus (Plan–Do–Check–Act). Alle risico’s zijn gericht op continuïteit, beschikbaarheid, veiligheid en kwaliteit van de IT-dienstverlening binnen een overheidssituatie.

Legenda:

- Kans: 1 (zeer laag) – 5 (zeer hoog)
- Impact: 1 (beperkt) – 5 (zeer groot)
- Score: Kans × Impact (prioriteit)
- Status: Voorkomend / Beheerst / Verbeteractie

Tabel 1 – Risicoregister Managed IT Services

Risico 1 Risico: Onvoldoende beschikbaarheid kritieke diensten (langdurige uitval) Kans: 3 Impact: 5 Score: 15 Beheersmaatregel: PLAN • Uiterlijk maand 1 na start raamovereenkomst is een beschikbaarheidsarchitectuur opgesteld en afgestemd met de opdrachtgever, met RTO/RPO-eisen per kritieke dienst (RTO ≤ 4 uur, RPO ≤ 15 minuten). • SLA’s leggen minimaal 99,8% maandelijkse beschikbaarheid vast voor kernservices (werkplekken, netwerk, centrale applicatiehosting).

DO • Implementatie van redundante componenten (servers, storage, netwerkpaden) en automatische failover binnen 3 maanden na start. • Inrichting 24/7 monitoring en incidentafhandeling met escalatiedienst.

CHECK • Maandelijkse rapportage over gerealiseerde beschikbaarheid per dienst en per tijdsvenster. • Kwartaalgewijze stress- en failovertests op geselecteerde diensten.

ACT • Indien beschikbaarheid onder 99,8% komt, wordt binnen 10 werkdagen een verbeterplan met root cause analyse opgesteld en samen met de opdrachtgever vastgesteld, met uitvoering binnen maximaal 2 maanden.

Eigenaar: Service Manager Digital Ease Status: Beheerst Link KPI/W-xx: KPI/W-01 – Beschikbaarheid kritieke diensten (≥ 99,8% per maand)

Risico 2 Risico: Onvoldoende informatiebeveiliging en datalekken Kans: 3 Impact: 5 Score: 15 Beheersmaatregel: PLAN • Binnen 2 weken na start is een gezamenlijke risico-inventarisatie Informatiebeveiliging uitgevoerd op basis van een gangbaar normenkader (bijvoorbeeld BIO/ISO 27001-principes), met classificatie van systemen en data. • Beveiligingsbeleid en -procedures zijn afgestemd met de opdrachtgever en goedgekeurd door het management van Digital Ease.

DO • Invoering van multi-factor authenticatie, versleuteling van data in transit en at rest, en rolgebaseerde toegangsrechten binnen 3 maanden. • Halfjaarlijkse security awareness-training voor alle betrokken medewerkers die toegang hebben tot de systemen van de opdrachtgever.

CHECK • Maandelijkse controle op logbestanden, mislukte inlogpogingen en privilegewijzigingen. • Jaarlijkse onafhankelijke penetratietest op de beheerde omgevingen en rapportage van bevindingen aan de opdrachtgever.

ACT • Beveiligingsincidenten worden binnen 4 uur na ontdekking gemeld aan de opdrachtgever, met binnen 24 uur een eerste analyse en mitigerende maatregelen. • Structurele verbeteringen worden binnen 30 dagen na incident in procedures en configuraties verwerkt.

Eigenaar: Security Officer Digital Ease Status: Voorkomend Link KPI/W-xx: KPI/W-02 – Aantal beveiligingsincidenten met impact “hoog” of “kritiek” (= 0 per jaar)

Risico 3 Risico: Onvoldoende regie en afstemming met opdrachtgever (bestuurlijke onduidelijkheid) Kans: 3 Impact: 4 Score: 12 Beheersmaatregel: PLAN • In de eerste maand wordt een governance-model vastgesteld, inclusief overlegstructuur (stuurgroep, operationeel overleg, architectuuroverleg), rollen, bevoegdheden en escalatiepaden. • Jaarplan met concrete doelen, projecten en verbeteracties wordt voorafgaand aan ieder kalenderjaar afgestemd en goedgekeurd.

DO • Maandelijks operationeel overleg met vast verslag en actielijst. • Kwartaalgewijze stuurgroepvergaderingen waarin voortgang, risico’s, financiële kaders en roadmap worden vastgesteld.

CHECK • Twee keer per jaar een tevredenheidsmeting onder sleutelfunctionarissen van de opdrachtgever over samenwerking, regie en overleg (score 1–10). • Jaarlijkse toetsing van de governance op effectiviteit (doorlooptijd besluiten, aantal escalaties).

