Productcatalogus

Sinds het Amerikaanse AICPA in 1982 *Statement on Auditing Standards No. 44, Special-Purpose Reports on Internal Accounting Controls at Service Organizations* uitbracht, zijn er door diverse beroepsregelgevende instanties en standaardisatielichamen regels en protocollen gepubliceerd voor de uitvoering van TPM-onderzoeken. Een aantal hiervan wordt in dit overzichtsartikel behandeld.

Het meest vergaand gestandaardiseerd zijn de certificeringen op basis van een standaard van de International Organization for Standardization. Het voordeel van een dergelijk certificaat is dat het over de hele wereld dezelfde betekenis heeft, waardoor de gebruiker ervan overal weet hoe hij dit dient te interpreteren. Als bezwaar tegen de grote uniformiteit wordt wel genoemd dat het weinig recht doet aan de specifieke omstandigheden van elke organisatie en elke klant-leverancierrelatie. Ook wordt wel gesteld dat de diepgang van een ISO-onderzoek aan de beperkte kant is.
In dit artikel worden certificeringen op basis van ISO 9001 (quality systems) en ISO 17799 (code of practice for information security management) behandeld.

Wereldwijd ook gezaghebbend zijn de standaarden die door het Amerikaanse en Canadese accountantsberoep zijn uitgebracht voor de attestatie van websites (WebTrust) en informatiesystemen (SysTrust), inmiddels samengevoegd tot Trust Services. Een geslaagde attestatie resulteert in het verstrekken van een webzegel met bijbehorend rapport dat de opdrachtgever op zijn website mag plaatsen. Niet-Amerikaanse of niet-Canadese beroepsorganisaties kunnen in aanmerking komen voor een licentie om deze zegels ook te mogen verstrekken.

Een certificering met vooral een Europese betekenis is de certificering tegen de standaard van het European Telecommunication Standards Institute (ETSI) voor verstrekkers van digitale certificaten die kunnen worden gebruikt voor de elektronische handtekening.

SAS 44 is in 1992 vervangen door SAS 70, die in 1999 nog weer is aangepast op basis van SAS 88. Hoewel uitsluitend Amerikaanse CPA's aan deze standaard gehouden zijn, vindt toepassing ervan ook navolging buiten de Verenigde Staten. Het lijkt er zelfs op dat de Amerikaanse standaard internationaal meer bekendheid geniet dan de dienovereenkomstige en meer geëigende standaard van IFAC (ISA 402: Audit Considerations Relating to Entities Using Service Organizations). In dit artikel wordt stilgestaan bij SAS 70.

Voor het Nederlandse IT-auditberoep zijn vooral de attestatiehandleidingen van de NOREA van belang. In dit artikel wordt stilgestaan bij ZekeRE Business.

Voor privacy – met name op internet – bestaan wereldwijd talloze keurmerken, waaronder ook de eerdergenoemde Trust Services. In Nederland werkt het College Bescherming Persoonsgegevens samen met een aantal beroepsorganisaties hard aan een privacycertificaat. Verder kan in dit verband nog het privacykeurmerk van NOREA, ZekeRE Privacy, worden genoemd.

Tot slot zijn er talloze 'proprietary'-certificaten, webzegels en vergelijkbare uitingen van belangenorganisaties en andere not-for-profitorganisaties aan de ene kant en accountantskantoren en andere zakelijke dienstverleners aan de andere kant. Van deze categorie wordt in dit artikel het softwarecertificaat behandeld.

Bij de behandeling van bovengenoemde standaarden en richtlijnen is zoveel mogelijk het volgende stramien aangehouden:
* inleiding: introductie, korte typering, mate van toepassing;
* betrokken partijen: kenmerken serviceprovider, type dienst, afnemer, onderzoeker;
* onderzoek: object, normen aan het object, uitvoeringsnormen, aanpak;
* uitkomsten: verschijningsvorm van rapport, prijsindicatie, toegevoegde waarde voor serviceprovider en afnemer.

Achtereenvolgens komen zo aan bod:
* certificering op basis van NEN-EN-ISO 9001;
* certificering van informatiebeveiliging;
* Trust Services: WebTrust- en SysTrust-zegels;
* certificering van de elektronische handtekening;
* SAS 70;
* ZekeRE Business;
* privacycertificering;
* softwarecertificering.

Certificering op basis van NEN-EN-ISO 9001

Mw. drs. W.C.N. van Oeveren

Inleiding

De ontwikkelingen voor vele organisaties – zoals toenemende concurrentie, nieuwe aansprakelijkheidsregelingen, eisen ten aanzien van certificatie door de opdrachtgever, verhoogde tijdsdruk, internationalisering, grotere mondigheid van opdrachtgevers en een kritischer houding van medewerkers – vragen van het management een gewijzigde houding ten aanzien van de aansturing van de organisatie. Eén van de waarneembare reacties op deze ontwikkelingen is de toenemende populariteit van het kwaliteitsmanagementsysteem.

Primair doel van het kwaliteitsmanagementsysteem is zeker te stellen dat afspraken die worden gemaakt met de opdrachtgever, worden nagekomen. Klantgerichtheid staat centraal. Bij de inrichting van het systeem ligt de nadruk op procesbeheersing. Zij dient gericht te zijn op de beheersing van afbreukrisico's ten aanzien van de kernactiviteiten van de organisatie. Daartoe worden eenduidige afspraken gemaakt over het uitvoeren van de werkzaamheden.

Organisaties die kwaliteitszorg als managementfilosofie toepassen, herkennen de noodzaak tot veranderen eerder, aangezien de medewerkers gericht zijn op de klant met zijn veranderende eisen en wensen en zich bewust zijn van de veranderende omgeving. Door middel van het kwaliteitsmanagementsysteem wordt zeker gesteld dat de kwaliteit van de dienstverlening een structureel onderwerp op de agenda is en blijft. Het systeem dient nadrukkelijk gericht te zijn op het continu initiëren, implementeren en borgen van verbeteringen. Aangezien het (kwaliteits)beleid en de doelstellingen als sturingsinstrumenten dienen, is ook een duidelijk verband te leggen met bijvoorbeeld het ondernemingsplan.

De internationaal geldende norm NEN-EN-ISO 9001 biedt een praktisch handvat om te komen tot een goed functionerend kwaliteitsmanagementsysteem, dat is ingericht naar de wensen van de eigen organisatie. Deze norm is wereldwijd toepasbaar voor alle typen organisaties – zowel profit als non-profit – binnen alle branches. Veel organisaties integreren het kwaliteitszorgsysteem met andere zorgsystemen op het gebied van milieu, veiligheid, arbo en de administratieve procedures en internecontrolemaatregelen (AO/IC). Door het toepassen van de risicobenadering is tevens de relatie met de Code voor Informatiebeveiliging – BS 7799 – eenvoudig te leggen. Deze benadering maakt het mogelijk integrale controles uit te voeren, waardoor een breder zicht ontstaat op het functioneren van de organisatie als geheel.

Betrokken partijen

Een dergelijk kwaliteitsmanagementsysteem kan gecertificeerd worden tegen de norm NEN-EN-ISO 9001. Certificatie is de beoordeling van het kwaliteitsmanagementsysteem door een erkende instelling – welke is geaccrediteerd door de Raad voor Accreditatie – op basis van de ISO 9000-norm. De beoordeling wordt uitgevoerd door auditors die een erkende lead assessor-training hebben gevolgd. Het certificaat biedt naar derden een extra bevestiging dat de organisatie beschikt over een effectief systeem om aan de eisen van de opdrachtgever te voldoen. In verschillende branches wordt door opdrachtgevers vereist dat de leveranciers een ISO-certificaat hebben; hierbij valt te denken aan de automobielindustrie.

Onderzoek

De organisatie dient helder te omschrijven wat de scope is van het kwaliteitsmanagementsysteem. Deze scope wordt tijdens het certificatieonderzoek getoetst tegen de eisen van de norm NEN-EN-ISO 9001. Dit betekent dat alle activiteiten die van invloed zijn op het vastgestelde toepassingsgebied, tot het onderzoeksobject behoren.

Het onderzoek bestaat uit twee onderdelen, te weten het vooronderzoek en de implementatie-audit. Tijdens het vooronderzoek wordt het gedocumenteerde systeem getoetst aan de ISO-norm en worden de resultaten van de interne audits en de directiebeoordeling beoordeeld. Afwijkingen worden gerapporteerd en dienen te worden verholpen vóór de implementatie-audit.

Het vervolg is de implementatie-audit. Tijdens deze audit wordt getoetst of het gedocumenteerde systeem op effectieve wijze is ingevoerd. Dit gebeurt door middel van interviews en door het beoordelen van registraties. Centraal in het onderzoek staan de vragen of er aantoonbaar sprake is van een klantgerichte benadering en van een effectieve procesbeheersing. Ten tijde van het onderzoek dient er een functionerend kwaliteitsmanagementsysteem te zijn, waaruit blijkt dat de directie daadwerkelijk in staat is de organisatie naar verbeterde prestaties te leiden. Gedurende de auditdagen vindt een continue terugkoppeling plaats van de bevindingen.

