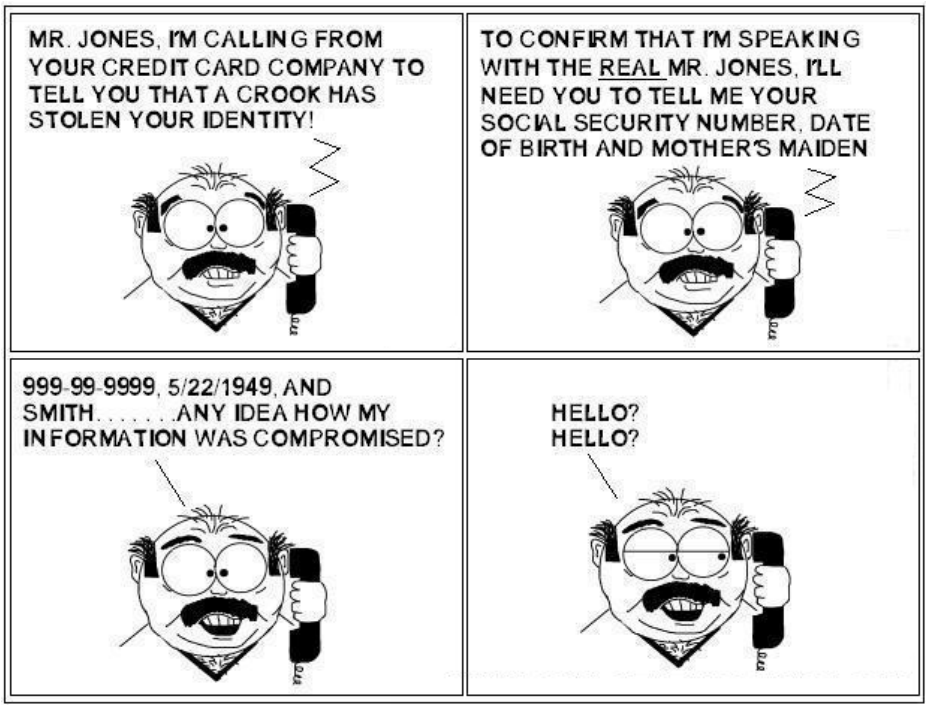
Beveiligingsbewustzijn efficiënt en meetbaar ingericht bij SNS REAAL

Het proces naar een hoger volwassenheidsniveau

Afstudeerscriptie



Uitgebracht aan	Dhr. Ben van Zuijlen, Dhr. John Verkooijen (SNS REAAL) Dhr. Rob van Stratum, Dhr. Martin van de Rijt, Stagebureau (Fontys) Dhr. S. Mulder (extern deskundige)
Datum	10 juni 2010
Bedrijf	SNS REAAL
Organisatieonderdeel	SNS IT & Change
Bedrijfsdeel	Architectuur & Beleid
Bedrijfsonderdeel	Informatiebeveiliging
Project	Beveiligingsbewustzijn efficiënt en meetbaar ingericht bij SNS REAAL
Opdrachtgever	Ben van Zuijlen
Opdrachtnemer	Stef Peeters
Plaats	's-Hertogenbosch
Versie	1.0
Auteur	Stef Peeters
Classificatie	Intern

Titelpagina

Naam stageverlenende instelling:	SNS REAAL
Bedrijfsonderdeel:	Informatiebeveiliging (IB)
Bezoekadres:	Pettelaarpark 120, 5201 DZ Den Bosch
Postadres:	Postbus 70053
Telefoonnummer:	073-6833333
Faxnummer:	073-6833600
Naam bedrijfsbegeleiders:	Dhr. John Verkooijen
Functie bedrijfsbegeleider:	Adviseur Informatiebeveiliging

Naam school:	Fontys Hogeschool ICT
Adres:	Rachelsmolen 1
Postcode/Plaats:	5600 AH Eindhoven
Telefoonnummer:	0877-877-299
Naam 1ste afstudeerstagedocent:	Dhr. Rob van Stratum
Naam 2de afstudeerstagedocent:	Dhr. Martin van de Rijt

Naam stagiair:	Stef Peeters
Studentnummer:	2069713
Adres:	Prinsenhof 3
Postcode/Woonplaats:	5616 TE Eindhoven
E-mailadres:	stef.peeters@student.fontys.nl
Telefoonnummer:	06-46022155
Stageperiode:	1 februari 2010 t/m 10 juni 2010

Voorwoord

Deze scriptie is geschreven in het kader van de vierdejaars afstudeerstage voor de opleiding Bedrijfskundige Informatica van de Fontys Hogeschool ICT te Eindhoven. Tijdens deze afstudeerperiode heb ik mij binnen SNS REAAL bezig gehouden met de afstudeeropdracht: 'Beveiligingsbewustzijn efficiënt en meetbaar ingericht bij SNS REAAL'. Met veel plezier en energie heb ik me ingezet om dit afstudeerproject tot een goed resultaat te leiden.

