PvIB Expertbrief – Januari 2009
ISSN 1872-4876, jaargang 5 – Nr. 1

Een Standaard keuze!

De aanleiding voor deze expertbrief is de groeiende behoefte aan een methode die leidt tot een adequate selectie van te implementeren informatiebeveiligingstandaarden.
Door de vele standaarden die inmiddels bestaan binnen het vakgebied, zien we soms door de bomen het bos niet meer. Welke standaarden moeten we wanneer hanteren? Zijn alle standaarden even zinvol en/of toepasbaar in elke sector? Wat voor soort standaarden zijn er? Zomaar een greep uit de vragen die over dit onderwerp spelen. Deze expertgroep heeft zich gebogen over de vraag hoe zo'n proces eruit zou kunnen zien om te komen tot een adequate selectie van informatie-beveiligingstandaarden.

Mark van der Beek

Ranil Korf

Hendrik-Jan Smit

Vincent Alwicher

Bart Bokhorst

Erno Duinhoven

Bert van Ingen

Kees Jongejans

Jeroen Lambregts

Paul Petraeus

Steven Timmer

Pagina

2 INLEIDING EN SITUATIESCHETS

Tegenwoordig kunnen we niet meer om standaarden heen. Van een standaard voor het zetten van thee (ISO 3103) tot een standaard die drieletter codes definieert voor valuta (ISO 4217). Overal kom je ze tegen. Ook binnen het werkveld informatiebeveiliging hebben we met diverse nationale maar ook internationale standaarden te maken. In de afgelopen periode lijkt het aantal standaarden zelfs exponentieel te zijn gegroeid.

Deze wildgroei aan standaarden binnen het vakgebied informatiebeveiliging dwingt tot het maken van keuzes. Immers het conformeren aan alle bestaande standaarden brengt hoge kosten met zich mee en is praktisch onmogelijk. Er is een groot aantal redenen die het maken van een weloverwogen keuze van een standaard rechtvaardigen, zoals:

- Standaarden zijn er in overvloed;
- Standaarden overlappen elkaar vaak;
- Standaarden richten zich op verschillende partijen en/of niveaus in organisaties;
- Standaarden kunnen verschillende structuren en benaderingen hebben;
- Standaarden worden in verschillende talen aangeboden;
- Standaarden kunnen zich richten op verschillende soorten controls, zoals: proces controls, business controls, technische controls, applicatieve controls, user controls, etcetera;
- Standaarden kunnen variëren van technologie-afhankelijk tot technologie-onafhankelijk;
- Standaarden worden aangeboden en /of verplicht gesteld door diverse partijen;

De grote hoeveelheid aan beschikbare standaarden maakt het voor een organisatie een uitdaging om te komen tot een adequate selectie van standaarden. Adequaat betekent onder meer dat de gekozen standaarden bijdragen aan het behalen van de bedrijfsdoelstellingen en dat wordt voldaan aan de vereisten en ‘best practices’ van een mogelijke externe (regulerende) omgeving. Tevens dienen de gekozen standaarden te passen bij de cultuur en de volwassenheid van een organisatie. De vraag is nu hoe men kan komen tot een juiste selectie van standaarden. Een specifieke methodiek om te komen tot een keuze bestaat helaas niet. Dit is natuurlijk vreemd aangezien standaarden een uiterst relevant onderdeel vormen binnen het vakgebied informatiebeveiliging.

Een groep van informatiebeveiligingsexperts heeft tijdens een expertsessie, naar aanleiding van bovenstaande situatieschets, gekeken hoe het selectieproces van informatiebeveiligingstandaarden eruit zou kunnen zien. Het streven is om uiteindelijk een ‘standaard’ te ontwikkelen die een proces beschrijft voor het selecteren van standaarden.

Deze publicatie is een weergave van de resultaten van de expertsessie en is tot stand gekomen met medewerking van de op de voorpagina genoemde personen met Vincent Alwicher als probleemeigenaar, Erno Duinhoven als facilitator en Mark van der Beek, Ranil Korf en Hendrik-Jan Smit als ghostwriters, in het kader van hun afstudeeronderzoek (IT-audit opleiding) aan de Vrije Universiteit te Amsterdam.

DE ONDERZOEKSVRAGEN

De expertgroep heeft zich gebogen over de volgende centrale vraagstelling:

Wat is het ideale proces voor het selecteren van de meest geschikte en effectieve set van informatiebeveilingstandaarden?