Aan het einde van de implementatie-audit volgt een terugkoppeling van het auditteam. Of kan worden overgegaan tot het verstrekken van het certificaat, hangt af van de gevonden tekortkomingen. Indien er sprake is van zwaarwegende (kritieke) tekortkomingen, dan moeten deze eerst worden opgelost. Tijdens een extra audit – een follow-up, waarin alleen op de afwijkingen wordt ingegaan – wordt beoordeeld of effectieve maatregelen ter verbetering zijn genomen. Indien dit het geval is, kan worden overgegaan tot verlening van het certificaat. Zijn er geen zwaarwegende tekortkomingen, dan kan zonder aanvullend onderzoek worden overgegaan tot certificatie. Hiertoe zal het auditteam de organisatie voordragen voor certificatie. De feitelijke certificatiebeslissing wordt genomen door de certificatiecommissie van de betreffende certificerende instelling. Deze staat onafhankelijk van de auditor en toetst of het onderzoek conform de geldende procedures is uitgevoerd. Indien de beslissing positief is, kan worden overgegaan tot het verlenen van het certificaat.

Uitkomsten

Rapportage
Het certificatieonderzoek wordt afgesloten met een schriftelijke rapportage omtrent de bevindingen en het versturen van het ISO-certificaat. De rapportage vormt de basis voor het beoordelen van de ontwikkelingen en verbeteringen binnen het managementsysteem. Tevens geeft deze rapportage sturing aan de planning van de diverse auditfasen, zowel intern als extern.
Het certificaat kent een looptijd van drie jaar. Gedurende die periode wordt een aantal controleaudits uitgevoerd: de eerste na een half jaar, de tweede na twaalf maanden en de derde audit vierentwintig maanden ná verlening van het certificaat. Tijdens de controleaudits wordt beoordeeld of bij voortduring kan worden voldaan aan de kwaliteitsdoelstellingen – met name bij wijzigingen in de organisatie – en of de processen continu worden bewaakt en verbeterd. Tijdens de controleaudit wordt steeds een deel van het systeem beoordeeld. Het behoud van het certificaat is afhankelijk van de resultaten van deze controles. Indien sprake is van kritieke afwijkingen en er geen passende maatregelen worden genomen, kan worden overgegaan tot het intrekken van het certificaat.

Het behalen van een ISO 9001-certificaat bevordert de integriteit van het kwaliteitsmanagementsysteem.

Na drie jaar – dus na afloop van het certificaat – volgt een verlengingsonderzoek. Dit is in principe weer een volledige audit.

De kosten
Het aantal dagen dat wordt besteed, is afhankelijk van een aantal factoren. De belangrijkste zijn de omvang van de organisatie, het aantal vestigingen en de complexiteit van dienst of product. Indien offertes worden vergeleken, dient niet alleen te worden gekeken naar de initiële kosten maar ook naar de kosten over de certificatieperiode van drie jaar. Hierin kunnen aanmerkelijke verschillen zitten.

Toegevoegde waarde van het certificaat en van de externe audit
Het behalen van een ISO-certificaat kan het volgende aan het kwaliteitszorgprogramma toevoegen:
* Het werkt motiverend en stimulerend naar de medewerkers toe.
* Het bevordert de integriteit van het kwaliteitsmanagementsysteem.
* Het versterkt het imago van de organisatie in de markt. Het wordt gezien als een keurmerk en er is sprake van internationale acceptatie. Verder wordt het certificaat door veel bedrijven als marketing- en pr-tool gebruikt.

Externe auditors zijn in staat de organisatie als geheel te overzien en met een zogenaamde 'helikopterview' naar de processen te kijken. Daarnaast zijn externe auditors beter in staat een onafhankelijke positie in te nemen. Rapportages zijn dan ook gebaseerd op objectieve waarnemingen en worden niet beïnvloed door interne aangelegenheden. Tot slot kan de kennis – over het uitvoeren van doelmatige audits – worden overgedragen van de externe naar de interne auditors. Deze kennis kan door de medewerkers gebruikt worden bij het uitvoeren van de interne audits. Bovendien houden regelmatige audits het systeem actueel en levend.

Uit de ervaring van KPMG Certification blijkt dat veel organisaties een externe prikkel kunnen gebruiken om hun systemen actueel te houden en te werken aan continue verbetering van het systeem. De regelmatig terugkerende controleaudits dwingen een voortdurende aandacht voor het kwaliteitssysteem af.

Mw. drs. W.C.N. van Oeveren
is als lead auditor werkzaam bij KPMG Certification, waar zij zich bezighoudt met het beoordelen en controleren van kwaliteitssystemen op basis van de ISO 9000-normen.

vanoeveren.willeke@kpmg.nl

Certificering van informatiebeveiliging

Dr. ir. P.L. Overbeek RE

Certificatie van informatiebeveiliging – vertrouwen voor de organisatie zelf én haar partners

Er zijn organisaties die de informatiebeveiliging goed op peil hebben, en dat ook willen tonen aan relaties, klanten of de buitenwereld. Bij andere organisaties is informatiebeveiliging bijna op het gewenste niveau, maar is net een zetje extra nodig.
Voor deze situaties is certificatie van informatiebeveiliging een goed middel. Ter versterking van het vertrouwen tussen handelspartners onderling of tussen serviceproviders en hun klanten is het mogelijk een uitspraak over de informatiebeveiliging te onderbouwen met een certificaat. Dit certificaat is gebaseerd op de breed geaccepteerde standaard 'de Code voor Informatiebeveiliging' (ISO 17799 / BS 7799). Dit certificaat wordt door certificatie-instellingen afgegeven na uitvoering van een audit van het managementsysteem voor informatiebeveiliging door IT-auditors. Deze certificatie-instellingen zijn hiervoor erkend door de Raad voor Accreditatie. Hierdoor zijn de certificaten ook internationaal erkend.

De Code voor Informatiebeveiliging als basis voor certificatie

Waarom certificatie op basis van de Code
De Code voor Informatiebeveiliging is breed geaccepteerd als de leidraad voor het opzetten en implementeren

van informatiebeveiliging. Deze acceptatie geldt zowel binnen het bedrijfsleven als binnen de overheid, en zowel in Nederland als in de rest van de wereld.
Een certificaat geeft zowel binnen een organisatie als tussen organisaties meer vertrouwen in de opzet en het bestaan van het managementsysteem voor de informatiebeveiliging en het daadwerkelijk getroffen stelsel van maatregelen. Aangezien de Code uitgaat van een managementcyclus en het certificaat steunt op periodieke controleaudits kan men ook meer vertrouwen hebben dat het beoogde niveau van beveiliging ook *blijvend* wordt geboden.

De voordelen van certificatie tegen de Code
Met certificatie worden verschillende doelen gediend. In de eerste plaats kan door middel van certificatie op basis van de Code in eigen huis orde op zaken worden gesteld. Immers, 'opgaan' voor een certificaat creëert een objectieve interne doelstelling, met een duidelijk eindpunt: het certificaat. In de tweede plaats kan certificatie helpen bij het maken van afspraken tussen (handels)partners. Deze afspraken hebben vaak de vorm van service level agreements of interchange agreements bij electronic commerce. Een belangrijk onderdeel hiervan vormen de afspraken over informatiebeveiliging. Met een certificaat kan, bijvoorbeeld, een serviceprovider laten zien dat hij zich aan de gemaakte afspraken houdt. Certificatie biedt zo een vertrouwensbasis tussen partners, waarbij één certificaat vertrouwen kan bieden aan meerdere relaties.
Voor een serviceprovider kan het bijvoorbeeld zeer aantrekkelijk zijn om in een service level agreement de Code als uitgangspunt te nemen en, om aan te tonen dat dit uitgangspunt wordt gehaald, een certificaat tegen de Code te halen. Ook in andere overeenkomsten kunnen partijen afspreken dat ze zich aan de Code zullen houden en deze afspraak wederom onderbouwen met een certificaat.

Certificatie op basis van de Code voor Informatiebeveiliging is ook internationaal mogelijk. De certificaten zijn breed erkend. In de Angelsaksische landen is certificatie zelfs zeer gebruikelijk en veelal wordt een certificaat verwacht. In Amerika zijn de certificaten wel erkend, maar helaas nog niet zo ingeburgerd.

Certificatie van informatiebeveiliging: proces en betrokken partijen

De belangrijkste partij bij certificatie is de organisatie zelf! Deze zorgt ervoor dat er een beveiligingsplan ligt en is geïmplementeerd dat voldoet aan de Code. Indien de organisatie besluit 'op te gaan' voor het certificaat is de eerste stap in het certificatieproces de aanvraag tot certificatie. De organisatie stelt dan de 'Verklaring van Toepassing' op. De certificatie-instelling, die moet zijn erkend door de Raad voor Accreditatie, stelt een auditteam samen met auditors die ten minste vier jaar IT-ervaring hebben en ten minste twee jaar ervaring met informatiebeveiliging. Bovendien moeten de auditors aantoonbare auditervaring hebben. Hoewel de audit sterk leunt op de kennis en ervaring van de auditors, is de post-doctorale EDP-auditopleiding niet verplicht.

