Assessmentprocedure audits informatiebeveiliging 2026-2027

1. Toepassingsgebied

1.1 Deze procedure:

1.1.1 Is geldig vanaf 1 januari 2026.

1.1.2 Is van toepassing op alle certificeringsaudits informatiebeveiliging, uitgevoerd op basis van het NEN 7510 normenkader.

1.2 Scope audits informatiebeveiliging

- De zorgorganisatie stelt het toepassingsgebied van het managementsysteem voor informatiebeveiliging vast tijdens de implementatie van informatiebeveiliging.
- De scope van het certificeringstraject omvat de norm NEN7510: Informatiebeveiliging in de zorg. Dit in overeenstemming met het toepassingsgebied van het managementsysteem voor informatiebeveiliging en de Verklaring van Toepasselijkheid van de zorgorganisatie.
- Het toepassingsgebied van het managementsysteem voor informatiebeveiliging van de zorgorganisatie moet duidelijk maken welke activiteiten, producten en/of diensten betrekking hebbende op het beheer van persoonlijke gezondheidsinformatie zijn uitbesteed, waarbij de van toepassing zijnde beheersmaatregelen uit de Verklaring van Toepasselijkheid (VvT) worden gespecificeerd.
- Voor de zorgorganisaties die een aanvraag indienen voor audit informatiebeveiliging is het, conform NCS 7510, niet acceptabel dat het toepassingsgebied van het managementsysteem voor informatiebeveiliging beperkt is tot delen van de organisatie die niet betrokken zijn bij de primaire gezondheidszorgprocessen. Het toepassingsgebied van het managementsysteem voor informatiebeveiliging omvat derhalve altijd de primaire gezondheidszorgprocessen van de zorginstelling.

1.2.1 Qualicor Europe en de zorgorganisatie leggen de afspraken minimaal zes maanden voor de initiële- of hercertificeringsaudit vast in de intakeagenda:

1.2.1.1 De zorgorganisatie draagt zorg dat de in- en exclusiecriteria (welke locaties worden meegenomen in de audit) vastgelegd worden in de intakeagenda tijdens het intakegesprek voorafgaand aan de initiële- of hercertificeringsaudit informatiebeveiliging.

- Ondersteunende dienstverlening van leveranciers die wordt gefaciliteerd op basis van SLA's (servicelevel agreements) en verwerkersovereenkomsten en zijn geëxcludeerd in dit certificeringstraject. De zorgorganisatie draagt er zorg voor dat de in- en exclusies van de audit (lijst met deze ondersteunende dienstverlening) correct vastgelegd worden tijdens het intakegesprek voorafgaand aan de initiële audit informatiebeveiliging.
- De organisatie geeft aan welke beheersmaatregelen van de NEN7510-2 in en buiten scope vallen (zie ook NEN7510:1-6.1.3) en legt dit vast in de VvT.

1.2.1.2 De zorgorganisatie wordt getoetst op de versie van de van toepassing zijnde normenset informatiebeveiliging, die Qualicor Europe minimaal twaalf maanden voorafgaand aan de initiële of hercertificeringsaudit informatiebeveiliging publiceert. De van toepassing zijnde versie van de normenset wordt vastgelegd in de intakeagenda.

1.3 Audits informatiebeveiliging als onderdeel van het Continu Verbeterprogramma

1.3.1 De audits informatiebeveiliging in de zorg worden in principe tegelijkertijd met de sequential audits uitgevoerd.

- De certificering voor informatiebeveiliging in de zorg geldt voor een periode van vijf jaar, mits voldaan wordt aan de certificeringsvoorwaarden (zie paragraaf 4).
- Minimaal vier en maximaal zes weken voor de initiële of hercertificeringsaudit vindt een documentanalyse plaats door het auditteam. Dit is een analyse van de verplichte documentatie (zie bijlage 1) van het information security managementsystem (ISMS). De documenten worden minimaal zes weken voor de documentanalyse door de zorgorganisatie aangeleverd.
  De zorgorganisatie stemt met Qualicor Europe af hoe de gevraagde documenten aangeleverd kunnen worden. Op basis van de documentanalyse wordt in overleg met de zorgorganisatie besloten of de audit informatiebeveiliging door kan gaan op de geplande data.
- Tijdens de initiële- en hercertificeringsaudit worden alle eisen voor informatiebeveiliging, op basis van de NEN7510 deel 1 (het ISMS) getoetst en wordt minimaal 80% van de NEN7510 deel 2 (de beheersmaatregelen) getoetst.

