Beware!

Security Awareness voor retail banking in Nederland

Afstudeerthesis
Master of Security in Information Technology
Technische Universiteit Eindhoven

Jasper A. Essers
Juni 2008

Afstudeerbegeleiders: Ing. Bert Snel, dr. Benne de Weger

< this page intentionally left blank >

Inhoudsopgave

< this page intentionally left blank >

Inleiding

Risico's voor de informatiebeveiliging van een organisatie kunnen in belangrijke mate worden verminderd en onder controle gebracht door middel van technische en organisatorische maatregelen. De menselijke factor blijkt echter een zwakke schakel: met kennis van, en inzicht in de organisatie en de gebruikte informatietechnologie kunnen medewerkers, door onwetendheid, onachtzaamheid en onoplettendheid, bewust of onbewust, de risico's vergroten. Het aanscherpen van het interne beleid, met daarbij horende controle en sancties, is onvermijdelijk om medewerkers ervan te doordringen dat de organisatie risicobeheersing serieus neemt. Maar, zoals Furnell, Gennatou en Dowland (2002) verwoorden: '*a security policy can only be effective if staff know, understand and accept the necessary precautions*' (Furnell, Gennatou en Dowland 2002: 352). Het kennen, begrijpen en accepteren van de nodige maatregelen vraagt om een besef binnen de organisatie en bij zijn medewerkers dat het terugbrengen van risico's daadwerkelijk belangrijk is. Dit besef, ofwel *security awareness*, ontstaat niet vanzelf, maar moet worden ontwikkeld en onderhouden. Security awareness gaat verder dan alleen het acteren op incidenten, maar zal geborgd moeten zijn in een continu proces waarin een organisatie risico's kan terugbrengen tot een acceptabel niveau.

Binnen de Nederlandse *retail banking* sector, een doelgroep waarbinnen informatiebeveiliging topprioriteit heeft, is security awareness vanuit de wet- en regelgeving verplicht. De bestaande normenkaders bevatten enkel een verwijzing naar *goed huisvaderschap*, maar geen verwijzing naar exacte methodieken en normen op het gebied van security awareness of een op de doelgroep toegespitste methode om de normen te ontwikkelen.

Gezien het ontbreken van een exacte methodiek voor security awareness binnen de Nederlandse retail banking sector, is de doelstelling van deze scriptie te komen tot een praktische en minimalistische methode voor deze sector. Het uitgangspunt is dat met dit systeem kosteneffectief aan de regels en wetgeving voldaan kan worden en dat daarbij het vertrouwen in de integriteit van de organisatie versterkt kan worden. Hierbij is belangrijk dat de methodiek meetinstrumenten bevat die ervoor kunnen zorgen dat er een optimale balans is tussen de kosten en baten. Daarnaast is het meten relevant ten behoeve van het opleveren van verantwoording aan het management.

Inkadering en vraagstelling

Het wetenschappelijke veld van informatiebeveiliging is interdisciplinair, bestaande uit technologische, economische, financiële, juridische, beleidskundige, psychologische en socio-culturele componenten. Binnen het deelgebied van security awareness ligt de focus op de menselijke factor, zodoende speelt (organisatie-) psychologie een belangrijke rol in de inkadering van deze scriptie. Een belangrijke theoretische propositie is hierbij dat mensen op twee manieren omgaan met informatie betreffende gewenst gedrag, te weten oppervlakkig en systematisch. 'When people engage in *superficial processing*, they rely on accessible or salient information to make rather simple inferences about the attitude object. When people engage in *systematic processing*, they go beyond simple cues and also consider the strength of the arguments and their implications for the evaluation of the attitude object' (Smith en Mackie 2000: 255). Wanneer medewerkers een meer systematische verwerking wordt aangeboden, wordt er verondersteld dat de gewenste gedragsverandering meer structureel kan worden bewerkstelligd: 'When people pay attention to a message, understand its content, and react favorably to it, persuasion occurs. Attitudes resulting from such careful consideration are much more resistant to later change than most attitudes produced by superficial processing' (ibid.: 264).

Informatiebeveiliging is een toegepaste wetenschap. Zodoende kan security awareness niet enkel vanuit de theorie bekeken worden. In retail banking moet er aan de wet- en regelgeving die geldt voor financiële instellingen, voldaan worden. Daarnaast beoogt iedere organisatie doeltreffend en kosteneffectief te opereren. Het continue bestendigen van het vertrouwen dat consumenten hebben in de organisatie, is tevens van groot belang voor deze specifieke sector: in retail banking is vertrouwen het product dat wordt verkocht. Een methodiek voor security awareness zal dan ook aan deze randvoorwaarden moeten voldoen.

Aangezien er door de prudentieel toezichthouder in Nederland geen concrete eisen gesteld worden aan de invulling tot de plicht voor goed huisvaderschap, wordt er in deze scriptie beoogd een antwoord te vinden op de volgende vraagstelling:

In hoeverre is het mogelijk te komen tot een praktische en minimalistische methode voor security awareness binnen de Nederlandse retail banking?

Om deze hoofdvraag te kunnen beantwoorden, zijn de volgende deelvragen opgesteld:

- Welke eisen stelt de wet- en regelgeving aan instituten in de retail banking op het vlak van security awareness?
- Welke criteria komen uit deze eisen voort?
- Welke criteria zijn er te benoemen ten aanzien effectiviteit en efficiëntie van een awareness programma?
- Welke *key performance indicators* (KPI's) kunnen worden opgesteld, waarbij elke KPI SMART (Specific – Measurable – Achievable – Result-oriented or Relevant – Time-bound) zal moeten zijn?
- Voor welke doelgroepen binnen de organisatie (mits zij afzonderlijk verschillend moeten worden benaderd) zijn de onderscheiden criteria van specifiek belang?
- Welke maatregelen kunnen een security awareness programma vormen, waarbinnen deze criteria worden behandeld?
- In hoevere is er binnen de methode een maturity model te formuleren?

De eerste drie deelvragen zullen in het eerste hoofdstuk worden behandeld. De overige vier vragen komen in het tweede hoofdstuk aan de orde.

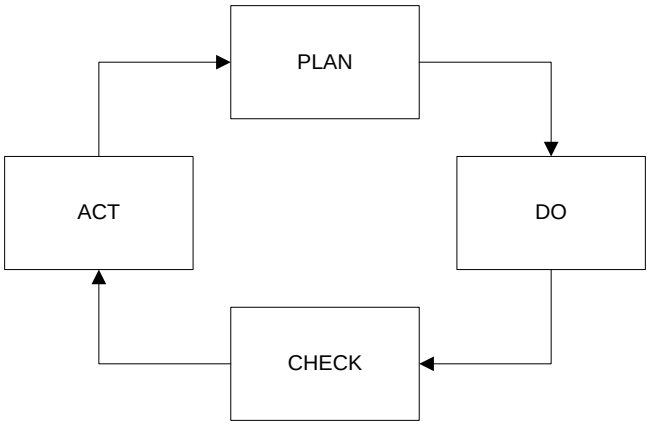
Operationalisatie en methodologie

Onder retail banking wordt de sector verstaan zoals deze is aangeduid in het International Convergence of Capital Measurement and Capital Standards, het zogenoemde Basel II. De indeling van retail banking in Basel II ziet er als volgt uit (Basel Committee on Banking Supervision 2006: 302):

Level 1	Level 2	Activities
Retail Banking	Retail Banking	Retail lending and deposits, banking services, trust and estates
	Private Banking	Private lending and deposits, banking services, trust and estates, investment advice
	Card Services	Merchant/commercial/corporate cards, private labels and retail

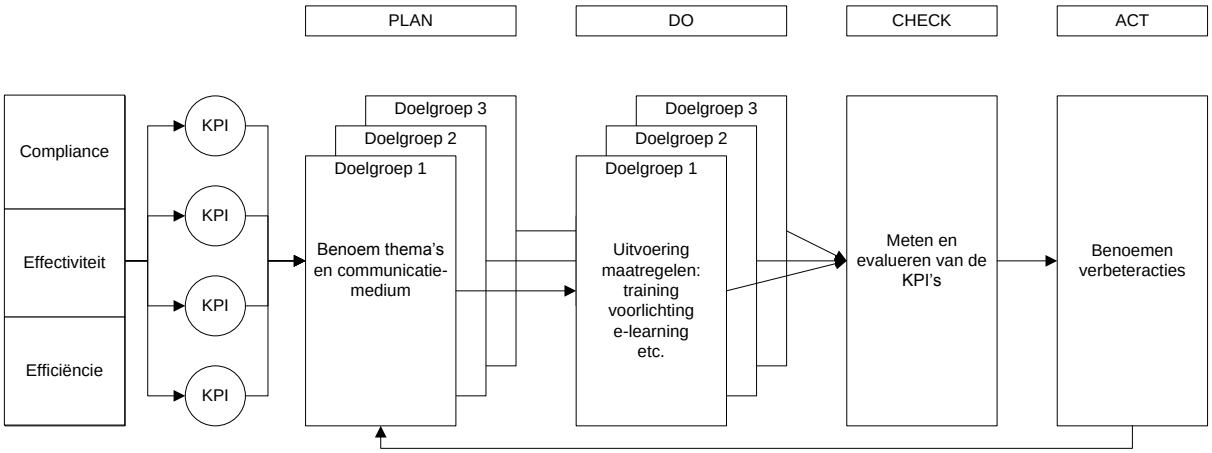
Onder het begrip security awareness wordt over het algemeen verstaan dat de medewerkers van een organisatie het besef hebben dat elementen binnen en buiten de betreffende organisatie er op uit zouden kunnen zijn oneigenlijk gebruik te maken van informatie welke eigendom is van de organisatie. De Engelse term security awareness wordt vaker gebruikt dan het Nederlandse synoniem beveilingsbewustzijn, en zal om deze reden in deze scriptie gebruikt worden.

De kern van de probleemstelling is te komen tot een praktische en minimalistische methode. In deze scriptie wordt deze methode benaderd vanuit de Deming-cyclus (ofwel PDCA-cyclus), een bekende systematiek voor continue kwaliteitsverbetering. Deze systematiek werd in 1986 beschreven door de Amerikaan W. Edwards Deming. Binnen de Deming-cyclys worden vier fasen onderscheiden: Plan-Do-Check-Act (PDCA).



In de Plan-fase worden kwaliteitsverbeteringen pro-actief benaderd, doordat er een plan of planning wordt opgesteld om op de verwachte veranderingen in te spelen. Dit plan (of planning) vormt de basis voor de tweede fase, de Do-fase. In de Do-fase wordt het plan stapsgewijs en gecontroleerd uitgevoerd. In de Check-fase wordt het plan geevalueerd: de resultaten worden bekeken en geanalyseerd. Daarnaast worden nodige of mogelijke verbeteringen benoemd. In de laatste fase, de Act-fase, wordt op grond van de evaluaties uit de Check-fase actie ondernomen om het proces te verbeteren. De Deming-cyclus beschrijft een proces van continue verbeteringen, zodoende gaat na de Act-fase weer een Plan-fase van start, waarbinnen nieuwe verbeteringen worden geformuleerd en gepland.

Voor het proces van security awareness kunnen de fasen van de Deming-cyclus specifiek worden ingevuld. Het onderstaande diagram geeft de stappen en de relaties tussen de procescomponenten weer, en vormt daarmee de basis van de in deze scriptie gepresenteerde methodiek.



De basis van de methodiek wordt gevormd door drie pijlers: Compliance, Effectiviteit en Efficiëntie. Vanuit deze pijlers worden key performance indicators (KPI's) afgeleid. Voor de evaluatie van deze KPI's is er in deze scriptie gekozen om gebruik te maken van het concept Six Sigma. De methode van Six Sigma is eind jaren tachtig ontwikkeld door het Japanse Motorola. Six Sigma is gebaseerd op de DMAIC-aanpak (Define, Measure, Analyse, Improve en Control), en daarmee een variatie op de Deming-cyclus. Volgens De Mast en Does (2005) is deze aanpak dan ook niet nieuw, maar verenigt het innovaties op het gebied van kwaliteitsverbetering. Een belangrijk element van Six Sigma is dat medewerkers (zogenaamde black belts) worden getraind om met adequate procedures relevante data te verzamelen en te analyseren. De Mast en Does stellen: 'Bovendien plaatst Six Sigma, beter dan eerdere initiatieven als TQM, kwaliteits- en efficiëntieverbetering in een bedrijfseconomische context, en maakt aldus de kloof tussen technisch georienteerde procesmensen en financieel georienteerde managers kleiner' (De Mast en Does 2005: 29).

In de systematische benadering voor dataverzameling en -analyse van Six Sigma speelt statistiek een grote rol. De term Six Sigma is gebaseerd op de griekse letter sigma (σ) welke in de statistiek wordt gebruikt om de spreiding binnen een populatie aan te duiden. De sigma is de standaarddeviatie, en geeft de afwijking ten aanzien van het gemiddelde of de streefwaarde weer. Six Sigma geeft een statistische weergave van de proceskwaliteit. Met sigma wordt het niveau van het aantal incidenten binnen een organisatie aangeduid. Met een niveau van 6 (six sigma) ligt het aantal op ongeveer 3,4 incidenten per miljoen en heeft de notatie 'world-class performance' (ReVelle 2004: 39). Met Six Sigma kan voor een bepaald proces binnen de organisatie het aantal incidenten worden vastgesteld, en op grond daarvan kan het aantal per miljoen worden berekend en kan de organisatie het kwaliteitsniveau van het proces vaststellen. Doordat het aantal incidenten inzichtelijk wordt gemaakt, kan er specifiek worden onderzocht hoe dit kan worden teruggebracht. Daarnaast is Six Sigma een manier voor benchmarking.

De toepassing van Six Sigma binnen deze scriptie zal nader beschouwd worden bij de beschrijving van de methodiek voor een awareness programma.

Om te komen tot een methodiek voor een awareness programma, is er een literatuuronderzoek uitgevoerd. Voor de belangrijkste criteria die de basis vormen voor de pijler compliance, is er gekeken naar relevante wetteksten, regelingen en (internationale) richtlijnen en normenkaders. Voor de criteria welke betrekking hebben op de pijlers effectiviteit en efficiëntie, alsook voor de ontwikkeling van de methodiek is gebruik gemaakt van literatuur op het gebied van security awareness.

Hoofdstukindeling

Deze scriptie is opgedeeld in twee hoofdstukken. In het eerste hoofdstuk zal aandacht worden besteed aan de onderbouwing van een awareness programma voor de retail banking. Het beoogt de eerste drie deelvragen te beantwoorden, en daarmee weer te geven waarom een awareness programma relevant is voor de sector. De drie pijlers -compliance, effectiviteit en efficiëntie- vormen hierin de basis. In het tweede hoofdstuk wordt de methodiek van het awareness programma ontwikkeld en uitwerkt, waarmee de overige vier deelvragen beantwoord zullen worden. Hierin wordt gesteld hoe een awareness programma voor de retail banking vorm kan worden gegeven. De scriptie wordt afgesloten met een conclusie, waarin de belangrijkste bevindingen worden samengevat en aanbevelingen worden gedaan.

Onderbouwing van een awareness programma

In dit hoofdstuk zal onderzocht worden welke thema's in een awareness programma aan bod dienen te komen. Deze thema's zijn gestoeld op drie pijlers, te weten: compliance, effectiviteit en efficiëntie.