Om deze vraag te beantwoorden zijn we tijdens de expertsessie tot de volgende twee deelvragen gekomen, welke de expertgroep graag wil beantwoorden:

- Welke stappen moeten worden doorlopen bij het selectieproces?
- Wat zijn de criteria waarop je de diverse standaarden van elkaar kan onderscheiden? Hierdoor kan een gerichte keuze gemaakt worden tussen verschillende (gedeeltes van) standaarden.

De expertgroep heeft zich vooraf gerealiseerd dat het onwaarschijnlijk is dat deze vragen in één expertsessie volledig beantwoord konden worden. Uiteindelijk wil zij door vervolgactiviteiten wel graag een volledig antwoord kunnen formuleren. Bovenal verwacht de expertgroep, met de in deze expertbrief voorgestelde aanpak, een doorstart te maken naar een serieuze aanpak die kan doorgroeien tot een methodiek.

STANDAARDEN VOOR INFORMATIEBEVEILIGING

Standaarden in het algemeen

Wat is nu precies een standaard? Een standaard zet een principe of norm neer en kan aangeven hoe deze moet worden uitgewerkt en geïmplementeerd. In essentie is het een set van ‘best practices’ die zijn ontwikkeld door experts in het vakgebied. Standaarden ontstaan door praktijkervaring en beschikbare bestaande kennis in het vakgebied te combineren. Hier dient een zorgvuldig proces van totstandkoming aan vooraf te gaan wil het zinvolle resultaten opleveren. Er kan onderscheid gemaakt worden in:

- Bedrijfsspecifieke standaard (gehanteerd binnen een bepaalde organisatie)
- Industriestandaard (gehanteerd door een min of meer officiële groep bedrijven)
- De facto standaard (door de markt zelf bepaald)
- De jure standaard (door bevoegd overheidsorgaan voorgeschreven)

Standaarden binnen informatiebeveiliging

Er bestaan diverse standaarden binnen het vakgebied informatiebeveiliging. Het toepassen van informatiebeveiligingstandaarden is bedoeld om de beveiliging van informatie te optimaliseren, met name gericht op de aspecten: vertrouwelijkheid, integriteit en beschikbaarheid. In het navolgende zullen enkele belangrijke uitgevende organisaties van standaarden, met daarbij een aantal belangrijke standaarden, worden toegelicht. Het is niet de bedoeling een compleet overzicht te geven, maar om een indruk te geven van de diversiteit aan beschikbare standaarden.

4

ISO
De International Organization for Standardization (ISO) is een internationale organisatie die normen vaststelt. De organisatie is een samenwerkingsverband van nationale standaardisatieorganisaties in 156 landen. ISO heeft op het gebied van informatie technologie een samenwerkingsverband met IEC (the International Electrotechnical Commission), waaruit onder andere de ISO 27000 serie is ontstaan.
Enkele relevante en bekende informatiebeveiligingsstandaarden van ISO, met betrekking tot informatiebeveiliging, betreffen ISO 27001 en ISO 27002.
De ISO 27001 specificeert eisen voor het vaststellen, implementeren, uitvoeren, controleren, beoordelen, bijhouden en verbeteren van een gedocumenteerd 'Information Security Management System' (ISMS).
ISO 27002, beter bekend als de 'Code voor Informatiebeveiliging', beschrijft normen en maatregelen, die van belang zijn voor het realiseren van een afdoende niveau van informatiebeveiliging.
Naast deze standaarden heeft ISO vele gedetailleerde (operationele) informatiebeveiligingstandaarden uitgegeven.

NIST
De 'National Institute of Standards and Technology' (NIST) is een onderdeel van het Amerikaanse ministerie van Economische Zaken. Bij NIST worden standaarden, voor Amerikaanse overheidsinstanties ontwikkeld ter bevordering van de innovatie en industriële concurrentie in de VS.
Een relevante en bekende standaard van NIST betreft NIST SP 800-53: 'Recommended Security Controls for Federal Information Systems'. In deze standaard worden de minimale beveiligingsmaatregelen opgesomd voor het realiseren van een acceptabel niveau van informatiebeveiliging. Naast deze standaard heeft NIST vele gedetailleerde (operationele) informatiebeveiligingstandaarden uitgegeven.

ISF
Het Information Security Forum (ISF) is een internationale onafhankelijke non-profit organisatie gericht op benchmarking en best practices van informatiebeveiliging. The Standard of Good Practice (SGOP) is een belangrijke publicatie uit het ISF programma. Deze standaarden bieden gedetailleerde documentatie van geïdentificeerde 'best practices' voor informatiebeveiliging.

