Het voorliggende afstudeerverslag is een weergave van de specifieke stappen die zijn uitgevoerd gedurende het uitvoeren van de afstudeeropdracht. Verder wordt er ook een evaluatie gegeven betreffende de uitgevoerde werkzaamheden en de producten die zijn opgeleverd.

Afstudeer verslag

Het ontwerpen en implementeren van een nieuwe IS Awareness & Learning Strategie

Giovanni Kromosemito

Referaat

In de periode van 29 oktober 2012 t/m 25 maart 2013 heeft student Giovanni Kromosemito in het kader van zijn studie Information Security Management aan De Haagse Hogeschool een afstudeeropdracht uitgevoerd bij ABN AMRO Bank N.V., gevestigd te Amsterdam.

Omschrijving afstudeeropdracht:

Het ontwerpen en implementeren van een nieuwe IS Awareness & Learning strategie die leidend zal zijn voor ABN AMRO in de komende jaren voor de jaarlijkse Information Security Awareness cyclus.

Het voorliggende afstudeerverslag is een weergave van de specifieke stappen die zijn uitgevoerd gedurende het uitvoeren van de afstudeeropdracht. Verder wordt er ook een evaluatie gegeven betreffende de uitgevoerde werkzaamheden en de producten die zijn opgeleverd.

Descriptoren:

- Afstudeerverslag
- ABN AMRO Bank N.V.
- De Haagse Hogeschool
- NIST SP 800-50
- Information Security Awareness

Voorwoord

Giovanni Kromosemito is een student Information Security Management aan De Haagse Hogeschool (dependance te Zoetermeer). Zijn interesse ligt meer aan de organisatorische en menselijke kant van informatiebeveiliging. Vandaar ook een afstudeeropdracht in de richting van de mens, namelijk Information Security Awareness.

Dit is het verslag geschreven naar aanleiding van de afstudeeropdracht met als doel om de examinatoren inzicht te geven in de uitgevoerde werkzaamheden en de aanpak die ik heb gevolgd gedurende het afstudeertraject. De uitgevoerde werkzaamheden en gevolgde aanpak zijn tevens onderbouwd.

Graag wil ik van deze gelegenheid gebruik maken om een aantal mensen hartelijk te bedanken. Ten eerste wil ik mijn bedrijfsmentor dhr. Joop Zomer bedanken voor de goede begeleiding en ondersteuning tijdens de afstudeerperiode en dhr. Cock Frijters voor het bieden van de mogelijkheid om een opdracht uit te voeren binnen mijn interessegebied. Ook ben ik mijn andere collega's van ABN AMRO dankbaar voor de gezellige en leerzame samenwerking.

Verder wil ik mijn examinatoren vanuit De Haagse Hogeschool, mw. Marjolein Faassen en dhr. Jaap de Bie, bedanken voor hun steun, waardevolle adviezen en begeleiding. Uiteraard gaat mijn dank ook uit naar mijn naasten die mij hebben ondersteund en gemotiveerd gedurende de afstudeerperiode.

De afstudeerperiode heb ik als prettig, leerrijk en uitdagend ervaren!

Ik wens u veel leesplezier toe!

Den Haag, 25 maart 2013

Giovanni Kromosemito

Inhoud

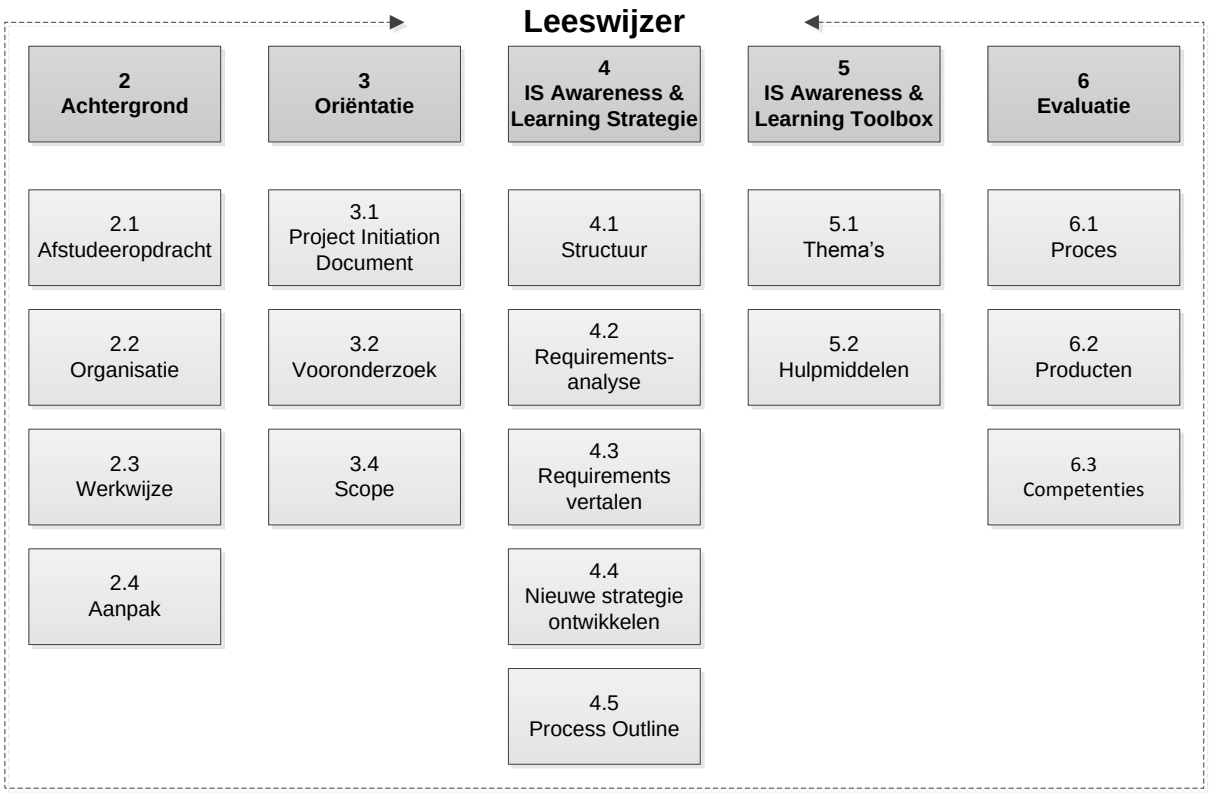
1. Inleiding

Het doel van dit afstudeerverslag is het inzichtelijk maken voor de examinatoren hoe de afstudeeropdracht is uitgevoerd, de werkzaamheden die zijn verricht om dit te bereiken en de aanpak die hiervoor is gehanteerd.

De afstudeeropdracht luidde als volgt:
"Het ontwikkelen en implementeren van een nieuwe informatiebeveiliging awareness en learning strategie voor ABN AMRO"

Deze opdracht heb ik uitgevoerd voor en in samenwerking met de afdeling Information Security Risk Management Nederland (ISRM-NL), die als onderdeel van Information Security Office (ISO) de missie heeft: ervoor zorgdragen dat de vertrouwelijkheid, integriteit en beschikbaarheid van informatie en informatiesystemen van de geografisch in Nederland gelegen ABN AMRO onderdelen en haar relaties, gewaarborgd is.

In de onderstaande figuur is de opbouw van dit afstudeerverslag weergegeven.



Figuur 1: Leeswijzer

2. Achtergrond

2.1. Afstudeeropdracht

Aanleiding
Bij ABN AMRO werd voor de periode van 2008 tot en met 2012 een aanpak gevolgd om de security awareness bij de medewerkers tijdens de integratieperiode van ABN AMRO NL en Fortis NL te bewaken en waar nodig te verhogen.

Probleemstelling
De in 2008 tot en met 2012 gevolgde IS awareness aanpak verloor aan kracht. Uit een evaluatie is gebleken dat het management en de medewerkers niet meer positief waren over deze aanpak. Reacties luidden dat zij de uitgevoerde survey en campagne te eentonig en algemeen vonden omdat zij jaarlijks nagenoeg dezelfde vragen voorgelegd kregen en dat de resultaten uit de survey te globaal waren om er gerichte acties uit te halen. Dit heeft tot gevolg gehad dat de motivatie binnen de business lines voor het uitvoeren van gerichte campagnes afnam, waardoor de hulpmiddelen onvoldoende werden ingezet en er geen significante vooruitgang meer werd bereikt t.a.v. de IS Awareness.

Omdat Security Awareness hoog in het vaandel staat bij ABN AMRO, is er besloten om de huidige aanpak te evalueren en opdracht te geven om voor de komende 3 - 5 jaar een vernieuwde IS Awareness Strategie te bepalen die aansluit op de nieuwe wensen van de organisatie en bij de nieuwe ontwikkelingen in de markt.

Doelstelling
Mijn doel bij deze opdracht is geweest om de opdrachtgever te helpen met het neerzetten van een strategie die aansluit bij de eisen en wensen van de stakeholders, waarin er “state of the art” aanpakken en middelen op het gebied van IS Awareness zijn opgenomen. Dit heb ik bereikt door de eisen en wensen van de stakeholders in kaart te brengen en door onderzoek nieuwe aanpakken en middelen te vinden die aansluiten op de eisen en wensen.

Resultaat
Er is een nieuwe IS Awareness & Learning Strategie vastgesteld voor de komende 3 – 5 jaar die aansluit op de eisen en wensen van de stakeholders. De gerealiseerde invulling van de strategie is afwisselend genoeg om de aandacht van het management en de medewerkers te blijven trekken. Daarnaast is er een IS Awareness & Learning Toolbox samengesteld met middelen die zijn gekozen op basis van de vraag van de stakeholders en het uitgevoerde onderzoek.

Opgeleverde producten

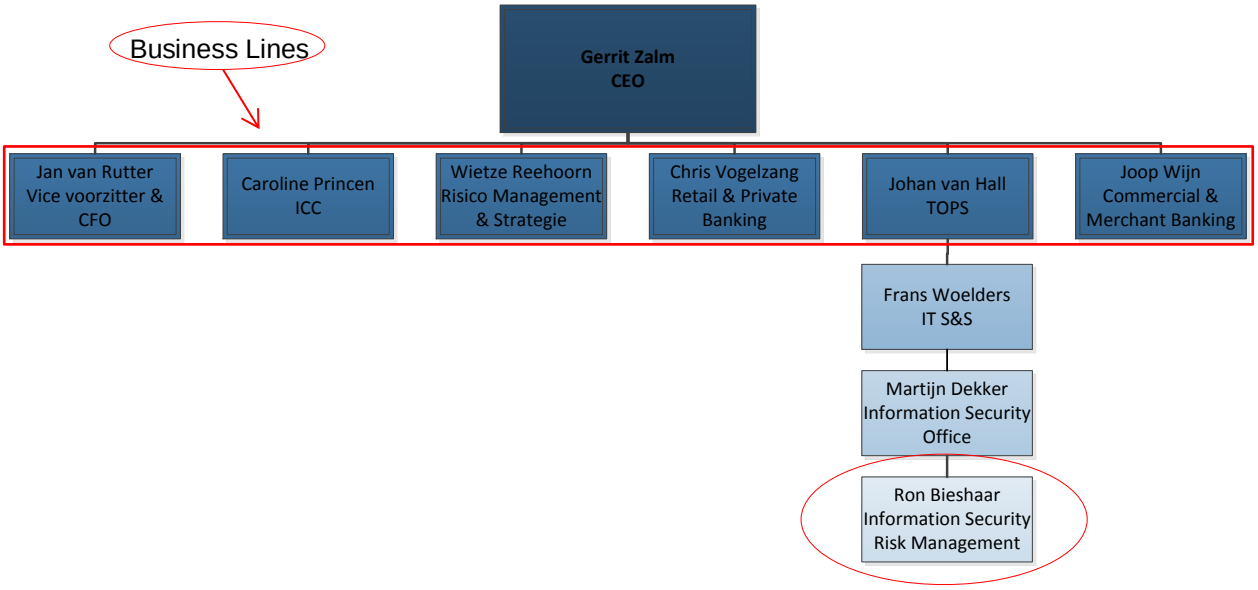
- Project Initiation Document
- IS Awareness & Learning Strategie
- IS Awareness & Learning Toolbox

2.2. Organisatie

ABN AMRO biedt haar particuliere, private banking en zakelijke klanten een volledig producten- en dienstenpakket aan. De bank biedt diepgaande financiële expertise, brede kennis van vele sectoren en een internationaal netwerk ten behoeve van nationale en internationale activiteiten.

Het uitgangspunt van de bank is het inspelen op de veranderende markt en dus op de eveneens veranderende behoeften van de klanten. Daar vraagt deze tijd ook om. Een bank die handelt in de context en realiteit van nu, die de klant met open vizier tegemoet treedt, leert van zijn ervaringen en beseft dat niets belangrijker is dan optimale service.
ABN AMRO is zich bewust van haar verantwoordelijkheid ten opzichte van al haar stakeholders. Vanzelfsprekend wil de bank uitstekende financiële resultaten behalen, maar zonder dat de klanten onverantwoorde risico's lopen.

In 2008 heeft de Nederlandse staat het eigendom verworven van de Nederlandse activiteiten van ABN AMRO Holding N.V. en van Fortis Bank Nederland. In 2010 zijn ABN AMRO en Fortis Bank Nederland gefuseerd. Hierdoor ontstond het huidige ABN AMRO.



Figuur 2: Organogram

Information Security Risk Management (ISRM) is, als onderdeel van Information Security Office (ISO) georganiseerd in twee afdelingen: een nationaal en internationaal opererende afdeling. Mijn focus ligt op de nationale afdeling: Information Security Risk Management Nederland (ISRM NL). De missie van ISRM NL is: ervoor zorgdragen dat de vertrouwelijkheid, integriteit en beschikbaarheid van informatie en informatiesystemen van de geografisch in Nederland gelegen ABN AMRO onderdelen en haar relaties, gewaarborgd is.

De bank is verdeeld in business lines. Binnen iedere business line is een Business Information Security Officer (BISO) aangesteld die verantwoordelijk is voor de coördinatie van informatiebeveiliging binnen de business line. Hiertoe behoort ook de IS Awareness. ISO ondersteunt en bewaakt de kwaliteit van de aanpak van de BISO's.

2.3. Werkwijze

Dit hoofdstuk beschrijft een aantal attitudes en ideeën die ik heb gehanteerd bij het uitvoeren van de afstudeeropdracht. Deze werkwijze heeft als instrument gediend om de afstudeeropdracht te realiseren.

✓ **Doelgericht**
Een manier van handelen die altijd het doel ingedachte houdt en niet afdwaalt van de doelstelling tijdens het voorbereiden en uitvoeren van de stappen die leiden tot de desbetreffende doelstelling.

✓ **Klantgericht**
Stel de klant centraal en stel het belang van de klant voorop. Luister goed en speel in op de eisen en wensen van de klant. Houd wel de balans goed in de gaten van de verschillende eisen en wensen.

✓ **Oplossingsgericht**
Altijd op zoek naar mogelijke oplossingen voor een probleem of vraag. Zonder oorzaken en/of problemen uitgebreid te analyseren zijn oplossingen mogelijk waar de klant tevreden mee kan zijn.

✓ **Bruikbaarheid**
Streven is om producten op te leveren die inzetbaar zijn door de opdrachtgever. Kwalitatieve producten waar de opdrachtgever echt wat mee kan.

✓ **Maatwerk**
Bij het ontwerpen van een oplossing dient deze altijd zo optimaal mogelijk afgestemd te zijn op het te bereiken doel.

✓ **KISS (Keep it Short and Simple)**
KISS is een Engels acroniem, al is de precieze betekenis niet altijd onomstreden. Drie bekende versies zijn Keep It Simple, Stupid, Keep It Short and Simple en Keep it Simple & Straightforward mijn persoonlijke definitie is de tweede van deze drie.

2.4. Aanpak

Om het project in goede banen te leiden, heb ik het project aangepakt volgens de NIST Special Publication 800-50 *"Building an Information Technology Security Awareness and Training Program"*.

1. Components: Awareness, Training, Education
2. Designing an Awareness and Training Program
3. Developing Awareness and Training Material
4. Implementing the Awareness and Training Program

Deze fases worden op de volgende pagina verder toegelicht; er wordt ook beschreven hoe ze toegepast zijn in mijn situatie.

De eerste fase heb ik geïnterpreteerd als het bepalen van een mate van leren die toegepast zal worden bij het opstellen van de strategie. Volgens de publicatie is leren een continuüm; dat begint bij bewustzijn, ontwikkelt naar training en verder evolueert naar educatie. Op basis van het continuüm ga ik het niveau van leren bepalen voor de nieuwe strategie.

De tweede fase heb ik geïnterpreteerd als het ontwikkelen van de nieuwe strategie, die weer uit zes stappen bestaat. Deze zes stappen heb ik bestudeerd en een vertaling gemaakt die meer van toepassing was op de situatie. Zo zijn de volgende stappen ontstaan:

1. Structureren van de organisatie
   Dit gaat om de organisatie die ervoor gaat zorgen dat de strategie wordt geïmplementeerd en uitgewerkt in de business lines.
2. Requirements-analyse
   In de publicatie wordt deze stap Needs Assessment genoemd, waaronder ik versta het evalueren van de oude aanpak en het inventariseren van de eisen en wensen van de stakeholders voor de nieuwe strategie. Binnen ABN AMRO wordt de term requirements-analyse hiervoor gehanteerd.
3. Requirements vertalen naar input
   Deze stap miste ik in de publicatie, namelijk de brug van requirements naar strategie. Daarom heb ik in de fase deze stap opgenomen, waarin de requirements vertaald worden naar input voor de strategie op basis van onderzoeken die zijn gedaan.
4. Nieuwe strategie ontwikkelen
   In deze stap heb ik de drie laatste stappen samengevoegd omdat ze mijns inziens gepaard gaan. Hierin is dus de strategie ontwikkeld op basis van de input en de tijdslijnen en is de inhoud van de hulpmiddelen bepaald.
5. Uitwerken van de Process Outline
   Nog een extra stap die is toegevoegd omdat het standaard is in de organisatie. Voor elk nieuw proces wordt een Process Outline opgesteld op basis van een template.

De derde fase heb ik geïnterpreteerd als het (laten) ontwikkelen van hulpmiddelen. Hierin zijn twee stappen opgenomen, namelijk het selecteren van Awareness Topics en het kiezen van bronnen voor hulpmiddelen.

1. IS Awareness thema’s
   Samen met mijn collega’s heb ik thema’s vergaard die als speerpunt in een campagne kunnen worden gebruikt en de basis kunnen vormen voor het (laten) ontwikkelen van hulpmiddelen. De lijst met thema’s heb ik vervolgens gehouden tegen de beschikbare thema’s om uit te zoeken of er hulpmiddelen voor specifieke thema’s ontwikkeld moesten worden.
2. IS Awareness hulpmiddelen
   Op basis van een onderzoek naar de verschillende leveranciers van IS Awareness hulpmiddelen, heb ik hulpmiddelen ontwikkeld of geadviseerd om te laten ontwikkelen. Het onderzoek heb ik gestart toen uit de evaluatie bleek dat er behoefte was naar nieuwe hulpmiddelen. Ik heb het iteratief uitgevoerd met de ontwikkeling van de nieuwe strategie, omdat ik dan het onderzoek kon aansturen op basis van de nieuwe ontwikkelingen uit de strategie.

De vierde fase heb ik geïnterpreteerd als het uitvoeren van de campagnes. Dit viel buiten de scope van mijn opdracht zoals op voorhand afgesproken is met de opdrachtgever en bedrijfsmentor.

3. Oriëntatie

Voor het oriënteren in de opdracht en de omgeving heb ik extra tijd genomen voor de inwerking, omdat ik bij mijn oriënterende stage heb gemerkt hoeveel tijd dat kan kosten. Om mezelf te oriënteren heb ik een vooronderzoek gedaan, waarin ik documentatie die binnen de organisatie beschikbaar was en externe literatuur over het onderwerp heb geraadpleegd. In deze paar weken heb ik ook de eerste fase van de aanpak uitgevoerd en het Project Initiation Document opgesteld.

3.1. Project Initiation Document

Zoals ik gewend ben voor de projecten van de opleiding, heb ik voor mijn afstudeeropdracht ook een Project Initiation Document (PID) opgesteld. Het afstudeerplan heeft onder andere als input gediend voor het PID, doordat het afstudeerplan uitgebreid beschreven was. Dit zorgde ervoor dat het opstellen van het PID weinig tijd in beslag nam.

Nadat het PID was opgesteld, heb ik het ter goedkeuring opgeleverd bij mijn bedrijfsmentor. Hij heeft het op enkele opmerkingen na goedgekeurd. Het PID is toegevoegd als Bijlage 2: Project Initiation Document.

3.2. Vooronderzoek

Ik ben de afstudeeropdracht gestart met de beperkte kennis en ervaringen over Information Security Awareness die ik binnen mijn opleiding heb opgedaan. Dit vooronderzoek is uitgevoerd om mezelf een expert te maken op het gebied Information Security Awareness.

Daarvoor heb ik eerst literatuuronderzoek uitgevoerd waarin is gezocht naar interessante documenten uit best practices en standaarden met betrekking tot het onderwerp van de opdracht. Ook heb ik aan mijn collega's gevraagd of zij op de hoogte zijn van soortgelijke publicaties of boeken. Mijn collega's gaven aan dat er niet veel zijn en dat zij door middel van gesprekken met experts op het gebied up-to-date blijven met de verschillende ontwikkelingen. Uit het literatuuronderzoek is gebleken dat er over awareness en bewustzijn wel veel literatuur is, maar weinig specifiek over informatiebeveiliging.

In de onderstaande tabel is een overzicht weergegeven van de veelgebruikte zoektermen, de zoekmachines (internet) en bronnen die gehanteerd zijn tijdens het onderzoek.

Zoekwoorden	• Information Security Awareness • Bewustzijn • Awareness • Informatiebeveiliging • Strategie • Awareness Strategie • Social Engineering • Security Awareness financiële sector
Zoekmachines/zoekplaatsen	• Google • Bing • HBO-kennisbank.nl
Bronnen	• Bibliotheek De Haagse Hogeschool

Tabel 1: Zoekwoorden vooronderzoek

De zoektermen zijn tevens gecombineerd om zoveel mogelijk zoekresultaten te realiseren.

Het vooronderzoek heeft niet veel materiaal opgeleverd, maar wel twee interessante stukken die ik goed heb bestudeerd. Namelijk het evaluatierapport van de voorgaande strategie en de NIST SP 800-50 *"Building an Information Technology Security Awareness and Training Program"*.

Het evaluatierapport heb ik goed bestudeerd om snel in te lezen over de voorgaande strategie. Hierdoor kon ik begrijpen hoe deze in elkaar zat en wat de voor- en nadelen ervan waren. Dit heb ik dan als input gebruikt voor de nieuwe strategie.
Verder heeft dit mij ook inzicht gegeven in wat de definitie is voor de organisatie van een strategie. Wat mij opviel is dat de strategie een document is, waarin is opgenomen hoe binnen de bank omgegaan wordt met Information Security Awareness. Daarbij is de aanpak uitgewerkt in stappen en aandachtgebieden.

De NIST SP 800-50 *"Building an Information Technology Security Awareness and Training Program"* is een speciaal gepubliceerde richtlijn over informatiebeveiliging dat is ontwikkeld door het National Institute of Standards and Technology (NIST). NIST is verantwoordelijk voor het ontwikkelen van standaarden en richtlijnen voor het zorgdragen van een adequate informatiebeveiliging voor organisaties.

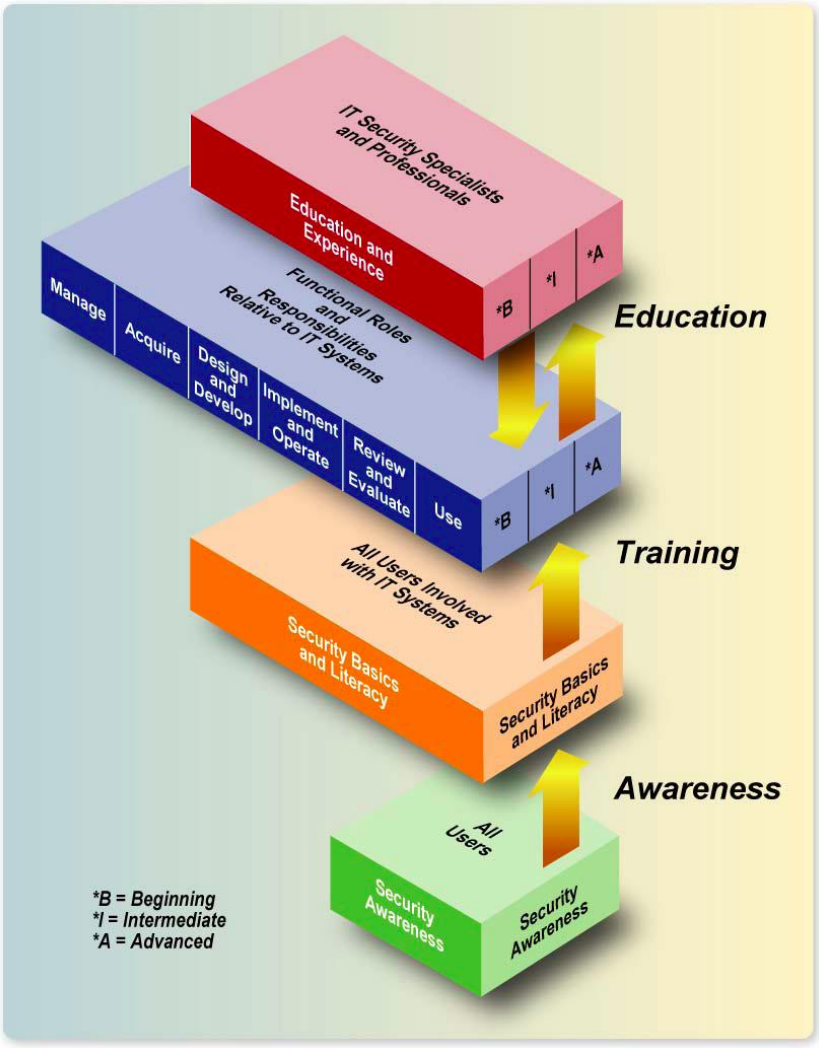
Deze richtlijn biedt ondersteuning in het ontwikkelen van een effectief informatiebeveiligingsprogramma. Deze ondersteuning samen met de betrouwbaarheid van publicaties van het NIST heeft er toe geleid dat ik dit document heb toegepast voor het ontwikkelen van de nieuwe strategie. Daarnaast herkende de bedrijfsmentor ook de werkwijze van de bank in deze richtlijn.

