

				Voer hier de naam van de geregistreerde rechtspersoon in							
Documentnummer: PII02				Documenttitel: Beleid inzake privacyrollen, verantwoordelijkheden en verantwoordingsplicht							
Versie: 1.0		Ingangsdatum: 01.01.2025		Documenteigenaar:							
X	Beleid		Standaard		Procedure		Formulier		Register		Overig

Revisiegeschiedenis				
Revisienummer	Revisiedatum	Wijzigingen	Beoordeeld door	Proceseigenaar

Goedkeuringen			
Naam	Functie	Datum	Handtekening

Juridische kennisgeving (auteursrecht en gebruiksbeperkingen)
(C) 2025 Clarysec LLC. All rights reserved.

Dit document is intellectueel eigendom van Clarysec LLC. Geen enkel deel van dit document mag zonder voorafgaande uitdrukkelijke schriftelijke toestemming worden gekopieerd, hergebruikt, verspreid of gewijzigd voor commerciële of implementatiedoeleinden.

Ongeautoriseerd gebruik is strikt verboden en kan leiden tot juridische stappen.

Neem voor licentiëring contact op via: info@clarysec.com

Afgestemd op normen en regelgeving

Norm/regelgeving	Clausule/beheersmaatregel/artikel	Toepasselijkheid	Dekkingssoort	Opmerking
ISO/IEC 27701:2025	Clause 4.1	Both	Primary	Context van PIMS-rollen
ISO/IEC 27701:2025	Clause 5.1	Both	Primary	Leiderschap en verantwoordingsplicht
ISO/IEC 27701:2025	Clause 5.3	Both	Primary	PIMS-rollen, verantwoordelijkheden en bevoegdheden
ISO/IEC 27701:2025	Clause 7.2	Both	Primary	Rolcompetentie
ISO/IEC 27701:2025	Clause 7.3	Both	Primary	Rolbewustzijn
ISO/IEC 27701:2025	Clause 7.4	Both	Supporting	Rolcommunicatie
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Gedocumenteerde informatie over rollen
ISO/IEC 27701:2025	Clause 8.1	Both	Primary	Eigenaarschap van operationele beheersing
ISO/IEC 27701:2025	Clause 9.2	Both	Supporting	Onafhankelijke auditrol
ISO/IEC 27701:2025	Clause 9.3	Both	Supporting	Directiebeoordeling van verantwoordingsplicht
ISO/IEC 27701:2025	Clause 10.2	Both	Supporting	Rolgerelateerde non-conformiteit en corrigerende maatregelen
ISO/IEC 27701:2025	Annex A.1.2.7	Controller	Supporting	Verantwoordelijkheid voor verwerkerscontracten
ISO/IEC 27701:2025	Annex A.1.2.8	Joint Controller	Primary	Rollen en verantwoordelijkheden van gezamenlijke verwerkingsverantwoordelijken
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Primary	Registraties van verantwoordingsplicht
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Primary	Klantovereenkomsten en instructies voor verwerkers
ISO/IEC 27701:2025	Annex A.2.2.3	Processor	Supporting	Afstemming van verwerkersdoeleinden
GDPR	Article 5(2)	Controller	Supporting	Bewijsmateriaal voor verantwoordingsplicht

GDPR	Article 24	Controller	Supporting	Verantwoordelijkheid en maatregelen van de verwerkingsverantwoordelijke
GDPR	Article 26	Joint Controller	Supporting	Regelingen voor gezamenlijke verwerkingsverantwoordelijken
GDPR	Article 28	Both	Supporting	Governance van verwerkers en instructies
GDPR	Article 30	Both	Supporting	Verwerkingsregistraties en bewijsmateriaal voor verantwoordelijkheid
GDPR	Article 37	Conditional	Referenced	DPO-aanwijzing waar van toepassing
GDPR	Article 38	Conditional	Supporting	Positie en onafhankelijkheid van de DPO waar van toepassing
GDPR	Article 39	Conditional	Supporting	DPO-taken waar van toepassing
ISO/IEC 29100:2020	Clause 4.1; Clause 4.2	Both	Supporting	Actoren en rollen binnen het privacyraamwerk
ISO/IEC 29100:2020	Clause 5.12	Both	Supporting	Verantwoordingsplicht voor privacynaleving
ISO/IEC 29151:2022	Clause 6.1.2; Clause 6.1.3	Both	Supporting	Rollen en functiescheiding voor PII-bescherming
ISO/IEC 27002:2022	Control 5.2	Both	Supporting	Rollen en verantwoordelijkheden voor informatiebeveiliging
ISO/IEC 27002:2022	Control 5.3	Both	Supporting	Functiescheiding