Om te komen tot een minimalistische methodiek, zal de methodiek gestoeld zijn op het minimaal noodzakelijke, wat inhoudt het voldoen aan wet- en regelgeving (compliance). Daartoe is het ten eerste noodzakelijk om naar normen en waarden, en de wet- en regelgeving te kijken welke de handhaving van een security awareness programma gewenst en/of verplicht maken. Uit de betreffende wet- en regelteksten zullen criteria worden afgeleid, die in een kader onder elke tekst worden weergegeven. Vervolgens wordt gekeken naar de jurisprudentie betreffende security awareness. Om te komen tot een praktische methodiek, zal de methodiek gericht zijn op optimalisatie, wat inhoudt dat gestreefd wordt naar een juiste balans tussen effectiviteit en efficiëntie. Daartoe zullen er voor zowel de pijler effectiviteit als de pijler efficiëntie criteria worden afgeleid welke van belang zijn voor een doeltreffend en doelmatig awareness programma. Tenslotte worden de criteria gepresenteerd in een samenvattende tabel.

Pijler I: Compliance

Normen en waarden

Een belangrijk aspect voor security awareness bestaat uit de onderwerpen gedistilleerd uit de normen en waarden afkomstig uit de gedragscode van de organisatie. Binnen de bancaire sector is het hebben van een gedragscode gemeengoed, omwille van de vele normenkaders die dit vereisen (PCI-DSS, ISO 27001, etc.). Eventueel kan de gedragscode aangevuld worden met de protocollen die er gelden voor het gebruik van de bedrijfsgoederen zoals printers en de internetverbinding.
Bij het opstellen van de gedragscode dient rekening gehouden te worden met de minimale standaardvereiste aan het gedrag. Deze minimale standaard kan bepaald worden aan de hand van de volgende bronnen:

- De ethiek van de organisatie – Het gaat hier om het uitdragen van een bepaald imago, bijvoorbeel ecologisch bewust, lean and mean, een specifieke dresscode, etc. Dit beeld dient versterkt te worden door ondersteunende gedragsregels te onderkennen, waarmee de organisatie zijn ethiek uitdraagt. Doorgaans wordt er in de gedragscode ook een sanctiebeleid benoemd dat aangeeft dat de organisatie zijn regels serieus neemt.
- Gedrag vereist vanuit derden – Grote credit card scheme's zoals MasterCard en VISA, maar ook leveranciers en licentieverleners, kunnen regels ten aanzien van moreel gedrag hanteren die strenger zijn dan de lokale wetgeving. Een voorbeeld hiervan is de regel voor credit card acquiring organisaties ten aanzien van merchants welke bepaalde type on-line content aanbieden die op zedelijk vlak onacceptabel wordt geacht door de licentieverlener.
- Wet- en regelgeving – Relevant zijn hier lokale en internationale wetgeving, regels en normenkaders.

De compliance criteria die uit de eerste twee bronnen voortkomen wisselen sterk per organisatie. Deze kunnen zodoende niet universeel benoemd worden. Wet- en regelgeving is wel breed te benoemen voor organisaties binnen de retail banking. De relevante wet- en regelgeving zal hieronder besproken worden.

Compliance Criteria	
1.	Regels vereist vanuit derden dienen opgenomen te zijn binnen het awareness programma
2.	De interne regels, zoals die uit een gedragscode, dienen opgenomen te zijn binnen het awareness programma

Wet- en regelgeving

De volgende wet- en regelgeving is van toepassing binnen de kaders van deze scriptie:

- Regeling Organisatie en Beheersing (ROB)
- Wet Financieel Toezicht (WFT)
- Payment Card Industry - Data Security Standard (PCI-DSS)
- ISO/IEC 17799:2005
- Wet Bescherming Persoonsgegevens (WBP)
- Directive 95/46/EC
- Code Tabaksblat
- Basel II / Core Principles for Systemically Important Payment Systems

Voor bepaalde branches binnen de retail banking kan aanvullende wet- en regelgeving gelden, deze meer specifieke wetten en regels zijn hier buiten beschouwing gelaten. De onderstaande bespreking beoogt niet uitputtend te zijn, maar de meest relevante wet- en regelgeving ten aanzien van security awareness uit te werken.

Regeling Organisatie en Beheersing

In 2001 trad de Regeling Organisatie en Beheersing (ROB) in werking. Deze regeling was van toepassing op alle onder toezicht van de Nederlandsche Bank vallende instellingen. De Nederlandsche Bank heeft deze regeling ontwikkeld om de integriteit van financiële instellingen te waarborgen en richtlijnen en aanbevelingen te benoemen. De regeling onderkent de volgende risicogebieden:

- Kredietrisico
- Marktrisico
- Liquiditeitsrisico
- Operationeel Risico
- Informatietechnologie (IT)
- Uitbesteding van (delen van) bedrijfsprocessen
- Integriteitsrisico
- Rechten en plichten van potentiële cliënten

Ten aanzien van security awareness zijn binnen de ROB artikel 7, artikel 57, artikel 65 en artikel 67 van toepassing:

> **Artikel 7**
> **De instelling beschikt over helder geformuleerde beleidsuitgangspunten die gericht zijn op risicobeheersing en integer handelen.**
> Ter uitvoering van haar doelstellingen en strategie dient de instelling heldere beleidsuitgangspunten te formuleren die gericht zijn op de realisatie van een beheerste en integere bedrijfsvoering. Hieraan ten grondslag ligt de bevordering van een bedrijfscultuur waarin risicobeheersing en integer handelen zijn ingebed.
> [...]
>
> **Artikel 57**
> **De instelling draagt zorg voor specifieke maatregelen die een afdoende beveiliging van de informatie en de continuiteit van de IT waarborgen. De rechtszekerheid en de privacy van de cliënten dienen bij gebruikmaking van IT-toepassingen in voldoende mate te zijn gewaarborgd.**

Specifieke maatregelen met betrekking tot beveiliging van informatie dienen het exclusiviteits- en integriteitsrisico in voldoende mate te beperken.
Het belang van een toereikende beveiliging is groter naarmate de IT van de instelling door middel van netwerken is verbonden met de buitenwereld. Dit brengt risico's met zich mee zoals het onderscheppen en manipuleren van berichten en documenten, alsmede ongeautoriseerde toegang tot de IT-omgeving, waartegen de instelling afdoende maatregelen dient te treffen. Voorts behoeft in dat kader de handhaving van de privacy van cliënten en zijn gegevens bijzondere aandacht.
[...]

Artikel 65

De instelling beschikt over helder geformuleerde beleidsuitgangspunten ter beheersing van integriteitsrisico's en draagt zorg voor een bedrijfscultuur waarin integriteitsnormen en -regels op een hoog niveau staan. De beleidsuitgangspunten worden vastgelegd en gecommuniceerd aan alle relevante geledingen van de instelling.

De beheersing van integriteitsrisico's omvat de bewustwording, bevordering en handhaving van integer handelen binnen alle lagen van de organisatie. Eén van de hulpmiddelen daartoe is een – door het bestuur vast te stellen – beleidsplan, waarin de normen ten aanzien van het omgaan met cliënten en andere externe relaties, het omgaan met informatie, het aangaan van cliëntrelaties, het verrichten van beleggingstransacties in de privé-sfeer en het aanstellen van integer en deskundig personeel aan de orde komen. Daarbij wordt op geïntegreerde wijze aandacht besteed aan de voor de instelling relevante wet- en regelgeving, alsmede het waken voor strafrechtelijke verwijtbare betrokkenheid bij witwassen, actieve betrokkenheid bij ontwijking van fiscale maatregelen, benadeling van cliënten en het gebruik van voorwetenschap. Als voorbeelden van relevante wet- en regelgeving kunnen worden genoemd: de Wet Melding Ongebruikelijke Transacties en de Wet Identificatie bij Financiële dienstverlening, de Richtlijn insiderregeling, de Regeling bestuurderskredieten en de Regeling afgeschermde rekeningen.
Integriteitsnormen en -regels dragen bij aan de vorming van de bedrijfscultuur van de instelling. De bedrijfscultuur is een belangrijke interne omgevingsfactor ter inbedding van integer handelen (en risicobeheersing in het algemeen), wat een wezenlijk aspect van het dagelijks handelen van de medewerkers behoort te zijn.
Het bestuur van de instelling heeft ter zake in haar eigen gedragingen een voorbeeldfunctie te vervullen. Binnen het bestuur dient duidelijk te zijn wie primair verantwoordelijk is voor integriteitsaspecten van de bedrijfsvoering (in overeenstemming met artikel 25).
De raad van commissarissen dient actief betrokken te zijn bij de vaststelling van het integriteitsbeleid en de voorgestelde uitwerking daarvan in normen en regels (in overeenstemming met artikel 29).

Artikel 67

De instelling draagt zorg voor de uitwerking en implementatie van de beleidsuitgangspunten in organisatorische en administratieve procedures en maatregelen, welke geïntegreerd zijn in de bedrijfsprocessen en die bijdragen aan een integriteitsbewuste bedrijfscultuur.

Voor zover noodzakelijk worden de verschillende aspecten van het in artikel 65 genoemde beleidsplan nader te worden uitgewerkt in interne richtlijnen (o.a. handboeken en gedragscodes). Ook het uitgeven van voorlichtingsbrochures voor personeel en cliënten kan een bijdrage leveren. Met het oog hierop kan het maken van onderscheid tussen algemene normen voor alle medewerkers en regels die slechts op specifieke groepen medewerkers van toepassing zijn de duidelijkheid en transparantie bevorderen.
Adequate procedures en maatregelen voorzien er tevens in dat (wijzigingen in) de richtlijnen en rapportagevoorschriften van financiële toezichthouders bij de betrokken medewerkers bekend zijn.
De onder artikel 69 genoemde 'compliance'-functie kan een nuttige rol vervullen bij de formulering van de interne regelgeving, bij de communicatie daarvan binnen de organisatie middels trainingen en als vraagbaak ter zake van de interpretatie van de interne regelgeving.

> Bij het ter beschikking stellen van personeel en budgetten dient voldoende oog te zijn voor de implementatie van integriteitsbevorderende maatregelen.

De ROB is principle-based: organisatie en medewerkers handelen vanuit de beginselen die de organisatie hanteert. Uit artikel 7 blijkt het integriteit hierin een basisprincipe. Het artikel kent een duidelijke doelstelling ter bestendiging van de integriteitsnormen binnen de bedrijfscultuur. Integriteitsrisico's voor een organisatie worden binnen de ROB geformuleerd als de aantasting van reputatie en de bedreiging van vermogen en resultaat in het kader van ontoereikende compliance. Met ontoereikende compliance wordt gedoeld op:
'een ontoereikende naleving van
- privaat-, bestuurs-, fiscaal- of strafrechtelijke verplichtingen,
- regelgeving en/of rapportagevoorschriften van de toezichthouders,
- door de instelling zelf opgestelde normen, voorschriften of gedragsregels [...].'
(De Nederlandse Bank 2001: 53).

Uit de artikelen blijkt dat er in de ROB een sterke nadruk wordt gelegd op het komen tot en handhaven van een integere bedrijfscultuur, er blijken geen concrete eisen te worden gesteld aan een awareness programma. Artikel 57 geeft weer dat specifieke maatregelen getroffen dienen te worden, ten einde onderschepping en manipulatie van informatie, ongeautoriseerde toegang en aantasting van privacy van cliënten te voorkomen. In de ROB worden de specifieke maatregelen niet expliciet benoemd, er zou gekozen kunnen worden voor technische maatregelen. Deze specifieke maatregelen zouden echter ook binnen een awareness programma vorm kunnen krijgen, bijvoorbeeld door middel van training en educatie. Binnen artikel 65 wordt gewezen op de bewustwording, bevordering en handhaving van integer handelen, dat uitgewerkt kan worden in een beleidsplan. In dit artikel komt het aspect van compliance, wat binnen de ROB gezien kan worden als de belangrijkste basis voor een integere organisatie, ook duidelijk naar voren. De betrokkenheid van het bestuur en de raad van commissarisen wordt als essentieel beschouwd. In artikel 67 worden er enkele mogelijke maatregelen om te komen tot een integere organisatie, genoemd (handboeken, gedragscodes, voorlichtingsbrochures) en er wordt gewezen op het hanteren van een doelgroepenbeleid. Deze aanduidingen zijn echter niet dwingend.

Compliance Criteria	
3.	Ten grondslag aan een awareness programma dient een vastgesteld beleid te liggen ten aanzien van risicobeheersing en integer handelen.
4.	Het awareness programma moet maatregelen bevatten die bewustwording ten aanzien van risico's (zoals onderschepping en manipulatie van informatie, ongeautoriseerde toegang en aantasting van privacy van cliënten) bevorderen
5.	Het awareness programma moet geintegreerd zijn in de bedrijfsprocessen
6.	Het awareness programma moet procedures en maatregelen bevatten die bijdragen aan toereikende compliance, ofwel aan een integere organisatie
7.	Het bestuur en de raad van commissarissen moeten actief betrokken zijn bij de vorming en handhaving van het awarenessprogramma

Wet Financieel Toezicht

Sinds 1 januari 2007 is de Regeling Organisatie en Beheersing (ROB) vervangen door de Wet Financieel Toezicht (Wft), de ROB heeft daarbinnen de status gekregen van *best practice*. De doelstelling van de Wft is wetgeving voor de financiële markten doelgerichter, marktgerichter en inzichtelijker te maken. De Wft vervangt daarmee acht toezichtwetten. Daarnaast zijn binnen de Wft de taken van het prudentieel toezicht (De Nederlandsche Bank) en het gedragstoezicht (Autoriteit

Financiële Markten) gescheiden. In het kader van security awareness is artikel 3:10, lid 1 van toepassing:

> **Artikel 3:10**
> 1. Een clearinginstelling, kredietinstelling of verzekeraar met zetel in Nederland voert een adequaat beleid dat een integere uitoefening van haar onderscheidenlijk zijn bedrijf waarborgt. Hieronder wordt verstaan dat:
> a. belangenverstrengeling wordt tegengegaan;
> b. wordt tegengegaan dat de financiële onderneming of haar werknemers strafbare feiten of andere wetsovertredingen begaan die het vertrouwen in de financiële onderneming of in de financiële markten kunnen schaden;
> c. wordt tegengegaan dat wegens haar cliënten het vertrouwen in de financiële onderneming of in de financiële markten kan worden geschaad;
> en
> d. wordt tegengegaan dat andere handelingen door de financiële onderneming of haar werknemers worden verricht die op een dusdanige wijze ingaan tegen hetgeen volgens het ongeschreven recht in het maatschappelijk verkeer betaamt, dat hierdoor het vertrouwen in de financiële onderneming of in de financiële markten ernstig kan worden geschaad.

Met de Wft zijn de teugels aangetrokken, door de borging van integriteit binnen financiële instellingen uit het domein van regelgeving te halen en naar het domein van wetgeving te dragen. De wetgever hanteert voor de uitvoering van de Wft een best practice-aanpak. De ROB wordt aangeduid als best practice en kan zodoende gebruikt worden om invulling te geven aan de Wft. Andere voorbeelden van best practices zijn ISO/IEC 17799:2005 en IT Infrastructure Library (ITIL).