De opdracht die ik heb uitgevoerd betreft het duidelijk maken waar voor SNS REAAL de kansen liggen om het proces Informatiebeveiligingsbewustzijn efficiënt en meetbaar in te richten. Ook heb ik een aantal van deze kansen (aanbevelingen uit het onderzoek) uitgewerkt zodat SNS REAAL nieuwe praktische middelen heeft om het proces beter uit te voeren en het beveiligingsbewustzijn te verhogen. Een belangrijk deel van de praktische uitwerking van deze opdracht was het integreren van drie sites in één centrale site. Hierdoor kan de communicatie een stuk efficiënter en effectiever verlopen.

Dit werk kon slechts tot stand komen dankzij de steun en hulp van vele mensen. Dank gaat uit naar mijn opdrachtgever en afdelingshoofd Informatiebeveiliging, dhr. Ben van Zuijlen, voor het mogelijk maken van deze afstudeerstage en dat mij de kans is geboden om praktijkervaring op te doen op het gebied van informatiebeveiliging binnen de SNS REAAL. Speciale dank gaat uit naar mijn stagebegeleider dhr. John Verkooijen en zijn collega dhr. Gerd Damen voor hun begeleiding en de ondersteuning tijdens mijn afstudeerperiode, evenals voor de terugkoppeling op mijn gerealiseerde producten.

Verder was dit project nooit zo goed verlopen zonder de fijne samenwerking met de medewerkers van Informatiebeveiliging. Daarom wil ik hen hiervoor graag bedanken.

Ook wil ik Fontys Hogeschool ICT en in het bijzonder dhr. Rob van Stratum en dhr. Martin van de Rijt bedanken, zij hebben mij tijdens het afstuderen begeleid vanuit de opleiding Bedrijfskundige Informatica.

Als laatste gaat mijn dank uit naar alle mensen die ik niet heb benoemd, maar wel hebben bijgedragen aan en mij steun hebben gegeven bij deze afstudeerstage.

's-Hertogenbosch, 10 juni 2010,

Stef Peeters
Bedrijfskundige Informatica
Fontys Hogeschool ICT

Inhoudsopgave

Samenvatting

Informatiebeveiliging (IB) is onderdeel van het bedrijfsdeel IT & Change, het IT deel van de financiële dienstverlener SNS REAAL. IB draagt o.a. zorg voor beveiligingsbewustzijn bij de medewerkers. Dit betekent dat medewerkers de regels van informatiebeveiliging kennen en zich er ook naar gedragen. Als bank- en verzekeringsbedrijf vindt SNS REAAL het belangrijk dat er geen vertrouwelijke informatie op straat komt. Als er geen of in onvoldoende mate beveiligingsbewustzijn bestaat dan loopt het concern overmatige risico's. IB houdt zich al jaren bezig met het verhogen van het beveiligingsbewustzijn en is van mening dat dit een continu proces is waaraan gewerkt moet blijven worden. In het verleden zijn meerdere activiteiten met betrekking tot beveiligingsbewustzijn uitgevoerd. Het project 'Beveiligingsbewustzijn efficient en meetbaar ingericht' ontstond uit de wens om het proces Informatiebeveiligingsbewustzijn meer volwassen te maken om zo de efficiëntie en meetbaarheid te verhogen. Hiervoor moest duidelijk worden waar de kansen liggen om het proces efficiënt en meetbaar in te richten. Voor het bepalen van deze kansen is een onderzoek uitgevoerd. Uit dit onderzoek is onder andere gebleken welk volwassenheidsmodel het beste geschikt is om het niveau te bepalen. Na het onderzoek moesten de aanbevelingen zo ver als mogelijk worden uitgewerkt. Één van de aanbevelingen die gegarandeerd uit het onderzoek zou komen was het integreren van de drie sites naar één centrale. Dit was daarom al vastgelegd in de opdrachtomschrijving.

