EERSTE HULP BIJ IMPLEMENTATIE EN VERBETERING VAN UW ISMS

NICO BASTEN

TUSSEN DE REGELS ISO 27001

Wat er niet staat en u wél moet weten

Uitgeverij Trespaises

NICO BASTEN

TUSSEN DE REGELS ISO 27001

Wat er niet staat en u wél moet weten

Uitgeverij:	Trespaises
ISBN:	9789090407845
NUR:	982 (Informatica & management)
Versie:	20251010
Trefwoord:	Informatiebeveiliging

Vormgeving:	Astrid Honcoop
Boekomslag:	Astrid Honcoop
Afbeeldingen:	Nico Basten
Druk en bindwerk:	Pumbo
Foto auteur:	Nico Basten

INHOUD

DANKWOORD

Een boek schrijf je nooit alleen. Hoewel mijn naam op de omslag staat, hebben velen direct of indirect bijgedragen aan de totstandkoming.

Allereerst wil ik mijn dank uitspreken aan mijn klanten, collega's, vakgenoten en auditors, met wie ik de afgelopen jaren heb mogen werken. Jullie uitdagingen, visies, vragen en soms ook frustraties waren de inspiratie voor de praktijkvoorbeelden, valkuilen en tips in dit boek. Jullie hebben laten zien hoe ISO 27001 in de échte wereld werkt – en soms juist niet werkt.

Een speciaal woord van dank gaat uit naar mijn twee vaktechnische reviewers: Cees van der Wens en Gerrit-Jan Spruijt. Jullie zaten lekker kritisch in de wedstrijd, en onze discussies waren onmisbaar om mijn visie aan te scherpen. We waren het niet altijd eens, maar dat hoeft ook niet in dit vak. Jullie feedback heeft het boek beter gemaakt.

Dank ook aan u, de lezer. Door dit boek ter hand te nemen laat u zien dat u bereid bent verder te kijken dan alleen de norm. Ik hoop dat de kennis, voorbeelden en hulpmiddelen u helpen om ISO 27001 niet alleen te begrijpen, maar er ook plezier in te vinden om ermee te werken.

Natuurlijk ook dank aan mijn vrouw Lizzy: voor je geduld, zowel in Nederland, Spanje als Suriname. Je bracht me af en toe terug naar het hier en nu, wanneer ik weer eens eindeloos in gedachten achter mijn laptop zat. En het is leuk, nuttig en verfrissend om af en toe te discussiëren over dit taaie onderwerp met iemand die er inhoudelijk nét iets verder vanaf staat.

Tot slot een woord van dank aan drie mensen die mij tijdens het schrijfproces hebben ondersteund. Het was mijn eerste keer, dus ik was enorm blij met jullie hulp:

Perdiep Ramesar, van Het Schrijvershuis. Jij was mijn coach en begeleider tijdens deze reis. Je was de katalysator en hield de 'rijdende trein' op de rails, gaf veel tips en stuurde bij waar nodig.

Astrid Honcoop, van Het Ontwerploket. Jij hebt de vormgeving verzorgd. Het resultaat is strak en professioneel geworden, waar ik trots op ben.

Martijn Tamboer, van Het Nederlands Tekstbureau. Jij bent er taaltechnisch nog eens met de stofkam doorheen gegaan, en hebt de puntjes op de i gezet.

VOORWOORD

Toen Nico mij vroeg een voorwoord te schrijven voor zijn boek voelde ik me vereerd en nieuwsgierig, omdat dit onderwerp essentieel is voor het bijdragen aan veilige informatiebeveiliging.

In mijn rol als Country Head Director Internal Audit binnen een internationale bank, zie ik dagelijks hoe cruciaal het is dat informatiebeveiliging geen abstract begrip blijft, maar een verankerd onderdeel is van de bedrijfsvoering. ISO 27001 biedt daarvoor een krachtige leidraad. Het is meer dan een norm, het is een fundament voor vertrouwen.

