

# **Naar een Belgische Strategie voor Informatiebeveiliging**

Door particuliere verenigingen en academici

September 2008

## Ondertekenende organisaties



### Redacteuren van dit document:

Marijke De Soete	Vicevoorzitter ISO/IEC JTC1 SC27, Lid van de Raad van Bestuur van LSEC
Bart Preneel	Professor K.U. Leuven, ESAT/COSIC, Voorzitter Raad van Bestuur LSEC, ISO-IEC/SC27 Belgian Shadow Committee
Georges Ataya	VP international ISACA and ITGI, Professor aan de Solvay Business School
Ulrich Seldeslachts	CEO LSEC
Bart Moerman	Voorzitter, ISSA Brussels European Chapter
Alain De Greve	ISO/IEC JTC1 SC27 Belgian Shadow Committee (coördinator wg1/wg4 – 27000 series)
Jean-Luc Allard	Vicevoorzitter Information Security – ISACA Belgium, ISO/IEC JTC1 SC27 Belgian Shadow Committee (coördinator wg3)
Thierry Villers	Directeur INFOPOLE Cluster TIC
Gautier Dallons	Coordinator van de Team en R&D Project leader, CETIC

### Revisoren van dit document:

Dany Van de Ven,	Brigade-generaal e.r., Director Agoria/BSDI
...	

# Naar een Belgische Strategie voor Informatiebeveiliging

Versie 2

## Inleiding

Dit witboek is ontstaan naar aanleiding van de vaststelling door onze oprichtende organisaties (vzw's rechtstreeks betrokken bij informatiebeveiliging in alle economische sectoren) dat de bestaande initiatieven inzake informatiebeveiliging nood hadden aan promotie, sensibilisering en een betere coördinatie.

De volgende organisaties hebben dit document ondertekend:

- Belgische deskundigen actief binnen ISO/IEC JTC1 SC27, een internationaal comité voor normalisatie van informatiebeveiligingstechnieken, daaronder begrepen ISMS-aspecten (Information Security Management System).
- CETIC
- INFOPOLE Cluster TIC
- de Belgische Afdeling van ISACA
- de Brussels-Europese Afdeling van ISSA
- K.U. Leuven, ESAT/COSIC
- LSEC (Leaders in Security)
- Solvay Business School

Deze ondertekenende organisaties vertegenwoordigen meer dan 3.000 Belgische informatiebeveiligingsactoren uit meer dan 500 particuliere, openbare en onderzoeksorganisaties.

Wat informatiebeveiliging in België betreft, hebben de ondertekenende organisaties een aantal problemen en tekortkomingen vastgesteld bij de structuur, de regelgeving, het onderwijs en de communicatie bij bedreigingen of in crisissituaties. Uit de talrijke internationale contacten die de organisaties hebben gehad tijdens hun business- en netwerkactiviteiten is gebleken dat België op het vlak van Informatiebeveiliging achteroploopt in vergelijking met de meeste andere Europese landen. Op bepaalde gebieden staat België zelfs minder ver dan sommige Oost-Europese landen. Nochtans staan onze nationale experts wereldwijd hoog aangeschreven; deze tekortkomingen zijn met andere woorden niet te wijten aan een gebrek aan kennis of knowhow.

De huidige initiatieven van de regering en het parlement, zoals de Kamercommissie voor infrastructuur en het Ministeriële Comité voor Inlichting en Veiligheid (de grondlegger van BeNIS, het Belgian Network Information Security platform), tonen aan dat de autoriteiten ook hebben ingezien dat de federale (en regionale) overheden nood hebben aan betrouwbare informatiebeveiliging.

De ondertekenende organisaties hebben zes strategische doelstellingen geïdentificeerd. Deze moeten gerealiseerd worden indien men de informatiebeveiliging wenst te verbeteren. Op deze doelstellingen wordt nader ingegaan in dit document. België heeft er alle baat bij deze doelstellingen te verwezenlijken.

## Achtergrond

Onze maatschappij hangt sterk af van informatie en informatieprocessen. Beiden moeten aan een opgelegd kwaliteitsniveau voldoen als men wil dat het maatschappelijke verkeer vlot verloopt. Informatiebeveiliging betekent dat dit kwaliteitsniveau niet in het gedrang mag komen door onaanvaardbare risico's. Deze informatieprocessen worden heden ten dage ondersteund door Informatie- en Communicatietechnologieën (ICT), met als doel deze betrouwbaarder en efficiënter te maken. Teneinde onze informatiebeveiliging te verbeteren, moeten specifieke doelstellingen worden vastgesteld. Hoe deze doelstellingen verwezenlijkt moeten worden, hangt echter af van het specifieke domein waarin men zich begeeft.