Het project is opgedeeld in drie hoofdfasen; de definitie- en initiatiefase, de uitvoeringsfase, en de afsluitingsfase. Deze fases komen uit de projectmanagementmethodiek PMW Professional, de standaard binnen SNS REAAL voor het beheren van projecten. Tijdens de definitie- en initiatiefase is het projectplan geschreven en is het onderzoek voorbereid. Daarna is in de uitvoeringsfase het onderzoek uitgevoerd en zijn een deel van de aanbevelingen uit het onderzoek uitgewerkt, zoals het integreren van de drie sites, het opstellen van een procesbeschrijving en het ontwerpen van middelen ter verhoging van het beveiligingsbewustzijn. Door de projectgroep wordt aanbevolen de site een nieuwe uitstraling te geven, hier was tijdens het project geen tijd meer voor. Op het einde van deze fase is nog een pilot uitgevoerd. In deze pilot is onderzocht welke verbeterpunten een ontwikkelde enquête voor het meten van beveiligingsbewustzijn nog bevat. Tijdens de afsluitingsfase is het project afgerond en is deze afstudeerscriptie geschreven en zijn er een aantal afrondende presentaties gehouden.

Uit onderzoek bleek dat de Security Awareness Maturity Tables het beste geschikt zijn voor het meten van de volwassenheid van het proces. Het onderzoek heeft daarnaast tot veel aanbevelingen geleid om het proces efficiënt en meetbaar in te richten. Een deel van deze aanbevelingen zijn verwerkt in een procesbeschrijving voor het proces Informatiebeveiligingsbewustzijn. Kenmerken uit een hoger volwassenheidsniveau zijn in deze procesbeschrijving verwerkt. Door deze procesbeschrijving te gebruiken functioneert het proces op een hoger volwassenheidsniveau, dit wordt dan ook door de projectgroep aanbevolen. Naast het verwerken van de aanbevelingen in de procesbeschrijving zijn een groot deel uitgewerkt. Dit zijn echter aanbevelingen die continu moeten worden uitgevoerd, SNS REAAL wordt dan ook aanbevolen om alle aanbevelingen uit te blijven voeren.

Summary

The department Information Security (IS) is part of the business unit IT & Change, the IT part of the financial service provider SNS REAAL. Among other areas of attention, security awareness is one of the tasks of IS. This means that employees are being made aware of the rules of information security and behave accordingly. For a bank and insurance company it is highly important not to lose any confidential information. If there is no or insufficient security awareness then SNS REAAL runs excessive risk. That is why IS is active in raising the security awareness for quite some years now. SNS REAAL believes it is an ongoing process where they have to keep paying attention to. In the past there have been several activities initiated trying to raise the security awareness. The project 'Security awareness efficient and measurable arranged' arose from the wish to make the process of Security Awareness operating at a higher maturity level to make it more efficient and measurable. To clarify the options to reach this goal, research needs to be conducted. During this research the most suitable maturity model to reach this maturity level has been determined. The recommendations from the research must, as far as possible, be followed in the rest of the project. One of the recommendations which definitely should be followed from the research is the integration of three sites into one central site. This was already part of the task description.

The project has been divided in three main phases; the definition- and initiation phase, the execution phase, and the conclusive phase. These phases arise from the project management method PMW professional; this is the standard within SNS REAAL for managing projects. During the definition and initiation phase the project plan was written and the research is prepared. Subsequently, the research was conducted and some of the recommendations were executed in the execution phase, such as integrating the three sites into one central site, writing a process description and creating new material for increasing security awareness. A recommendation is to create a new look for the site. During this project there was not enough time left to make all the improvements the project group desired. At the end of this phase a pilot has been executed. During this pilot a survey to measure the security awareness was tested. During the conclusive phase the project was completed. At this stage this thesis has been written and a number of conclusive presentations have been held.

The research indicates that the Security Awareness Maturity Tables are the best suitable model for defining the maturity of the process. The findings of my research give credence to the many recommendations to make the process more efficient and measurable. A number of these recommendations are included in the process description for the Security Awareness process. Also characteristics of a higher maturity level are included in this process description. By using this process description the process operates at a higher maturity level. The use of this process description is therefore recommended by the project group. Besides including the recommendations in the process description a large part has been executed. It should be noted that these recommendations must be carried out continuously to be most effective; SNS REAAL is therefore recommended to keep executing all the recommendations from the research on an ongoing basis.

Verklarende woordenlijst

In onderstaande lijst zijn afkortingen, termen en onbekende begrippen opgenomen. Het aansluitende paginanummer verwijst naar de pagina van uitleg over de betreffende afkorting, term of het begrip.