Compliance Criterium	
3.	Ten grondslag aan een awareness programma dient een vastgesteld beleid te liggen ten aanzien van risicobeheersing en integer handelen

Payment Card Industry – Data Security Standard

De Payment Card Industry – Data Security Standard (PCI-DSS) is een beveiligingsstandaard die gericht is op meerdere aspecten van account beveiliging. De PCI-DSS is verplicht gesteld door de grote kaartlicentie uitgevende instanties (American Express, Discover Financial Services, JCB, MasterCard Worldwide en Visa International) voor de acceptatie (*acquiring)* en uitgifte (*issuing)* van credit cards. De normen gesteld in de PCI-DSS bevinden zich doorgaans op tactisch of operationeel niveau en zijn geinspireerd door de ISO 19977 Code voor Informatiebeveiliging. Het grote verschil zit in de verschuiving van focus naar de zogenaamde account data. De volgende tabel wordt in de PCI-DSS Security Audit Procedures weergegeven als voorbeeld van onder dit regime vallende data (PCI Security Standards Council 2006: 2):

	Data Element	Storage Permitted	Protection Required	PCI-DSS Req. 3.4
Cardholder Data	Primary Account Number (PAN)	YES	YES	YES
	Cardholder Name*	YES	YES*	NO
	Service Code*	YES	YES*	NO
	Expiration Date*	YES	YES*	NO
Sensitive Authentication Data**	Full Magnetic Stripe	NO	N/A	N/A
	CVC2/CVV2/CID	NO	N/A	N/A
	PIN / PIN Block	NO	N/A	N/A

* These data elements must be protected if stored in conjunction with the PAN. […]
** Sensitive authentication data must not be stored subsequent to authorization (even if encrypred)

Uit de bovenstaande tabel blijkt dat alleen kaarthoudergegevens opgeslagen mogen worden, waarbij deze gegevens altijd beschermd dienen te zijn.
Deze gegevens vallen tevens onder de bepalingen in de Wet bescherming persoonsgegevens. De redundantie van deze normen komen voort uit het feit dat de PCI-DSS een internationaal kader is. Hierdoor zijn bepalingen opgenomen die in gevallen door lokale overheden al afgedwongen worden. In regio's waar echter niet voorzien is in privacywetgeving, zorgen deze regels ervoor dat in ieder geval een gelijksoortig niveau bereikt wordt inzake de bescherming van kaarthoudergegevens.

In het kader van security awareness relevante passage, artikel 12 sub 6 *Maintain an Information Security Policy*, blijkt dat alle medewerkers die ingezet worden op credit card verwerkingen, dienen te worden onderwezen op de risico's die gepaard gaan bij het gebruik van kaarthoudergegevens, en de correcte omgang met deze gegevens.

> **12.6** Implement a formal security awareness program to make all employees aware of the importance of cardholder data security.
>
> **12.6.1** Educate employees upon hire and at least annually (for example, by letters, posters, memos, meetings, and promotions)
>
> **12.6.2** Require employees to acknowledge in writing that they have read and understood the company's security policy and procedures.

De eisen zijn binnen de PCI-DSS erg concreet geformuleerd. Naast implementatie van een awareness programma ten aanzien van bewustwording van het belang van beveiliging van kaarthoudergegevens, wordt specifiek gesteld dat medewerkers bij in diensttreding en daarna ten minste jaarlijks, onderwezen dienen te worden binnen het awareness programma. Daarnaast dienen werknemers op schrift te stellen dat zij het beleid en de beveiligingsprocedures hebben gelezen en begrepen. Hiermee reguleert artikel 12.6.2 het bewijs voor auditors voor de acties welke worden verondersteld in artikel 12.6.1.

Compliance Criteria	
4.	Het awareness programma biedt werknemers inzicht in het belang van de beveiliging van kaarthoudergegevens
8./9.	Werknemers dienen minstens één maal per jaar en bij in diensttreding onderwezen te zijn op de verschillende aspecten van beveiliging van kaarthoudergegevens
10.	Werknemers dienen controleerbaar (op schrift) aan te geven het beleid en de beveiligingsprocedures gelezen en begrepen te hebben

ISO/IEC 17799:2005

ISO/IEC 17799:2005 is een best practice, welke algemene normen en maatregelen op het gebied van IT informatiebeveiliging bevat. Dit algemene kader dient niet zonder interpretatie toegepast te worden, en is alleen inzetbaar binnen de context van de organisatie. Security awareness is een cruciaal begrip binnen het normenkader. Beleid ten aanzien hiervan dient dan ook te zijn opgenomen in het beleidsdocument geldend voor de informatiebeveiliging van de organisatie. ISO/IEC 17799:2005 is expliciet over waar de verschillende verantwoordelijkheden dienen te liggen. Er komt naar voren dat het initieren van een awareness programma een managementverantwoordelijkheid is, maar dat de coordinatie en de evaluatie een zaak is van vertegenwoordigers uit verschillende organisatieonderdelen, welke vanuit hun functie een relevante bijdrage kunnen leveren.

Ten aanzien van een awareness programma biedt artikel 8.2.2 een concrete beschrijving:

8.2.2 Information security awareness, education, and training

Control

All employees of the organization and, where relevant, contractors and third party users should receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.

Implementation guidance

Awareness training should commence with a formal induction process designed to introduce the organization's security policies and expectations before access to information or services is granted.

Ongoing training should include security requirements, legal responsibilities and business controls, as well as training in the correct use of information processing facilities e.g. log-on procedure, use of software packages and information on the disciplinary process (see 8.2.3).

Other Information

The security awareness, education, and training activities should be suitable and relevant to the person's role, responsibilities and skills, and should include information on known threats, who to contact for further security advice and the proper channels for reporting information security incidents (see also 13.1).

Training to enhance awareness is intended to allow individuals to recognize information security problems and incidents, and respond according to the needs of their work role.

Naast de implementatie van een awareness programma besteedt de norm ook aandacht aan disciplinaire maatregelen bij overtreding van een bepaling:

8.2.3 Disciplinary process

Control

There should be a formal disciplinary process for employees who have committed a security breach.

Implementation guidance

The disciplinary process should not be commenced without prior verification that a security breach has occurred (see also 13.2.3 for collection of evidence).

The formal disciplinary process should ensure correct and fair treatment for employees who are suspected of committing breaches of security. The formal disciplinary process should provide for a graduated response that takes into consideration factors such as the nature and gravity of the breach and its impact on business, whether or not this is a first or repeat offence, whether or not the violator was properly trained, relevant legislation, business contracts and other factors as required. In serious cases of misconduct the process should allow for instant removal of duties, access rights and privileges, and for immediate escorting out of the site, if necessary.

Other Information

The disciplinary process should also be used as a deterrent to prevent employees, contractors and third party users in violating organizational security policies and procedures, and any other security breaches.

In het normenkader wordt gesteld dat voor alle medewerkers een awareness programma moet worden opgesteld, naarmate dit relevant is voor hun functie, en bijbehorende verantwoordelijkheden en vaardigheden. Een aspect hierin is dat medewerkers training hebben moeten doorlopen, nog voordat zij daadwerkelijk toegang krijgen tot informatie en diensten. Daarnaast wordt aangegeven dat trainingen niet eenmalig gevolgd moeten worden, maar dat er sprake moet zijn van een doorlopend proces. De doelstellingen van een awareness programma liggen volgens ISO/IEC 17799:2005 in het herkennen van en het reageren op dreigingen ten aanzien van informatiebeveiliging.

Uit artikel 8.2.3 blijkt dat er belang wordt gehecht aan disciplinaire maatregelen ten aanzien van beleidsovertredingen. Hierin wordt een terugkoppeling gemaakt naar het awareness programma, of de beleidsovertreder getraind was en daarmee zich bewust had moeten zijn van de overtreding.
In dit kader wordt er vanuit gegaan dat disciplinaire maatregelen ook een preventief karakter kunnen hebben: de maatregelen moeten dan ook binnen het awareness programma naar medewerkers worden gecommuniceerd.

Compliance Criteria	
4.	Het awareness programma biedt medewerkers inzicht in het herkennen van en het reageren op dreigingen ten aanzien van informatiebeveiliging
9.	Medewerkers dienen voordat zij toegang krijgen tot informatie en diensten, een training doorlopen te hebben
11.	Het awareness programma moet voor medewerkers toegespitst zijn op de relevantie voor hun functie, en bijbehorende verantwoordelijkheden en vaardigheden
12.	Het awareness programma moet een continu proces van training bevatten
13.	Disciplinaire maatregelen behorend bij beleidsovertreding moeten binnen het awareness programma naar medewerkers worden gecommuniceerd

Wet Bescherming Persoonsgegevens

Op 1 september 2001 is de Wet bescherming persoonsgegevens (Wbp) in werking getreden. De Wbp heeft de Wet persoonsregistraties vervangen. Deze aanpassing viel samen met de implementatie van de Europese privacy-richtlijn:
'Die aanpassing is in één adem gerealiseerd met de implementatie in het Nederlandse recht van de EU Richtlijn betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (Richtlijn 95/46/EG van het Europees parlement en de Raad van 24 oktober 1995 PbEG 1995 L 281/31). De richtlijn dicteert voor een belangrijk deel de inhoud van de WBP. Het belangrijkste doel van de richtlijn is te waarborgen dat in alle lidstaten van de Europese Unie een gelijkwaardig niveau van bescherming van persoonsgegevens bestaat' (Van der Heijden, Van Slooten en Verhulp 2004: 647).

Binnen dit wettelijke kader staan de basisbeginselen voor gegevensbescherming centraal. Deze zijn als volgt:

a) Doelbinding
b) Kwaliteit
c) Transparantie
d) Rechten van de betrokkene
e) Beveiliging
f) Verantwoordelijkheid

De toezicht en handhaving van de wet is opgedragen aan het College bescherming persoonsgegevens (CBP). Het is mogelijk om binnen een organisatie of op het niveau van een branche een 'interne' toezichthouder aan te stellen. De aanstelling van deze functionaris heeft geen invloed op de bevoegdheden van het CBP.

Aangezien de gegevensverwerkingen binnen de bancaire sector nagenoeg altijd gerelateerd zijn aan, onder de noemer persoonsgegevens vallende, gegevens dient deze wet zorgvuldig geinterpreteerd te worden. De voornaamste taak van de retail banking is immers om op de juiste (vertrouwelijke) wijze verwerkingen met deze gegevens uit te voeren. Doorgaans maakt dit de kenmerken waarmee deze gegevens verrijkt worden binnen bancaire verwerkingen ook tot identificerende gegevens en daarmee dus ook vallende onder deze wet.

Ten aanzien van security awareness is binnen de Wbp artikel 13 van toepassing:

> **Artikel 13**
> De verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.

De Wbp stelt dat er maatregelen getroffen dienen te worden om beveiliging van persoonsgegevens te garanderen, er worden echter geen specifieke maatregelen benoemd. Om de stand van zaken ten aanzien van Wbp te kunnen analyseren, is er een quickscan en een WBP Zelfevaluatie ontwikkeld. Binnen de quickscan wordt kort ingegaan op het niveau van beveiligingsbewustzijn in een organisatie, in de zelfevaluatie is dit uitgebreider, waarbij het niveau van beveiligingsbewustzijn op een vijf-puntschaal kan worden beoordeeld. Ten aanzien van de niveaus van beveiligingsbewustzijn wordt gesteld (Samenwerkingsverband Audit Aanpak / Werkgroep Zelfevaluatie, 2000):

1. Er wordt hiervoor geen inspanning geleverd. Er zijn ook geen procedures voor het vaststellen van de mate waarin de WBP begrepen is en of er behoefte is aan opleiding en training op dit terrein.
2. De medewerkers worden geïnformeerd over informatiebeveiliging. Beveiliging komt reeds ter sprake tijdens de sollicitatieprocedure. Er zijn eerste aanzetten voor de vaststelling van de mate waarin de WBP begrepen is en er is sprake van enige identificatie van de behoefte aan training en opleiding op dit terrein.
3. De medewerkers worden geïnformeerd over informatiebeveiliging en zij ontvangen instructies. Het komt ter sprake tijdens de sollicitatieprocedure en er worden gerichte vragen gesteld aan sollicitanten. Er is een systeem voor de bepaling van de mate waarin de WBP begrepen is en de meting van behoefte aan opleiding en training.
4. De medewerkers worden geïnformeerd over informatiebeveiliging en ontvangen daarover instructies. Er wordt regelmatig gecontroleerd of de medewerkers de maatregelen naleven. Beveiliging wordt ter sprake gebracht tijdens de sollicitatieprocedure en daarover worden gerichte vragen gesteld aan sollicitanten. De antwoorden van de sollicitanten worden nagetrokken. De naleving van het systeem van meting van opleiding en training wordt bewaakt.
5. De medewerkers worden geïnformeerd over informatiebeveiliging, zij ontvangen instructies. Er wordt regelmatig gecontroleerd of de medewerkers de maatregelen naleven. Bij niet-naleving worden maatregelen getroffen tegen de betreffende medewerkers. Beveiliging komt ter sprake tijdens de sollicitatieprocedure en er worden gerichte vragen gesteld aan sollicitanten. Beveiligingsbewustzijn is een selectiecriterium.

Hieruit blijkt dat er op het gebied van beveiliging van persoonsgegevens concrete maatregelen kunnen worden getroffen, met uitzondering van het laagste niveau blijkt uit de overige niveaus dat medewerkers geinformeerd dienen te worden. Dit kan door middel van opleiding en training. Hiermee wordt indirect gewezen op een awareness programma als mogelijke uitwerking van een van de maatregelen die binnen artikel 13 worden genoemd om beveiliging van persoonsgegevens te garanderen.

Compliance Criterium	
4.	Het awareness programma moet maatregelen bevatten die bewustwording ten aanzien van beveiliging van persoonsgegevens bevorderen

Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Deze Europese richtlijn is overgenomen in de Wet Bescherming Persoonsgegevens. Aangezien de Wet Bescherming Persoonsgegevens in dit hoofdstuk is behandeld, is het niet relevant om nog verder over deze richtlijn uit te weiden.

Code Tabaksblat

De Nederlandse corporate governance code werd opgesteld door een commissie onder leiding van Morris Tabaksblat, en staat zodoende bekend als de code Tabaksblat. De code is een gedragcode voor beursgenoteerde bedrijven en trad op 30 december 2004 in werking. Doelstellingen van de code zijn betere verantwoording van de Raad van Commissarissen, betere zeggenschap en bescherming van aandeelhouders en betere transparantie van de jaarrekening. De code kent de 'pas toe of leg uit'-regel: in het jaarverslag dient aangegeven te worden of de regels van de code zijn toegepast, en wanneer dit niet zo is, dient dit uitgelegd te worden.

Ten aanzien van security awareness kent de code Tabaksblat geen specifieke regels. Er is wel in de code opgenomen dat de leden van de Raad van Commissarissen voldoende kennis moeten hebben om het beleid in algemene zin te kunnen volgen. Hiertoe is in de code opgenomen dat de leden een introductieprogramma dienen te volgen, waarbij er jaarlijks gekeken wordt of nadere training noodzakelijk is:

> III.3.3 Alle commissarissen volgen na benoeming een introductieprogramma, waarin in ieder geval aandacht wordt besteed aan algemene financiële en juridische zaken, de financiële verslaggeving door de vennootschap, de specifieke aspecten die eigen zijn aan de desbetreffende vennootschap en haar ondernemingsactiviteiten, en de verantwoordelijkheden van een commissaris. De raad van commissarissen beoordeelt jaarlijks op welke onderdelen commissarissen gedurende hun benoemingsperiode behoefte hebben aan nadere training of opleiding. De vennootschap speelt hierin een faciliterende rol.

Uit het artikel blijkt dat de leden van de Raad van Commissarissen voldoende kennis moeten hebben van de specifieke aspecten van de organisatie. Voor de retail banking zijn integriteit en security awareness belangrijke elementen. Vanuit de code Tabaksblat beredeneerd, zou een trainingselement toegespitst op de Raad van Commissarissen binnen een awareness programma een plaats kunnen hebben.

Compliance Criterium	
7.	Het awareness programma bevat een trainingselement welke toegespitst is op de Raad van Commissarissen

Basel II / Core Principles for Systemically Important Payment Systems

In 2004 werd de International Convergence of Capital Measurement and Capital Standards, oftewel Basel II, uitgebracht door de Basel Committee on Banking Supervision, een commissie bestaande uit vertegenwoordigers van centrale banken en toezichthoudende instanties uit verschillende landen. Basel II verving het verouderde Basel I, en biedt banken richtlijnen ten aanzien van het kapitaal dat banken opzij dienen te zetten om verliezen uit financiële en operationele risico's op te kunnen vangen. Basel II is hierbij gericht op drie pijlers: minimum kapitaaleisen, toezicht en marktwerking.