3.3. Scope van de strategie

De eerste stap van de aanpak is beschreven als het bepalen van de mate van leren dat wordt toegepast in de strategie. Het opstellen van kaders voor de nieuwe strategie, oftewel de scope bepalen. In de richtlijn is deze beperkt tot de mate van leren, maar ik heb van het moment gebruik gemaakt om ook twee andere kaders in de vorm van het uitbreiden van de strategie naar risk-brede aanpak en de doelgerichtheid.

Continuüm van leren

Zoals in de onderstaande figuur is weergegeven kan leren zich ontwikkelen naar verschillende niveaus.



Figuur 3: The IT Security Learning Continuum

Het niveau dat toegepast wordt in de strategie hangt af van de doelgroep die wordt gedefinieerd. In dit geval zijn dat de medewerkers die omgaan met informatie en de informatiesystemen van de organisatie. Echter wordt er wel een onderscheid gemaakt in de functies die direct of indirect betrokken zijn met information security. Deze worden buiten beschouwing gelaten omdat zij de benodigde training al via hun functie krijgen.

Op basis hiervan is ervoor gekozen om de eerste twee niveaus toe te passen in de strategie, namelijk:

- Security Awareness
- Security Basics and Literacy (verder Security Learning genoemd)

Daarvoor heb ik de volgende aanbeveling gedaan:
Uit de vergelijking is geconcludeerd dat IS Awareness en IS Learning dicht bij elkaar liggen en daardoor elkaar aanvullen en versterken. Medewerkers overhalen het juiste gedrag te vertonen gebeurt door middel van de juiste houding en voldoende kennis op gebied van informatiebeveiliging. Door een goede combinatie in te zetten van Awareness en Learning kan zowel de houding als de kennis van de medewerkers verhoogd worden, waardoor ook het gedrag wordt verbeterd.

Strategie uitbreiden naar risk-brede aanpak
Bij de evaluatie van de voorgaande strategie werd er commentaar ontvangen op de samenwerking tussen de verschillende Risk-partijen (met name Compliance, Business Continuity Management, Security & Intelligence Management, Operational Risk Management etc.). In deze overweging heb ik gekeken naar de voordelen en nadelen van een gecombineerde aanpak.

Daarvoor heb ik de volgende aanbeveling gedaan:
Een gecombineerde aanpak van Security / Risk Awareness heeft als voordeel dat het een eenduidig geïntegreerde aanpak betreft. Een aanpak waardoor de kennis, houding en gedrag van de medewerkers wordt verhoogd inzake informatiebeveiliging, maar ook fysieke beveiliging, BCM, Compliance en andere operationele risico's.

Een voorwaarde daarbij is wel dat de andere Risk-partijen bereidheid moeten tonen in het samenwerken aan een geïntegreerde aanpak. Indien er geen support is voor een samenwerking dat is het raadzaam om de nieuwe strategie te richten op de Information Security-aanpak. Tevens kan de strategie wel zo ingericht worden dat het uitbreidbaar is naar een Security / Risk-aanpak.

Doelgroepgerichte aanpak
Er was ook commentaar ontvangen waarin werd aangeduid dat de voorgaande aanpak onvoldoende doelgroepgericht was, waardoor het niet aansloot op de verschillende doelgroepen die er aanwezig zijn binnen de organisatie.

Daarvoor heb ik de volgende aanbeveling gedaan:
Het onderscheiden van specifieke doelgroepen kan de effectiviteit van een IS Awareness aanpak verhogen. Om deze doelgroepgerichte aanpak op een goede wijze in te voeren moet wel aan bepaalde voorwaarden worden voldaan:

- Duidelijke definitie van doelgroepen
- Duidelijk aangeven van de aanpak per doelgroep inclusief de voor de doelgroep relevante producten en diensten

4. IS Awareness & Learning Strategie

Het hoofddoel van mijn afstudeeropdracht was het ontwerpen van een nieuwe IS Awareness & Learning strategie voor de opdrachtgever. Een strategie die in de hele organisatie ingezet kan worden om de awareness te verhogen omtrent informatiebeveiliging. Deze strategie moet voldoen aan de eisen en wensen van de verschillende stakeholders, waaronder de toezichthoudende instanties, het management en de business. Hoe ik te werk ben gegaan met het ontwerpen van de nieuwe IS Awareness & Learning strategie en deze te laten voldoen aan de eisen en wensen van de stakeholders, wordt in dit hoofdstuk behandeld.

In dit hoofdstuk wordt dus behandeld hoe de organisatie is opgezet voor het uitvoeren van de awareness strategie. Vervolgd door het opstellen van de Requirements van de verschillende stakeholders en hoe deze dan is vertaald naar de nieuwe strategie.

4.1. Structuur

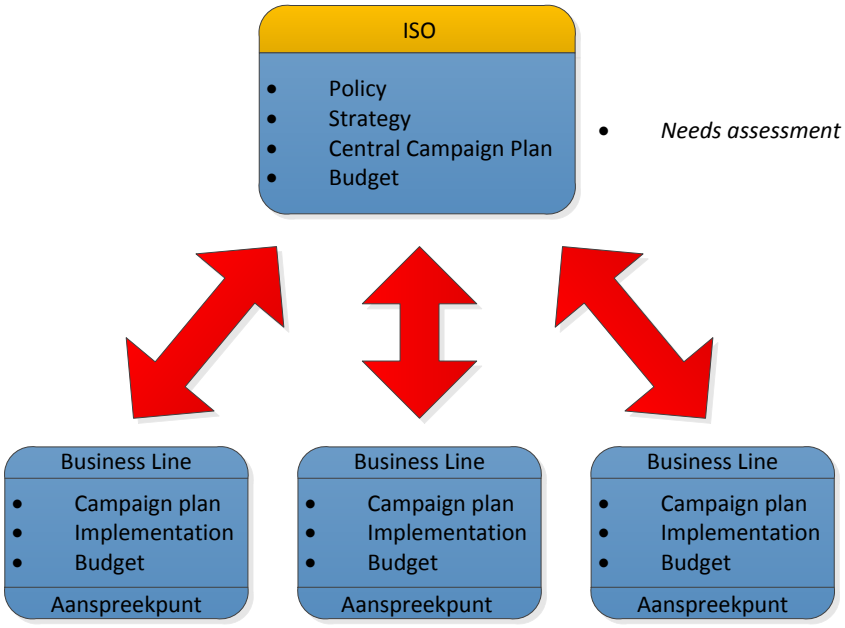
Volgens de NIST SP 800-50 kan de strategie op verschillende manieren ontworpen, ontwikkeld en geïmplementeerd worden. Drie vaak toegepaste modellen worden als volgt beschreven:

- Model 1: Centrale policy, strategie en implementatie
- Model 2: Centrale policy en strategie en decentrale implementatie
- Model 3: Centrale policy en decentrale strategie en implementatie

Naar aanleiding van wat ik heb begrepen van de voorgaande strategie en uit gesprekken met mijn bedrijfsmentor was het duidelijk dat binnen de bank het tweede model wordt toegepast. Waarbij vertegenwoordigers van de business lines wel bij het uitwerken van de policy en strategie betrokken zijn.

Figuur 4: Model 2 – Gedeeltelijk decentrale programma management

Dat houdt in dat centraal door de afdeling Information Security Office in samenwerking met vertegenwoordigers van de business lines de policy en strategie is bepaald voor IS awareness. De implementatie van de policy en strategie voor IS awareness wordt dan gedelegeerd naar aangestelde aanspreekpunten (voornamelijk Business Information Security Officers) in de verschillende business lines. In de onderstaande figuur is dat visueel weergegeven.



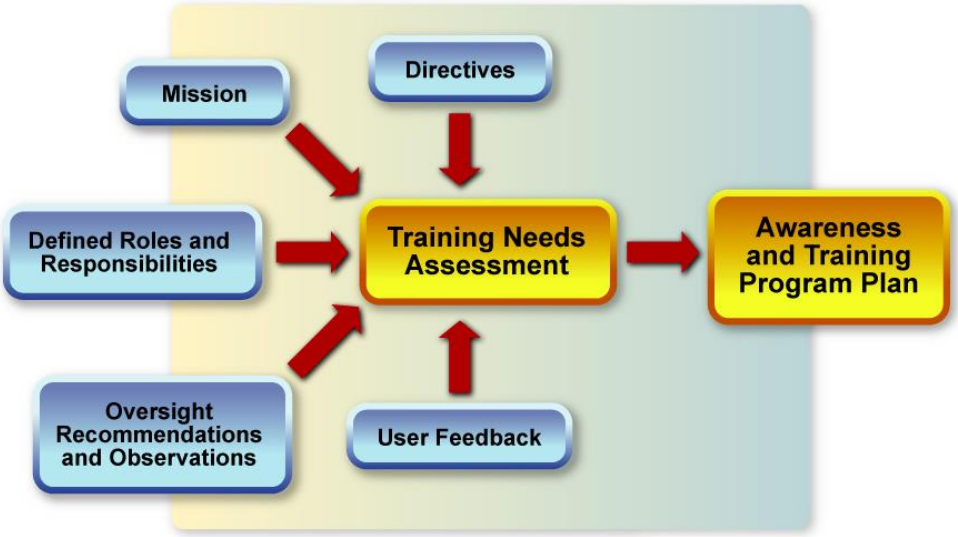
Figuur 5: Model 2 – Toegepast binnen de bank

De aanspreekpunten maken dus gebaseerd op de strategie een plan van hoe zij IS awareness willen aanpakken in hun business lines. Vervolgens voeren zij dit uit na afstemming met ISO en goedkeuring door het management team van de betreffende business line.

Ik vond deze aanpak wel logisch, omdat de ABN AMRO een grote organisatie is met verschillende business lines, waardoor het moeilijk is om centraal de specifieke risico's en behoeftes van iedere business line te kennen. De aanspreekpunten zitten dichterbij de business line, hierdoor zijn zij beter in staat om een aanpak te bepalen.

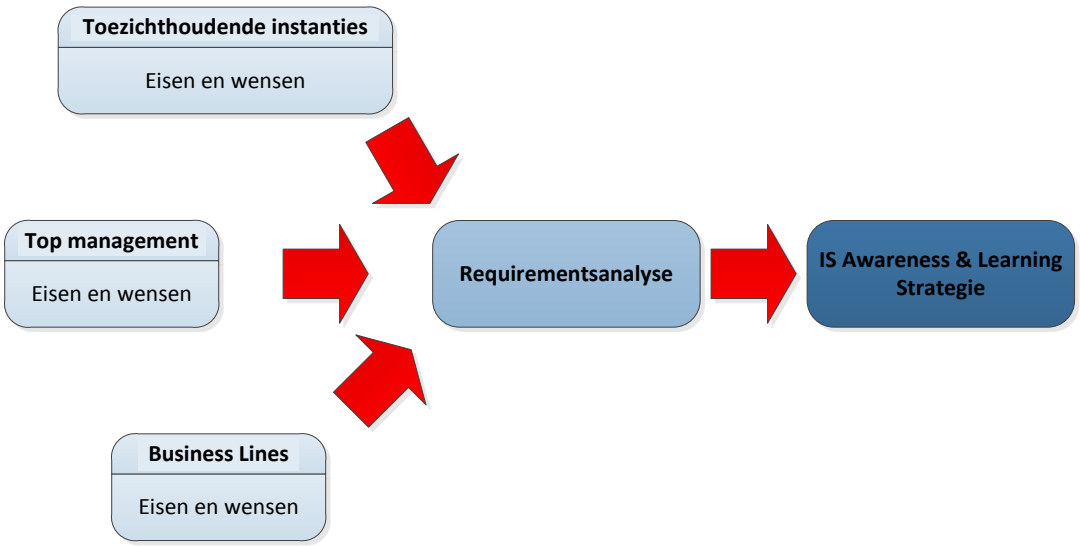
4.2. Requirements-analyse

De requirementsanalyse is uitgevoerd om de eisen en wensen van de stakeholders van de nieuwe strategie in kaart te brengen. Om deze analyse te doen is het dus van belang dat de stakeholders voor de nieuwe strategie ook in kaart worden gebracht. In figuur 6 is weergegeven hoe de Needs Assessment volgens de NIST gedaan wordt en in figuur 7 is weergegeven hoe ik dat heb toegepast.



Figuur 6: Needs Assessment volgens NIST

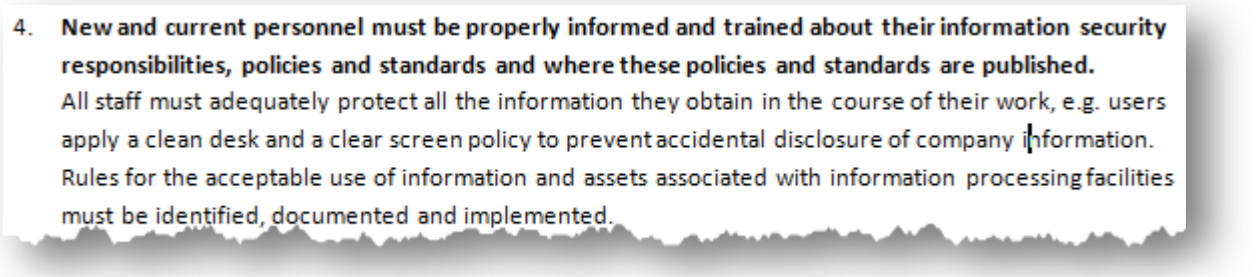
Als stakeholders heb ik de onderstaande partijen herkend na een gesprek met de bedrijfsmentor. De toezichthoudende instanties (zoals de DNB) en het centrale beleid omdat zij via wetten en regels eisen hebben opgelegd over IS awareness. Daarnaast heeft het top management ook eisen en wensen die in de strategie opgenomen moeten worden. Verder heb ik de business lines als stakeholder herkent omdat zij als gebruikers gezien kunnen worden van de strategie die het verder implementeren.



Figuur 7: Requirementsanalyse

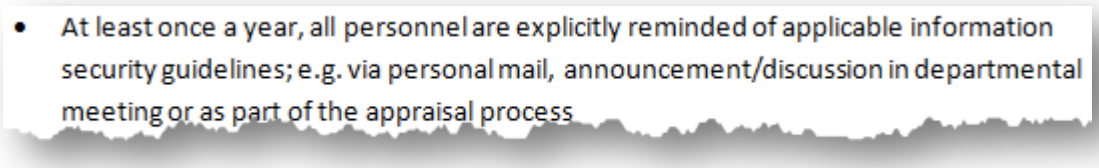
4.2.1. Requirements van de toezichthoudende instanties

Om de voor IS awareness relevante policies te kunnen vinden heb ik de bedrijfsmentor om advies gevraagd. Hij heeft mij dan gewezen op de AIM-pagina (ABN AMRO Instruction Manual) waar diverse policies staan die zijn opgesteld voor de organisatie. Daarop vond ik de GISP (Group Information Security Policy) dat een bundeling is van policies voor de verschillende aspecten van informatiebeveiliging. In de GISP heb ik in het hoofdstuk Human Resources Security de volgende policy rule gevonden:


4. **New and current personnel must be properly informed and trained about their information security responsibilities, policies and standards and where these policies and standards are published.**
All staff must adequately protect all the information they obtain in the course of their work, e.g. users apply a clean desk and a clear screen policy to prevent accidental disclosure of company information.
Rules for the acceptable use of information and assets associated with information processing facilities must be identified, documented and implemented.

Figuur 8: Policy rule 5.4.4 uit de GISP

Dit artikel vond ik relevant voor de nieuwe strategie omdat het aangeeft dat alle medewerkers, zowel nieuwe als bestaande, adequaat geïnformeerd moeten worden over hun verantwoordelijkheid omtrent informatiebeveiliging. Wat mij wel opviel is dat de policy heel globaal opgesteld is en dat je dan vrij bent in de invulling ervan. Dus je zou met een minimale invulling al kunnen voldoen aan deze policy. Daarom is deze policy rule in de Personnel Security Policy verder uitgewerkt in de volgende standaard:


- At least once a year, all personnel are explicitly reminded of applicable information security guidelines; e.g. via personal mail, announcement/discussion in departmental meeting or as part of the appraisal process

Figuur 9: Policy 2.2

Dit vond ik relevant omdat het aangeeft dat alle medewerkers jaarlijks herinnerd moeten worden aan de richtlijnen omtrent informatiebeveiliging. Dit artikel geeft wel meer invulling aan wat er wordt verwacht. Hieruit heb ik dan ook herleid waarom de voorgaande strategie gebaseerd was op een jaarlijkse aanpak.

Nadat de requirements van de toezichthoudende instanties in kaart waren gebracht, heb ik daarna dat van de business lines (gebruikers) in kaart gebracht en heeft mijn bedrijfsmentor van het management team gedaan.

4.2.2. Requirements van de gebruikers

Verder heb ik de requirements van de gebruikers in kaart gebracht. Dit heb ik gedaan door de ontvangen commentaar op de voorgaande strategie te vertalen naar requirements en deze vervolgens af te stemmen met de klankbordgroep via een meeting. De klankbordgroep is samengesteld uit BISO's van verschillende business lines. Zij hebben als luisterend oor gefungeerd en input geleverd op basis van wat er in de business leeft en de eisen en wensen die zij als gebruikers hadden. Hiervoor heb ik maandelijks een meeting ingepland. Door deze klankbordgroep heb ik draagvlak gecreëerd voor de verschillende ideeën die ik wilde invoeren.

In het evaluatierapport heb ik het volgende commentaar herkend als commentaar op de beschikbare middelen, zoals de jaarlijkse survey en de e-learnings. Uit dit commentaar begreep ik dat de gebruikers ontevreden waren over de huidige hulpmiddelen die ingezet worden.

- te veel rule-based: meer dilemma's;
- alweer…;ieder jaar dezelfde vragen en dezelfde medewerkers (m.n. bij kleine afdelingen)
- rapportage laat te lang op zich wachten
- antwoorden op open vragen gebeurt niets mee
- tooling soms verouderd (niet geheel in lijn met nieuwe ontwikkelingen en (vernieuwde) policies
- tooling onvoldoende ingezet (met name set 2 QLP's & NF's worden nog maar weinig gevolgd, dit geldt vooral voor de Engelse modules)
- er wordt vaak verteld wat niet mag maar er wordt onvoldoende verteld wat er dan wel mag en hoe men dan veilig kan handelen.

Figuur 10: Ontvangen commentaar op de hulpmiddelen

Op basis van het commentaar concludeerde ik dat zij ontevreden waren over de inhoud omdat het niet aansloot op hun eisen en wensen, maar ook niet op de nieuwe ontwikkelingen. Daarnaast kan ook geconcludeerd worden dat ze ontevreden waren rondom het proces van de survey en de tooling. Daarvoor had ik dan twee requirements bedacht: een "vitrine" opstellen met de huidige hulpmiddelen aangevuld door diverse actuele hulpmiddelen en dat ze betrokken worden bij de selectie en invulling van de hulpmiddelen.

Het onderstaande commentaar heb ik gegroepeerd als commentaar op de doelgroep gerichtheid van de voorgaande strategie. Hieruit begreep ik dat de voorgaande strategie onvoldoende gericht was op de verschillende doelgroepen die zich bevinden binnen de organisatie.

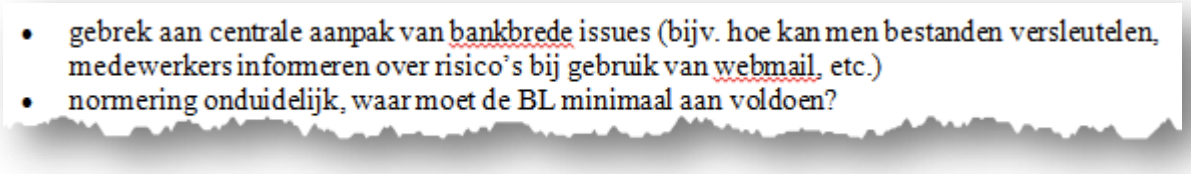
- resultaten zijn vaak te globaal waardoor betreffende BL onvoldoende gerichte acties kan uitvoeren.
- verschil in belangrijkheid van IS issues. Bij de ene afdeling is het afsluiten van kasten minder urgent dan bij de ander.
- weinig significante vooruitgang op specifieke onderwerpen (bijv. Kasten afsluiten blijft een slecht scorend onderdeel)

Figuur 11: Ontvangen commentaar op doelgroepgerichtheid

Hiervoor heb ik twee requirements opgenomen, één daarvan is afkomstig uit de voorgaande strategie. Daarin was één van de activiteiten dat elke gebruiker voor zijn/haar business line een plan moest maken waarin beschreven staat hoe IS awareness aangepakt zal worden. Ik heb besloten deze aan te houden omdat de gebruikers uit de verschillende business lines het beste weten wat er in hun business line speelt. Hierdoor zijn zij beter in staat te bepalen wat er relevant of interessant is voor die specifieke business line.

Daarnaast heb ik ook opgenomen in de requirements dat de plannen die opgesteld worden, stuurbaar moeten zijn op doelgroepen die zij herkennen. Hiermee wilde ik bereiken dat de gebruikers nog specifieker invulling kunnen geven aan de campagnes.

Verder heb ik uit het onderstaande commentaar begrepen dat gebruikers vonden dat ze eerder onvoldoende centrale ondersteuning kregen. Dit vond ik echter verwarrend, omdat uit het vorige commentaar bleek dat gebruikers vonden dat er centraal te veel bepaald werd. Het was dus onduidelijk in welke mate en op welke wijze zij centrale ondersteuning wensten.


- gebrek aan centrale aanpak van bankbrede issues (bijv. hoe kan men bestanden versleutelen, medewerkers informeren over risico's bij gebruik van webmail, etc.)
- normering onduidelijk, waar moet de BL minimaal aan voldoen?

Figuur 12: Ontvangen commentaar op centrale ondersteuning

Ik heb toen wel als requirement opgenomen dat er meer centrale ondersteuning vanuit ISO gegeven moest worden. Maar dit was zeker een punt waarvoor ik meer opheldering nodig had om er een concrete requirement van te maken.

Nadat ik het ontvangen commentaar van de gebruikers had vertaald naar requirements, heb ik deze behandeld in een klankbordgroep-meeting. In deze meeting wilde ik de requirements afstemmen met de gebruikers, om ervoor te zorgen dat ik het goed heb vertaald en of er nog opmerkingen waren of aanvullende eisen en wensen.

In de klankbordgroep meeting stond dus de requirements van de gebruikers centraal. Hieronder staan deze nogmaals op een rij:

1. De huidige IS awareness hulpmiddelen aangevuld met actuele hulpmiddelen in een "vitrine"
2. De medewerkers worden meer betrokken bij de selectie en invulling van de hulpmiddelen
3. Er wordt een plan opgesteld per business line
4. De plannen moeten stuurbaar zijn op doelgroepen
5. Meer centrale ondersteuning vanuit ISO

De klankbordgroep stemde in met de meeste van deze requirements, maar hadden op sommige wel enkele opmerkingen. Bij de tweede requirement hebben zij aangegeven niet zo zeer betrokken willen worden bij de selectie van de hulpmiddelen. Ze zouden wel invloed willen hebben op de invulling van de

hulpmiddelen voordat het ingezet wordt voor hun specifieke business line. Zo willen zij bijvoorbeeld de hulpmiddelen meer inrichten voor specifieke doelgroepen. Samen met de klankbordgroep-leden ben ik dan tot het besluit gekomen om de tweede requirement aan te passen.

In de meeting met de klankbordgroep heb ik opheldering gevraagd over wat er bedoeld was met de centrale ondersteuning van ISO die zij wensten. Hierin werd dan duidelijk dat zij voornamelijk ondersteuning wensen bij het implementeren van de nieuwe strategie. Bijvoorbeeld dat als er in de strategie wordt opgenomen dat wij van hen een IS awareness plan verwachten, dat wij dan ook een template leveren met de minimale vereisten van een dergelijke plan. Tevens hebben zij ook aangegeven ondersteuning nodig te hebben bij het implementeren van nieuwe hulpmiddelen, bijvoorbeeld als "mystery guest"-aanpak wordt opgenomen als hulpmiddel dat er toegelicht wordt hoe zij het middel effectief in kunnen zetten. Op basis van deze gegevens heb ik de requirement aangevuld met extra gegevens.

Verder hadden zij nog een aanvullende wens dat zij aan het begin van het jaar duidelijkheid wilden hebben over eventuele (nieuwe) verplichte trainingen zowel op het gebied van informatiebeveiliging als andere risicogebieden. Dit kwam blijkbaar omdat zij hierover eerder onvoldoende werden geïnformeerd waardoor de uitvoering van andere awareness activiteiten werd verstoord. Zij gaven aan het belangrijk te vinden omdat de campagnes ook gericht kunnen worden op deze verplichte trainingen.

4.2.3. Requirements van het management team

Om de requirements van het management team in kaart te brengen heeft mijn bedrijfsmentor het op de agenda van het management team-meeting gekregen. Hij heeft in die meeting de evaluatie van de voorgaande strategie behandeld met name de ontvangen commentaar en de requirements van de klankbordgroep. Daarmee wilde hij achterhalen welke eisen het management team had voor de nieuwe strategie.

Ik heb mijn bedrijfsmentor geholpen voorbereiden op deze meeting door samen de requirements van de klankbordgroep door te nemen. Waar de requirements voor grote verandering zorgde is er extra aandacht besteed in de meeting. Bijvoorbeeld over de jaarlijkse survey waar de klankbordgroep niet meer positief over waren.