ICT-systemen zijn almaar sterker aanwezig in onze samenleving: de meeste burgers en organisaties worden steeds meer afhankelijk van allerhande ICT-diensten en – toepassingen. Dit heeft een impact op alle economische actoren, met inbegrip van de overheden en kritieke infrastructuren (vb. energie, vervoer, volksgezondheid, telecommunicatie). Deze nieuwe omgeving brengt ook nieuwe risico's met zich mee: van overal ter wereld kan iemand geautomatiseerde, grootschalige aanvallen uitvoeren op deze ICT-systemen. Voorbeelden hiervan zijn aanvallen tegen individuele personen (vb. virus, spam), *denial of service*-aanvallen tegen landen (vb. tegen Estland in 2007 [1]), economische en industriële spionage (vb. aantijgingen dat China zich ongeoorloofd toegang zou verschaffen tot de nationale systemen van de Europese landen [2]) en fraude (vb. banksector [3]).

De afgelopen twee decennia is veel geïnvesteerd in onderzoek, ontwikkeling, implementatie en auditing, waardoor wij beter beschermd zijn tegen een aantal van deze dreigingen. Desalniettemin blijkt uit de talrijke incidenten dat de globale Informatiebeveiliging er niet echt op vooruitgaat. Hier zijn verschillende redenen voor:

- 1) Onze informatiesystemen evolueren zeer snel en worden almaar complexer (onze computers, die uit honderden miljoenen kleine onderdelen bestaan, sluiten wij aan op netwerken die op hun beurt honderden miljoenen computers tellen). Bovendien zijn wij niet zo goed in het beveiligen van complexe systemen, waardoor deze diverse tekortkomingen kunnen vertonen.
- 2) Naarmate almaar meer applicaties online gaan, wordt ook de financiële verleiding groter om cybermisdaden te plegen. Nochtans is het belangrijk op te merken dat dergelijke problemen slechts zelden in het nieuws komen: daders hebben er namelijk alle belang bij om weinig ruchtbaarheid te geven aan hun successen.
- 3) Informatiebeveiliging is een uiterst interdisciplinair gegeven. De ontwikkeling van oplossingen moet dan ook op een geïntegreerde wijze beheerd worden: technologische aspecten en interne en externe regelgeving mogen niet langer los van elkaar behandeld worden. Tevens moet men de menselijke of sociale factoren onderzoeken en deze in overweging nemen. Met andere woorden: de overheid, het bedrijfsleven en onderzoeksinstellingen moeten nauw met elkaar samenwerken als men vooruitgang wil boeken.

Voor de ontwikkeling en toepassing van veilige ICT-systemen zijn een viertal zaken nodig: de uitwerking van normen, de evaluatie van producten of systemen, en coördinatie en handhaving op mondiaal niveau. Hoewel veel van deze vraagstukken op internationaal niveau behandeld moeten worden, is het duidelijk op de nationale overheden een grote gedeelde verantwoordelijkheid rust. In België bestaat er vooralsnog geen agentschap voor

informatiebeveiliging dat aanbevelingen uitbrengt en ondersteuning biedt aan de Belgische overheden, instellingen en organisaties van de verschillende niveaus. De situatie in België staat dan ook in schril contrast met veel andere Europese landen, daaronder begrepen de meeste Oost-Europese landen [zie Bijlage A]. Om deze reden vertonen de thans ondernomen activiteiten een gebrek aan coherentie, compatibiliteit en efficiëntie.

België beschikt evenmin over een regeling voor de certificering van beveiligingsproducten en –diensten. Bij wijze van voorbeeld vermelden wij de regelingen die uitgaan van de Gemeenschappelijke Criteria en toegepast worden door onze buurlanden en landen als Griekenland, Polen en Hongarije [zie Annex B]. Om deze reden kunnen Belgische ondernemingen zeer vaak niet deelnemen aan internationale aanbestedingen. Indien wij alsnog willen deelnemen, moeten wij onze nationale knowhow overdragen aan andere landen. Dat leidt er op zijn beurt weer toe dat banen verloren gaan of bedrijven naar het buitenland trekken.

