| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Voer hier de naam van de geregistreerde rechtspersoon in | | | | | | | |
| Documentnummer:<br>P33 | | | | | Documenttitel:<br>**Beleid inzake audit- en nalevingsmonitoring** | | | | | | | |
| Versie:<br>1.0 | | Ingangsdatum:<br>01.01.2025 | | | Documenteigenaar: | | | | | | | |
| X | Beleid | | Standaard | | Procedure | | Formulier | | Register | | Overig | |

| **Revisiegeschiedenis** | | | | |
|---|---|---|---|---|
| **Revisienummer** | **Revisiedatum** | **Wijzigingen** | **Beoordeeld door** | **Proceseigenaar** |
| | | | | |
| | | | | |

| **Goedkeuringen** | | | |
|---|---|---|---|
| **Naam** | **Functie** | **Datum** | **Handtekening** |
| | | | |
| | | | |

Afgestemd op normen en regelgeving waar van toepassing

| Norm/regelgeving | Clausule/artikel | Opmerking |
|---|---|---|
| ISO/IEC 27001:2022 | Clausules 9.2, 9.3, 10 | |
| ISO/IEC 27002:2022 | Beheersmaatregelen 5.35–5.37 | |
| NIST SP 800-53 Rev.5 | CA-2, CA-5, CA-7 | |
| AVG | Artikelen 24, 32, 33 | |
| EU NIS2 | Artikel 21(2)(g), 27 | |
| EU DORA | Artikelen 10(2)(e), 25 | |
| COBIT 2019 | MEA01, MEA03 | |

**1. Doel**

**1.1 Het doel van dit beleid is het vaststellen en aansturen van het audit- en nalevingsmonitoringsprogramma van de organisatie om:**

1.1.1 de doeltreffendheid van beveiligings- en privacymaatregelen te valideren;

1.1.2 afstemming op toepasselijke normen, wettelijke kaders en contractuele verplichtingen te waarborgen;

1.1.3 niet-conformiteiten, inefficiënties en nalevingsrisico's tijdig te signaleren;

1.1.4 voortdurende verbetering en gereedheid voor certificeringen, beoordelingen en toezichtsonderzoeken te ondersteunen.

1.2 Dit beleid ondersteunt de integriteit en volwassenheid van het managementsysteem voor informatiebeveiliging (ISMS) door gestructureerde, risicogedreven en op bewijsmateriaal gebaseerde audit- en monitoringspraktijken te verankeren.

**2. Reikwijdte**

**2.1 Dit beleid is van toepassing op alle:**

2.1.1 interne bedrijfseenheden, functies en afdelingen;

2.1.2 fysieke locaties, cloudomgevingen, SaaS-platformen en uitbestede diensten;

2.1.3 informatiesystemen, toepassingen, infrastructuur en gegevensactiva die onder het ISMS vallen;

2.1.4 werknemers, contractanten en externe dienstverleners met audit- of nalevingsverplichtingen.

**2.2 Dit beleid omvat:**

2.2.1 interne audits;

2.2.2 externe audits en certificeringsaudits;

2.2.3 technische nalevingsmonitoring;

2.2.4 audits van leveranciers en derde partijen;

2.2.5 corrigerende en preventieve maatregelen (CAPA);

2.2.6 metrieken, dashboards en rapportageprocessen.

2.3 Het is van toepassing op alle relevante raamwerken waaraan de organisatie is onderworpen, waaronder ISO/IEC 27001, AVG, NIS2, DORA en SOC 2.

**3. Doelstellingen**

3.1 Verifiëren van de geschiktheid en doeltreffendheid van geïmplementeerde beheersmaatregelen, beleidslijnen en procedures binnen het ISMS en gerelateerde omgevingen.

3.2 Identificeren en remediëren van tekortkomingen, niet-conformiteiten of beheersingslacunes voordat deze escaleren tot incidenten of overtredingen.

3.3 Waarborgen van blijvende gereedheid voor governancebeoordelingen, externe audits en onafhankelijke certificeringen.

3.4 Genereren van verdedigbaar bewijsmateriaal en audittrails ter ondersteuning van verzoeken van toezichthouders, juridische procedures of assuranceverzoeken van klanten.

3.5 Integreren van auditresultaten in het bredere risicobeheer, de beveiligingsmetrieken en de activiteiten voor voortdurende verbetering van de organisatie.

**4. Rollen en verantwoordelijkheden**

**4.1 Verantwoordelijke voor interne audit / nalevingsmanager**

4.1.1 Plant, roostert en voert interne audits uit op basis van risicoprioriteit.

4.1.2 Beheert het auditregister, coördineert auditactiviteiten en volgt corrigerende maatregelen op.

**4.2 Chief Information Security Officer (CISO)**

4.2.1 Waarborgt dat de auditreikwijdte alle relevante ISMS-elementen en Annex A-beheersmaatregelen omvat.

4.2.2 Houdt toezicht op de verificatie van CAPA en integreert auditresultaten in het beveiligingsprogramma.

[ ... Secties 4.3–8 zijn niet opgenomen in dit voorbeeld. Koop het volledige document voor toegang tot de volledige inhoud. ... ]

**9. Eisen voor herziening en actualisering**

**9.1 Dit beleid moet ten minste jaarlijks worden beoordeeld door de nalevingsmanager en de CISO, of eerder naar aanleiding van:**

9.1.1 wijzigingen in regelgevende, contractuele of certificeringsraamwerken;

9.1.2 significante auditbevindingen of herhaald falen van beheersmaatregelen;

9.1.3 organisatorische herstructurering of wijzigingen in GRC-systemen;

9.1.4 aanbevelingen van externe auditors of feedback van toezichthouders.