Dan volgt de documentatiebeoordeling. In dit onderzoek wordt vastgesteld of de verklaring en de bijbehorende documentatie voldoen aan de gestelde eisen uit deel 2 van de Code, met name de selectie van categorieën uit de Code met een verantwoording, doorgaans in de vorm van een risicoanalyse. Indien kritische afwijkingen worden vastgesteld, wordt de audit niet eerder voortgezet dan nadat deze zijn verholpen.

De volgende stap is de implementatiebeoordeling. Zoals gezegd zijn op dat punt door de organisatie en de certificatie-instelling in onderling overleg verschillende benaderingen te kiezen. Indien de organisatie een goede interne managementstructuur kent met goede interne controles, audits of zelfbeoordelingen, bestaat het grootste deel van het werk van de certificatie-instelling uit het beoordelen van deze werkzaamheden. Daarnaast zal de certificatie-instelling ook onafhankelijke waarnemingen uitvoeren (interviews en verwerven van 'evidence'). De verdeling van werkzaamheden tussen de organisatie en de certificatie-instelling is dus niet in beton gegoten, er zijn hier de nodige vrijheidsgraden. De laatste stap is de beslissing tot certificatie. Indien geen kritische afwijkingen zijn blijven bestaan en de onvermijdelijke tekortkomingen niet te ernstig zijn, kan het certificaat worden verleend. Bij de jaarlijkse controleaudit worden uiteraard met name de geconstateerde tekortkomingen opnieuw onder de loep genomen.

Met een certificaat wordt vertrouwen geboden dat de organisatie aan haar zorgplicht voldoet.

Tot slot: kosten en baten

Certificatie van informatiebeveiliging beoogt een stimulans te zijn voor de betreffende organisatie en haar medewerkers. Het inrichten van informatiebeveiliging vraagt vaak een ruime doorlooptijd. Maar zodra de organisatie het management rond informatiebeveiliging goed heeft ingericht, is de feitelijke certificatie laagdrempelig: eerder een kwestie van weken dan van maanden.

Op voorhand kan certificatie helpen 'orde in eigen huis' te scheppen: door te streven naar een certificaat wordt een duidelijk en meetbaar einddoel gesteld. Voor de partners en klanten van de organisatie wordt met een certificaat meer vertrouwen geboden dat de organisatie aan haar zorgplicht voldoet.

Dr. ir. P.L. Overbeek RE is director bij KPMG Information Risk Management en medeverantwoordelijk voor de dienstverlening van KPMG met betrekking tot Information Security Management. Hij is nauw betrokken bij de Code voor Informatiebeveiliging en één van de auteurs van de ITIL-module Security Management.

overbeek.paul@kpmg.nl

2003/3

Trust Services: WebTrust- en SysTrust-zegels

Mw. ir. L. Yap

Inleiding

De afgelopen jaren hebben de Amerikaanse en Canadese accountantsinstituten (AICPA en CICA) drie e-assurancediensten ontwikkeld voor het attesteren van IT-systemen: twee onder het label van WebTrust en één onder het SysTrust-label. Deze diensten kunnen leiden tot de uitgifte van een webzegel. SysTrust is ontwikkeld voor het attesteren van IT-systemen in het algemeen en WebTrust is bedoeld voor het attesteren van een IT-systeem in een e-commerceomgeving. De derde dienst, WebTrust voor *Certification Authorities*, is bedoeld voor het attesteren van dienstverleners op het gebied van digitale certificaten en digitale handtekeningen. WebTrust en SysTrust zijn inmiddels uitgegroeid tot internationale standaarden, maar het aantal uitgegeven zegels van deze diensten heeft de verwachting niet gehaald.

Ondanks de verschillen in aanpak en doelen adresseren WebTrust en SysTrust betrouwbaarheidsaspecten van IT-systemen. Mede om verwarring in de markt tegen te gaan hebben AICPA en CICA besloten de onderliggende programma's en normenkaders van WebTrust en SysTrust te harmoniseren tot 'Trust Services Principles and Criteria'. De twee verschillende producten met bijbehorende zegels en logo's blijven echter wel bestaan. Hoewel WebTrust langer bestaat dan SysTrust, is WebTrust in feite een specifieke toepassing van het SysTrust-raamwerk.

Door de specifieke vereisten van WebTrust voor *Certification Authorities* (CA's) zijn de normen betreffende CA's niet in de harmonisatie meegenomen en blijven zij dus als een apart normenkader met bijbehorend programma bestaan. De normen en kwaliteitsaspecten voor CA's zijn zo specifiek omdat zij zich richten op de betrouwbaarheid van digitale certificaten en digitale handtekeningen.

Betrokken partijen

De betrokken partijen bij een webzegelonderzoek zijn de verantwoordelijke partij, de gebruiker, de auditor en de opdrachtgever.

De verantwoordelijke partij (auditee) is de eigenaar van de online-dienst of het IT-systeem. Deze eigenaar is tevens de opdrachtgever. Het doel van de eigenaar is het vertrouwen van de markt te vergroten in de diensten die hij levert.

Het webzegel is, met bijbehorend rapport, publiekelijk toegankelijk op internet en dus openbaar.

Het typerende van een webzegel is dat het zegel (met bijbehorend rapport) publiekelijk toegankelijk is op internet en dus openbaar. De gebruikers (*relying parties*) zijn de deelnemers in het maatschappelijk verkeer die vertrouwen op het zegel dat wordt geassocieerd met de bijbehorende online-dienst. Voor de auditor is in deze situatie de gebruiker anoniem.

De auditor moet voldoen aan bepaalde kwalificaties. De auditor dient werkzaam te zijn bij een door WebTrust of SysTrust geaccrediteerde organisatie. In beginsel moet de auditor in het bezit zijn van een beroepskwalificatie, zoals een CPA-licentie van de Verenigde Staten of Canada. NIVRA heeft met het AICPA/CICA een licentieregeling getroffen voor Nederlandse accountantskantoren. Andere gebieden waarvan de accountants soortgelijke regelingen hebben getroffen voor WebTrust, zijn Australië, Argentinië, Denemarken, Engeland, Frankrijk, Hongkong, Italië, Schotland, Spanje en Wales.

Onderzoek

Het zegel wordt door de gekwalificeerde auditor verstrekt op basis van een assuranceopdracht, waarop internationale standaarden, zoals de International Standard on Assurance Engagements (ISAE 100), van toepassing zijn. De mate van zekerheid die het zegel (met bijbehorend rapport) biedt is dezelfde als die van een accountantsverklaring.

Het onderzoek kan betrekking hebben op één of meer kwaliteitsaspecten van de getroffen maatregelen van een website (*subject matter*) of op een bewering van het management van de organisatie over de betreffende website (*management assertion*). De keuze van de rapportagevorm heeft geen grote gevolgen voor de uitvoering van het onderzoek. Het management is altijd verplicht een formele verantwoording te verstrekken aan de auditor. Aanbevolen wordt om deze verantwoording of managementbewering openbaar te maken (bijvoorbeeld via de betreffende website).

Het AICPA en het CICA hebben gezamenlijk normen (of *criteria*) ontwikkeld waaraan het onderzoeksobject dient te voldoen ([AICP03]). Deze normen zijn volledig en dwingend. Het normenkader onderscheidt de volgende kwaliteitsaspecten (of *principles*): *security, availability, processing integrity, online privacy* en *confidentiality*. Per kwaliteitsaspect zijn de normen onderverdeeld in vier gebieden: *policies*, *communications*, *procedures* en *monitoring*. Hoewel de normen volledig en dwingend zijn, zijn deze vaak niet concreet genoeg om als basis te dienen voor een onderzoek. Daarom worden voor elke norm een aantal gedetailleerde voorbeeldmaatregelen opgesomd. Voor elke norm dient de auditor een overweging te maken of het object gezien de risico's in de betreffende situatie voldoet aan de norm.
De reikwijdte van het onderzoek betreft altijd minimaal opzet en bestaan (van bijvoorbeeld de beveiligingsmaatregelen). Indien de auditor het onderzoek in een periode herhaaldelijk heeft uitgevoerd, is het behalve over opzet en bestaan ook mogelijk een oordeel te geven over de werking.

Een zegel mag een beperkte tijd worden gevoerd. Onder normale omstandigheden is de maximale herhalingsfrequentie van het onderzoek elke twaalf maanden. Om het zegel op de website te behouden moet het onderzoek zijn afgerond met uiteraard een goedkeurend oordeel.

Uitkomsten

Bij een zegel hoort altijd een rapport, dat de gebruiker kan zien door op het zegel te klikken. Dit gebruikersrapport bestaat doorgaans uit één pagina en bevat minimaal de volgende onderwerpen:
- object van onderzoek;
- verwijzing naar managementbewering (indien van toepassing);
- datum of periode van onderzoek;
- verwijzing naar gehanteerde normen;
- verantwoordelijkheden van de auditee en van de auditor;
- door de auditor gehanteerde (onderzoeks)standaarden;
- inherente risico's;
- oordeel;
- ondertekening.