# Strategische doelstellingen

## 1. Information Security Awareness Forum

Er zou een Belgisch Information Security Awareness Forum moeten worden opgericht. Dit forum kan een platform zijn voor de uitwisseling van informatie over initiatieven inzake informatiebeveiliging en normen en ervaringen met implementatie/certificering, zoals informatiebeveiligingsbeheer, risicobeheer, informatie- en IT-beveiligingstechnieken, enz. Verder zou het een platform kunnen zijn voor communicatie over beveiligingsinitiatieven tussen de nationale overheid en haar instellingen (zoals de federale politie) of Europese organisaties zoals ENISA [4].

In het ideale geval zou dit forum gebaseerd zijn op samenwerking tussen organisaties gespecialiseerd in informatiebeveiliging, zoals de ondertekenende organisaties en de overheid, maar ook de beveiligingssector, de dienstensector en de wereld van het onderwijs en onderzoek.

Een tweede aanbeveling betreft de oprichting van een Belgische denktank over informatiebeveiliging. Deze denktank zou advies kunnen verlenen aan het Belgische Agentschap voor Informatiebeveiliging, waarop verder in dit document wordt ingegaan. Deze denktank zou verbonden kunnen zijn aan het forum.

Het Information Security Awareness Forum zou ook WARP's (Warning, Advice and Reporting Points) over informatiebeveiliging kunnen oprichten, zoals die in het Verenigd Koninkrijk [5] en Nederland [6].

## 2. Normalisatie van informatiebeveiliging

Een aantal minimumvoorschriften voor informatie- en ICT-beveiliging zouden opgenomen moeten worden in de regelgeving van toepassing is op de verschillende sectoren. Deze voorschriften zouden op internationale normen [zie Bijlage C] gebaseerd moeten zijn en betrekking moeten hebben op zaken zoals het beheer van informatiebeveiliging, een controlekader, risicobeheer, incidentbeheer, de continuïteit van zakelijke activiteiten, evaluaties en audits, rapportage en naleving van de voorschriften, enz. Tevens zouden deze vereisten de noodzaak tot accreditatie van kritieke systemen moeten vermelden. Op dit vlak moet de overheid het goede voorbeeld geven aan sectoren en particuliere organisaties die vooralsnog geen accreditaties verlenen voor hun beveiligingsoplossingen.

Evaluatie/certificering is mogelijk dankzij een aantal informatiebeveiligingsnormen. Op dit ogenblik moeten Belgische producenten en organisaties naar het buitenland gaan voor de certificering van hun informatiebeveiligingsproducten en –diensten. Aangezien deze sector almaar professioneler wordt en de vraag naar gecertificeerde producten en diensten steeds blijft toenemen, zou België een eigen certificeringskader voor informatiebeveiligingsdiensten en –producten moeten creëren. Dit kader dient gebaseerd te zijn op de internationale normen en moet overeenstemmen met de Belgische wet- en regelgeving. In dit geval zou de Belgische Accreditatie-instelling (BELAC) moeten instaan voor de accreditatie van deze certificeringsautoriteit en de eventuele evaluatiecentra. Op die manier zou dit overheidsagentschap de vereiste certificeringen van producten en

diensten kunnen afleveren. Het initiatief dat op dit vlak reeds ondernomen werd, moet de nodige steun blijven krijgen teneinde deze doelstellingen te realiseren.

Deze geaccrediteerde certificeringsinstantie zou in het kader van het Common Criteria Recognition Agreement [7] moeten samenwerken met andere nationale certificeringsinstanties in de EU. Op die manier kan men een harmonieus certificeringskader met de andere lidstaten creëren, dat instaat voor de omzetting in de nationale certificeringsprogramma's van normen die via Europese richtlijnen worden opgelegd. Op een grotere schaal (wereldwijd) dient dit orgaan kaderstructuren te creëren voor de wederzijdse erkenning van certificeringen.

De Belgische inspanningen op het vlak van de internationale normalisatie van informatiebeveiliging moeten beter gecoördineerd worden. Hoewel de Belgische experts in deze forums uitstekend werk leveren, levert het Belgische Bureau voor Normalisatie voor geen enkele ondersteuning of erkenning. Deze rol van coördinator zou bijvoorbeeld vervuld kunnen worden door Agoria, dat een enig contactpunt voor de ICT-sector zou kunnen vormen ("sectoraal operator"). Deze gecoördineerde activiteiten dienen onder het toezicht te staan van het Ministerie van Economische Zaken en het Departement Wetenschapsbeleid.