Het management team had daarvoor één eis en dat was namelijk dat er wel input moet zijn om accenten te kunnen leggen aan de campagnes. Maar zij vonden het niet noodzakelijk dat deze input alleen uit de huidige survey wordt gehaald. Dit vond ik een goede invulling aan de requirement omdat er dan meer vrijheid ontstaat voor het bepalen hoe input wordt geleverd voor de campagnes. Zo kon de jaarlijkse survey, die de kracht verloor bij de gebruikers, vervangen worden door andere meetmogelijkheden.

Nadat de requirements verzameld waren van de verschillende stakeholders, heb ik ze samengevoegd in het opgestelde requirements document.

4.2.4. Requirements document

Aangezien er niet heel veel requirements waren opgesteld voor de nieuwe strategie heb ik ervoor gekozen om deze te verwerken in een Word-document. Die heb ik kort en simpel gehouden om een snelle overzicht te kunnen bieden in de requirements die cruciaal zijn voor de nieuwe strategie. De requirements zijn opgenomen als bijlage van het product IS Awareness & Learning Strategie.

De requirements zijn daarna geprioriteerd volgens de **M**o**SC**o**W**-methode, waarvan de letters staan voor:

- **M - must haves**: deze eisen (*requirements*) *moeten* in het eindresultaat terugkomen, zonder deze eis is het product niet bruikbaar;
- **S - should haves**: deze eisen zijn zeer gewenst, maar zonder is het product wel bruikbaar;
- **C - could haves**: deze eisen zullen alleen aan bod komen als er tijd genoeg is;
- **W - won't haves**: deze eisen zullen in dit project niet aan bod komen maar kan in de toekomst, bij een vervolgproject, interessant zijn.

1.	• GISP 5.4.4. : new and current personnel must be properly informed and trained about their information security responsibilities, policies and standards and where these policies and standards are published. • Personnel Security Policy: Responsible line management, if necessary supported by Human Resources personnel, must ensure the following: ○ At least once a year, all personnel are explicitly reminded of the applicable information security guidelines	AIM policy	**M**
2.	Jaarlijkse IS awareness cyclus	AIM policy, DNB	**M**
3.	Een vorm van awareness-meting is noodzakelijk om accenten te kunnen leggen in de jaarlijkse awareness plannen	M. Dekker	**M**
4.	IS Awareness plan per Business Line	Proj. meeting	**S**
5	Stuurbaar per onderscheiden doelgroep	Proj. meeting	**C**
6.	Overzichtelijke “vitrine” van beschikbaar IS awareness hulpmiddelen; actueel, state of the art	Proj. meeting	**S**
7.	De BL-aanspreekpunten hebben invloed op de invulling van de hulpmiddelen bij het inzetten in de business lines	Proj. meeting	**C**
8.	Vooraf duidelijkheid over (nieuwe) verplichte trainingen	Proj. meeting	**C**
9.	Goede centrale ondersteuning (b.v. standaard template voor IS Awareness plan, ondersteuning bij uitvoering e.d.)	Proj. meeting	**C**

Tabel 2: Overzicht requirements

4.3. Requirements vertalen

Op basis van de opgestelde requirements zijn er wijzingen aangebracht in de voorgaande strategie. Deze wijzigingen hebben tevens als input gediend voor de nieuwe strategie. De belangrijkste wijzigingen zijn hieronder opgesomd met een toelichting van hoe deze wijziging tot stand zijn gekomen.

- De jaarlijkse IS Awareness Survey vervalt

Deze beslissing heb ik samen met mijn bedrijfsmentor gemaakt op basis van het ontvangen commentaar en de zesde requirement in tabel 2. De derde requirement geeft echter aan dat er wel een vorm van awareness meting noodzakelijk is om accenten te kunnen leggen aan de campagnes.

Mijn invulling aan deze requirements was om de jaarlijkse survey te laten vervangen door meerdere (andere) meetmiddelen. Bijvoorbeeld door een “mystery guest” aanpak waarmee het feitelijke gedrag gemeten kan worden of een awareness game die een survey inzet op een spelenderwijs waardoor er een meer uitdagende factor in zit.

Het idee achter deze invulling was om de requirements van de klankbordgroep over beschikbare hulpmiddelen te dekken. De aanspreekpunten zouden dan meer keuzes hebben en vrijheid om te bepalen hoe er binnen de business line wordt gemeten.

De bedrijfsmentor gaf dan aan mijn insteek te steunen, maar had er zelf ook één. Zijn idee was om de speerpunten (accenten) te bepalen op basis van inzicht in gedrag en nieuwe ontwikkelingen. Inzicht in gedrag kon bijvoorbeeld verkregen worden op basis van security incidentenrapportages, signalen vanuit security monitoring (b.v. ten aanzien van data leakage) en waarnemingen ten aanzien van clean desk, gebruik social media e.d.

Dit vond ik zelf ook een goede insteek omdat deze metingen continu worden gedaan en er daardoor snel input gehaald kan worden voor de campagnes. Dit snellere voortraject zorgt dan voor meer ruimte voor de campagnes zelf.

Samen met de bedrijfsmentor ben ik dan tot de beslissing gekomen om beide insteken toe te passen. Dit is gedaan door zijn insteek te gebruiken aan het begin om de speerpunten te bepalen. Mijn insteek is gebruikt om de “vitrine” aan te vullen met andere meetmiddelen die ingezet kunnen worden om te informeren en/of te prikkelen.

- Meer ruimte voor een doelgroepgerichte en Business Line specifieke aanpak

Deze wijziging is aangebracht omdat het bleek uit het ontvangen commentaar en de requirement vier en vijf in tabel 2 dat de voorgaande strategie niet doelgroepgericht was en daardoor soms niet relevant was voor bepaalde afdelingen.

Er is meer ruimte gemaakt door de huidige hulpmiddelen aan te vullen met andere hulpmiddelen en zo een uitgebreidere “vitrine” van hulpmiddelen te bieden. De aanspreekpunten kunnen dan zelf bepalen voor de betreffende business line welke hulpmiddelen zij inzetten en aan welke speerpunten zij aandacht willen besteden.

Door dit mogelijk te maken denk ik dat de aanspreekpunten hun campagnes meer doelgroepgericht kunnen maken en op die manier ook meer relevant zullen zijn voor de doelgroep.

- Meer nadruk op verbetering van houding en gedrag dan op kennis

De insteek van de voorgaande strategie was om de campagnes te richten op zowel kennis, houding als gedrag. Maar na de ingezette middelen goed te bestuderen, viel het mij op dat hiermee echter de houding en kennis niet optimaal gemeten en/of gestimuleerd kon worden.

Zo werd de survey ingezet om kennis, houding en gedrag te meten. Het is echter bewezen dat een survey houding en gedrag niet optimaal kan meten. In de survey werd bijvoorbeeld dilemma’s gebruikt om het gedrag te meten. Maar het ingevulde antwoord kan verschillen van het feitelijke gedrag omdat er de intentie gemeten wordt. De intentie kan verschillen met het gedrag dat uiteindelijk wordt uitgevoerd wanneer men echt geconfronteerd wordt met de dilemma.

Omdat

- Beter gebruik van de beschikbare tooling (met name E-learnings, QLP’s en NF’s e.d.).

Naast het uitbreiden van de "vitrine" met aanvullende hulpmiddelen, wilde ik ook dat de huidig beschikbare hulpmiddelen meer gebruikt moest worden. Omdat het bleek uit het commentaar van de klankbordgroep dat de huidige middelen onvoldoende werden ingezet.

In een meeting met de klankbordgroep heb ik geprobeerd te achterhalen waarom zij denken dat de hulpmiddelen onvoldoende werden ingezet. Daar hadden zij verschillende ideeën over, zoals dat de hulpmiddelen moeilijk benaderbaar was door een registratiesysteem (My Learning & Development) waar alle digitale leermiddelen binnen de bank worden geplaatst.

Verder vonden zij dat de hulpmiddelen niet voldoende gestimuleerd worden om te volgen. Nieuw ontwikkelde middelen werden wel gecommuniceerd via een artikel op intranet en waren er ook regelmatig verwijzingen, maar dat bleek niet voldoende te zijn om gebruik te verhogen.

Sommige leden overwogen ook het verplichtstellen van de hulpmiddelen, maar zagen het niet als de beste oplossing voor dit probleem. Omdat de medewerkers dan geforceerd worden om deze middelen te volgen, waardoor het mogelijk is dat een verkeerde houding zou ontstaan betreffende informatiebeveiliging.

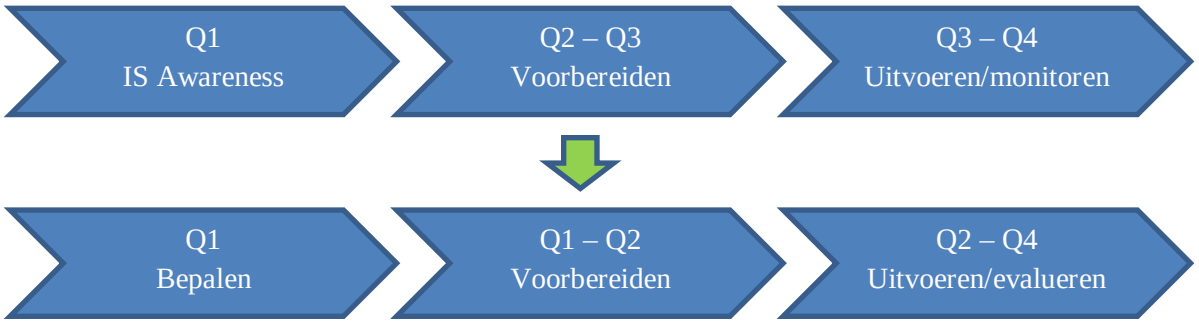
Uit een gesprek met Wilbert Pijnenburg van InfoSecure, een expert op het gebied van IS awareness, ben ik te weten gekomen over Blended Learning (verrijkt leren). Dat is een combinatie van e-learning en groepsbespreking. Dit vond ik interessant omdat we op deze manier het gebruik van de e-learnings kunnen stimuleren en kan het meer effectief zijn door de stof met elkaar te behandelen en elkaar daarna op gedrag aanspreken.

Nadat ik de requirements had vertaald naar input voor de strategie, ben ik aan de slag gegaan met het opstellen van de nieuwe strategie.

4.4. Nieuwe strategie ontwikkelen

De nieuwe strategie heb ik verwerkt in Powerpoint-sheets, omdat ik vind dat het een snel overzicht biedt van tekst. Dit maakt het makkelijker om de strategie als geheel te presenteren. Daarvoor heb ik eerst geïnventariseerd wat ik allemaal als input had. De IS Awareness & Learning strategie is als Externe Bijlage 1 toegevoegd.

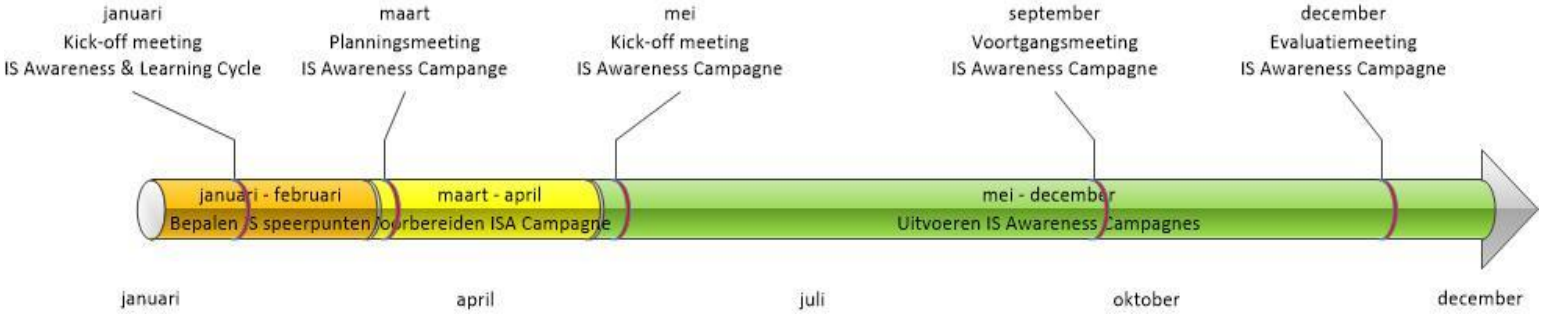
Uit het evaluatierapport heb ik kunnen afleiden dat de jaarcyclus het hoofdonderdeel was van de vorige strategie. De belangrijkste wijzigingen moesten dus verwerkt worden in een jaarcyclus. Daarvoor heb ik eerst de voorgaande jaarcyclus erbij gepakt met het idee daarin de wijziging op te nemen. En dat is als volgt gebeurt.



Figuur 13: Jaarcyclus

Omdat de IS Awareness Survey is komen te vervallen is deze fase vervangen door het bepalen van speerpunten op basis van metingen die continu lopen waaruit input sneller gehaald kan worden. Dit kort dan ook de tijd van de fase in, waardoor er eerder begonnen kan worden aan het voorbereiden van de campagnes. Het uitvoeren van de campagne begint daardoor ook eerder.

De wijzigingen hebben ook voor andere stappen gezorgd in de verschillende fases. Wat deze stappen inhouden is verwerkt in sheet 5 van Externe Bijlage 1 IS Awareness & Learning Strategie. Dit heb ik samen met de bedrijfsmentor ook in de volgende tijdslijn opgenomen.



Ik denk dat ik met deze twee PowerPoint-sheets het duidelijk is geworden hoe de IS Awareness Jaarcyclus eruit ziet, wat er gedaan moet worden, door wie en wanneer. Hiervoor heb ik gebruikt gemaakt van een voorbeeld van een Process Outline die binnen de bank wordt gehanteerd voor het uitwerken van processen. Deze heb ik gebruikt omdat ik dezelfde kenmerken herkende zoals ik dat ook in de theorie heb geleerd tijdens de opleiding.

Om de nieuwe strategie te verduidelijken heb ik ervoor gekozen om een inleiding toe te voegen. In de inleiding heb ik de aanleiding voor een nieuwe strategie en een leeswijzer verwerkt. Daarna heb ik op een sheet de scope behandeld van de strategie. Daarvoor heb ik de policy beschreven die relevant was voor IS Awareness. Met de policy en de maatregelen ervoor wilde ik de lezer van de strategie wijzen op de noodzaak van een IS Awareness strategie. Met deze twee sheets wil ik de lezer wijzen op de redenen voor een nieuwe strategie en waarom er überhaupt een strategie is opgesteld.

De volgende sheet gaat in op de uitgangspunten die geformuleerd zijn op basis van de vereisten vanuit de GISP, de evaluatie van de voorgaande aanpak en oriëntatie omtrent “best practice”. Daarna heb ik op een sheet de belangrijkste wijzigen van de nieuwe aanpak uitgelicht. Verder heb ik de documenten als bijlage toegevoegd die input hebben geleverd voor de nieuwe strategie, zoals het evaluatierapport en de requirements.

Daarnaast heb ik nog drie documenten als bijlage toegevoegd om de grootste wijzigingen toe te lichten, namelijk het bepalen van de speerpunten, het toepassen van Blended Learning en de IS A&L toolbox. De documenten geven inzicht in wat deze wijzigingen inhouden en hoe ze eruit zien. Daarmee wilde ik de wijzigingen duidelijker maken voor de lezer.

4.5. Process Outline

Om ervoor te zorgen dat de strategie gewaarborgd wordt in de komende jaren, is er een onderhoudsplan opgesteld. In het onderhoudsplan zijn aspecten opgenomen die noodzakelijk zijn om voor borging te zorgen. Aspecten zoals: process flow, rollen, verantwoordelijken en bevoegdheden, KPI's. Deze pocess outline is als bijlage toegevoegd aan de Externe Bijlage 3: IS Awareness & Learning Strategie.

Mijn bedrijfsmentor heeft daarvoor een voorbeeld van een process outline geleverd die binnen de organisatie wordt gehanteerd voor het uitschrijven en onderhouden van processen. Dit voorbeeld heb ik bestudeerd en gehouden tegen de aspecten die ik erin verwacht. Op basis daarvan besloot ik het document ook in te zetten voor de strategie.

Binnen de bank wordt er voor nieuwe processen een outline gemaakt, waarin het proces verder in details wordt uitgewerkt. Hiervoor is er binnen de bank een template gemaakt met vaste onderdelen die voor het proces uitgewerkt dienen te worden. Deze onderdelen zorgen ervoor dat er meer inzicht wordt verkregen in het proces.

De strategie heeft voor veranderingen gezorgd in de voorgaande aanpak, waardoor het jaarlijkse IS awareness proces degelijk is veranderd. Omdat het proces veranderd is, heb ik de nieuwe strategie ook uitgewerkt in een process outline. Ik heb besloten de template te gebruiken die ze binnen de ABN AMRO hanteren, omdat ik de onderdelen erin herken zoals ik dat geleerd heb van de opleiding voor onderhoudsplannen.

Tijdens de opleiding heb ik ook onderhoudsplannen moeten maken en daarin was het volgens de theorie verplicht dat de volgende zaken opgenomen waren:

- Algemene informatie van het plan zoals het doel, de scope, etc.,
- Activiteiten,
- Rollen en verantwoordelijkheden en
- Betrokken partijen

Deze zaken zijn ook opgenomen in de process outline template die de bank hanteert.

Voor het invullen van de process outline heb ik de template en een voorbeeld van een ander proces goed bestudeerd om ervoor te zorgen dat ik het op een goede wijze invul.

5. IS Awareness & Learning Toolbox

De derde en volgende stap in het proces was het (laten) ontwikkelen van nieuwe hulpmiddelen. Deze stap bestond uit twee stappen, namelijk:

- Het kiezen van thema's voor de hulpmiddelen
- Het (laten) ontwikkelen van hulpmiddelen

Deze stappen worden in dit hoofdstuk verder uitgelicht waardoor het inzichtelijk wordt hoe de IS Awareness & Learning Toolbox is samengesteld.

5.1. IS Awareness & Learning thema's

Op het gebied van informatiebeveiliging zijn er verschillende thema's waarvoor er hulpmiddelen ontwikkeld kunnen worden. Om deze thema's te inventariseren heb ik van een collega de lijst met thema's ontvangen die werd gehanteerd om de voorgaande survey in te richten. Deze lijst is verkregen van de leverancier InfoSecure, die zij hanteren voor hun e-learning hulpmiddelen.

Na deze lijst goed te hebben bestudeerd kon ik geen aanvullende thema's bedenken, maar kon ik wel clustering aanbrengen in de lijst. Dit heb ik gedaan om te voorkomen dat er een onoverzichtelijk lijst wordt opgeleverd dat het moeilijker kan maken om gericht thema's te kiezen.

Thema	Vraagstelling voor themasessie	Hulpmiddelen	Vorm
IB verantwoorde-lijkheden LG	Wat zijn de verantwoordelijkheden van de leidinggevende op het gebied van IB. Is de leidinggevende zich hiervan bewust en worden ze goed ingevuld. Waar kan het beter?	Informatiebeveiliging door leidinggevenden	E-learning
IB verantwoorde-lijkheden MW	Wat zijn de verantwoordelijkheden van de medewerker op het gebied van IB. Is de medewerker zich hiervan bewust en worden ze goed ingevuld. Waar kan het beter?	Basisopleiding uitgebreid Richtlijnen Basisprogramma Gouden Regels Gedragsregels Informatiebeveiliging	E-learning Brochur e

Figuur 15: Lijst met thema's

De lijst met thema's heb ik vervolgens vergeleken met de thema's van de beschikbare hulpmiddelen om af te leiden of er thema's zijn die nog niet voorzien zijn van hulpmiddelen. Uit deze vergelijking bleek dat de huidige hulpmiddelen redelijk dekkend zijn qua thema's. Er was maar één thema waar nog geen hulpmiddel voor beschikbaar was en dat was "Werken in the cloud", de reden hiervoor was omdat er in de organisatie gekozen is om "Werken in the cloud" niet toe te staan.

5.2. IS Awareness & Learning hulpmiddelen

De toolbox is een uitstekend idee om de aanspreekpunten van de business lines meer keuze te bieden in hulpmiddelen die zij kunnen inzetten in de campagnes. De toolbox moet dan wel bestaan uit hulpmiddelen die relevant en bruikbaar zijn voor de aanspreekpunten. De selectie van de hulpmiddelen voor de toolbox is daarom gedaan op basis van de lijst met thema's, input van de strategie en een onderzoek dat is uitgevoerd. Hoe dit is verlopen wordt in dit hoofdstuk behandeld.

5.2.1. Onderzoek

Gedurende vrijwel de hele afstudeeropdracht heb ik onderzoek gedaan naar trends op het gebied van information security awareness en state of the art hulpmiddelen. Dit onderzoek is een iteratief proces geweest die op basis van vraagstukken en/of ontwikkelingen van de strategie werd aangestuurd.

Hier heb ik voor gekozen zodat ik direct input kon leveren voor de strategie en de te volgen toolbox. De resultaten van het onderzoek kon ik meteen toetsen bij de klankbordgroep, waardoor ik de resultaten kon laten aansluiten op de eisen en wensen van de stakeholders.

Het doel van dit onderzoek was om input te leveren voor de strategie en de toolbox. Dit heeft geresulteerd in de Externe Bijlage 1: IS Awareness & Learning Strategie en de Externe Bijlage 2: IS Awareness & Learning Toolbox. Er is geen apart rapport opgesteld voor de onderzoeksresultaten, maar deze zijn wel als bijlage opgenomen in de twee producten.

Tijdens het onderzoek heb ik twee onderzoeksmethoden gebruikt, namelijk bureauresearch en diepte-interviews. Bureauresearch heb ik voornamelijk gebruikt om met name via sites en publicaties op internet de vraagstukken van de strategie te beantwoorden en ook de verschillende leveranciers te inventariseren. De diepte-interviews heb ik gebruikt om selectieve leveranciers te spreken over hun producten/diensten, in deze interviews heb ik tevens ook vraagstukken voorgelegd die ik door middel van bureauresearch niet kon beantwoorden. In deze paragraaf wordt toegelicht hoe de inventarisatie is gedaan en daarna hoe de vraagstukken zijn opgelost.

5.2.1.1. Inventarisatie van de leveranciers en producten/diensten

Uit de evaluatie was duidelijk geworden dat de klankbordgroep niet meer tevreden was met de huidige selectie van (passief gebruikte) hulpmiddelen. Daarom ben ik aan het begin van de afstudeerperiode begonnen met het inventariseren van leveranciers en de producten/diensten die zij leveren.

Hiervoor heb ik eerst gekeken naar de leveranciers waar ik kennis mee heb gemaakt via de opleiding, zoals LBVD, VKA, Sogeti en Trust in People. Van deze bedrijven heb ik de websites bezocht om te achterhalen welke producten en diensten zij leveren op het gebied van IS Awareness & Learning.

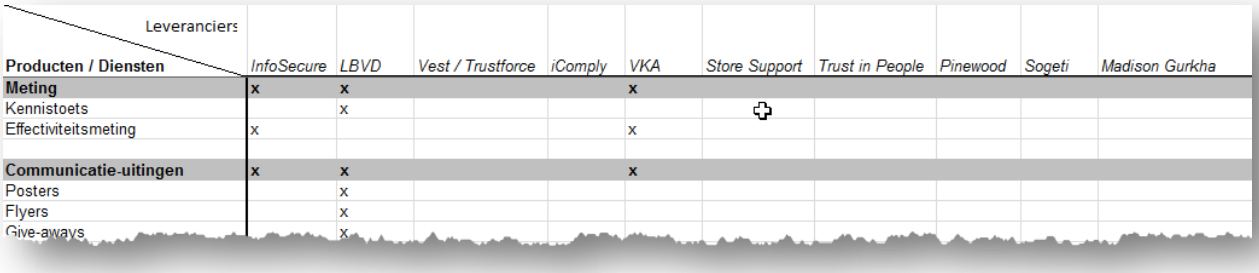
Daarnaast heb ik ook door middel van de onderstaande zoekwoorden en zoekmachines gezocht naar meerdere leveranciers.

Zoekwoorden	• Information Security Awareness • Bewustzijn • Awareness • Informatiebeveiliging • Social Engineering • Mystery guest • Awareness Game •
Zoekmachines/zoekplaatsen	• Google

Tabel 3: Zoekwoorden voor leveranciers

De zoektermen zijn tevens gecombineerd om zoveel mogelijk zoekresultaten te realiseren.

De resultaten zijn verwerkt in een Excel-spreadsheet, waarin is opgenomen welke producten/diensten er zijn en door welke leveranciers ze geleverd worden. Dat zag er volgt uit:



Leveranciers / Producten / Diensten	InfoSecure	LBVD	Vest / Trustforce	iComply	VKA	Store Support	Trust in People	Pinewood	Sogeti	Madison Gurkha
Meting	x	x			x					
Kennistoets		x								
Effectiviteitsmeting	x				x					
Communicatie-uitingen	x	x			x					
Posters		x								
Flyers		x								
Give-aways		x								

Figuur 16: Inventarisatie van leveranciers en producten/diensten

Met de inventarisatie van de producten en diensten wilde ik aan de klankbordgroep presenteren wat er tegenwoordig op de markt aanwezig is omtrent IS awareness. Daarna wilde ik van de klankbordgroep weten wat zij denken dat effectief zou kunnen zijn voor hun business lines. Op basis hiervan wilde ik dan bepalen wat op te nemen in de toolbox.

Naast de bureauresearch heb ik ook diepte-interviews afgenomen met verschillende leveranciers. Dit heb ik gedaan via de bedrijvendag van De Haagse Hogeschool en de InfoSecurity-beurs. Daar ben ik in contact gekomen met bedrijven die ik al kende zoals LBVD en Sogeti, maar ook bedrijven die ik nog niet kende zoals Pinewood en Madison Gurkha.

De bedrijvendag en InfoSecurity-beurs heb ik bezocht om in contact te komen met de leveranciers en te achterhalen welke producten/diensten zij bieden op het gebied van IS awareness. Wat tevens het doel was van de korte diepte-interviews die ik heb afgenomen.