Naast het gebruikersrapport dat op internet wordt gepubliceerd, is het gebruikelijk voor de verantwoordelijke partij of opdrachtgever een uitgebreider rapport op te stellen met gedetailleerde bevindingen en aanbevelingen.

De afweging van de opdrachtgever of de kosten opwegen tegen het gewonnen vertrouwen is vooraf moeilijk te kwantificeren. Dit vertrouwen zal enerzijds bestaan uit het vertrouwen van de gebruikers in het zegel (de markt) en anderzijds het verhoogde vertrouwen van de eigenaar in zijn eigen systeem of dienstverlening. Hoe onbekender de merknaam van de organisatie in de markt is, hoe groter de toegevoegde waarde van een webzegel zal zijn.

Bronnen

[AICP03]
AICPA/CICA, *Suitable Trust Services Criteria and Illustrations for Security, Availability, Processing Integrity, Online Privacy, and Confidentiality* (Including WebTrust and SysTrust), 2003, www.aicpa.org

[Keij02]
Suzanne Keijl, *SAS 70 en SysTrust, Internationale standaarden voor third party assurance bij IT-serviceorganisaties*, de EDP-Auditor, nummer 3, 2002.

www.webtrust.org/

www.systrustservices.com/

Mw. ir. L. Yap
is werkzaam bij KPMG Information Risk Management en is gespecialiseerd in de beheersing en beveiliging van internettoepassingen. Zij heeft hierbij op het gebied van e-assurance bijzonder veel praktijkervaring opgedaan in verschillende industriesectoren.

yap.lidwien@kpmg.nl

Certificering van de elektronische handtekening?

Drs. P.A. van Walsem

Inleiding

In deze bijdrage wordt een specifiek onderzoek belicht, namelijk het certificeren van een organisatie die digitale certificaten uitgeeft en beheert en waarvan het beheer- en uitgifteproces wordt getoetst aan de eisen die staan verwoord in de Europese richtlijn elektronische handtekening en de hiervan afgeleide Nederlandse Wet elektronische handtekening.

Op het internet kunnen partijen zich anders voordoen dan ze in werkelijkheid zijn. Met behulp van een digitaal certificaat kan een gedeelte van deze problematiek worden verholpen. Door middel van een digitaal certificaat kan zekerheid worden verkregen omtrent de identiteit van een organisatie of natuurlijk persoon. Een organisatie die digitale certificaten uitgeeft waarmee een elektronische handtekening kan worden gezet, wordt ook wel een Certification Service Provider (CSP) genoemd. Organisaties die dergelijke digitale certificaten uitgeven, kunnen zich laten certificeren. Hierdoor genereren ze vertrouwen naar eventuele afnemers van digitale certificaten en kunnen ze zich op een eenvoudige wijze laten registreren bij de Nederlandse overheid (OPTA) als een organisatie die digitale certificaten conform de Wet elektronische handtekening uitgeeft, genereert en beheert. Indien zij niet over een dergelijk conformiteitscertificaat beschikken wordt het registratieproces bij de OPTA verzwaard door aanvullende onderzoeken en een extra geldelijke bijdrage.

ECP.nl, de organisatie die is opgericht om elektronische handel binnen Nederland te stimuleren, heeft een certificeringsschema (TTP.nl-schema) opgesteld. Dit certificeringsschema hanteert de Europese richtlijn elektronische handtekening[1] als grondslag en het ETSI TS 101456[2]-normenkader als basisnormenkader. Een TTP.nl-certificeringsonderzoek wordt zowel nationaal als internationaal (binnen Europa) uitgevoerd. KPMG heeft in 2002 het allereerste TTP.nl-certificeringsonderzoek in Nederland uitgevoerd.

Betrokken partijen

In het ETSI TS 101456-normenkader wordt een onderscheid gemaakt tussen een digitaal certificaat waarbij gebruik wordt gemaakt van een zogenaamd Secure Signature Creation Device (SSCD) en een digitaal certificaat waarbij geen gebruik van een SSCD wordt gemaakt. Indien er gebruik wordt gemaakt van een SSCD, staan de digitale certificaten op een smartcard.

De vereisten in ETSI TS 101456 zijn geschreven voor een aantal specifieke diensten, en wel: registration service,

1) Richtlijn 1999/93/EG van het Europees Parlement en de Raad van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen.
2) Het ETSI TS 101456-normenkader is opgesteld door het European Telecommunication Standards Institute (ETSI). De laatste versie is van april 2002. TS staat voor technical specification.

certificate generation service, dissemination service, revocation management service, revocation status service en subject device provision service. Functies als time-stamping, attribute certificaten en vertrouwelijkheidsdiensten liggen buiten de scope van het document. Dit betekent dat deze onderdelen tijdens een certificatieonderzoek niet worden beoordeeld.

Bij een TTP.nl-certificering zijn drie partijen betrokken, namelijk:
- Certification Service Provider (CSP);
- certificerende instelling;
- gebruiker.

De Certification Service Provider
De Certification Service Provider is opdrachtgever van het onderzoek. Deze organisatie heeft een Public Key Infrastructure geïmplementeerd waarmee de digitale certificaten worden gegenereerd en beheerd. Randvoorwaarde voor de uitvoering van het onderzoek is dat de CSP een Certificate Policy en een Certification Practice Statement heeft opgesteld. Dit zijn documenten waarin de CSP beschrijft aan welke eisen zijn diensten voldoen en welke maatregelen hij hiervoor heeft geïmplementeerd. Daarnaast moet de CSP een verklaring van toepasselijkheid invullen. In deze verklaring wordt door de CSP aangegeven voor welke certification service hij wil worden gecertificeerd.

Het conformiteitscertificaat biedt de zekerheid dat een elektronische handtekening gelijke rechtskracht bezit als de gewone handtekening.

De certificerende instelling
De organisatie die het certificeringsonderzoek gaat uitvoeren, moet geaccrediteerd zijn door de Raad voor Accreditatie. Accreditatie vindt plaats tegen de EN 45011-norm (productcertificering). Na accreditatie heeft de certificerende instelling de mogelijkheid om een conformiteitscertificaat uit te reiken aan een CSP. Accreditatievoorwaarden zijn onder andere het hebben van kennis over het normenkader ETSI TS 101456 en het hebben van ervaring met het beoordelen van managementsystemen. Daarnaast moet de certificerende instelling IT-auditors in dienst hebben die ten minste vier jaar praktijkervaring hebben op het auditgebied, en ruime kennis en ervaring hebben met het normenkader ETSI TS 101456.

De gebruiker
Afnemers van het conformiteitscertificaat zijn onder andere overheidsorganisaties zoals ministeries, zelfstandige bestuursorganen (ZBO's), provincies en lokale gemeenten. Om digitale certificaten te hanteren als elektronische handtekening binnen de overheid heeft de overheid als randvoorwaarde gesteld dat deze van een gecertificeerde en bij de OPTA geregistreerde CSP afkomstig moeten zijn. Daarnaast steunen particulieren, middenstanders en bedrijven op het conformiteitscertificaat. Het verschaft vertrouwen in de kwaliteit van het digitale certificaat en geeft zekerheid dat indien zich een dispuut voordoet, het gebruik van een digitaal certificaat afkomstig van een gecertificeerde CSP niet in een rechtbank mag worden geweigerd en dezelfde rechtskracht heeft als een normale handtekening.

Onderzoek

De stappen die in een TTP.nl-certificeringsonderzoek worden doorlopen, zijn:
- *Uitvoeren van een proefbeoordeling*. De proefbeoordeling is optioneel en dus niet verplicht. Door middel van de proefaudit kan worden bepaald of de CSP klaar is voor certificatie. De proefaudit staat los van het certificatieonderzoek. Indien er sprake is van een negatief resultaat heeft dit op zichzelf geen gevolgen voor het formele certificatietraject.
- *Documentatieonderzoek*. De certificerende instelling toetst of de documentatie voldoet aan de eisen die staan vermeld in ETSI TS 101456. Indien zich een materiële afwijking van de norm voordoet (een zogenaamde non-conformiteit), dient de CSP deze op te lossen voordat het implementatieonderzoek kan plaatsvinden.
- *Implementatieonderzoek*. Het implementatieonderzoek dient te worden uitgevoerd volgens de eisen zoals verwoord in ISO 10011 'guidelines for auditing quality systems' en beslaat het grootste deel van de activiteiten. De CSP toont in deze fase aan dat de norm, zoals beschreven in het ETSI TS 101456, in voldoende mate is geïmplementeerd.
- *Rapportage en uitreiking van het certificaat*. De certificerende instelling rondt de eindrapportage af, en gaat indien geen non-conformiteiten zijn gesignaleerd, over tot uitreiking van het certificaat.
- *Uitvoeren van controleaudits*. Voor de komende drie jaar voert de certificerende instelling controleaudits uit om te toetsen in hoeverre de CSP-dienstverlening voldoet aan de eisen zoals verwoord in het document ETSI TS 101456. Indien zich non-conformiteiten voordoen zal de certificerende instelling het uitgereikte certificaat intrekken.