1. Reikwijdte

- 1.1 Dit beleid definieert het PIMS-rollenmodel, de verantwoordingsstructuur, de regels voor toewijzing van verantwoordelijkheden, regels voor rolcombinaties, escalatieverwachtingen en eisen aan bewijsmateriaal voor privacygovernance.
- 1.2 Dit beleid is van toepassing op personeel, functies, systemen, leveranciers, verwerkers, subverwerkers en relaties met gezamenlijke verwerkingsverantwoordelijken die deelnemen aan of invloed hebben op PII-verwerking binnen de PIMS-scope.
- 1.3 Dit beleid is van toepassing in contexten van verwerkingsverantwoordelijke, gezamenlijke verwerkingsverantwoordelijke, verwerker en subverwerker.
- 1.4 Dit beleid creëert geen nieuwe organisatorische functietitels. Het definieert canonieke PIMS-rollen die aan bestaand personeel of bestaande functies kunnen worden toegewezen, mits de roltoewijzing, competentie, onafhankelijkheid en eisen inzake belangenconflicten zijn gedocumenteerd.

2. Doel

- 2.1 Het doel van dit beleid is te waarborgen dat PIMS-verantwoordelijkheden duidelijk worden toegewezen, begrepen, gecommuniceerd, onderbouwd met bewijsmateriaal, beoordeeld en verbeterd.
- 2.2 Dit beleid stelt de organisatie in staat verantwoordingsplicht aan te tonen voor privacygovernance, eigenaarschap van PII-verwerking, bepaling van rollen als verwerkingsverantwoordelijke en verwerker, verdeling van verantwoordelijkheden tussen gezamenlijke verwerkingsverantwoordelijken, afhandeling van verwerkersinstructies, privacyverantwoordelijkheid van leveranciers, onafhankelijke beoordeling en rolgebaseerde escalatie.

3. Doelstellingen

3.1 De doelstellingen van dit beleid zijn:

- 3.1.1 de canonieke PIMS-rollen definiëren die binnen de PIMS-beleidsset worden gebruikt;
- 3.1.2 waarborgen dat voor elke materiële PIMS-verantwoordelijkheid een verantwoordelijke rol is toegewezen;
- 3.1.3 verantwoordingsplicht ondersteunen voor verwerkingsverantwoordelijken, gezamenlijke verwerkingsverantwoordelijken, verwerkers en subverwerkers;
- 3.1.4 praktische rolcombinaties voor kleine en middelgrote organisaties toestaan, terwijl belangenconflicten worden beheerst;
- 3.1.5 onafhankelijke beoordeling door de Internal Audit / Compliance Reviewer behouden;
- 3.1.6 waarborgen dat roltoewijzingen en rolwijzigingen worden vastgelegd in canonieke bewijsobjecten;
- 3.1.7 waarborgen dat PIMS-rolhouders passende communicatie en bewustwording ontvangen;
- 3.1.8 waarborgen dat rolgerelateerde hiaten, conflicten en non-conformiteiten worden geëscaleerd en gecorrigeerd.

4. Beleidsverklaringen

4.1 PIMS-rollenmodel en toewijzing

- 4.1.1 [All] Top Management moet het canonieke PIMS-rollenmodel in REG01 goedkeuren vóór de initiële PIMS-implementatie en daarna jaarlijks.
- 4.1.2 [All] De Privacy Lead / PIMS Manager moet benoemde PIMS-roltoewijzingen in REG01 onderhouden vóór PIMS-implementatie en binnen 10 werkdagen na personele of organisatorische wijzigingen.