Dit boek is een praktische gids voor iedereen die de vertaalslag wil maken van beleid naar realiteit. Of u nu begint aan een implementatie of de lat hoger wilt leggen, het biedt inzichten die er écht toe doen.

Beveiliging is geen einddoel, maar een voortdurend proces. Ik hoop dat dit boek van Nico u inspireert om die reis met overtuiging en visie voort te zetten.

Marlon Jodhabier RE

Group Audit Country Head Director bij Deutsche Bank, voor de locaties in Nederland, Luxemburg, Frankrijk, Zweden en Portugal

Dit voorwoord is geschreven op persoonlijke titel en weerspiegelt mijn eigen inzichten

INLEIDING

Het is ruim 25 jaar geleden, begin 1998, dat ik mijn eerste functie kreeg op het gebied van informatiebeveiliging: security officer bij een pensioenbedrijf. In die tijd startte ik ook met de IT-auditingopleiding aan de Erasmus Universiteit in Rotterdam. Het vakgebied stond nog in de kinderschoenen en ik was geïntrigeerd door het fenomeen *security awareness.* Dit is de reden geweest dat ik dit onderwerp heb gekozen voor mijn afstudeerreferaat. Mijn overtuiging was - en is nog steeds - dat een positieve securitycultuur een randvoorwaarde is voor een effectieve informatiebeveiliging. Iedereen moet zijn rol, taken en verantwoordelijkheden goed kennen en daar ook naar handelen. Dit is onderdeel van de *governance*, maar ik noem het 'het schaakbord'.

Het mag geen verrassing zijn dat informatiebeveiliging steeds prominenter is geworden in het bedrijfsleven. De dreigingen nemen toe, net als de complexiteit van het IT-landschap. Legacy systemen ('de monsters in de kelder') moeten communiceren met moderne cloudtoepassingen, Artificial Intelligence dringt zich steeds meer op (als kans én risico) en bedrijven concentreren zich op hun kernbedrijfsprocessen (*core business*). Daardoor groeit hun toeleveringsketen *(supply chain)* snel. Maar weten ze nog steeds precies waar en door wie de beveiligingsmaatregelen worden uitgevoerd, en welke afspraken hierover zijn gemaakt?

Naast de (cyber)dreigingen en complexiteit, nemen ook de wet- en regelgeving en verantwoordingsplicht steeds verder toe. Bedrijven worstelen met NIS2, AVG, DORA, DNB, ISO 27001, ISAE 3402, SOC 2 et cetera. Hoe weten we zeker dat we aan alle eisen voldoen? Kunnen we onze *compliance* transparant maken

voor klanten of toezichthouders die daarom vragen? En kunnen we nog wel zaken doen wanneer we in aanbestedingstrajecten geen vinkje kunnen zetten bij 'in bezit van ISO 27001-certificaat'?

De hiervoor geschetste ontwikkelingen hebben een grote invloed gehad op de populariteit van ISO 27001. Het is een relatief klein document met een eenvoudige structuur en een bijlage met de meest voorkomende beveiligingsmaatregelen. Daarmee is ISO 27001 dé benchmark geworden waarmee bedrijven kunnen laten zien dat ze het belang van informatiebeveiliging inzien en zich inspannen om deze ook doeltreffend te laten zijn.

ISO 27001 heeft de afgelopen 25 jaar een ontwikkeling doorgemaakt met diverse nieuwe versies. Hierbij is vooral het managementsysteem (de Plan-Do-Check-Act- cyclus) doorontwikkeld en in lijn gebracht met andere ISO-standaarden, zoals ISO 9001 en ISO 14001. Voor de duidelijkheid: ISO 27001 bestaat uit twee delen. Het eerste deel betreft de hoofdstukken 4 tot en met 10, oftewel het Information Security Management System (ISMS). Het tweede deel betreft bijlage A, waarin 93 beveiligingsmaatregelen zijn opgenomen.