Uitkomsten

Resultaat van een TTP.nl-certificering is een conformiteitscertificaat. Het conformiteitscertificaat biedt de gebruiker de zekerheid dat de organisatorische structuur, verantwoordelijkheden, procedures, processen en voorzieningen voor het ten uitvoer brengen van de uitgifte van gekwalificeerde certificaten voldoet aan ETSI TS 101456. Daarnaast biedt het de gebruiker de zekerheid dat een elektronische handtekening die geplaatst is met een digitaal certificaat afkomstig van een CSP die gecertificeerd is tegen ETSI TS 101456, overeenkomstig is aan de Wet elektronische handtekening en hierdoor een gelijke rechtskracht bezit als de gewone handtekening.

Drs. P.A. van Walsem is werkzaam bij KPMG Information Risk Management en houdt zich als IT-auditor bezig met het uitvoeren en managen van complexe IT-auditopdrachten en het geven van advies over het implementeren van complexe informatiesystemen, zoals een PKI.

vanwalsem.peter@kpmg.nl

SAS 70

Drs. R.P. Schouten RE RA en drs. M.A. Francken RA

Inleiding

Diverse ondernemingen hebben bepaalde activiteiten uitbesteed aan een serviceorganisatie, zoals een Application Service Provider, een fund-administratiekantoor of een vermogensbeheerder. Indien de uitbesteding van materiële invloed is op de financiële verslaggeving, zal de accountant die belast is met de jaarrekeningcontrole van de uitbestedende onderneming, controlezekerheid moeten krijgen over de interne beheersingsstructuur bij de serviceorganisatie.

Het American Institute of Certified Public Accountants (AICPA) heeft hiertoe de 'Statement on Auditing Standards' (SAS) nummer 70, 'Reports on the processing of Transactions by Service Organisations' ontwikkeld. Deze richtlijn maakt deel uit van AU section 324 'Service Organisations'. SAS 70 is een algemeen geaccepteerde richtlijn, die erop neerkomt dat een serviceorganisatie haar interne beheersingsstructuur laat beoordelen door een onafhankelijke auditor. Deze beoordeling kan eveneens vanuit het perspectief van de userorganisatie worden toegepast. SAS 70 stelt de serviceorganisatie in staat het niveau van de interne beheersing te tonen; niet alleen aan de controlerend accountant van de organisatie die uitbesteedt, maar ook aan (potentiële) klanten.

Betrokken partijen

In een SAS 70-audit zijn de volgende partijen betrokken: 'userorganisatie' en haar 'userauditor' ten opzichte van de 'serviceorganisatie' en haar 'serviceauditor'. Het SAS 70-onderzoek, en hiermee vergelijkbare onderzoeken, worden binnen Nederland relatief veel toegepast in de financiële dienstverleningssector. De serviceauditor is de partij die uiteindelijk een 'audit opinion' afgeeft bij het, door het management opgestelde, SAS 70-achtige rapport, waarin de interne beheersingsstructuur op een gedetailleerde wijze is beschreven. Doorgaans wordt het rapport, inclusief de verklaring, beschikbaar gesteld aan mogelijke 'prospects'. In onderling overleg tussen de userorganisatie en de serviceorganisatie worden de rapporten, in de Nederlandse situatie, beschikbaar gesteld aan de toezichthouder(s).

De opdracht voor het SAS 70-onderzoek kan worden verstrekt door de userorganisatie of de serviceorganisatie. De userorganisatie kan de opdracht geven aan de serviceorganisatie om een dergelijk onderzoek te laten uitvoeren, gezien haar eindverantwoordelijkheid voor de betreffende transacties. Daarnaast is er, met de komst van de Sarbanes-Oxley regelgeving, corporate governance-regels en regelgeving door toezichthouders (Richtlijn Organisatie en Beheer van DNB, uitbestedingsrichtlijn van de PVK), sprake van een verhoogde behoefte om zekerheid te verkrijgen inzake de betrouwbaarheid van de uitbestede activiteiten.

Onderzoek

SAS 70 is van toepassing op onderzoeken in het kader van een financial audit, die worden uitgevoerd ten behoeve van de accountant van een userorganisatie. Deze accountant heeft als object van onderzoek de jaarrekening van de userorganisatie en zal willen weten wat de controlerisico's zijn inzake de beheersing van de relevante processen door de serviceorganisatie.

Opzet, bestaan en werking
Het SAS 70-onderzoek richt zich op de opzet en het bestaan van de betreffende beheersingsmaatregelen van de serviceorganisatie, maar kan tevens gericht zijn op de werking. In SAS 70 worden twee soorten van onderzoek beschreven:

1. *Policies and procedures placed in operation (Type I-onderzoeken).*
   Dit type onderzoek geeft de gebruiker inzicht in de opzet en het bestaan van de beheersingsmaatregelen bij de serviceorganisatie, maar geeft geen evidence over de werking van de beheersingsmaatregelen.
2. *Policies and procedures placed in operation and tests of operating effectiveness (Type II-onderzoeken).*
   Bij dit type onderzoek wordt tevens de voldoende effectieve werking van gedefinieerde maatregelen getest, uitgaande van een hoge mate van zekerheid.

Er is sprake van een verhoogde behoefte om zekerheid te verkrijgen inzake de betrouwbaarheid van de uitbestede activiteiten.

Normen
De SAS 70-richtlijn geeft geen kwaliteitseisen; het is aan de opdrachtgever om in samenspraak met de serviceorganisatie en de auditor de gepaste normenset op te stellen. De normen zelf kunnen afkomstig zijn van de organisatie die wordt beoordeeld, de serviceorganisatie of de auditor waarvoor de audit plaatsvindt, een toezichthoudende instantie of een andere bron. Voor het beoordelen c.q. vaststellen van de normen zijn diverse normenkaders voorhanden, zoals:

- Code voor Informatiebeveiliging van het Nederlands Normalisatie Instituut (NNI);
- Information Technology Infrastructure Library van de Central Computer & Telecommunications Agency (CCTA);
- ISO 9000-9004 van de International Organization for Standardization (ISO).

Het SAS 70-onderzoek zal meermalen per jaar kunnen worden uitgevoerd, afhankelijk van de benodigde diepgang van het onderzoek en de specifieke situatie bij de serviceorganisatie.

Rapportage

SAS 70 geeft gedetailleerde voorschriften voor de inrichting en bewoordingen van de verklaring van de serviceauditor. Zo verklaart hij, met een redelijke mate van zekerheid en rekening houdend met de materialiteit, dat de beschreven beheersingsmaatregelen ('uit de bijlage') de relevante aspecten afdekken voor de beheersingsorganisatie van een userorganisatie. Daarnaast geeft hij aan dat de beheersingsmaatregelen in opzet geschikt zijn om, met een redelijke mate van zekerheid, de specifieke controledoelstellingen te realiseren, indien de beschreven beheersingsmaatregelen ('uit de bijlage') worden nageleefd. Indien tevens de werking wordt beoordeeld, zal de serviceauditor aangeven welke tests zijn uitgevoerd in relatie tot de controledoelstellingen en wat de uitkomsten hiervan waren.

De uitkomsten van de audit zijn vastgelegd in de bijlage, in de vorm van een onderzoeksmatrix. Per kwaliteitseis en daarbinnen per beheersingsmaatregel is aangegeven met welke diepgang en frequentie de beheersingsmaatregel is getoetst en wat de bevindingen naar aanleiding van de toetsing zijn. De rapportage is in principe voor alle gebruikers dezelfde.

Richtprijs en toegevoegde waarde

SAS 70 laat zeer weinig ruimte om een beperkte audit uit te voeren. Er zal een full scope audit moeten worden uitgevoerd, die vaak kostbaar is. Echter, voor de serviceorganisatie zijn significante voordelen te behalen doordat zij niet meer wordt belast met een veelheid van userauditors. Een serviceorganisatie heeft te maken met een veelheid van userauditors met elk hun eigen wens om zekerheid te verkrijgen over de effectiviteit bij de serviceorganisatie. Zonder een dergelijk rapport zou een serviceorganisatie al deze userauditors langs krijgen, hetgeen een kostbare zaak is. Richting de klanten van een serviceorganisatie kan ook veel waarde worden toegevoegd door aan te tonen dat de interne beheersing adequaat is. Een klant en diens accountant kunnen zekerheid c.q. vertrouwen ontlenen aan het rapport.

Ook aan de kant van de userorganisatie is voordeel te behalen doordat de userauditor geen additionele werkzaamheden hoeft uit te voeren.