Daarnaast heb ik ook contact opgenomen met twee leveranciers, namelijk Trustforce, InfoSecure en VKA. Bij VKA heb ik contact opgenomen met Déjaniera Rampersad, medestudent die daar werkzaam is, om te informeren naar hun producten/diensten op het gebied van IS awareness. Daarvan heb ik hun aanbod aan producten/diensten ontvangen met extra toelichting. Hierover zou er nog een gesprek ingepland worden met VKA.

Met Wilbert Pijnenburg, contactpersoon voor InfoSecure, heb ik samen met mijn bedrijfsmentor een uitgebreidere interview gehad. In de interview is dieper ingegaan op de producten die in ontwikkeling zijn en daarnaast zijn de vraagstukken ook voorgelegd waar er nog een oplossing voor werd gezocht. Zo heeft hij aangegeven de jaarlijkse cyclus volgens de kwaliteitscirkel van Deming een sterk component van de voorgaande aanpak te vinden.

Hij heeft in deze interview ook Blended Learning geadviseerd zoals eerder vermeld is, als mogelijke oplossing voor de vraagstuk het gebruik van de huidige e-learnings te verhogen. Daarnaast heeft hij ook de Awareness App uitgelicht die in ontwikkeling is. Dit hulpmiddel vond ik heel erg interessant omdat het de barrière verlaagt van informatiebeveiliging. Omdat medewerkers dan niet meer lastig gevallen worden met lange surveys of e-learnings die veel tijd kosten, maar via de App gewoon periodiek enkele vragen gepusht krijgen. Verder heeft hij ons ingelicht over de voor- en nadelen van mystery guest acties.

In de meetings met de klankbordgroep werd het duidelijk dat budget een belangrijk aspect was in de selectie van de middelen. Om hiermee rekening te houden werd er eerst gekeken of de producten die interessant zijn door de afdeling intern verzorgd kunnen worden. Zoals dat bijvoorbeeld is gedaan met de Clean Desk-actie of presentaties en workshops. Als de producten interessant waren en intern niet verzorgt konden worden, dan werd er verder gekeken naar het hulpmiddel. Nadat duidelijk is geworden waar de klankbordgroep naar op zoek is, ben ik met deze criteria verder op zoek gegaan en heb verschillende voorstellen gedaan. Het resultaat hiervan wordt in de volgende paragraaf beschreven.

5.2.1.2. Oplossen van vraagstukken

Bij het ontwikkelen van de nieuwe strategie wilde ik ervoor zorgen dat voldaan wordt aan de wensen van de stakeholders. Daardoor ontstonden vraagstukken waar een oplossing voor moest worden gevonden. Door middel van het onderzoek heb ik de oplossingen via bureauresearch of diepte-interviews gevonden.

Zo is bijvoorbeeld het vraagstuk opgelost van verhoogd gebruik van de beschikbare e-learnings. De vraagstukken van het vervangen van de survey en het richten van de strategie op houding en gedrag. Deze oplossingen zijn meteen verwerkt in de strategie en de toolbox.

5.2.2. IS Awareness & Learning hulpmiddelen

Op basis van de strategie en het onderzoek is een aantal aanvullende hulpmiddelen geselecteerd om toe te voegen aan de toolbox. Deze hulpmiddelen worden in deze paragraaf verder beschreven en er wordt ook toegelicht waarom ik deze hulpmiddelen opgenomen wil hebben in de toolbox. In enkele van deze hulpmiddelen heb ik mezelf kunnen verdiepen om uit te zoeken hoe de implementatie gerealiseerd kon worden. Voor de overige moet nog verdere verdieping plaatsvinden.

5.2.2.1. Blended Learning

Blended Learning is een combinatie van e-learning en het klassikaal behandelen van de stof, zoals in een vergadering. Een term die ik leerde kennen in een gesprek met Wilbert Pijnenburg, directeur Benelux van InfoSecure. InfoSecure is de huidige leverancier van e-learning middelen voor de bank.

Dit sprak mij echt aan, voornamelijk om de extra aandacht die je dan besteedt aan de e-learning middelen. Extra aandacht dat kan leiden tot het beter beklijven van de stof bij de medewerkers en elkaar op verkeerd gedrag aanspreken. Zeker ook om gebruik van de e-learning hulpmiddelen te verhogen, wat uit de evaluatie bleek te ontbreken. Informatiebeveiliging als onderwerp ook meer besproken te krijgen. En dit tussen leidinggevenden en medewerkers in plaats van de traditionele expert van informatiebeveiliging die alleen zijn kennis en regels probeert over te brengen naar de medewerkers. Een middel dus die veel voordelen heeft, maar ook simpel te realiseren lijkt.

Het concept van Blended Learning heb ik in de meeting met de klankbordgroep voorgesteld en besproken. De leden vonden dit ook een goed idee en er waren ook al twee die binnen hun business lines het concept willen inzetten. Een wilde het zelfs verplichten wat aantoonde dat de animo er zeker voor is vanuit de groep. Vandaar dat ik hen heb gevraagd mij op de hoogte te houden van de ontwikkelingen.

Verder ben ik zelf gaan brainstormen over hoe dit het beste aan te pakken en heb ik ook bureauresearch gedaan. Wat uit het bureauresearch bleek is dat het een heel algemene methode is die je in verschillende situaties kan toepassen. Daardoor realiseerde ik me dat je er een eigen invulling aan moet geven.

Voor de invulling heb ik teruggekeken naar de behoefte die er is en die ingevuld kan worden door de Blended Learning sessies. Op basis hiervan heb ik een handleiding opgesteld voor een Blended Learning sessie. Deze handleiding heb ik verwerkt op PowerPoint-slides, omdat ik zoals bij de strategie vond dat het de instructies op een overzichtelijk wijze kan weergeven. Ik heb dan slides waarop er eerst een inleiding met een toelichting van Blended Learning, daarna drie slides waarop er instructies beschreven is vóór de sessie, tijdens de sessie en na de sessie.

De invulling van de slides heb ik gedaan op basis van hoe ik dacht dat een dergelijke sessie zou kunnen verlopen. Daarvoor heb ik wel instructies gebruikt die online te vinden was over algemene vergadering. De handleiding is te vinden in de Externe Bijlage 2: IS Awareness & Learning Toolbox.

De handleiding heb ik echter nog niet kunnen testen vanwege het naderen van de einde van mijn afstudeerperiode. Ik heb dan met de bedrijfsmentor afgestemd hoe deze handleiding het beste te kunnen testen. Er zal met de eerste geïnteresseerde BL-aanspreekpunten worden afgesproken dat ISO begeleiding zal aanbieden bij de eerste soortgelijke sessies. Op basis van deze eerste sessies zal de handleiding worden aangescherpt indien nodig. Dit heb ik afgesproken omdat ik dacht dat je hiermee de handleiding aangescherpt wordt op basis van wat er in de praktijk gebeurt.

5.2.2.2. Awareness App

De Awareness App is een app voor de smartphone en tablets waarmee er via push-berichten een vraag, dilemma of iets dergelijks “gepusht” kan worden naar de gebruiker. De vraag of dilemma die gepusht wordt of de frequentie in push-berichten kon dan bepaald worden door de organisatie. Dit hulpmiddel vind ik heel erg interessant omdat het een heel laagdrempelige oplossing is die de vaak langdurige survey’s en e-learnings kan vervangen.

Om deze redenen heb ik de Awareness App voorgesteld om op te nemen in de toolbox. De bedrijfsmentor zag hier eerst niet in omdat hij twijfelt over de populatie binnen de bank die een smartphone in bezitting heeft. Zijn reden zie ik ook in, vooral omdat er niet lang geleden binnen de bank het concept Bring Your Own Device (BYOD) is ingevoerd. Maar omdat ik de Awareness App dermate interessant vond en er van overtuigd was dat het een effectief middel kan zijn, heb ik het geadviseerd als hulpmiddel die wel uitgeprobeerd moet worden. Op basis van de resultaten uit de pilot van de Awareness App kan dan besloten worden of het opgenomen toolbox.

5.2.2.3. Awareness Game

De Awareness Game is een survey-achtige spel waarbij er op zowel individueel als afdelingsniveau gestreden kan worden om wiens kennis hoger is op het gebied van informatiebeveiliging. Dit vond ik interessant als alternatief voor de normale survey omdat het een spelende effect kan hebben op de medewerkers. Echter zag ik wel in dat een dergelijke game spelen wel tijd neemt van de medewerkers om eerst de survey in te vullen en vervolgens bij te houden wie hoger heeft gescoord. Daarnaast had ik het idee dat je er na één keer uitgespeeld was.

Voor de Awareness Game heb ik een pilot gedaan met leden van de klankbordgroep om te kijken wat zij uit de business hiervan vinden. Daarna heb ik in één van de meetings om de meningen gevraagd over de Awareness Game. Uit deze pilot bleek dus dat er problemen waren met het aanloggen in de game en dat het verder amateuristisch leek. Ik heb hierbij aangegeven dat ik dacht dat het zou kunnen liggen aan het feit dat het een demo was, waardoor er misschien een incomplete versie werd ingezet.

Er werd ook aangegeven dat de game wel een meer uitdagend effect verzorgde, waardoor het niet als tijdrovend en lastig werd ervaren. Het competitief aspect van de game gaven de leden van de klankbordgroep ook een motivatie om hun kennis te verhogen en beter te scoren.

Op basis hiervan heb ik geadviseerd om de leverancier te vragen om een tweede pilot te draaien en hiervoor een complete versie van de game in te zetten.

5.2.2.4. Social Engineering Awareness testing

In toolbox heb ik als hulpmiddel Social Engineering acties opgenomen. Omdat ik denk dat het een effectief middel kan zijn om het gedrag te meten, maar ook om de medewerkers te prikkelen met de mogelijkheden. Doordat de acties uitgevoerd worden onder medewerkers in normale omstandigheden kan het de daadwerkelijk gedrag meten van de medewerkers wanneer zij geconfronteerd worden met een dergelijke aanval. En door de resultaten van deze meting te presenteren aan de medewerkers kan gewezen worden op de kwetsbaarheden en consequenties daarvan.

Voor deze acties heb ik externe leveranciers gevonden die deze diensten aanbieden. InfoSecure, LBVD en VKA waren hierbij de grootste aanbieders. Echter is er na een gesprek met Wilbert Pijnenburg de nadelen van soortgelijke acties boven tafel gekomen. Deze waren vooral dat een mystery guest actie gericht is op kleinere doelgroepen, en moeilijk inzetbaar zijn voor grotere doelgroepen. De kosten voor een dergelijke actie kan ook redelijk oplopen, omdat er zorgvuldige voorbereiding noodzakelijk is, en het geen one-size-fits-all oplossing is, waardoor het veel tijd kan nemen en dat gepaard gaat met meer kosten.

Ik heb een handleiding opgesteld om de BISO's te helpen met het voorbereiden van een dergelijke actie. Hiervoor heb ik eerst een dergelijke actie bestudeerd om de benodigdheden van deze acties voor te stellen. Deze heb ik vervolgens opgenomen in de handleiding Social Engineering. Deze handleiding zou ik vervolgens afstemmen met een leverancier van "mystery guest" acties, maar dat is mij vanwege tijdgebrek niet meer gelukt.

Bij het opstellen van de handleiding realiseerde ik me dat de tool in de toolbox aangeboden zou worden, maar dat er nog geen concrete keuze is gemaakt in de leverancier van deze tool. Ik heb dus geadviseerd om een pilot te draaien van een mystery guest actie en op basis daarvan te bepalen of het opgenomen moet worden in de toolbox.

5.2.2.5. Interne survey tool

De voorgaande jaarlijkse IS Awareness Survey was komen te vervallen nadat er uit de commentaar bleek dat het niet aansloot op de wensen van de gebruikers. De gebruikers vonden dit wel een goede beslissing en waren tevreden met de hogere mate van vrijheid die zij dan hadden. Maar dat nam niet weg dat een survey wel een effectief middel is om kennis te meten.

Ik had het idee om de keuze van meetmiddelen in de toolbox aan te vullen met een alternatief survey tool. Hiervoor keek ik naar de verschillende opties die er waren. Ik wist dat er genoeg alternatieve leveranciers waren die wij konden benaderen, maar dan zou het dezelfde verhaal zijn zoals wij die nu met de jaarlijkse survey tool hadden.

Maar dan realiseerde ik mij dat er binnen de bank door diverse afdelingen verschillende survey tools werden ingezet. Hiervoor hebben de andere afdelingen al contracten afgesloten met de leveranciers. Deze survey tools zouden wellicht ook ingezet kunnen worden door ons, indien er geen limiet is aan de hoeveelheid surveys of responses.

Hiervoor heb ik twee survey tools gevolgd waar ik eerder in contact mee ben gekomen. Voor één daarvan heb ik informatie kunnen inwinnen om het in te zetten als survey, mocht er een business line hier interesse in hebben en dit willen opnemen in de campagneplan.

Vanwege tijdsgebrek heb ik de tool niet verder in details kunnen verwerken en te testen. De informatie die ik tot dan heb ingewonnen heb ik overgedragen aan mijn collega's, die de inwerking van de tool verder gaan afhandelen.

6. Evaluatie

Over het algemeen ben ik positief over mijn inzet en kan ik tevreden terugblikken op de afgelopen 20 weken. In dit hoofdstuk is er kritisch en subjectief teruggeblikt op de afstudeerperiode met het oog op de leer- en verbeterpunten die naar voren zijn gekomen. Er is gekeken naar het proces en de opgeleverde producten. Daarnaast is er ook een verantwoording gegeven van de vooraf gestelde competenties.

6.1. Proces

Het afstudeertraject heb ik als een zeer prettig en leerzaam, maar zeker ook als een uitdagend proces ervaren. Het was misschien wel een te hoog gegrepen complexiteitsniveau waarvoor er veel achtergrondkennis van de organisatie en ervaring in het vakgebied vereist was. Zonder de goede begeleiding van mijn bedrijfsmentor en het advies van de klankbordgroep zou het niet gelukt zijn om deze opdracht succesvol af te ronden.

Achtergrondkennis van de organisatie miste ik in situaties zoals het bekijken naar oplossingen binnen organisatie in plaats van naar externe; wat meestal gepaard gaat met hogere kosten. Dit was zeker een aspect wat ik interessant en uitdagend vond om te ervaren, namelijk het rekening houden met budget. Bij projecten van de opleiding werd er nauwelijks kosten betrokken in de overwegingen, waardoor er meerdere mogelijkheden waren. Maar ik denk wel dat ik een frisse blik heb kunnen bieden in het project en dat ik daardoor mijn collega's heb ondersteund.

Door het missen van de achtergrondkennis merkte ik dat ik te weinig initiatief nam, omdat ik soms niet wist hoe verder te gaan. Maar de dagelijkse samenwerking met mijn bedrijfsmentor heeft wel gezorgd dat ik zijn kennis en ervaring direct mee kon nemen in mijn werkzaamheden, waardoor ik toch verder kon gaan.

De samenwerking met de klankbordgroep heeft als aanvullende begeleiding gezorgd omdat zij mijn vooruitgang gedeeltelijk ook beoordeelden en leverden hun ideeën als input. In mijn oriënterende stage was één van mijn verbeterpunten sneller advies te vragen van collega's omdat ik daardoor veel vertraging opliep. Deze samenwerking heeft dit punt zeker verbeterd en is iets dat ik vaker ga toepassen in mijn carrière omdat je daarmee verschillende kennis en ervaring verzameld maar ook meteen draagvlak creëert voor nieuwe ontwikkelingen.

Tijdens het afstudeertraject ben ik naar mijn mening wel te veel mee gegaan met de aanpak van mijn collega's, waarin zij ontwikkelingen in mondeling met elkaar behandelen. Hierdoor heb ik niet alles gerapporteerd, bijvoorbeeld wat ik heb ontdekt en waarom ik het interessant vond. Dit resulteerde in dat ik meer moeite had om in mijn afstudeerverslag de producten goed te presenteren en te verantwoorden. Maar ik ben wel tevreden met dat ik mijn collega's heb kunnen overtuigen om mijn adviezen te volgen. Dit is bijvoorbeeld te zien aan de middelen die ik heb geadviseerd, waarvoor zij een pilot gaan starten.

Ik heb wel bewust geacteerd in deze situatie omdat ik naast afgestudeerd zijn ook een tevreden opdrachtgever wilde hebben. Waarvoor ik wist dat ik op beide vlakken bepaalde dingen zou moeten opofferen en hoop ik dat ik een balans heb gevonden om beide doelen te bereiken.

6.2. Producten

6.2.1. Project Initiation Document

Over het PID heb ik weinig op te merken omdat ik het hebt opgesteld volgens de Prince2 methodiek dat ik vaker heb gedaan voor de projecten van de opleiding. Voor de invulling heb ik de inhoud van het afstudeerplan aangehouden die al eerder is afgestemd met de bedrijfsmentor.

Wat ik wel als verbeterpunt voor mezelf heb gesteld is dat ik wel moet inzien dat het PID een levende document is door het hele project waarop terug gevallen kan worden indien er wijzigingen komen in de planning en andere zaken dat beschreven worden in het PID.

Hiervoor moet ik mijn beeld van de PID/PVA veranderen door het niet te zien als alleen startdocument of acceptatiedocument, maar ook te zien als kader voor mijn project. Als ik me deze beeld kan aanleren dan zal ik bij vragen eerder terugvallen op de PID en vervolgens de opdrachtgever te benaderen indien het nog niet duidelijk is.

6.2.2. IS Awareness & Learning Strategie

Met de strategie dat als eindproduct is opgeleverd ben ik heel erg tevreden omdat het goedgekeurd is door de IS Core Team en wordt thans ingevoerd. Ik vind dat het zeker aansluit op de meeste eisen en wensen van de stakeholders. Aandacht voor de eisen van de toezichthoudende instanties en van het management team met het betrekken van de klankbordgroep in de ontwikkelingen van de strategie heeft gezorgd voor een kwalitatief product.

Er wordt in de strategie goed toegelicht waarom er een nieuwe strategie is, wat het inhoud, wat de scope er van is, wat er wordt verwacht en wat gedaan gaat worden. Ik vind wel dat er in alles wat te verbeteren of te optimaliseren valt, maar dat kan ik nauwelijks vinden van de strategie. Ik zou eventueel voor bepaalde vraagstukken meer verdiepen in de verschillende mogelijkheden die er zijn, maar aangezien de korte tijdsbestek was dat ook niet altijd mogelijk. Zo kon bijvoorbeeld voor de scope van de strategie meer onderzoek gedaan kunnen worden naar wat er echt speelt en wat de best practices daarvan zijn.

Maar naast het verdiepen in de mogelijkheden vind ik dat er een kwalitatief product is opgeleverd dat bankbreed geïmplementeerd wordt.

6.2.3. IS Awareness & Learning Toolbox

Over het algemeen ben ik wel tevreden over de IS Awareness & Learning Toolbox, maar ik vind het wel jammer dat ik niet meer betrokken kon zijn bij het proefdraaien van de verschillende middelen die ik heb onderzocht en geadviseerd.

Ik ben wel tevreden omdat ik wel op basis van de vraagstukken uit de strategie middelen heb onderzocht en geselecteerd. Ik zou het wel beter gevonden heb om zelf te achterhalen of dit inderdaad zo is. Maar dat zou een aparte opdracht betekenen, wat dan wel beschikbaar is gekomen voor een volgende stagiair.

Omdat de toolbox geen tastbaar product is, vind ik het lastig om dit te presenteren als bijlage van dit verslag. Dat ik geen rapporten heb opgesteld waarin wordt onderbouwd waarom ik vind dat de hulpmiddelen in de toolbox opgenomen moeten worden, heeft ook niet geholpen bij het verantwoorden van mijn opgeleverde producten.

6.3. Competenties

In dit hoofdstuk is een verantwoording afgelegd, waarin staat uitgelegd hoe aan de vooraf gestelde algemene- en vakspecifieke competenties is gewerkt. Deze zijn geselecteerd op basis van de aard van de opdracht en opgenomen in het afstudeerplan. Er is aan de competentie gewerkt door verschillende activiteiten uit te voeren en voor de verantwoording zal er per competentie een activiteit worden beschreven op de volgende wijze:

- *Situatie:* binnen welke situatie is gewerkt aan de competentie?
- *Taken:* wat waren de taken?
- *Acties:* welke acties zijn er uitgevoerd?
- *Resultaten:* wat waren de resultaten?
- *Reflectie:* wat was hier goed/fout aan? Wat was hiervan geleerd?

6.3.1. Algemene competenties

1. Het uitvoeren van een probleemoriëntatie. [niveau 3]

Situatie: Een nieuwe strategie ontwikkelen die de voorgaande strategie moet vervangen. De voorgaande strategie werd al vier jaar gevolgd en heeft in die tijd gefunctioneerd.
Taken: Om een nieuwe strategie te ontwikkelen moet ik weten waarom er precies een nieuwe strategie gewenst is en wat er mis was met de voorgaande.
Acties: Ik heb gesprekken gevoerd met de bedrijfsmentor en collega's die betrokken waren bij de ontwikkeling van de huidige strategie. Daarnaast heb ik de evaluatierapport van de voorgaande strategie bestudeerd die reeds opgesteld was.
Resultaten: Ik was goed geïnformeerd aan de opdracht begonnen omdat ik wist waarom er een nieuwe strategie gewenst was en in het evaluatierapport heb ik door middel van het ontvangen commentaar kunnen achterhalen wat zij vonden dat er ontbrak in de voorgaande strategie.
Reflectie: Met mijn aanpak hiervan ben ik wel tevreden omdat ik me snel heb kunnen inwerken in de situatie. Dat er al een evaluatie was gedaan van de voorgaande strategie heeft in mijn voordeel gewerkt, omdat het bestuderen van het rapport minder tijd heeft gekost dan dat ik de evaluatie zelf zou doen.

2. Het kiezen van een passende aanpak. [niveau 3]

Situatie: Om de opdracht in goede banen te leiden moest er besloten worden over een aanpak die gaat leiden tot een kwalitatief goed eindproduct dat aansluit op de werkwijze van de opdrachtgever.
Taken: Ik moest dus een aanpak vinden die bekend staat om het leveren van kwaliteit, maar ook waarin de opdrachtgever zich kan herkennen.
Acties: Ik heb vooronderzoek gedaan naar best practices, standaarden en andere documentatie over information security awareness. De resultaten heb ik dan besproken met de bedrijfsmentor om te kijken of hij er enkele zijn die hij herkent.
Resultaten: Hiervoor heb ik de NIST SP 800-50 gevonden die specifiek over het onderwerp van de opdracht gaat en dat aansluit op de werkwijze van de opdrachtgever. Deze publicatie was ontwikkeld door NIST dat bekend staat om de vele standaarden op het gebied van informatiebeveiliging.
Reflectie: Ik denk dat ik op basis hiervan een passende aanpak voor de opdracht heb gekozen. Ik vond het wel lastig om security professionals te vertellen dat ik niet zonder enig onderzoek hun aanpak wil volgen. Maar ik kon hiermee wel bevestigen dat hun aanpak ook door anderen wordt ingezet via deze standaard.

3. Het lezen, begrijpen en gebruiken van onderzoek. [niveau 3]

Situatie: Ik ging de opdracht in met de beperkte kennis die ik heb opgedaan via de opleiding en de ervaring van mijn voorgaande stage.
Taken: Om de opdracht uit te kunnen voeren moest ik een expert worden op het gebied van information security awareness.
Acties: In het vooronderzoek heb ik hier ook aandacht aan besteed. Ik ben op zoek gegaan naar literatuur over information security awareness en ik ben in gesprek gegaan met experts op dit gebied.
Resultaten: Er was niet veel literatuur over information security awareness, maar heb wel genoeg kunnen vinden om een passende aanpak te kiezen en om in te lezen in het onderwerp van de opdracht.
Reflectie: Dat er niet veel literatuur beschikbaar was op het gebied van information security awareness vond ik wel jammer, maar ik ben wel tevreden met het feit dat ik met de beperkte literatuur wel een strategie heb kunnen ontwikkelen die voldoet aan de eisen en wensen van de stakeholders.

4. Het uitvoeren van onderzoek. [niveau 2]

Situatie: Het ontwikkelen van een nieuwe strategie heeft gezorgd voor verschillende vraagstukken. Vraagstukken die voorzien moeten worden van oplossingen. Eén van de grootste daarvan was het selecteren van aanvullende hulpmiddelen die "state of the art" waren.
Taken: Mijn taak hierbij was het oplossen van deze vraagstukken op basis van wat er beschreven staat in best practices en wat experts op dit gebied hebben ervaren. Daarnaast moest ik ook inventariseren welke producten/diensten er allemaal op de markt waren en welke leveranciers er daarvoor zijn.
Acties: Om de vraagstukken op te lossen heb ik een onderzoek uitgevoerd als iteratief proces waardoor ik op basis van de ontwikkelingen in de strategie het onderzoek bijstuurde. Voor het onderzoek heb ik bureauresearch gedaan en interviews afgenomen met experts.
Resultaten: Voor elke vraagstuk heb ik een oplossing kunnen vinden die dan verwerkt is in de strategie en in de toolbox.
Reflectie: Het onderzoek heeft zeker bijgedragen aan de ontwikkeling van de strategie en het samenstellen van de toolbox. Daarom ben ik van mening dat ik deze competentie heb behaald.

5. Het vormgeven van een adviesproces en het tot uitvoer brengen daarvan. [niveau 3]

Situatie: Dit is opdracht dat wordt uitgevoerd voor een opdrachtgever, die bepaalde verwachtingen heeft.
Taken: Mijn taak was om ervoor te zorgen dat ik aan de verwachtingen voldoe van de opdrachtgever.
Acties: Met de bedrijfsmentor heb ik wekelijks een meeting gehad waarin ik presenteerde wat de ontwikkelingen waren en ik ook om een "go/no go" vroeg.
Resultaten: Op deze manier heb ik ervoor gezorgd dat ik de bedrijfsmentor kan meenemen in mijn ontwikkelingen en ook meteen te toetsen aan zijn verwachtingen.
Reflectie: Ik ben niet zeker of ik deze competentie goed heb geïnterpreteerd, maar met de bovenstaande actie vind ik dat ik mijn interpretatie heb gehaald.