Het algemene principe van Basel II is dat hoe groter het risico wordt geacht, des te meer kapitaal een bank moet reserveren om de stabiliteit te waarborgen.
Basel II is in de meeste Europese landen als richtlijn geimplementeerd in de wetgeving. In Nederland is de richtlijn verwerkt in de Wet financieel toezicht (Wft). Op Europees niveau is Basel II uitgewerkt in de Capital Requirement Directive (CRD).

Ten aanzien van security awareness biedt Basel II geen concrete aanwijzingen. Evenals in de Wft wordt gesteld dat organisaties een systeem voor risicobeheersing dienen te hebben, maar de wijze waarop hieraan invulling wordt gegeven, wordt opengelaten.

De Basel Committee on Banking Supervision is een van de vier commissies welke vallen onder de Bank for International Settlements (BIS). De BIS is een internationale financiële koepelorganisatie waarbij nationale centrale banken en de Europese Centrale Bank zijn aangesloten. In 2001 bracht de BIS het rapport Core Principles for Systemically Important Payment Systems uit, waarin, naast vier hoofdverantwoordelijkheden voor een centrale bank, tien algemeen geldende richtlijnen voor het ontwerpen en het controleren van veiligere Systemically Important Payment Systems worden onderscheiden:

Core principles for systemically important payment systems

1. The system should have a well founded legal basis under all relevant jurisdictions.
2. The system's rules and procedures should enable participants to have a clear understanding of the system's impact on each of the financial risks they incur through participation of it.
3. The system should have clearly defined procedures for the management of credit risk and liquidity risk, which specify the respective responsibilities of the system operator and the participants and which provide appropriate to manage and contain those risks.
4. The system should provide prompt final settlement on the day of value, preferably during the day and at a minimum at the end of the day.
5. A system in which multilateral netting takes place should, at a minimum, be capable of ensuring the timely completion of daily settlements in the event of an inability to settle by the participant with the largest single settlement obligation.
6. Assets used for settlement should preferably be a claim on the central bank; where other assets are used, they should carry little or no credit risk and little or no liquidity risk.
7. The system should ensure a high degree of security and operational reliability and should have contingency arrangements for timely completion of daily processing.
8. The system should provide a means for of making payments which is practical for its users and efficient for the economy.
9. The system should have objective and publicly disclosed criteria for participation, which permit fair and open access.
10. The system's government arrangements should be effective, accountable and transparent.

Binnen het tweede basisprincipe van de Core Principles for Systemically Important Payment Systems wordt aandacht besteed aan security awareness, waarbij het essentieel wordt geacht dat organisaties en hun medewerkers risico's begrijpen. In de samenvatting van de bespreking van dit basisprincipe komt dit naar voren:

Core Principle II – Implementation summary

7.2.8 Participants need to understand the financial risks they bear. Operators should therefore have rules and procedures that:

- Are clear, comprehensive and up to date;
- Explain the system design, its timetable and risk management procedures;

- Explain the system's legal basis and roles of the parties;
- Are readily available;
- Explain where there is discretion and how it is exercised;
- Set out decision and notification procedures and timetables for handling abnormal situations.

It may also be useful to organise participant training and monitor the performance of participants as evidence of their understanding.

Onder basisprincipe VII wordt ingegaan op het belang van beveiligingsbewuste medewerkers:

> 7.7.6 A system needs to have adequate numbers of well trained, competent and trustworthy personnel. They must be able to operate the system safely and efficiently, and to ensure that the correct operational and risk management procedures are followed, in both normal and abnormal situations. Some of the personnel need to act as operational and security managers and have appropriate levels of knowledge, experiences and authority for those tasks. The training of personnel should include a wider understanding of payment systems and their importance, so that operational decisions of the system are made in the right context. […]

Uit artikel 7.2.8 blijkt dat een operator, welke functie organisaties binnen de retail banking kunnen hebben, verantwoordelijk is voor het informeren van de financiële risico's voor derden die gebruik maken van de betalingsinfrastructuur. Dit heeft tot gevolg dat er binnen de service level agreements (SLA) die worden afgesloten met derden een eis moet worden opgenomen om te voorzien in voorlichting en training. Er kan niet verwacht worden dat training aan derden een element vormt binnen het eigen awareness programma. Artikel 7.7.6 is toegespitst op de eigen medewerkers en laat zien dat gestreefd moet worden naar een breed begrip van betaalsystemen, zodat deze veilig en efficient werken.

Compliance Criterium	
4.	Het awareness programma biedt medewerkers een breed begrip in betalingsystemen en het belang van veiligheid en efficientie van deze systemen

Electronic Money System Security Objectives

In mei 2003 werd door de European Central Bank een rapport uitgegeven dat de kaders behandelt, waaraan electronic money (e-money) dient te voldoen op basis van de ISO/IEC 15408 common criteria for IT Security Evaluation methodiek. Hierbij wordt gesproken over de zogenaamde Target of Evaluation (TOE) als deel van het systeem dat geevalueerd dient te worden. In de paragraaf handelend over 'Competence and responsibility' is de volgende eis opgenomen:

> 3.2.18 Competence and responsibility
> People involved in the system know and follow their own contractual obligations, and have sufficient means, training and information to perform their role.
> […]
> - A state-of-the-art hiring policy, control of access to company premises and a security awareness programme apply to the personnel of all companies dealing in the production and the distribution of devices or software used by the TOE.

Dit onderdeel is, zoals valt op te maken uit de richtlijn, enkel van belang als de financiële instelling e-money producten/diensten levert, maar laat zien dat een awareness programma nodig is voor medewerkers die betrokken zijn bij de productie van hard- en software. Voor organisaties waarbij

‘zelfbouw’ van hard- en software ten behoeve van e-money aan de orde is, dient zodoende een awareness programma aanwezig te zijn.
Daarbij kan worden gesteld dat ook bij distributie van randapparatuur voor gebruik binnen een e-money infrastructuur medewerkers een awareness programma dienen te volgen

Compliance Criterium	
11.	Indien relevant voor de functie of verantwoordelijkheden en vaardigheden, dient er een awareness programma aanwezig te zijn

Jurisprudentie

Ten aanzien van overtreding van regels die voortkomen uit een gedragscode, zijn er in de jurisprudentie een aantal zaken bekend. De overtreder kan zich hierbij niet beroepen op het ontbreken van een gedragscode vanuit de organisatie waardoor hij vrijuit zou kunnen gaan. Aangezien de rechter zich baseert op de redelijkheid en geest van de wet, lijkt het onaannemelijk dat een gedragscode veel wettelijke relevantie met zich meedraagt daar waar het gaat om regels en normen die al door de wet geforceerd worden. Een gedragscode schept duidelijkheid naar medewerkers, maar deze duidelijkheid wordt in de eerste plaats geschapen door de wet die iedereen geacht is te kennen. Toch blijkt dat in zaken waarin de overtreder duidelijk is gewezen op de gevolgen van niet integer handelen, bijvoorbeeld in een gedragscode, dat de de overtreder expliciet wordt beschouwd als een 'gewaarschuwd mens' (onder andere in: LJN: BB5674, Rechtbank 's-Gravenhage, rep. nr. 688053 / 07-82332; LJN: AT9398, Rechtbank Almelo , 72047 / KG ZA 05-174). Wanneer is overgegaan tot veroordeling zijn de gronden echter altijd gebaseerd op wetgeving en niet op het breken van de gedragscode.

Daarnaast scheppen richtlijnen handelend over bijvoorbeeld de beveiliging van de ICT infrastructuur en de normen op het vlak van fysieke beveiliging kaders die de wet zelf niet schept. Het is bijvoorbeeld niet strafbaar om een smart card uit te lenen. Maar als de gedragscode stelt dat deze persoonsgebonden is en de technische eigenschappen van het product stellen in staat om dit in alle redelijkheid te borgen, dan zou overtreding door de rechterlijke macht opgevat kunnen worden als verzwarende omstandigheid.

Pijler II: Effectiviteit

De pijler effectiviteit dient het mogelijk te maken om compliant te worden. Immers als een awareness programma niet doeltreffend is, dan voldoet men nog steeds niet aan de eisen. Het is zaak om alle doelstellingen binnen het programma duidelijk te kunnen bepalen. Het hebben van goede Key Performance Indicators (KPI’s) is hierbij relevant. Dit zal de eerste stap zijn die binnen het volgende hoofdstuk genomen gaat worden.

De doeltreffendheid van een awareness programma is gericht op het kennen, begrijpen en accepteren van nodige maatregelen om risico’s te kunnen beperken.
Dit kan men doen door bijvoorbeeld medewerkers te toetsen aan het einde of gedurende het awareness programma. Door te bekijken of medewerkers de toets met een voldoende afronden, kan besloten worden dat de doelen van het awareness programma zijn gehaald. Het is voor onderlinge vergelijkbaarheid interessant om een standaardtoets voor iedere branch te ontwikkelen. Hierin zou de gedeelde wet- en regelgeving een belangrijke plaats dienen in te nemen.

Ook van belang voor de effectiviteit zijn controlemaatregelen. Hierbij kan gedacht worden aan bijvoorbeeld de eis vanuit de PCI-DSS om medewerkers in schrift te laten verklaren dat een awareness programma gevolgd is. Deze eis valt in dit geval onder zowel de compliance pijler als de pijler effectiviteit. Een andere maatregel is dat binnen een awareness programma wordt

gecommuniceerd dat medewerkers incidenten, situaties waarin een incident is voorkomen (near misses) en verdacht gedrag moeten melden.

Effectiviteit Criteria	
10.	Werknemers dienen controleerbaar (op schrift) aan te geven het beleid en de beveiligingsprocedures gelezen en begrepen te hebben
14.	Het awareness programma dient afgesloten te worden met een toets of oefening waarop medewerkers beoordeeld worden
15.	In het geval een branche gebruik wenst te maken van een maturity model, dienen toetsen in een awareness programma onderling vergelijkbaar te zijn
16.	Er dient altijd melding te worden gemaakt van incidenten (inclusief near misses) en verdacht gedrag

Pijler III: Efficiëntie

Efficiëntie dient de methodiek beheersbaar te maken vanuit economisch opzicht. Door efficiënt te werken kan men met goedkopere methoden eenzelfde resultaat verkrijgen als met duurdere methoden. Er is een duidelijke koppeling met effectiviteit. Een organisatie kan efficient werken zolang de doelen ten aanzien van het beveiligingsniveau worden bepaald. Compliance is hier ook aan gekoppeld: kostenbesparing is mogelijk zolang er aan de wet- en regelgeving wordt voldaan. Binnen de wet- en regelgeving worden er geen verplichtingen gesteld ten aanzien van de kosten voor informatiebeveiliging. Er wordt gesteld dat organisaties niet door de wetgever worden verplicht om "een kwartje uit te geven om een dubbeltje te beveiligen". In artikel 13 van de Wbp wordt zelfs expliciet gesteld dat bij maatregelen die een passend beveiligingsniveau moeten garanderen, rekening gehouden wordt met de kosten van de tenuitvoerlegging. In de handleiding voor verwerkers van persoonsgegevens, uitgebracht door het ministerie van justitie, wordt gesteld dat bij een passende beveiliging onder andere moet worden gekeken naar het kostenaspect (Ministerie van Justitie 2002: 38):

> Als de kosten van extra maatregelen uitzonderlijk hoog zijn ten opzichte van de toename in beveiligingsniveau, dan zijn die maatregelen niet passend en hoeft u ze dus niet te nemen. Kunt u echter tegen geringe kosten komen tot een beduidend veiliger systeem, dan moet u deze maatregelen zeker nemen.

Het bepalen van doelgroepen kan in belangrijke mate bijdrage aan de efficientie. Binnen het basisprincipe VIII van de Core Principles for Systemically Important Payment Systems wordt efficiëntie essentieel geacht, en gesteld dat er een afstemming moet zijn op de dagelijkse praktijk:

> 7.8.1 [...]
> Judgements on the type of system that is appropiate to the needs of its users will require an understanding of practices, technologies and skills in the local banking sector. For instance, if users need to make only a small number of payments each day, implementation of elaborate systems that require extensive investment and training may not be appropiate.

Het is zodoende van belang dat het awareness programma gedifferentieerd is. Het is bijvoorbeeld onnodig voor een secretaresse om geschoold te worden in Code Tabaksblat, daarentegen dient deze medewerker wel op de hoogte te zijn van onder andere een classificatiebeleid en een clear desk beleid.

Voor de efficiëntie is het van belang dat ingeschaald wordt wat het huidige niveau is van de medewerkers ten opzichte van het gewenste niveau.

Men kan dan het awareness programma afstemmen op de kennis die medewerkers al met zich meedragen zodat er geen moeite wordt gestoken in het aanbieden van kennis die al op peil is. Het is aan te raden om als men begint met gebruik van een nieuwe methodiek alle stof de eerste keer aan te stippen. Dit zodat de resultaten van de toetsmomenten gebruikt kunnen worden om te bepalen waaraan een volgende campagne minder aandacht besteed hoeft te worden.

Efficiëntie Criteria	
11.	Het awareness programma moet voor medewerkers toegespitst zijn op de relevantie voor hun functie, en bijbehorende verantwoordelijkheden en vaardigheden
17.	Het awareness programma dient zo laag mogelijke kosten te hebben, zolang de effectiviteit en complance van het programma gewaarborgd blijven
18.	Het awareness programma moet een lerend vermogen hebben en zodoende kunnen voortbouwen op elementen die eerder binnen het programma aan bod zijn gekomen

Opsomming van de criteria

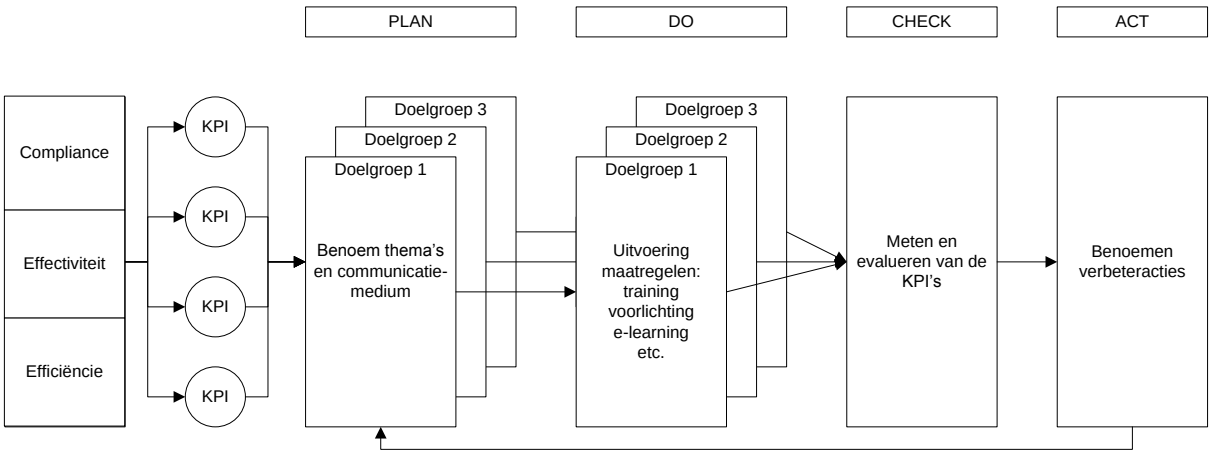
Criteria voor een awareness programma	Normen en waarden	ROB	Wft	PCI-DSS	ISO/IEC17799:2005	Wbp	Code Tabaksblat	Basel II / Core Principles for Systemically Important Payment Systems	Electronic Money System Security Objectives	Effectiviteit	Efficiëntie
1. Inzicht in regels vereist vanuit derden	x										
2. Inzicht in regels uit de gedragscode	x										
3. Onderbouwing vanuit vastgesteld beleid		x	x								
4. Inzicht bieden in bedreigingen en risico's		x		x	x	x		x			
5. Integratie in bedrijfsprocessen		x									
6. Kennis van relevante wet- en regelgeving		x									
7. Betrokkenheid bestuur en raad van commissarisen		x					x				
8. Jaarlijkse deelname				x							
9. Deelname bij indiensttreding				x	x						
10. Controleerbare bevestiging (op schrift)				x						x	
11. Doelgroepen-bepaling					x				x		x
12. Continue proces					x						
13. Inzicht bieden in disciplinaire maatregelen					x						
14. Toetsing van medewerkers										x	
15. Vergelijkbaarheid t.a.v. maturity model										x	
16. Opnemen meldingsplicht										x	
17. Laag mogelijke kosten											x
18. Lerend vermogen											x

< this page intentionally left blank >

Methodiek voor een awareness programma

In dit hoofdstuk wordt de voorgestelde methodiek voor security awareness binnen retail banking uiteengezet. De basis van de methodiek bestaat uit de criteria die zijn afgeleid uit de pijlers compliance, effectiviteit, efficiëntie.