Drs. R.P. Schouten RE RA is werkzaam als IT Audit Manager bij KPMG Information Risk Management en heeft zich gespecialiseerd in het bank- en verzekeringswezen.

schouten.rob@kpmg.nl

Drs. M.A. Francken RA houdt zich als manager bij KPMG Information Risk Management onder andere bezig met IT-audits ter ondersteuning van de jaarrekeningcontrole, projectaudits en Business Process Analysis-trajecten.

francken.marco@kpmg.nl

ZekeRE Business[1]

Drs. K.H.G.J.M. Ho RE RA

Inleiding

Bij business-to-business handel via internet (e-B2B) is het vertrouwen in de elektronische handelspartner van groot belang, niet alleen qua organisatie, maar zeker ook qua techniek. Vertrouwen dient enerzijds te worden verdiend en anderzijds door waarborgen te zijn omgeven, waardoor dit vertrouwen gehandhaafd blijft. De NOREA, de beroepsorganisatie van gekwalificeerde IT-auditors in Nederland, heeft op deze behoefte aan vertrouwen ingespeeld door de ontwikkeling van het certificeringsproduct ZekeRE Business.

Dit product heeft als doel de gekwalificeerde IT-auditor en diens opdrachtgever een handvat te bieden om in een aantal stappen na te gaan of en zo ja, in welke mate het gebruik van internet in een bepaald bedrijfsproces als 'veilig'[2] kan worden beschouwd dan wel kan worden gemaakt. ZekeRE Business is gericht op Nederland en tot op heden is slechts een beperkt aantal certificaten uitgereikt.

Betrokken partijen

ZekeRE Business beoogt een antwoord te zijn op een behoefte van managers aan steun en zekerheid wanneer zij internet gebruiken of willen gaan gebruiken in een bedrijfsproces dat is gericht op e-B2B (zowel handel als zakelijke dienstverlening). Bij de ontwikkeling van ZekeRE Business was het doel immers het verantwoordelijke management een goede 'nachTrust' te geven. De primaire gebruiker van ZekeRE Business en tevens opdrachtgever is dus het verantwoordelijke management van de e-B2B-toepassing.

Onder voorwaarden kan ook een openbaar certificaat worden afgegeven om op de internetsite van de e-B2B-toepassing te plaatsen. Hierdoor kan ook vertrouwen worden gegeven aan de e-B2B-handelspartners van de opdrachtgever. Een certificaat kan worden afgegeven door iedere organisatie, indien de eindverantwoordelijkheid voor het certificeringstraject bij een gekwalificeerde IT-auditor (RE) ligt.

In feite kan worden gesteld dat, indien de ZekeRE Business-mededeling niet aan derden wordt verstrekt en er geen openbaar certificaat wordt afgegeven, dit onderzoek is te classificeren als een adviesopdracht. Immers, voor een assuranceopdracht zijn drie partijen een vereiste, te weten de serviceprovider (in dit geval de opdrachtgever), de auditor en de gebruiker van de mededeling (zijnde niet de serviceprovider zelf). In het artikel van Van Langen elders in deze Compact, dat mede is gebaseerd op het auditframework 'International Standard on Auditing 100' van de International Federation of Accountants ([IFAC00]), wordt deze zienswijze verder toegelicht.

1) Dit artikel is in hoge mate gebaseerd op de handleiding ZekeRE-business van de NOREA ([NORE01]).

2) De NOREA verstaat onder het begrip veilig het ruime scala van kwaliteitsaspecten, zoals integriteit, exclusiviteit en continuïteit.

Onderzoek

De scope van ZekeRE Business beslaat alle beheermaatregelen die in het kader van het te auditen e-businessproces (zullen) zijn getroffen. Hiertoe behoren alle technologische en organisatorische maatregelen die invloed hebben op de veilige werking van het e-businessproces en dus op de zekerheid die de opdrachtgever aan zijn businesspartners kan bieden. Indien procesonderdelen zijn uitbesteed aan andere organisaties, dan behoren ook deze subprocessen tot de scope van de audit. De door de IT-auditor uit te voeren audit heeft onder andere betrekking op:

- het e-businessproces en de daarbijbehorende informatiesystemen;
- de relatie met de internetserviceprovider, inclusief het communicatietraject.

Aan de opdrachtgever wordt voorafgaand aan de ZekeRE Business-audit een beleidsdocument gevraagd waarin ten minste de volgende zes aandachtsgebieden dienen te zijn uitgewerkt: contentmanagement, infrastructuur, berichtenverkeer, transacties, logistieke organisatie en financiële organisatie.

Vervolgens wordt in samenspraak met de opdrachtgever het e-businessprofiel vastgesteld. Deze classificatie beoogt een kader te scheppen voor de beoordeling van de specifieke risico's en het gewenste veiligheidsniveau dat is afgestemd op de aard van de onderneming. De e-businessprofielen die worden onderscheiden, zijn:

- *Aanvullend*. E-business is een aanvulling op of uitbreiding van de dienstverlening. Beveiliging en inperking van risico's zijn impliciet wettelijk vereist. De opdrachtgever treedt op als *goed huisvader*.
- *Belangrijk*. E-business is van strategisch belang. Het beveiligingsniveau zal dus aan strengere eisen moeten voldoen.
- *Essentieel*. E-business van de organisatie heeft maatschappelijke impact. Schending van de beveiliging heeft dan ook maatschappelijke gevolgen.

Zoals in de *Handleiding ZekeRE-business* is beschreven, geeft *goed huisvaderschap* de ondergrens aan van de zorgvuldigheidsnorm: er kan pas sprake zijn van goed huisvaderschap als aan de wettelijke eisen is voldaan, zoals de Wet bescherming persoonsgegevens (Wbp). De meeste organisaties vallen dus in de categorie 'Aanvullend'. Slechts een beperkt aantal organisaties valt in de categorie 'Belangrijk'. Dit betreft organisaties die geen alternatieven hebben voor het gebruik van internet in hun bedrijfsproces. Hierbij kan worden gedacht aan webwinkels en pure internetbanken. In de categorie 'Essentieel' zijn slechts zeer weinig organisaties te classificeren. Immers, de maatschappelijke gevolgen van schending van de beveiliging zijn voor vrijwel alle organisaties beperkt. Een voorbeeld van een (in Nederland nog niet bestaande) organisatie waarbij die gevolgen wel zijn voor te stellen, is de (overheids)organisatie die het stemmen via internet exploiteert.

De scope van ZekeRE Business beslaat alle beheermaatregelen die in het kader van het te auditen e-businessproces (zullen) zijn getroffen.

De NOREA stelt in de ZekeRE Business-productbeschrijving een doelstellingenmatrix beschikbaar, bestaande uit enerzijds normen onderverdeeld in de genoemde zes aandachtsgebieden en anderzijds per norm de veiligheidscriteria die relevant zijn (exclusiviteit, integriteit, authenticiteit, onweerlegbaarheid, continuïteit en controleerbaarheid). Op basis van deze doelstellingenmatrix en het vastgestelde e-businessprofiel stelt de IT-auditor samen met de opdrachtgever de ZekeRE Business-normen vast waaraan het e-businessproces moet voldoen. Vervolgens voert de IT-auditor de audit uit en bepaalt op basis van professional judgement of het samenstel van getroffen beheermaatregelen gedurende de verslagperiode in opzet, bestaan en werking heeft voldaan aan de vastgestelde ZekeRE Business-normen.

Uitkomsten

Ter afsluiting van de ZekeRE Business-audit[3] zal aan de opdrachtgever worden gerapporteerd. Deze rapportage bevat de gehanteerde normen, de bevindingen en – met een redelijke mate van zekerheid – het oordeel over de mate waarin opzet, bestaan en werking van de getroffen beheermaatregelen met betrekking tot het e-businessproces gedurende de verslagperiode hebben voldaan aan de vastgestelde ZekeRE Business-normen.

Indien de opdrachtgever dat wil, kan onder voorwaarden een ZekeRE Business-certificaat worden afgegeven. Dit certificaat is openbaar en wordt door de NOREA geregistreerd. De NOREA kent aan het certificaat een geldigheidsduur toe en heeft die gesteld op zes maanden vanaf het einde van de verslagperiode. Organisaties en de stand van de techniek zijn immers continu aan verandering onderhevig, waardoor herhaling van de audit elke zes maanden noodzakelijk is.

Literatuur

[ISAC03]
Information Systems Audit and Control Association & Foundation (ISACA), *IS Auditing Guideline Reporting 070.010*, oktober 2002.

[NORE01]
Nederlandse Orde van Register EDP-auditors (NOREA), *Handleiding ZekeRE-business*, januari 2001.

3) In de ZekeRE Business-productbeschrijving, die op de NOREA-website beschikbaar is gesteld, is de aanpak uitgebreid beschreven. In deze beschrijving is ook informatie opgenomen over het certificaat en de administratiekosten die hierover aan de NOREA verschuldigd zijn.