### **3. Onderwijs, opleiding en onderzoek**

Er bestaat een dringende noodzaak tot coördinatie van de onderwijs-, opleidings- en onderzoeksinitiatieven genomen op het vlak van informatiebeveiliging. In België organiseren verschillende universiteitsgroeperingen en -colleges hun eigen programma's, waardoor de curricula sterk van elkaar verschillen. Er dient minstens een gemeenschappelijke basis te worden vastgesteld en bevorderd.

Er moet een onderzoeksplatform voor informatiebeveiliging worden opgericht en bevorderd (zie voorbeelden in Nederland [8] en Frankrijk [9]). Dit platform zou de vooropgestelde resultaten in het kader van de voormelde strategische doelstellingen in acht moeten nemen.

### **4. Kritieke infrastructuur en CERT**

Er moeten een Belgisch plan en een tijdpad uitgewerkt worden voor de bescherming van onze kritieke infrastructuren. Dit dient te gebeuren in samenwerking met de sector en met andere Europese landen. Dit plan en dit tijdpad moeten afgestemd zijn op het Europees Kader dat thans wordt uitgewerkt via het bijzonder Europees Programma. De kritieke infrastructuren omvatten energie, vervoer en gezondheidszorg (deze worden reeds als prioritair beschouwd), maar ook financiën, voedselvoorziening, water, gevaarlijke stoffen, telecommunicatie en bestuur [10].

Dit tijdpad moet tevens de geplande ontwikkeling steunen van de specifieke ISO ISMS-normen betreffende de informatiebeveiligingsaspecten van kritieke infrastructuur.

De Belgische overheid dient haar plannen voor de uitwerking van een beperkt crisisplan te versnellen. Dit plan kan later verder worden aangevuld met uitgebreidere scenario's en input van de sector.

Er moet snel een Belgisch CERT (Computer Emergency Response Team) [11], [12] worden opgericht. Dit CERT moet instaan voor de bescherming van de Belgische Internetinfrastructuur en voor de coördinatie van de bescherming tegen en antwoorden op internetaanvallen op het hele grondgebied. Dit alles dient te gebeuren in nauwe samenwerking met de sector. Er moet dan ook worden voortgebouwd op de in de sector aanwezige knowhow. Wij bevelen ten eerste aan om samen te werken met BELNET en voort te bouwen op eerder genomen initiatieven in verschillende sectoren (vb. financiële sector). Daarnaast bevelen wij aan deze activiteiten te coördineren met ECSA ([www.ecsa-eu.org](http://www.ecsa-eu.org)) en CFS-CSF ([www.csf-cfs.be](http://www.csf-cfs.be)).

De wet betreffende elektronische communicatie (Wet van 13 juni 2005, art. 113 en 114) is onduidelijk over de operationele rol van het BIPT/IBPT met betrekking tot het nationaal CERT. Door deze onduidelijkheid loopt men het risico dat niets ondernomen wordt.

## **5. Wetten en regelgeving**

Verschillende Belgische wetten inzake IT- en informatiebeveiliging (vb. wet over cryptografie, computercriminaliteit, enz.) moeten opnieuw bekeken worden. Op zijn minst moeten de wetten inzake computercriminaliteit en bescherming van de persoonlijke levenssfeer herbekeken worden, zodat de daarin opgenomen doelstellingen ondubbelzinnig zijn en niet voor verschillende interpretaties vatbaar. Bijvoorbeeld: ondernemingen die penetratietests aanbieden zouden misschien een speciaal statuut moeten krijgen. De rol van gerechtelijke deskundigen bij vraagstukken betreffende informatiebeveiliging moet tevens beter gedefinieerd worden, en hun bijdragen beoordeeld.

Er bestaat een acute nood aan regelgeving op het vlak van de privacyaspecten [13] van nieuwe technologieën, zoals de elektronische identiteit, de technologieën om burgers te lokaliseren en biometrie. De overheid moet deze vraagstukken op passende wijze aanpakken. De mate waarin organisaties uiteindelijk de wetgeving inzake de bescherming van de persoonlijke levenssfeer zullen naleven, hangt af van hoe nauwkeurig deze wet geformuleerd wordt. Te vage terminologie en voorschriften leiden tot een slechte naleving van de wet.

