

Voortgangsrapportage ISO 27001-certificering

Stand van zaken per 25 september 2026

Onderwerp	Voortgang ISO 27001-certificering
Organisatie	1Key ICT Solutions B.V.
Datum rapport	25 september 2026
Opgesteld door	Dennis Jumelet
Status	Proefaudit behaald — fase 1 audit op 29 september 2026
Doel	ISO 27001-certificaat in november 2026

1. Samenvatting

1Key heeft de proefaudit met goed resultaat doorlopen. Daarmee is aangetoond dat het ISMS in opzet en werking op het juiste niveau zit om de formele certificeringsaudit in te gaan. Het traject gaat nu de laatste fase in:

- **Fase 1 audit:** dinsdag 29 september 2026 — beoordeling van de ISMS-documentatie en de gereedheid voor certificering.
- **Fase 2 audit:** eind november 2026 — toetsing van de werking van het ISMS in de praktijk, afgesloten met het certificeringsbesluit.
- **Verwachte certificering:** november 2026.

Ten opzichte van de vorige rapportage is de oorspronkelijke planning (proefaudit 1 april, certificaat 1 mei) bijgesteld. Het einddoel blijft ongewijzigd: een ISO 27001-certificaat voor 1Key in 2026.

2. Planning en mijlpalen

Mijlpaal	Moment	Status
Kick-off met Dxfferent en inrichting projectomgeving	—	Afgerond
Opzet ISMS: beleid, risicoanalyse, procedures	—	Afgerond
Proefaudit	—	Behaald
Fase 1 audit (documentatiebeoordeling)	29 september 2026	Gepland
Fase 2 audit (certificeringsaudit)	Eind november 2026	Gepland
ISO 27001-certificaat	November 2026	Verwacht

3. Wat is gerealiseerd

Governance en organisatie

- Kick-off uitgevoerd met Dxfferent; gezamenlijke Teams-omgeving ingericht.
- Security Officer-rol belegd bij Linda, inclusief documentatie-update.
- Organogram geactualiseerd en rol Service Desk beschreven.

Documentatie en beleid

- Beleidsdocumenten opgesteld en beoordeeld op versiebeheer en normverwijzingen.
- ISO-procedures geïmporteerd in Autotask (categorieën, UDF's, formulieren).

Risicoanalyse en context

- Contextanalyse (stakeholders, eisen, SWOT) ingevuld.
- Risico-inventarisatie uitgevoerd (R1 t/m R30), inclusief kans/impact-scores en behandelmaatregelen.

Procesinrichting en bewijsvoering

- Onboarding/offboarding via tickets vastgelegd als aantoonbaar bewijs.
- Procedures voor klantapparatuur, labeling en registratie opgesteld.
- Assetregister ingericht voor laptops, SD-kaarten en telefoons.

Leveranciersbeheer

- Leveranciersdossier en risicobeoordeling opgezet.
- Contractdocumentatie Microsoft (MCA/BBP) verzameld.

Audit

- Proefaudit succesvol doorlopen.

4. Aandachtspunten richting fase 1 en fase 2

Fase 1 — 29 september 2026

In fase 1 beoordeelt de auditor of de verplichte ISMS-documentatie compleet en actueel is. Aandachtspunten voor de komende dagen:

- Definitieve, gepubliceerde versies van het informatiebeveiligingsbeleid en onderliggende beleidsstukken.
- Formele vastlegging van de Security Officer-rol.
- Risicobeoordeling en ondertekend risicobehandelplan, inclusief Verklaring van Toepasselijkheid.
- Jaarplanning ISMS (PDCA-cyclus).
- Opvolging van eventuele bevindingen uit de proefaudit.

Fase 2 — eind november 2026

In fase 2 toetst de auditor of het ISMS in de dagelijkse praktijk ook werkt. Tot eind november ligt de focus op:

- Doorlopend verzamelen van bewijsvoering: tickets, logs en rapportages.
- Volledig en actueel assetregister en leveranciersdossier (per leverancier: overeenkomst, risico, verantwoordelijkheden).
- Uitgevoerde en gedocumenteerde interne audit.
- Uitgevoerde managementreview met vastgelegde besluiten.
- Opvolging van eventuele bevindingen uit fase 1.

5. Na certificering

Een ISO 27001-certificaat is drie jaar geldig, met jaarlijkse surveillance-audits. Na certificering richten we ons op:

- Continue verbetering vanuit de risicoanalyse en auditbevindingen.
- Verdere optimalisatie van AI-ondersteunde processen binnen het ISMS.
- Voorbereiding op de eerste surveillance-audit in 2027.

6. Beleid, documentatie en vragenlijsten

Beleid of aanvullende documentatie opvragen

Klanten en relaties kunnen beleid of aanvullende documentatie bij 1Key opvragen. Wij vragen daarbij aan te geven welke informatie nodig is en met welk doel. Bij vertrouwelijke of beveiligingsgevoelige informatie beoordelen we per verzoek wat passend kan worden gedeeld en onder welke voorwaarden.

Security- of leveranciersvragenlijsten

Klanten kunnen ook een security- of leveranciersvragenlijst aanleveren. We stemmen vooraf af welke informatie nodig is en hoe eventuele documenten veilig kunnen worden aangeleverd.

7. Conclusie

Met het behalen van de proefaudit is de belangrijkste tussenstap gezet. 1Key ligt op koers voor certificering in november 2026, mits de documentatie voor fase 1 volledig is en de bewijsvoering tot en met fase 2 consequent wordt bijgehouden.