- 4.1.3 [All] De Privacy Lead / PIMS Manager moet de verantwoordelijkheidsreikwijdte en het bevoegdheidsniveau voor elke toegewezen PIMS-rol in REG01 documenteren voordat de toewijzing van kracht wordt.
- 4.1.4 [All] De Process Owner / Business Owner moet voor elke PII-verwerkingsactiviteit in REG02 een verantwoordelijke verwerkingseigenaar aanwijzen voordat de verwerkingsactiviteit begint.
- 4.1.5 [All] De System Owner / Application Owner moet de verantwoordelijke systeemeigenaar voor elk PII-verwerkend systeem in REG02 documenteren vóór livegang van het systeem.
- 4.1.6 [All] De Vendor / Procurement Owner moet de relatie-eigenaar voor elke verwerker, subverwerker, gegevensdeling met derden of relatie met een gezamenlijke verwerkingsverantwoordelijke in REG08 documenteren vóór onboarding of goedkeuring van de overeenkomst.

4.2 Rolcombinatie, functiescheiding en onafhankelijkheid

- 4.2.1 [All] De Privacy Lead / PIMS Manager moet elke PIMS-rolcombinatie in REG01 documenteren voordat de rolcombinatie van kracht wordt.
- 4.2.2 [All] Top Management moet rolcombinaties waarbij de Privacy Lead / PIMS Manager, Data Protection Officer / Privacy Advisor, Information Security Lead, Incident Response Coordinator of Internal Audit / Compliance Reviewer betrokken is, vóór toewijzing in REG01 goedkeuren.
- 4.2.3 [All] De Internal Audit / Compliance Reviewer moet vóór de start van elke PIMS-audit of nalevingsbeoordeling in REG12 documenteren dat hij onafhankelijk is van het PIMS-proces dat wordt beoordeeld.
- 4.2.4 [All] De Privacy Lead / PIMS Manager moet compenserende beheersmaatregelen voor onvermijdelijke conflicten in de functiescheiding in REG12 vastleggen voordat een rolcombinatie wordt goedgekeurd.
- 4.2.5 [All] De Data Protection Officer / Privacy Advisor moet zorgen over rOLONAFHANKELIJKHEID of belangenconflicten binnen vijf werkdagen na identificatie in REG12 vastleggen.

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

9. Uitzonderingen

- 9.1.1 [All] De Process Owner / Business Owner moet een uitzondering op rolverantwoordingsplicht in REG12 aanvragen voordat een PII-verwerkingsactiviteit zonder vereiste toegewezen rol wordt uitgevoerd.
- 9.1.2 [All] De Privacy Lead / PIMS Manager moet de impact en mitigatie van elke uitzondering op rolverantwoordingsplicht binnen 10 werkdagen na het verzoek in REG12 beoordelen.
- 9.1.3 [All] Top Management moet uitzonderingen op rolverantwoordingsplicht die langer dan 30 dagen duren of verwerking met hoog risico beïnvloeden in REG12 goedkeuren voordat de uitzondering van kracht wordt.
- 9.1.4 [All] De Privacy Lead / PIMS Manager moet voor elke goedgekeurde uitzondering op rolverantwoordingsplicht vóór goedkeuring in REG12 een vervaldatum vaststellen die niet langer is dan 90 dagen.
- 9.1.5 [All] De Privacy Lead / PIMS Manager moet elke uitzondering op rolverantwoordingsplicht binnen vijf werkdagen na afloop sluiten of opnieuw beoordelen in REG12.

10. Handhaving

- 10.1.1 [All] De Privacy Lead / PIMS Manager moet ontbrekende, onjuiste of verouderde PIMS-roltoewijzingen binnen vijf werkdagen na identificatie als non-conformiteiten in REG12 vastleggen.

- 10.1.2 [All] Top Management moet binnen 15 werkdagen corrigerende maatregelen in REG12 vereisen bij herhaalde of langdurige tekortkomingen in verantwoordingsplicht.
- 10.1.3 [All] De Process Owner / Business Owner moet livegang van nieuwe of gewijzigde PII-verwerking voorkomen wanneer vereist bewijsmateriaal over rollen en verantwoordingsplicht ontbreekt in REG02 of REG08.
- 10.1.4 [All] De Internal Audit / Compliance Reviewer moet de doeltreffendheid van corrigerende maatregelen voor non-conformiteiten inzake rolverantwoordingsplicht verifiëren in REG12 bij de volgende geplande audit of binnen 60 dagen na sluiting, afhankelijk van wat het eerst plaatsvindt.

