Auditrapport

NEN-EN-ISO/IEC 27001:2023 /A1:2024 nl
Transitie audit

Provincie Gelderland
Markt 11 6811CG Arnhem

Auditdatum
donderdag 2 oktober 2025

Remote

Auteur: 5.1.2e @digitrust.nl)
Datum: *Dinsdag 07-10-2025*

Gegevens

Klant:	
Naam	Provincie Gelderland
Adres	Markt 11 6811CG Arnhem
Contact	5.1.2e @gelderland.nl / 0652801997)

Certificerende instantie:	
Naam	DigiTrust B.V.
Adres	Achtseweg Zuid 159R, 5651 GW Eindhoven
KvK	59396822
Accreditatie	RvA C618

Audit:	
Scope ISMS	*Informatiebeveiliging gerelateerd aan en met betrekking tot het organisatieonderdelen Kwaliteit Openbaar Bestuur voor het uitvoeren en beheren van de activiteiten, producten en diensten van het proces BIBOB.* *Dit conform de vastgestelde verklaring van toepasselijkheid d.d. 6-april-2023 versie 1.1 waarin de eisen uit de Baseline Informatiebeveiliging Overheid (BIO) zijn opgenomen.*
Organisatorische en functionele eenheden	*Provincie Gelderland*
Vestigingen in scope	*Markt 11 6811CG Arnhem*
Vestigingen bezocht	*Markt 11 6811CG Arnhem*
Naam en versie VvT op certificaat	*Verklaring van Toepassing NEN-EN-ISO/IEC 27001:2023 A1:2024 nl* *Versie 1.0* *Datum 04-09-2025*
Aantal FTE	*10*

Auditoren:	
Leadauditor	5.1.2e @digitrust.nl)
Auditor(en)	N.v.t.
Auditor in opleiding	N.v.t.
Technisch/ Juridisch deskundige	N.v.t.
Waarnemer	N.v.t.

Auditee:	
Naam en functie	5.1.2e
Naam en functie	
Naam en functie	

Bijzonderheden:	
Audit gecombineerd met andere audit?	Nee
Speciale communicatie-middelen?	Nee
Welke ICT tool is gebruikt?	MS Teams
Was de inzet van het ICT middel effectief mbt het behalen van de auditdoelstellingen?	Ja
Klant werkt met ploegen-diensten?	Nee
Klant spreekt (deels) geen Nederlands?	Nee

Eind conclusie

Conclusie auditor	Op basis van onderstaande beoordeling geeft de Lead Auditor een POSITIEF oordeel. Het ISMS van de organisatie is effectief aangepast conform de nieuwe norm.
Onderbouwing	Uit de transitie audit is naar voren gekomen dat Provincie Gelderland op een juiste wijze het ISMS, wat met name geborgd wordt binnen het Trustbound systeem, op een juiste wijze heeft aangepast naar de nieuwe norm. Bij de overgang van de oude naar de nieuwe norm heeft men gelijk gebruik gemaakt van de wens om het ISMS om te zetten van SCC naar Trustbound. Bij de audit is een Kans voor verbetering vastgesteld op "A.8.9 Configuratiebeheer" (zie details in rapportage)
Tot slot	Wij willen de deelnemers aan deze audit hartelijk danken voor hun ondersteuning en medewerking. Deze rapportage en aanverwante documenten zijn uitsluitend opgesteld voor de cliënt van DigiTrust. DigiTrust aanvaardt geen verantwoordelijkheid (juridisch of anderszins) of aansprakelijkheid in relatie tot elk ander doel waarvoor het rapport kan worden gebruikt of derden die zich beroepen op de inhoud van dit rapport. Indien u kopieën van dit rapport wilt distribueren, dan dienen alle pagina's van dit rapport te worden toegevoegd. Dit auditrapport blijft eigendom van DigiTrust [17021-1:2015/9.4.8.1]

