Transitie ISO27001:2022

Informatie over de ISO27001:2022 transitie

Via deze laatste nieuwsbrief van dit jaar, willen we u op de hoogte brengen over de transitie van uw gecertificeerde ISMS naar de nieuwe ISO27001:2022 versie.
De nieuwsbrief is primair bedoeld voor klanten die een ISO27001 en/of NEN7510 certificering hebben. Maar ook voor alle relaties die willen weten hoe de transitie in zijn werk gaat. We organiseren ook enkele TEAMS sessies, waaraan u gratis kunt deelnemen.
De nieuwe versie van de ISO27001 en ISO27002 zijn beschikbaar, zowel in het Nederlands als in het Engels. Deze normen zijn te bestellen via de NEN website.
De NEN7510 is nog niet aangepast en zal later volgen.

De Transitie audit

Om uw gecertificeerde managementsysteem voor informatiebeveiliging (ISMS) over te laten gaan naar de nieuwe ISO27001:2022 versie zal onze partner een transitie audit bij u moeten uitvoeren. Hiervoor zijn deadlines bepaald. Welke deadline voor u van toepassing is, is afhankelijk vanaf wanneer u uw initiële certificering heeft behaald. Zie de tabel hieronder met alle details.

Wat moet u voorbereiden?

Om de transitie audit succesvol te doorlopen moet u uw ISMS aanpassen. Wat zijn voor u de te nemen acties?

1. Gap analyse

U dient een gap analyse uit te voeren. In deze analyse moet u vastleggen op welke onderdelen van uw ISMS die nieuwe norm impact heeft. Denk daarbij aan uw handboek, risicoanalyse, risicobehandelplan, VVT en inrichting van de nieuwe en veranderde controls.
Om het u makkelijk te maken hebben we voor het uitvoeren van de gap analyse een template opgesteld. U kunt deze gebruiken of u gebruikt uw eigen vergelijkbare methode. U vind deze template onderaan deze nieuwsbrief.
> Tijdens de transitie audit zullen we uw gap analyse beoordelen.

2. Actieplan

Vervolgens gaat u vanuit de vastgestelde gap analyse, per onderwerp acties vaststellen. Hoe gaat u de verandering vormgeven, wie gaat dat doen en wanneer moet dit klaar zijn.
> Tijdens de transitie audit zullen we uw actieplan beoordelen.

3. Aanpassen risicoanalyse en behandelplan

Binnen uw ISMS heeft u een risicoanalyse uitgevoerd en behandelplan. Daarin heeft u vastgelegd welke maatregelen heeft u zelf heeft genomen om de risico's te mitigeren. Deze genomen maatregelen moeten worden vergeleken t.o.v. de bijlage A, om te verifiëren of er geen noodzakelijke maatregelen zijn vergeten. Aangezien de bijlage A is veranderd zult u dit mechanisme moeten aanpassen naar de nieuwe Annex A.
> Tijdens de transitie audit zullen we uw risicoanalyse en behandelplan beoordelen.

4. Annex A controls aanpassen

De nieuwe norm heeft 11 nieuwe beheersmaatregelen en verschillende maatregelen uit de oude norm zijn samengevoegd. Uiteraard zult u even goed moeten kijken of deze controls voor u van toepassing zijn en hoe u deze beheersmaatregelen t.o.v. uw eigen risicoanalyse gaat invullen. De nieuwe ISO27002 geeft u hierbij veel 'best-practice' handreikingen.
> Tijdens de transitie audit zullen we uw bewijslast beoordelen over de werking van de nieuwe en aangepaste (samengevoegde) beheersmaatregelen.

5. Aanpassen VVT

Conform de norm eisen dient u een Verklaring van Toepasselijkheid (VVT) opstellen. Omdat de Annex A is veranderd, zult u de VVT in het geheel moeten herzien.
> Tijdens de transitie audit zullen we uw VVT beoordelen.

6. Interne audit

Voordat wij bij u de transitie audit komt uitvoeren, dient u zelf een interne audit hebben uitgevoerd. Dit moet u minimaal uitvoeren op de risicoanalyse + behandelplan en daarbij nieuwe en de gewijzigde (samengevoegde) controls uit de Annex A.
> Tijdens de transitie audit zullen we uw interne auditrapport beoordelen.

7. Directie beoordeling

Uitvoeren directiebeoordeling conform par 9.3. Een onderdeel hiervan is dat de resultaten van de interne audit moeten worden besproken.
> Tijdens de transitie audit zullen we uw (extra) uitgevoerde directiebeoordeling beoordelen.

Uitvoeren transitie audit door partner 12secure-u

De transitie audit neemt 4 uur in beslag en zal als een separate audit worden ingepland en uitgevoerd. Tijdens deze audit zullen de bovenstaande 7 onderwerpen worden beoordeeld. Deze audit zal door de auditor remote worden uitgevoerd samen met uw CISO of een andere contact persoon binnen uw organisatie. We zullen, in principe geen interviews uitvoeren met medewerkers binnen uw organisatie, tenzij de auditor dit tóch noodzakelijk zou vinden.
Het is belangrijk dat u van bovenstaande onderwerpen goed heeft voorbereid en de bewijslast beschikbaar heeft voor een soepele uitvoering van deze transitie audit.

Na de audit zal de auditor hiervan een rapportage opmaken (2h). Het dossier zal intern worden beoordeeld (1h) en indien alles akkoord is, zal onze partner uw nieuwe ISO27001:2022 certificaat opmaken en aan u versturen. (1h)

Kosten

De kosten voor deze transitie audit is 1 dag, tegen het dagtarief uit uw overeenkomst. Dat is inclusief de audit rapportage, opmaak en publicatie van uw nieuwe certificaat.