1.3.2 In bijlage 2 is uitgewerkt op welke wijze, in welke fase en op welke manier tijdens de initiële en hercertificeringsaudit de NEN7510 deel 1 en de NEN7510 deel 2 getoetst worden.

1.3.3 De eerste opvolgaudit wordt gepland 20 maanden, plus of min twee maanden, na de datum (maand) van de initiële audit, en tegelijkertijd met een sequential audit.

1.3.4 De tweede opvolgaudit wordt gepland 40 maanden, plus of min twee maanden, na de datum (maand) van de initiële audit, en tegelijkertijd met een sequential audit.

1.3.5 Tijdens de opvolgaudits worden getoetst:

- Alle minor non conformities (NC) (zie 3.3.1 voor de definitie van een NC);
- De in de initiële of hercertificeringsaudit niet getoetste beheersmaatregelen op basis van de NEN7510 deel 2;
- Een door de instelling aangegeven focus van de beheersmaatregelen;
- In bijlage 3 is uitgewerkt welke onderdelen van het ISMS en de beheersmaatregelen tijdens de opvolgaudits beoordeeld worden.
- Als de auditor op basis van bovenstaande onderdelen tot een bevinding komt, kan de auditor aanpalende normelementen en of beheersmaatregelen toetsen.

1.3.6 Vijf jaar na de initiële audit start een nieuwe cyclus, met een hercertificeringsaudit.

1.4 Audits informatiebeveiliging als onderdeel van het standaard auditprogramma (een keer per vier jaar een organisatiebrede audit)

1.4.1 De initiële of hercertificeringsaudit wordt indien mogelijk tegelijkertijd met de organisatiebrede accreditatieaudit uitgevoerd.

- De certificering voor informatiebeveiliging in de zorg geldt voor een periode van vier jaar bij voldoen aan de certificeringsvoorwaarden (zie paragraaf 4).
- Minimaal vier en maximaal zes weken voor de initiële of hercertificeringsaudit vindt een documentanalyse plaats door het auditteam. Dit is een analyse van de verplichte documentatie (zie bijlage 1) van het ISMS. De documenten worden minimaal zes weken voor de documentanalyse door de zorgorganisatie aangeleverd. De zorgorganisatie stemt met Qualicor Europe af hoe de gevraagde documenten aangeleverd kunnen worden. Op basis van de documentanalyse wordt in overleg met de zorgorganisatie besloten of de audit informatiebeveiliging door kan gaan op de geplande data.

1.4.2 In bijlage 2 is uitgewerkt op welke wijze, in welke fase en op welke manier tijdens de initiële en hercertificeringsaudit de NEN7510 deel 1 en de NEN7510 deel 2 getoetst worden.

1.4.3 Zestien maanden, plus of min twee maanden, na de initiële audit vindt de eerste opvolgaudit plaats en 32 maanden, plus of min twee maanden, na de initiële audit vindt de tweede opvolgaudit plaats.

- Tijdens de initiële- en de hercertificeringsaudit worden alle eisen voor informatiebeveiliging, op basis van de NEN7510 deel 1 getoetst en wordt minimaal 80% van de NEN7510 deel 2 getoetst.

1.4.4 In bijlage 2 is uitgewerkt op welke wijze, in welke fase en op welke manier tijdens de initiële audit de NEN7510 deel 1 en de NEN7510 deel 2 getoetst worden.

1.4.5 Tijdens de opvolgaudits worden getoetst:

- Alle minor non conformities (NC) (zie 3.3.1);
- De in de initiële- of hercertificeringsaudit niet getoetste beheersmaatregelen op basis van de NEN7510 deel 2;
- Een door de instelling aangegeven focus van de beheersmaatregelen;
- In bijlage 3 is uitgewerkt welke onderdelen van het ISMS en de beheersmaatregelen tijdens de opvolgaudits beoordeeld worden.
- Als de auditor op basis van bovenstaande onderdelen tot een bevinding komt, kan de auditor aanpalende normelementen en of beheersmaatregelen toetsen.

1.4.6 Vier jaar na de initiële audit start een nieuwe cyclus, met een hercertificeringsaudit.

2. Aanvraagprocedure

2.1 Planning audit(s)

2.1.1 In het geval van een initiële- of hercertificeringsaudit audit stuurt de zorgorganisatie een schriftelijk verzoek met voorkeursdata voor de audit naar Qualicor Europe.