Drs. K.H.G.J.M. Ho RE RA
is werkzaam als senior manager bij KPMG Information Risk Management. Hij heeft zich de afgelopen jaren primair beziggehouden met advisering en auditing op het gebied van planning en beheersing van IT-projecten, kwaliteit van systeemontwikkeling en beheer van rekencentra. Daarnaast houdt de heer Ho zich bezig met het verder ontwikkelen van de IRM-dienstverlening die leidt tot third-party-mededelingen. Verder is hij als vaktechnisch coördinator betrokken bij de postdoctorale EDP-Audit Opleiding van de Vrije Universiteit te Amsterdam.

ho.kaihang@kpmg.nl

2003/3

Privacycertificering

Mw. drs. L. Hoogeveen en drs. H.G.Th. van Gils RE RA

Inleiding

Na jarenlange voorbereiding is in september 2001 in Nederland de Wet bescherming persoonsgegevens (Wbp) officieel van kracht geworden. Na een overgangstermijn van een jaar moeten (vrijwel) alle organisaties in Nederland voldoen aan de eisen die de Wbp stelt ten aanzien van verwerkingen van persoonsgegevens. Persoonsgegevens zijn gegevens die betrekking hebben op natuurlijke en identificeerbare personen.

Naast de wettelijke sancties voor het zich niet houden aan de privacywet kan een organisatie ook bedrijfsschade oplopen in het geval zij niet voldoet aan de privacywetgeving. Misstappen op dit gebied kunnen voor een organisatie immers leiden tot negatieve publiciteit, geschonden vertrouwen, verlies van marktaandeel en civielrechtelijke schadeclaims.

Als gevolg van de toenemende mate van elektronische beschikbaarheid van een grote hoeveelheid persoonlijke gegevens en de toenemende technische mogelijkheden om op relatief eenvoudige wijze koppelingen tussen geautomatiseerde gegevensbestanden te realiseren is er begrijpelijkerwijs een maatschappelijke onrust over wat er met die persoonsgegevens allemaal achter de rug van de betrokkene om gebeurt. Door koppeling van gegevensbestanden worden de herkomst en het gebruik van gegevens nog moeilijker te traceren. Op deze wijze kunnen de persoonsgegevens die op het eerste oog relatief onschuldig zijn, een andere betekenis krijgen.

Daarom ontstaat er bij organisaties, waaronder zeker de overheid geschaard kan worden, soms de behoefte expliciet naar de markt toe duidelijk te maken dat zij in ieder geval goed omgaan met de bescherming van de bij hen aanwezige persoonsgegevens. Het kunnen overleggen van een 'bewijs van goed gedrag' zou daarbij zeer behulpzaam kunnen zijn.

Tabel 1. Overzicht diepgang productenset.

Behoefte/diepgang	Productenset
Globale indruk	Quickscan
Interne meting	Wbp Zelfevaluatie
Interne meting + beoordeling	Wbp Zelfevaluatie + review
Onafhankelijk onderzoek + certificaat	Privacy Audit

Bewijs van goed gedrag

Aan zo'n bewijs van goed gedrag, een privacycertificaat, wordt nu hard gewerkt. Het Samenwerkingsverband Audit Aanpak, bestaande uit het College Bescherming Persoonsgegevens (CBP) en een aantal beroepsorganisaties van auditors[1], heeft het Raamwerk Privacy Audit opgesteld op basis waarvan 'geaccrediteerde certificeerders' toetsen of een organisatie voldoet aan de (minimale) eisen die gesteld worden aan goed gedrag, dus in overeenstemming met de van toepassing zijnde wet- en regelgeving. De strekking van een privacycertificaat dient voor de maatschappelijke acceptatie helder en eenduidig geformuleerd te zijn. De wereld die achter een certificaat schuilgaat, is omvangrijk en complex. Het is daarom noodzakelijk eisen te formuleren over de betekenis en inhoud van het certificaat en eisen te formuleren over de deskundigheid van degene die het certificaat afgeeft. Het Samenwerkingsverband Audit Aanpak heeft daartoe een drietal producten ontwikkeld, die een gelaagde opbouw kennen en daardoor verschillen in reikwijdte en diepgang. Naar zwaarte gerangschikt zijn de volgende producten op het gebied van privacy beschikbaar: de Quickscan, de Wbp Zelfevaluatie en het Raamwerk Privacy Audit[2].

De Wbp Zelfevaluatie is een product dat ontwikkeld is ten behoeve van de leiding van een organisatie. De betreffende vragenlijst kan het beste in een soort van workshop worden ingevuld, waarbij de aanwezigen gezamenlijk kennis hebben van de bedrijfsprocessen waarin persoonsgegevens worden verwerkt, de veelal onderliggende automatisering en natuurlijk van de privacywet. De Wbp Zelfevaluatie is een methode om op systematische wijze tot een zelfstandig oordeel te komen over de mate van privacybescherming in de organisatie.

Zowel de Wbp Zelfevaluatie als het Raamwerk Privacy Audit is opgebouwd rondom negen aspecten die direct verband houden met de Wbp (zie tabel 2). In het Raamwerk Privacy Audit zijn verder nog eisen gesteld aan de 'organisatie van de verwerking', dus vrijwel de automatiseringsorganisatie, en het toezicht dat daarop wordt uitgeoefend (de 'evaluatie van de verwerking').

Op dit moment wordt nog hard gewerkt aan de zogenaamde accreditatie- en certificatieschema's. Het accreditatieschema regelt wie privacycertificaten mogen afgeven en wie daarop toezicht zal houden. Door deze regelingen ontstaat een nationaal erkend privacycertificaat, waarvan verzekerd is dat het is afgegeven en wordt onderhouden op basis van een deugdelijk onderzoek. Hoe dat deugdelijk onderzoek precies moet verlopen, staat vervolgens in het certificatieschema; voor de volledigheid zij nogmaals aangegeven dat wat onderzocht moet worden reeds is vastgelegd in het Raamwerk Privacy Audit.

Op weg naar het certificaat

Veelal zal een certificaat niet voor alle verwerkingen van persoonsgegevens in een organisatie nuttig zijn. Het management zal dus moeten aangeven welke verwerkingen met name voor certificering in aanmerking komen. Daarbij kan eventueel worden aangesloten op het in tabel 3 gegeven schema, afkomstig uit AV23 ([Blar01]). Voor deze processen zal het management, bijvoorbeeld via de zelfevaluatie of een gericht onderzoek van een privacydeskundige, zich eerst zelf willen vergewissen van de vraag of de organisatie inderdaad aan de vereiste wet- en regelgeving voldoet. Na eventuele correcties zal vervolgens de verantwoordelijke een verklaring van compliance afgeven, waarmee wordt aangegeven dat de organisatie gereed is voor de certificatie.

1) De volgende organisaties waren onder meer betrokken bij de ontwikkeling van privacy-assurance-producten: NOREA, NIVRA, NovAA en ISACA.

2) Deze producten kunnen worden gedownload via de website van het CBP op www.cbpweb.nl.

1	**Voornemen en melding:** in hoeverre heeft de organisatie maatregelen en procedures getroffen die ingaan op het gehele proces van gegevensverwerking (dat wil zeggen van het voornemen om persoonsgegevens te verwerken tot en met de melding bij het Cbp of de functionaris voor de gegevensverwerking).
2	**Transparantie:** zorgt de organisatie ervoor dat de verwerking van de persoonsgegevens transparant is voor de betrokkenen en voldoet de organisatie aan haar informatieverplichting naar betrokkenen.
3	**Doelbinding:** worden de persoonsgegevens voor een specifiek doel verzameld en verder verwerkt in overeenstemming met dit doel.
4	**Rechtmatige grondslag:** vindt de gegevensverwerking plaats op grond van de in de Wbp genoemde grondslagen.
5	**Kwaliteit:** de verwerking van persoonsgegevens moet voldoen aan kwaliteitseisen. Kwaliteit betekent in dit geval dat de persoonsgegevens toereikend, ter zake dienend, niet bovenmatig en juist en nauwkeurig zijn.
6	**Rechten van betrokkenen:** op welke wijze wordt invulling gegeven aan het recht op inzage, correctie, verwijdering, afscherming en verzet.
7	**Beveiliging:** heeft de organisatie passende technische en organisatorische maatregelen getroffen om persoonsgegevens te beveiligen tegen verlies of onrechtmatige verwerking en garanderen deze maatregelen een passend beveiligingsniveau, waarbij rekening is gehouden met de stand van de techniek en de kosten van de uitvoering.
8	**Uitbesteding van de gegevensverwerking:** is (een deel van) de gegevensverwerking uitbesteed en is dit vastgelegd in een overeenkomst (SLA).
9	**Gegevensverkeer met landen buiten de Europese Unie:** houdt de organisatie rekening met aanvullende regels in het geval dat persoonsgegevens worden verwerkt in of doorgegeven aan een land buiten de EU.

Tabel 2. De negen aspecten van de Wbp.

Hoeveelheid persoonsgegevens	Aard van de verwerking (complexiteit)	Aard van de persoonsgegevens		
		Algemeen	Bijzonder art. 16 Wbp	Financieel/ economisch
Weinig	Laag	Risicoklasse 0	Risicoklasse II	Risicoklasse II
Veel	Hoog	Risicoklasse I	Risicoklasse III	

Tabel 3. Schema voor het bepalen van de risicoklasse.