Combinatie ISO27001 en NEN7510

Indien u een certificering heeft voor zowel de ISO27001 en de NEN7510 is het ook mogelijk om alvast met uw ISO27001 certificering over te gaan naar de nieuwe versie van de norm. U moet wel beseffen dat hiermee de complexiteit van uw eigen ISMS gaat toenemen. Immers, de nieuwe en oude controls gaan door elkaar heen lopen. Tijdens de audit van de NEN7510 zullen we kijken naar de oude bijlage A.

Tijdslijn van deze transitie

De transitie deadline (wanneer u uiterlijk over moet) is afhankelijk van uw specifieke situatie. Kijk in de tabel, wanneer u uw initiële ISO27001 certificering heeft behaald. Vervolgens kunt u zien welk scenario voor u van toepassing is.

2020	2021	2022	2023		2024	
			< 1-11-23	*1-11-2023*		
INIT	C1	C2	HER		C1	
INIT	C1	C2		HER	C1	
	INIT	C1	C2		HER	
		INIT	C1		C2	
			INIT		C1	
				INIT	C1	

Blauw = 12secure-u partner kan en mag uw ISMS nog tegen de oude versie van de norm uitvoeren.
Groen = 12secure-u partner moet uw ISMS tegen de nieuwe ISO27001:2022 norm.

In 2025 moet u vóór 1/11/2025 zijn overgegaan.

Uiteraard, mag u voorafgaand aan uw komende controle audit al over naar de nieuwe norm en uw transitie audit inplannen. In de tabel zijn slechts de uiterste deadlines vermeld. Neem tijdig hierover contact op met onze backoffice.

Belangrijke data om te onthouden

tot 1/11/23 mag onze partner nog initiële- en her-certificatie audits uitvoeren tegen de oude versie van de norm

vanaf 1/11/23 mogen ze alleen nog initiële- en her-certificatie audits uitvoeren tegen de nieuwe versie van de norm.

Inplannen transitie audit

Indien u deze transitieaudit wilt laten uitvoeren, kunt u dit melden aan onze backoffice. U kunt hiervoor e-mail sturen naar; info@12secure-u.nl

Onze backoffice zal contact met u opnemen om de audit in te plannen. De audit zelf zal 4h duren en zal remote worden uitgevoerd. Belangrijk dat u dit tijdig doet, i.v.m. de beschikbaarheid van de auditoren.

De Transitie audit moet minimaal 2 weken voorafgaand aan uw reguliere audit worden ingepland. In deze 2 weken kunnen we uw transitie dossier afronden en uw nieuwe certificaat opmaken. Zodat uw reguliere audit dan tegen de nieuwe norm kan worden uitgevoerd.

Inhoudelijke norm veranderingen

De belangrijkste wijziging in de ISO27001:2022 is dat de Annex A is gewijzigd. De huidige ISO27001 bevatte 114 maatregelen, verdeeld over 14 hoofdstukken (Annex 5 tot en met Annex 18). Dit wordt in de nieuwe ISO 27001:2022 teruggebracht naar 4 hoofdstukken en 93 controls.

5 Organisatie	37 controls
6 Medewerkers	8 controls
7 Fysieke beveiliging	14 controls
8 Techniek	34 controls

Handig om te weten is dat er kruistabellen beschikbaar zijn tussen de nieuwe en oude controls. Deze zijn bij deze nieuwsbrief toegevoegd. (zie onderaan deze nieuwsbrief)

Annex A veranderingen

Nieuwe beheersmaatregelen.
Er zijn 11 nieuwe beheersmaatregelen.

Nieuwe control	Beheersmaatregel
A.5.7	Informatie en analyses over dreigingen
A.5.23	Informatiebeveiliging voor het gebruik van clouddiensten
A.5.30	ICT-gereedheid voor bedrijfscontinuïteit
A.7.4	Monitoren van de fysieke beveiliging
A.8.9	Configuratiebeheer
A.8.10	Wissen van informatie

A.8.11	Maskeren van gegevens
A.8.12	Voorkomen van gegevenslekken (data leakage prevention)
A.8.16	Monitoren van activiteiten
A.8.23	Toepassen van webfilters
A.8.28	Veilig coderen

Belangrijk om de ISO27002:2022 te raadplegen. Hierin staan de best-practice beschreven, die u kunt gebruiken om de control zo in te richten wat nodig is om het daarbij behorende risico (in uw eigen risico-analyse) te mitigeren.

Veranderde beheersmaatregelen
Daarnaast zijn er ook verschillende controls uit de oude norm samengevoegd in de nieuwe norm. In de kruistabellen kun je zien welke dat zijn. In uw ISMS moeten deze dus worden samengevoegd.

HLS veranderingen
Daarnaast zijn er ook wat kleine veranderingen in de HLS onderwerpen. (Hoofdstuk 4 t/m hoofdstuk 10). Geen grote veranderingen, maar update wel je ISMS handboek en beleidstukken.

§	Omschriving	Aanpassing
4.1	Context	Aanscherping
4.2	Stakeholders	Aanscherping
4.4	ISMS	Aanscherping
6.1.3	Risico behandeling	Aanscherping
6.2	Doelstellingen	Aanscherping
6.3	Verandermanagement	Toevoeging
7.4	Communicatie	Aanscherping
8.1	Operationele planning	Herschreven
9.1	Monitoring	Aanscherping
9.2	Algemeen en Auditprogramma	Splitsing
9.3	Algemeen, input en output	Splitsing
10.1	Verbeteren en Afwijkingen & Corrigerende maatregelen	Verandering nu