2.1.2 In het geval van een opvolgaudit, wordt de audit gepland conform de termijnen in 1.3 (audits die onderdeel zijn van het Continu Verbeterprogramma) of 1.4 (audits die onderdeel zijn van het standaard auditprogramma).

2.1.3 Qualicor Europe controleert de aanvraag en stuurt de zorgorganisatie de planning van het certificeringstraject. Zo nodig is er overleg over de datum met de instellingscontactpersoon.

2.1.4 De zorgorganisatie ontvangt een bevestiging van de aanvraag met de geplande audit datum/data.

3. De audit

3.1 Auditteam

3.1.1 De auditoren werken volgens het 'Reglement auditoren' en hebben het ISQua geaccrediteerde Surveyor Training Program van Qualicor Europe succesvol doorlopen. De auditoren hebben aantoonbaar kennis van de NEN7510.

3.1.2 De auditoren informatiebeveiliging voldoen aan de voorwaarden van het profiel auditor informatiebeveiliging.

3.1.3 Iedere auditor wordt voorgelegd aan de zorgorganisatie ter accordering.

3.1.4 De zorgorganisatie kan gemotiveerd bezwaar maken tegen de voorgedragen auditor(-en).

3.1.5 Als het bezwaar gegrond wordt geacht, wordt een andere auditor voorgesteld.

3.2 Auditorbevindingen

3.2.1 De zorgorganisatie verschaft Qualicor Europe alle informatie, stelt de medewerking van alle medewerkers beschikbaar, biedt inzage in bescheiden - binnen grenzen van wettelijke voorschriften -

en geeft Qualicor Europe toegang tot alle ruimtes in de zorgorganisatie, voor zover in redelijkheid nodig om de audit goed uit te kunnen voeren. De zorgorganisatie zal ook ongevraagd al die informatie aanreiken, waarvan zij in redelijkheid kan begrijpen dat die van belang is voor een zorgvuldige uitvoering van de audits.

3.2.2 De auditoren schrijven een auditverslag op basis van hun bevindingen tijdens de audit.

3.2.3 Qualicor Europe legt het concept auditverslag voor aan de verantwoordelijk bestuurder/algemeen directeur van de zorgorganisatie ter controle op feitelijke onjuistheden. De zorgorganisatie krijgt een week de tijd voor de reactie op feitelijke onjuistheden.

3.2.4 De door de zorgorganisatie aangereikte feitelijke onjuistheden worden door het auditteam beoordeeld en na beoordeling door de auditoren wordt het auditverslag eventueel aangepast. De zorgorganisatie ontvangt het definitieve verslag uiterlijk twee weken na de ontvangst van de feitelijke onjuistheden.

3.2.5 Een definitief verslag bij een initiële of hercertificeringsaudit wordt toegestuurd aan de zorgorganisatie na bespreking in het College Kwaliteitsverklaringen (CKV).

3.2.6 De motivatie om de feitelijke onjuistheden wel/niet te verwerken, wordt schriftelijk onderbouwd teruggekoppeld aan de zorgorganisatie.

3.3 Non conformities (NC)

3.3.1 Bij de beoordeling van de informatiebeveiliging maken de auditoren onderscheid tussen major en minor NC:

- 3.3.1.1 Een minor NC is een afwijking die niet van invloed is op het vermogen van het managementsysteem informatiebeveiliging om de beoogde resultaten te behalen.
- 3.3.1.2 Een major NC is een afwijking die van invloed is op het vermogen van het managementsysteem informatiebeveiliging om de beoogde resultaten te behalen.

3.3.2 De termijn om major NC op te volgen is maximaal zes maanden. Binnen deze periode wordt het volgende verwacht van de zorgorganisatie:

- 3.3.2.1 Onmiddellijke herstelmaatregel om de effecten van de NC als zodanig op te heffen.
- 3.3.2.2 Het uitvoeren van een oorzaakanalyse om corrigerende maatregelen vast te stellen om het opnieuw optreden van de tekortkoming te voorkomen.
- 3.3.2.3 Het implementeren van corrigerende maatregelen en het verifiëren van de doeltreffendheid van deze maatregelen.
- 3.3.2.4 Het rapporteren aan Qualicor Europe met daarbij gevoegd relevante ondersteunende documentatie.