Deze criteria worden in dit hoofdstuk uitgewerkt in key performance indicators (KPI's). Daarna wordt de methodiek beschreven aan de hand van de Deming-cyclus (Plan-Do-Check-Act). Hierin wordt uitgebreid aandacht besteed aan de ontwikkeling van een maturity model, waarin het concept Six Sigma een belangrijke rol speelt. Tot slot wordt als voorbeeld een scenario uitgewerkt, waarin alle processtappen aan bod komen. Het onderstaande figuur geeft een schematische weergave van de methodiek.



Key performance indicators

Door de criteria om te zetten in Key Performance Indicators (KPI's) en niet toe te spitsen op losse thema's, wordt bereikt dat de resultaten van het totale awareness programma helder bepaald kunnen worden. Elke afzonderlijke KPI moet daartoe SMART zijn (Specific – Measurable – Achievable – Result-oriented or Relevant – Time-bound):

Een KPI moet voldoende specifiek zijn, wat betekent dat de KPI concreet en werkbaar moet zijn (Specific). Daarnaast moet een KPI meetbaar zijn (Measurable), waarbij de doelstellingen die gemeten worden, haalbaar moeten zijn (Achievable). Een KPI moet ook resultaatgericht/relevant (Result-oriented or Relevant) zijn, wat inhoudt dat het voor de organisate van belang is om deze KPI te meten. Ten slotte hoort een KPI aan een bepaalde tijdsduur (Time-bound) gerelateerd zijn, zodat vergelijking ten aanzien van een verandering mogelijk is.

Vanuit de criteria voortkomend uit de drie pijlers voor de methodiek voor security awareness kunnen KPI's worden opgesteld:

Criteria	#	Key Performance Indicators
Inzicht in regels vereist vanuit derden	01	Onderdeel van het programma
Inzicht in regels uit de gedragscode	02	Onderdeel van het programma
Onderbouwing vanuit vastgesteld beleid	03	onderdeel van het programma
Inzicht bieden in bedreigingen en risico's	04	Aantal incidenten
	05	Aantal medewerkers dat training met succes afrondt
	06	Economische omvang van incidenten
	07	Mate waarin malware wordt aangetroffen
Integratie in bedrijfsprocessen	08	Aantal bezoekers van beveiligingsitems op intranet
	09	Aantal lezers van nieuwsbrief
	10	Mate waarin beveiliging binnen werkoverleggen aan de orde komt
Kennis van relevante wet- en regelgeving	11	Aantal medewerkers dat een voldoende scoort bij toetsing
	12	Resultaten van audit programma's (in het kader van compliance)
Betrokkenheid bestuur en raad van commissarisen	13	Aantal bestuursleden/commissarissen dat een presentatie/training heeft gevolgd
	14	Resultaten van periodieke zelfevaluaties van management
Jaarlijkse deelname	15	Aantal medewerkers dat de training jaarlijks heeft gevolgd
Deelname bij indiensttreding	16	Aantal nieuwe medewerkers dat bedrijfsintroductie heeft gevolgd
Controleerbare bevestiging (op schrift)	17	Aantal medewerkers dat schriftelijke bevestiging heeft getekend
Doelgroepen-bepaling	18	Onderdeel van het programma
Continu proces	19	Onderdeel van de gekozen methodiek
Inzicht bieden in disciplinaire maatregelen	20	Aantal medewerkers dat de training met succes afrondt
Toetsing van medewerkers	21	Aantal medewerkers dat een toets heeft afgelegd
Vergelijkbaarheid t.a.v. maturity model	22	Aantal gekozen standaard waarden uit de methodiek
Opnemen meldingsplicht	23	Onderdeel van het programma
Laag mogelijke kosten	24	Kosten van het awareness programma
Lerend vermogen	25	Onderdeel van het programma

Plan

Binnen de Plan-fase wordt een planning opgesteld om het awareness programma vorm the geven. Hiertoe is het noodzakelijk dat een organisatie de eigen doelstellingen en ambities ten aanzien van secutiry awareness concretiseert. Hier worden binnen de Plan-fase doelgroepen geformuleerd en gekoppeld aan verantwoordelijkheden die voor de specifieke doelgroep gelden. Daarnaast worden er maatregelen benoemd, waarbij gekeken wordt naar het kostenaspect.

Doelgroepen

Om tot een eenduidige doelgroepaanduiding te komen, is gebruik gemaakt van de lijst met standaardfuncties zoals deze is uitgebracht door het International Standard Classification of Occupation (ISCO). Deze lijst geeft op drie niveau's een indeling in standaardfuncties. Voor deze scriptie is gekeken naar het eerste niveau om de lijst met functies enigzins beperkt te houden. Daarnaast valt er voldoende onderscheid op dit niveau te maken om typerende functies te duiden. Kenmerkende functies van het tweede niveau zullen wel genoemd worden in de opsomming om een beeld te krijgen van welke functies er worden verstaan onder een noemer uit het eerste niveau. In de retail banking kunnen de volgende doelgroepen worden onderscheiden (ISCO 2008: 4-5):

- Managers
  Chief executives, senior officials and legislators, Administrative and commercial managers, Production and specialized services managers;
- Professionals
  Business and administration professionals, Information and communications technology professionals, Legal, social and cultural professionals;
- Technicians and associate professionals
  Business and administration associate professionals, Legal, social, cultural and related associate professionals, Information and communications technicians;
- Clerical support workers
  General and keyboard clerks, Customer services clerks, Other clerical support workers;
- Service and sales workers
  Personal service workers, Sales workers, Protective services workers;
- Elementary occupations
  Cleaners and helpers, Food preparation assistants.

Naast de doelgroepen afkomstig uit de ISCO is er ten behoeve van de Code Tabaksblat een functiegroep toegevoegd, te weten de raad van commissarissen. Hier wordt bewust een Nederlandse term gehanteerd aangezien het type van bestuur voor een commisaris kan verschillen per land.

- Raad van commissarissen.

Voor een methodiek toegespitst op de organisatie, kan gekozen worden om een doelgroepaanduiding te hanteren, welke gebaseerd is op het eigen functiehuis. De bovenstaande doelgroepaanduiding is echter in algemene zin toepasbaar op organisaties in de retail banking, en het hanteren van een gelijke aanduiding zou onderlinge vergelijkbaarheid vergemakkelijken.

Deze doelgroepen worden in het onderstaande schema gekoppeld aan verantwoordelijkheden die gelden voor de specifieke doelgroep ten aanzien van secutiry awareness binnen de organisatie. Hoewel de inhoud kan verschillen, komt de algemene aard van de verantwoordelijkheden voor de groepen professionals, technicians and associate professionals, clerical support workers, service and sales workers en elementary occupations overeen. Deze zijn samengebracht onder de noemer 'werknemers':

Doelgroepen	Verantwoordelijkheden
Managers	Onderschrijven van het belang Uitdragen belang Uitdragen beleid (voorbeeldfunctie) Begeleiding en controleren medewerkers Verantwoording Toezichthouden en signaleren
Werknemers	Op de hoogte zijn en naleven beleid in kader van de eigen functie Herkennen en melden incidenten Verantwoording in kader van eigen functie
Raad van Commissarissen	Onderschrijven van het belang Toezichthouden en signaleren

Maatregelen

Om medewerkers binnen de organisatie hun verantwoordelijkheden te laten nemen, is het van belang doeltreffende maatregelen te formuleren. Bij de keuze voor geschikte maatregelen is het van belang te bepalen of een maatregel een oppervlakkige of een systematische verwerking van informatie ten aanzien van gewenst gedrag biedt. Van een meer systematische verwerking wordt verondersteld dat de gewenste gedragsverandering meer structureel zal zijn. Toch kan oppervlakkige verwerking een bijdrage leveren aan gedragsverandering, maar op een andere manier dan systematische verwerking.

Systematische verwerking hangt samen met begrip en acceptatie van de inhoud van informatie. Oppervlakkige verwerking is verbonden met affectiviteit: 'people may agree with messages from attractive or expert sources or with familiair or long messages. They might also be influenced by positive or negative events associated with attitude object, or by feelings they are experiencing' (Smith en Mackie 2000: 256).

Op basis van een studie naar Security Measurements van Europese bedrijven geeft ENISA aan welke maatregelen deze bedrijven hebben genomen en welke daarvan doeltreffend worden geacht (ENISA 2007). Basten en Wijnmaalen (2003) bieden handvatten om mogelijke maatregelen voor management en werknemers te onderscheiden. Op basis hiervan kunnen de volgende maatregelen voor de retail banking worden geformuleerd, waarbij is aangegeven of een oppervlakkige of een systematische verwerking wordt bewerkstelligd. Enkele maatregelen kunnen zowel een oppervlakkige of een systematische verwerking bevatten, afhankelijk van de affectieve en inhoudelijke aard van de informatie.

Maatregelen gebaseerd op oppervlakkige informatieverwerking:

- Postercampagne met een focus op beveiligingsonderwerpen
- Verspreiden van promotiemateriaal onder medewerkers (bijvoorbeeld: screensavers, pennen, muismat, etc.)
- Publicatie's op het intranet
- Nieuwsbrief of email gedistribueerd aan medewerkers
- Video
- Quizzes over beveiligingsonderwerpen in het medewerkers magazine

Maatregelen gebaseerd op systematische informatieverwerking:

- Publicatie van een beveiligingsbeleid bevattende de uitgangspunten en richtlijnen (beleidshandboek)
- Opnemen van beveiligingsvereisten in procedures en werkinstructies
- Opnemen van security awareness training binnen het introductieprogramma voor nieuwe medewerkers
- Beveiligingsverantwoordelijkheden worden opgenomen binnen het contract dat de medewerker heeft met de organisatie
- Beveiligingsonderwerpen worden opgenomen binnen werkoverleggen
- Distributie van een brochure aangaande het beveiligingsbeleid
- Formeel communicatieplan over hoe het onderwerp beveiligingsbewustzijn door de organisatie structureel wordt aangepakt
- Nieuwsbrief of email gedistribueerd aan medewerkers
- Formele analyse van focus groepen
- Beveiligingsonderwerpen worden opgenomen binnen bestaande trainingsprogramma's voor medewerkers
- E-learning (computer gebaseerde security awareness training)
- Inschakelen van externe expertise (bijvoorbeeld security awareness training vendors)
- Verplichte klassikale training
- Presentaties
- Persoonlijke instructies en ondersteuning
- Quick scans

Opvallend is dat binnen het ENISA onderzoek een beleidshandboek voor medewerkers door ruime meerderheid van de respondenten als maatregel is uitgevoerd. Maar deze maatregel wordt door de respondenten als de minst effectieve maatregel gezien. Trainingen voor medewerkers blijken de meest doeltreffende maatregel te zijn. Binnen deze methodiek wordt training (klassikaal of e-learning) als een belangrijk onderdeel van een awareness programma in retail banking beschouwd.

In principe kunnen alle maatregelen aan de verschillende doelgroepen worden gekoppeld, maar hierbij moet een afweging ten aanzien van de doeltreffendheid worden gemaakt. Ten aanzien van de verantwoordelijkheid van managers om werknemers te begeleiden, zal een brochure minder effectief zijn dan een training gericht op de ontwikkeling van interpersoonlijke en communicatieve vaardigheden, wat onderbouwd wordt door een theoretisch kader: 'such skills can be developed by training that draws upon the research on leadership, motivation, and communication' (Berry 1997: 190). Om werknemers te stimuleren om het beleid na te leven, zal een theoretisch omkaderde training niet effectief zijn, maar kan er beter gekozen worden om te werken met een combinatie aan maatregelen zoals een postercampagne, distributie van nieuwsbrieven of e-mails, het opnemen van beveiligingsvereisten in procedures en werkinstructies, en in het contract dat de medewerker heeft met de organisatie, en een herhaling van de e-learning training.

Bij de planning van maatregelen speelt het kostenaspect een belangrijke rol. Naast effectief, moeten maatregelen efficient ingezet worden. Basten en Wijnmaalen (2003) schatten 14 maatregelen in een bewustwordingscampagne op een schaal van L(aag), M(iddel) en H(oog). Zij maken een onderscheid tussen directe kosten (D) en indirecte kosten (I). Voor de maatregelen die ten aanzien van de verantwoordelijkheden van de doelgroepen zijn geformuleerd, zal hieronder een indicatie van de kosten worden gemaakt, waar mogelijk gebaseerd op de inschattingen van Basten en Wijnmaalen.