ISACA
De 'Information Systems Audit and Control Association' (ISACA) is een Amerikaanse beroepsvereniging van IT-auditors en informatiebeveiligers. ISACA heeft als doel de uitoefening van het audit vakgebied op een hoger plan te brengen door het verder professionaliseren van het vakgebied en de leden van de vereniging te ondersteunen bij het uitoefenen van hun vak.
Eind jaren negentig werd een algemeen raamwerk voor algemene IT-beheersmaatregelen ontwikkeld door ISACA en het IT Governance Institute (ITGI). Dit zijn de'Control Objectives for Information and related Technology', oftewel CoBiT. Het CobiT framework is gebaseerd op het principe dat organisaties voorzien dienen te worden van de informatie die noodzakelijk is voor het realiseren van hun doelstellingen. CoBiT staat momenteel vooral in de vernieuwde belangstelling doordat deze bij uitstek geschikt is om een organisatie in staat te stellen aan te tonen te voldoen aan de regelgeving zoals die door Sarbanes-Oxley (SOX) en

COSO (Committee of Sponsoring Organizations of the Treadway Commission) worden gevraagd.

PROCES VOOR SELECTIE

Om een keuze te maken voor standaarden die passend zijn voor een organisatie is het belangrijk om een gedegen selectieproces in te gaan. Echter voordat wordt gestart met het selectieproces, is het belangrijk te beseffen dat het in principe een keuze is voor de middellange tot lange termijn (>2 jaar). Het heroverwegen van gemaakte keuzes en overstappen naar andere standaarden is niet wenselijk. Dit hangt samen met kosten die het implementeren van standaarden met zich mee brengt, maar ook de (extra) kosten die gemaakt moeten worden indien men overschakelt naar andere standaarden. Hier kan men bijvoorbeeld denken aan de opgedane kennis en ervaring met een standaard die verloren gaat bij het overstappen naar een andere standaard.

De te doorlopen stappen

In deze paragraaf schetsen wij globaal een proces dat organisaties kunnen hanteren om te komen tot een keuze voor standaarden. Het proces bestaat uit de volgende stappen:

1. Bepalen ‘key stakeholders’;
2. Vaststelen score criteria van de ‘key stakeholders’;
3. Keuze (o.b.v. gewogen criteria);
4. ‘Nazorg’.

De verschillende stappen worden hieronder nader uitgewerkt.

Stap 1: Bepalen ‘key stakeholders’
De eerste stap is het bepalen van de ‘key stakeholders’ met betrekking tot informatiebeveiliging binnen de organisatie. Bijvoorbeeld de afdeling Internal Audit, de Information Security Officer, de CEO en de CFO.
Deze stap in het proces draagt bij aan het creëren van een breed draagvlak en acceptatie voor de gekozen standaarden. Zonder dit draagvlak zal het implementeren van de gekozen standaarden een moeizaam proces worden en zal het wellicht vertraging van de implementatie met zich meebrengen.

Stap 2: Input ‘key stakeholders’
Het zijn de ‘key stakeholders’ die bepalen wat de belangrijkste aspecten zijn in de keuze voor bepaalde standaarden. Om de ‘key stakeholders’ handvatten te bieden zijn hier criteria opgesteld waarmee standaarden van elkaar kunnen worden onderscheiden. De volgende criteria zijn naar aanleiding van de expertsessie en een literatuurstudie opgesteld:

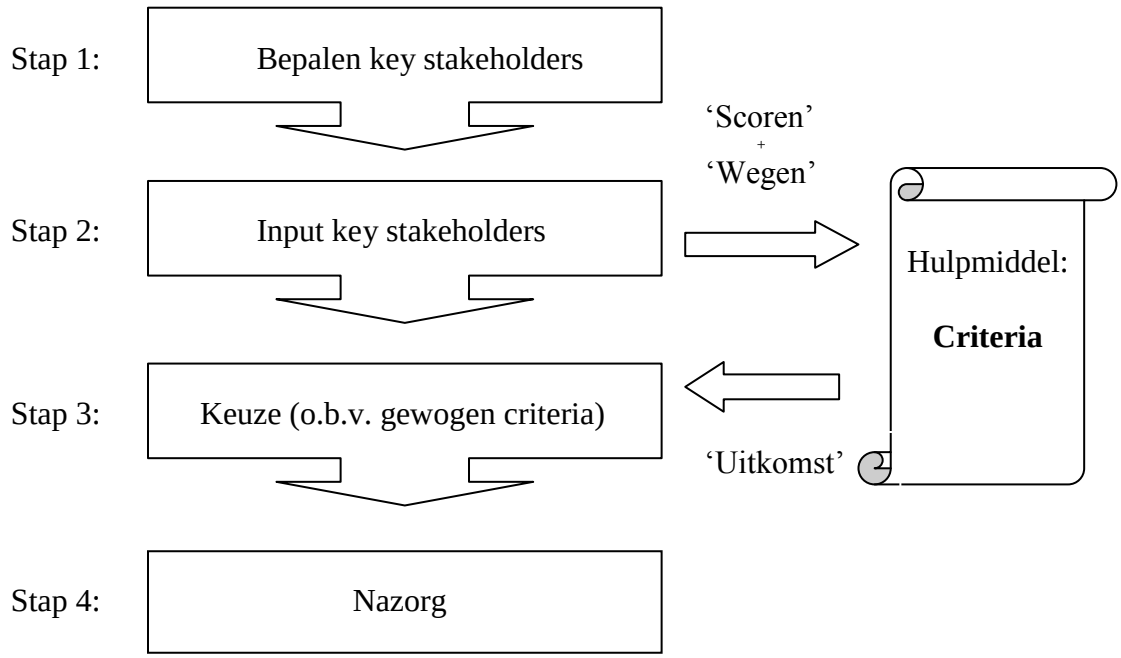
- breedte
- diepte
- flexibiliteit
- ratio
- kosten
- acceptatie
- taal