De populariteit van informatiebeveiliging en ISO 27001 heeft een grote aanzuigende werking gehad op de velen die inmiddels werkzaam zijn in dit vakgebied. Maar ondanks deze ontwikkeling is er nog steeds een tekort aan gekwalificeerde specialisten. De CISO's, security officers, securitymanagers en vCISO's (*virtual CISO*) zijn niet aan te slepen. Ook aan de kant van de auditors is er genoeg werk met veel nieuwe instroom (en vacatures) bij de certificerende instanties.

Het is daarom ook niet vreemd dat er zoveel interpretaties bestaan over de vereisten uit de standaard. We zijn allemaal mensen met onze eigen rugzak aan expertise, meningen en voorkeuren. ISO 27001 schrijft wel voor wat er moet worden gedaan maar niet hoe dat moet gebeuren. Organisaties moeten zelf duiding geven aan de ISO 27001-vereisten en moeten deze vereisten zelf inkleuren op een manier die passend is voor henzelf.

In de afgelopen jaren heb ik diverse kleine en grote organisaties, in verschillende bedrijfstakken, geholpen met hun ISO 27001-implementatie

en de voorbereiding op de certificering. Hierbij heb ik ook veel discussies meegemaakt tussen CISO's en auditors over bijzaken en over de persoonlijke mening van de auditor. En dat terwijl het juist zou moeten gaan over de vereisten uit de norm en hoe de organisatie deze heeft toegepast.

Dit boek is primair bedoeld om securityfunctionarissen sterker te maken. Enerzijds richting de eigen directie, om hen te overtuigen van de essentie van het hebben van een ISMS. Anderzijds richting management en medewerkers, om zinvolle discussies te kunnen voeren over het waarom van beveiligingsmaatregelen. En niet in de laatste plaats richting auditors, om constructieve discussies te kunnen voeren over de bedoeling achter de ISO 27001-vereisten. Gebruik dit boek vooral als aanvulling op andere vakliteratuur, om scherp te blijven en een open en eigen visie te ontwikkelen.

De inhoud van dit boek kan waardevol zijn voor organisaties die aan de vooravond staan van een ISO 27001-implementatie. De tips en templates kunnen ervoor zorgen dat het ISMS goed wordt ingericht en direct toegevoegde waarde heeft. Maar ook voor organisaties die recentelijk zijn gecertificeerd, kan de inhoud van dit boek bijdragen aan het heroverwegen van bepaalde uitgangspunten en het optimaliseren van het ISMS. Immers, net als een oude klok moet een ISMS 'inslingeren', waarmee ook de continue verbetering wordt bereikt - de essentie van een PDCA-cyclus.

Net als iedereen heb ik ook mijn eigen ervaring, expertise, mening en voorkeuren. Ik leer nog iedere dag: van mijn klanten, van auditors en van andere specialisten in mijn netwerk. Dit boek heb ik geschreven op persoonlijke titel en ik weet dat sommige vakgenoten anders aankijken tegen bepaalde onderwerpen - dat is natuurlijk prima. Alle interpretaties, voorbeelden en tips en tricks komen voort uit eigen ervaringen en mijn dagelijkse praktijk. Het blijft te allen tijde belangrijk om het 'boerenverstand' te gebruiken bij de implementatie van ISO 27001. De inhoud van dit boek kan uiteraard wél bijdragen aan de beeldvorming en besluitvorming binnen de eigen organisatie. Dit boek beoogt niet volledig te zijn en niet alles wordt met evenveel diepgang behandeld. Het is een bloemlezing met vooral veel praktische zaken die ik als waardevol beschouw.

In dit boek leg ik juist de nadruk op wat er niet expliciet in de norm staat - ISO 27001 tussen de regels.

De titel van dit boek is bewust gekozen, en misschien ook wel dé reden geweest dat ik het boek heb willen schrijven. ISO 27001 laat namelijk veel ruimte voor interpretaties die, voorzichtig gezegd, niet altijd naadloos op elkaar aansluiten. Maar tussen de regels (de vereisten) van deze standaard ligt juist de nuance. Tussen de regels ligt de ruimte. Gebruik deze ruimte daarom om ISO 27001 te plooien naar uw eigen organisatie in plaats van andersom. Spring dus niet alleen maar 'door het hoepeltje' van de auditor, maar stel uw eigen behoeften centraal, zodat uw ISMS past als een warme jas.

Deel 1 van dit boek gaat uitgebreid in op uitdagingen, en oplossingen, tijdens de ISO 27001-implementatie en -certificering.

In deel 2 staat het managementsysteem voor informatiebeveiliging (ISMS) centraal. Aan het eind van ieder normonderdeel treft u een handige checklist aan, die u kunt gebruiken om te controleren of u aan alles heeft gedacht.

In deel 3 wordt uitleg gegeven over de beheersing van door externen geleverde processen, producten of diensten die relevant zijn voor het ISMS. Dit is voor veel organisaties een actueel en complex onderwerp, waarop wet- en regelgeving en contractuele eisen van toepassing zijn.

Tot slot, treft u in de bijlage van dit boek een totaaloverzicht aan van alle checklists uit deel 2.

Vanuit praktische redenen wordt in dit boek regelmatig de term 'hij' gebruikt. Hiervoor in de plaats kan echter ook 'zij' of 'hen' worden gelezen.

Ten tijde van het schrijven van dit boek was NEN-EN-ISO/IEC 27001:2023 de meest actuele versie. Bij verwijzingen naar deze standaard worden in dit boek voor de leesbaarheid de begrippen 'ISO 27001', 'de standaard' of 'de norm' gebruikt.

Tot slot, dit boek gaat vooral over het eerste deel van ISO 27001: het ISMS met de hoofdstukken 4 tot met 10. Zeker, er worden diverse beheersmaatregelen

uit bijlage A van de norm als voorbeeld gebruikt. Maar die worden niet alle 93 in detail behandeld. Misschien iets voor een nieuw boek in de reeks 'Tussen de regels'? Laat het me vooral weten als daar behoefte aan is. Maar ook als u vragen of opmerkingen heeft naar aanleiding van dit boek, hoor ik graag van u: *nico.basten@awaretoday.nl*

Ik wens u veel leesplezier.

Nico

TUSSEN DE REGELS ISO 27001

ISO 27001 is razend populair. Begrijpelijk: informatiebeveiliging is complex en de dreigingen nemen voortdurend toe. ISO 27001 maakt dit inzichtelijk en bestuurbaar voor organisaties die samenwerken en behoefte hebben aan transparantie en zekerheid.

Die populariteit heeft echter ook geleid tot misverstanden, uiteenlopende interpretaties en discussies over wat de norm nu precies vraagt. Te vaak zijn implementaties vooral gericht op het tevredenstellen van auditors, in plaats van op het creëren van echte meerwaarde voor de organisatie. Dat is jammer en onnodig.

Dit boek is een praktische gids voor iedereen die betrokken is bij het organiseren of beoordelen van informatiebeveiliging. Voor iedereen die op zoek is naar nuance en ruimte tussen de regels. Het staat boordevol anekdotes, praktijkvoorbeelden, valkuilen, tips en bruikbare templates. Daarmee biedt het houvast aan organisaties die aan de start staan van een ISO 27001-implementatie én aan bedrijven die al gecertificeerd zijn en hun aanpak verder willen verfijnen.

OVER NICO BASTEN

Nico Basten RE CISA CISSP werkt al meer dan veertig jaar in het bedrijfsleven. Hij begon in 1985 als COBOL-programmeur en vervulde sindsdien uiteenlopende functies in systeemontwikkeling, IT-beheer, IT-audit, risicomanagement en informatiebeveiliging. Hij gaf jarenlang ISO 27001-trainingen en begeleidde talloze implementaties bij zowel kleine als grote organisaties. Nico is geboren in 1964, woont met zijn vrouw in Amersfoort en heeft twee dochters en vier kleinkinderen.

ISBN 9789090407845