Audit resultaten

Beoordeling transitie	Onderbouwing en bewijslast	Oordeel
GAP analyse	Het ISMS is omgezet van SCC naar Trustbound waarbij ook direct de nieuwe ISO27001:2023 + BIO2.0 is ingevoerd zodat er geborgd wordt dat er gelijk aan de nieuwe norm voldaan wordt. Gezien: Trustbound systeem Plan van aanpak Transitie PG 2027 2022 ISO BIO	Effectief
HLS aanpassingen (H4-H10)	In het beleid zijn alle aanpassingen doorgevoerd welke voortkomen uit de aanpassingen in de ISO27001:2023, als steekproef deze volgende onderdelen expliciet bekeken en beoordeeld. H 4.1 In het beleid is er een artikel opgenomen aangaande invloed van klimaatverandering op de infrastructuur en de operationele processen. Extreme weersomstandigheden kunnen fysieke en digitale infrastructuur verstoren. Hierin wordt bij de risico analyse ook rekening gehouden. H 4.2 Bij de eisen van de stakeholder is beschreven wat deze zijn en hoe deze geborgd worden. Bij de stakeholder analyse is beschreven dat buiten de provincie zelf er geen eisen van de stakeholder zijn aangaande klimaatverandering dan die de eisen c.q. het streven van de provincie zelf om te streven naar duurzame oplossingen. H 4.3 Raakvlakken en afhankelijkheden tussen de activiteiten die door de organisatie en de activiteiten die door andere organisaties worden uitgevoerd is geborgd middels het koppelen van de leveranciers aan de maatregelen waarvan de diensten en maatregelen zijn uitbesteed aan die leveranciers. H 6.2 De doelstellingen worden gemonitord middels diverse overleggen en het bewaken van taken welke zijn opgenomen in het ISMS taakbord in MS teams (Algemeen - Security Team - Algemeen - Bord) H 6.3 In het beleid is er een specifiek artikel gewijd aan wijzigingen in het managementsysteem voor informatiebeveiliging, en hoe deze dan volgens een geplande werkwijze worden uitgevoerd. H 7.4 In een apart document is de gehele communicatie beschreven waarbij ook expliciet is beschreven hoe deze communicatie plaats (kan) vinden. Gezien: DOC-B01 Beleid Informatiebeveiliging PG v1.2 MS teams - Algemeen - Security Team - Algemeen - Bord (KanBan bord) Communicatieplan ISMS PGLD	Effectief
VVT (versie en datum)	De VVT is aangepast naar alle beheermaatregelen vanuit de Annex A van de NEN-EN-ISO/IEC 27001:2023 /A1:2024 nl en de BIO 2.0 norm. De beschrijving in de VVT van de maatregelen komen nog wel voort uit de ISO27002 (waar wordt gesproken over "behoren" in plaats van "moeten". Maar deze wordt door PNB samen met Trustbound nog omgezet naar de beschrijvingen uit de Annex A zodat de VVT weer voldoet aan de eisen vanuit de norm en aantoonbaar gebruik maakt van de beheermaatregelen uit de Annex A. Gezien: VVT ISO27001 Provincie Gelderland	Effectief
Risicoanalyse en behandelplan	Alle risico's zijn opgenomen in TrustBound waarbij dan ook als behandeling de maatregelen uit de Annex A zijn gekoppeld. Gezien: Trustbound - Risk	Effectief
Interne audit (mbt de transitie)	Er is een interne audit uitgevoerd over de hoofdstukken 4 t/m 10 en een steekproef over de beheermaatregelen waarbij in alle nieuwe maatregelen en deel van de aangepaste maatregelen is geaudit. Gezien: Auditplan en verslag Transitie ISO27001 2022 BIO2.0	Effectief
Managementreview (mbt de transitie)	Middels een jaarlijkse directiebeoordeling wordt het volledige ISMS beoordeeld waar alle verplichte onderdelen van de norm zijn opgenomen. Naar aanleiding van interne audit aangaande de transitie is er een apart annotatie opgesteld welke is voorgelegd aan de directie Gezien: Directieannotatie interne audit 24092025 Besluiten, Beoordeling, monitoren actielijst Forum/Directieoverleg (DOC-B-04) Forum en Directieoverleg Datum: 18-06-2025	Effectief

De DigiTrust auditor heeft beoordeeld of de nieuwe en samengevoegde beheersmaatregelen op een juiste en effectieve zijn doorgevoerd in uw ISMS.