Deze lijst is niet uitputtend en kan voor individuele situaties aangevuld worden.
Het inzicht hoe bepaalde standaarden 'scoren' op de diverse criteria is essentieel in het keuzeproces. Nadat het gehele proces is geschetst, zullen we een omschrijving geven van de verschillende criteria en is een eerste exercitie gedaan om de eerder besproken standaarden te positioneren op basis van deze criteria. De naar aanleiding hiervan ontstane tabel is een belangrijk hulpmiddel bij het selectieproces.

Stap 3: Keuze (o.b.v. gewogen criteria)
De volgende stap in het proces is het uiteindelijk komen tot een keuze voor de meest passende standaard(en). Deze keuze is gebaseerd op de verschillende wegingen per criteria, toegekend door de diverse stakeholders en wordt uitgesproken door het verantwoordelijke management. Hierbij is het van belang dat de keuze van bepaalde standaarden aansluit op de bedrijfsdoelstellingen.

Stap 4: 'Nazorg'
De laatste stap betreft de nazorg van de gemaakte keuze, ofwel is de keuze nog steeds de juiste. Als de standaarden slecht blijken te zijn geïmplementeerd, was het wellicht de verkeerde keuze en moeten andere standaarden worden overwogen.

In de volgende figuur is het proces schematisch weergegeven:



Om het uiteindelijke gebruik van de standaarden te vergemakkelijken wordt geadviseerd aan te sluiten bij dominante stromen die bepaalde zaken voorschrijven binnen de organisatie, bijvoorbeeld: compliance, risicomanagement, kwaliteitsdenken, -etc. Hiermee wordt het draagvlak en de acceptatie vergroot.

HULPMIDDEL: SELECTIECRITERIA

Om een goede afweging te maken tussen bepaalde standaarden moeten ze onderling vergeleken kunnen worden. Hiertoe zijn selectiecriteria opgesteld. Wij hebben hierbij gekozen voor vier standaarden die onderling vergelijkbaar zijn: ISO 27002, NIST SP 800-53, ISF Standard of Good Practice en COBIT 4.1. Waar nodig zal worden verwezen naar overige standaarden uit de betreffende reeks (bijvoorbeeld in het geval van ISO, naar ISO 27001).

Daarnaast is het goed om in het achterhoofd te houden dat de selectiecriteria niet per se een positieve of negatieve impact hebben op een keuze. Bijvoorbeeld een breed geaccepteerde norm betekent niet meteen dat deze het beste past bij een bepaalde organisatie. Of dat minder brede standaarden niet nog steeds zeer bruikbaar zijn op bepaalde onderdelen omdat deze standaarden erg diepgaand zijn uitgewerkt. Met andere woorden, de factoren zijn bruikbaar om de verschillende standaarden te vergelijken, echter men kan niet verwachten dat een ‘hogere’ score altijd beter is. In het navolgende worden allereerst de onderscheiden criteria toegelicht.

Breedte
Dekt de betreffende standaard de belangrijkste beveiligingsdomeinen die de organisatie als belangrijk identificeert? Domeinen kunnen zowel IT als niet IT gerelateerd zijn (zoals fysieke en personele beveiliging).

Diepte:
Bevatten de standaarden informatie op zowel strategisch, tactisch als operationeel gebied? Bijvoorbeeld: ISO werkt doelstellingen, beheersingsmaatregelen en implementatierichtlijnen gedetailleerd uit (tactisch en operationeel gebied) waar CobiT meer algemene doelstellingen geeft en minder concreet over de invulling er van spreekt (strategisch).