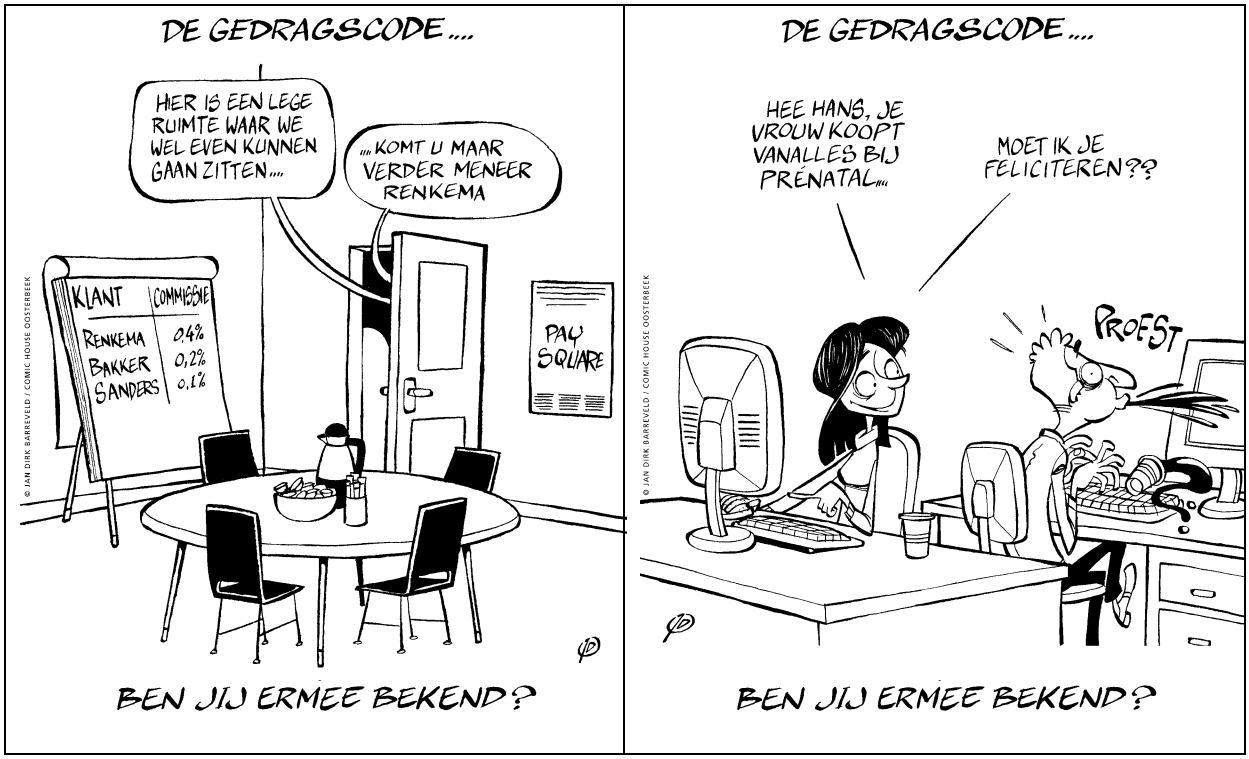
Maatregel	D	I
Postercampagne met een focus op beveiligingsonderwerpen	**M**	**L**
Verspreiden van promotiemateriaal onder medewerkers	**M**	**L**
Publicatie's op het intranet	**M**	**M**
Nieuwsbrief of email gedistribueerd aan medewerkers	**M**	**M**
Video	**H**	**H**
Quizzes over beveiligingsonderwerpen in het medewerkers magazine	**M**	**L**
Beleidshandboek	**H**	**H**
Opnemen van beveiligingsvereisten in procedures en werkinstructies	**M**	**L**
Security awareness training binnen het introductieprogramma voor nieuwe medewerkers	**L**	**M**
Beveiligingsverantwoordelijkheden opnemen binnen het contract	**L**	**L**
Beveiligingsonderwerpen worden opgenomen binnen werkoverleggen	**L**	**H**
Distributie van een brochure aangaande het beveiligingsbeleid	**M**	**L**
Formeel communicatieplan	**M**	**L**
Formele analyse van focus groepen	**M**	**L**
Beveiligingsonderwerpen worden opgenomen binnen bestaande trainingsprogramma's	**L**	**M**
E-learning (computer gebaseerde security awareness training)	**M**	**H**
Inschakelen van externe expertise (bijvoorbeeld security awareness training vendors)	**H**	**M**
Verplichte klassikale training (met afsluitende toets)	**M**	**H**
Presentaties	**L**	**M**
Persoonlijke instructies en ondersteuning	**L**	**L**
Quick scans	**M**	**H**

Do

In de Do-fase worden de maatregelen per doelgroep uitgevoerd. In deze scriptie worden twee voorbeelden van de implementatie van een maatregel gepresenteerd

Voorbeeld 1: Postercampagne

Onderstaande figuren zijn voorbeelden van de postercampagne van PaySquare B.V. ten aanzien van security awareness. Deze campagne bewerkstelligt een oppervlakkige verwerking. De humoristische cartoons moeten de aandacht trekken, de geboden informatie is in slechts enkele zinnen geformuleerd. Een postercampagne wordt vaak in combinatie met andere maatregelen ingezet. Een postercampagne kan effectief zijn, omdat het bijdraagt aan het 'mere exposure effect'. Dit effect houdt in: 'people prefer things to which they have been more frequently exposed' (Smith en Mackie 2000: 260). Daarnaast kan het middel efficient worden ingezet, zeker wanneer de productie in eigen beheer en/of op grote schaal wordt uitgevoerd.



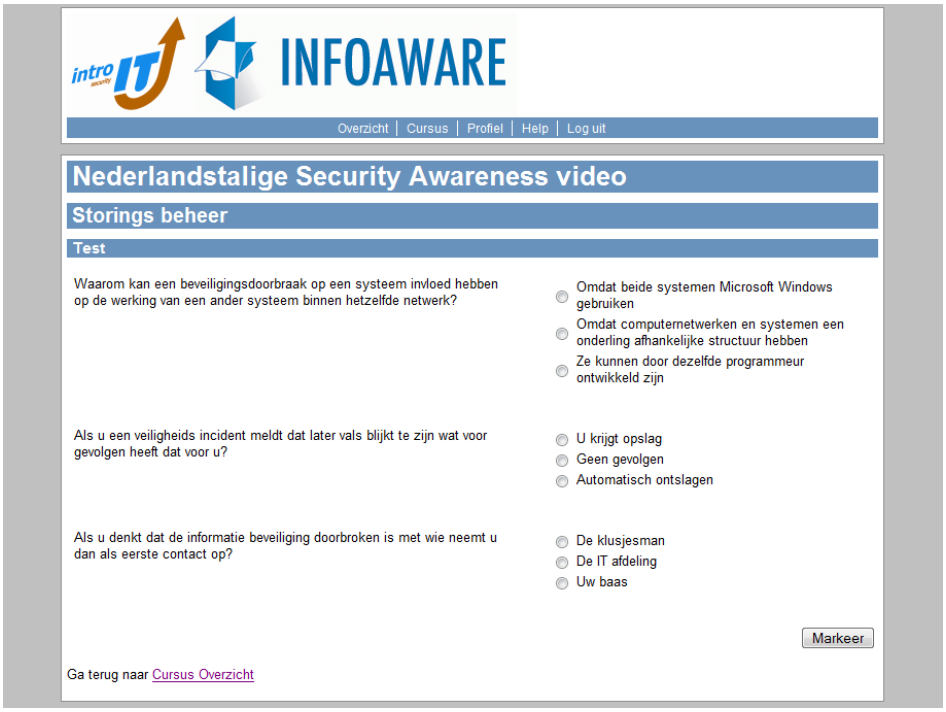
poster concurrentiegevoelige informatie

poster privacygevoelige informatie

Bron: PaySquare B.V.

Voorbeeld 2: E-learning

Een e-leaming omgeving biedt een platform voor een interactieve training in een awareness programma. Het onderstaande figuur biedt een voorbeeld van een test. E-learning biedt een systematische manier om informatie te verwerken, waarbij medewerkers zelfstandig een geschikt moment kunnen kiezen om zich te verdiepen in het onderwerp en de toets te maken. E-learning leent zich goed om verschillende doelgroepen op maat te trainen: 'The computer interacts with the testee to develop and administer a test customized for the individual. It can do this because it contains a bank of questions that have been developed specifically to represent different level of difficulty on a test' (Berry 1997: 150). Het interactieve element binnen e-learning is belangrijk voor de effectiviteit, aangezien medewerkers worden gestimuleerd actief met de informatie bezig te zijn. De maatregel is efficient, omdat het een gestandardiseerde training is (waarbinnen variatie mogelijk is) en de verwerking en opslag van resultaten geautomatiseerd zijn.



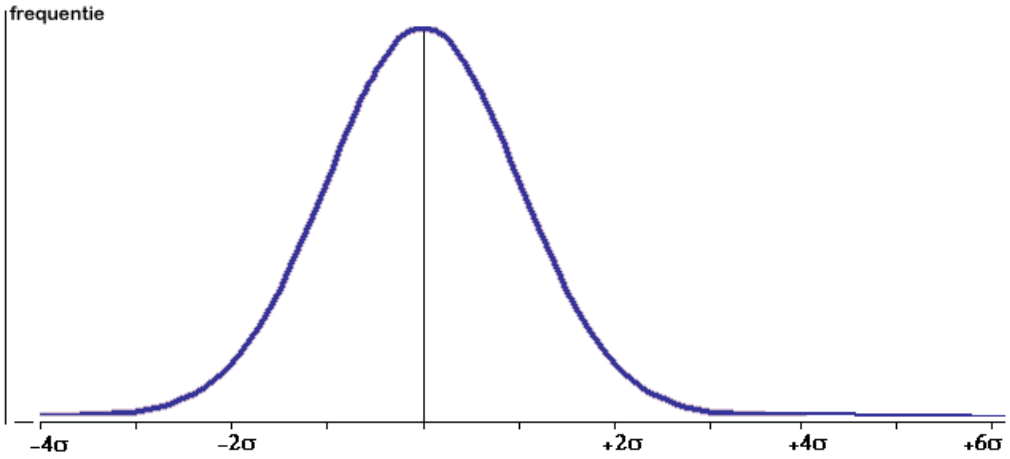
Bron: Intro IT Security

Check

In Check-fase worden de key performance indicators (KPI's) gemeten, wat jaarlijks gebeurt. Dit wordt uitgevoerd aan de hand van een evaluatiekader. Dit kader is gebaseerd op de Six Sigma benadering, welke hieronder besproken zal worden. Niet alle KPI's zullen echter met Six Sigma geevalueerd kunnen worden, sommige KPI's worden binair gemeten en zodoende geevaleerd in het wel of niet kunnen voldoen aan het criterium.

Six Sigma

De Six Sigma benadering is ontwikkeld om kwaliteitsverbetering in organisatieprocessen op een gestructureerde manier aan te pakken. Statistiek is een belangrijk element binnen deze benadering. De griekse letter sigma (σ) geeft de standaarddeviatie weer. Met Six Sigma wordt een statistische weergave van de proceskwaliteit weergegeven, waarbij er gebruik wordt gemaakt van de normaalverdeling (of Gauss-verdeling). Bij de normaalverdeling geldt dat 68,2 % van de waarden binnen de grenzen van -1 standaarddeviatie of +1 standaarddeviatie van het gemiddelde of de streefwaarde ligt. In Six Sigma komt een kwaliteitsniveau van 1 sigma overeen met 68,2 %. In termen van proceskwaliteit betekent dit dat het proces in 68,2 % van de gevallen zonder fouten verloopt. Voor een kwaliteitsniveau van 2 sigma is deze succeskans 95,4 % (in de normaalverdeling ligt 95,4 % van de waarden in het interval van -2 standaarddeviaties tot +2 standaarddeviaties).
Met het verhogen van het kwaliteitsniveau wordt zodoende de afwijking van het gemiddelde of de streefwaarde binnen een proces verkleind. Voor een kwaliteitsniveau van 6 sigma is de succeskans 99,99966 % (ReVelle 2004: 42).



Six Sigma wordt hier uitgedrukt in de succeskans, maar wordt vaker uitgedrukt in het aantal incidenten. Doordat het aantal incidenten inzichtelijk wordt gemaakt, kan er specifiek worden onderzocht hoe dit kan worden teruggebracht. Met een niveau van 6 sigma ligt dat aantal op ongeveer 3,4 incidenten per miljoen. In theorie is het aantal incidenten 2 per miljard, maar in de praktijk vindt er op de lange termijn een verschuiving (process shift) van 1,5 standaarddeviaties plaats. Hoewel het kwaliteitsniveau van 6 sigma (3,4 incidenten per miljoen) zeer streng lijkt en een groter aantal incidenten in een bepaalde processtap acceptabel kan zijn, neemt bij meerdere processtappen de totale kans op incidenten toe. Binnen de literatuur wordt gekozen voor het niveau van 6 sigma als streefwaarde. Met een hogere sigma zou er sprake moeten zijn van een nagenoeg perfect proces: bij 7 sigma is het aantal incidenten 0,2 per miljoen. Bij een lagere sigma dan 6 sigma zal het aantal incidenten groter zijn en daarmee minder acceptabel zijn.
De niveau-indeling voor de proceskwaliteit is als volgt (ReVelle 2004: 41):

σ Level	Process Centered	Process Shift = ± 1.5s
0,5	617.075 ppm	841.345 ppm
1,0	317.311	691.462
1,5	133.614	500.000
2,0	45.500	308.538
2,5	12.419	158.655
3,0	2.700	66.807
3,5	465	22.750
4,0	63	6.210
4,5	7	1.350
5,0	57 ppb	233
5,5	38	32
6,0	2	3,4
6,5	0,1	0,3
7,0	0,001	0,02

Evaluatie van de KPI's

De meting van de KPI's wordt, zoals gebruikelijk binnen de Six Sigma benadering, niet uitgedrukt in de succeskans. Er is hier gekozen om te kijken naar de faalfactor. Het sigmaniveau kan aan de hand van de volgende formule bepaald worden:

([faalfactor] / [totaal]) * 1.000.000

Per KPI is de faalfactor vastgesteld:

KPI #	Faalfactor
01	Aantal niet opgenomen regels van derden
02	Aantal van de niet opgenomen gedragsregels
03	Aantal van de niet opgenomen beleidsregels
04	Aantal incidenten per proces (ten opzichte van het totaal aantal werkuren)
05	Aantal medewerkers dat de training niet succesvol afrondt
06	Kosten van incidenten te wijten aan menselijk gedrag
07	Aantal, aan menselijk gedrag te wijten, aangetroffen malware
08	Aantal bezoekers van intranet dat beveiligingsitems niet hebben bekeken
09	Aantal medewerkers dat geen nieuwsbrief heeft gekregen
10	Aantal werkoverleggen waarin niet over beveiliging gesproken wordt
11	Aantal medewerkers met een onvoldoende voor de toets
12	Aantal aan menselijk gedrag te wijten afwijkingen op auditresultaten
13	Aantal bestuursleden dat geen presentatie/training heeft gevolgd
14	Aantal slecht ingevulde zelfevaluaties
15	Aantal medewerkers dat jaarlijks geen training heeft gevolgd
16	Aantal nieuwe medewerkers die geen introductietraining hebben gevolgd
17	Aantal medewerkers zonder getekende schriftelijke bevestiging
18*	Doelgroepen niet bepaald
19	Niet geimplementeerde processtappen binnen methodiek
20*	Geen opname sanctiebeleid binnen awarenessprogramma
21	Aantal medewerkers dat geen toets heeft afgelegd
22	Aantal ontbrekende KPI's vanuit de methodiek
23*	Geen opname meldingsplicht binnen awareness programma
24	Kosten van het awareness programma (t.o. van de kosten vorig meetmoment)
25	Niet ondernomen activiteiten op basis van de act fase

* deze KPI wordt binair gemeten en zodoende het wel (6 sigma) of geen opname (0 sigma) van betreffende onderdeel.

Om de werking van Six Sigma in het evaluatiekader te verhelderen, zullen hier twee voorbeelden worden uitgewerkt:

- KPI 04
  In een proces worden drie incidenten gemeld. In dit proces werken zes mensen, 8 uur per dag, vijf dagen per week, 46 weken per jaar. Het proces bevat zodoende (6x8x5x46=) 11.040 werkuren. Om het sigmaniveau te kunnen berekenen, wordt de faalfactor 3 gedeeld door het totaal 11.040, wat wordt vermenigvuldigd met een miljoen. Dit is 271,7 incidenten per miljoen werkuren. De waarde 271,7 ligt tussen 4,5σ en 5σ, dus dit proces is redelijk goed aan de maat.

- KPI 08
  Het beleid is dat er minstens 12 keer per jaar in een werkoverleg wordt gesproken moet worden over beveiliging. Blijkens de agenda en de notulen, is er binnen een afdeling elf maal een beveiligingsgerelateerd onderwerp aan de orde gekomen. De faalfactor 1 wordt gedeeld door het totaal 12, dat wordt vermenigvuldigd met een miljoen. Dit geeft een waarde van 8333,33, dat ligt tussen 3,5σ en 4σ.

Dit geeft een redelijke kwaliteit aan, hoewel er slechts eenmaal niet is gesproken over beveiliging. Toch is het heel duidelijk voor deze afdeling waar de verbetermogelijkheden liggen. Hierbij moet worden opgemerkt dat deze KPI hier dus op afdelingsniveau is besproken, maar dat deze ook op organisatieniveau kan worden gemeten.