3.3.3 In het geval één of meerdere major NC geconstateerd zijn tijdens de audit, vindt, binnen zes maanden nadat het definitief verslag ontvangen is, een toets op uitgesteld besluit (TUB) plaats.

3.3.4 In het geval één of meerdere minor NC geconstateerd zijn tijdens de audit, vindt follow up in de regel plaats in de vorm van een schriftelijk verificatie op basis van de aangeleverde documentatie waaruit blijkt dat de minor NC is gemitigeerd. Qualicor Europe kan ervoor kiezen de follow-up plaats te laten vinden in de vorm van een TUB.

3.3.5 Een onvoldoende reactie op NC of het onvoldoende uitvoeren van corrigerende maatregelen kan leiden tot het intrekken van de certificering.

4. Assessmentbesluit

4.1.1 Het auditverslag van een initiële- en een hercertificeringsaudit wordt, nadat de zorgorganisatie heeft gereageerd op de feitelijke onjuistheden, ter validatie voorgelegd aan een onafhankelijke auditor

(validatie auditor) die niet betrokken is geweest bij de audit, of de organisatie die geaudit is. De validatie auditor beoordeelt het auditverslag en de onderbouwing van de geconstateerde non conformities aan de hand van het validatieformulier en stelt een advies op over de te verstrekken certificering.

4.1.2 Het validatieformulier wordt vervolgens toegestuurd aan het auditteam.

4.1.3 Na de validatie wordt het auditverslag definitief vastgesteld.

4.1.4 Verslagen zonder major NC en waarbij aan meer dan 70% van de getoetste beheersmaatregelen is voldaan, worden met het validatieformulier en certificeringsadvies ter beoordeling voorgelegd aan het College Kwaliteitsverklaringen (CKV). Het CKV adviseert de CEO van Qualicor Europe over het besluit tot certificering, op basis van het schema in bijlage 4.

4.1.5 Qualicor Europe kan een positief (zie 4.2), uitgesteld (zie 4.3) of negatief (zie 4.4) besluit nemen.

4.1.6 Qualicor Europe stelt na het besluit van de CEO het definitieve auditverslag ter beschikking aan de zorgorganisatie.

4.1.7 Zorgorganisaties met één tot drie major NC zijn nog niet certificeerbaar. Qualicor Europe neemt dan een uitgesteld besluit (UB) en voert binnen zes maanden een on-site TUB uit (artikel 4.3).

4.1.8 Zorgorganisaties met vier of meer major non conformities zijn niet certificeerbaar en ontvangen een negatief besluit (zie 4.4). Een nieuwe initiële audit is nodig om voor certificering in aanmerking te komen

4.1.9 Zorgorganisaties die geen major non conformity scoren zijn certificeerbaar (zie 4.2) als minimaal 80% van de beheersmaatregelen is getoetst, waarvan minimaal 70% is voldaan. Zorgorganisaties die hier niet aan voldoen zijn nog niet certificeerbaar. Qualicor Europe neemt dan een uitgesteld besluit en voert binnen zes maanden een on-site TUB uit (artikel 4.3).

4.2 Positief besluit

4.2.1 Qualicor Europe neemt een positief besluit als er geen major NC zijn vastgesteld en als de zorginstelling aan meer dan 70% van de beheersmaatregelen die getoetst zijn heeft voldaan.

4.2.2 Bij een positief besluit kent Qualicor Europe certificering toe aan de organisatie met een bepaalde geldigheidsduur (1.3.1 en 1.4.1).

4.2.3 Aan een positief besluit kan als voorwaarde een voortgangsrapportage zijn verbonden, op basis van de geconstateerde minor NC.

4.2.4 De voortgang van de NC wordt bij de eerstvolgende opvolgaudit geverifieerd.

4.2.5 Een onvoldoende reactie op de NC of het onvoldoende uitvoeren van corrigerende maatregelen kan leiden tot het intrekken van de certificering.

4.3 Uitgesteld besluit

4.3.1 Bij een uitgesteld besluit wordt nog geen certificering toegekend aan de zorgorganisatie.

4.3.2 Binnen zes maanden na het uitgesteld besluit voert Qualicor Europe een TUB uit om de major NC en/of de minor NC van het ISMS te toetsen op voortgang, waarna besloten wordt of de certificering alsnog wordt toegekend aan de zorgorganisatie.