Flexibiliteit:
Kunnen andere gebruikers dan informatiebeveiligers de standaarden gebruiken? Bijvoorbeeld het management en/of auditor voor het aantonen van interne beheersing.

Ratio:
Beschrijven de standaarden de redenen van de opgesomde maatregelen? Doordat de ratio is opgenomen is het voor gebruikers makkelijker om de toepasbaarheid en consistentie vast te stellen.

Acceptatie:
Hoe breed zijn de standaarden geaccepteerd binnen het vakgebied? Is er bijvoorbeeld veel discussie omtrent de inhoud van bepaalde standaarden of is er een algemene, negatieve of positieve, mening over gebruik van bepaalde standaarden.

Taal:
Zijn de standaarden alleen in het Engels te verkrijgen, of is er ook een Nederlandse vertaling beschikbaar?

Kosten:
Gaan er kosten gepaard met de aanschaf van standaarden? Zijn er eventueel delen gratis? De kanttekening die hierbij wel moet worden gemaakt is dat de kosten voor de bronliteratuur ten opzichte van het totale invoeringstraject van de standaarden marginaal zijn.

In de onderstaande tabel zijn de eerder besproken standaarden gepositioneerd ten aanzien van de criteria.

Criteria	ISO	NIST	COBIT	ISF
Breedte[1]	• Dekt de hoofdgebieden van IB • Onderwerpen overzichtelijk gerangschikt	• Dekt de hoofdgebieden van IB • Onderwerpen versnipperd behandeld • Veel product-standaarden	• Beperkt op het gebied van IB • Niet specifiek IB, gericht op de beheersing van IT in het algemeen	• Dekt de hoofdgebieden van IB • Periodieke update en eventuele aanpassingen
Diepte:	• Tactisch en operationeel • Management cyclus is opgenomen in 27001.	• Tactisch en operationeel • Tactisch niet heel uitgebreid uitgewerkt in NIST SP 800-53, echter wel verder, verspreid, uitgewerkt in overige NIST reeksen.	• Strategisch en tactisch • Operationeel niet uitgewerkt. • Verwijst naar ISO • Kent ook specifieke COBIT Practices en Security Baselines	• Tactisch en operationeel
Flexibiliteit:	• Weinig gebruik door anderen dan IB specialisten	• Weinig gebruik door anderen dan IB specialisten .	• Veel gebruik door anderen dan IB specialisten • Verbondenheid met audit processen (auditor)	• Weinig gebruik door anderen dan IB specialisten
Ratio:	• Doelstellingen hangen samen met richtlijnen	• Op basis van een risk assessment kunnen de minima-le beveiligingsmaat-regelen worden geselecteerd (NIST SP 14, FIPS 199+200).	• Elementen hangen samen met business drivers en input en output	• Principes hangen samen met doelstellingen
Acceptatie:	• Meest geaccepteerde norm in Nederland	• Verplicht voor US federale overheid • Private sector beperkt.	• Goede ondersteuning voor Sox compliance • Breed geaccepteerd	• Niet breed geaccepteerd • Met name geaccepteerd door leden ISF. • Bv niet in US
Taal:	• Nederlands en Engels	• Engels	• Engels	• Engels
Kosten:	• Gehele reeks betaald	• Gehele reeks gratis	• Betaald	• De standaard (SGOP) is gratis. • Overige producten tegen een betaald lidmaatschap.

[1] Voor meer informatie over de uitkomsten met betrekking tot dit criterium verwijzen wij naar het gerelateerde afstudeeronderzoek “Standaarden, is door de bomen het bos nog te zien?”

DISCUSSIEPUNTEN

Tijdens de expertsessie zijn discussies gevoerd over verschillende aspecten en invalshoeken. Niet elke discussie was relevant voor het beantwoorden van de onderzoeksvraag van deze expertbrief. Wij vinden het wel relevant om deze discussiepunten hier vast te leggen, omdat bepaalde onderwerpen als input kunnen dienen voor eventuele (vervolg)expertbrieven.

Ontwerpcriteria voor standaarden
Uit discussie is gebleken dat een aantal criteria wel als erg nuttig worden ervaren. Echter geen van de standaarden heeft deze criteria verwerkt. Hierbij betreft het de volgende criteria:

- De mate waarin de standaard proces- en productnormen onderscheiden;
- De mate waarin de verhouding klant versus leverancier is verwerkt;
- De mate waarin een volwassenheidsmodel is opgenomen in de standaarden;
- De mate van prioriteitsstelling binnen de standaarden aan de hand van een risicomodel.