6. Creëren van draagvlak voor implementatie van IB-beleid, -richtlijnen en –procedures. [niveau 3]

Situatie: Er waren verschillende stakeholders met elk andere eisen en wensen voor de strategie en de toolbox.
Taken: Het was mijn taak om de strategie en toolbox aan zoveel mogelijk van deze eisen en wensen te laten voldoen.
Acties: De ontwikkelingen van de strategie en de toolbox heb ik in een maandelijkse meeting gepresenteerd aan de klankbordgroep om hun mening en ideeën te vragen over de ontwikkelingen.
Resultaten: Het resultaat was een strategie en toolbox waar de klankbordgroep over had meegedacht.
Reflectie: Ik vind dat ik op deze wijze zeker draagvlak heb gecreëerd voor de ontwikkelingen van de strategie en toolbox. Het was voor mij op deze manier ook prettiger werken, omdat ik geloof in de kracht van samenwerking en dat op deze manier heb bereikt.

6.3.2. Vakspecifieke competenties

13. Het ontwerpen van IB-oplossingen op technisch, organisatorisch en menselijk vlak. [niveau 3]

Situatie: De afstudeeropdracht was in de richting
Taken: Ik moest een strategie ontwikkelen voor het aanpakken van information security awareness binnen de ABN AMRO.
Acties: Voor het aanpakken van information security awareness heb ik een strategie ontworpen en een toolbox samengesteld met verschillende hulpmiddelen.
Resultaten: Een, bij de nieuwe behoeften aansluitende, IS Awareness & Learning strategie en toolbox; verbeterde kennis op et gebied van IS awareness.
Reflectie: Gekeken naar de competentie en mijn producten vind ik dat ik zeker IB-oplossingen op organisatorisch en menselijk vlak heb ontworpen. En voor de technische vlak kan je zeggen dat dit wel betrokken was in de hiervoor genoemde oplossingen.

15. Het overdragen van kennis m.b.t. IB aan stakeholders. [niveau 3]

Situatie: De opdracht ging over information security awareness wat inhoudt het bewust maken van de doelgroep over de risico’s en gevaren van de omgang met informatie en informatiesystemen..
Taken: Ik moest dus ervoor zorgen dat het bewustzijn omtrent informatiebeveiliging van de medewerkers wordt verhoogd.
Acties: Ik heb bij het samenstellen van de toolbox met middelen gewerkt waar het doel van is om kennis met betrekking tot informatiebeveiliging over te dragen aan de doelgroep van de middelen en een zorgvuldige omgang met informatie en informatiesystemen te bevorderen. Daarbij heb ik gekeken naar de aanpak van de middelen, maar ook naar de inhoud.
Resultaten: Er zijn hulpmiddelen in de toolbox opgenomen waarvan ik overtuigd ben dat zij effectief gaan zijn in het bewustzijn opwekken over informatiebeveiliging.
Reflectie: Deze competentie was de hoofdzaak van mijn opdracht waar ik mij ook in heb verdiept.

7. Bijlagen

Hieronder is een overzicht gegeven van de bijlagen van mijn afstudeerverslag.

- Bijlage 1: Afstudeerplan
- Bijlage 2: Project Initiation Document
- Bijlage 3: Literatuurlijst
- Bijlage 4: Lijst met tabellen en figuren

Er zijn twee externe bijlagen, namelijk:

- Externe Bijlage 1: IS Awareness & Learning Strategie
- Externe Bijlage 2: IS Awareness & Learning Toolbox

Bijlage 1: Afstudeerplan

Informatie afstudeerder en gastbedrijf

Afstudeerblok: 2012-2.2 (start uiterlijk 19 november 2012)
Startdatum uitvoering afstudeeropdracht: 19 november 2012
Inleverdatum afstudeerdossier volgens jaarrooster: 25 maart 2013

Studentnummer: 08000417
Achternaam: dhr Kromosemito
Voorletters: G.R.
Roepnaam: Giovanni
Adres: Ingenhouszplein 8
Postcode: 2522 BA
Woonplaats: Den Haag
Telefoonnummer: -
Mobiel nummer: +31681360806
Privé emailadres: g.r.kromosemito@gmail.com

Opleiding: Information Security Management (ISM)
Locatie: Zoetermeer
Variant: voltijd

Naam studieloopbaanbegeleider: Leo van Koppen
Naam begeleidend examinator: Marjolein Faassen
Naam tweede examinator: Jaap de Bie

Naam bedrijf: ABN AMRO
Afdeling bedrijf: Information Security Office
Bezoekadres bedrijf: Foppingadreef 22
Postcode bezoekadres: 1102 BS
Postbusnummer: -
Postcode postbusnummer: -
Plaats: Amsterdam
Telefoon bedrijf: 020-4301500
Telefax bedrijf: -
Internetsite bedrijf: https://www.abnamro.nl/nl/prive/index.html#/?s=0/:S0

Achternaam opdrachtgever: dhr. Frijters
Voorletters opdrachtgever: C
Titulatuur opdrachtgever:
Functie opdrachtgever: Information Security Officer
Doorkiesnummer opdrachtgever: 020-6293561
Email opdrachtgever: cock.frijters@nl.abnamro.com

Achternaam bedrijfsmentor: dhr. Zomer
Voorletters bedrijfsmentor: J.A.
Titulatuur bedrijfsmentor:
Functie bedrijfsmentor: Sr. Expert Information Security
Doorkiesnummer bedrijfsmentor: 020-6285468
Email bedrijfsmentor: joop.zomer@nl.abnamro.com
NB: bedrijfsmentor mag dezelfde zijn als de opdrachtgever

Doorkiesnummer afstudeerder: N.t.b.
Functie afstudeerder (deeltijd/duaal): ISO Stagiair

Titel afstudeeropdracht:

Ontwikkelen en implementeren van een nieuwe informatiebeveiliging awareness strategie voor ABN AMRO

Opdrachtomschrijving

1. Bedrijf

ABN AMRO biedt haar particuliere, private banking en zakelijke klanten een volledig producten- en dienstenpakket aan. De bank biedt diepgaande financiële expertise, brede kennis van vele sectoren en een internationaal netwerk ten behoeve van nationale en internationale activiteiten.

Het uitgangspunt van de bank is het inspelen op de veranderende markt en dus op de eveneens veranderende behoeften van de klanten. Daar vraagt deze tijd ook om. Een bank die handelt in de context en realiteit van nu, die de klant met open vizier tegemoet treedt, leert van zijn ervaringen en beseft dat niets belangrijker is dan optimale service.

ABN AMRO is zich bewust van haar verantwoordelijkheid ten opzichte van al haar stakeholders. Vanzelfsprekend wil de bank uitstekende financiële resultaten behalen, maar zonder dat de klanten onverantwoorde risico's lopen.

De bank trekt lessen uit ervaringen uit het verleden, werkt in alle openheid aan verdere verbeteringen binnen de eigen organisatie en levert een bijdrage aan hervormingen binnen de gehele bancaire sector.

In 2008 heeft de Nederlandse staat het eigendom verworven van de Nederlandse activiteiten van ABN AMRO Holding N.V. en van Fortis Bank Nederland. In 2010 zijn ABN AMRO en Fortis Bank Nederland gefuseerd. Hierdoor ontstond het huidige ABN AMRO.

Information Security Risk Management (ISRM) is, als onderdeel van Information Security Office (ISO) georganiseerd in twee afdelingen: een nationaal en internationaal opererende afdeling. Mijn focus ligt op de nationale afdeling: Information Security Risk Management Nederland (ISRM NL). De missie van ISRM NL is: ervoor zorgdragen dat de vertrouwelijkheid, integriteit en beschikbaarheid van informatie en informatiesystemen van de geografisch in Nederland gelegen ABN AMRO onderdelen en haar relaties, gewaarborgd is.

ISRM NL levert zowel bankbrede als doelgroepspecifieke producten en diensten. Hieronder staat een overzicht van de ISRM NL diensten.

Diensten voor de hele bank:

- Identity & Access Management
- ✓ *IS Awareness & Learning*
- Information Security Organization & Communication
- Relationship management
- Risk Management Control

Diensten voor IT Solutions & Services (IT S&S):

- Management Assessment
- Risk Management & Control
- BCM Coordination
- Information Security Reporting

2. Aanleiding

Bij ABN AMRO werd voor de periode 2008 – 2012 eenzelfde aanpak gevolgd om de security awareness bij de medewerkers tijdens de integratieperiode van ABN AMRO NL en Fortis NL te bewaken en waar nodig te verhogen. Deze aanpak was gebaseerd op een jaarlijkse cyclus met de volgende fasering:

1. Uitvoeren van een IS Awaraness Survey: het meten van de IS awareness (kennis, houding, gedrag) met behulp van een vragenlijst die steekproefsgewijs uitgezet werd onder medewerkers,
2. Analyse van de meetresultaten per business line en ontwikkeling van aan zorgpunten gerelateerde aanvullende awareness hulpmiddelen (bv. flyers, Quick Learning Programs, News Flashes),
3. Plannen en uitvoeren van IS awareness campagnes per business line, met focus op de specifieke resultaten en zorgpunten van de business line en gebruik van de beschikbare awareness hulpmiddelen.

Na vier jaar deze aanpak gevolgd te hebben, verloor deze aan kracht. Daarom is, samenvallend met de afronding van de integratieperiode, opdracht gegeven om een nieuwe IS Awareness strategie voor de bank te ontwikkelen.

3. Probleemstelling

De in 2008 – 2012 gevolgde IS awareness aanpak verloor aan kracht. Uit onderzoek is gebleken dat medewerkers niet meer zo positief waren over deze aanpak. Reacties van de medewerkers luidden als volgt: zij vonden de uitgevoerde survey en campagne te eentonig omdat zij jaarlijks dezelfde vragen voorgelegd kregen, verder vonden ze het ook te generiek omdat één en dezelfde lijst naar alle deelnemers werd gestuurd. De resultaten uit de survey waren te globaal om er gerichte acties uit te halen. Dit heeft tot gevolg gehad dat de motivatie binnen de business Lines voor het uitvoeren van gerichte campagnes afnam, dat de hulpmiddelen onvoldoende werden gebruikt en dat er geen significante vooruitgang wordt bereikt t.a.v. de IS Awareness. .

Omdat Security Awareness hoog in het vaandel staat bij ABN AMRO, is er besloten om de huidige aanpak te evalueren en opdracht te geven om voor de komende 3 – 5 jaar een Vernieuwde IS Awareness Strategie te bepalen die aansluit bij de nieuwe wensen van de organisatie en bij de nieuwe ontwikkelingen in de markt.

4. Doelstelling van de afstudeeropdracht

Mijn doel bij deze opdracht is om de opdrachtgever te helpen met het neerzetten van een strategie die aansluit bij de wensen van het management en de medewerkers, waarin er “state of the art” aanpakken en middelen op het gebied van IS Awareness zijn opgenomen. Dit wil ik bereiken door een onderzoeksrapport over trends in de IS Awareness, Scopingsrapport en Onderhoudsrapport als onderdeel voor de nieuwe strategie op te leveren.

5. Resultaat

Er is een nieuwe IS Awareness strategie vastgesteld voor de komende 3 – 5 jaar waarmee de door het management gewenste vooruitgang wordt bereikt. De te realiseren invulling van de strategie is afwisselend genoeg is om de aandacht van management en medewerkers te blijven trekken. Dit wordt mede bereikt door een door mij uit te voeren evaluatie van de huidige situatie, door mijn onderzoek naar de “state of the art” op het gebied van IS Awareness en door mijn opzet en uitwerking van de te volgen nieuwe strategie in samenwerking met betrokkenen van de bank. Voorts oplevering van een invoeringsplan voor de nieuwe strategie.

6. Uit te voeren werkzaamheden, inclusief een globale fasering, mijlpalen en bijbehorende activiteiten

Periode	Activiteiten
Week 47	Oriënteren in het project en de afdeling en het opstellen van de Project Initiation Document (volgens Prince2)
Week 48	Onderzoeken: trends in IS Awareness *door deskresearch, literatuuronderzoek en gesprekken met professionals*
Week 49	Onderzoeken: belangrijkste leveranciers en producten/diensten (voor kennis, houding en gedrag) op gebied van IS Awareness in Nederland *door deskresearch, IS beurzen en bedrijven te bezoeken*
Week 50	Onderzoeksresultaat verwerken in een rapport: "**State of the Art – IS Awareness & Training**"
Week 51	Scoping bepalen voor "New IS Awareness Strategy" *door verschillende aanpakken te vergelijken: een informatiebeveiliging (IB)-aanpak vs. een Risk Awareness-aanpak (naast IB ook BCM en Compliance), alleen Awareness-aanpak of met Training erbij*
Week 52	**"New IS Awareness Strategy"** met onderzoeksresultaten over Trends in IS Awareness en gekozen scoping presenteren aan opdrachtgever.
Week 1	Huidige IS Awareness tooling van de bank evalueren+ organiseren van presentaties en demo's over producten/diensten van leveranciers aan de opdrachtgever+ inrichten "vitrine" met IS Awareness producten/diensten
Week 2	Oplevering "vitrine"
Week 3	Handleiding/procesbeschrijving/SOP maken voor de uitvoering en bewaking van de strategie incl. process flow, rollen, verantwoordelijken en bevoegdheden, KPI's
Week 4	Vervolg week 3
Week 5	Vervolg week 3
Week 6	Oplevering handleiding/procesbeschrijving/SOP
Week 7	Template uitwerken voor plan voor IS Awareness campagne voor Business Lines
Week 8	Oplevering template
Week 9	Overdracht
Week 10	Opbouwen van het afstudeerdossier
Week 11	Afronden afstudeerdossier
Week 12	Inleveren afstudeerdossier

7. Op te leveren (tussen)producten

- **Project Initiation Document (PID)**
- Onderzoeksrapport "**State of the Art - IS Awareness & Training**"
- Rapport "**New IS Awareness Strategy"**
    - Onderdeel "**Scoping of "New IS Awareness Strategy**"
    - Onderdeel "**IS Awareness Strategy Maintenance**"
    - Onderdeel "**IS Awareness Campaign Template for Business Lines**"

8. Te demonstreren competenties en wijze waarop

De verplicht uit te voeren beroepstaken in de afstudeeropdracht zijn:

1. Het uitvoeren van een probleemoriëntatie. [niveau 3]
Ik ga inlezen en bestuderen van de evaluatie van de vorige strategie en de middelen die daarbij gebruikt waren.

2. Het kiezen van een passende aanpak. [niveau 3]

Ik ga de kennis die ik heb opgedaan en netwerk die ik heb opgebouwd met verschillende bedrijven tijdens de opleiding inzetten voor het uitvoeren van de opdracht.

3. Het lezen, begrijpen en gebruiken van onderzoek. [niveau 3]
Ik ga literatuur, best practices en standaarden zoals de NIST SP800-50 raadplegen om een expert te worden van de onderwerpen die spelen in mijn afstudeeropdracht.

4. Het uitvoeren van onderzoek. [niveau 2]
Ik ga een kort onderzoek doen naar de trends in de Information Security Awareness. Dit ga ik doen door deskresearch te doen, literatuur raadplegen, in gesprek gaan met professionals, beurzen en bedrijven bezoeken.

5. Het vormgeven van een adviesproces en het tot uitvoer brengen daarvan. [niveau 3]
Mijn input voor de strategie zal ik ten eerste als advies overbrengen en deze na overleg met de opdrachtgever ook daadwerkelijk uitvoeren.

6. Creëren van draagvlak voor implementatie van IB-beleid, -richtlijnen en -procedures. [niveau 3]
Er is een werkgroep opgesteld waaraan ik mijn tussentijdse resultaten ga presenteren en zij mij daarover gaan adviseren en mij een go/no go geven.

13. Het ontwerpen van IB-oplossingen op technisch, organisatorisch en menselijk vlak. [niveau 3]
Ik ga een strategie opstellen voor de organisatie die de informatiebeveiliging gaat bewaken op organisatorisch en menselijk vlak.

15. Het overdragen van kennis m.b.t. IB aan stakeholders. [niveau 3]
Ik zal een advies geven over middelen die ingezet kunnen worden om kennis over te dragen aan de stakeholders. Daarbij zal ik ook betrokken zijn bij het bepalen van de inhoud van de middelen.

9. Risicomanagement

De volgende tabel geeft een overzicht van de bedreigingen ten aanzien van het project met voorgestelde tegenmaatregelen, de kans van optreden en de mate van negatief effect op het project (aangegeven op een schaal van 1tot 5)[1]. De laatste kolom geeft het risico aan (kans*effect). Op deze wijze kan gefundeerd worden afgewogen welke bedreigingen de meeste aandacht of hulpbronnen verdienen.

Bedreiging	Tegenmaatregel	Kans	Effect	Risico
Tijdsgebrek	Planning goed aanhouden(gebruik maken van timeboxen). Indien het niet lukt, de opdrachtgever hierover informeren middels een Exception Report om uitstel of een andere oplossing voor te vragen.	4	4	16
Gebrek aan begeleiding	Dit bij de begeleiders signaleren en hiervoor samen een oplossing zoeken.	2	3	6
Gebrek aan kennis	Zelf inlezen (deskresearch/literatuur) over onbekende onderwerpen en indien men er niet uitkomt, tijdig begeleiding opzoeken.	4	3	12

[1] 1 = kleine kans of gering effect, 5 = grote kans of groot effect

Bijlage 2: Project Initiation Document

1. Inleiding en achtergrond project

Bij ABN AMRO was er voor de afgelopen vier jaar een strategie ontworpen om security awareness bij de interne medewerkers aan te pakken. Deze strategie is gebaseerd op een jaarlijkse cyclus waarbij er eerst gemeten wordt, daarna wordt de campagne uitgevoerd en ten slotte een evaluatie met verbeteren. Door middel van de IS Awareness Survey wordt het niveau van bewustzijn bij medewerkers getoetst op verschillende onderwerpen. Op basis hiervan wordt de IS Awareness Campagne uitgevoerd. Tijdens de evaluatie wordt er gekeken naar het eventueel ontwikkelen van extra middelen, zoals "newsflashes", filmpjes, quick learnings, flyers en artikelen op het intranet.

Uit onderzoeken is echter gebleken dat de huidige strategie niet meer het gewenste resultaat levert. Zo is er in de afgelopen vier jaar geen significante vooruitgang meer bereikt. Verder is er ook negatieve feedback ontvangen van de eindgebruikers. Zij vonden de uitgevoerde survey en campagne te eentonig, waarbij steeds weer dezelfde vragen en zelfde middelen worden gebruikt. Verder vonden ze het ook te generiek, waardoor onderwerpen niet altijd van toepassing waren. De resultaten uit de campagne was te globaal om er gerichte acties uit te halen. Dit heeft tot gevolg gehad dat de huidige middelen niet voldoende worden gebruik en dat er geen significante vooruitgang is bereikt.

Omdat Security Awareness hoog in het vaandel staat bij ABN AMRO is er besloten om de huidige strategie aan te pakken. Door een helemaal vernieuwt strategie te formuleren die aansluit bij de wensen van zowel het management als dat van de medewerkers.

In de volgende hoofdstukken komt achtereenvolgens aan de orde:

- de projectdefinitie (o.a. doelstellingen, aanpak en resultaten);
- de organisatiestructuur;
- de initiële projectplanning;
- de beheersingsmechanismen (tolerantie, rapportage en uitzonderingsprocedure);
- de projectrisico's, inclusief tegenmaatregelen.

In de bijlagen zijn opgenomen:

- de Competenties;
- projectplanning met grafische weergaven.

2. Projectdefinitie

2.1. Doelstellingen

Doel van het project is om de opdrachtgever een nieuwe strategie te ontwikkelen die aansluit bij de wensen van het management en de medewerkers, maar ook voldoet aan de eisen van de toezichthoudende instanties. Tevens wordt in de strategie “state of the art” aanpakken en middelen op het gebied van IS Awareness opgenomen.

2.2. Aanpak en fasering

Het project wordt aangepakt volgens de NIST SP 800-50 en bestaat uit de volgende fasen:

1. Scope bepalen IS Awareness & Learning Strategie
2. Ontwikkelen IS Awareness & Learning Strategie
3. Ontwikkelen IS Awareness & Learning Toolbox
4. Opstellen afstudeerdossier

2.3. Resultaten

Het project levert de volgende hoofdproducten op, die elk nader gespecificeerd kunnen worden:

- IS Awareness & Learning Strategie
- IS Awareness & Learning Toolbox
- Afstudeerdossier

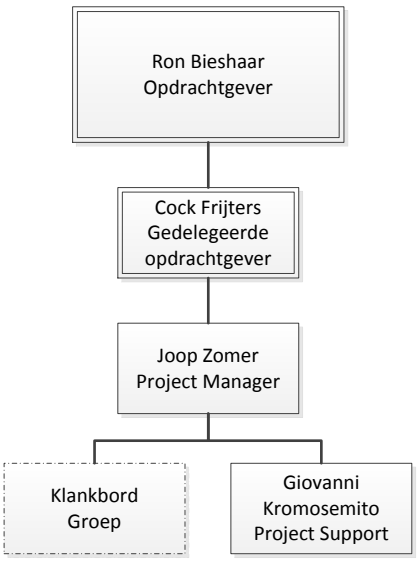
De eerste twee producten zullen aan de opdrachtgever opgeleverd worden en zullen deel uitmaken van het afstudeerdossier. Het afstudeerdossier wordt als eindresultaat van de afstudeerstage opgeleverd aan de examinatoren van de opleiding.

2.4. Omvang

De afstudeeropdracht zal inhouden het ontwikkelen van de nieuwe strategie en de bijbehorende toolbox. De implementatie ervan zal echter buiten beschouwing gelaten worden, aangezien de beperkte tijdsduur. Wat betreft het budget zal ik weinig invloed hebben; er zal wel bewust omgegaan worden met ontwikkelingen en selectie op basis van zo weinig mogelijk budget.

3. Organisatiestructuur

Voor de duur van het project wordt een tijdelijke organisatie opgezet:



Hierna worden de verantwoordelijkheden van de diverse betrokken groepen algemeen toegelicht.

Projectmanagement	
Na(a)m(en)	**Rol**
Ron Bieshaar	Opdrachtgever
Cock Frijters	Gedelegeerde opdrachtgever

Projectmanagement is verantwoordelijk voor de optimale inpassing van het project in het programma en aansluiting bij de bedrijfsdoelstellingen.

Project Manager & Project Support	
Na(a)m(en)	**Rol**
Joop Zomer	Project Manager
Giovanni Kromosemito	Project Support

De Projectmanager krijgt van de gedelegeerde opdrachtgever de verantwoordelijkheid en bevoegdheid voor de dagelijkse gang van zaken in het project. De Project Manager kan beslissingen nemen binnen de grenzen zoals aangegeven door het Projectmanagement. De belangrijkste verantwoordelijkheid van de Project Manager is het zekerstellen dat het project de gewenste producten oplevert, binnen tijd, binnen budget en volgens de afgesproken kwaliteit. De Project Manager rapporteert aan het Projectmanagement.

Project Support ondersteunt de Project Manager met de projectwerkzaamheden dat leidt tot de gewenste producten.

Klankbordgroep	
Na(a)m(en)	**Rol**
Jolanda Ciapa	Senior User (COO/C&MB/CC)
Michiel Vreugdenburg	Senior User (COO/PB Int)
Bert Reemer	Senior User (BS/FM)
Eva Maas	Senior User (SIM)
Mart Perrels	Senior User (IT S&S/ISO) Centrale 47oordinator IS Awareness aanpak

De klantbordgroep bestaat uit potentiële gebruikers van de te ontwikkelen strategie en bijbehorende producten. De klankbordgroep komt formeel alleen bij elkaar voor het geven van advies over de in ontwikkeling zijnde strategie en bijbehorende producten.

4. Initiële Projectplanning

De projectplanning geeft aan welke acties wanneer door wie worden ondernomen en wat de bijbehorende kosten zijn. Deze planning kan gedurende de loop van het project aangepast worden op basis van ervaringen in het project en / of nieuwe gegevens.

4.1. Randvoorwaarden

Aan de volgende randvoorwaarden dient te zijn voldaan om onderstaande planning te kunnen halen:

- benodigde hulpbronnen beschikbaar conform aanvraag;
- tijdige besluitvorming;
- bereidheid van de collega's om input te leveren;

4.2. Externe afhankelijkheden

Voor de IS Awareness & Learning Toolbox zal er onderzoek gedaan worden naar externe leveranciers van producten/diensten op het gebied van information security awareness. Voor dit onderzoek zal interviews afgenomen worden met:

- Hildo Krop van Trustforce
- Wilbert Pijnenburg van InfoSecure
- Déjaniera Rampersad van VKA

Daarnaast zal er ook een bedrijvendag bezocht worden en de infosecurity beurs om meer leveranciers te spreken over hun producten/diensten.

4.3. Projectplanning

In de bijlagen zijn grafische weergaven opgenomen van de planning op projectniveau, waarbij de verschillende fasen van het project met hun doorlooptijd en afhankelijkheden zijn weergegeven. In de gedetailleerde faseplanningen kunnen als gevolg van opgedane ervaringen en nieuwe gegevens nog aanpassingen plaatsvinden.

Fase	**Geplande Startdata**	**Geplande Einddata**	**Doorlooptijd cumulatief**
Oriëntatie	29.10.2012	12.11.2012	10
Scope bepalen	12.11.2012	19.11.2012	5
Strategie ontwikkelen	19.11.2012	28.01.2013	50
Toolbox ontwikkelen	28.01.2013	04.03.2013	25
Opstellen afstudeerdossier	04.03.2013	25.03.2013	15
		TOTAAL:	**105 dagen**

5. Beheersingsmechanismen

Hierna wordt aangegeven welke mechanismen worden toegepast om te waarborgen dat het project beheersbaar blijft.

