ISO27002:2022

De aanpassingen

Na heel lang wachten is door de standaardsorganisatie ISO/IEC in maart 2022 de aangepaste ISO/IEC 27002 norm gepubliceerd. Deze aanpassing heeft een aantal zeer nuttige verrijkingen en uitbreidingen om informatiebeveiliging binnen bedrijven beter te managen.
Is de aanpassing van deze norm van toegevoegde waarde en heeft het zin om deze te implementeren?

Door: Maurice van der Woude, CEO BPdelivery B.V.
Tags: #ISO27002, #NEN-ISO, #Certificering, #ISMS

Historie
Door de jaren heen is de ISO2700x normreeks de *de facto* standaard geworden op het gebied van informatiebeveiliging binnen ondernemingen. De ISO27002 norm gaat al een tijdje mee en de maatregelen/controls van deze norm waren wel toe aan een opknapbeurt. Dreigingen voor informatiebeveiliging hebben immers niet stil gestaan. De basis van deze norm bestaat al bijna 10 jaar, het werd dus wel tijd dat er een 'upgrade' kwam. Alhoewel de 27002 formeel wel als norm in de markt is neergezet, kunnen bedrijven zich hier niet tegen certificeren. Dat heeft er alles mee te maken dat deze norm geen managementsysteem bevat en daarvoor sterk leunt op de ISO27001. In het kort zijn de beide normen als volgt aan elkaar gerelateerd:

ISO27001 en ISO27002
De ISO27001 norm bevat wel de beschrijving en normelementen van een managementsysteem en de Annex A van deze norm bevat de controle-elementen (ook wel 'controls' of 'maatregelen' genoemd) van de ISO27002. Deze controls in de Annex A zijn echter zo summier beschreven, dat het erbij halen van de 27002 noodzakelijk is om

te begrijpen wát er nu eigenlijk geïmplementeerd zou moeten worden en hoe dat aantoonbaar te maken is. De 27002 is hiermee een verlengstuk van de ISO27001 en beide worden daarom vaak als één geheel gezien. Ook de ISO27001 norm dateert in de basis al van 2013 en heeft een laatste, kleine, revisie in 2015 ondergaan (ISO/IEC 27001:2013/COR 2:2015).

ISO zelf schrijft dat normen eens in de 5 jaar gereviewd worden. Voor de ISO2700x normenstelsels is dit duidelijk niet publiekelijk het geval geweest waarbij dit leidde tot te implementeren aanpassingen. Wel is het zo dat de ISO27001 norm momenteel de laatste fase van een nieuwe review heeft ondergaan (*90.93 International standard confirmed*). De laatste stap van dit review proces draagt het ID 90.99 en heeft als omschrijving "*Withdrawal of International Standard proposed bij TC or SC*". Een tijdschema wordt hierbij echter niet afgegeven. Zie hieronder het review proces van de ISO27001 per april 2022;

(source: ISO.ORG)

Met in het achterhoofd de wetenschap dat ISO27002 de controle aspecten van de ISO27001 omvat, lijkt het logisch dat ook de ISO27001 de opstap maakt naar een 2022 versie. Men kan wel verwachten dat de upgrade van de ISO27001 mogelijk uitsluitend een aanpassing van de Annex A zal zijn. Desgevraagd geeft NEN aan dat "*Afhankelijk van de uitkomsten bij ISO is het deze zomer of in het 4de kwartaal van haar jaar dat ISO 27001 wordt gepubliceerd*". NEN geeft zelf aan dat de Nederlandse publicatie van de 27002

binnen enkele weken te verwachten is.

De wijzigingen van de 27002 norm
Logisch is de vraag welke wijzigingen nu in de ISO/IEC 27002 zijn opgenomen, maar vooral welke nieuw zijn. Hieronder volgt een overzicht van de belangrijkste wijzigingen en vernieuwingen ten opzichte van de oude variant;

Om te beginnen is de naam gewijzigd. Deze is nu:
"*Information security, cybersecurity and privacy protection — Information security controls*"

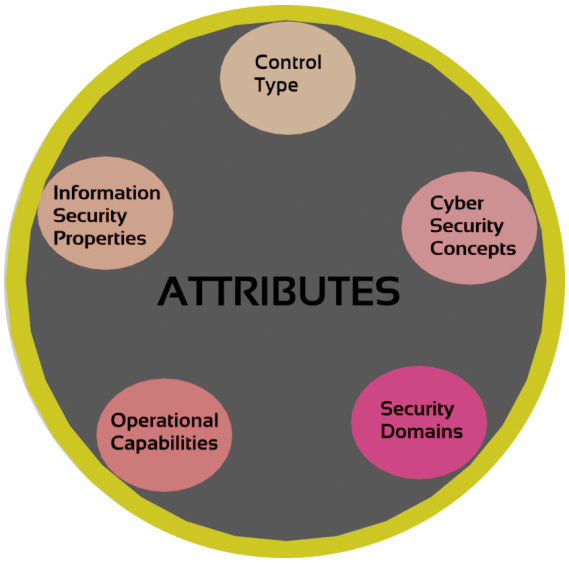
Voorheen was de normnaam
"*Information technology — Security techniques — Code of practice for information security controls*"

De wijziging in de naam verraadt al dat er meer aandacht is gekomen voor privacy aspecten en cybersecurity. Op zich is dat alleen al een goede ontwikkeling omdat deze elementen vooral in de huidige tijd bijzonder veel, en terechte, aandacht krijgen.