ISO 27001 als standaardnorm: de linking pin naar andere beveiligingsstandaarden
ISO 27001 wordt in de meeste gevallen gezien als een referentiekader en kan daarmee worden beschouwd als de linking pin. Sommige standaarden verwijzen zelfs naar ISO 27001, zoals bijvoorbeeld COBIT.

Mapping
Het nut van mapping blijft een punt van discussie. Op dit moment zijn er mappings tussen standaarden uitgevoerd welke alle voornamelijk gericht zijn op overeenkomsten. Een overzicht welke gericht is op de hiaten lijkt veel zinvoller, aangezien dan duidelijk wordt welke onderwerpen missen wanneer voor bepaalde standaarden wordt gekozen. Het idee van een ‘draaitabel’ wordt geopperd. Dit maakt het mogelijk de mapping uit verschillende invalshoeken te bekijken.

Overkoepelende standaard voor standaarden
Een algemeen toepasbare overkoepelende standaard voor standaarden lijkt niet nuttig. Indien er een standaard voor standaarden zou bestaan, welke alle informatie zou bevatten van de huidige standaarden, zou deze groot en onoverzichtelijk zijn en niet toegankelijk.

Uitbesteden van IT
Het kan voorkomen dat een aanbieder (aan wie IT werkzaamheden zijn uitbesteed) beschikt over een reeks gebruikte standaarden. Het is mogelijk dat deze niet voldoen aan de eisen van de afnemer. Deze wenst vaak dat voldaan wordt aan zijn standaarden en daarmee komt de aanbieder in een lastige situatie gezien de vaak vele afnemers. Ook komt de relatie tussen aanbieder en afnemer in vrijwel geen enkele standaard terug.
Gezien de ontwikkelingen in de markt, waarbij steeds meer activiteiten worden uitbesteed, is de vraag of deze ketenafhankelijkheid en verhoudingen zijn verwerkt in een standaard, steeds belangrijker. Bijvoorbeeld bij ISO is hierover niets te vinden. Vorig jaar heeft de NOREA, in samenwerking met het PVIB, hiervoor een apart studierapport uitgegeven.

10 CONCLUSIES EN VERVOLG

De expertgroep is er deels in geslaagd om antwoorden te geven op de gestelde vragen.

Er is op hoofdlijnen een proces geschetst welke kan helpen bij het kiezen van standaarden (of alleen bepaalde delen). Het geschetste proces behoeft echter nog nadere uitwerking, in detail, om daadwerkelijk een praktisch handvat te bieden bij het selecteren van standaarden.

Er zijn belangrijke selectiecriteria onderscheiden die een rol spelen in het proces om te komen tot een selectie van standaarden. Daarnaast is een eerste aanzet gegeven enkele relevante standaarden naar deze selectiecriteria te 'scoren'.

Tot slot zijn in de discussie nuttige constateringen gedaan die kunnen helpen bij het verder uitwerken van de openstaande punten.

Hoe verder?
Door de complexiteit van de materie en de beperkte tijd waarin dit onderwerp besproken is, zijn er nog vele vragen onbeantwoord gebleven:

1. Zijn we in staat om op basis van deze aanzet een raamwerk te maken van verschillende standaarden die bestaan?
2. Een aantal selectiecriteria zijn onderkend. Welke selectiecriteria zijn nog meer te onderkennen?
3. Zijn de weergegeven standaarden correct 'gescoord' op de onderkende selectiecriteria?

Daarnaast waren er nog en groot aantal vragen die bij de opzet van de probleemstelling buiten beschouwing zijn gelaten zoals opgenomen in bijlage 1.

Deze expertbrief is niet meer dan een aanzet om een bredere vakinhoudelijke discussie op gang te brengen, waarbij de input van zoveel mogelijk betrokkenen gewenst is. De expertgroep nodigt u dan ook uit om te reageren. U kunt uw reacties sturen naar expertbrief@pvib.nl. Ook indien u deze expertbrief heeft kunnen waarderen stellen wij een e-mailtje op prijs!

Op de site www.ibpedia.nl kunt u meewerken aan verdere verrijking en kennisdeling over IB-standaarden en andere onderwerpen met betrekking tot informatiebeveiliging. Iedereen is van harte uitgenodigd om hieraan deel te nemen.

BIJLAGE 1

Definities
- Wat is de definitie van een standaard?
- Wat zijn de definities van gebruikte termen in de standaard?
- Moeten standaarden termen gebruiken als moeten of mogen en is dat relevant, waarom? En in welke omstandigheden?