11. Beoordeling en onderhoud

- 11.1.1 [All] De Privacy Lead / PIMS Manager moet dit beleid jaarlijks en binnen 30 dagen na een wezenlijke wijziging van het PIMS-rollenmodel beoordelen.
- 11.1.2 [All] De Data Protection Officer / Privacy Advisor moet voorgestelde wijzigingen in dit beleid vóór goedkeuring in REG12 beoordelen op impact op privacyrollen.
- 11.1.3 [All] Top Management moet materiële wijzigingen in dit beleid vóór publicatie in REG12 goedkeuren.
- 11.1.4 [All] De Privacy Lead / PIMS Manager moet REG01 en REG11 binnen 15 werkdagen bijwerken na goedgekeurde wijzigingen in PIMS-rollen, verantwoordelijkheden of communicatievereisten.

12. Gerelateerde beleidslijnen

- 12.1 Dit beleid wordt ondersteund door de volgende gerelateerde beleidslijnen:
- 12.2 PII01 - Beleid inzake privacy-informatiemanagementsysteem
- 12.3 PII03 - Beleid inzake PII-verwerkingsinventaris en rechtsgrondslag
- 12.4 PII07 - Beleid inzake privacyrisicobeoordeling en DPIA
- 12.5 PII08 - Beleid inzake privacy by design en privacy by default
- 12.6 PII12 - Beleid inzake privacybeheer voor verwerkers, subverwerkers en derden
- 12.7 PII14 - Beleid inzake PII-beveiliging en toegangscontrole
- 12.8 PII15 - Beleid inzake PII-incidenten en datalekbeheer
- 12.9 PII16 - Beleid inzake privacytraining, bewustwording en competentie
- 12.10 PII17 - Beleid inzake gedocumenteerde PIMS-informatie en bewijsmateriaalbeheer
- 12.11 PII18 - Beleid inzake PIMS-monitoring, audit en verbetering

13. Referentienormen en -raamwerken

- 13.1 Dit beleid is gekoppeld aan de volgende normen en regelgeving. De koppeling licht toe hoe het beleid de aangehaalde eisen ondersteunt en identificeert de interne clausules die deze implementeren of ondersteunen.

13.2 ISO/IEC 27701:2025

- 13.2.1 **Clause 4.1** - Gekoppeld aan het bepalen van de context van PIMS-rollen, toepasselijkheid voor verwerkingsverantwoordelijke en verwerker, verwerkingseigenaarschap en registraties van relatieverantwoordelijkheid. Addressed by clauses [4.3.5; 5.1.5; 5.1.7; 7.1.2].
- 13.2.2 **Clause 5.1** - Gekoppeld aan goedkeuring door Top Management, toezicht op verantwoordingsplicht, jaarlijkse directiebeoordeling, metrieken over verantwoordingsplicht en corrigerende maatregelen voor tekortkomingen in rollen. Addressed by clauses [4.1.1; 4.2.2; 5.1.1; 6.1.1; 8.1.6; 10.1.2; 11.1.3].
- 13.2.3 **Clause 5.3** - Gekoppeld aan toewijzing, documentatie, communicatie en onderhoud van PIMS-rollen, verantwoordelijkheden, bevoegdheden, systeemeigenaarschap,