5.1. Toleranties

Tijdens de uitvoering van het project controleert de Projectmanager regelmatig de voortgang. Indien de afwijking van de plannen naar verwachting groter is dan de afgesproken tolerantie, wordt daarover apart gerapporteerd aan de Project Board. De tolerantie op projectniveau is als volgt gedefinieerd:

- doorlooptijd plus of min 10%;

Per fase kunnen afwijkende toleranties worden opgenomen in de faseplanningen, afhankelijk van de omvang en impact van risico's.

5.2. Voortgangsbewaking

Er zijn twee momenten waarop de voortgang van het project besproken zal worden:

- Wekelijkse BiLa met bedrijfsmentor
- Maandelijkse meeting met klankbordgroep

Naast deze twee periodieke momenten zal ik nauw samenwerken met de bedrijfsmentor en andere collega's van wie ik advies kan vragen.

5.3. Uitzonderingsprocedure ('Management by Exception')

De uitzonderingsprocedure treedt in werking als van een fase of van het project verwacht wordt dat het niet binnen de afgesproken tolerantiegrenzen ten aanzien van tijd en geld blijft. Zodra de Project Manager dit op basis van aangeleverde informatie verwacht, meldt de Project Support dit in een BiLa met de Project Manager. In onderling overleg wordt de aanleiding en oorzaak besproken. Daarna wordt besloten tot één van de volgende situaties:

- de Project Manager treft maatregelen ter voorkoming/opheffing van de aanleiding;
- de Project Manager besluit geen actie te ondernemen, omdat het denkt dat de overschrijding van de tolerantie niet plaats zal vinden;

De eerste drie situaties worden vermeld in het eerstvolgende Highlight Report. De laatste situatie kan op verzoek van het Projectmanagement leiden tot het opstellen van een Exception Plan met alternatieven voor de aanpak van het vervolg van het project en aangepaste planningen.

6. Projectrisico's

De volgende tabel geeft een overzicht van de tot nu toe onderkende bedreigingen ten aanzien van het project met voorgestelde tegenmaatregelen, de kans van optreden en de mate van negatief effect op het project (aangegeven op een schaal van 1tot 5) [2]. De laatste kolom geeft het risico aan (kans*effect). Op deze wijze kan gefundeerd worden afgewogen welke bedreigingen de meeste aandacht of hulpbronnen.

Bedreiging	Tegenmaatregel	Kans	Effect	Risico
Tijdsgebrek	Planning goed aanhouden (gebruik maken van timeboxen). Indien het niet lukt, de opdrachtgever hierover informeren middels een Exception Report om uitstel of een andere oplossing voor te vragen.	4	4	16
Gebrek aan begeleiding	Dit bij de begeleiders signaleren en hiervoor samen een oplossing zoeken.	2	3	6
Gebrek aan kennis	Zelf inlezen (deskresearch/literatuur) over onbekende onderwerpen en indien men er niet uitkomt, tijdig begeleiding opzoeken.	4	3	12

[2] 1 = kleine kans of gering effect, 5 = grote kans of groot effect

Bijlage 1: Competenties

De verplicht uit te voeren beroepstaken in de afstudeeropdracht zijn:

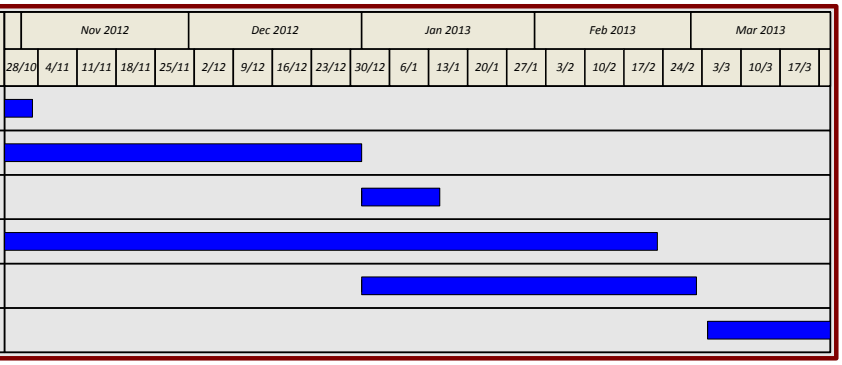
1. Het uitvoeren van een probleemoriëntatie. [niveau 3]
   Zoals bijvoorbeeld een intake, krachtenveldanalyse, cultuurscan etc. die kan leiden tot probleem- en opdrachtformulering (scope, fiattering)
2. Het kiezen van een passende aanpak. [niveau 3]
   Uitgangspunt is hierbij dat aan randvoorwaarden voor integriteit en vertrouwelijkheid (VOG, vrijwaring etc.) wordt voldaan. Kiezen van passend referentiekader bij het uitvoeren van onderzoek en/of IB-werkzaamheden.
3. Het lezen, begrijpen en gebruiken van onderzoek. [niveau 3]
   Waaronder het lezen en gebruiken van literatuur/publicaties.
4. Het uitvoeren van onderzoek. [niveau 2, evt. niveau 3]
   Het formuleren van een onderzoeksvraag, het structureren van een onderzoek, het verzamelen van gegevens en het verwerken van gegevens tot conclusies.
5. Het vormgeven van een adviesproces en het tot uitvoer brengen daarvan. [niveau 3]
   Hierbij dient rekening te worden gehouden met doelgroep en mogelijkheden
6. Creëren van draagvlak voor implementatie van IB-beleid, -richtlijnen en -procedures. [niveau 3]
   Geldend voor alle geledingen van de organisatie en voor alle soorten van maatregelen.

13. Het ontwerpen van IB-oplossingen op technisch, organisatorisch en menselijk vlak. [niveau 3]
15. Het overdragen van kennis m.b.t. IB aan stakeholders. [niveau 3]

Bijlage 2: Grafische weergaven projectplanning

Hieronder is een grafische weergaven van de projectplanning opgenomen.

ID	Task Name	Start	Finish	Duration
1	PID opstellen	10/29/2012	11/2/2012	1w
2	IS Awareness Strategie ontwerpen	10/29/2012	12/31/2012	9.2w
3	Onderhoudsplan	1/1/2013	1/14/2013	2w
4	“State of the art” onderzoek	10/29/2012	2/22/2013	17w
5	Vitrine ontwikkelen	1/1/2013	3/1/2013	8.8w
6	Afsudeerdossier opstellen	3/4/2013	3/25/2013	3.2w



Bijlage 3: Literatuurlijst

Deze bijlage betreft de literatuur die ik heb geraadpleegd tijdens het afstudeertraject ter ondersteuning van de opdracht en dit verslag. Daarnaast zijn de experts ook opgenomen die ik in het afstudeertraject heb gesproken.

Boeken

Daniël Jumelet, *DYA | Infrastructuur,* Sdu Uitgevers bv 2007

Paul Overbeek, Edo Roos Lindgreen, Marcel Spruit, *Informatiebeveiliging onder controle 2e editie,* Pearson Education Benelux bv 2006

Nel Verhoeven, *Wat is onderzoek?,* Boom Onderwijs 2007

P.L. Overbeek, Edo Roos Lindgreen, *Informatiebeveiliging onder controle,* FT Prentice Hall 2005

Publicaties en rapporten

Joop Zomer, *Evaluatierapport,* ABN AMRO 2012

Mark Wilson and Joan Hash, *Building an Information Technology Security Awareness and Training Program,* National Institute of Standards and Technology 2003

Déjaniera Rampersad, *Scriptie "Onderzoek naar de kritieke succesfactoren voor de inrichting van Identity & Access Management,* De Haagse Hogeschool 2011

Safira Ilahibaks, *Afstudeerverslag,* De Haagse Hogeschool 2012

Experts

Hildo Krop, *Principal Consultant,* Trustforce

Wilbert Pijnenburg, *Director Benelux,* InfoSecure

Déjaniera Rampersad, *Information Security Management Consultant,* Verdonck, Klooster & Associates

Bijlage 4: Lijst met tabellen en figuren

Tabellen

Figuren

AFSTUDEERVERSLAG

Het ontwerpen en implementeren van een nieuwe IS Awareness & Learning Strategie

DATUM:	25 maart 2013
STATUS:	Definitief
VERSIE:	1.0

STUDENT:	Giovanni Kromosemito
STUDENTNUMMER:	08000417
EXAMINATOREN:	Mw. M.M. Faassen (Begeleidend) Dhr. J.A. de Bie

ONDERWIJSINSTELLING:	De Haagse Hogeschool
OPLEIDING:	Information Security Management

ORGANISATIE:	ABN AMRO Bank N.V.
AFDELING:	Information Security Office
OPDRACHTGEVER:	Dhr. C. Frijters
BEDRIJFSMENTOR:	Dhr. J.A. Zomer

Opgeleverde producten

Afstudeerstage

Giovanni Kromosemito
08000417

Information Security Management
De Haagse Hogeschool

25 maart 2013
Versie 1.0

Strategy

IS Awareness & Learning

Joop Zomer | Giovanni Kromosemito
ISO
januari 2013

Aanpak IS Awareness & Learning - Inleiding-

- De huidige IS Awareness (ISA) aanpak wordt zo'n 5 jaar gevolgd en heeft tijdens de integratieperiode goed gewerkt.

- Omdat de integratieperiode is beëindigd en omdat signalen van "slijtage" werden ontvangen, is besloten om de huidige aanpak te evalueren, de requirements en "best practice" t.a.v. ISA-aanpak te onderzoeken en op basis daarvan een vernieuwde strategie voor de komende jaren te definiëren.

- Dit project is in september 2012 opgepakt door ISO, ondersteund door een klankbordgroep met aanspreekpunten vanuit de business die zich via een verzoek in het IS-Core team hadden aangemeld (deelnemers van COO/C&MB, COO/PB Int., BS/FM, SIM).

- Deze presentatie gaat in op de nieuwe aanpak.

- In bijlage 1 wordt nader ingegaan op de nieuwe aanpak voor het bepalen van campagne speerpunten en op Blended Learning. Deze worden in de toolbox nader uitgewerkt.

  Bijlage 2 geeft een overzicht van de inhoud van de huidige IS Awareness en Learning toolbox.

  In bijlage 3 wordt kort ingegaan op de "huidige" aanpak en de evaluatieresultaten.

  .

Aanpak IS Awareness & Learning - Scope -

- Uitgangspunt voor de overall IS Awareness & Learning aanpak is GISP policy rule 5.4.4.: *new and current personnel must be properly informed and trained about their information security responsibilities and the related policies and standards.*

- De belangrijkste maatregelen voor de implementatie van deze policy rule zijn:
  1. Verstrekking van de brochure “Richtlijnen Informatiebeveiliging” aan nieuwe medewerkers;
  2. Opname en volgen van twee verplichte e-learnings op My Learning & Development:
     - Basisprogramma Gouden Regels: verplicht voor nieuwe medewerkers
     - Informatiebeveiliging door leidinggevenden: verplicht voor nieuwe leidinggevenden
  3. Uitvoering van een jaarlijks IS awareness-programma voor de “zittende” bezetting, inclusief de ontwikkeling van ondersteunende hulpmiddelen.

- De eerste twee punten zijn/worden via HR verankerd in reguliere processen (o.a. on-boarding) en worden bewaakt via control assessments vanuit het Risk Control Framework. Dit document gaat verder in op punt 3: de uitvoering van het jaarlijkse IS Awareness & Learning programma.

Aanpak IS Awareness & Learning - Uitgangspunten -

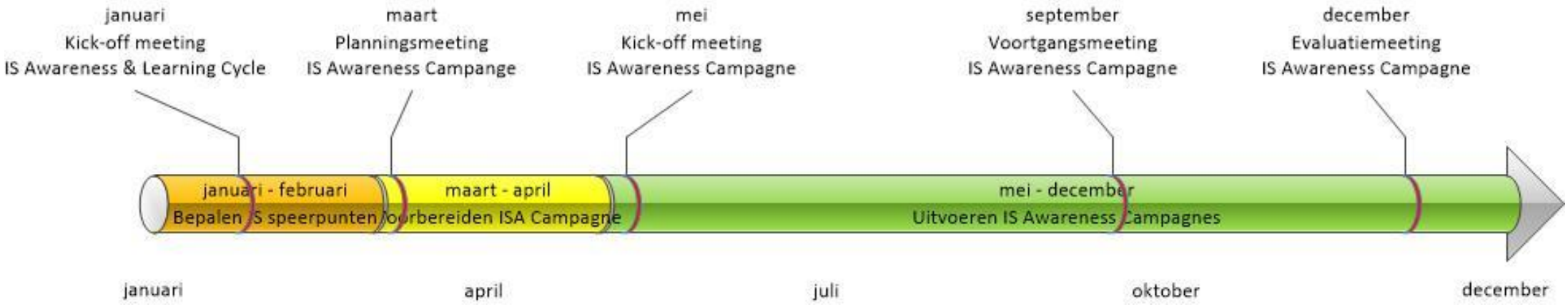
Op basis van vereisten vanuit GISP, de evaluatie van de huidige aanpak en oriëntatie omtrent “best practice” zijn de volgende uitgangspunten voor de nieuwe aanpak geformuleerd:

1. Handhaven van jaarlijkse cyclus met duidelijke fasering en start in Q1
2. Aansturing, ondersteuning en monitoring door ISO
3. Duidelijke aanspreekpunten voor BLs, dochters en ISO
4. Handhaving van onderbouwde vaststelling van campagne-speerpunten; zowel centraal (ISO) als per BL; actueel en aansprekend
5. Campagne op basis van campagneplannen per BL en centraal (ISO):
   - goedgekeurd en bewaakt door MT BL
   - grotere variatie en mogelijkheid voor doelgroepgerichte aanpak
   - meer nadruk op gedragsverbetering en positieve voorbeelden
   - meer toepassing van “Blended Learning”
   - adequate en inzichtelijke IS Awareness & Learning toolbox
6. Uitbreidbaar naar AAB-International en dochters en andere risicopartijen (risk awareness)

Process Outline - Jaarcyclus -

Activity	Description	Products (output)	Involved parties
1. Define	➢Bepalen BL-aanspreekpunten voor IS A&L ➢Bepalen IS A&L speerpunten voor campagne ➢Bepalen van evt. aanvullende IS A&L tooling	- Overzicht BL-aanspreekpunten voor IS A&L - IS A&L speerpunten voor campagne (centraal en + per BL ; evt. per doelgroep) - Overzicht aanvullend benodigde IS A&L tooling	ISO + leden IS Core team ISO + BL-aanspreekpunten ISO + BL-aanspreekpunten
2. Prepare	➢Ontwikkelen van IS A&L-campagneplannen ➢Evt. Ontwikkelen aanvullende IS A&L tooling	- Centraal IS A&L-campagneplan (ISO) - IS A&L campagneplannen per BL - Evt. aanvullende IS A&L-tooling	ISO BL-aanspreekpunten ISO + evt. BL-aanspreekpunten
3. Execute	➢Uitvoeren centraal IS A&L campagneplan ➢Uitvoeren IS A&L campagneplannen per BL	- Risicobewuste medewerkers	ISO BL-aanspreekpunten + evt. ISO (ondersteuning)
4. Evaluate	➢Evaluatie van IS A&L campagnes	- Evaluatieresultaten als input voor volgende cyclus	ISO+ BL-aanspreekpunten

Process Outline - Jaarcyclus -



Aanpak IS Awareness & Learning - Belangrijkste veranderingen -

De belangrijkste veranderingen van de nieuwe aanpak zijn:

- De jaarlijkse IS Awareness Survey vervalt (uitgevoerd door ISO i.s.m. Millward Brown)
- Door sneller voortraject meer ruimte voor campagne (start in mei)
- De campagne-speerpunten worden in belangrijke mate bepaald op basis van inzicht in gedrag en nieuwe ontwikkelingen (zie bijlage 1.1.)
- Meer ruimte voor BL-specifieke en doelgroepgericht aanpak
- Meer gericht op gedragsverbetering (o.a. Blended Learning; zie bijlage 1.2.)
- Uitgebreidere toolbox en beter gebruik van beschikbare tooling
- Ontwikkeling tooling “on demand” en niet standaard jaarlijks 3 nieuwe QLP’s en 3 nieuwe NF’s

Bijlage 1-1 - Bepalen IS speerpunten voor campagne -

- Hulpmiddel: IS Awareness & Learning thema lijst (zie toolbox)

Belangrijke vragen

- **Wat zijn specifieke verbeterpunten voor medewerkers binnen de BL?**

  B.v. onderbouwing op basis van:

  - bevindingen vorige campagne
  - signalen van het management en eigen bevindingen
  - resultaten clean desk acties
  - opgetreden security incidenten (gebruik incident rapportages, CLDB)
  - -------

- **Wat zijn nieuwe ontwikkelingen/risico's waaraan aandacht besteed moet worden?**

Implementatie bij ISO voor centrale speerpunten:

Overleg met SIM:	➔ inzicht in gerapporteerde IS incidenten + trends
Overleg met ISO/IS Strategy Policy & Arch.	➔ inzicht in nieuwe ontwikkelingen en IS-risico's
Overleg met ISO/Security Operations:	➔ inzicht in IT security incidenten en security monitoring resultaten (b.v. Data Leakage)
Overleg met Compliance	➔ inzicht in IS-related compliance incidenten
Afstemming in MT ISO	➔ feedback van/approval door MT
…….	

Blended Learning: combinatie van face-to-face onderwijs en e-learning.

Toepassing ten behoeve van IS Awareness (zie gedetailleerde beschrijving in toolbox)

- Bepalen relevant IS Awareness onderwerp
- Agendering teamsessie (b.v. 20 minuten) ter behandeling van onderwerp
- Voorbereiding door deelnemers b.v. op basis van bij het onderwerp aansluitend Quick Learning Program, News Flash, flyer, news item e.d.
- Facilitator bepaalt opzet van teamsessie, bereidt deze voor en leidt deze

Voordelen:

- Effectief voor bereiken gedragsverbetering
- Betrokkenheid leidinggevende
- Beter gebruik van beschikbare tooling (QLPs, NFs)
- Sluit aan bij CE-aanpak

Bijlage 2: Inhoud IS A&L toolbox

- **IS Awareness & Learning hulpmiddelen**
  - Huidige IS E-learnings, QLP's, NF's (zie MyL&D)
  - Flyers (zie Intranet)
  - Brochure "Gedragsregels Informatiebeveiliging"
  - Themapagina Intranet "Richtlijnen Informatiebeveiliging"
  - Handleiding voor Blended Learning aanpak
  - Standaard IS Awareness & Learning presentatie voor managers
  - Survey vragenlijst
  - Cleandesk-toolkit
  - P.M. Beschrijving mystery guest/social engineering aanpak
  - P.M. IS Awareness game

- **IS Awareness & Learning programma- management hulpmiddelen**
  - Overzicht IS Awareness & Learning-cyclus
  - Aanpak voor het bepalen van IS campagne speerpunten (incl. IS A&L themalijst)
  - Templates voor:
    - Presentatie IS campagne speerpunten (omschrijving speerpunt, doelgroep, onderbouwing)
    - IS Awareness & Learning Campagne plan
    - Proces-monitor IS Awareness & Learning

Aanpak 2007 – 2012

- Centrale aansturing, monitoring en ondersteuning door ISO
- Brede, niet doelgroep gerichte aanpak
- Papieren IS brochure in on-boarding pakket voor nieuwe medewerkers
- Jaarlijkse cyclus opgesplitst in 3 fases:
  1. Q1: Survey: meten van IS-kennis, -houding en -gedrag onder een representatieve groep random geselecteerde medewerkers
     - Uitvoering: ISO i.s.m. MillwardBrown
     - Vragenlijst in Nederlands en Engels; rule-based, jaarlijks geactualiseerd;
     - IS specifiek, summiere input van andere risicopartijen
     - scope: ABN AMRO-NL en IS-specifiek
  2. Q2, Q3: Voorbereiding IS awareness campagne:
     - rapportage en analyse van meetresultaten; bepalen aandachtspunten (centraal en per BL)
     - bepalen en ontwikkelen van aanvullende IS Awareness tooling (jaarlijks 3 nieuwe QLP's en 3 nieuwe NF's in NL en UK i.s.m. InfoSecure, flyers, nieuwsberichten, templates e.d.)
     - plannen van IS awareness campagnes per BL
  3. Q3, Q4: Uitvoeren en monitoren IS awareness campagne per BL

Evaluatie aanpak 2007 - 2012

- **Feedback vanuit klankbordgroep en medewerkers**:
  - Centrale rol van ISO t.a.v. aansturing en monitoring blijft wenselijk
  - Grotere variatie wenselijk met doelgroepgerichte aanpak
  - Elk jaar “weer” dezelfde vragen; te veel rule-based, te weinig dilemma’s
  - De behandelde onderwerpen sluiten niet altijd aan op de situatie van de medewerkers
  - Rapportage laat te lang op zich wachten
  - De resultaten zijn vaak te globaal waardoor er onvoldoende gerichte acties uit gehaald kunnen worden
  - Te weinig antwoorden op de vragen “waarom” en “hoe”
  - Met de antwoorden op de open vragen gebeurt niets
  - Te veel gericht op kennis; weinig aansprekend en weinig effect op gedragsverbetering
  - De MyL&D tooling is soms verouderd en moeilijk toegankelijk
- **Feedback vanuit ISO en andere risicopartijen**
  - Scope verbreding wenselijk: ABN AMRO International + dochters
  - Meer samenwerking met andere risicopartijen zoals SIM, Compliance, ORM, Legal
  - Meer richten op verbetering gedrag
  - De BL-campagne-plannen komen niet of moeizaam tot stand;
  - Plannen worden soms niet of gedeeltelijk uitgevoerd;
  - Geen controle/zichtbaarheid op uitvoering awareness plannen
- **Feedback van InfoSecure:**
  - De jaarlijkse cyclus met herkenbare fasering is nog steeds “best practice”
  - Met een survey kun je het feitelijke gedrag niet meten
  - De 2 E-learnings, 9 QLP’s en 9 NF’s dekken het gebied redelijk af maar verouderen wel
  - Er zijn goede ervaringen met z.g. “Blended Learning” en gebruik van positieve voorbeelden
  - Er wordt weinig gebruik gemaakt van nieuwe mogelijkheden zoals Apps en Social Media

Bijlage 4-1 Requirements

- Eisen waaraan de nieuwe aanpak dient te voldoen, zijn:

Nr.	Requirements	Origin
1.	• GISP 5.4.4. : new and current personnel must be properly informed and trained about their information security responsibilities, policies and standards and where these policies and standards are published. • Personnel Security Policy: Responsible line management, if necessary supported by Human Resources personnel, must ensure the following: ○ New ABN AMRO personnel receive a personal copy of the Information Security Guidelines as part of the induction process ○ Current ABN AMRO personnel receive a new copy of the Information Security Guidelines after revision ○ Contractors and other temporary staff receive a copy of the published Information Security Guidelines. ○ At least once a year, all personnel are explicitly reminded of the applicable information security guidelines	**AIM policy**
2.	Jaarlijkse IS awareness cyclus	**AIM policy, DNB**
3.	Een vorm van awareness-meting is noodzakelijk om accenten te kunnen leggen in de jaarlijkse awareness plannen	**M. Dekker**
4.	IS Awareness plan per Business Line	**Proj. meeting**
5	Stuurbaar per onderscheiden doelgroep	**Proj. meeting**
6.	Overzichtelijke “vitrine” van beschikbaar IS awareness hulpmiddelen; actueel, state of the art	**Proj. meeting**
7.	Vooraf duidelijkheid over (nieuwe) verplichte trainingen	**Proj. meeting**
8.	Goede centrale ondersteuning (b.v. standaard template voor IS Awareness plan, ondersteuning bij uitvoering e.d.)	**Proj. meeting**

Opmerkingen

Ad 3. Martijn vindt het niet noodzakelijk om de huidige Survey te continueren. Hij is sterk voorstander van het in de praktijk meten van de kwaliteit van informatiebeveiliging (gedrag) zoals bij “Clean Desk” gebeurt. Ook een “mystery-aanpak” lijkt hem wel wat. De meetresultaten hiervan kunnen mogelijk een goede input zijn voor awareness-plannen binnen de business Lines.

Ad 4. De scope van het awareness plan zou evt. breder kunnen zijn dan alleen IS Awareness; bv. Security (ISO, SIM, BCM) of Risk (ISO, SIM, BCM, Compliance, ORM).
In plaats van Awareness zou het plan ook Awareness & Learning genoemd kunnen worden waarbij onder “Learning” alleen de algemene security trainingen (E-learnings, QLPs, NFs) worden verstaan; en geen functie-specifieke trainingen zoals specifieke trainingen op het gebied van security administratie, Role Based Access, Cryptografie, Windows- of Netwerkbeveiliging.

Ad 5. Doelgroepen kunnen bv. zijn: nieuwe medewerkers (incl. inhuur, stagiaires e.d.); huidige medewerkers, nieuwe leidinggevenden, huidige leidinggevenden, medewerkers met klantcontact; medewerkers zonder klantcontact.

Ad 6. De “vitrine” zou zowel interne als goed bevonden externe producten kunnen inhouden en ook breder qua scope kunnen zijn (zie 4).

ABN·AMRO

Scopingsrapport
IS Awareness Strategie

Giovanni Kromosemito
19-11-2012
Versie 0.2

Inleiding

In dit document worden de kaders aangegeven voor de nieuwe IS Awareness Strategie. Awareness kan op verschillende manieren aangepakt worden. Daarom is er voor gekozen de verschillende aanpakken in kaart te brengen en deze te analyseren om zo tot de juiste kaders te komen voor de nieuwe strategie.

De volgende aanpakken zijn geanalyseerd en onderverdeeld in de volgende drie groepen:

- IS Awareness-aanpak vs. IS Training-aanpak
- IS Awareness-aanpak vs. Security Awareness-aanpak vs. Risk Awareness-aanpak
- Algemene-aanpak vs. Doelgroepgerichte-aanpak

In de hoofdstukken wordt er per onderdeel een beschrijving gegeven van de bijbehorende aanpakken en is er ook een aanbeveling te vinden.