Een toereikende coördinatie en volledige samenwerking tussen het Belgische Agentschap voor Informatiebeveiliging en de Commissie voor de bescherming van de persoonlijke levenssfeer is van vitaal belang. Het Belgische Agentschap voor Informatiebeveiliging, waarvan de oprichting hieronder wordt voorgesteld, zou de Belgische overheid moeten adviseren over hoe zij een juridisch kader best kan oprichten en in stand houden. De daaruit voortvloeiende wetgeving dient overeen te stemmen met de wetgeving en regelgeving inzake informatiebeveiliging en moet rekening houden met de uitgebreide bestaande knowhow inzake informatiebeveiliging in België.

De voormelde doelstellingen zullen enkel efficiënt gecoördineerd kunnen worden indien een gecentraliseerde strategie wordt uitgewerkt. Dit vereist een zesde doelstelling.

## **6. Belgisch Agentschap voor Informatiebeveiliging**

Er zou een Belgisch overheidsagentschap voor Informatiebeveiliging moeten worden opgericht (zoals het BSI in Duitsland). Dit agentschap moet verantwoordelijk zijn voor de beslissingen over het informatiebeveiligingsbeleid en –strategie in België en moet nauw samenwerken met de sector en andere gouvernementele departementen. Daarnaast moet het de standaarden/normen inzake informatiebeveiliging vaststellen waaraan de overheid en haar (dienst)verleners zich dienen te houden.

De expertise van het BIPT/IBPT of een ander geschikt federaal agentschap zou nuttig kunnen zijn bij de oprichting van dit agentschap. Daarnaast moet echter ook een onafhankelijk comité worden opgericht waarin een aantal particuliere Belgische informatiebeveiligingsdeskundigen zetelen (zowel beroepsbeoefenaars als onderzoekers). Waar nodig, kan dit comité uitgaan van de ervaringen van onze buurlanden en ENISA. De strategie moet gericht zijn op een Europees Kader en rechtstreeks verbonden zijn met Europese organisaties zoals ENISA, evenals met nationale instanties en agentschappen van andere Europese landen.

Het Agentschap voor Informatiebeveiliging moet opgericht worden door de federale overheid, zodat het weliswaar onafhankelijk is van de betrokken openbare entiteiten (BIPT-IBPT, NVO/ANS, enz.), maar toch aan hen verbonden is. Het Agentschap moet alle betrokken partijen van de overheden (federaal niveau, gemeenschappen en gewesten) bij elkaar brengen om samen met de sector een tijdpad vast te leggen voor informatiebeveiliging. Daarnaast moet het de overheidsdiensten, de federale staat en de Gewesten een duidelijke toekomstvisie verschaffen.

Dit Agentschap moet instaan voor de coördinatie met alle Belgische instanties die zich toeleggen op het onderzoek naar informatiebeveiliging.

Het Agentschap moet de vertegenwoordiging van België coördineren in alle internationale groepen waar België op grond van nationale belangen aanwezig dient te zijn.

De ondertekenende organisaties zijn bereid de rol van deze voorgestelde onafhankelijke Belgische deskundigengroep voor informatiebeveiliging waar te nemen totdat deze officieel is opgericht.

## **Conclusie**

De ondertekenende organisaties roepen de Belgische regering op de relevante belanghebbende partijen dringend actie te laten ondernemen, teneinde de voormelde strategische doelstellingen te verwezenlijken.

De ondertekenende organisaties zijn bereid zich hiervoor in te zetten en hun verantwoordelijkheid op te nemen, teneinde de kwaliteit van de informatiebeveiliging in België op te tillen tot een gepast niveau.

Meer informatie over dit document kan bij onderstaande vertegenwoordigers van de ondertekenende organisaties verkregen worden: Jean-Luc Allard (ISACA) en Bart Moerman (ISSA).

## Referenties:

- CAWET Werkgroep 55: Beveiliging van Digitale Informatie, 26 oktober 2007, <http://www.kvab.be/downloads/CAWET/beveiliging%20van%20digitale%20informatie.pdf>
- “Voor een nationaal beleid van de informatieveiligheid”, *White Paper* opgesteld door het overlegplatform voor de informatieveiligheid (BeNIS)
- DOC 52 0898/001, Chambre 2e Session de la 52e Législature - Kamer 2de Zitting van de 52ste Zittingperiode 2007-2008, Commissie voor de infrastructuur, het verkeer en de overheidsbedrijven, uitgebracht door de Heer Roel Deseyn.