Structuur van de standaarden
- Wat voor type IB standaarden zijn er?
- Zijn er verschillende gebruikersgroepen? Waarom (niet), wie zijn zij?
- Moeten standaarden gekoppeld zijn met organisatiedoelstellingen? Waarom (niet)?
- Is een link met bedrijfsprocessen belangrijk? Waarom (niet)? En hoe zou dit er uit zien?
- Is een link met architectuur belangrijk? Waarom (niet)? En hoe zou dit er uit zien?

Selectie van standaarden
- Welke organisaties kunnen goede kwalitatieve standaarden uitgeven?
- Wat is een betrouwbare organisatie? Wat zijn hiervoor de criteria?
- Hoe beïnvloedt het volwassenheidsniveau van de organisatie de selectie en het gebruik van standaarden?
- Hebben organisaties verschillende behoeften met betrekking tot standaarden? Waarom (niet)? Bijvoorbeeld:
    - organisaties waarbij IT kern activiteit is
    - organisaties waarbij IT niet kern activiteit is
    - organisaties die hun IT activiteiten hebben uitbesteed
    - organisaties die wel en niet vallen onder wet- en regelgeving van de overheid met betrekking tot IB.
- Hoe wordt de kwaliteit van standaarden bepaald? Wat zijn hiervoor de criteria? Hoe is de continuïteit van standaarden gewaarborgd?
- Zijn er verschillen in kwaliteit van standaarden uitgegeven door een commerciële of niet commerciële instelling?

Implementatie van standaarden
- Hoe worden de toepassingsgebieden en de maatregelen in scope van standaarden bepaald?
- Wanneer is een implementatie van standaarden succesvol? Wat zijn hiervoor de criteria? Hoe kan dat worden gemeten?

12 LITERATUURLIJST

Voor het tot stand brengen van deze expertbrief heeft de werkgroep de volgende literatuur geraadpleegd:

Main bodies:

- ISO 27000 reeks http://www.27000.org/ http://www.iso27001security.com/ http://www2.nen.nl/nen/servlet/dispatcher.Dispatcher?id=192437
- NIST reeks http://csrc.nist.gov/
- ISF SOGP https://www.securityforum.org/
- COBIT 4.1 http://www.isaca.org/

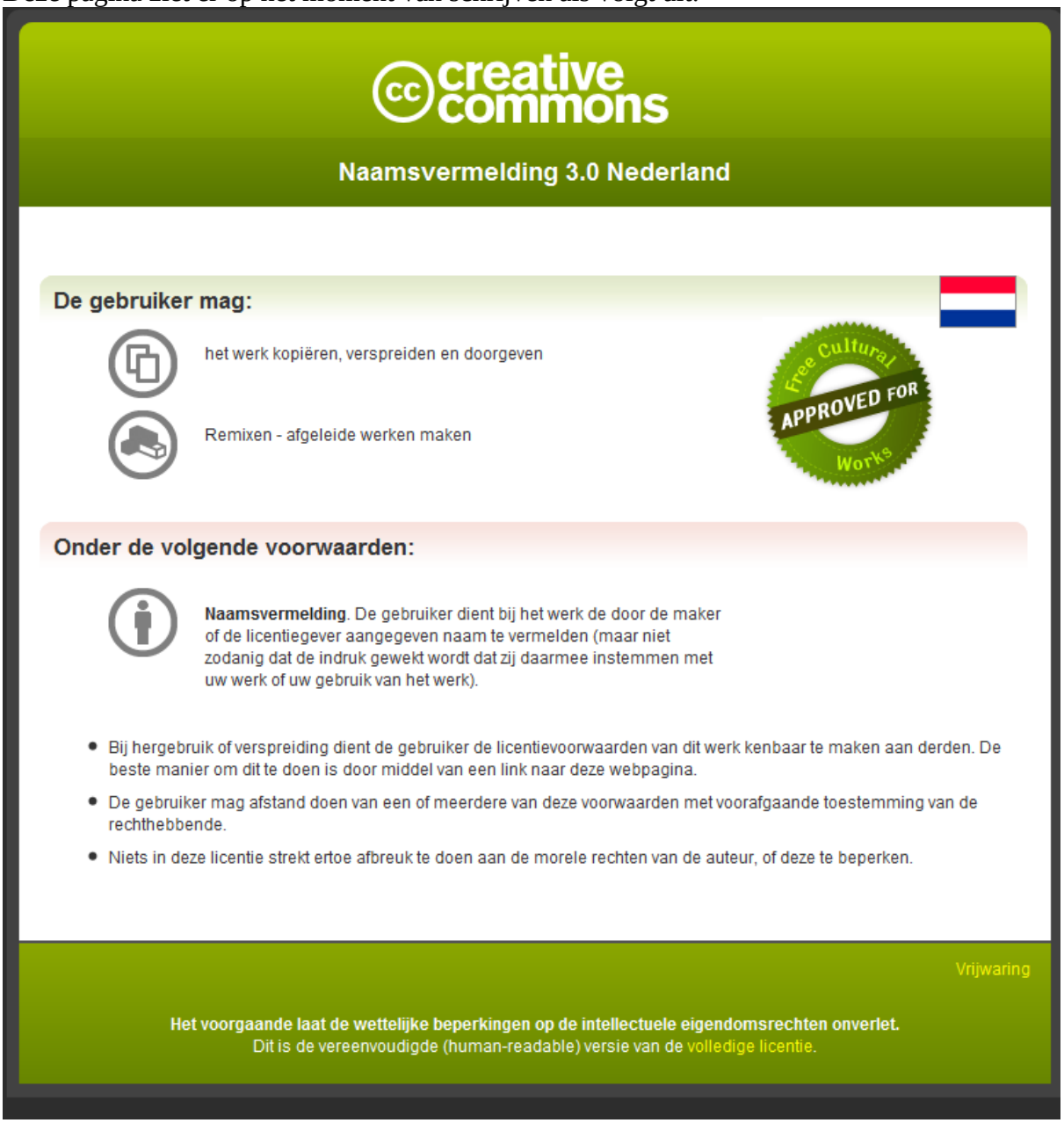
Artikelen:

- *Aligning COBIT 4.1, ITIL v3 and ISO/IEC 27002 for business benefit*, ITGI and OGC, 2008

APPENDIX GEBRUIKTE LICENTIEVORM

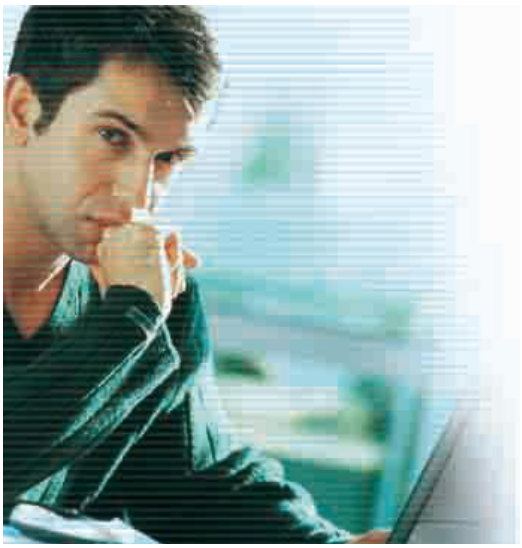
De expertbrief wordt gepubliceerd onder de volgende licentie:
http://creativecommons.org/licenses/by/3.0/nl/

Deze pagina ziet er op het moment van schrijven als volgt uit:



14

WORDT LID VAN HET PVIB, SPEEL OP ZEKER EN BEVEILIG SAMEN…



Informatiebeveiliging is reeds jaren lang een noodzakelijk, spannend en dynamisch vakgebied. Vrijwel alle beroepen hebben meer dan ooit te maken met vertrouwelijkheid, beschikbaarheid en integriteit van informatie. Of u nu als directeur, manager, adviseur of programmeur werkzaam bent. Het Platform voor Informatiebeveiliging kan u behulpzaam zijn bij al uw vraagstukken op het gebied van informatiebeveiliging.

Wat is het Platform voor Informatiebeveiliging?
Het PvIB is een open, breed samengesteld platform waarin professionals elkaar vinden om professioneel inhoud te geven aan informatiebeveiliging, door het uitwisselen van ideeën, informatie, kennis, inzichten en vooral veel praktijkervaring.

Wat willen wij bereiken?
Wij willen de fysieke, (systeem)technische & organisatorische beveiliging van gegevens en van de gegevensverwerkende middelen tegen inbreuken van binnenuit of buitenaf bevorderen. Ook willen wij de uitwisseling van kennis en ervaring en het netwerken van de in het vakgebied werkzame personen bevorderen. Bijvoorbeeld door middel van deze expertbrief.

De doelgroep
De doelgroep van het PvIB omvat iedereen, die door studie of beroepshalve te maken heeft met informatiebeveiliging, of hiervoor een bijzondere belangstelling heeft. Het snel groeiende ledenbestand kent vele disciplines zoals studenten, informatiearchitecten, technici, managers, organisatieadviseurs, juristen, beveiligingsfunctionarissen en IT auditors. Onze leden komen voort uit alle mogelijke opleidingen, bedrijven, overheden, organisaties en leveranciers.

Voor de diverse soorten van lidmaatschap verwijzen wij u gaarne naar:

https://www.pvib.nl/abonnementsinformatie