1 IS Awareness vs. IS Training

Onderscheid in IS Awareness en IS Training is als volgt te definiëren:

- **IS Awareness** richt zich primair op de bewustmaking van medewerkers inzake risico's en maatregelen rond informatiebeveiliging. Het is erop gericht medewerkers de IT-security-risico's te laten herkennen en daarbij hun kennis, houding en gedrag te verbeteren inzake de van kracht zijnde beveiligingsregels en maatregelen.

- **IS Training** heeft een hoger ambitieniveau met als doel de medewerkers ook op specifieke deelgebieden daadwerkelijk de benodigde vaardigheden en competenties bij te brengen. Training is ook nog als volgt te onderscheiden:
    - *Algemene IS training* betreft IS trainingen die voor iedereen (of iedereen binnen een bepaalde doelgroep) van belang zijn (verder *IS Learning* genoemd)
    - *Gespecialiseerde IS training* betreft IS trainingen die ontwikkeld zijn voor specifieke functies die direct of indirect betrokken zijn met Information Security (verder *IS Specializing* genoemd)

IS Specializing wordt in deze nota verder buiten beschouwing gelaten, omdat IS specialisten de benodigde training al via hun functie krijgen. In de volgende paragrafen worden de verschillen tussen IS Awareness en IS Learning in kaart gebracht en is er vervolgens een aanbeveling gedaan.

1.1 Verschillen in de aanpak

IS Awareness	IS Learning
Betreft zaken als IS awareness survey, IS awareness game, IS awareness presentaties, IS awareness flyers, folders e.d. Verhoogt met name het risicobewustzijn ten aanzien van informatiebeveiliging met mogelijk verbetering van kennis, houding en gedrag.	Betreft zaken als E-learnings, Quick Learning Programs, interactieve trainingsessies op specifieke IS deelgebieden of voor specifieke doelgroepen. Verhoogt het risicobewustzijn ten aanzien van informatiebeveiliging en de kennis omtrent de maatregelen met mogelijk verbetering van houding en gedrag.

1.2 Aanbeveling

Uit bovenstaande vergelijking is te concluderen dat IS Awareness en IS Learning dicht bij elkaar liggen en elkaar aanvullen en versterken. Medewerkers overhalen om het juiste gedrag te vertonen gebeurt door middel van de juiste houding en voldoende kennis op gebied van informatiebeveiliging. Door een goede combinatie in te zetten van IS Awareness en Learning kan zowel de houding als de kennis van de medewerkers verhoogt worden, waardoor ook het gedrag ook wordt verbeterd.

2 IS Awareness vs. Risk Awareness

Voor een effectieve aanpak kan het nuttig zijn om het Awareness programma niet specifiek te richten op Information Security, maar breder te trekken naar bijvoorbeeld Security of nog breder Risk. In dit hoofdstuk worden deze aanpakken gedefinieerd en tegen elkaar gehouden.

In een Security Awareness-aanpak worden alle facetten van beveiliging betrokken, dus naast informatiebeveiliging ook fysieke beveiliging en Business Continuity Management (BCM).
In een Risk Awareness-aanpak worden naast de facetten van Security Awareness-aanpak ook nog Compliance en andere operationele risico's betrokken.

In de volgende paragrafen worden de voor- en nadelen van de verschillende aanpakken geïnventariseerd en wordt er op basis daarvan een aanbeveling gedaan.

2.1 Verschillen in de aanpak

Information Security Awareness	**Security / Risk Awareness**
Verhoogt kennis, houding en gedrag inzake informatiebeveiliging	Verhoogt kennis, houding gedrag inzake informatie-, fysieke beveiliging en BCM / Compliance en andere operationele risico's
Niet afhankelijk van andere partijen	Afhankelijk van andere partijen
Centraal aanstuurbaar	Diverse verantwoordelijke partijen
Focus op IS Awareness Campagne	Overzicht van alle Awareness Campagnes
Partijen hanteren verschillende aanpakken	Eenduidig geïntegreerd aanpak
Duidelijkheid in verantwoordelijke afdeling	Mogelijk onduidelijkheid over verantwoordelijke afdelingen
	Partijen kunnen elkaar ondersteunen
	Evt. overlap goed te managen

2.2 Aanbeveling

Een gecombineerde aanpak van Security / Risk Awareness heeft als voordeel dat het een eenduidig geïntegreerde aanpak betreft. Een aanpak waardoor de kennis, houding en gedrag van de medewerkers wordt verhoogd inzake informatiebeveiliging, maar ook fysieke beveiliging, BCM, Compliance en andere operationele risico's.

Echter zijn er wel zaken waar aandacht aan besteed moet worden:

- De verantwoordelijke partijen moeten bereid zijn om samen te werken aan de gecombineerde aanpak (**BCM**, **Compliance**, **ISO**, **Operational Risk** en **SIM**)
- Doordat elke partij een eigen aanpak heeft, kan het wat moeilijkheden opleveren om tot een eenduidig aanpak te komen
- In de gecombineerde aanpak moet er een duidelijk onderscheid zijn tussen de verschillende onderdelen en welke partijen daarvoor verantwoordelijk zijn

Indien er geen support is voor een samenwerking dan is het raadzaam om de nieuwe strategie te richten op de Information Security-aanpak. Tevens kan de strategie wel zo ingericht worden dat het uitbreidbaar is naar een Security / Risk-aanpak.

3 Algemene aanpak vs. Doelgroepgerichte aanpak

Een doelgroepgerichte aanpak voor de nieuwe strategie kan de effectiviteit verhogen. In de onderstaande tabel zijn de verschillen aangeduid tussen een algemene aanpak en een doelgroepgerichte aanpak.

3.1 Verschillen in de aanpak

Algemeen	Doelgroepgericht
Voor iedereen inzetbaar	Gericht op bepaalde groepen
Standaard aanpak	Wordt specifiek gemaakt voor elke groep
Minder betrokkenheid bij medewerkers	Meer betrokkenheid bij de medewerkers
Ontwikkelen kost minder tijd	Ontwikkelen voor de verschillende doelgroepen kost meer tijd

3.2 Aanbeveling

Het onderscheiden van specifieke doelgroepen kan de effectiviteit van een IS Awareness aanpak verhogen. Om deze doelgroepgerichte aanpak op een goede wijze in te voeren moet wel aan bepaalde voorwaarden worden voldaan:

- Duidelijke definitie van doelgroepen
- Duidelijk aangeven van de aanpak per doelgroep inclusief de voor de doelgroep relevante producten en diensten

Voor de strategie zijn de onderstaande doelgroepen gedefinieerd:

- Nieuwe medewerkers met klantcontact
- Nieuwe medewerkers zonder klantcontact
- Huidige medewerkers met klantcontact
- Huidige medewerkers zonder klantcontact
- Nieuwe managers van extern
- Nieuwe managers van intern
- Huidige managers
- Risico gevoelige functies

Outline

Annual Information Security Awareness Process

Version 0.2
February 06, 2013
ISO | ISRM NL

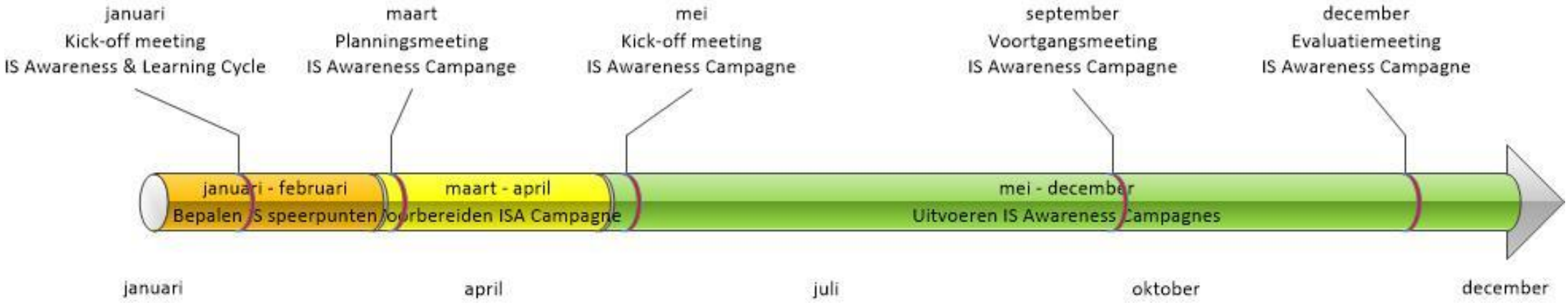
Policies

# AIM	Title	Description
108-49-00	Group Information Security Policy	The Group Information Security Policy (GISP) is the overarching information security policy document that provides management direction and support for the implementation of information security within ABN AMRO. GISP policy rule 5.4.4. specifically applies to IS Awareness and Learning.
108-49-29	Personnel Security Policy	The purpose of this policy is to specify the requirements for acceptable personnel behaviour in respect of information security, and to reduce human-related information security risks.
108-30-25	Employee Handbook Policy	The objective(s) of this policy is to ensure that during the on boarding process, new employees are made aware of general employment conditions, HR policies & procedures, and codes of conduct. One of the codes of conduct focuses on information security.

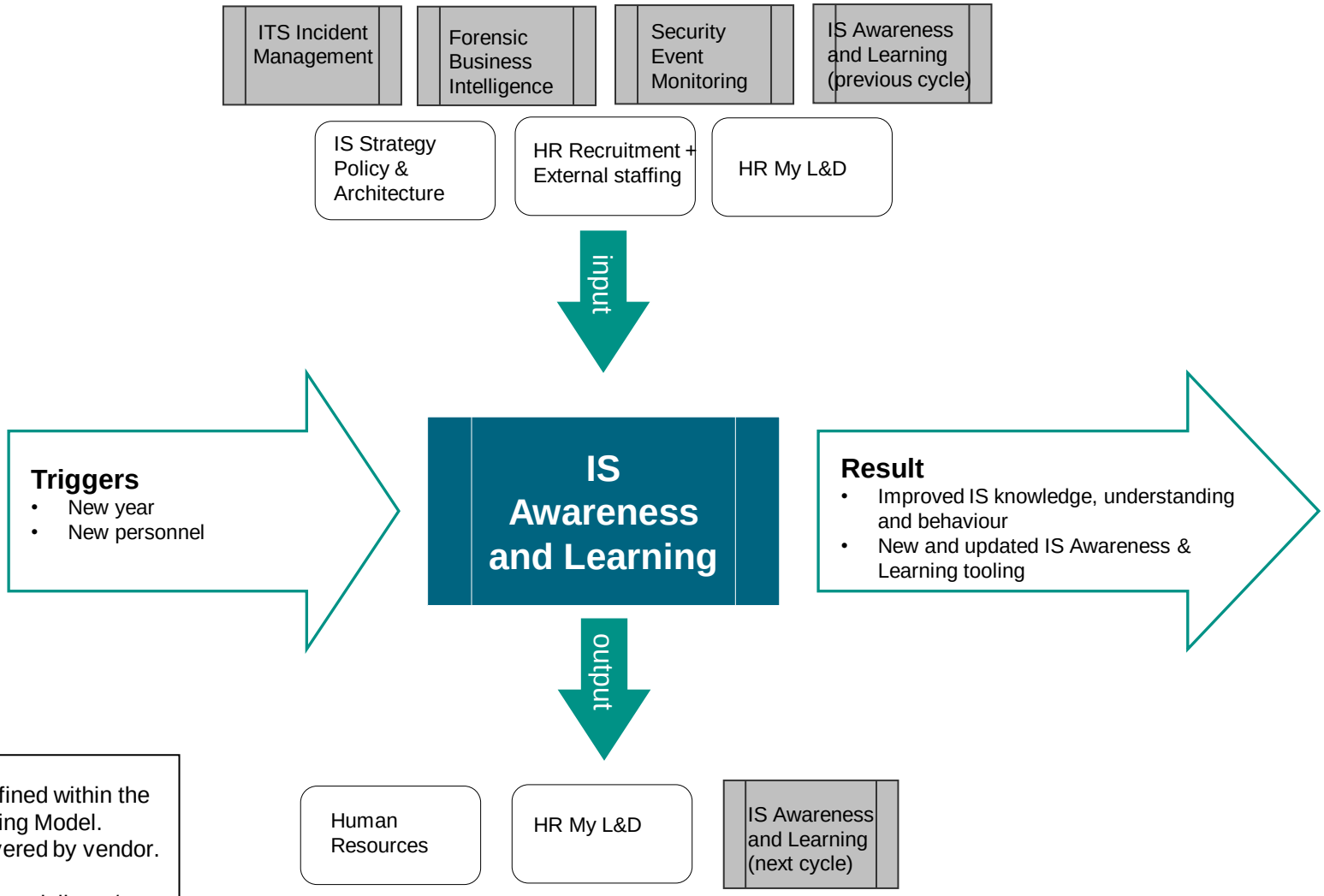
Process Description

Definition	Process for organizing, executing and evaluating an annual IS awareness & learning campaign to keep knowledge, attitude and behaviour regarding information security among ABN AMRO staff at an acceptable level
Objectives	Achieve responsible and secure behaviour of staff
In Scope	All personnel working with NL-Business Lines; including ABN AMRO employees, contractors, third party staff and other staff with access to ABN AMRO-related information and information systems.
Out of Scope	ABN AMRO international and subsidiaries
Main Products	➢Improved knowledge, understanding and behaviour re. information security among ABNAMRO-NL staff ➢New and updated IS Awareness & Learning tooling ➢Experiences and input for themes for next campaign

Process Timeline



Context Diagram



Context Diagram - Interfaces

	Process/Service	Product
Input	IT Security Incident Management	Trends in IT related IS incidents
	Forensics Business Intelligence	Trends in IS incidents with criminal background
	Security Event Monitoring	Findings from security monitoring (e.g. re. data leakage)
	IS Strategy, Policy & Architecture	New developments in IS risks and measures
	HR recruitment + External staffing	New personnel
	HR My Learning & Development	E-learning's, QLP's and NF's
	IS Awareness & Learning cycle (previous)	Process improvements and input for themes
Output	Human Resources	Improved IS knowledge, attitude and behavior
	HR My Learning & Development	New and updated E-learnings, QLP's and NF's
	IS Awareness & Learning cycle (next)	Process improvements and input for new themes

Activities and Products

Activity	Description	Products (output)
1. Define	➔Assign contacts responsible for IS A&L within each LoB ➔Determine IS A&L themes for the next campaign ➔Determine if (and which) additional IS A&L tooling is needed	➔Overview of responsible contacts for IS A&L ➔Overview of IS A&L themes for the next campaign ➔Requirements for new/to be updated IS A&L tooling
2. Prepare	➔Develop plans for the IS A&L campaign ➔Develop new or update current IS A&L tooling (if needed)	➔Plan for IS A&L campaign at ABN AMRO level (ISO) ➔Plans for IS A&L campaigns per LoB ➔New or updated IS A&L tooling (if needed)
3. Execute	➔ Execute plan for IS A&L campaign at ABN AMRO level ➔ Execute plans for IS A&L campaigns per LoB	➔Improved IS knowledge, attitude and behaviour of ABN AMRO management and staff
4. Evaluate	➔Evaluate IS A&L campaigns	➔ Process improvements and input for themes for the next IS A&L process cycle

Product Responsibility Matrix

Products (output)	Responsible	Accountable	Supporting	Consulted	Informed
Overview of responsible contacts for IS A&L per LoB	ISO-A&L Process Manager	BISO's/leden IS Core team			IS A&L contacts LoB's ISO A&L Process Owner
Overview of IS A&L themes for the next campaign	ISO-A&L Process Manager	ISO A&L Process Owner		ISO, SIM, Compliance, IS A&L contacts LoB's	MT LoB's ISO A&L Process Owner
Requirements for new/to be updated IS A&L tooling	ISO-A&L Process Manager	ISO A&L Process Owner	IS A&L contacts LoB's	IS A&L contacts LoB's	ISO A&L Process Owner
Plan for IS A&L campaign at ABN AMRO level (ISO)	ISO-A&L Process Manager	ISO A&L Process Owner		IS A&L contacts LoB's	ISO A&L Process Owner IS A&L contacts LoB's
Plans for IS A&L campaigns per LoB	IS A&L contacts LoB's	MT LoB's	ISO-A&L Process Manager	ISO-A&L Process Manager	MT LoB (plan) Risk Cie; IS Core team (dashboard)
New or updated IS A&L tooling (if needed)	ISO A&L Process Manager	ISO A&L Process Owner	IS A&L contacts LoB's	IS A&L contacts LoB's HR My L&D	HR My L&D Staff
Improved IS knowledge, attitude and behavior of ABN AMRO management and staff	IS A&L contacts LoB management LoB staff	MT LoB's	ISO-A&L Process Manager	ISO-A&L Process Manager	MT LoB (execution of plan) Risk Cie; IS Core team (dashboard)
Process improvements and input for themes for the next IS A&L process cycle	ISO-A&L Process Manager	ISO A&L Process Owner		IS A&L contacts LoB's	ISO A&L Process Owner

Process Assets

Job Aids	See the overview of the IS Awareness & Learning toolkit. This toolkit includes: - Process Support tooling for ISO - Process Support Tooling for the LoB-contacts - IS Awareness & Learning tooling
Methods	n.a.

Key Controls

No.	Key Control	Remarks
1.	New ABN AMRO employees, contractors, third party staff and other temporaries must be properly informed of their IS responsibilities and the applicable IS policies, standards and guidelines as part of the introduction process.	HR must ensure that the IS code of conduct (Gedragsregels Informatiebeveiliging) is part of the introduction packet that is handed out to new staff (including contractors)
2.	Current ABN AMRO employees, contractors and third party staff must be annually reminded of their IS responsibilities and the applicable IS policies, standards and guidelines by or on behalf of responsible management.	This must be ensured by the execution of the annual IS Awareness & Learning cycle
3.		
4.		
5.		

Process Governance

Version	Date	Commitment of	Name	Department	Date MT
1.0		Business Process Owner	Martijn Dekker/Ron Bieshaar	AAB / ISO / ISRM NL	
		Business Process Manager(s)	Cock Frijters/Mart Perrels	AAB / ISO / ISRM NL	

Participants

Participants	Representative of
Joop Zomer	ISRM NL
Giovanni Kromosemito	ISRM NL
Bert Reemer	BS / FM
Jolanda Ciapa	COO / C&MB / CC
Eva Maas	SIM
Michiel Vreugdenburg	COO / PB Int.

Version Log

Version	Date	Edited by	Reason
0.1	1-2-2013	Giovanni Kromosemito	New draft inline with process layout and New IS Awareness & Learning Strategy
0.2	6-2-2013	Joop Zomer	Review
1.0			

Appendix A – Terminology

Used term	Description
IS A&L	Information Security Awareness & Learning
Quick Learning Program (QLP)	Short e-learning modules
Newsflashes (NFs)	Very short informative movies

Toolbox
IS Awareness & Learning

Giovanni Kromosemito
25-03-2013
Versie 1.0

Inleiding

De IS Awareness & Learning Toolbox bestaat uit de hulpmiddelen die geselecteerd zijn om beschikbaar te stellen voor de aanspreekpunten van de business lines om in te zetten voor de campagnes.

Omdat ik niet aan alle hulpmiddelen een bijdrage heb geleverd, heb ik alleen de hulpmiddelen aan deze toolbox toegevoegd waar ik betrokken was geweest bij de selectie. Daarnaast zijn de ook de resultaten van het onderzoek naar de leveranciers en producten/diensten hierin opgenomen.

De volgende onderdelen zij in deze toolbox opgenomen:

- Beschrijving van de onderdelen van de Toolbox
- Onderzoek naar leveranciers en producten/diensten
- Information Security thema's
- Handleiding Blended Learning
- Handleiding Social Engineering
- Instructie voor Awareness Game

Vitrine

In deze vitrine is een overzicht te vinden van de beschikbare IS Awareness hulpmiddelen met een korte toelichting, categorie aanduiding, waar ze te vinden zijn en hoe het gebruikt kan worden.

E-learning

Is een basis training voor alle medewerkers over informatiebeveiliging met daarin film clips, interactieve oefeningen en test jezelf elementen.

Categorie: Learning

Waar te vinden
Er zijn 2 e-learnings beschikbaar (zowel Nederlands- als Engelstalig) in My Learning & Development onder Catalogus, Informatiebeveiliging.

- Basisprogramma Gouden Regels (verplicht voor nieuwe medewerkers)
  In dit programma leer je hoe belangrijk het is dat je veilig omgaat met informatie en informatiedragers van ABN AMRO.
- Informatiebeveiliging door leidinggevenden
  Deze e-learning is er een in de reeks van e-learnings op het gebied van Informatiebeveiliging speciaal met de focus op de rol van de Leidinggevenden.

Quick Learning Programma's (QLP)

Zijn korte e-learning modules met een unieke combinatie van film clips, training materiaal, interactieve oefeningen en een zelftest. Deze bewustwordingsprogramma's duren 3-5 minuten.

Categorie: Learning

Waar te vinden:
Er zijn 8 QLP's beschikbaar (zowel Nederlands- als Engelstalig) in My Learning & Development onder Catalogus, Informatiebeveiliging.

- Bescherming van klanteninformatie
- Flexwerken
- Identiteitsdiefstal via Social Media
- Juist gebruik van e-mail
- Melden van security incidenten
- Omgaan met logingegevens
- Toepassen van Informatie Classificatie
- Veilig gebruik van Internet

NewsFlashes (NFs)

Zijn korte 2 tot 5 minuten durende video modules opgenomen in een journaal setting zorgen ervoor dat medewerkersop de hoogte blijven van het laatste nieuws op informatiebeveiliging binnen uw bedrijf.

Categorie: Learning

Waar te vinden:
Er zijn 9 NewsFlashes beschikbaar (zowel Nederlands- als Engelstalig) in My Learning & Development onder Catalogus, Informatiebeveiliging.

- Integer omgaan met vertrouwelijke informatie
- Risico's bij het gebruik van mobiele apparaten
- Sociale Netwerken
- Social Engineering
- Veilig gebruik eigen apparatuur
- Veilig werken in openbare ruimtes
- Werken buiten de bank
- Werken met derde partijen
- Werkomgeving opgeruimd

Flyers Informatiebeveiliging

Er zijn diverse flyers beschikbaar waarin een specifiek informatiebeveiligingsonderwerp wordt toegelicht. De flyers kunnen worden uitgedeeld aan nieuwe medewerkers of kunnen als input dienen voor het afdelingsoverleg.

Categorie: Learning

Waar te vinden
Er zijn 4 NewsFlashes beschikbaar (zowel Nederlands- als Engelstalig) onder IT & Faciliteiten, Informatiebeveiliging.

- Veilig gebruik van vertrouwelijke informatie buiten de bank
- Richtlijnen voor het gebruik van Bluetooth (apparatuur)
- Social Engineering
- Veilig werken met een laptop

Survey

Survey's kunnen ingezet worden om op basis van een vragenlijst te meten wat de niveau van kennis, houding en gedrag is van de medewerkers. Hiervoor kan er externe (Millward Brown) en interne (NetQ) survey hulpmiddelen ingezet worden.

Categorie: Meten

Awareness Game

Het is algemeen bekend dat spelenderwijs leren zeer effectief is. Het informeren van personeel via een Awareness Game zal daarom snel resultaat boeken. Medewerkers spelen op individueel niveau de game.

Categorie: Meting

Waar te vinden
De Awareness Game wordt aangeboden door Vest.

Social Engineering-toolbox

Bestaat uit “mystery guest”-acties die ingezet kunnen worden om het feitelijke gedrag te meten van medewerkers die geconfronteerd worden met Social Engineering. Acties die mogelijk zijn:

- Mystery Guest
- Mystery Caller
- Mystery E-mailer
- Mystery Website
- Mystery Filmer

Categorie: Meting

Waar te vinden
Mystery Guest-acties worden door verschillende vendors als dienstverlening geleverd.

Clean office programma

ISO heeft een clean office programma ontwikkeld waarin een leidinggevende/medewerker op zijn afdeling de werkplekken van de collega’s langsloopt en te controleren op de aandachtspunten van clean desk. Collega’s krijgen een ✓- of ✗-briefje als hun werkplek niet “clean” is.

Categorie: Meting

Waar te vinden
Op aanvraag bij ISO.Awareness@nl.abnamro.com kan er een draaiboek geleverd worden met beschrijving van de procedure en de aandachtspunten waarop gecontroleerd moet worden.

Risicostickers

Zijn stickers die risico’s aangeven die zich voor kunnen doen in een situatie (bv. een bureau die niet “clean” is)

Categorie: Learning

Waar te vinden

Op aanvraag bij ISO.Awareness@nl.abnamro.com kan er een template sticker worden geleverd met voorbeelden van veel voorkomende risico’s.

Hoe te gebruiken

Bij het Clean office programma wordt er momenteel twee kaarten gebruikt om aan te duiden of een bureau “clean”” is, de prima- en jammerkaart. De risicostickers is een goede vervanging van deze kaarten, omdat het wijst op de risico’s die zich voor kunnen doen. Deze sticker geeft ook niet aan dat men in de “fout”zit, waardoor het meer positief kan worden ervaren.

Blended Learning

Is een combinatie van online en offline leren. Door groepsgewijs (team/afdeling) de stof van een e-learning (QLP/NF) te behandelen, is kans groot dat de stof beter aanslaat.

Categorie: Learning

Waar te vinden

Op aanvraag bij ISO.Awareness@nl.abnamro.com kan er een SOP geleverd worden met instructies voor het uitvoeren van een Blended Learning – sessie.

Hoe te gebruiken

In de SOP staat instructies voor het combineren van een e-learning met een sessie waarin de stof van de e-learning behandeld wordt.

ISO Presentatie

In deze presentatie gaat een Security specialist in op de hoe en waarom van een selectie van gedragsregels van informatiebeveiliging.

Categorie: Learning

Waar te vinden

Op aanvraag bij ISO.Awareness@nl.abnamro.com kan er door een Security specialist een presentatie worden verzorgd.