27001:2023	27001:2013	Beheersmaatregel 27001:2023	
5. Organisatorische beheersmaatregelen			**Conclusie**
5.1	5.1.1, 5.1.2	Beleidsregels voor informatiebeveiliging	Effectief verwerkt in het ISMS
5.7 - nieuw	6.1.4	Informatie en analyses over dreigingen	
5.8	6.1.5, 14.1.1	Informatiebeveiliging in projectmanagement	
5.9	8.1.1, 8.1.2	Inventarisatie van informatie en andere gerelateerde bedrijfsmiddelen	
5.10	8.1.3, 8.2.3	Aanvaardbaar gebruik van informatie en andere gerelateerde bedrijfsmiddelen	
5.14	13.2.1, 13.2.2, 13.2.3	Overdragen van informatie	
5.15	9.1.1, 9.1.2	Toegangsbeveiliging	
5.17	9.2.4, 9.3.1, 9.4.3	Authenticatie-informatie	
5.18	9.2.2, 9.2.5, 9.2.6	Toegangsrechten	
5.22	15.2.1, 15.2.2	Monitoren, beoordelen en het beheren van wijzigingen van leveranciersdiensten	
5.23 - nieuw	15.x	Informatiebeveiliging voor het gebruik van clouddiensten	
5.29	17.1.1, 17.1.2, 17.1.3	Informatiebeveiliging tijdens een verstoring	
5.30 - nieuw	17.1.3	ICT-gereedheid voor bedrijfscontinuïteit	
5.31	18.1.1, 18.1.5	Wettelijke, statutaire, regelgevende en contractuele eisen	
5.36	18.2.2, 18.2.3	Naleving van beleid, regels en normen voor informatiebeveiliging	

A.5.7
Het bewaken van kwetsbaarheden en monitoren van afwijkend gedrag is uitbesteed aan KPN/Inspark waarbij zij een SOC dienst leveren. Hierbij worden alle dreigingen en/of afwijkingen gesignaleerd en beoordeeld. Indien er dreigingen en/of afwijkend gedrag wordt geconstateerd zal er (eventueel direct) actie worden ondernemen en de provincie direct worden geïnformeerd. Daarnaast wordt een jaarlijks een dreigingsanalyse opgesteld.

Gezien:
e-mail: [#INC-1601075] - InSpark - Security Prov. Gelderland - Suspicoius deletion of certificate database entries - Medium d.d. 29-9-2025

A.5.23
Er is een beleid voor leveranciersrelatie opgesteld waarin de 10 standaard zorgplicht punten vanuit NIS2/CBW zijn opgenomen en hoe deze zijn gekoppeld aan de 23 eisen welke worden gesteld aan de leveranciers.

Gezien:
Algemeen IB Beleid Leveranciers management 2025

A.5.30
In het BCP zijn de eisen opgenomen aangaande ICT-continuïteit. Middels periodieke test wordt er bepaald of er aan voldaan kan worden.
In het IT Herstelplan zijn de Disaster recovery tests opgenomen. Er zijn tevens ook taken gepland om deze aan te passen naar aanleiding van de overgang van de huidige centrale omgeving (OGD) naar de Azure omgeving.

Gezien:
Business Continuiteitsplan BCP (template) 2025 v1.1
IT Service Herstelplan
E-mail: CMP test op Azure server d.d. 30-9-2025

► Aanpassingen in de overige beheermaatregelen van de nieuwe Annex A hebben voor Provincie Gelderland geen invloed gehad op het ISMS.

27001:2023	27001:2013	Beheersmaatregel 27001:2023	
6. Mensgerichte beheersmaatregelen			**Conclusie**
6.8	16.1.2, 16.1.3	Melden van informatiebeveiligingsgebeurtenissen	Effectief verwerkt in het ISMS

A 6.8
► Aanpassingen in de overige beheermaatregelen van de nieuwe Annex A hebben voor Provincie Gelderland geen invloed gehad op het ISMS.

27001:2023	27001:2013	Beheersmaatregel 27001:2023	
7. Fysieke beheersmaatregelen			**Conclusie**
7.2	11.1.2, 11.1.6	Fysieke toegangsbeveiliging	Effectief verwerkt in het ISMS
7.4 - nieuw	9.2.5	Monitoren van de fysieke beveiliging	
7.10	8.3.1, 8.3.2, 8.3.3, 11.2.5	Opslagmedia	

A.7.4
Het provinciehuis van Gelderland wordt actief bewaakt middels o.a. een inbraak alarmsysteem wat gekoppeld is aan Alarmcentrale, bewakers welke een fysieke rondgang doen buiten de openingstijden, Camera bewaking door bewakingspersoneel tijdens openingstijden.

Gezien:
Richtlijn Fysieke toegang (DOC-BB-01H)

► Aanpassingen in de overige beheermaatregelen van de nieuwe Annex A hebben voor Provincie Gelderland geen invloed gehad op het ISMS.