ACT • Bij een gemiddelde tevredenheidsscore < 8 wordt binnen 4 weken een verbeterplan opgesteld (aanpassing overlegfrequentie, rollen, rapportages) en in de stuurgroep vastgesteld. • Governance-model wordt minimaal jaarlijks herzien en geactualiseerd.

Eigenaar: Contractmanager Digital Ease Status: Beheerst Link KPI/W-xx: KPI/W-03 – Tevredenheid opdrachtgever over samenwerking en regie (≥ 8,0)

Risico 4 Risico: Capaciteits- en kennis tekort (onderbezetting of onvoldoende expertise) Kans: 3 Impact: 4 Score: 12 Beheersmaatregel: PLAN • Binnen 1 maand is een capaciteits- en competentieplan per rol (servicedesk, beheerders, architecten, projectleiders) opgesteld, gekoppeld aan de afgesproken dienstverlening en volumes. • Minimale bezetting en skills per rol zijn in SLA’s en/of DAP (DienstverleningsAfspraakPlan) vastgelegd.

DO • Inzet van een vaste kern van specialisten voor de opdrachtgever, met duidelijk vastgelegde vervanging bij afwezigheid. • Jaarlijkse opleidingsplannen voor alle betrokken medewerkers, gericht op relevante technologieën, security en proceskennis.

CHECK • Maandelijkse analyse van workload, bezettingsgraad en openstaande tickets. • Halfjaarlijkse evaluatie van kennisniveau (certificeringen, evaluaties per project, feedback opdrachtgever).

ACT • Indien structureel > 10% achterstand op de werkvoorraad ontstaat, wordt binnen 2 weken een opschalingsplan voorgesteld (extra FTE, herverdeling taken, inzet experts). • Competentieplan wordt jaarlijks geactualiseerd op basis van roadmap en technologische ontwikkelingen.

Eigenaar: Teamleider Operations Digital Ease Status: Verbeteractie Link KPI/W-xx: KPI/W-04 – Bezettingsgraad en doorlooptijd tickets (≥ 95% binnen afgesproken norm)

Risico 5 Risico: Onvoldoende transitie en migratie naar de nieuwe Managed IT-omgeving Kans: 2 Impact: 5 Score: 10 Beheersmaatregel: PLAN • Voor de start van de feitelijke migratie is een gedetailleerd transitieplan opgesteld en akkoord bevonden door de opdrachtgever, met scope, fasering, rollback-scenario’s en communicatieplan. • Elke migratiestap wordt voorzien van expliciete go/no-go-criteria en acceptatietesten.

DO • Migraties worden gefaseerd uitgevoerd buiten piekuren, met een heldere impactanalyse per deelstap. • Testomgevingen worden vooraf ingericht, waarin representatieve gebruikersacceptatietesten plaatsvinden.

CHECK • Na elke migratiefase worden resultaten geëvalueerd aan de hand van vooraf gedefinieerde succescriteria (beschikbaarheid, performance, incidenten). • Lessons learned-sessies met opdrachtgever na iedere majeure stap.

ACT • Bij overschrijding van afgesproken KPI's wordt de volgende migratiefase pas gestart na aanvullende mitigerende maatregelen. • Transitieplan wordt dynamisch bijgesteld op basis van de uitkomsten van eerdere fasen.

Eigenaar: Transitiemanager Digital Ease Status: Beheerst Link KPI/W-xx: KPI/W-05 – Succesratio migratiestappen (≥ 95% zonder kritieke incidenten)

Risico 6 Risico: Niet voldoen aan afgesproken responstijden en oplostijden (SLA-schending) Kans: 3 Impact: 4 Score: 12 Beheersmaatregel: PLAN • SLA met prioriteitsclassificatie (P1–P4) inclusief maximale responstijden en oplostijden wordt binnen 1 maand gezamenlijk vastgesteld. • Servicedeskprocedure met eenduidige intake, triage en escalatie wordt uitgewerkt en gecommuniceerd.

DO • Inrichting van een ITSM-tool waarin alle meldingen, doorlooptijden en statussen worden geregistreerd. • 24/7 bereikbaarheid voor P1-incidenten indien overeengekomen, met directe telefonische escalatie.

CHECK • Dagelijkse monitoring van openstaande tickets en doorlooptijden. • Wekelijkse interne reviews van SLA-prestaties en maandelijkse rapportage richting opdrachtgever.

ACT • Bij SLA-score < 98% in een kalendermaand volgt binnen 10 werkdagen een analyse en verbeterplan (extra capaciteit, aanpassing proces, toolingverbetering). • Structurele procesaanpassingen worden geborgd in werkinstructies en gecommuniceerd naar alle betrokken medewerkers.