- verwerkingseigenaarschap, eigenaarschap van leveranciersrelaties, eigenaarschap van incidentescalatie en verantwoordelijkheid voor onafhankelijke beoordeling. Addressed by clauses [4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.1.6; 4.4.2; 4.4.3; 5.1.2; 5.1.3; 5.1.4; 5.1.5; 5.1.6; 5.1.7; 5.1.8; 5.1.9].
- 13.2.4 **Clause 7.2** - Gekoppeld aan rolspecifieke competentie en bewustwordingsbewijsmateriaal voor toegewezen PIMS-verantwoordelijkheden. Addressed by clauses [7.1.4; 8.1.5].
- 13.2.5 **Clause 7.3** - Gekoppeld aan bewustzijn van toegewezen PIMS-verantwoordelijkheden, bewijsmateriaal van kennisname en jaarlijkse rapportage over rolbewustwording. Addressed by clauses [4.5.1; 4.5.2; 7.1.4; 8.1.5].
- 13.2.6 **Clause 7.4** - Gekoppeld aan communicatie van roltoewijzingen, rolwijzigingen, escalaties en informatie over roloverdracht. Addressed by clauses [4.5.1; 4.5.4; 6.1.5; 7.1.6].
- 13.2.7 **Clause 7.5** - Gekoppeld aan gedocumenteerde informatie voor PIMS-roltoewijzingen, verantwoordelijkheidsreikwijdten, bevoegdheidsniveaus, jaarlijkse bewaring van bewijsmateriaal en onderhoud van de rollenmatrix. Addressed by clauses [4.1.2; 4.1.3; 4.5.3; 7.1.1; 11.1.4].
- 13.2.8 **Clause 8.1** - Gekoppeld aan eigenaarschap van operationele beheersing voor verwerkingsactiviteiten, systemen, leveranciers, verwerkers, subverwerkers, relaties met gezamenlijke verwerkingsverantwoordelijken en beheersmaatregelen voor livegang. Addressed by clauses [4.1.4; 4.1.5; 4.1.6; 7.1.2; 7.1.3; 7.1.5; 10.1.3].
- 13.2.9 **Clause 9.2** - Gekoppeld aan onafhankelijke audit en nalevingsbeoordeling van bewijsmateriaal van roltoewijzing, bewijsmateriaal van rolcombinaties, bewijsmateriaal van onafhankelijkheid, bevindingen en sluiting van corrigerende maatregelen. Addressed by clauses [4.2.3; 5.1.9; 6.1.4; 8.1.4; 10.1.4].
- 13.2.10 **Clause 9.3** - Gekoppeld aan directiebeoordeling van volledigheid van PIMS-roltoewijzingen, rolconflicten, uitzonderingen, metriecken over verantwoordingsplicht en resultaten van beoordelingen van verantwoordingsplicht. Addressed by clauses [5.1.1; 6.1.1; 8.1.6; 11.1.1].
- 13.2.11 **Clause 10.2** - Gekoppeld aan escalatie, vastlegging van non-conformiteiten, corrigerende maatregelen, sluiting van uitzonderingen en verificatie van doeltreffendheid voor kwesties rond rolverantwoordingsplicht. Addressed by clauses [4.2.5; 4.4.5; 6.1.5; 9.1.5; 10.1.1; 10.1.2; 10.1.4].
- 13.2.12 **Annex A.1.2.7** - Gekoppeld aan het toewijzen en documenteren van verantwoordelijkheid voor verwerkerscontracten en escalatie van verantwoordelijkheid van derden vóór contractgoedkeuring of -verlenging. Addressed by clauses [4.1.6; 4.4.4; 5.1.7; 7.1.3].
- 13.2.13 **Annex A.1.2.8** - Gekoppeld aan het documenteren van verantwoordelijkheidsverdeling tussen gezamenlijke verwerkingsverantwoordelijken en bewijsmateriaal van relatieverantwoordelijkheid voordat verwerking door gezamenlijke verwerkingsverantwoordelijken begint. Addressed by clauses [4.3.2; 5.1.7; 7.1.3; 8.1.3].
- 13.2.14 **Annex A.1.2.9** - Gekoppeld aan het onderhouden van registraties van verantwoordingsplicht voor verwerkingseigenaarschap door de verwerkingsverantwoordelijke, rolclassificatie en eigenaarschap van bewijsmateriaal. Addressed by clauses [4.3.1; 4.3.5; 4.5.3; 8.1.1].
- 13.2.15 **Annex A.2.2.2** - Gekoppeld aan verantwoordelijkheid voor klantovereenkomsten van verwerkers, eigenaarschap van klantinstructies en bewijsmateriaal van verwerkersrelaties. Addressed by clauses [4.3.3; 5.1.7; 7.1.3; 8.1.3].

13.2.16 **Annex A.2.2.3** - Gekoppeld aan afstemming van doelen en instructies van verwerkers via eigenaarschap van klantinstructies en verificatie van rollen als verwerkingsverantwoordelijke/verwerker. Addressed by clauses [4.3.3; 4.3.5; 5.1.7].

13.3 GDPR

13.3.1 **Article 5(2)** - Gekoppeld aan bewijsmateriaal voor verantwoordingsplicht inzake roltoewijzingen, verwerkingseigenaarschap, rolbeoordelingen, non-conformiteiten en auditbevindingen. Addressed by clauses [4.5.3; 6.1.2; 8.1.1; 10.1.1].