Beveiligingsincident, 30
Commitment, 53
Effectief en breed inzetbaar, 39
E-learning, 23
Face-to-face interviews, 31
FTE , 18
Give-aways, 59
Gouden regels, 17
Hoge acceptatiegraad, 39
IB-contactmomenten, 18
IB-coördinatoren,18
IB-jaarplan, 54
Informatiebeveiliging (IB), 17
(Informatie)beveiligingsbewustzijn, 29
Information Security Competence Maturity Model (ISCMM), 32
Intranet, 37
IT-dienstverlening, 16
Kennis, houding en gedrag, 29
Kostenefficiënt, 39
KPI, 55
Lijnmanagement, 17
Mystery guest, 30
Online ib-peiling, 31
Organisatorische maatregelen, 17
Out of pocket, 39
Pilot, 26
Plan-do-check-act (PDCA), 52
PRINCE2, 24
Prototype ter meting van informatiebeveiligingsbewustzijn, 34
SCORM, 62
Security Awareness Maturity Tables (SAMT), 36
SharePoint, 38
Synergievoordelen, 19
Technische maatregelen, 17
Volwassenheidsmodel, 21
Volwassenheidsniveau, 20
Web-based, 31

1. Inleiding

"Informatie deel je! Maar niet met iedereen…"
Een financiële dienstverlener heeft tegenwoordig bijna geen fysiek geld meer in huis. Alle bezittingen zijn digitale gegevens op grote computersystemen, zo ook bij SNS REAAL. Wil men niets verliezen dan zal men met grote zorgvuldigheid met de informatiebezittingen om moeten gaan. Dit zijn niet alleen geldelijke bezittingen, het niet goed beschermen van persoonsgegevens kan net zo schadelijk zijn. Het zijn van een goede financiële dienstverlener is gebaseerd op vertrouwen, het vertouwen dat een (potentiële) klant heeft in het plaatsen van al zijn financiële bezittingen en belangen bij die dienstverlener. Als dit vertrouwen schade oploopt zullen klanten weglopen en nieuwe klanten wegblijven. Informatie deel je! Maar niet met iedereen…

SNS REAAL heeft voor het beveiligen van de informatie het bedrijfsonderdeel Informatiebeveiliging in het leven geroepen. Zij bieden o.a. ondersteuning bij het bewust en bekwaam selecteren en implementeren van de juiste beveiligingsmaatregelen. Om deze maatregelen te communiceren en er voor te zorgen dat medewerkers zich eraan houden is ook informatiebeveiligingsbewustzijn voor IB een belangrijk aandachtsgebied.

Voor dit aandachtsgebied bestaat een apart proces. Dit proces draagt zorg voor het uitvoeren van diverse activiteiten om het beveiligingsbewustzijn te verhogen. Tijdens deze activiteiten worden diverse soorten middelen gebruikt. De één effectiever dan de ander, maar allen dragen ze bij aan het beveiligingsbewustzijn dat op dit moment bij de medewerkers van SNS REAAL bestaat.

SNS REAAL is zich ervan bewust dat wil het zich meten met de besten in de financiële dienstverlening zij altijd moeten presteren. Zo ook het proces Informatiebeveiligingsbewustzijn. En ook al is het proces al goed georganiseerd en is het beveiligingsbewustzijn van de medewerkers op een hoog niveau, toch wil SNS REAAL weten op welke vlakken zij nog meer vooruitgang kunnen boeken.

Om te ontdekken waar en hoe voor SNS REAAL nog kansen bestaan voor progressie bij het proces Informatiebeveiligingsbewustzijn is besloten om een onderzoek te houden. Een deel van de aanbevelingen uit dit onderzoek zijn ook werkelijk uitgewerkt om het proces beter te laten presteren.

Hoofdstuk 2 bevat algemene informatie over SNS REAAL, en in het bijzonder over het bedrijfsonderdeel Informatiebeveiliging (IB). In hoofdstuk 3 worden alle details van de opdracht beschreven. In hoofdstuk 4 wordt op de gehanteerde methodiek en werkelijk aanpak ingehaakt. In hoofdstuk 5 wordt de definitie- en initiatiefase beschreven, in deze fase zijn alle voorbereidingen op het project getroffen. In hoofdstuk 6 worden alle activiteiten en producten uit de uitvoeringsfase beschreven, de kernfase van dit project. In hoofdstuk 7 wordt ingegaan op een aantal afsluitende activiteiten van het project. In hoofdstuk 8 wordt tot slot op de conclusie en aanbevelingen ingegaan.

2. Het bedrijf[1]

In dit hoofdstuk volgt een beschrijving van het stagebedrijf, wat de ontstaansgeschiedenis is, wat de missie en visie zijn, hoe de organisatie eruit ziet en hoe het bedrijfsonderdeel Informatiebeveiliging is opgebouwd en functioneert. Verder wordt kort ingegaan op belangrijke thema's binnen SNS REAAL relevant aan dit project.

2.1. SNS REAAL[2]

SNS REAAL is een Nederlandse financiële dienstverlener op het gebied van verzekeren en bankieren (zie Figuur 1 voor het huidige organogram van SNS REAAL). De diensten en producten zijn toegespitst op particulieren en midden- en kleinbedrijf. De bancaire diensten worden verleend via eigen winkels, onafhankelijke intermediairs, regiokantoren, internet en de telefoon. Verzekeringsproducten en -diensten worden uitsluitend via onafhankelijke intermediairs verkocht.