Privacycertificering

In Nederland is er nog geen organisatie die in het bezit is van een privacycertificaat afgegeven op basis van het Raamwerk Privacy Audit, maar dat zal niet lang meer op zich laten wachten, omdat het genoemde Samenwerkingsverband inmiddels vergevorderd is met het accreditatie- en certificatieprogramma.
Naar verwachting zal begin 2004 het eerste certificaat kunnen worden afgegeven. Daarbij zal het volgende model waarschijnlijk van toepassing zijn:
* geldigheidstermijn van drie jaar, met enkele tussenliggende herhalingsaudits;
* geen kritische non-conformaties en
* gericht op negen V-normen uit tabel 1 en aanvullende zekerheid dat de standaard-beveiligingsmaatregelen rond de automatisering van de gegevensverwerking zijn gewaarborgd. Deze normen zijn ook opgenomen in het Raamwerk Privacy Audit.

ZekeRE Privacy

Op eigen initiatief heeft NOREA de *Handleiding ZekeRE-privacy* uitgegeven. Deze handleiding is gebaseerd op het Raamwerk Privacy Audit en bedoeld voor de IT-auditor die in opdracht van een cliënt de kwaliteit van de verwerking van persoonsgegevens beoordeelt. De beoordeling richt zich hoofdzakelijk op het stelsel van internecontrolemaatregelen ter bescherming van de privacy. Hiertoe behoren zowel organisatorische als technische controlemaatregelen.

In bijlage I van de *Handleiding ZekeRE-privacy* heeft NOREA een matrix opgenomen waarin voor de aspecten rondom de verwerking van persoonsgegevens, de aard en de diepgang van de werkzaamheden nader zijn beschreven. Per aspect wordt daarbij ingegaan op toleranties (deficiënties) en non-conformiteiten die tijdens de audit naar voren zouden kunnen komen. Bijlage II van de handleiding bevat een voorbeeld voor een eventueel af te geven ZekeRE Privacy-oordeel door de gekwalificeerde IT-auditor.

Literatuur

[Blar01]
G.W. van Blarkom en drs. J.J. Borking, *Beveiliging van persoonsgegevens*, Registratiekamer, Achtergrondstudies en Verkenningen 23, april 2001.

[Gils01]
H.G.Th. van Gils en J.P.M.J. Leerentveld, *De rol van de auditor bij de implementatie van de Wbp*, Compact 2001/4.

[NORE02]
Nederlandse Orde van Register EDP-Auditors (NOREA), *Handleiding ZekeRE-privacy*, 2001/2002.

[SAAC01a]
Samenwerkingsverband Audit Aanpak/Cbp, *Raamwerk Privacy Audit*, Den Haag 2001.

[SAAC01b]
Samenwerkingsverband Audit Aanpak/Cbp, *Wbp Zelfevaluatie*, Den Haag 2001.

[SAAC01c]
Samenwerkingsverband Audit Aanpak/Cbp, *Quickscan*, Den Haag 2001.

Mw. drs. L. Hoogeveen
is werkzaam als consultant bij KPMG Information Risk Management. Zij heeft zich de afgelopen jaren primair beziggehouden met advisering en auditing op het gebied van privacy, advisering over het (her)inrichten van het stelsel van internecontrolemaatregelen (AO/IC) en het verlenen van EDP-auditondersteuning in het kader van de jaarrekeningcontrole.

hoogeveen.linda@kpmg.nl

Drs. H.G.Th. van Gils RE RA
is senior medewerker bij KPMG Information Risk Management. Hij is medecoördinator van de TPM-dienstverlening van KPMG aan haar klanten en heeft reeds gedurende vele jaren voor organisaties TPM-onderzoeken uitgevoerd. Naast de TPM-onderzoeken houdt hij zich de laatste jaren ook nadrukkelijk bezig met andere certificeringsopdrachten, zoals software- en privacycertificering.

vangils.herman@kpmg.nl

2003/3

Softwarecertificering

Drs. A.R.J. Basten RE

Inleiding

Softwareleveranciers hebben vaak moeite om hun klanten te overtuigen van de hoge kwaliteit van hun softwarepakket. Op basis van een softwarecertificeringsonderzoek kan een softwareleverancier de kwaliteit van zijn softwarepakket aan derden aantoonbaar maken. Nadat een certificeringsonderzoek is afgerond en het pakket als voldoende is beoordeeld, ontvangt de softwareleverancier een certificaat. Met dit certificaat kan aan klanten gemakkelijk aantoonbaar worden gemaakt dat het pakket beschikt over voldoende internecontrolemaatregelen. Daarbij kan de softwareleverancier zich onderscheiden van zijn concurrenten die geen certificaat hebben.

Betrokken partijen

Door de grote accountantsorganisaties zijn inmiddels diverse certificaten bij softwarepakketten afgegeven. Uit de praktijk blijkt dat vooral de leveranciersmarkt van boekhoudsystemen geïnteresseerd is in het verkrijgen van een certificaat.
De opdrachten worden uitgevoerd door ICT-auditors die kennis hebben van de functionaliteit van het te onderzoeken pakket. Deze kennis is benodigd om een pakketspecifieke normenset te kunnen opstellen en op een efficiënte wijze de toetsing te kunnen uitvoeren.

> Vooral de leveranciersmarkt van boekhoudsystemen is geïnteresseerd in het verkrijgen van een certificaat.

Onderzoek

Tijdens de opdrachtformulering is afgesproken welke modules van het softwarepakket worden beoordeeld en welke kwaliteitscriteria van toepassing zijn. Daarbij gaat het meestal om de volgende (kwaliteits)aspecten:
- *integriteit:* biedt het pakket voldoende internecontrolemaatregelen om de juistheid, volledigheid en tijdigheid van de geautomatiseerde gegevensverwerking te kunnen waarborgen;
- *exclusiviteit:* biedt het pakket voldoende internecontrolemaatregelen, zodat vertrouwelijke informatie kan worden afgeschermd (van reguliere gebruikers);
- *controleerbaarheid:* biedt het pakket voldoende internecontrolemaatregelen om achteraf te kunnen vaststellen hoe één of meer transacties door het systeem zijn verwerkt (bijvoorbeeld audit trail en het netwerk van controletotalen).

Het onderzoek heeft als doel te toetsen of het pakket voldoende internecontrolemaatregelen bevat, zodat een betrouwbare gegevensverwerking kan worden gerealiseerd. De benodigde internecontrolemaatregelen worden bepaald op basis van een risicoanalyse en komen tot uitdrukking in de normenset. Tijdens het onderzoek wordt door middel van een aantal testgevallen aantoonbaar gemaakt of aan een norm wordt voldaan. Kortom, door deze wijze van opdrachtuitvoering worden opzet en bestaan beoordeeld.

Zoals reeds vermeld richt het onderzoek zich op een aantal modules van het softwarepakket. Het object van onderzoek betreft dan deze modules van één bepaalde release. Belangrijk is dat het object van onderzoek goed met de softwareleverancier wordt besproken, omdat dit ook in het certificaat wordt vermeld. In principe geldt dat het certificaat niet van toepassing is op andere releases van hetzelfde pakket. Natuurlijk kan via onder andere releasenotes worden vastgesteld hoeveel inspanning benodigd is om een update van het onderzoek uit te voeren. De update zal altijd minder inspanning vergen dan de initiële opdracht.

Beperking

Indien tot een positief oordeel wordt gekomen, betekent dit niet dat iedere implementatie (van het pakket) ook voldoet aan de normenset. Dit wordt veroorzaakt doordat vele internecontrolemaatregelen kunnen worden geïnactiveerd door het wijzigen van instellingen (parameters). De waarde van een certificeringsonderzoek is dat vastgesteld is welke internecontrolemaatregelen in het softwarepakket aanwezig zijn of kunnen worden geactiveerd. Dit wordt geïllustreerd met een voorbeeld.

> De norm is: Het pakket ondersteunt functiescheiding tussen de invoer van journaalboekingen en de verwerking van boekingen.
>
> In het certificeringsonderzoek wordt getoetst of de softwarefuncties invoer en verwerking aan twee afzonderlijke medewerkers *kunnen* worden toegewezen.
>
> Het toewijzen van deze softwarefuncties aan medewerkers vindt plaats door een autorisatie-instelling en functiescheiding hoeft dus niet aanwezig te zijn bij iedere implementatie. Kortom, de waarde van het certificaat is dat functiescheiding mogelijk is.

Uitkomsten

Het resultaat van het onderzoek is een rapport waarin het uitgevoerde onderzoek wordt beschreven inclusief de normenset, bevindingen en de conclusie. Desgewenst kan ook een certificaat worden verkregen dat de belangrijkste uitkomsten van het onderzoek weergeeft, en dat volledigheidshalve ook verwijst naar het rapport.

Drs. A.R.J. Basten RE
is werkzaam als IT-auditor bij KPMG Information Risk Management. Hij heeft ruime ervaring met het reviewen van en adviseren over IT-beheerprocessen en het beoordelen van applicatieve toepassingen binnen de financiële dienstverlening.

basten.fons@kpmg.nl