4.3.3 De kosten voor de TUB worden doorbelast aan de zorgorganisatie.

4.3.4 In het geval een TUB leidt tot een positief besluit gaat de geldigheidsduur in op de eerste van de maand volgend op de datum van de initiële of hercertificeringsaudit.

4.4 Negatief besluit

4.4.1 Als de zorgorganisatie niet voldoet aan de vereisten voor de informatiebeveiliging (4.1.1 tot en met 4.1.9) kan Qualicor Europe een negatief besluit nemen. Aan de organisatie wordt dan geen certificering toegekend.

4.4.2 Een eventueel eerder door Qualicor Europe afgegeven en nog geldige certificering vervalt op de datum van het negatief besluit.

4.4.3 Na een negatief besluit zal een zorgorganisatie opnieuw een initiële audit informatiebeveiliging moeten laten uitvoeren om voor certificering in aanmerking te komen.

4.5 Klachten en Beroep

4.5.1 Tegen het besluit van Qualicor Europe staat beroep open volgens het Reglement Klachten en Beroep dat is gepubliceerd op de website van Qualicor Europe.

Bijlage 1: Overzicht verplichte documentatie audit informatiebeveiliging

NEN7510: Deel 1

Nummer	Verplichte documentatie	NEN 7510-1:2017	NEN 7510-1:2024
1.	Toepassingsgebied	4.3	4.3
2.	Informatiebeveiligingsbeleid	5.2	5.2
3.	Risicobeoordelingsprocedure	6.1.2	6.1.2
4.	Risicobehandelingsprocedure	6.1.3	6.1.3
5.	Verklaring van Toepasselijkheid (VvT)	6.1.3d	6.1.3d
6.	Plan behandeling informatiebeveiligingsrisico's	6.1.3e	6.1.3e
7.	Informatiebeveiligingsdoelstellingen	6.2	6.2
8.	Bewijs van competenties	7.2	7.2
9.	Informatie over proces(beheersing)	8.1	8.1
10.	Resultaten van risicobeoordelingen	8.2	8.2
11.	Resultaten van behandeling risico's	8.3	8.3
12.	Resultaten van monitoring en meten	9.1	9.1
13.	Bewijsmateriaal auditprogramma	9.2	9.2.2
14.	Resultaten van (interne) audits	9.2	9.2.2
15.	Resultaten van management review/directiebeoordeling	9.3	9.3.3
16.	Bewijsmateriaal aard van de afwijkingen en getroffen maatregelen	10.1	10.2
17.	Resultaten van correctieve acties	10.1	10.2

NEN7510: deel 2

Nummer	Verplichte documentatie	NEN 7510-2:2017	NEN 7510-2:2024
1.	Informatiebeveiligingsbeleid	A.5.1.1	A.5.1
2.	Definities verantwoordelijkheden	A.6.1.1	A.5.2
3.	Inventaris van bedrijfsmiddelen	A.8.1.1	A.5.9
4.	Regels t.a.v. aanvaardbaar gebruik van bedrijfsmiddelen	A.8.1.3	A. 5.10
5.	Logisch toegangsbeleid	A9.1.1	A.5.15
6.	Gedocumenteerde bedieningsprocedures	A.12.1.1	A.5.37
7.	Vertrouwelijkheids- of geheimhoudingsovereenkomst	A.13.2.4	A.6.6
8.	Principes voor engineering van beveiligde systemen	A.14.2.5	A.8.27
9.	Informatiebeveiligingsbeleid voor leveranciersrelaties	A.15.1.1	A.5.19
10.	Leveranciersovereenkomsten		A.5.20
11.	Respons op informatiebeveiligingsincidenten	A.16.1.5	A.5.26
12.	Informatiebeveiligingscontinuïteit implementeren	A.17.1.2	A.5.29
13.	Vaststellen van toepasselijke wetgeving en contractuele eisen	A.18.1.1	A.5.31
14.	Informatiebeveiligingseisen voor nieuwe of verbeteringen aan bestaande informatiesystemen.		A.5.38
15.	PEN-test rapportage		A.8.8
16.	Configuratiebeheer		A.8.9
17.	Herstel procedures		A.8.13
18.	Logging beleid		A.8.15
19.	Eisen kloksynchronisatie		A.8.17
19.	OTAP-beleid		A.8.31
20.	Wijzigingsbeheer		A.8.32