De vestigingen van SNS REAAL zijn over het hele land verspreid, met de belangrijkste in Alkmaar, Utrecht en Den Bosch. Van oudsher is in Alkmaar het verzekeringsdeel gevestigd en in Den Bosch en Utrecht het bancaire deel, daarnaast is ook het hoofdkantoor in Utrecht te vinden.

Met een balanstotaal van € 129 miljard en circa 7500 (FTE) medewerkers is SNS REAAL een belangrijke speler op de Nederlandse bank- en verzekeringsmarkt. Het aandeel is genoteerd aan NYSE Euronext en maakt deel uit van de Amsterdam Midkap Index. In 2009 maakte SNS REAAL een nettowinst van € 17 miljoen nadat in 2008 nog een nettoverlies van € 504 miljoen in de boeken is weggeschreven.

2.2. Geschiedenis[3]

SNS REAAL is ontstaan in 1997 uit een fusie van de SNS Groep en de Reaal Groep. Deze concerns bestonden uit verschillende regionale spaarbanken (SNS Groep) en diverse verzekeringmaatschappijen (Reaal Groep).

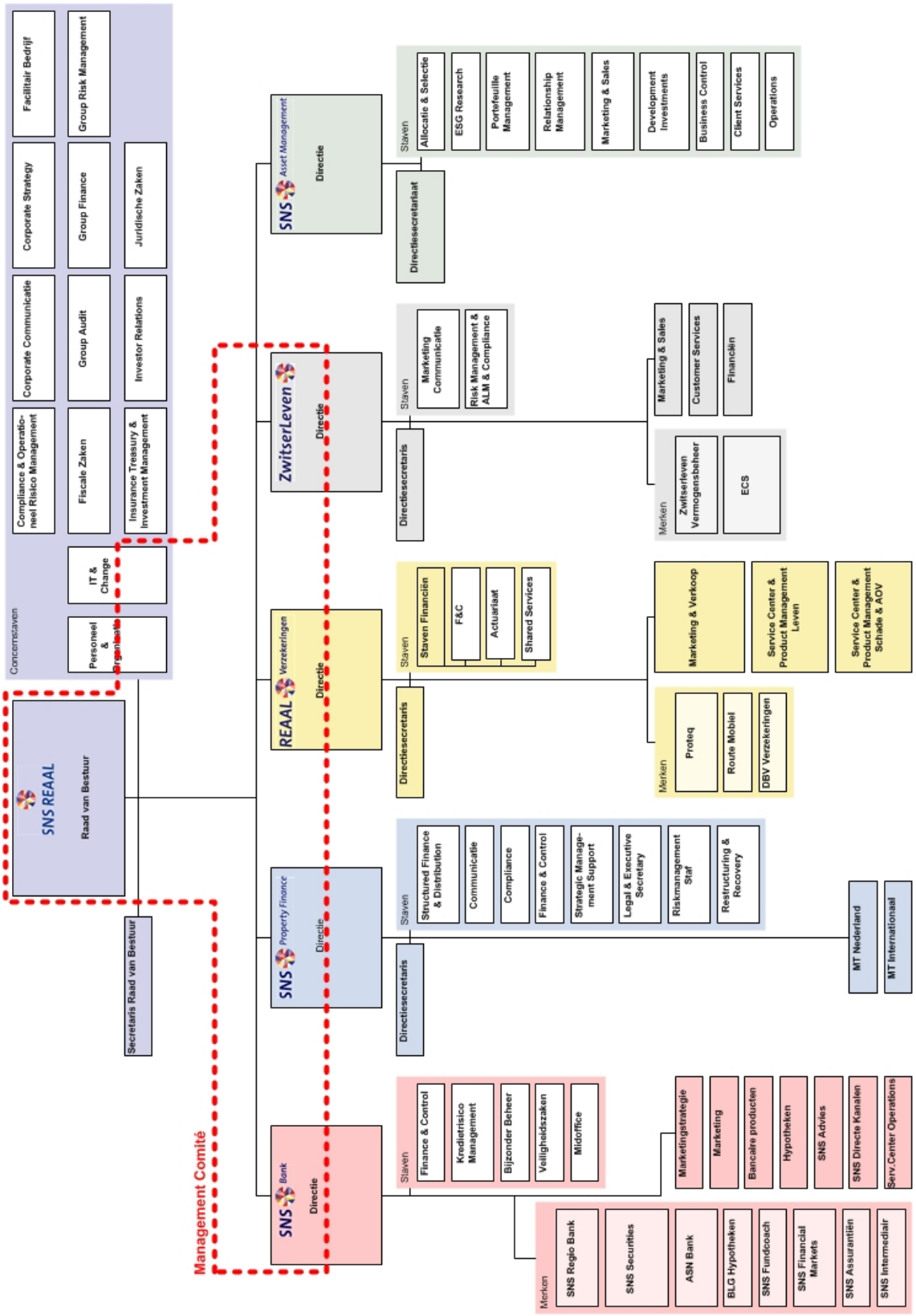
SNS Groep

De SNS Groep is in 1987 tot stand gekomen na een fusie van twee regionale spaarbanken, de naam SNS is dan ook een afkorting voor Samenwerkende Nederlandse Spaarbanken. In de jaren erna is de SNS Groep met nog meer regionale spaarbanken gefuseerd, waaronder in:

[1] Bron: SNS REAAL financieel jaarverslag 2009

[2] Bron: http://nl.wikipedia.org/wiki/SNS_REAAL

[3] Bron: http://www.snsreaal.nl/index.asp?NID=6545



Figuur 1 Uitgebreid organogram SNS REAAL. [4]

[4] Bron: Organogram SNS REAAL

- 1990: Stichting Bondsspaarbank Midden, Noord en Oost Nederland;
- de jaren negentig: BLG Hypotheken, CVB Bank en NOG Verzekeringen;
- 1996: Banque de Suez Nederland, inclusief Suez Nederland Securities (nu SNS Securities).

Reaal Groep

De Reaal Groep is tot stand gekomen na de fusie van verschillende vennootschappen, waaronder de verzekeringsmaatschappijen De Centrale en Concordia, de Hollandse Koopmansbank en de Algemene Spaarbank. De Reaal Groep bewerkstelligde de grootste groei tussen 1990 en 1997, onder andere door de overname van Hooge Huys Verzekeringen.

SNS REAAL

Na de fusie in 1997 zijn bedrijfseenheden van de fusiepartners gehergroepeerd en geïntegreerd. Zo werd NOG Verzekeringen geïntegreerd in Reaal Verzekeringen en ASN Bank en de Hollandse Koopmansbank werden dochtervennootschappen van SNS Bank.

