BEST PRACTICE

BASISKENNIS INFORMATIE-BEVEILIGING

OP BASIS VAN ISO27001 EN ISO27002

4de herziene druk

Jule Hintzbergen | Kees Hintzbergen | Hans Baars

Van Haren PUBLISHING

Basiskennis informatiebeveiliging op basis van ISO 27001 en ISO 27002
Vierde herziene druk

Andere uitgaven bij Van Haren Publishing

Van Haren Publishing (VHP) is gespecialiseerd in uitgaven over Best Practices, methodes en standaarden op het gebied van de volgende domeinen:

- IT en IT-management;
- Enterprise-architectuur;
- Projectmanagement;
- Businessmanagement.

Deze uitgaven zijn beschikbaar in meerdere talen en maken deel uit van toonaangevende series, zoals *Best Practice, The Open Group series, Project management* en *PM series.*

Van Haren Publishing is tevens de uitgever voor toonaangevende instellingen en bedrijven, onder andere: Agile Consortium, ASL BiSL Foundation, CA, Centre Henri Tudor, CM Partners, Gaming Works, IACCM, IAOP, IPMA-NL, ITSqc, NAF, KNVI, PMI-NL, PON, The Open Group, The SOX Institute.

Onderwerpen per domein zijn:

IT en IT-management
ABC of ICT
ASL®
CMMI®
COBIT®
e-CF
ISM
ISO/IEC 20000
ISO/IEC 27001/27002
ISPL
IT4IT®
IT-CMF™
IT Service CMM
ITIL®
MOF
MSF
SABSA
SAF
SIAM™
TRIM
VeriSM
XLA®

Enterprise-architectuur
ArchiMate®
BIAN
GEA®
Novius Architectuur Methode
TOGAF®

Projectmanagement
A4-Projectmanagement
DSDM/Atern
ICB / NCB
ISO 21500
MINCE®
M_o_R®
MSP®
P3O®
PMBOK® Guide
Praxis®
PRINCE2®

Businessmanagement
BABOK® Guide
BiSL® en BiSL® Next
BRMBOK™
BTF
CATS CM®
DID®
EFQM
eSCM
FSM
IACCM
ISA-95
ISO 9000/9001
OBM
OPBOK
SixSigma
SOX
SqEME®

Voor een compleet overzicht van alle uitgaven, ga naar onze website: www.vanharen.net

Basiskennis informatiebeveiliging

op basis van ISO 27001 en ISO 27002

vierde volledig herziene druk

Jule Hintzbergen
Kees Hintzbergen
Hans Baars

Van Haren PUBLISHING

Colofon

Titel:	Basiskennis informatiebeveiliging op basis van ISO 27001 en ISO 27002 - Vierde volledig herziene druk
Auteurs:	Jule Hintzbergen, Kees Hintzbergen, Hans Baars
Uitgever:	Van Haren Publishing, 's-Hertogenbosch, www.vanharen.net
ISBN hard copy:	978 94 018 0991 7
ISBN eBoek (pdf):	978 94 018 0992 4
ISBN ePub:	978 94 018 0993 1
Druk:	Tweede druk, eerste oplage, mei 2010 Derde druk, eerste oplage, april 2015 Vierde druk, eerste oplage, april 2023
Lay-out en dtp:	Coco Bookmedia, Amersfoort
Copyright:	© Van Haren Publishing, 2010, 2015, 2017, 2023

Voor verdere informatie over Van Haren Publishing, e-mail naar: info@vanharen.net.

Voorwoord door de auteurs

Dit is de vierde druk van dit boek dat is bedoeld om meer te leren over informatiebeveiliging en u kan helpen bij het behalen van een ISFS-certificering van EXIN. Het verschil met de vorige – 3de – druk is dat de inhoud van deze nieuwe druk is afgestemd op een totaal herziene versie van de ISO 27002 die in 2022 is verschenen.

Een herziening van de ISO 27002 standaard blijft meestal beperkt tot wat nieuwe onderwerpen, het verwijderen van bepaalde achterhaalde termen of technieken en aanpassingen aan de tijd. Zo verdween de floppydisk in de loop van de tijd en werd in 2013 het onderwerp cryptografie als een nieuw hoofdstuk toegevoegd.

In de nieuwe 2022 versie van de ISO 27002 is echter veel niet gebleven zoals het was. Er werden 24 onderwerpen samengevoegd en er kwamen 13 nieuwe maatregelen (controls) bij. De grootste veranderingen waren echter het terugbrengen van 14 hoofdstukken naar vier hoofdstukken waarbinnen de maatregelen opnieuw gegroepeerd werden. Deze vier hoofdstukken worden nu thema's genoemd.

Hiermee is de standaard compleet nieuw beschreven en ingedeeld. Ook werd de structuur van de maatregelbeschrijving aangepakt. Daar waren twee redenen voor:

1. De voorgaande (2013) versie werd de afgelopen jaren steeds meer gebruikt als niet meer dan een checklist. Er werd niet meer zorgvuldig nagedacht over het doel van de maatregel, maar er werd alleen gekeken of de maatregel geïmplementeerd was en dan werd het afgevinkt als 'klaar'. Er zit echter wel verschil tussen het implementeren van de goedkoopste virusscanner en het niet dagelijks updaten ervan of uitzoeken welke virusscanner de beste beveiliging in uw specifieke situatie biedt en zorgen dat deze in een dagelijkse update-cyclus actueel wordt gehouden. Zo kunnen we bij vrijwel ieder onderwerp wel een voorbeeld bedenken.
2. Men is na de introductie in de jaren '90 anders tegen de zaak aan gaan kijken. Er wordt nu meer in thema's, attributen en KPI's gedacht. Deze nieuwe versie van de ISO-standaard speelt daarop in en laat de security professionals meer en beter nadenken over de wijze waarop zij de security voor hun bedrijf vorm willen geven. Velen zullen moeten wennen aan de nieuwe opzet.

Dit boek neemt de wijzigingen in de nieuwe ISO 27002 over en zal de komende jaren als leidraad dienen voor wie zich in het onderwerp gaat verdiepen, en zeker voor wie zich gaat (her)certificeren op basis van de ISO 27001.

De ISO 27002 standaard heeft een nieuwe titel gekregen. De oude titel was: *Informatietechnologie - Beveiligingstechnieken - Praktijkcode voor informatiebeveiligingscontroles*. De keuze is nu gemaakt voor *Informatiebeveiliging, cybersecurity en privacybescherming - Informatiebeveiligingscontroles*. De zinsnede "Praktijkcode" is uit de titel van dit document verwijderd om het doel van het document beter weer te geven. Het betreft een referentieset van informatiebeveiligingsmaatregelen.

Het doel van de ISO27002:2022 standaard is niet gewijzigd ten opzichte van de oude versies uit de jaren 2013-2020. De bedoeling van de ISO/IEC 27002 standaard is altijd geweest om organisaties te helpen ervoor te zorgen dat noodzakelijke maatregelen niet over het hoofd worden gezien.

Een van de doelstellingen van de ISO/IEC 27002 standaard is dat organisaties hun eigen informatiebeveiligingsmanagement kunnen afstemmen. Als vanouds maken de begrippen Beschikbaarheid, Integriteit en Vertrouwelijkheid een onlosmakelijk onderdeel uit van de ISO 27002. Daarbij zijn nu echter ook de vijf attributen uit de in 2018 geïntroduceerde ISO 27103, *Cybersecurity Framework* bijgekomen: Identify, Protect, Detect, Respond en Recover. Een dergelijke waarde wordt voorafgegaan door een "#" waardoor het gemakkelijk is om een attribuut te vinden of om op een dergelijk attribuut te filteren. Hiermee is onder andere het cybersecurity framework uit de in 2018 verschenen ISO/IEC 27103 standaard, een integraal onderdeel geworden van ISO/IEC 27002.

De auteurs

Inhoudsopgave

1 Introductie

Dit boek is bedoeld voor iedereen in een organisatie die basiskennis van informatiebeveiliging op wil doen. Kennis over informatiebeveiliging is belangrijk voor iedere medewerker. Het maakt geen verschil of u in een commercieel of een niet-commercieel bedrijf werkt. Elke organisatie heeft te maken met risico's op het gebied van informatiebeveiliging.

Medewerkers moeten weten waarom zij in hun dagelijkse werkzaamheden beveiligingsvoorschriften moeten naleven. Lijnmanagers moeten kennis hebben van informatiebeveiliging omdat zij daarvoor binnen hun afdeling verantwoordelijk zijn. Deze basiskennis is ook belangrijk voor alle directieleden en zelfstandigen zonder personeel (zzp'ers). Ook zij zijn verantwoordelijk voor het beschermen van de eigendommen en informatie die zij bezitten. Een bepaald gevoel van bewustwording is ook voor de thuissituatie belangrijk. En natuurlijk is deze basiskennis onontbeerlijk als u besluit van informatiebeveiliging, IT, of procesmanagement uw beroep te maken.

Iedereen heeft te maken met informatiebeveiliging, al is het maar met de beveiligingsmaatregelen die een organisatie genomen heeft. Deze beveiligingsmaatregelen zijn soms afgedwongen door wet- en regelgeving. Soms worden ze geïmplementeerd op basis van intern beleid. Neem als voorbeeld het gebruik van een wachtwoord op de computer. Vaak beschouwen we beveiligingsmaatregelen als lastig en overbodig. Ze kosten tijd en het is lang niet altijd duidelijk waartegen ze ons beschermen.

In informatiebeveiliging moet worden nagestreefd om de gulden middenweg te vinden tussen een aantal aspecten:

- De kwaliteitseisen die een organisatie stelt aan zijn informatie.
- De risico's die geassocieerd worden met die kwaliteitseisen.
- De beveiligingsmaatregelen die genomen worden om die risico's af te dekken.
- Ervoor zorgen dat bedrijfsprocessen doorgaan in het kader van de bedrijfscontinuïteit.
- Vaststellen wanneer en op welke manier incidenten buiten de organisatie gerapporteerd worden.

1.1 BELANGRIJKE WIJZIGINGEN IN DE ISO/IEC 27002:2022

1.1.1 Vormgeving van de beveiligingsmaatregelen in de ISO/IEC 27002: 2013

De 2013-versie van de ISO/IEC 27002 en de updates gedurende de jaren tot 2020 kenden vier inleidende hoofdstukken en 13 hoofdstukken inclusief beveiligingsrichtlijnen: de hoofdstukken 5 t/m 18. Elk hoofdstuk bevatte paragrafen met daarin een 'doel' en één of meer sub-paragrafen inclusief een richtlijn- en een implementatieleidraad.

1.1.2 Gewijzigde aanpak van de beveiligingsmaatregelen in de ISO/IEC 27002:2022

De nieuwe versie ISO/IEC 27002:2022 bevat vier inleidende hoofdstukken. De beveiligingsmaatregelen zijn nu anders gegroepeerd in vier thema's. Ieder thema omvat één hoofdstuk. Hierdoor is het aantal hoofdstukken met beveiligingsmaatregelen van 14 in de oude standaard teruggebracht naar vier in de nieuwe standaard. Dit heeft gevolgen voor organisaties die hun Information Security Management System (ISMS) hebben opgebouwd op basis van de oude standaard, de referenties naar de nieuwe ISO kloppen nu niet meer. Dit betekent veel werk in het aanpassen van het bestaande ISMS.

De standaard-indeling van beheersmaatregelen is aangepast. Naast de naam en attributen (zie tabel 1.1) worden per beheersmaatregel de volgende vijf beveiligingsaspecten getoond:

Tabel 1.1 Beveiligingsaspecten

Type beheersmaatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligingsdomeinen
#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren	#Governance	#Governance_ en_Ecosysteem #Veerkracht

Het doel van deze verdeling is dat de securitymanager van het bedrijf zelf kan bepalen langs welke aandachtsgebieden hij beveiligingsmaatregelen wil beschouwen. Wat wordt leidend? Blijven de van oudsher bekende BIV- (CIA-) classificaties leidend? Of gaan we de beveiligingsmaatregelen groeperen rond de vijf Cybersecurity-aspecten? Met deze verdeling kijkt de ISO eindelijk ook eens verder dan zichzelf en zie je een duidelijke verbinding naar de indeling van de vorige versie van de ISO 27002, maar ook naar andere (niet-ISO) standaarden. In hoofdstuk 4 worden deze concepten verder toegelicht.
Zoals in tabel 1.1 is te zien, staat voor ieder van de aspecten een #. Dit is bedoeld om snel te kunnen zoeken op zo'n aspect. Zou u zoeken op de term 'integriteit', dan komen er 221 resultaten. Zoekt u echter op #Integriteit, dan blijven er 183 resultaten over, die direct aan een beveiligingsmaatregel gekoppeld zijn.

1.2 WAT IS KWALITEIT?

Kwaliteit is een maat voor de overeenkomst tussen prestatie en verwachting. In het algemeen wordt met kwaliteit aangegeven of eigenschappen van een product of dienst overeenkomen met wat ervan verwacht wordt.

Eerst zult u als organisatie moeten bepalen wat u onder kwaliteit verstaat. Op het eenvoudigste niveau dient kwaliteit twee vragen te beantwoorden: "wat wordt er gevraagd?" en "hoe doen we het?"

Vanzelfsprekend ligt de basis van kwaliteit altijd in het gebied van de werkprocessen. Aan de hand van kwaliteitsaspecten, zoals beschreven in de ISO 9000, en procesbeschrijvingen volgens het concept van 'Total Quality Management' (TQM), specificeren, meten en verbeteren kwaliteitsprofessionals de processen, en indien nodig herontwerpen zij processen om er zeker van te zijn dat organisaties krijgen wat ze willen.

Waar zijn we nu?
Er zijn net zoveel definities voor het woord 'kwaliteit' als er kwaliteitsconsultants zijn, maar algemeen aanvaarde omschrijvingen zijn:

- Voldoen aan eisen ('Conformance to requirements') – P.B. (Phil) Crosby.
- Passend binnen het gewenste gebruik ('Fitness for use') – Joseph Juran.
- Het totaal van karakteristieken dat een entiteit draagt in zijn mogelijkheid om aan vastgestelde en onuitgesproken eisen te voldoen. - ISO 8402:1995.
- Kwaliteitsmodellen voor bedrijven, inclusief de kwaliteitscirkel van Deming, het EFQM excellence model en de Baldrige prijs.

Het primaire doel van dit boek is om studenten voor te bereiden op het examen Information Security Foundation based on ISO/IEC 27001 van EXIN. Het boek is gebaseerd op de internationale standaard NEN-ISO/IEC 27002:2022.

Docenten kunnen de informatie in dit boek gebruiken om de kennis van hun studenten te toetsen. Aan het eind van ieder hoofdstuk is een case opgenomen. Alle cases gaan in op de onderwerpen die in het desbetreffend hoofdstuk zijn behandeld en geven veel vrijheid in de wijze waarop de vragen beantwoord kunnen worden. Voorbeelden van recente incidenten op het gebied van informatiebeveiliging zijn 'vertaald' naar de casestudie en verduidelijken de teksten in het boek.

De case start op een basisniveau en naar gelang we verder komen in het boek, wordt het niveau hoger. De case is gebaseerd op de boekhandel Springbooks. In het begin telt Springbooks enkele medewerkers en heeft ze beperkte informatiebeveiligingsrisico's. In de achtereenvolgende hoofdstukken zien we de boekhandel groeien en aan het eind is het een grote organisatie met 120 winkels en haar internetwinkel kent een uitgebreid assortiment. De risico's en dreigingen nemen met de groei van de winkelketen ook toe.

Dit boek is bedoeld om de verschillen tussen risico's en kwetsbaarheden uit te leggen en de beveiligingsmaatregelen die kunnen helpen om deze risico's en kwetsbaarheden zo veel mogelijk in te perken. Door het algemene karakter van dit boek is het ook goed bruikbaar als materiaal voor een bewustwordingstraining of als naslagwerk tijdens een bewustwordingscampagne.

Dit boek is zowel gericht op profit- als op non-profitorganisaties. Het is echter ook goed toepasbaar in de huiselijke situatie en voor kleine bedrijven (MKB) die geen eigen beveiligingsmedewerkers in dienst hebben. In het MKB is beveiliging meestal een (bij)taak voor een enkele medewerker.

Na het lezen van dit boek heeft u algemene kennis opgedaan over de onderwerpen waar informatiebeveiliging over gaat. U weet ook waarom die onderwerpen belangrijk zijn en heeft u kennis verworven van de meest algemene concepten die gebruikt worden binnen de informatiebeveiliging.