### Achtergrond:

#### [1] Aanvallen: Estland

- Assessing the Cyber Security Threat (SDA Monthly Roundtable), A Security & Defence Agenda Rapporteur: John Chapman, Publicatiejaar: 2008, Solvay Bibliotheek, Brussel

#### [2] Aanvallen: China (vermeende aanval)

- Belgische Kamer van Volksvertegenwoordigers – Chambre des Représentants de Belgique
  - CRIV 52 PLEN 035 – Plenumvergadering/Séance plénière donderdag/jeudi 08-05-2008 (pm)
- CRABV 52 COM 209 – Commissie voor Landsverdediging/Commission de la Défense Nationale: woensdag mercredi 14-05-2008 (avond/soir)

#### [3] Money mules in de banksector:

[http://www.ecp.nl/nieuws/id=101482/Banken\\_pakken\\_money\\_mules\\_aan\\_met\\_start\\_campagne.html](http://www.ecp.nl/nieuws/id=101482/Banken_pakken_money_mules_aan_met_start_campagne.html)

### Information Security Awareness Forum

#### [4] referentie van ENISA naar Information Security Awareness:

[www.enisa.europa.eu/pages/ENISA\\_Working\\_Group\\_on\\_Awareness\\_Raising.htm](http://www.enisa.europa.eu/pages/ENISA_Working_Group_on_Awareness_Raising.htm)

- [5] WARP in het VK: [www.warp.gov.uk](http://www.warp.gov.uk)
- [6] WARP in Nederland: [www.onderwijswarp.nl](http://www.onderwijswarp.nl), [www.ictu.nl](http://www.ictu.nl) (NICC) en [www.samentegencybercrime.nl](http://www.samentegencybercrime.nl)

### Normalisatie van Informatiebeveiliging

[7] Voor de CCRA: <http://www.commoncriteriaportal.org/members.html>

### Onderwijs en onderzoek

[8] Voorbeelden in Nederland: Veilig Verbonden: [http://www.ictregie.nl/iip/pdf\\_pagina.php?pageId=34](http://www.ictregie.nl/iip/pdf_pagina.php?pageId=34)

[9] Voorbeelden in Frankrijk: ANR programme Sécurité et Sûreté Informatique

### Kritieke Infrastructuur, CERT, CSIRT

[10] Kritieke infrastructuren: <http://europa.eu/scadplus/leg/en/lvb/l33259.htm>

[11] Voor een volledig overzicht van de huidige situatie van CERT's in Europa:

[http://www.enisa.europa.eu/cert\\_inventory/index\\_inventory.htm](http://www.enisa.europa.eu/cert_inventory/index_inventory.htm)

### Gattiker, CyTRAP Labs

(<http://papers.weburb.dk/frame.php?loc=archive/00000149/>)

## Wetgeving & Regelgeving

### [13] Aanbevelingen i.v.m. privacyaspecten:

- [http://ec.europa.eu/justice\\_home/fsj/privacy/docs/lawreport/walrave\\_en.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/lawreport/walrave_en.pdf)
- [http://www.enisa.europa.eu/doc/pdf/Country\\_Pages/Belgium.pdf](http://www.enisa.europa.eu/doc/pdf/Country_Pages/Belgium.pdf)

## Bijlage A

### Lijst van nationale informatiebeveiligingsinstanties in Europa

*Te vervolledigen met info te bezorgen door DCSSI*

Sommige onderstaande instanties maken deel uit van het Nationaal Agentschap voor Veiligheid, anderen niet.

Spanje	CNI	<a href="http://www.cni.es">http://www.cni.es</a>
	AISE	
Verenigd Koninkrijk	CESG	<a href="http://www.cesg.gov.uk/">http://www.cesg.gov.uk/</a>
	DCSSI	<a href="http://www.ssi.gouv.fr">http://www.ssi.gouv.fr</a>
	MIVB	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Duitsland	BSI	<a href="http://www.bsi.bund.de">http://www.bsi.bund.de</a>
	Information Board	....
Polen	ABW	<a href="http://www.abw.gov.pl">http://www.abw.gov.pl</a>
	ORNISS	<a href="http://www.orniss.ro">http://www.orniss.ro</a>
	Utrikesdepartementet SSSB	...