Na de fusie heeft SNS REAAL meerdere overnames gedaan:

- 2003: de Nederlandse levensverzekeringsportefeuille en een gedeelte van de Nederlandse schadeverzekeringsportefeuille van Zürich;
- 2004: de levensverzekeringsportefeuille van Univé;
- 2005: Nieuwe Hollandse Lloyd;
- 2006: Bouwfonds Property Finance en van Route Mobiel;
- 2007: Regiobank en van AXA Nederland, Winterthur Verzekeringen en DBV Holding;
- 2008: SNS REAAL Zwitserleven.

2.3. Missie en visie[5]

Missie

De missie van SNS REAAL is: ‘Eenvoud in geldzaken‘. In het kort komt het er op neer dat men geldzaken eenvoudig wil maken. Dat betekent zo eenvoudig mogelijke procedures, eenvoudige producten en communicatie. Bij alles wat gedaan word, moet men zich afvragen of het eenvoudig genoeg is voor de klant, en of het nog eenvoudiger kan. Met eenvoud in geldzaken wil SNS REAAL de beste zijn in het winnen, helpen en behouden van klanten.

SNS REAAL wil zich onderscheiden van de rest van de markt door:

- de behoeften van haar klanten als uitgangspunt te nemen bij het ontwikkelen en aanbieden van producten, bij het verlenen van al haar diensten en bij het inrichten van processen;

[5] Bron: http://www.snsreaal.nl/index.asp?NID=6562

- aantrekkelijke prijsstellingen en gezonde marges op basis van standaardproducten en een klantgerichte en kostenbewuste organisatie;
- sterke marktposities op basis van een scherpe focus op specifieke product- en klantgroepen.

Visie

SNS REAAL wil een verantwoord handelende onderneming zijn, dit staat in hun visie gelijk aan het realiseren van de doelstellingen van de onderneming op een manier die rekening houdt met alle belanghebbenden (klanten, aandeelhouders, zakelijke partners en de samenleving). Dit komt in de praktijk erop neer dat binnen alle lagen van de organisatie, van bestuurders tot medewerkers, gehandeld wordt volgens vier gemeenschappelijke waarden: klantgericht, professioneel, integer en betrokken.

Klantgericht

Men luistert naar de wensen en behoeften van klanten en wil de klanten helpen groeien in zijn financiële mogelijkheden. Dit wil men bereiken door producten en diensten aan te bieden die voorzien in de behoeften van de klanten.