Act

In de Act-fase worden aan de hand van de evaluatie verbeteringen opgesteld, waarna weer een Plan-fase van start gaat waarin de verbeteringen worden gepland. In deze scriptie wordt onder de Act-fase aandacht besteed aan een maturity model. Dit model geeft weer op welk niveau een organisatie zit, waarbij het niveau afgezet kan worden tegen het niveau van organisaties binnen dezelfde branch of sector.

Maturity model

Met een maturity model wordt het niveau van een organisatie ten aanzien van security awareness geindexeerd. Doordat organisaties niet onderling hun score per KPI vergelijken, geven zij niet te veel prijs ten aanzien van hun concurrenten. Daarnaast is het overzichtelijker om één waarde te vergelijken, dan 25 scores. Het maturity model bestaat uit 5 levels, gebaseerd op het Capability Maturity Model (CMMI Product Team, 2002).

De maturity levels bestaan uit een aantal KPI's die voor het desbetreffende maturity level relevant geacht worden. Om een KPI te kunnen meetellen in het maturity model, kan er een minimum sigmaniveau voor de betreffende KPI worden geformuleerd. Sommige KPI's kunnen worden meegeteld als er minstens 6 sigma gescoord wordt, terwijl voor andere KPI's een score van bijvoorbeeld minstens 3,5 sigma voldoende wordt geacht. Deze weging kan voor elke branch of sector worden opgesteld. In de onderstaande uitwerking is een mogelijke weging van de KPI's voor de retail banking geformuleerd. Daar statistische gegevens inzake de gebruikte KPI's niet voorhanden zijn, is er hier sprake van een inschatting.

Maturity Level 1: Initial

Het maturity level 1 is het laagste niveau en kenmerkt zich doordat er geen structuur is in het beleid ten aanzien van security awareness. De organisatie reageert slechts op incidenten. Het awareness programma kan niet worden geëvalueerd op basis van KPI's.

# KPI	Minimale σ
geen	n.v.t.

Maturity Level 2: Managed

Op het tweede maturity level is er sprake van management van processen. De methodiek voor security awareness wordt gevolgd. Er wordt ook gebruik gemaakt van kennis die eerder is opgedaan.

# KPI	Minimale σ	# KPI	Minimale σ
18	6	22	1,5
19	2,5		

Maturity Level 3: Defined

Maturity level 3 wordt gekenmerkt door een goede integratie van standaarden en procedures in de belangrijkste processen, welke zijn beschreven tot op groot detail. Het grootste verschil met maturity level 2 ligt in de standaardisatie van de verschillende processen.

# KPI	Minimale σ	# KPI	Minimale σ
01	2	18	6
02	2	19	6
03	2	22	2,5
12	2	25	4
17	4		

Maturity Level 4: Quantitatively Managed

Het vierde maturity level bouwt voort op het derde level, maar onderscheidt zich doordat processen gemeten worden en dat op basis van deze metingen bijsturing plaats kan vinden. Op dit niveau is de voorspelbaarheid van het proces groot doordat gebruik wordt gemaakt van statistische en andere kwantitatieve technieken.

# KPI	Minimale σ	# KPI	Minimale σ
01	3	14	5
02	3	15	5
03	3	16	5
04	3	17	6
05	5	18	6
06	2	19	6
07	4	20	6
08	3	21	4
09	3	22	3,5
10	4	23	6
11	5	24	0,5
12	3	25	6
13	6		

Maturity Level 5: Optimizing

Het maturity level 5 is het hoogste niveau, waarbinnen de nadruk ligt op een continue verbetering van de processen. Een belangrijk verschil met het vierde level is dat gestreefd wordt om de variatie binnen het proces onder controle te hebben, zodat het niet afhankelijk is van specifieke omstandigheden.

# KPI	Minimale σ	# KPI	Minimale σ
01	6	14	6
02	6	15	6
03	6	16	6
04	6	17	6
05	6	18	6
06	6	19	6
07	6	20	6
08	6	21	6
09	6	22	6
10	6	23	6
11	6	24	1
12	6	25	6
13	6		

Scenario

Dit scenario dient als voorbeeld voor de toepassing van de methodiek binnen de retail banking. Het betreft een denkbeeldige organisatie binnen de retail banking, die een awareness programma wil implementeren en daartoe gebruik maakt van de methodiek. Om te laten zien dat het gaat om een proces van continue verbeteringen, zal binnen dit scenario de cyclus tweemaal worden doorlopen.

In dit scenario wil een organisatie een awareness programma implementeren. Deze organisatie opereert in de private lending, en bestaat uit consultants en een telefonische gecombineerde sales en service desk. De ICT-diensten zijn uitbesteed, deze leverancier heeft geen regels ten aanzien van gewenst gedrag van hun klanten. Met het awareness programma beoogt de organisatie in de eerste plaats compliance te bereiken en in de tweede plaats hoopt men door gebruik van een methodiek hier effectief en efficiënt invulling aan te geven. De concrete doelstellingen zijn tweeleding: de kosten van het programma moeten zo laag mogelijk zijn en de organisatie wil weten waar hij staat ten opzichte van andere organisaties in dezelfde branche. De organisatie heeft nog geen awareness programma, dus hoeft in dit scenario geen inventarisatie uit te voeren om het beginniveau te bepalen. Het maturity level van de organisatie is zodoende level 1. De organisatie besluit na een jaar een evaluatie uit te voeren.

Plan I

In de Plan-fase worden er doelgroepen geformuleerd. De organisatie volgt de ISCO-lijst, maar versimpelt deze door de medewerkers in twee groepen in te delen. Het bestuur en de consultants vallen onder de doelgroep ‘managers / (associate) professionals’. De overige medewerkers vallen onder de doelgroep ‘clerical support workers / service and sales workers’.

Aangezien het een doelstelling is om het programma met zo laag mogelijke kosten uit te voeren, wordt er gekozen voor maatregelen met de indicatie laag of middel op de kostenschaal. Voor beide doelgroepen wordt er bepaald dat de maatregel *Beveiligingsverantwoordelijkheden opnemen binnen het contract* en de maatregel *Postercampagne met een focus op beveiligingsonderwerpen* wordt uitgevoerd. Daarnaast wordt de maatregel *Presentaties* voor de doelgroep managers / (associate) professionals gekozen. Voor de doelgroep clerical support workers / service and sales workers wordt

gekozen voor de maatregel *Persoonlijke instructies en ondersteuning*. De onderstaande tabel geeft de koppeling tussen de criteria en de maatregelen weer.

Criteria	Maatregelen
Inzicht in regels vereist vanuit derden	n.v.t.
Inzicht in regels uit de gedragscode	Binnen contract / Presentaties / Persoonlijke begeleiding
Onderbouwing vanuit vastgesteld beleid	Binnen contract / Presentaties / Persoonlijke begeleiding
Inzicht bieden in bedreigingen en risico's	Posters / Presentaties / Persoonlijke begeleiding
Integratie in bedrijfsprocessen	Presentaties / Persoonlijke begeleiding
Kennis van relevante wet- en regelgeving	Presentaties / Persoonlijke begeleiding
Betrokkenheid bestuur en raad van commissarisen	Presentaties
Jaarlijkse deelname	Presentaties / Persoonlijke begeleiding
Deelname bij indiensttreding	Persoonlijke begeleiding
Controleerbare bevestiging (op schrift)	Binnen contract
Doelgroepen-bepaling	Opgenomen in Plan-fase
Continu proces	Planning voor uitvoer en evaluatie
Inzicht bieden in disciplinaire maatregelen	Presentaties / Persoonlijke begeleiding
Toetsing van medewerkers	-
Vergelijkbaarheid t.a.v. maturity model	Opgenomen in Act-fase
Opnemen meldingsplicht	Binnen contract / Posters / Presentaties / Persoonlijke begeleiding
Laag mogelijke kosten	-
Lerend vermogen	-

Niet alle criteria kunnen worden gekoppeld aan een maatregel. Het eerste criteria is bijvoorbeeld niet van toepassing omdat de ICT dienstenleverancier geen gedragsregels stelt. De criteria Doelgroepen-bepaling, Continu proces en Vergelijkbaarheid t.a.v. maturity model zijn niet te relateren aan een maatregel, maar komen aan bod binnen de fasen van de methodiek. Het criterium Toetsing van medewerkers heeft de organisatie bewust niet opgenomen in de methodiek, omdat de organisatie heeft gekozen voor goedkope maatregelen. Ten aanzien van de criteria Laag mogelijke kosten en Lerend vermogen kan deze organisatie nog niet vergelijken, aangezien de methodiek voor het eerst is opgestart. Dit zal betekenen dat er nul sigmawaarde wordt gescoord op de KPI's die horen bij deze betreffende criteria.

Do I

In de Do-fase worden de maatregelen uitgevoerd.

- Het management krijgt de opdracht om er zorg voor te dragen dat in de contracten van nieuwe medewerkers wordt opgenomen dat zij op de hoogte dienen te zijn van het beleid en de regels uit de gedragscode. Daarnaast is er in het contract opgenomen dat de medewerker een meldingsplicht heeft ten aanzien van beveiligingsincidenten.
- De posters worden in eigen beheer ontworpen en geproduceerd. De posters worden opgehangen in de gangen. De posters blijven een jaar hangen.
- Na de start van het programma worden er twee bijeenkomsten georganiseerd waarbij een presentatie wordt verzorgd voor de doelgroep managers / (associate) professionals. Hierbij is er aandacht voor een breed scala aan beveiligingsonderwerpen, waarbij onder andere het

beleid, de gedragscode, de relevante wet- en regelgeving, de mogelijke bedreigingen en risico's en de disciplinaire maatregelen bij overtreding aan de orde komen.

- De maatregel *Persoonlijke begeleiding* ten aanzien van ondersteuning van de doelgroep clerical support workers / service and sales workers wordt door het management uitgevoerd in het inwerktraject en de dagelijkse begeleiding.

Check I

Na een jaar wordt een evaluatie uitgevoerd. In deze Check-fase worden de key performance indicators (KPI's) gemeten en de sigma-waarde bepaald. De volgende sigmawaarden zijn binnen dit voorbeeld gekozen ter illustratie van de methodiek.

KPI #	Faalfactor op totaal	σ
01	Aantal niet opgenomen regels van derden	6
02	Aantal van de niet opgenomen gedragsregels	3
03	Aantal van de niet opgenomen beleidsregels	3
04	Aantal incidenten per proces (ten opzichte van het totaal aantal werkuren)	2,5
05	Aantal medewerkers dat de training niet succesvol afrondt	0
06	Kosten van incidenten te wijten aan menselijk gedrag	2
07	Aantal, aan menselijk gedrag te wijten, aangetroffen malware	1
08	Aantal bezoekers van intranet dat beveiligingsitems niet hebben bekeken	0
09	Aantal medewerkers dat geen nieuwsbrief heeft gekregen	0
10	Aantal werkoverleggen waarin niet over beveiliging gesproken wordt	1
11	Aantal medewerkers met een onvoldoende voor de toets	0
12	Aantal aan menselijk gedrag te wijten afwijkingen op auditresultaten	1
13	Aantal bestuursleden dat geen presentatie/training heeft gevolgd	6
14	Aantal slecht ingevulde zelfevaluaties	0
15	Aantal medewerkers dat jaarlijks geen training heeft gevolgd	0
16	Aantal nieuwe medewerkers die geen introductietraining hebben gevolgd	0
17	Aantal medewerkers zonder getekende schriftelijke bevestiging	2
18	Doelgroepen niet bepaald	6
19	Niet geimplementeerde processtappen binnen methodiek	2,5
20	Geen opname sanctiebeleid binnen awarenessprogramma	6
21	Aantal medewerkers dat geen toets heeft afgelegd	0
22	Aantal ontbrekende KPI's vanuit de methodiek	1,5
23	Geen opname meldingsplicht binnen awareness programma	6
24	Kosten van het awareness programma (t.o. van de kosten vorig meetmoment)	0
25	Niet ondernomen activiteiten op basis van de act fase	0

Uit deze evaluatie blijkt dat er veel incidenten zijn die te wijten zijn aan medewerkers, en dat deze incidenten hoge kosten met zich meebrengen. Uit de auditresultaten blijkt dat het merendeel aan incidenten plaatsvindt op de sales en service desk. Aangezien alleen medewerkers met een nieuw contract of verlenging van het contract, hebben moeten tekenen voor het ter kennis nemen van het geldende beleid en gedragsregels, wordt hierop laag gescoord.

Act I

Het startniveau in het maturity model was voor deze organisatie level 1. Na een jaar blijkt de organisatie maturity level 2 bereikt te hebben. De organisatie had zich geen doel gesteld ten aanzien

van het te bereiken maturity level, maar is teleurgesteld in het aantal incidenten dat, ondanks het awareness programma, is voorgekomen. De organisatie heeft bij de brancheverenigingde gegevens ten aanzien van het maturity level van andere organisaties opgevraagd en hieruit blijkt dat de organisatie een lager maturity level heeft dan de concurrenten.

Om het aantal incidenten terug te dringen en te komen tot een hoger maturity level, worden er verbeteringen geformuleerd. Gezien de incidenten op de werkvloer en de auditresultaten moet de organisatie concluderen dat de maatregel *Persoonlijke begeleiding* niet doeltreffend is. In de dagelijkse praktijk blijkt security awareness onvoldoende aandacht te krijgen. Een voorgestelde verbetering is om deze maatregel beter vorm te geven, en een extra maatregel voor de doelgroep clerical support workers / service and sales workers te formuleren.

Ten aanzien van het tekenen van het contract met daarin de bepaling dat de medewerker op de hoogte dient te zijn van het beleid, de gedragscode en de meldingsplicht, wil de organisatie alle medewerkers een addendum op het contract voorleggen.

Plan II

De organisatie wil er zeker van zijn dat het gehele spectrum aan beleid is opgenomen binnen het awareness programma. Daartoe spreekt de organisatie de ambitie uit om minimaal maturity level 3, te weten defined, te behalen. Om een goede structuur in het programma te bereiken en de kosten terug te dringen van incidenten waaraan menselijke fouten ten grondslag liggen, is de organisatie bereid meer te investeren in het awareness programma.

Hoewel de maatregel *Persoonlijke begeleiding* niet doeltreffend bleek te zijn, komt deze maatregel niet te vervallen. De organisatie is van mening dat het beleid gedragen dient te worden door de gehele organisatie, en dat dit in de dagelijkse praktijk een plaats moet hebben. Binnen de prestaties aan het management dient hiertoe meer aandacht te worden besteed. De organisatie heeft daarnaast de interne controleur gevraagd de controle op de uitvoering van deze maatregel te intensiveren.

Om de incidenten op de werkvloer te beheersen, wordt er bepaald dat er een extra maatregel nodig is voor de doelgroep clerical support workers / service and sales workers. Zodoende wordt er gekozen om de maatregel *Verplichte klassikale training (met afsluitende toets)* voor deze doelgroep in te voeren.

De onderstaande tabel geeft de koppeling tussen de criteria en de maatregelen weer.

Criteria	Maatregelen
Inzicht in regels vereist vanuit derden	n.v.t.
Inzicht in regels uit de gedragscode	Binnen contract / Presentaties / Persoonlijke begeleiding / Training en toets
Onderbouwing vanuit vastgesteld beleid	Binnen contract / Presentaties / Persoonlijke begeleiding / Training en toets
Inzicht bieden in bedreigingen en risico's	Posters / Presentaties / Persoonlijke begeleiding / Training en toets
Integratie in bedrijfsprocessen	Presentaties / Persoonlijke begeleiding
Kennis van relevante wet- en regelgeving	Presentaties / Persoonlijke begeleiding / Training en toets
Betrokkenheid bestuur en raad van commissarisen	Presentaties
Jaarlijkse deelname	Presentaties / Persoonlijke begeleiding
Deelname bij indiensttreding	Persoonlijke begeleiding
Controleerbare bevestiging (op schrift)	Binnen contract
Doelgroepen-bepaling	Opgenomen in Plan-fase
Continu proces	Planning voor uitvoer en evaluatie
Inzicht bieden in disciplinaire maatregelen	Presentaties / Persoonlijke begeleiding / Training en toets
Toetsing van medewerkers	Training en toets
Vergelijkbaarheid t.a.v. maturity model	Opgenomen in Act-fase
Opnemen meldingsplicht	Binnen contract / Posters / Presentaties / Persoonlijke begeleiding
Laag mogelijke kosten	Opgenomen in Check-fase
Lerend vermogen	Opgenomen in Check-fase

Do II

In de Do-fase worden de maatregelen uitgevoerd.