ISO Online Brochure

In de brochure is er meer informatie te vinden over verschillende informatiebeveiligingsonderwerpen.

Categorie: Learning

Waar te vinden

Intranet > IT & Faciliteiten > Informatiebeveiliging & Operationele Risico’s

Hoe te gebruiken

Medewerkers kunnen hiernaar verwezen worden voor vragen of onduidelijkheden over informatiebeveiligingsonderwerpen

Vendors

De matrix voor Leveranciers geeft een beeld over leveranciers die IS Awareness producten/diensten leveren. Inzicht wordt gegeven in:

- Beschikbare (of in ontwikkeling zijnde) producten/diensten gerangschikt per categorie;
- De hoeveelheid klanten die zij aan kunnen leveren (referenties);
- De mate van innovatie in de producten/diensten;
- De indicatie van de kosten.

Deze gegevens zijn gebaseerd op bezoek, analyse van de website en gesprek of zijn een eigen inschatting.

Leveranciers / Beoordelingscriteria	InfoSecure	LBVD	Vest / Trustforce	iComply	VKA	Store Support	Sogeti	Trust in People	Pinewood	Madison Gurkha
Producten/diensten	5	4	2	2	6	1	1	2	1	1
Referenties	+++	?	+++	+++	+++	++	?	?	+	+
Innovatieve producten/diensten	+	+	+	-	+	-	-	-	-	-
Kosten	Wordt nog aangevuld									

Leveranciers	Achtergrond en toegepaste aanpakken
InfoSecure	http://www.infosecuregroup.nl/ Contactpersoon: Wilbert Pijnenburg (*Director Benelux*) InfoSecure: bewustwordingstrainingen op het gebied van informatiebeveiliging. InfoSecure is een internationale speler die e-learning programma's op het gebied van Informatiebeveiliging, Compliance en Business Continuity Management levert. Deze programma's vergroten de bewustwording in allerlei organisaties in meer dan 90 landen.
LBVD	http://www.lbvd.nl/diensten/verbeteren-beveiliging/bewustzijnprogramma-s.html Contactpersoon: Ronald Valk (*Product Specialist Awareness* via Frans Woelders) U kunt bij ons terecht voor een uiterst compleet dienstenpakket dat zich uitstrekt over de facetten Organisatie, Techniek en Mens. Daarbij helpen we u in de meest brede zin: vanaf het in beeld brengen van de huidige situatie tot en met het verankeren van een verbeterd beveiligingsniveau. In alle diensten die we bieden keert onze eigenzinnige visie op informatiebeveiliging terug. Op basis van deze fases hebben wij onze diensten onderverdeeld in drie groepen: Bepalen van informatiebeveiliging, Verbeteren van informatiebeveiliging en Behouden van informatiebeveiliging.

VKA	http://www.vka.nl/ Contactpersoon: Steven Debets (*Managing Consultant*) Verdonck, Klooster & Associates onderscheidt zich door inhoudelijke kennis en oog voor resultaat te combineren met uitgelezen kennis van de sector en gevoel voor de menselijke factor. Door het bundelen van kennis wordt een inspirerende omgeving gecreëerd, waarbinnen collega's elkaar stimuleren en aanvullen.
Vest/ Trustforce	http://www.vest.nl/Oplossingen/SecurityAwareness/tabid/77/language/nl-NL/Default.aspx Contactpersoon: Hildo Krop (*Principal Consultant*) Vest legt zich sinds 2002 volledig toe op informatiebeveiliging voor organisaties. Haar gecertificeerde adviseurs werken onafhankelijk, effectief en uiterst pragmatisch. Vest weet sneller tot betere oplossingen te komen, doordat zij beschikt over een team waarbinnen alle benodigde disciplines verenigd zijn. Vest onderscheidt binnen haar organisatie een viertal vakgebieden waarbinnen de kennis en ervaring wordt gebundeld, ontwikkeld en voor hergebruik aangewend: Audit & Forensics, Security Management, Security Architectuur, Continuity
iComply	https://www.icomply.nl/diensten.html Contactpersoon: *N.t.b.* De iComply dienstverlening is gespecialiseerd in het inzicht geven in security en compliance normen. Met iComply haalt u alle specialistische expertise in huis om uw security en compliance normen te implementeren, te onderhouden en te monitoren op zowel organisatorisch als technisch niveau.

Beschikbare (of in ontwikkeling zijnde) producten en/of diensten

Elke leverancier levert verschillende type producten/diensten. Elke product/dienst heeft zo weer bepaalde doeleinden en is gemaakt voor bepaalde doelgroepen. In het onderstaande overzicht zijn de leveranciers te vinden met de aangeboden producten/diensten en een beschrijving daarvan.

Leveranciers	Producten / diensten
InfoSecure	Huidige partner voor ontwikkelen **E-learnings (Basis Introductie Programma's en Special Topics)**, **QLPs**, **NewsFlashes** op het gebied van Informatiebeveiliging. *Nieuwe ontwikkelingen*: – **Security Awareness Magazine**: die meer nadruk legt op risico besef dan op pure kennis – **Simulaties**: voor het herkennen van betrouwbare e-mail en webpagina's in het kader van Cybersecurity – **IT Professionals** – speciale programma voor IT professionals – **Security Game**: Serious Gaming gebaseerd op Cluedo waarbij je als speler op zoek gaat naar hoe informatie binnen de afdeling is gelekt

	– **Security Awareness App**: die op een frequente manier cases oid neerlegt bij medewerkers – **Social Media voor Kids** van medewerkers. Verbeteringen in privé gedrag zullen ook uitwerking hebben op de werkvloer. – **Social Engineering Toolbox** o *Mystery Guest* o *Mystery Caller* o *Mystery E-mailer* o *Mystery Website* o *Mystery Filmer*
LBVD	– Prikkelen o **Mystery Guest** o **Telefonische Mystery Guest** o **Hackaanval zowel van buiten als van binnen** o **Nep-virus** o **Phishing e-mail** o **Wachtwoordenval** – Uitdagen o **Security Quiz** De Security Quiz is een prijsvraag waarbij een beloning plaatsvindt voor het geven van de goede antwoorden. o **Appelflappen-race (Ontmasker de Mystery Guest)** De appelflappen-race is een variant van de MysteryGuest-actie. Ze is er in deze vorm op gericht om ontdekt en aangesproken te worden. Iedereen die de MysteryGuest durft te vragen wie hij/zij is en wat hij/zij komt doen krijgt direct iets lekkers voor bij de koffie of thee! o **Koffie-teaser** Bij de koffie-automaat (of een andere plek waar medewerkers zich dagelijks minimaal een keer ophouden) komen de resultaten van een gehouden werkplek-inspectie versluierd te hangen, met een beloning voor degene die er achter komt wat het cryptische diagram te betekenen heeft. – Informeren en enthousiasmeren o **Demo-hack** o **Ronde-tafelsessies** o **Workshops (diverse doelgroepen)** o **Communicatie-uitingen (posters, flyers, intranet, etc.)** o **Give-away's** o **Themabijeenkomsten** o **Enquête** *Zie LBVD Leaflet Awareness Campagne voor toelichting van de Awareness Acties.*

Vest/ Trustforce	– **Awareness Campagne** beschikt over een uitgebreid arsenaal aan interactieve middelen om het bewustzijn van de medewerker te prikkelen, uit te dagen en te stimuleren. Door begrip en betrokkenheid van uw medewerkers, helpt Vest op uiteenlopende wijze met het ontwikkelen van betere, gevoeligere zintuigen en de juiste mindset bij medewerkers en het bereiken van een hogere effectiviteit van uw genomen maatregelen – **Awareness Game** Het security awareness niveau onder medewerkers is in veel organisaties lager dan gewenst. Het incidenteel verspreiden van posters of het geven van workshops heeft te weinig effect. De materie beklijft niet. Vest speelt hier op in met haar security awareness game. Verhoog spelenderwijs awareness in uw organisatie.
VKA	– **Bordspel "A Heart Effort"** Het bordspel is ontwikkeld om deelnemers met elkaar te laten discussiëren over allerlei mogelijke onderwerpen, die te maken hebben met hun werk en de organisatie. – **Interactieve workshops** In deze workshops wordt meningsvorming gestimuleerd waarmee zicht ontstaat op de weerstand tegen het invoeren van bepaalde maatregelen, maar ook veranderbereidheid om bepaalde maatregelen versneld in te voeren. – **Social Engineering** VKA adviseurs hebben ervaring met diverse social engineeringstechnieken. Van telefonische social engineering tot en met het indringen bij een organisatie als 'mystery guest'.. – **Masterclasses** VKA Masterclasses zijn kennissessies van twee uur tot een dag waarin onze adviseurs hun kennis en kunde en praktijkervaringen met u delen. – **Implementeren van e-learning** Een e-learning omgeving wordt bij veel organisaties ingezet om het kennisniveau van medewerkers voor meerdere onderwerpen te verhogen. – **Bedrijfsfilms** Het inzetten van een film is een krachtig instrument om het bewustwordingsniveau te verhogen. – **Training informatiebeveiliging** Het maatwerkopleidingsprogramma wordt gericht op kennisoverdracht en het veranderen van gedrag van medewerkers. – **Effectiviteitsmeting bewustwordingsactiviteiten** VKA kan een nulmeting uitvoeren naar het huidige bewustwordingsniveau van medewerkers van de ABN Amro, gevolgd door periodieke metingen.
iComply	Door het inzetten van een **Mystery Guest** wordt een goed beeld verkregen van het bewustzijnsniveau van de medewerkers. De iComply Mystery Guest test (volgens afgesproken scenario) uw beveiliging door onopgemerkt binnen te komen en zich toegang te verschaffen tot kritieke ruimten en vertrouwelijke informatie. Naast het inzetten van een Mystery Guest kunnen met behulp van **E-learning software** uw medewerkers getest worden op kennis van de regelgeving. In de E-learning software zijn testen opgenomen waarmee u voor verschillende normen uw medewerkers kunt testen.

Awareness & Learning thema's informatiebeveiliging. V2

Onderstaand wordt een overzicht gegeven van thema's die geschikt zijn voor behandeling in z.g. Blended Learning sessies:

1. voorbereiding van thema door teammedewerkers m.b.v. QLP, NF, flyer, thema op themapagina, newsitem op intranet, internet of in andere media;
2. bespreking van thema in teamsessie:

- instruerend: wat, waarom, hoe?
- probleem oplossend: wat is er gebeurd, wat was de oorzaak, hoe kunnen we dat voorkomen?

Thema	Vraagstelling voor themasessie	Hulpmiddelen	Vorm
IB verantwoorde-lijkheden LG	Wat zijn de verantwoordelijkheden van de leidinggevende op het gebied van IB. Is de leidinggevende zich hiervan bewust en worden ze goed ingevuld. Waar kan het beter?	Informatiebeveiliging door leidinggevenden	E-learning
IB verantwoorde-lijkheden MW	Wat zijn de verantwoordelijkheden van de medewerker op het gebied van IB. Is de medewerker zich hiervan bewust en worden ze goed ingevuld. Waar kan het beter?	Basisopleiding uitgebreid Richtlijnen Basisprogramma Gouden Regels Gedragsregels Informatiebeveiliging	E-learning Brochure
Veilige omgang met vertrouwelijke bankinformatie	Wat verstaan we onder vertrouwelijke bankinformatie. Hoe moeten we daar mee omgaan en waarom? Welke maatregelen kunnen we nemen bv. t.a.v.: • zichtbaar maken dat het om vertrouwelijke informatie gaat; hoe lang en voor wie? • opslag, kopiëren, uitwisseling, printen, vernietigen. Gaan we hier goed mee om. Wat kan beter?	Integer omgaan met vertrouwelijke informatie (NL + ENG) Toepassen van Informatie Classificatie (NL + ENG) Bescherming van klanteninformatie (NL + ENG)	NF QLP QLP
Veilig gebruik van login middelen	Wat zijn de login middelen (UID, wachtwoord, PIN, M-pas e.d.). Waartoe dienen ze? Hoe moet je er mee omgaan en waarom? Aan wat voor eisen moet een sterk wachtwoord voldoen en hoe kun je zo'n wachtwoord kiezen? Hoe kun je het best je wachtwoorden beheren; kun je hiervoor apps gebruiken en zo ja welke? Wat behelst de SSO-oplossing onder Worksquare?	Omgaan met logingegevens (NL + ENG)	QLP
Standaard IT oplossingen	Welke standaard-IT oplossingen zijn beschikbaar voor eindgebruikers (standaard desktop, laptop, Worksquare@home, Worksquare Mobility App, USB-stick, privacy filter)? Waarvoor dienen ze c.q. tegen welke risico's beveiligen ze en wanneer moeten we ze gebruiken. Hoe, waar kan ik ze krijgen.	Veilig werken met een laptop	Flyer

Secure mobile working/HNW	Welke vormen van mobile working onderscheiden we (flexplekken op kantoor, thuiswerken en werken in publieke ruimtes). Wat zijn de specifieke risico's en maatregelen. Waartoe dienen deze maatregelen en passen we ze toe? Zijn we ons bewust van de risico's en maatregelen?	Werken buiten de bank (NL + ENG) Veilig werken in openbare ruimtes (NL + ENG) Flexwerken (NL + ENG) Veilig gebruik van vertrouwelijke informatie buiten de bank (NL + ENG)	NF NF QLP Flyer
Clean desk (incl. office, screen)	Wat zijn de regels t.a.v. clean desk? Waarom zijn deze regels er? Passen we ze goed toe en spreken we elkaar aan op overtredingen? Waar kan het beter?	Clear office (NL + ENG)	NF
Veilig gebruik van draagbare gegevensdragers	Om wat voor gegevensdragers gaat het (laptops, USB-sticks, smartphones, tablets e.d.). Wat zijn de specifieke risico's en welke maatregelen kunnen we zelf nemen? Waar kan het beter?	Risico's bij gebruik van mobiele apparaten	NF
Veilig gebruik van privé devices	Om wat voor devices gaat het (PC, laptop, smartphone, tablet e.d.). Hoe en in welke mate kunnen we die veilig gebruiken voor bankwerkzaamheden. Waarom moet je, buiten de door de bank geboden oplossingen, zelf nooit bankgegevens opslaan op privé devices?	Veilig gebruik van eigen apparatuur (NL + ENG)	NF
Acceptabel gebruik van internet	Welke sites/internetcontent mag je via het netwerk van de bank niet benaderen en waarom niet? Hoe kan misbruik worden geconstateerd en wat kunnen de gevolgen zijn, zowel voor de bank als voor jezelf?	Veilig gebruik van internet (NL + ENG)	QLP
Veilig gebruik van internet	Welke gevaren zijn er op internet en hoe kunnen die van invloed zijn op werk en privé situatie? Welke maatregelen kun je nemen? Wat zijn de Do's en Don'ts?	Veilig gebruik van internet (NL + ENG)	QLP
Data Leakage	Via welke kanalen kan vertrouwelijke data "weglekken" naar buiten. Hoe kan dit weglekken worden geconstateerd en wat kunnen de gevolgen zijn, zowel voor de bank als voor jezelf? Zijn we ons hiervan voldoende bewust?		
Veilig gebruik van e-mail	Wat is "boosaardige" mail (SPAM, virussen, phishing mails e.d.)? Hoe kun je ze herkennen en wat moet je ermee doen? Welke extra maatregelen kun je nemen indien je vertrouwelijke mail naar iemand anders intern dan wel extern verstuurt? we	Juist gebruik van e-mail (NL + ENG)	QLP
Social Engineering	Wat is social engineering en hoe wordt het door criminelen gebruikt (persoonlijk contact, via telefoon, e-mail, social media). Zijn we hierop voldoende voorbereid en alert? Wat moet je doen als je slachtoffer bent van Social Engineering? Wat kunnen we doen en waar kan het beter?	Social Engineering Social Engineering	Flyer NF
Social Media/Social Networking	Wat verstaan we onder Social Media en wat zijn de risico's? Hoe moeten we hiermee omgaan c.q. wat zijn voorbeelden van slecht en goed gedrag? Ben je bekend met de richtlijnen t.a.v. Social Media. Wat kan de impact zijn van slecht gebruik zowel voor de bank als voor jezelf?	Sociale Netwerken (NL + ENG) Identiteitsdiefstal via Sociale Media	NF QLP

Werken “in the cloud”	Wat zijn de risico’s van het werken met en opslaan van bankgegevens “in the cloud”. Welke regels gelden en waarom? Gaan we daar goed mee om? Wat kan beter?		
Rapporteren van beveiligingsincidenten of -lekken	Wat zijn beveiligingsincidenten en -lekken en welke worden onderscheiden? (criminele achtergrond, IT gerelateerd, vernieling/diefstal, organisatiegerelateerde, compliance gerelateerd, anoniem melden). Wanneer, waar en hoe moet ik deze melden. Waarom is het belangrijk om incidenten en –lekken snel te melden.	Melden van security incidenten (NL + ENG)	QLP
Bepaald intern of extern opgetreden beveiligingsincident	Wat was het incident precies? Hoe kon het ontstaan en wat was de oorzaak. Kan het bij ons ook gebeuren en wat kunnen we doen om dit te voorkomen of de kans hierop te verkleinen?	Melden van incidenten (NL + ENG)	QLP

Handleiding
Blended Learning

31 January 2013
ISO Awareness

Blended Learning

Blended Learning is een geïntegreerde combinatie van het traditionele onderwijs (college of workshop vorm) en online onderwijs (e-learning e.d.).

Blended Learning-sessie

Dat is dus een sessie waarin je Blended Learning toepast door een vergadering te voeren over een thema die voorbereid wordt middels beschikbare e-learning middelen zoals de verschillende Quick Learning Programs of NewsFlashes op My Learning & Development.

Een blended learning sessie kan in verschillende vormen uitgevoerd worden. Hieronder staan er twee voorbeelden:

- Informatieve vergadering

  In deze vorm staat het uitwisselen van ideeën en kennis centraal.

- Brainstorm vergadering (KAIZEN-sessie)

  In deze vorm staat het nadenken over en zoeken naar verschillende oplossingen voor een bepaald probleem centraal. Als thema voor een dergelijke vergadering kan bijv. een recentelijk voorgekomen incident gebruikt worden.

Het doel van een dergelijke sessie is dat de deelnemers de nodige kennis opdoen en samen als een team een vertaalslag maken naar hun werkzaamheden.

Vóór een Blended Learning-sessie…

Als voorzitter van een sessie moeten de volgende stappen vooraf genomen worden:

1. Kiezen van een thema voor de sessie
2. Bijbehorende middelen kiezen voor de sessie
3. De thema en middelen aanleveren ter voorbereiding aan de deelnemers van de sessie

Een thema kan je kiezen door te kijken naar de:

- Aandachtspunten die de bank herkent uit survey's of incidentrapportages
- Aandachtspunten die je zelf herkent in je omgeving, (Bijv. het niet vergrendelen van de desktops of unclean desks door collega's)
- Incidenten die recentelijk hebben plaatsgevonden in je omgeving
- Trends op het gebied van informatiebeveiliging (Bijv. Skimming of Phishing)

Er zijn verschillende online leermiddelen beschikbaar over verschillende onderwerpen die toegepast kunnen worden, zoals:

- Quick Learning Programs
- NewsFlashes
- Flyers

Maar er kunnen ook andere middelen gekozen worden om ter voorbereiding aan te leveren, zoals:

- Nieuwsartikelen van incidenten
- Inhoudelijke artikelen over trends

Tijdens een Blended Learning-sessie…

In de sessie wil je dat medewerkers zoveel mogelijk hun kennis en mening geven over de thema. Daarom is het van belang dat je let op:

- De medewerkers comfortabel laten voel door aan te duiden dat het doel van de sessie is om elkaar te helpen en niet beoordelen
- De medewerkers genoeg aan het woord te laten
- De medewerkers met elkaar in gesprek brengen
- De medewerkers samen onduidelijkheden laten weg nemen
- Noteer vragen en onduidelijkheden waar je samen niet uitkwam

ABN·AMRO

Na een Blended Learning-sessie

Tijdens de sessie kan het voor komen dat er toch nog vragen en onduidelijkheden zijn over de thema. Indien dat zo is kan je de volgende stappen maken:

1. Stuur de vragen en onduidelijkheden door naar een expert (ISO.Awareness@nl.abnamro.com)
2. Koppel de antwoorden op de vragen en onduidelijkheden terug naar de deelnemers
3. Plan indien nodig een vervolg meeting

Handleiding “Social Engineering”

Doel:
Bewust inzetten van de juiste Social Engineering acties voor de juiste doelgroepen.

Hulpmiddelen uit de toolbox:
- Handleiding “Social Engineering”
- Flyer “Social Engineering”
- Newsflash “Social Engineering”

Uitvoering:
- Opnemen in de IS Awareness Campagne plannen als in te zetten hulpmiddel
- Uitvoeren als deel van de Campagne binnen de Business Line

Voorbereiding:
1. Bepaal de doelgroep waarvoor een Social Engeering actie ingezet moet worden
    a. Ga na of de doelgroep wel geschikt is voor een Social Engineering actie:
        i. Heeft de doelgroep te maken met risicogevoelige informatie
        ii.
2. Bepaal het doel van de actie
    a. Zit de doelgroep op een afgeschermde afdeling, dan is het toegang verschaffen tot die afdeling al interessant
    b. Behandelt de doelgroep veel vertrouwelijke gegevens, dan is het verkrijgen van deze vertrouwelijke informatie interessant, wat op verschillende manier kan:
        i. Fysiek
        ii. Telefonisch
        iii. Filmend
        iv. Mailend
3. Kies de juiste actie op basis van het doel en de doelgroep
    a. Per doelgroep kan het verschillen welke actie je inzet bv.
    b. bij medewerkers met klantcontact is een telefonische MysteryGuest wel interessant
    c. een afdeling waar de toegang gesloten moet zijn en er veel met vertrouwelijke informatie wordt omgegaan, is een Mystery Guest wel geschikt
4. Stel zoveel mogelijk informatie voor de betreffende actie beschikbaar voor de specialist, bv.
    a. Veel voorkomende incidenten
    b. Waarnemingen over bv. deur open houden voor onbekenden, niet afloggen van PC’s

Social engineering is een aanval gericht op het los krijgen van vertrouwelijke of geheime informatie. Door dergelijke aanvallen te simuleren kan het feitelijke gedrag van de medewerkers gemeten worden als zij geconfronteerd worden met social engineering aanvallen.

Vormen van gesimuleerde Social Engineering aanvallen:

- MysteryGuest

  Een specialist tracht zich toegang te verschaffen tot het kantoor (afdeling) en een bepaalde missie te volbrengen. Dit kan zijn het verkrijgen van toegang tot verboden ruimters, maar ook het ontfutselen van allerhande informatie met een vertrouwelijk karakter, al dan niet met het gebruik van social engineering.

- Telefonische MysteryGuest

  Bepaalde informatie mag niet via de telefoon worden prijsgegeven. En zeker niet aan een volslagen vreemde. De telefonische MysteryGuest probeert via social engineering de medewerkers toch vertrouwelijke informatie te ontfutselen.

- Filmende MysteryGuest

  Deze aanval is soortgelijk aan de MysteryGuest aanval, maar is het doel primair om de omgang met informatie door de medewerkers te filmen. Hiermee kan achterhaald worden hoe de medewerkers omgaan met clean desk, afschermen van de desktop, careless talking, etc.

- Nep-virus

  Op diverse werkplekken wordt een nep-virus geïnstalleerd om te kijken hoe de medewerkers hierop reageren. Houden ze zich aan het beleid of proberen ze het op een andere manier op te lossen?

- Phishing e-mail

  Via listige e-mails naar de medewerkers wordt geprobeerd vertrouwelijke informatie te ontfutselen. Hiermee wordt achterhaald of de medewerkers dergelijke e-mails wel herkennen of toch de vertrouwelijke informatie zomaar prijsgeven.

Het hoofddoel van deze acties is het meten van het gedrag van de medewerkers wanneer zij geconfronteerd worden met informatiebeveiliging situaties. Maar deze acties kunnen ook een prikkelend effect hebben. Het prikkelende effect van deze acties zit hem in het bekendmaken van de resultaten tijdens een later te houden bijeenkomst, met het tonen van bewijsmateriaal, zoals foto’s, vertrouwelijke documenten, etc.

Instructie voor Awareness Game

Beschrijving:
De game is te vergelijken met een competitie. Een competitie waarin je je kennis kan toetsen over informatiebeveiliging. Hierin nemen medewerkers het tegen elkaar op en/of afdelingen tegen elkaar. Als deelnemer speel je individueel mee door op een zet van meerkeuzevragen over verschillende informatiebeveiliging thema's je kennis los te laten. Daarna zie je middels een score hoe jouw kennis staat tegenover die van je collega's en hoe dat van je afdeling gemiddeld staat ten opzichte van andere afdelingen. Over de thema's waarop laag is gescoord, zal het spel direct een aantal tips geven.

Vendor:
Vest / Trustforce

Website:
http://www.vest.nl/Oplossingen/SecurityAwareness/Awarenessgame/tabid/144/Default.aspx

---

Instructies:

1. Bepaal de doelgroep en groepsindeling
    a. Bepaal de Business Line en afdelingen waar de game ingezet zal worden
    b. Bepaal het aantal deelnemers en stel een bestand op met de namen en e-mailadressen
    c. Bepaal of de deelnemers in groepen (bv. per afdeling) gedeeld moeten worden en verwerk dit dan ook in het deelnemersbestand
2. Kies de relevante thema's
    a. Voor de game is er een set van informatiebeveiliging thema's gedefinieerd
    b. Kies daaruit de voor de doelgroep relevante thema's (bv. op basis van incidenten, trends, lage scores uit vorige campagne)
    c. Bepaal of elk groep een andere set van thema's krijgt
3. Kies de relevante vragen
    a. Bepaal hoeveel vragen er per thema ingesteld moet worden
    b. Per thema is er een vaste set aan vragen gedefinieerd
    c. Kies daaruit per thema de relevante vragen voor de doelgroep