Professioneel

Een financiële dienstverlener staat of valt met het vertrouwen van klanten, aandeelhouders, zakelijke partners en de samenleving in de onderneming, zo ook bij SNS REAAL. Professionaliteit is hierbij een belangrijke factor. Dit komt onder meer tot uitdrukking in de inzet, kennis en vaardigheiden van de medewerkers en de kwaliteit van de dienstverlening.

Integriteit

SNS REAAL streeft naar kwalitatief hoogwaardige dienstverlening. In hun visie is dit alleen mogelijk indien iedereen binnen SNS REAAL integer handelt. Men moet zich niet alleen houden aan de wet, maar de onderneming en haar medewerkers moeten het vertrouwen dat belanghebbenden hebben ook in woord en daad waarmaken. Dit wordt bereikt door een hoge mate van transparantie in hoe SNS REAAL rekening houdt met de belangen van belanghebbenden.

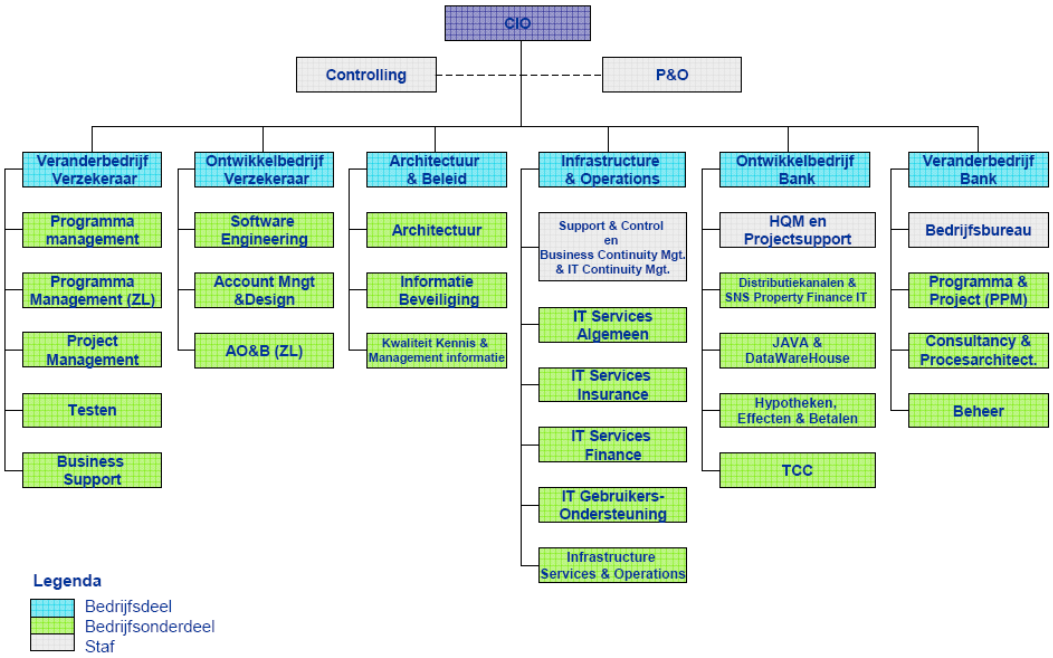
Betrokken

Naast de betrokkenheid bij de belanghebbenden heeft SNS REAAL ook oog voor haar omgeving. SNS REAAL stelt van oudsher belang in de sociale en economische ontwikkeling van de samenleving en draagt daaraan actief bij. Men bereikt dit door bij te dragen aan ontwikkelingen in de samenleving door kennis te delen, maatschappelijke initiatieven te ondersteunen en door medewerkers in staat te stellen maatschappelijke relevante bijdrage te leveren.

2.4. IT & Change

Voor het (goed) kunnen functioneren van de primaire processen van SNS REAAL is het aanbod van een afgestemd pakket aan IT-diensten een randvoorwaarde, omdat bij alle activiteiten informatie wordt verwerkt. Bij een financiële dienstverlener als SNS REAAL spelen bij haar activiteiten vertrouwen en wettelijke verplichtingen (ten aanzien van de kwaliteitseisen) van de registratie centraal. Het organisatiedeel IT & Change (IT&C) draagt zorg voor het op peil houden van de kwaliteit van de IT-dienstverlening[6]. Met ongeveer 1500 medewerkers verzorgt het binnen SNS REAAL de IT-dienstverlening en de realisatie van veranderingen op IT en organisatorisch vlak. IT&C bestaat uit meerdere bedrijfsdelen (zie Figuur 2), en bevat naast een Verander- en Ontwikkelbedrijf voor het verzekering- en bankdeel het bedrijfsdeel Infrastructure & Operations (I&O) en Architectuur & Beleid (A&B).
Het afstudeeronderzoek is bij het bedrijfsonderdeel Informatiebeveiliging uitgevoerd (zie Figuur 2, derde kolom).