Eigenaar: Servicedesk Manager Digital Ease Status: Voorkomend Link KPI/W-xx: KPI/W-06 – SLA-naleving responstijd/oplostijd (≥ 98% per maand)

Risico 7 Risico: Onvoldoende documentatie en kennisborging (afhankelijkheid van personen) Kans: 3 Impact: 3 Score: 9 Beheersmaatregel: PLAN • Binnen 2 maanden na start is een kennis- en configuratiemanagementplan opgesteld, met minimale documentatie-eisen (CMDB, netwerkdiagrammen, procedures, how-to's). • Alle bedrijfskritieke processen krijgen een formele werkinstructie en beheerprocedure.

DO • Stapsgewijze opbouw van een centrale kennisdatabase (wiki/portaal) specifiek voor de opdrachtgever, toegankelijk voor alle relevante medewerkers van Digital Ease. • Cross-training: iedere kritieke beheerfunctie heeft minimaal één aantoonbaar ingewerkte back-up.

CHECK • Kwartaalgewijze audits op volledigheid en actualiteit van CMDB en documentatie. • Jaarlijkse review van de kennisdatabase samen met de opdrachtgever op bruikbaarheid en volledigheid.

ACT • Bij geconstateerde lacunes (>10% van kritieke items onvolledig) wordt binnen 1 maand een gerichte documentatie- en trainingsoffensief uitgevoerd. • Lessons learned uit incidenten worden binnen 4 weken vertaald naar geactualiseerde documentatie.

Eigenaar: Kennismanager / Configuration Manager Digital Ease Status: Verbeteractie Link KPI/W-xx: KPI/W-07 – Actualiteit CMDB en documentatie (≥ 95% van kritieke items actueel)

Risico 8 Risico: Onvoldoende aandacht voor continuïteit en disaster recovery bij calamiteiten Kans: 2 Impact: 5 Score: 10 Beheersmaatregel: PLAN • Binnen 3 maanden is een Business Continuity Plan (BCP) en Disaster Recovery Plan (DRP) opgesteld, afgestemd op de kritieke processen van de opdrachtgever. • Prioritering van diensten en maximale uitvaltijd per dienst zijn expliciet vastgelegd en goedgekeurd.

DO • Inrichting van back-upvoorzieningen met dagelijkse back-ups, bewaartermijnen volgens afspraak en periodieke restore-tests. • Definiëren en oefenen van noodprocedures (bijvoorbeeld verlies datacenter, cyberaanval, langdurige stroomuitval).

CHECK • Jaarlijkse integrale DR-oefening met betrokkenheid van de opdrachtgever, inclusief test van communicatie en escalatie. • Kwartaalgewijze rapportage over back-upsucces en uitgevoerde hersteltests.

ACT • Naar aanleiding van DR-oefeningen worden binnen 6 weken alle verbeterpunten verwerkt in BCP/DRP. • Bij iedere relevante wijziging in infrastructuur wordt binnen 1 maand beoordeeld of aanpassing van het DRP nodig is.

Eigenaar: Business Continuity Manager Digital Ease Status: Voorkomend Link KPI/W-xx: KPI/W-08 – Succesratio back-ups en restore-tests (≥ 99%)

Risico 9 Risico: Onvoldoende focus op vernieuwing en doorontwikkeling (verouderde IT-omgeving) Kans: 3 Impact: 3 Score: 9 Beheersmaatregel: PLAN • Jaarlijks wordt een gezamenlijke roadmap opgesteld voor technologische vernieuwing, standaardisatie en rationalisatie, gekoppeld aan de organisatiedoelen van de opdrachtgever. • Lifecycle-managementbeleid (end-of-life, end-of-support, vervangingscriteria) wordt in de eerste 6 maanden vastgelegd.

DO • Kwartaalgewijze innovatiesessies met de opdrachtgever waarin marktontwikkelingen, pilots en optimalisaties worden besproken. • Actief voorstellen van minimaal twee concrete verbeterinitiatieven per jaar (bijvoorbeeld kostenreductie, securityverhoging, efficiëntie).

CHECK • Jaarlijkse evaluatie van de roadmaprealisatie (wat is geïmplementeerd, welke voordelen zijn gerealiseerd). • Meten van de mate van standaardisatie en actualiteit (percentage systemen binnen vendor-support).

ACT • Indien minder dan 80% van geplande roadmapactiviteiten is gerealiseerd, wordt samen met de opdrachtgever binnen 2 maanden een bijsturingsplan gemaakt. • Roadmap wordt minimaal jaarlijks geactualiseerd op basis van evaluatie en nieuwe behoeften.