**9.2 In het beoordelingsproces moet het volgende worden beoordeeld:**

9.2.1 de auditplanningsmethodologie en frequentie;

9.2.2 wijzigingen in het ISMS-toepassingsgebied of de infrastructuur;

9.2.3 actualisaties van de beheersmaatregelencatalogus of het juridisch register;

9.2.4 consistentie en kwaliteit van auditbewijsmateriaal en CAPA-processen.

**9.3 Alle beleidswijzigingen moeten:**

9.3.1 worden gedocumenteerd in een repository onder versiebeheer;

9.3.2 worden goedgekeurd door het topmanagement;

9.3.3 worden gecommuniceerd aan al het betrokken personeel en worden geïntegreerd in geactualiseerde procedures en bewustwordingsprogramma's.

9.4 Validatie na beoordeling moet bevestigen dat geactualiseerde vereisten zijn verwerkt in het auditregister, nalevingstools en interne monitoringsdashboards.

**10. Gerelateerde beleidslijnen en samenhang**

**10.1 Dit beleid is afgestemd op de volgende gerelateerde beleidslijnen van de organisatie:**

10.1.1 P1 – Informatiebeveiligingsbeleid: definieert het ISMS en legt verantwoording vast voor naleving en voortdurende verbetering.

10.1.2 P5 – Wijzigingsbeheerbeleid: waarborgt auditzichtbaarheid op wijzigingen in infrastructuur en configuratie die van invloed zijn op beheersomgevingen.

10.1.3 P6 – Beleid inzake risicobeheer: integreert audituitkomsten in de evaluatie en behandeling van ondernemingsrisico's.

10.1.4 P14 – Gegevensbewarings- en vernietigingsbeleid: regelt de bewaring van auditbewijsmateriaal, logbestanden en nalevingsregistraties.

10.1.5 P18 – Beleid inzake cryptografische beheersmaatregelen: ondersteunt veilige opslag en overdracht van gevoelige auditgegevens.

10.1.6 P26 – Leveranciersbeveiligingsbeleid: omvat auditrechten, assurancedocumentatie en nalevingstoezicht op leveranciers.

10.1.7 P30 – Incidentresponsbeleid (P30): stemt audits van incidentafhandelingsprocessen af op de assurancedoelstellingen van het ISMS.

10.1.8 P32 – Beleid inzake bedrijfscontinuïteit en herstel na verstoringen: vereist verificatie van continuïteitstesten en naleving van herstelplannen tijdens auditcycli.

## 11. Referentienormen en -raamwerken

11.1 Dit beleid is afgestemd op mondiale normen en wettelijke vereisten voor auditing en continue validatie van naleving.

### 11.2 ISO/IEC 27001:

11.2.1 Clausule 9.2 – Interne audit: vereist regelmatige, risicogebaseerde audits van het ISMS om doeltreffendheid en conformiteit te evalueren.

11.2.2 Clausule 9.3 – Managementbeoordeling: audituitkomsten moeten worden meegenomen in strategische beoordeling en verbetering.

11.2.3 Clausule 10.1 – Niet-conformiteit en corrigerende maatregel: auditbevindingen moeten worden afgehandeld via gedocumenteerde CAPA-procedures.

### 11.3 ISO/IEC 27002:2022 – Beheersmaatregelen 5.35–5.37:

11.3.1 Annex A-beheersmaatregelen 5.35–5.37: bestrijken onafhankelijke beoordeling, naleving van wettelijke en contractuele vereisten en auditlogging.

11.3.2 Bieden implementatierichtlijnen voor het plannen, uitvoeren en verbeteren van audit- en nalevingsprogramma's.

### 11.4 NIST SP 800-53 Rev.5:

11.4.1 CA-2 – Beoordelingen van beheersmaatregelen: vereist routinematige beoordeling van geïmplementeerde beveiligingsmaatregelen.

11.4.2 CA-5 – Plan of Action and Milestones (POA&M): sluit aan op het volgen en remediëren van auditbevindingen.

11.4.3 CA-7 – Continue monitoring: ondersteunt proactieve, geautomatiseerde nalevingsbeoordelingen.

### 11.5 AVG (2016/679):

11.5.1 Artikelen 24 en 32: vereisen aantoonbaar bewijsmateriaal van de implementatie en doeltreffendheid van beveiligingsmaatregelen via passende governancestructuren.

11.5.2 Artikel 33: ondersteunt de noodzaak van geverifieerde audittrails voor respons op inbreuken en meldingen.

### 11.6 EU NIS2-richtlijn (2022/2555):

11.6.1 Artikel 21(2)(g): vereist auditing van beleidslijnen en procedures als onderdeel van minimale maatregelen voor cyberbeveiligingsrisicobeheer.

11.6.2 Artikel 27: nationale autoriteiten kunnen audits uitvoeren of vereisen voor essentiële en belangrijke entiteiten.

**11.7 EU DORA (2022/2554):**

11.7.1 Artikel 10(2)(e): entiteiten moeten interne en externe audits uitvoeren van ICT-risicobeheerpraktijken.

11.7.2 Artikel 25 – Auditvereisten: verplicht periodieke audits door interne of onafhankelijke externe auditors met zichtbaarheid voor toezichthouders.

**11.8 COBIT 2019:**

11.8.1 MEA01 – Monitoren, evalueren en beoordelen van prestaties en conformiteit: waarborgt dat de doeltreffendheid van beheersmaatregelen wordt geverifieerd en gerapporteerd aan governanceorganen.

11.8.2 MEA03 – Monitoren, evalueren en beoordelen van naleving: vereist afstemming van organisatiepraktijken op wettelijke, contractuele en normgebaseerde vereisten.