CIIO De certificeerder voor de professionele dienstverlening

Inleiding

- In 2022 is de 27002:2022 uitgebracht.
- De publicatie van 27001:2022 wordt Q4 2022 verwacht.
- Na publicatie van 27001:2022 hebben reeds gecertificeerde organisaties 3 jaar de tijd om over te stappen naar de nieuwe norm.
- Op dit moment is nog niet duidelijk wanneer de Raad van Accreditatie toestemming zal geven aan Certificerende Instellingen om te certificeren conform de nieuwe norm.
- De in de ISO 27001:2022 doorgevoerde aanpassingen zullen door de NEN ook moeten worden doorgevoerd in NEN 7510; nog onbekend is wanneer dit gereed is. Op sheet 6 wordt specifiek ingegaan op de impact voor NEN 7510 certificaathouders.

Inhoud van deze presentatie:

- De belangrijkste wijzigingen in ISO 27001:2022
- Impact voor certificaathouders
- Onderwerpen transitie-onderzoek

CIIO De certificeerder voor de professionele dienstverlening

Verschillen ISO 27001:2022 t.o.v. ISO 27001:2013

Belangrijkste wijzigingen ISO 27001:2022:

- Andere volgorde en indeling van beheersmaatregelen in de Annex A;
- Van indeling naar onderwerp (bijvoorbeeld A.9 – Logische Toegang en A.17 – beschikbaarheid) naar indeling naar 4 categorieën –processen/ organisatie, mensen, technologie en fysieke beveiliging;
- In vergelijking met de oude editie neemt het aantal maatregelen in de Annex A van ISO/IEC 27002:2022 af van 114 maatregelen in 14 clausules naar 93 maatregelen in 4 clausules (categorieën);
- Voor de maatregelen in ISO/IEC 27002:2022 zijn 11 maatregelen nieuw, 24 maatregelen zijn samengevoegd uit de bestaande maatregelen en 58 maatregelen zijn bijgewerkt. Bovendien is de maatregelenstructuur herzien, die voor elke maatregel “attribuut” en “doel” introduceert en niet langer “doelstelling” gebruikt voor een groep maatregelen;
- Tip: in de al gepubliceerde ISO 27002:2022 norm zit een “van – naar” tabel van de oude en nieuwe annex A; Deze norm is te bestellen bij de NEN: https://www.nen.nl/iso-iec-27002-2022-nl-295235

  Zie de volgende 2 slides voor wat meer details omtrent de verschillen tussen de 2013 en 2022 versies.

CIIO De certificeerder voor de professionele dienstverlening

Verschillen – samengevoegde maatregelen

Samengevoegde beheersmaatregelen

Compactere en (soms) meer logische indeling (bijvoorbeeld de samenvoeging van de in 2013 versie verspreide onderdelen op change management/ wijzigingsbeheer in beheersmaatregel - 8.32

ISO/IEC 27002 control identifier	ISO/IEC 27002:2013 control identifier	Control name
5.1	05.1.1, 05.1.2	Policies for information security
5.8	06.1.5, 14.1.1	Information security in project management
5.9	08.1.1, 08.1.2	Inventory of information and other associated assets
5.10	08.1.3, 08.2.3	Acceptable use of information and associated assets
5.14	13.2.1, 13.2.2, 13.2.3	Information transfer
5.15	09.1.1, 09.1.2	Access control
5.17	09.2.4, 09.3.1, 09.4.3	Authentication information
5.18	09.2.2, 09.2.5, 09.2.6	Access rights
5.22	15.2.1, 15.2.2	Monitoring, review and change management of supplier services
5.29	17.1.1, 17.1.2, 17.1.3	Information security during disruption
5.31	18.1.1, 18.1.5	Identification of legal, statutory, regulatory and contractual requirements
5.36	18.2.2, 18.2.3	Compliance with policies and standards for information security
6.8	16.1.2, 16.1.3	Information security event reporting
7.2	11.1.2, 11.1.6	Physical entry controls
7.10	08.3.1, 08.3.2, 08.3.3	Storage media
8.1	06.2.1, 11.2.8	User endpoint devices
8.8	12.6.1, 18.2.3	Management of technical vulnerabilities
8.15	12.4.1, 12.4.2, 12.4.3	Logging
8.19	12.5.1, 12.6.2	Installation of software on operational systems
8.24	10.1.1, 10.1.2	Use of cryptography
8.26	14.1.2, 14.1.3	Application security requirements
8.29	14.2.8, 14.2.9	Security testing in development and acceptance
8.31	12.1.4, 14.2.6	Separation of development, test and production environments
8.32	12.1.2, 14.2.2, 14.2.3, 14.2.4	Change management

CIIO De certificeerder voor de professionele dienstverlening

Verschillen - nieuwe maatregelen

Nieuwe beheersmaatregelen:

	ISO/IEC 27002 control identifier	ISO/IEC 27002:2013 control identifier	Control name
	5.7	New	Threat intelligence
	5.23	New	Information security for use of cloud services
	5.30	New	ICT readiness for business continuity
	7.4	New	Physical security monitoring
	8.9	New	Configuration management
	8.10	New	Information deletion
	8.11	New	Data masking
	8.12	New	Data leakage prevention
	8.16	New	Monitoring activities
	8.22	New	Web filtering
	8.28	New	Secure coding

CIIO De certificeerder voor de professionele dienstverlening

Impact voor certificaathouders ISO 27001:2013

- Transitie-periode voor de klant is **maximaal** 3 jaar na publicatie van de nieuwe ISO 27001:2022;
- De transitie is verplicht. Indien 3 jaar na publicatie het ISMS niet voldoet aan de ISO 27001:2022, wordt het certificaat geschorst hetgeen inhoudt dat de klant niet meer is gecertificeerd voor ISO 27001;
- In overleg met CIIO (de Teamleider) wordt de transitie-periode afgestemd en het transitie onderzoek ingepland;
- Er is minimaal 0,5 dag extra tijdsbesteding nodig voor het transitie onderzoek (verplichting vanuit de RvA/ IAF MD 26:2022). De Teamleider bepaalt de benodigde extra tijdsbesteding;
- De transitie kan tijdens een regulier gepland onderzoek worden uitgevoerd. Op verzoek van de klant kan ook een Speciaal Onderzoek worden uitgevoerd.
- CIIO organiseert in 2022 een aantal inloopsessies (digitaal). Tijdens deze sessies zal worden ingegaan op de nieuwe maatregelen, waarbij voorbeelden gegeven worden van onderzoeksvragen die je tijdens het transitie onderzoek kunt verwachten. Tevens zal dan de stand van zaken worden besproken omtrent de vraag vanaf wanneer CIIO gaat toetsten conform de nieuwe norm;
- Op de volgende slide staan de onderwerpen die altijd aan de orde zullen komen bij een transitie-onderzoek.

CIIO De certificeerder voor de professionele dienstverlening

Impact voor certificaathouders NEN 7510

- Zoals op sheet 1 aangegeven is op dit moment nog niet duidelijk wanneer de NEN 7510 norm in lijn wordt gebracht met de ISO 27001:2022.
- Voor klanten met alleen NEN 7510 is de impact van de ISO 27001:2022 publicatie nihil; deze klanten blijven conform de huidig geldende NEN 7510 norm beoordeeld worden, totdat de nieuwe NEN norm gepubliceerd wordt.
- Met klanten die voor zowel NEN 7510 als ISO 27001 gecertificeerd zijn, zal CIIO in overleg treden om de mogelijkheden door te bespreken. Hieronder zijn staan wel alvast wat opties opgesomd, met de voor- en nadelen.

Opties	Voordelen	Nadelen
ISO en NEN transitie na elkaar	ISO eerder afgerond; mogelijk commercieel voordeel t.o.v. vergelijkbare organisaties die nog op “de oude norm zitten” Geen afhankelijkheid met NEN; bij een vertraging van de nieuwe NEN, bestaat het risico dat organisatie “gehaast” over moet naar de nieuwe ISO vanwege de 3 jaar termijn	2 inhoudelijk verschillende systemen tegelijk actief houden, hetgeen wellicht minder efficiënt is 2 transitie audits noodzakelijk
ISO en NEN transitie tegelijk	In 1 x klaar (1 transitie-audit) Klant hoeft maar 1 systeem actief te houden	Afhankelijkheid met NEN; bij een vertraging van de nieuwe NEN, bestaat het risico dat organisatie “gehaast” over moet naar de nieuwe ISO vanwege de 3 jaar termijn

CIIO De certificeerder voor de professionele dienstverlening

Onderwerpen transitie-onderzoek

Bron/ eisen: IAF MD 26:2022 (zie eventueel: https://iaf.nu/iaf_system/uploads/documents/IAF_MD_26_Transition_requirements_for_ISOIEC_27001-2022_09082022.pdf)

De volgende onderwerpen zullen (minimaal) aan de orde komen tijdens het transitie onderzoek:

3) Het transitie onderzoek omvat, maar is niet beperkt tot:

- de gap-analyse van ISO/IEC 27001:2022, evenals de noodzaak van wijzigingen in het ISMS van de klant;
- het actualiseren van de Verklaring van Toepasselijkheid (VvT);
- indien van toepassing, het actualiseren van het risicobehandelplan;
- de implementatie en effectiviteit van de nieuwe of gewijzigde controles gekozen door de klant.

Vrij vertaald door CIIO:
Belangrijke actie klant: opnieuw (aantoonbaar) uitvoeren van 6.1.3.c: vergelijk de vastgestelde maatregelen uit het risico behandelplan met (de nieuwe ISO 27001:2022!!) Annex A om te verifiëren dat noodzakelijke maatregelen niet zijn weggelaten.
Volledige her-structuren van het ISMS zal naar inschatting van CIIO niet noodzakelijk zijn; wel moet de klant de Verklaring van Toepasselijkheid herzien;
Hiervoor heeft de klant maximaal 3 jaar de tijd na publicatie van de ISO 27001:2022 norm.