De nieuwe norm bevat 93 controls. Het aantal controls is met meer dan 20 elementen afgenomen. Daarnaast is ook de hoofdstukindeling anders geworden. Er zijn nu nog maar vier hoofdstukken met controls:

- Organizational controls ==> Organisatie en haar omgeving
- People controls ==> Mensen / medewerkers
- Physical controls ==> Fysieke omgeving
- Technological controls ==> Technische omgeving

Per normelement is nu ook opgenomen welke attributen en subattributen dit normelement heeft. Er worden in totaal 5 attributen onderscheiden;



Control type
Het controle type identificeert het type risico dat zich kan voordoen en in welke mate dit van invloed kan zijn op de maatregelen. In deze categorie worden 3 control typen onderscheiden: Preventive (voorkoming), Detective (opmerkbaar) en Corrective (direct te nemen maatregelen)

Informatie beveiligingseigenschappen
Dit is de bekende BIV (Beschikbaarheid, Integriteit & Vertrouwelijkheid) classificatie. Deze worden in de (momenteel nog) Engelstalige norm "*Confidentiality*", "*Integrity*" en "*Availability*" genoemd.

Cybersecurity concepten
Deze attributen geven een link aan naar cybersecurity aspecten en zijn gelinkt aan de ISO/IEC TS27110. De benoemde aspecten bestaan uit de classificaties "*Identify*", "*Protect*", "*Detect*", "*Respond*" en "*Recover*".

Operationele mogelijkheden
Dit attribuut gaat uit van de operationele mogelijkheden die gevolgd kunnen worden. Dit is een vrij uitgebreid rijtje van classificaties. Zonder hier al teveel op in te gaan betreffen dit de volgende classificaties; "*Governance*", "*Asset Management*", "*Information Protection*", "*Human Resource Security*", "*Physical Security*", "*System and Network Security*", "*Application Security*", "*Secure Configuration*", "*Identity and Access Management*", "*Threat and Vulnerability Management*", "*Continuity*", "*Supplier Relationship Security*", "*Legal and Compliance*", "*Information Security Event Management*" en "*Information Security Assurance*".

Beveiligings domein
Dit attribuut wordt gebruikt om vanuit vier verschillende invalshoeken naar de maatregelen te kijken. Deze vier vallen ook weer uiteen in verschillende aspecten. Voor de leesbaarheid van deze briefing worden uitsluitend de hoofdelementen benoemd: "*Governance and Ecosystem*" ,"*Protection*", "*Defence*" en "*Crisis Management*".

Het inbedden van deze attributen in de maatregelen die de onderneming neemt om risico's te adresseren heeft als voordeel dat vrij eenvoudig is vast te stellen hoe met een bepaalde maatregel het beste omgegaan kan worden en welke onderdelen hier een rol in hebben. Bij iedere maatregel wordt nu weergegeven welke attributen hierbij passen en een rol spelen. Het maakt de implementatie van deze norm wel enigszins complexer omdat verwacht kan worden dat auditerend Nederland ook naar deze attributen zal gaan kijken. Hoe deze attributen echter meegenomen zullen gaan worden tijdens externe audits is momenteel nog onhelder.

De nieuwe normelementen
Er was al geschreven dat de norm qua hoofdstukindeling een behoorlijke slag gemaakt heeft. Daarnaast zijn een aantal maatregelen uit de oude norm samengevoegd naar één nieuwe of al bestaande maatregel. Uiteindelijk gaat het erom welke elementen nieuw zijn opgenomen. Dat overzicht is hieronder weergegeven met een korte omschrijving;

Threat intelligence
Het identificeren van mogelijke security risico's. Dit valt mogelijk te combineren met de al bestaande risico analyse.

Information Security for use of Cloud Services
Het proces voor aanschaf, gebruik en exit van Cloud Services moet passen bij de vereisten van de organisatie. Zie voor meer informatie over dit onderwerp onze eerdere public briefing: Negotiation Powers for Cloud Customers. (Engelstalig).

ICT Readiness for Business Continuity
Business Continuity was al onderdeel van de oude norm, hier wordt met name de focus

gelegd naar het gereed zijn van de ICT omgeving om continuïteit te waarborgen.