13.3.2 **Article 24** - Gekoppeld aan verantwoordelijkheid van de verwerkingsverantwoordelijke, verantwoord verwerkingseigenaarschap, toezicht door Top Management, jaarlijkse beoordeling en maatregelen voor verantwoordingsplicht. Addressed by clauses [4.1.1; 4.3.1; 5.1.1; 6.1.1; 8.1.6].

13.3.3 **Article 26** - Gekoppeld aan het documenteren van verantwoordelijkheidsverdeling tussen gezamenlijke verwerkingsverantwoordelijken en bewijsmateriaal van relatieverantwoordelijkheid voordat verwerking door gezamenlijke verwerkingsverantwoordelijken begint. Addressed by clauses [4.3.2; 5.1.7; 7.1.3; 8.1.3].

13.3.4 **Article 28** - Gekoppeld aan verantwoordelijkheidsverdeling voor verwerkers en subverwerkers, eigenaarschap van klantinstructies, contractverantwoordelijkheid en escalatiepaden voor derden. Addressed by clauses [4.3.3; 4.3.4; 4.4.4; 5.1.7; 7.1.3].

13.3.5 **Article 30** - Gekoppeld aan verwerkingsregistraties, verwerkingseigenaarschap, PIMS-rolclassificatie en verificatie van rollen als verwerkingsverantwoordelijke/verwerker. Addressed by clauses [4.1.4; 4.3.1; 4.3.5; 8.1.1].

13.3.6 **Article 37** - Gekoppeld aan het documenteren van de rol Data Protection Officer / Privacy Advisor waar aanwijzing van toepassing is of vrijwillig is toegewezen. Addressed by clauses [4.1.2; 4.1.3; 5.1.3; 11.1.2].

13.3.7 **Article 38** - Gekoppeld aan de positie, onafhankelijkheid, betrokkenheid en afhandeling van belangenconflicten van de Data Protection Officer / Privacy Advisor waar van toepassing. Addressed by clauses [4.2.5; 5.1.3; 6.1.3; 11.1.2].

13.3.8 **Article 39** - Gekoppeld aan privacyadvies, observaties uit toezicht, adviserende beoordeling en beoordeling van privacy-impact met betrekking tot rollen door de Data Protection Officer / Privacy Advisor waar van toepassing. Addressed by clauses [4.4.1; 5.1.3; 6.1.3; 11.1.2].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 4.1; Clause 4.2** - Gekoppeld aan actoren binnen het privacyraamwerk en roltoewijzing voor betrokkenen, PII-verwerkingsverantwoordelijken, PII-verwerkers, derden en PIMS-rolclassificatie. Addressed by clauses [4.1.4; 4.1.6; 4.3.5; 5.1.5; 5.1.7].

13.4.2 **Clause 5.12** - Gekoppeld aan verantwoordingsplicht voor privacy naleving, rolbewijsmateriaal, beoordeling, auditbevindingen en verificatie van corrigerende maatregelen. Addressed by clauses [4.5.3; 6.1.2; 8.1.4; 10.1.4].

13.5 ISO/IEC 29151:2022

13.5.1 **Clause 6.1.2; Clause 6.1.3** - Gekoppeld aan definitie van PII-beschermingsrollen, roldocumentatie, rolcommunicatie, coördinatie tussen beveiliging en privacy, en functiescheiding voor PII-bescherming. Addressed by clauses [4.1.1; 4.2.1; 4.2.3; 4.2.4; 4.4.2; 5.1.4; 7.1.4].

13.6 ISO/IEC 27002:2022

- 13.6.1 Control 5.2 - Gekoppeld aan het definiëren, toewijzen, documenteren, communiceren en onderhouden van PIMS- en informatiebeveiligingsverantwoordelijkheden. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.1; 4.4.2; 4.5.1; 5.1.4; 7.1.1].
- 13.6.2 Control 5.3 - Gekoppeld aan functiescheiding, goedkeuring van rolcombinaties, onafhankelijke beoordeling, conflictbeheersmaatregelen en verificatie van corrigerende maatregelen voor rolconflicten. Addressed by clauses [4.2.2; 4.2.3; 4.2.4; 9.1.2; 10.1.4].