27001:2023	27001:2013	Beheersmaatregel 27001:2023	
8. Technologische beheersmaatregelen			**Conclusie**
8.1	6.2.1, 11.2.8	User endpoint devices'	Effectief verwerkt in het ISMS
8.8	12.6.1, 18.2.3	Beheer van technische kwetsbaarheden	
8.9 - nieuw	14.2.5	Configuratiebeheer	
8.10 - nieuw	18.1.3	Wissen van informatie	
8.11 - nieuw	14.3.1	Maskeren van gegevens	
8.12 - nieuw	12.6.1	Voorkomen van gegevenslekken (data leakage prevention)	
8.15	12.4.1, 12.4.2, 12.4.3	Logging	
8.16 - nieuw	12.4.x	Monitoren van activiteiten	
8.19	12.5.1, 12.6.2	Installeren van software op operationele systemen	
8.23 - nieuw	13.1.2	Toepassen van webfilters	
8.24	10.1.1, 10.1.2	Gebruik van cryptografie	
8.26	14.1.2, 14.1.3	Toepassingsbeveiligingseisen	
8.28 - nieuw	14.2.1	Veilig coderen	
8.29	14.2.8, 14.2.9	Testen van de beveiliging tijdens ontwikkeling en acceptatie	
8.31	12.1.4, 14.2.6	Scheiding van ontwikkel-, test- en productieomgevingen	
8.32	12.1.2, 14.2.2, 14.2.3, 14.2.4	Wijzigingsbeheer	

A.8.9
Middels Intune worden de configuratie (vanuit de policies) worden de werkplekken afgedwongen en beheerd zodat werkplekken qua configuratie altijd voldoen aan het beleid hiervoor.
KVV: Voor overige systemen zoals infrastructuur, applicaties e.d. waren deze tijdens de audit voor de transitie niet aantoonbaar gemaakt.

Gezien:
MS Intune

A.8.10
Binnen de Provincie Gelderland is er een aparte afdeling (DIV - Documentaire Informatievoorziening) welke er op toeziet en werkzaamheden uitvoert zodat er blijvend voldaan wordt aan de archiefwet.

Gezien:
Beleid en inrichtingsprincipes op het gebied van de documentaire informatievoorziening (DIV)

A.8.11
Indien informatie gepubliceerd/vrijgegeven moet worden (Bv WOO) dan wordt er gebruik gemaakt van Zylab om vertrouwelijke (niet openbare informatie) te maskeren (zwart maken).

Gezien:
https://docs.zylab.com/documentation/Home.html

A.8.12
Alle werkplekken van de Provincie Gelderland zijn zodanig ingericht middels policies in MS Intune zodat de kans op datalekken wordt geminimaliseerd. Deze inrichting van de werkplekken zijn ook middels een Pentest door Securesult beoordeeld

Gezien:
Rapport Provincie Gelderland infrastructuur v1.0.pdf (o.a pentest van Veilige Digitale Werkplek)

A.8.16
Het bewaken van kwetsbaarheden en monitoren van afwijkend gedrag is uitbesteed aan KPN/Inspark waarbij zij een SOC dienst leveren. Hierbij worden alle dreigingen en/of afwijkingen gesignaleerd en beoordeeld. Indien er dreigingen en/of afwijkend gedrag wordt geconstateerd zal er (eventueel direct) actie worden ondernemen en de provincie direct worden geïnformeerd. Daarnaast wordt een jaarlijks een dreigingsanalyse opgesteld.

Gezien:
e-mail: [#INC-1601075] - InSpark - Security Prov. Gelderland - Suspicoius deletion of certificate database entries - Medium d.d. 29-9-2025

A.8.23
Alle werkplekken worden beschermd middels MS Defender waarbij in de M365 tenant van de prov. Gelderland aanvullend bepaalde websites met specifieke content ook wordt geblokkeerd. Ms Defender blokkeert standaard al kwaadaardige inhoud van websites.

Gezien:
MS Intune

A.8.28
De principes voor veilig coderen zijn opgenomen in de Richtlijn Softwareontwikkeling. Hierin is bijvoorbeeld opgenomen dat wanneer codewijzigingen door een ontwikkelaar middels een PullRequest klaarzet een co-ontwikkelaar deze moet beoordelen en deze dan kan afkeuren of goedkeuren alvorens deze op te nemen in de Branch

Gezien:
Richtlijn Softwareontwikkeling (DOC-BB-01P)

► Aanpassingen in de overige beheermaatregelen van de nieuwe Annex A hebben voor Provincie Gelderland geen invloed gehad op het ISMS.