Physical Security Monitoring
Niet alleen interne ICT systemen moeten worden gemonitord, ook de fysieke omgeving wordt nu in de monitoring meegenomen. Hierbij moet vooral gedacht worden aan gebouwbewaking en/of (camera)bewaking van de omgeving.

Configuration Management
Hiermee wordt aangegeven dat de beveiliging van configuraties ook moet worden meegenomen zoals van hardware, software, services en netwerken. Deze zullen per onderdeel nu apart beschreven moeten worden.

Information Deletion
Een uiterst zinvolle aanvulling ten opzichte van de oude norm. Dit item vereist dat organisaties ook gaan nadenken hoe en op welke wijze informatie verwijderd moet worden. Hierbij wordt ook bijzondere en specifieke aandacht geschonken aan persoonsgevoelige informatie.

Data Masking
Waar data bestaat, moet deze ook aanvullend beschermd worden. Met name als het privacy gevoelige data betreft. Hoe wordt data zodanig afgeschermd dat deze niet zonder meer toegankelijk is en wie mogen bij die data (en waarom).

Data Leakage Prevention
Als data benaderbaar is, dient ook voorkomen te worden dat data bedoeld of onbedoeld op straat komt te liggen. Hier gaat het nadrukkelijk om de maatregelen die genomen (moeten) worden om te voorkomen dat een datalek ontstaat.

Monitoring activities
Netwerken, systemen en applicaties moeten voorzien worden van adequate monitoring die verstoringen kan detecteren. Daarnaast moeten hierbij potentiële informatie beveiligings incidenten al vooraf geëvalueerd worden.

Web Filtering
Toegang tot externe websites moet zodanig gefilterd worden dat voorkomen wordt dat men naar verdachte websites kan gaan.

Secure Coding
Bij het ontwikkelen van eigen applicaties zal nadrukkelijk aandacht gegeven moeten worden aan beveiligd ontwikkelen (Security by default en Security by Design).

ISO geeft aan dat de maatregelen zeker niet uitputtend zijn en organisaties worden in alle omstandigheden gestimuleerd om deze norm naar eigen inzicht uit te breiden met voor de eigen organisatie passende en aanvullende maatregelen.

Links naar andere normen (NEN, BIO)

Andere normenstelsels, zoals de NEN7510-2 (Informatiebeveiliging in de zorg) en de BIO (Baseline Informatiebeveiliging Overheid) leunen sterk op de maatregelen zoals deze in de oude 27002 waren opgenomen. Om aansluiting te blijven houden, zullen ook deze normstelsels wellicht een wijziging moeten ondergaan. Gezien de hoeveelheid wijzigingen en de gewijzigde insteek van de vernieuwde ISO/IEC 27002 norm, is de verwachting dat de aanpassingen op gerelateerde normen nog wel even op zich zullen laten wachten. Voor de 27002 geeft NEN aan de Nederlandstalige versie binnen enkele weken te kunnen publiceren.

Conclusie

Wat opvalt in deze vernieuwde norm is dat er niet alleen veel meer aandacht wordt geschonken aan cybersecurity en Cloud maar vooral ook aan de beveiliging van privacy gevoelige informatie. Dit is een zeer sterke aanpassing van de norm die ook daadwerkelijk nodig was. Daarnaast zijn de toegevoegde classificaties een verrijking die de norm duidelijker en beter implementeerbaar maken. De norm is momenteel uitsluitend nog in het Engels beschikbaar en zonder de (te verwachten) aanpassing van de 27001 norm, nog niet heel erg bruikbaar. Wel is het goed om deze norm alvast op te nemen in eventuele plannen voor een Informatiebeveiligings certificering of de aanpassing van uw huidige ISO27001 certificering. Met deze public briefing kunt u zich daar goed op voorbereiden. Uiteraard kunt u ook BPdelivery inschakelen om u te adviseren over stappen die u kunt nemen om beter voorbereid te zijn voor implementatie van deze norm en informatiebeveiliging binnen uw onderneming niet alleen te optimaliseren, maar ook robuuster en veiliger te maken.

Achtergrond details

Dit artikel wordt u kosteloos aangeboden door BPdelivery B.V.
DE specialist in Digitale Transformatie, ISO/NEN begeleidingstrajecten en Bedrijfs proces optimalisaties. Meer informatie kunt u vinden op www.bpdelivery.com

About BPdelivery

BPdelivery B.V. focusses on the improvement of business processes within the cloud chain between supply and demand. **BPd**elivery also provides for strategies on how to move businesses successfully to the Cloud and is often asked as specialist to help organizations acquire certifications on quality and security and digital transformation.

---

www.bpdelivery.com

Info@bpdelivery.com
Kerkstraat 85
6871 BJ RENKUM
The Netherlands

Voor dit artikel zijn de volgende bronnen geraadpleegd:

ISO/IEC 27001:2013

ISO/IEC 27002: 2013
ISO/IEC 27002: 2022
www.ISO.org
Www.nen.nl
www.nen.hivebrite.com