

EV

EERLIJK VEILIG

VOORBEELDRAPPORT - SYNTHETISCHE ORGANISATIE

Eerlijke Security Scan

Van aandachtspunten naar een uitvoerbaar verbeterpad

Voorbeeldbedrijf B.V.

Scope: Microsoft 365, digitale basis, SaaS en AI-gebruik

Rapportdatum: juli 2026 | Status: concept voor menselijke review

READINESS

62 / 100

RISICOBAND

Middel

EVIDENCE

68%

Dit document bevat uitsluitend fictieve data en laat de vorm en diepgang van een scan zien.



MANAGEMENTOVERZICHT

Waar de organisatie nu staat

Voorbeeldbedrijf B.V. heeft een bruikbare digitale basis, maar de inrichting is niet overal aantoonbaar beheerst. De hoogste prioriteit ligt bij beheeraccounts, hersteltoegang, e-mailvertrouwen en eigenaarschap van SaaS- en AI-tools. De score is een praktische readiness-inschatting op basis van beperkte, synthetische evidence.

62 / 100	Middel	68%
Readinessscore	Risicoband	Evidence-dekking

Directiebesluit voor de komende 30 dagen

1. Wijs een eigenaar aan voor identity, hersteltoegang en e-mailvertrouwen.
2. Laat beheerrollen, MFA-dekking en herstelaccounts aantoonbaar controleren.
3. Maak een compact register van SaaS- en AI-tools met eigenaar en toegestane data.

Domeinbeeld

Identity en toegang		52
Back-up en continuïteit		71
Incidentrespons		58
AI-governance		46
Leveranciers		63

TOP FINDINGS

Aandachtspunten die eerst bewijs en actie vragen

Hoog

F-01 | Beheeraccounts en hersteltoegang niet volledig aantoonbaar

Niet voor alle globale beheerders is sterke MFA en een afzonderlijk herstelpad aangetoond. Hierdoor kan een incident langer duren en is de impact van accountmisbruik groter.

Evidence: Q-ID-02, Q-ID-05 | Confidence: middel

Hoog

F-02 | DMARC staat nog niet op een handhavend beleid

SPF en DKIM zijn gedeeltelijk aanwezig, maar de organisatie heeft nog geen gevalideerd pad naar quarantine of reject. Dit vergroot het risico op misbruik van het e-maildomein.

Evidence: Q-EXT-03, DNS-observatie-01 | Confidence: hoog

Middel

F-03 | SaaS- en AI-tools missen een vaste eigenaar

Tools worden functioneel gebruikt, maar doel, eigenaar, datacategorie en exit-afspraken zijn niet overal vastgelegd. Daardoor blijven leveranciers- en datarisico's impliciet.

Evidence: Q-AI-04, Q-SUP-06 | Confidence: middel

Middel

F-04 | Hersteltest is niet recent gedocumenteerd

Back-ups zijn ingericht, maar een recente hersteltest met resultaat, eigenaar en opvolgactie ontbreekt. Aanwezigheid van een back-up bewijst nog niet dat herstel binnen de gewenste tijd lukt.

Evidence: Q-BC-03 | Confidence: middel

ACTIEPLAN

30 dagen: risico terugbrengen en bewijs opbouwen

Actie	Eigenaar	Termijn	Bewijs
Beheerrollen en sterke MFA controleren	IT-beheer	Week 1	Export + reviewnotitie
Herstelaccounts en break-glass-proces testen	IT + directie	Week 1	Testverslag
DMARC-pad naar handhaving vastleggen	IT-partner	Week 2	DNS + rapportage
SaaS- en AI-toolregister afronden	Operations	Week 3	Register v1
Hersteltest uitvoeren en evalueren	IT-beheer	Week 4	Herstelbewijs

90 dagen: van losse acties naar beheersing

DAG 31-60	DAG 61-90
Conditional Access-baseline formaliseren, leveranciersregister aanvullen en incidentprocedure oefenen.	Managementreview uitvoeren, open evidence sluiten en een hercheckmoment met scope vastleggen.

Menselijke review vereist: acties, eigenaars en evidence worden voor klantdeling gevalideerd.



SCOPE EN BEPERKINGEN

Wat deze readiness-inschatting wel en niet bewijst

In scope

Microsoft 365 identity en beheer, e-mailvertrouwen, back-up en herstel, incidentbasis, SaaS- en AI-gebruik, leveranciers en managementeigenaarschap.

Aannames

De aangeleverde antwoorden zijn actueel. Technische observaties zijn momentopnames. Niet getoonde configuratie wordt als niet aangetoond behandeld, niet automatisch als afwezig.

Niet uitgevoerd

Geen penetratietest, forensisch onderzoek, broncode-audit, volledige Microsoft Graph-inventarisatie, juridische beoordeling of formele certificeringsaudit.

Vaste disclaimer

Dit rapport is een praktische readiness-inschatting op basis van de aangeleverde informatie en beperkte technische observaties. Het is geen juridisch advies, geen certificering en geen garantie op naleving van AVG, NIS2/Cyberbeveiligingswet of andere wet- en regelgeving.

Over dit voorbeeld

Alle organisatienamen, scores, findings en evidence-referenties in dit document zijn fictief. Het voorbeeld laat zien hoe Eerlijk Veilig managementtaal, herleidbaarheid en uitvoering samenbrengt.

Eerlijk inzicht. Praktisch advies. Hulp bij uitvoering.

Eerlijk Veilig | app.wouterg.nl