## Bijlage B

### Lijst van CCRA-lidstaten van de CCRA (Common Criteria Recognition Agreement)

#### Europa:

Zweden, Spanje, Noorwegen, Nederland, Italië, Hongarije, Griekenland, Duitsland, Frankrijk, Denemarken, Tsjechië, Oostenrijk, Verenigd Koninkrijk, Finland.

#### Wereld:

VS, Turkije, Singapore, Maleisië, Zuid-Korea, Japan, Israël, India, Canada, Australië en Nieuw-Zeeland (samen).

## Bijlage C

### Lijst van potentiële normen die binnen de Belgische overheid bevorderd kunnen worden

#### ISO

- De volledige ISO/IEC 2700x-reeks (vb. 27001 'ISMS requirements' en 27002 'ISMS Good Practices') en de ISO 2701X-reeks (specifieke toepassingen van 27002, bijv. voor kritieke infrastructuur, e-government, enz.)
- ISO/IEC 15408 (Common Criteria for security evaluation) en hieraan verbonden normen
- ISO/IEC 21827 (System Security Engineering – Capability Maturity Model)

#### ISF

- Standard of Good Practice for Information Security

#### ISACA

- CobiT 4.1

#### ENISA

- [http://www.enisa.europa.eu/rmra/files/D1\\_Inventory\\_of\\_Methods\\_Risk\\_Management\\_Final.pdf](http://www.enisa.europa.eu/rmra/files/D1_Inventory_of_Methods_Risk_Management_Final.pdf)

En tal van andere normen gepubliceerd door nationale instanties (Bijlage A) of nationale normalisatie-instituten (zoals het NIST in de VS).

NIST SP 800 : <http://csrc.nist.gov/publications/PubsSPs.html>

NST FIPS : <http://csrc.nist.gov/publications/PubsFIPS.html>

## Wie zijn wij?

- De Belgische Afdeling van ISACA, een wereldwijde beroepsvereniging die professionals inzake IT Governance ondersteunt d.m.v. onderzoek en cursussen over IT Assurance en IT Audit, IT Governance en Informatiebeveiligingsbeheer. ISACA certificeert informatiebeveiligingsmanagers wereldwijd (meer dan 8.000 gecertificeerde professionals) en is sinds 1986 actief in België. Deze organisatie publiceert regelmatig belangrijke bijdragen en verdeelt deze gratis, teneinde alle betrokken actoren te sensibiliseren voor informatiebeveiliging en goed bestuur.
- De Brussels-Europese Afdeling van ISSA, een wereldwijde beroepsvereniging die ondersteuning biedt op het vlak van veiligheid van informatiesystemen door een platform te zijn voor permanente beroepsopleidingen, sensibilisering en training.
- LSEC (Leaders in Security), een Belgische vzw die ondersteuning biedt aan de Belgische informatiebeveiligingsbranche. Onder haar leden telt LSEC vertegenwoordigers van onderzoeksinstellingen, individuele beroepsbeoefenaars en tal van verschillende ondernemingen.
- INFOPOLE Cluster TIC, het Waalse netwerk van IT-sectoren en onderzoekscentra (particulier en openbaar), waarvan sommigen actief zijn in de beveiligingssector.
- CETIC (Centre d'Excellence en Technologies de l'Information et de la Communication) is actief in toegepast onderzoek naar softwareontwikkeling, GRID-technologieën en elektronische systemen. CETIC is een verbindingsagent voor de overdracht van technologie tussen het universitair onderzoek en het bedrijfsleven.
- K.U. Leuven, ESAT/COSIC, actief in talrijke IT-beveiligingssectoren, organiseert een postgraduaatopleiding over Informatiebeveiliging.
- De Solvay Business School legt het verband tussen technologie en bedrijfsbeheer en organiseert master- en postgraduaatopleidingen in IT Governance en IT Audit and Security.
- Belgische deskundigen betrokken bij ISO/IEC JTC1 SC27, een internationaal normalisatiecomité van informatiebeveiligingstechnieken dat zich toelegt op ISMS (WG1), cryptografische systemen (WG2), evaluaties, certificeringen en assurance (WG3), technologiebeveiliging (WG4) en privacy- en accessbeheer (WG5).