Bijlage 2: Specifieke aandachtspunten Initiële audit/hercertificeringsaudit

Scope audit	Fase 1 - documentanalyse	Fase 2 – audit op locatie	Relevante NEN 7510 Normelementen
Interne audit	**Check op volledigheid:** **Initiële audit** Volledig uitgevoerde interne audit deel 1 en 2. **Hercertificering** In afgelopen cyclus zijn alle onderdelen deel 1 en 2 minimaal eenmaal tijdens interne audit gecontroleerd.	**Gedetailleerde beoordeling**	9.2 Interne audit
Directiebeoordeling/ Management review	**Check op volledigheid**: Volledig uitgevoerde beoordeling met besluitvorming	**Gedetailleerde beoordeling**	9.3 Directiebeoordeling (2017) 9.3 Management review (2024)
Scope en toepassingsgebied ISMS	**Check op volledigheid**: Toepassingsgebied vastgesteld en passend bij organisatie	**Gedetailleerde beoordeling**	4.1 Organisatie en haar context 4.2 Belanghebbenden en hun eisen 4.3 Toepassingsgebied
Verklaring van Toepasselijkheid (VvT)	**Check op volledigheid**: VvT vastgesteld en passend bij toepassingsgebied	**Gedetailleerde beoordeling**	6.1.3 Behandeling van informatiebeveiligingsrisico's
Verplichte documentatie deel 1	**Check op volledigheid en beoordeling documenten**: zie bijlage 1	**Gedetailleerde beoordeling**	7.5 Gedocumenteerde informatie
Verplichte documentatie deel 2	**Check op volledigheid en beoordeling documenten**: zie bijlage 1	**Gedetailleerde beoordeling**	7.5 Gedocumenteerde informatie
NEN 7510 Deel 1		**Gedetailleerde beoordeling**	
NEN 7510 Deel 2		**Globale beoordeling** (minimaal 80 % van de beheersmaatregelen)	

Bijlage 3: Specifieke aandachtspunten opvolgaudits

Scope audit	Opvolgaudits	Relevante NEN 7510 Normelementen
Interne audit	**Verificatie uitvoering** conform eigen planning zorgorganisatie	9.2 Interne audit
Directiebeoordeling/ Management review	**Verificatie uitvoering** conform eigen planning zorgorganisatie	9.3 Directiebeoordeling (2017) 9.3 Management review (2024)
Scope en toepassingsgebied ISMS	**Herbevestiging / verificatie wijzigingen**	4.1 Organisatie en haar context 4.2 Belanghebbenden en hun eisen 4.3 Toepassingsgebied
Verklaring van Toepasselijkheid (VvT)	**Herbevestiging / verificatie wijzigingen***	6.1.3 Behandeling van informatiebeveiligingsrisico's
Verplichte documentatie deel 1	**Steekproef**	7.5 Gedocumenteerde informatie
Verplichte documentatie deel 2	**Steekproef**	7.5 Gedocumenteerde informatie
NEN 7510 Deel 1	• Minor NC's voorgaande audit • Focus zorgorganisatie	
NEN 7510 Deel 2	• Minor NC's voorgaande audit • Nog niet eerder getoetste beheersmaatregelen • Focus zorgorganisatie	
Beleid	**Verificatie uitvoering** conform eigen planning zorgorganisatie (minimaal jaarlijks en bij significante gebeurtenissen)	5.2 Beleid A.5 Informatiebeveiligingsbeleid (2017) A.5.1 Beleidsregels voor informatiebeveiliging (2024)
Uitvoering IB-processen	**Steekproef verificatie uitvoering** conform eigen planning zorgorganisatie	8.1 Operationele planning en beheersing

Risicobeoordeling	**Verificatie uitvoering** conform eigen planning zorgorganisatie (minimaal jaarlijks en bij significante veranderingen)	8.2 Risicobeoordeling van IB
Monitoren, meten, analyseren en evalueren	**Verificatie uitvoering** conform eigen planning zorgorganisatie	9.1 Monitoren, meten, analyseren en evalueren
Afwijkingen	**Verificatie uitvoering**	10.1 Afwijkingen en corrigerende maatregelen (2017) 10.2 Afwijkingen en corrigerende maatregelen (2024)
Continue verbetering	**Verificatie uitvoering**	5.2**d** Beleid 10.2 Continue verbetering (2017) 10.1 Continue verbetering (2024)

* Als er na een wijziging van de organisatie meer of minder beheersmaatregelen van toepassing zijn, kan een update van het certificaat nodig zijn.

Bijlage 4: Stroomschema audits informatiebeveiliging