- Het management krijgt de opdracht om er zorg voor te dragen dat in de contracten van nieuwe medewerkers wordt opgenomen dat zij op de hoogte dienen te zijn van het beleid, de gedragscode en de meldingsplicht. De maatregel om alle medewerkers een addendum op het contract voor te leggen, wordt ingepland voor het eerst volgende functioneringsgesprek van een medewerker.
- Er worden in eigen beheer nieuwe posters ontworpen en geproduceerd. De posters worden opgehangen in de gangen. De posters blijven een jaar hangen.
- In deze tweede Do-fase wordt er een bijeenkomst georganiseerd waarbij een presentatie wordt verzorgd voor de doelgroep managers / (associate) professionals.
- De maatregel *Persoonlijke begeleiding* voor de doelgroep clerical support workers / service and sales workers wordt door het management uitgevoerd in het inwerktraject en de dagelijkse begeleiding. Dit staat onder controle van de interne controleur, die de evaluaties van het inwerkprogramma bekijkt.
- De klassikale training voor de clerical support workers / service and sales workers wordt eens per kwartaal gehouden, waarbij elke medewerker de verplichting heeft om voor het einde van het jaar een van de georganiseerde sessies bijgewoond te hebben. Daarnaast moeten de medewerkers de bijbehorende toets met succes hebben voltooid.

Check II

Na een jaar wordt een tweede evaluatie uitgevoerd. De sigma-waarde van de key performance indicators (KPI's) wordt bepaald. De sigmawaarden in de onderstaande tabel zijn weer ter illustratie, maar nu gebaseerd op de prestaties van de organisatie in de eerste cyclus.

KPI #	Faalfactor op totaal	σ
01	Aantal niet opgenomen regels van derden	6
02	Aantal van de niet opgenomen gedragsregels	6
03	Aantal van de niet opgenomen beleidsregels	4
04	Aantal incidenten per proces (ten opzichte van het totaal aantal werkuren)	4
05	Aantal medewerkers dat de training niet succesvol afrondt	3,5
06	Kosten van incidenten te wijten aan menselijk gedrag	4
07	Aantal, aan menselijk gedrag te wijten, aangetroffen malware	3
08	Aantal bezoekers van intranet dat beveiligingsitems niet hebben bekeken	0
09	Aantal medewerkers dat geen nieuwsbrief heeft gekregen	0
10	Aantal werkoverleggen waarin niet over beveiliging gesproken wordt	2,5
11	Aantal medewerkers met een onvoldoende voor de toets	1,5
12	Aantal aan menselijk gedrag te wijten afwijkingen op auditresultaten	2
13	Aantal bestuursleden dat geen presentatie/training heeft gevolgd	6
14	Aantal slecht ingevulde zelfevaluaties	0
15	Aantal medewerkers dat jaarlijks geen training heeft gevolgd	3,5
16	Aantal nieuwe medewerkers die geen introductietraining hebben gevolgd	0
17	Aantal medewerkers zonder getekende schriftelijke bevestiging	4
18	Doelgroepen niet bepaald	6
19	Niet geimplementeerde processtappen binnen methodiek	6
20	Geen opname sanctiebeleid binnen awarenessprogramma	6
21	Aantal medewerkers dat geen toets heeft afgelegd	3,5
22	Aantal ontbrekende KPI's vanuit de methodiek	2,5
23	Geen opname meldingsplicht binnen awareness programma	6
24	Kosten van het awareness programma (t.o. van de kosten vorig meetmoment)	0
25	Niet ondernomen activiteiten op basis van de act fase	6

Uit de evaluatie blijkt dat er sprake is van verbetering op de voorgenomen onderdelen. Ten aanzien van het aantal incidenten is er bijvoorbeeld een daling waarneembaar.

Act II

Na het eerste jaar had de organisatie maturity level 1 bereikt en na het tweede jaar blijkt de organisatie de ambitie om maturity level 3 te halen, waargemaakt te hebben. Desalnietemin zijn er voor de organisatie nog voldoende verbetermogelijkheden te identificeren, bijvoorbeeld de implementatie van de volledige methodiek (zodat er op alle KPI's gescoord kan worden). Door de investering blijken de kosten hoger te zijn, dit zal de komende jaren terugverdiend kunnen worden als het aantal incidenten waar medewerkers schuld aandragen en welke hoge kosten kennen, terug worden gebracht. Het is aan de organisatie om een juiste balans te vinden tussen deze investeringen en de kosten van non-compliance gecombineerd met de kosten van incidenten waar menselijke fouten aan ten grondslag liggen.

Slotopmerkingen bij het scenario

Binnen dit scenario is tweemaal de methodiek doorlopen om een voorbeeld te schetsen van de mogelijke toepassing. Dit scenario betreft een denkbeeldige organisatie. Met statistische gegevens van organisaties in de retail banking kan er in werkelijkheid worden bepaald wat goede sigma waarden voor de verschillende KPI's zijn. Daarnaast dient de praktijk uit te wijzen of bepaalde kenmerken van de organisatie, zoals organisatieomvang, structuur en kapitaal, van invloed zijn op potentieel te behalen sigma waarden.

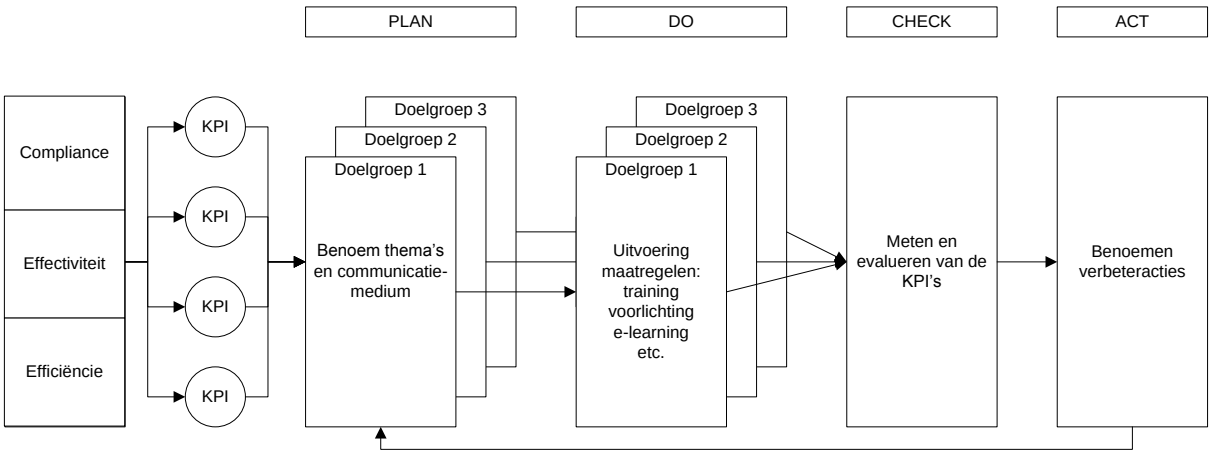
< this page intentionally left blank >

Conclusie en aanbevelingen

Hoewel security awareness vanuit de wet- en regelgeving verplicht is voor de Nederlandse retail banking bevatten de bestaande normenkaders geen verwijzing naar een exacte methodiek om een awareness programma vorm te geven. De doelstelling van de scriptie is te komen tot een eenduidige en meetbare methode welke gebaseerd is op de noodzaak te voldoen aan wet- en regelgeving waarbij daarnaast rekening is gehouden met de kosteneffectiviteit. Daartoe vormde de volgende vraagstelling de basis van deze scriptie:

In hoeverre is het mogelijk te komen tot een praktische en minimalistische methode voor security awareness binnen de Nederlandse retail banking?

Centraal in de beantwoording van de hoofdvraag staat de onderbouwing van de methodiek. Hoewel wet- en regelegeving geen concrete handvatten bieden voor een methodiek, zijn er wel eisen en normen ten aanzien van security awareness. Een belangrijke pijler van de methodiek is zodoende compliance. Aangezien voor de retail banking, net als voor elke commerciële sector, kosteneffectiviteit essentieel is, zijn effectiviteit en efficiëntie de twee andere pijlers. Hiermee is bereikt dat de methodiek onderbouwd kon worden met criteria voortkomend uit de drie pijlers, die vervolgens omgezet zijn naar meetbare eenheden (Key Perfomance Indicators). De methodiek is gebaseerd op de Deming-cydus welke wordt weergegeven in de volgende figuur:



In hoeverre er binnen deze scriptie is gekomen tot een invulling van de methodiek, is per fase verschillend. Voor de eerste drie fasen kan geconcludeerd worden dat er is gekomen tot een praktische en minimalistische methode voor security awareness binnen de Nederlandse retail banking. Ten aanzien van de Plan-fase biedt de methodiek een indeling in doelgroepen en een ruime set aan maatregelen die ten aanzien van security awareness genomen kunnen worden. Dit vormt de basis voor de uitvoer van een awareness programma in de Do-fase. Binnen de Check-fase is er binnen de methodiek een evaluatiekader geformuleerd. Dit kader is gebaseerd op de Six Sigma benadering, waarbinnen de opgestelde KPI's daadwerkelijk gemeten kunnen worden. Hierbij zijn de KPI's uitgewerkt in faalfactoren, die kunnen worden afgezet naar een sigmaniveau. Door te werken met faalfactoren, kan er concreet worden aangetoond waar verbeteringen noodzakelijk zijn. Onder de Act-fase is in deze scriptie aandacht besteed aan ontwikkelen van een maturity model. Hierbij is per maturity level uitgewerkt welke KPI's relevant zijn. Daarnaast is er getracht een indicatie te geven van het minimale sigmaniveau dat een KPI op een bepaald maturity level zou moeten hebben. Dit niveau is wegens het ontbreken van onderzoeksgegevens gebaseerd op een ruwe inschatting van mogelijke faalfactoren en de daarbij horende vertaling naar een sigmaniveau.

Aanbevelingen

De belangrijkste aanbevelingen richten zich op de verdere uitwerking van de methodiek voor security awareness, en onderzoek naar de praktische toepassing:

- Aan de hand van verder onderzoek bij verschillende organisaties in de retail banking, of de financiële sector in bredere zin, zou voor elke KPI bepaald moeten worden wat de 'normale' sigma afwijking zou moeten zijn.
- De gekozen KPI's kunnen verder geoptimaliseerd worden door het inwinnen van statistische gegevens van bedrijven die de methodiek toepassen of het simuleren van de methodiek gebaseerd op bestaande data (voor zover beschikbaar) van onderdelen uit de methodiek.
- Er zou onderzocht moeten worden wat het minimale sigmaniveau is, dat een KPI op elk maturity level zou moeten zijn om voor de retail banking compliance te bereiken.
- Door verder onderzoek naar faalfactoren kan een weging van deze toegepast worden waardoor de nauwkeurigheid van de methode toe zal nemen.
- Onderzocht moet worden of binnen de branch een beheerder van de standaard aangesteld dient te worden. Mocht blijken dat voor de onderlinge opmaat de door deelnemers gehanteerde interpretatie van KPI's teveel afwijkt, dan zal een centraal orgaan de regie in handen moeten nemen. Dit geldt eveneens als blijkt dat de deelnemers een onderling sterk afwijkend *audit risk* (het risico dat een auditor een onjuiste verklaring afgeeft) kennen. Het centraal orgaan kan verbeteringen voorstellen, de formele standaard aanpassen en de onderlinge vergelijkbaarheid versterken. Bij veelvuldige toepassing van de standaard zal een als zodanig ingesteld orgaan noodzakelijk blijken.
- Wat betreft de inhoudelijke maatregelen binnen de methodiek, zal verder onderzocht moeten worden of er een onderverdeling valt te maken in functiegroepen en het best daarbij aansluitende leertype (superficial processing versus systematic processing).

Literatuurlijst

Bank for International Settlements (BIS) (2001). *Core Principles for Systemically Important Payment Systems*. Basel: Bank for International Settlements.

Basel Committee on Banking Supervision (2006). *International Convergence of Capital Measurement and Capital Standards*. Basel: Bank for International Settlements.

Basten, N. en M. Wijnmaalen (2003). 'Greep op security awareness'. *ITBeheer* 7 (september 2003): pp. 49-52.

Berry, L.M. (1997). *Psychology at Work; An introduction to Industrial and Organizational Psychology*. Boston: McGraw-Hill.

British Standards Institution (2005). *ISO/IEC 17799:2005 - Information technology -Security techniques; Code of practice for information security management*. Londen: British Standards Institution.

CMMI Product Team (2002). *Capability Maturity Model Integration (CMMI[SM]) Version 1.1*. Pittsburgh: Carnegie Mellon Software Engineering Institute.

Commissie Corparate Governance (2003). *De Nederlandse Corparate Governance Code; Beginselen van deugdelijk ondernemingsbestuur en best practice bepalingen*. Den Haag: Monitoring Commissie Corporate Governance Code.

De Nederlandsche Bank (2001). *Regeling Organisatie en Beheersing*. Amsterdam: De Nederlandsche Bank.

European Network and Information Security Agency (ENISA) (2007). *Current Practice and the measurement of success*. Heraklion: ENISA.

European Central Bank (2003). *Electronic Money System Security Objectives*. Frankfurt: European Central Bank.

European Commission (1995). *Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data*. Luxembourg: European Commission.

Furnell, S.M., M. Gennatou en P.S. Dowland (2002). 'A prototype tool for information security awareness and training'. *Logistics Information Management* 15 (5/6): pp. 352 – 357.

Heijden, P.F. van der, J.M. van Slooten, E. Verhulp (eds) (2003). *Arbeidsrecht; de tekst van Titel 7.10 BW en andere relevante regelgeving met betrekking tot het arbeidsrecht, voorzien van commentaar*. Deventer: Kluwer.

International Standard Classification of Occupation (ISCO) (2008). *Resolution Concerning Updating the International Standard Classification of Occupations*. Geneve: ISCO.

Mast, J. de en R. Does (2005). 'Six Sigma als blauwdruk voor de kenniseconomie'. *Sigma* 3 (juni 2005): pp. 28 – 29.

Ministerie van Justitie (2002). *Handleiding voor verwerkers van persoonsgegevens; Wet bescherming persoonsgegevens*. Den Haag: Ministerie van Justitie.

PCI Security Standards Council (2006). *Payment Card Industry (PCI) Data Security Standard (Version 1.1)*. Wakefield: PCI Security Standards Council.

ReVelle, J.B. (2004). 'Six Sigma; Problem-solving techniques create safer, healthier worksites'. *Professional Safety* (oktober 2004): pp. 38 – 46.

Samenwerkingsverband Audit Aanpak/ Werkgroep Zelfevaluatie (2000). Wpb Zelf evaluatie. Den Haag: College bescherming persoonsgegevens.

Smith, E.R. en D.M. Mackie (2000). *Social Psychology*. Philadelphia: Psychology Press.

Bronvermelding figuren:

Intro IT Security. *E-learning screenshot.* Informatie verkregen van Robert Esschendal. http://www.introitsecurity.com/

PaySquare B.V. *Poster campagne security awareness*. Informatie verkregen van afdeling communicatie. http://www.paysquare.nl/