Eigenaar: Lead Architect / Innovatiemanager Digital Ease Status: Voorkomend Link KPI/W-xx: KPI/W-09 – Realisatie innovatie- en roadmapactiviteiten (≥ 80% per jaar)

Risico 10 Risico: Onvoldoende aandacht voor duurzaamheid en Maatschappelijk Verantwoord Ondernemen in de IT-keten Kans: 2 Impact: 3 Score: 6 Beheersmaatregel: PLAN • Binnen 6 maanden is een duurzaamheidsplan voor de dienstverlening opgesteld, met doelstellingen op het gebied van energieverbruik, hardwarelevensduur, recycling en sociale aspecten. • Doelen worden kwantitatief gemaakt, bijvoorbeeld reductie energieverbruik in datacenters en werkplekken.

DO • Voorkeursinzet van energiezuinige hardware en virtualisatie om de fysieke footprint te beperken. • Ondersteuning van de opdrachtgever bij verantwoord afvoeren en recyclen van IT-middelen conform geldende wet- en regelgeving.

CHECK • Jaarlijkse rapportage over gerealiseerde duurzaamheidsdoelen (energiegebruik, aantal gerecyclede apparaten, CO_2-indicatoren waar beschikbaar). • Evaluatie in de stuurgroep over MVO-prestaties en

aanvullende kansen.

ACT • Bij achterblijvende resultaten worden binnen 2 maanden aanvullende maatregelen voorgesteld (andere hardwareprofielen, optimalisatie capaciteit, aanvullende bewustwordingsacties). • Duurzaamheidsplan wordt jaarlijks herijkt met concrete nieuwe doelen.

Eigenaar: MVO-/Sustainability Officer Digital Ease Status: Voorkomend Link KPI/W-xx: KPI/W-10 – Realisatie duurzaamheidsdoelen (≥ 80% van jaarplan)

Risico 11 Risico: Onvoldoende naleving wet- en regelgeving (o.a. AVG, archiefwetgeving, overheidsrichtlijnen) Kans: 2 Impact: 4 Score: 8 Beheersmaatregel: PLAN • In de eerste 3 maanden wordt een compliance-scan uitgevoerd op relevante wet- en regelgeving en sectorrichtlijnen die van toepassing zijn op de opdrachtgever. • Gezamenlijk worden verwerkersafspraken en privacy-by-design/basisprincipes expliciet vastgelegd in procedures en werkafspraken.

DO • Structurele inbedding van privacy- en compliancechecks in change management en projectaanpak (elke wijziging wordt getoetst op impact op privacy en regelgeving). • Betrokken medewerkers volgen minimaal eenmaal per jaar een privacy- en compliance-training.

CHECK • Jaarlijkse interne audit op naleving van relevante verplichtingen (logging, bewaartermijnen, rechten van betrokkenen, beveiligingsmaatregelen). • Periodieke afstemming met de Functionaris Gegevensbescherming of privacycontactpersoon van de opdrachtgever.

ACT • Bij vastgestelde afwijkingen wordt binnen 4 weken een corrigerend actieplan opgesteld met concrete termijnen en verantwoordelijkheden. • Procesbeschrijvingen worden na elke significante wijziging in wet- of regelgeving binnen 3 maanden aangepast.

Eigenaar: Compliance Officer Digital Ease Status: Voorkomend Link KPI/W-xx: KPI/W-11 – Aantal significante non-compliance bevindingen (= 0 per jaar)

Risico 12 Risico: Onvoldoende gebruikersadoptie en eindgebruikerservaring Kans: 3 Impact: 3 Score: 9 Beheersmaatregel: PLAN • Voor iedere majeure wijziging (nieuwe werkplekomgeving, nieuwe functionaliteit) wordt een adoptie- en communicatieplan opgesteld, inclusief doelgroepen, middelen en timing. • Heldere servicecatalogus en gebruiksinstructies worden vooraf afgestemd met de opdrachtgever.

DO • Inzet van laagdrempelige ondersteuning (handleidingen, korte instructievideo’s, inloopsessies) rondom grote wijzigingen. • Monitoring van gebruikersfeedback via servicedesk-registraties, korte enquêtes na afgeronde meldingen en pilots met key users.

CHECK • Tweejaarlijkse eindgebruikers-tevredenheidsmeting over ondersteuningskwaliteit, gebruiksvriendelijkheid en bereikbaarheid (score 1–10). • Analyse van herhaalde meldingen per functionaliteit om knelpunten in gebruik te identificeren.

ACT • Bij een gemiddelde eindgebruikersscore < 8 wordt een gericht verbeterprogramma ingericht (aanpassing instructies, extra trainingen, interface-optimalisaties) met uitvoering binnen 3 maanden. • Verbeteringen worden na implementatie gemeten via gerichte follow-up-enquête.

Eigenaar: Change & Adoption Lead Digital Ease Status: Voorkomend Link KPI/W-xx: KPI/W-12 – Tevredenheid eindgebruikers (≥ 8,0)

Benodigde input: