Discussion paper

‘Hoe verhoudt de ISO27701 zich tot andere raamwerken?’

Een vergelijking van de ISO27701 met andere raamwerken[1] op het gebied van privacy

Door: drs. Ing. Jessica Maes CISA LA ISO27001, drs. Harry van den Brink RE CISM CRISC CDPSE LA ISO27001 LA ISO27701, Stephan van der Ende MScBA CISM CISA CRISC.

Inleiding en introductie discussion papers ISO27701

In augustus 2019 is de privacy gerelateerde standaard met de naam: ‘ISO/IEC[2] 27701:2019 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines’ (hierna: ‘ISO27701’) uitgekomen.

Vanuit de focusgroep ISO27701 brengen wij een serie discussion papers uit (verder kortweg ‘paper’ genoemd) over de ISO27701. Dit is de tweede in de reeks. De eerste paper: ‘Wat is de ISO27701 en waarom is dit belangrijk voor mij of mijn organisatie?’ kun je vinden op de ISACA-website. In deze paper hebben wij besproken wat de ISO27701 inhoudt en waarom deze belangrijk kan zijn voor jou en je organisatie. In deze tweede paper kijken we hoe de ISO27701 zich verhoudt tot bestaande privacy raamwerken. Hiervoor beschrijven wij de belangrijkste verschillen en overeenkomsten met de meest bekende raamwerken gerelateerd aan privacy die wereldwijd gebruikt worden.
Voor de genoemde raamwerken hebben wij dankbaar gebruik gemaakt van openbare informatie op de sites van de verschillende organisaties.

[1] NB: in deze paper gebruiken we de term raamwerk voor een document dat formeel uitgebracht kan zijn als framework, baseline, norm, best practice, enz. Het doel is echter voor al deze soorten documenten gelijk: het geven van een handvat voor beleid en implementatie.
[2] International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

Inventarisatie privacy raamwerken en de onderscheidende kenmerken

Er zijn veel raamwerken die je kunnen helpen om je privacybeleid en bijbehorende maatregelen op te baseren. Het doel van deze raamwerken verschilt nogal. Zo heb je raamwerken die zich hoofdzakelijk richten op het managementsysteem, de te treffen maatregelen, het meten of verhogen van de volwassenheid of het uitvoeren van risicoanalyses zoals een Data Protection Impact assessment (DPIA). Ook kunnen raamwerken gebruikt worden als hulpmiddel bij het voldoen aan wet- en regelgeving. ISO27701 heeft als basis het Privacy Information Management System (PIMS).
In Tabel A Overzicht raamwerken in relatie tot ISO27701 hebben we een overzicht gegeven van een aantal van deze bekende raamwerken en de kenmerken van deze raamwerken op een rijtje gezet. Wij hebben ons geconcentreerd op raamwerken die een relatie met ISO-normen voor privacy hebben, dan wel zich specifiek richten op privacy.

Het door ISACA ontwikkelde raamwerk COBIT is ook in deze vergelijking betrokken, omdat een aantal in Nederland gebruikte raamwerken op COBIT gebaseerd zijn. Denk daarbij bijvoorbeeld aan organisaties in de financiële sector die gebruik moeten maken van het DNB Security raamwerk, welk op COBIT 4 is gebaseerd.
Na Tabel A volgt een verder uitwerking per raamwerk, waarbij de doelgroep, het doel, het verschil met de ISO27701 en de eventuele toegevoegde waarde van de combinatie met ISO27701 wordt beschreven.

Personally Identifiable Information (PII) versus Personal Data

In deze paper bespreken wij nationale – en internationale raamwerken. Waar in internationale en Noord-Amerikaanse raamwerken vaak wordt gesproken over “PII” (Personally Identifiable Information), wordt er in Europese raamwerken voornamelijk over personal data gesproken. Deze begrippen, die overigens per raamwerk kunnen verschillen, lijken op elkaar, maar betekenen niet precies hetzelfde. Zonder het verschil exact te duiden, kun je stellen dat de definitie van personal data in het algemeen wat breder is dan die van PII. Daarom is het per situatie van belang om te kijken welke definitie passend is voor de organisatie om mee te werken.
In lijn met de Europese definitie van personal data wordt er in de in Nederland gebruikte raamwerken gesproken over persoonsgegevens. Specifiek voor de inzet van ISO27701 in een Nederlandse setting, betekent dat in plaats van PII te gebruiken als uitgangspunt, de organisatie zich moet concentreren op de verwerking van persoonsgegevens. Het begrip persoonsgegeven is in de Algemene verordening gegevensbescherming (AVG) overigens gedefinieerd in artikel 4.

TABEL A: Overzicht raamwerken in relatie tot ISO27701

Voor een uitgebreidere toelichting op de antwoorden, zie tekst paper

Raamwerk/ Element	**ISO27701**	**ISO27001 & ISO27002**	**COBIT**	**ISACA Privacy Principles**	**NIST Privacy Framework**	**NOREA**	**ISO29100**	**CIP Baseline**	**AICPA/CICA Privacy Maturity Model**
Type raamwerk	Norm	Norm	Framework	Principles	Framework	Control Framework	Framework	Best Practice	Volwassen-heidsmodel
Primaire invalshoek	Privacy	Security	IT algemeen	Privacy	Privacy	Privacy	Privacy	Privacy	Privacy
Relatie tot GDPR/AVG	Via cross-reference	Indirect via wet/regelgeving	Via aparte White Paper van ISACA	Via cross-reference	Via cross-reference	Via cross reference	Geen directe relatie	AVG is basis voor normenkader	Geen directe relatie
Primaire doelgroep gebruikers	**FG, PO** CISO, SecOff / Auditors	**CISO, SecOff** PO / Auditors	Generiek	**FG, PO**	**FG, PO** CISO, SecOff	**Auditors** FG, PO	**FG, PO**	**Auditors** FG, PO	**Auditors** FG, PO
Certificeer baar	ISO Certificering	ISO Certificering	Nee	Nee	Nee	Privacy Audit Proof Certificering	Nee	Nee	Nee
Voornaamste geografische toepassing	Internationaal	Internationaal	USA, oorsprong België	USA	Internationaal / USA	Nederland	Internationaal	Nederland	USA/Canada
Opmerkingen	Eerste keus voor gebruikers die al ISO27001 zijn gecertificeerd				Eerste keus voor Internationale organisaties die al gebruik maken van het NIST CSF.	Geeft een beeld van hoe een organisatie ervoor staat op het gebied van privacy.	Holistische approach t.a.v. privacy binnen organisatie. De ISO29100 is mede de basis (begrippen) voor ISO27701	Specifiek op overheid gericht.	

In de rij primaire gebruikers wordt door ons de eerstgenoemde en vetgedrukte functie gezien als de primaire hoofdgebruiker. FG staat voor Functionaris Gegevensbeveiliging (formele functie in AVG), PO voor Privacy Officer, CISO voor Chief Information Security Officer, SecOff voor Security Officers.

Detailbevindingen per raamwerk

ISO27001 (en de bijbehorende ISO27002)

Benaming: NEN[3]-EN-ISO/IEC 27001:2017+A11:2020 -Information Technology-Security techniques-Information security management systems-requirements.
Doelgroep: Het raamwerk is bedoeld om breed inzetbaar te zijn voor organisaties van elke omvang en onafhankelijk van technologie, sector, wet of jurisdictie. In Nederland zijn bij de overheid deze normen als bron gebruikt en aangevuld met specifieke overheidsmaatregelen; deze vormen de Baseline Informatiebeveiliging overheid (BIO). Voor de zorg geldt een soortgelijke systematiek voor de NEN7510.
Doel: ISO27001 is gericht op het opstellen van een Information Security Management System (ISMS). De norm specificeert eisen voor het vaststellen, implementeren, uitvoeren, controleren, beoordelen, bijhouden en verbeteren van een gedocumenteerd ISMS. Nauw aan de ISO27001 verbonden is de ISO27002. De ISO27002 biedt daadwerkelijk een verdiepingsslag. In deze norm wordt namelijk gedetailleerd aangegeven welke maatregelen genomen kunnen worden om aan de normeisen van ISO27001 te voldoen.
Verschil met de ISO27701: De ISO27001 is primair gericht op het managementsysteem voor informatiebeveiliging en niet zozeer op het managementsysteem voor privacy, al is er natuurlijk een verband.
Toegevoegde waarde van de combinatie: De waarde van deze combinatie is evident. Omdat de ISO27701 een extensie is van de ISO27001 kunnen beiden niet los van elkaar gezien worden. Het Privacy Information Management System (PIMS) van de ISO27701 moet (bij certificering) toegepast worden in samenhang met het ISMS van de ISO27001/ISO27002, waardoor informatiebeveiliging en privacy op managementsysteemniveau worden geïntegreerd.

[3] Stichting Koninklijk Nederlands Normalisatie Instituut

COBIT

Benaming: COBIT 2019, Oktober 2018
Doelgroep: Alle organisaties die behoefte hebben aan een effectieve beheersing en besturing (governance) van informatie en IT.
Doel: Het ondersteunen van organisaties bij het implementeren en beheersen van een effectieve governance van IT, informatiemanagement en controls om de bijbehorende risico's te mitigeren. COBIT 2019 is een zeer uitgebreid raamwerk wat als basis wordt gebruikt in vele andere raamwerken. Het kent onder andere zes governance principles, drie framework principes, vijf domeinen, focus areas, design factors en een zeer uitgebreide set van controls en performance indiciatoren. Door aansluiting op het CMMI-model kan COBIT ook eenvoudig gebruikt worden om de volwassenheid op het gebied van IT governance van een organisatie te bepalen. COBIT is bij uitstek geschikt om in combinatie met andere raamwerken te gebruiken. Naast COBIT heeft ISACA ook Privacy Principles opgesteld (hierna uitgewerkt).
Verschil met de ISO27701: COBIT is vele malen breder in scope dan Privacy. COBIT zelf is niet certificeerbaar.
Toegevoegde waarde van de combinatie: als COBIT en de ISACA Privacy Principles beiden zijn geïmplementeerd, kan men bij ISO27701 certificering hier gebruik van maken en zal de ISO27701 implementatie daarom relatief eenvoudig zijn.

ISACA Privacy Principles

Benaming: Privacy Principles and Program Management Guide, 2017
Doelgroep: Organisaties die zich aan het oriënteren zijn op een privacy governance and managementprogramma en die bij voorkeur al gebruik maken van COBIT.
Doel: Het belangrijkste doel van ISACA Privacy Principles is om privacy principes te beschrijven die aansluiten bij de meest gebruikte privacystandaarden, kaders en best practices, en de hiaten opvullen die tussen de verschillende normen bestaan om een geharmoniseerd privacykader te bieden. Deze praktische uitwerking kan separaat gebruikt worden of in combinatie met andere privacykaders en standaarden. Er is specifiek aandacht voor het opzetten van een privacy raamwerk waarmee je gebruik maakt van COBIT 5. Hierbij wordt gebruik gemaakt van de 14 ISACA Privacy Principles.
Deze privacy principes zijn vergeleken met de OECD[4] 2013, ISO29100:2011, APEC[5] en GAPP[6].
Het document geeft een overzicht van privacy concepten, definieert een geharmoniseerde reeks privacy principes, biedt stapsgewijze richtlijnen voor het identificeren van privacyvereisten en het creëren, implementeren en onderhouden van een privacyprogramma dat voldoet aan bedrijfsspecifieke behoeften.
Verschil met de ISO27701: Het is geen norm maar een praktische uitwerking waarmee je een eigen privacy raamwerk kan opzetten.
Toegevoegde waarde combinatie: Door het gebruik van het theoretisch kader van de ISACA Privacy Principles en COBIT wordt de praktische invulling van ISO27701 onderbouwd. Als COBIT en de ISACA Privacy Principles beiden zijn geïmplementeerd, kan men bij een ISO27701 certificering hier gebruik van maken en zal de ISO27701 implementatie daarom relatief eenvoudig zijn. Met name voor internationale organisaties is een overkoepelend model, niet gekoppeld aan Europeese wetgeving, een meerwaarde.

[4] Organization for Economic Cooperation and Development
[5] The Asia-Pacific Economic Cooperative
[6] Generally Accepted Privacy Principles

NIST Privacy Framework

Benaming: The NIST[7] Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management, Version 1.0 (January 2020)
Doelgroep: Het raamwerk is bedoeld om breed inzetbaar te zijn voor organisaties van elke omvang en onafhankelijk van technologie, sector, wet of jurisdictie.
Doel: Het Privacy Framework volgt de structuur van het Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework) om het gebruik van beide frameworks samen te vergemakkelijken. Net als het Cybersecurity Framework bestaat het Privacy Framework uit drie delen: Core, Profiles en Implementation Tiers.
De indeling is gebaseerd op de categorieën en de functies Identify-P, Govern-P, Control-P, and Communicate-P. In het Cybersecurity Framework is er een uitgebreide bijlage met controls opgenomen, gebaseerd op deze indeling.
Verschil met de ISO27701: Het PIMS is niet als zodanig een expliciet onderwerp binnen NIST. Privacy Risk management is wel een fundament waar de controls op gebaseerd zijn. Het raamwerk is niet certificeerbaar in NL.
Toegevoegde waarde combinatie: de ISO27701 controls kunnen een aanvulling zijn op de NIST privacy controls door de focus op een PIMS. Ook als certificatie vereist is, is ISO27701 een voor de hand liggende oplossing.

[7] National Institute of Standards and Technology

NOREA Privacy Framework (NOREA PCF)

Benaming: NOREA Handreiking - Privacy Control Framework - Beheersingsdoelstellingen en beheersingsmaatregelen voor privacy audits en privacy-assurance opdrachten - Versie 2.0 Augustus 2019
Doelgroep: Deze handreiking is uitgegeven door NOREA, de beroepsorganisatie van IT-auditors in Nederland, en is ontwikkeld om Nederlandse gekwalificeerde IT-auditors (Register IT-auditors, RE's) handvatten te bieden om een assurance rapport op te stellen in lijn met de Europese Algemene Verordening Gegevensbescherming (AVG) en relevante standaarden voor assurance opdrachten.
Doel: Het primaire doel van het NOREA PCF is het bieden van ondersteuning aan (audit)professionals bij de beoordeling of de beheersingsdoelstellingen van een entiteit met betrekking tot privacy en bescherming van persoonsgegevens worden behaald. Het PCF kan worden gebruikt als startpunt voor privacyaudits op maat. Het PCF bevat de voorgeschreven beheersingsdoelstellingen en voorbeelden van maatregelen voor privacyopdrachten op basis van de NOREA Richtlijn 3000. Het PCF kan eveneens worden gebruikt om invulling te geven aan het privacy-deel van een SOC2 assurance rapport voor een entiteit die moet voldoen aan de Algemene Verordening Gegevensbescherming (AVG). In bijlage 3 van het NOREA PCF is een cross reference opgenomen met ISO27001, ISO27701 en ISO29100.
Verschil met de ISO27701: Het NOREA PCF is geheel en al gericht op auditors en hun audit werkzaamheden. ISO27701 is gericht op het inrichten van een Privacy Information Management System bij organisaties.
Toegevoegde waarde van de combinatie: Het PCF kan gebruikt worden om de wettelijke eisen van de AVG toetsbaar in het PIMS op te nemen.

ISO29100

Benaming: ISO/IEC 29100:2011 Information technology — Security techniques — Privacy framework.
Doelgroep: Het is bedoeld om breed inzetbaar te zijn door organisaties van elke omvang en onafhankelijk van technologie, sector, wet of jurisdictie.
ISO29100 is bedoeld om gebruikt te worden door personen en organisaties die betrokken zijn bij het ontwerp, de aanschaf, het opstellen van de architectuur, het testen, het onderhouden en het bedienen van ICT-systemen waar privacy controls nodig zijn voor het verwerken van persoonsgegevens.
Doel: ISO29100 is ontwikkeld met als doel om organisaties handvatten te bieden bij het definiëren van hun maatregelen om privacy te beschermen. Om dit te bereiken biedt de ISO29100 een raamwerk dat een organisatie helpt met de volgende zaken:

- het specificeren van een gemeenschappelijke privacy terminologie;
- het definiëren van actoren en hun rol bij het verwerken van persoonsgegevens;
- het beschrijven maatregelen om privacy te beschermen;
- het bieden van referenties naar bekende privacy principes voor IT.

Verschil met de ISO27701: Waar ISO29100 meer op hoofdlijnen blijft en gebruikt kan worden door organisaties om aan de slag te gaan met privacy en om te bepalen hoe de organisatie met privacy omgaat, gaat de ISO27701 dieper in op specifieke privacy controls. Een voorbeeld hiervan zijn de controls vanuit ISO27701 om tijdelijke files waarin persoonsgegevens worden verwerkt te wissen of verwijderen invulling geeft aan het principe van limitatie van het gebruik, bewaren en ontsluiten van persoonsgegeven (zoals genoemd in ISO29100).
De ISO29100 is reeds gepubliceerd in 2011. In de meer recente ISO27701 uit 2019 is een mapping opgenomen in Annex C, waarin de (meer specifieke) controls uit de ISO27701 zijn gekoppeld aan de (meer algemenere) principes beschreven in ISO29100.
Op de ISO29100 kun je je als organisatie niet laten certificeren en op de ISO27701 wel.
Toegevoegde waarde van de combinatie: Omdat ISO29100 meer algemeen van aard is en de ISO27701 zich specifieker richt op de controls, zijn de normen naast elkaar of in elkaars verlengde te gebruiken.

CIP Centrum informatiebeveiliging en privacybescherming:

De Privacy Baseline

Benaming: De Privacy Baseline: de AVG ontrafeld voor toepassing in organisaties, versie 3.3, 27 oktober 2020
Doelgroep: Organisaties die (aantoonbaar) willen voldoen aan de AVG en zoeken naar een praktisch normenkader. In de praktijk zijn dit vaak Nederlandse overheids- en/of publieke organisaties.
Doel: In de privacy baseline zijn de eisen van de AVG vertaald naar normen die ondersteunen bij het voldoen aan de AVG. De basis van het document zijn dertien principes (of richtlijnen) die helpen te kunnen voldoen aan de AVG. Per richtlijn is een referentie is opgenomen naar de artikelen uit de AVG.
Het helpt bij de verantwoordingsplicht die inhoudt dat naleving van de wet moet worden aangetoond. Naleving van de baseline brengt een organisatie naar een volwassenheidsniveau dat doorgaans voldoende is om een basale compliance-toets te doorstaan.
Verschil met de ISO27701: Er kan niet gecertificeerd worden op basis van het CIP model, het helpt organisaties wel om doelgericht te voldoen aan de AVG.
Toegevoegde waarde van de combinatie: Bij de baseline hoort een daarop gebaseerd volwassenheidsmodel en een privacy self assessment. De ISO27701 is een relevante toevoeging (op een overkoepelend niveau) om het beheerssysteem van de organisatie te verbeteren. Door het implementeren van ISO27701 wordt een uitgebreid privacy managementsysteem opgezet.

AICPA/CICA Privacy Maturity Model

Benaming: American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) Privacy Maturity Model (PMM)
Doelgroep: AICPA/CICA vertegenwoordigt de Certified Public Accountants (CPA) - beroepsgroep in de Verenigde Staten en Canada op nationaal niveau met betrekking tot het opstellen van regels en normen. Daarnaast treedt de AICPA op als pleitbezorger voor wetgevende organen, organisaties van openbaar belang en andere professionele organisaties. De AICPA ontwikkelt standaarden voor audits van particuliere bedrijven en andere diensten door CPA's.
Het model kan nuttig zijn voor management, consultants en auditors en kan gebruikt worden om een sterk privacy programma op te zetten en om de voortgang hiervan bij te houden. Het model kan in principe door iedere organisatie worden toegepast.
Doel: Een organisatie kan met behulp van het volwassenheidsmodel inzicht verkrijgen in de volwassenheid van de privacy functie binnen de organisatie. Daarnaast kan het ook gebruikt worden om te bepalen welke stappen er nodig zijn om naar een hoger volwassenheidsniveau te komen.
Het AICPA/CICA Privacy Maturity Model is gebaseerd op de Generally Accepted Privacy Principles (GAPP). Op basis van deze GAPP zijn 73 meetbare criteria opgesteld en op elk van deze criteria kan de volwassenheid van de organisatie worden bepaald. De GAPP zijn overigens ook van belang bij een SOC2 audit. Hierbij worden ze meegenomen bij het deel dat betrekking heeft op privacy.
Verschil met de ISO27701: Bij de ISO27701 gaat het om de implementatie van een beheerssysteem, met de kenmerkende risicoanalyse, PDCA-cyclus en controls. Het privacy maturity model is een volwassenheidsmodel bedoeld om inzicht te krijgen in de huidige status en de kloof met de gewenste situatie.
De ISO27701 sluit aan bij de ISO27001 en daarom is de rol van informatiebeveiliging vrij groot. In het PMM is informatiebeveiliging ook opgenomen, maar speelt het een kleinere rol. Verder is er sprake van een redelijke grote overlap maar zijn er toch ook wel nuance verschillen. Bijvoorbeeld heeft de ISO27701 toestemming in twee controls opgenomen, terwijl het PMM zeven criteria heeft voor keuze en toestemming.
Op de ISO27701 kan gecertificeerd worden. Op het PMM kan een organisatie zich niet certificeren. De principes waarop het PMM is gebouwd komen wel terug in SOC2 audits.
Toegevoegde waarde van de combinatie: De ISO27701 (implementatie PIMS) en het PMM (meten volwassenheid) hebben beide een ander doel. De combinatie van beide raamwerken kan door de verschillen in uitwerking verwarrend zijn bij de implementatie. Daarom is de toegevoegde waarde onzes inziens in de praktijk beperkt.

Hoe ISO27701 in combinatie met andere raamwerken te gebruiken?

Wij onderkennen drie scenario's:

- Scenario 1: De organisatie heeft geen raamwerk in gebruik, noch voor privacy, noch voor informatiebeveiliging;
- Scenario 2: De organisatie is ISO27001 gecertificeerd;
- Scenario 3: De organisatie heeft al één of meer andere raamwerken in gebruik.

Scenario 1: de organisatie heeft geen raamwerk in gebruik, noch voor privacy, noch voor informatiebeveiliging

Als de organisatie nog geen raamwerken in gebruik heeft, kan de keuze voor ISO27701 verstandig zijn. De keuze voor een raamwerk (of combinatie van raamwerken) is fundamenteel en moet op boardroomniveau worden genomen; hij moet passend zijn voor de organisatie en haar stakeholders. Een belangrijk element is de mogelijkheid tot certificering, maar ook zaken als gebruikelijk in de branche (adoptiegraad) spelen een rol. Vanzelfsprekend geldt bij de keuze voor ISO27701 dat er ook een keuze gemaakt wordt voor ISO27001 in combinatie met ISO27002 omdat de ISO27701 een extensie is van de ISO27001.

Scenario 2: de organisatie gebruikt ISO27001

Als de organisatie reeds een managementsysteem heeft geïmplementeerd op basis van ISO27001 ligt het voor de hand om de ISO27701 aanvullend te gebruiken in verband met de overlap van het PIMS met het ISMS. Integratievoordelen zijn dan te behalen en de ISO-terminologie en structuur zijn éénduidig.

Scenario 3: de organisatie heeft al één of meer andere raamwerken in gebruik.

Gebruikt een organisatie een ander raamwerk (bijvoorbeeld de NIST suite) dan is het logisch om binnen de gehanteerde systematiek de beschikbare privacy uitbreidingen (indien beschikbaar) te gebruiken. ISO27701 ligt inhoudelijk dan minder voor de hand.

Gebruikt een organisatie de COBIT-systematiek dan kan via de ISACA Privacy Principles aansluiting met de vereisten vanuit de ISO27701 worden gezocht. Echter, als compliance moet worden aangetoond door certificering is ISO27701 bijna vereist. Afhankelijk van het in gebruik zijnde raamwerk kan de implementatie van ISO27701 wel (relatief) veel extra werk voor de organisatie betekenen omdat de ISO27001 ook geïmplementeerd moet worden.

Onze conclusie

De toegevoegde waarde van de ISO27701 hangt af van welke raamwerken bij een organisatie in gebruik zijn. In combinatie met de ISO27001 verwachten wij dat veel organisaties deze standaard hoogst waarschijnlijkheid in de volgende jaren gaan implementeren. Het grote voordeel is dan de mogelijkheid om het PIMS te integreren met het ISMS.

Bij organisaties die gebruik maken van andere standaarden zal de kernvraag zijn of certificering (richting klanten, leveranciers en overige stakeholders) noodzakelijk is. Zo ja, dan is de combinatie ISO27001/ISO27701 één van de weinige mogelijkheden. De ISACA-raamwerken als COBIT en de Privacy Principles zijn relatief eenvoudig met de ISO27701 te combineren, waardoor het extra werk zeer beperkt is.

De volgende papers

In onze derde paper gaan wij in op de implementatie van ISO27701, met daarin ook de integratie van ISMS en PIMS. Tevens hebben wij plannen voor een paper over de certificering op basis van ISO27701.

Contact

Voor vragen en opmerkingen kunt u contact opnemen met de focusgroep. Deze kunt u bereiken via ISO27701@gdpr.isaca.nl.

Over de ISACA-kennisgroep Privacy & GDPR

De kennisgroep Privacy & GDPR is onderdeel van ISACA Netherlands Chapter. De kennisgroep volgt de implementatie van de GDPR/AVG en van andere normatieve kaders op het gebied van bescherming van persoonsgegevens in de EU/EER, waarbij zij context en duiding verschaft rondom relevante, actuele ontwikkelingen en andere aspecten met betrekking tot deze kaders.
De kennisgroep bestaat uit ongeveer tien leden die allemaal werkzaam zijn in privacy, information security, governance en risk. Om de kennis te delen met de overige ISACA-leden organiseren we Round en Square Tables en schrijven we artikelen, discussion- en whitepapers. Binnen de kennisgroep is er een focusgroep die ontwikkelingen over de ISO27701 bijhoudt.
De focusgroep ISO27701, verantwoordelijk voor deze discussion paper, bestaat uit Jessica Maes, Harry van den Brink en Stephan van der Ende. Wij willen de Privacy & GDPR werkgroep bedanken voor hun inhoudelijke commentaar en aanvullingen.

Over de auteurs (ISACA-focusgroep ISO27701)

De ISACA-focusgroep ISO27701 is binnen de ISACA Netherlands Chapter onderdeel van de kennisgroep Privacy & GDPR. De focusgroep bestaat uit Jessica Maes, Harry van den Brink en Stephan van der Ende.

Drs. Ing. Jessica Maes CISA CIPP/E Lead Auditor ISO27001
Zelfstandig adviseur op het gebied van Information Security, Privacy, Risk en Compliance. Onder andere werkzaam geweest als privacy en security officer bij diverse organisaties.
Linkedin Profiel

Drs. Harry van den Brink RE CISM CRISC CDPSE Lead Auditor ISO27001 en ISO27701
Zelfstandig adviseur/programmamanager op het gebied van Information Security, Privacy, Risk en Compliance. Brengt bedrijven 'in control' over hun geautomatiseerde bedrijfsvoering. Namens ISACA lid van de NEN Werkgroep en Normcommissie inzake Privacy & Security.
Linkedin Profiel

Stephan van der Ende MScBA B ICT CISM CISA CRISC CISSP CIPP/E CIPM CIPT FIP
Privacy & security consultant bij Cegeka Consulting. Werkzaam geweest als privacy officer, security officer, consultant en projectmanager bij diverse organisaties. Naast de ISACA-focusgroep ook lid van de CIP-domeingroep Privacy.
Linkedin Profiel