De missie van IT&C is: *'IT & Change*
Motor in verandering
Betrouwbaar en Betaalbaar'[7]



Figuur 2 Organogram IT & Change[8]

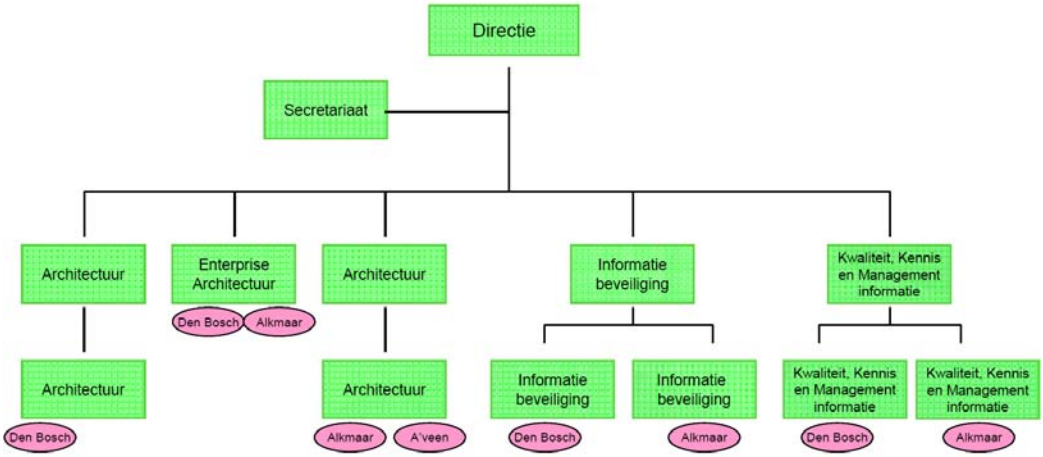
[6] Dienstverlening op het gebied van informatietechnologie (IT).

[7] Bron: Bedrijfsplan Informatiebeveiliging 2010 v1.0

[8] Bron: Organogram ITC per 01-01-2010

2.5. Architectuur & Beleid

Het bedrijfsdeel A&B is met 108 medewerkers (eind 2009) 9 verantwoordelijk voor architectuur, informatiebeveiliging, kwaliteit, kennis en managementinformatie. Het bedrijfsdeel heeft drie onderdelen (zie Figuur 3) die een soortgelijke naam dragen als de verantwoordelijkheden.



Figuur 3 Organogram Architectuur & Beleid [10]

2.6. Informatiebeveiliging[11]

Informatiebeveiliging is een zaak van alle medewerkers omdat je dit niet bereikt door alleen organisatorische[12] en technische[13] maatregelen in te zetten. De regels voor informatiebeveiliging moeten daarvoor ook gevolgd worden. Daarnaast is het een verantwoordelijkheid van het lijnmanagement[14] van SNS REAAL. Het beheersen van IT (beveiligings-)risico's is een onderdeel van de verschillende bedrijfs- en IT-processen.
IB ondersteunt het management bij het bewust en bekwaam selecteren en implementeren van de juiste beveiligingsmaatregelen, en zorgt voor het informatiebeveiligingsbewustzijn bij de SNS REAAL medewerkers. Daarnaast maakt IB ook nog de (rest-)risico's en bijbehorende verbeterpunten zichtbaar voor het management.

Een van de belangrijkste boodschappen die IB uitdraagt zijn de 7 Gouden regels. Hiermee maken zij het management, de leidinggevenden en de medewerkers van SNS REAAL bewust van het feit dat de regels voor informatiebeveiliging nageleefd dienen te worden.

[9] Bron: Presentatie Architectuur en Beleid 10 november 2009

[10] Bron: Presentatie Architectuur en Beleid 10 november 2009

[11] Bron: Bedrijfsplan Informatiebeveiliging 2010 v1.0

[12] Organisatorische maatregelen zijn maatregelen die te maken hebben met procedures, instructies en afspraken.

[13] Technische maatregelen worden met behulp van o.a. software, hardware, netwerken en andere infrastructuur ingezet.

[14] Is de leiding van een bedrijfsonderdeel.

De 7 Gouden regels voor Informatiebeveiliging[15]

1. Houd je aan de gedragsregels.
2. Behandel informatie met zorg.
3. Houd wachtwoorden/pincodes geheim.
4. Weet met wie je handelt.
5. Ga zorgvuldig om met internet en e-mail.
6. Geef aandacht aan fysieke beveiliging en gebruik van mobiele apparatuur.
7. Meld incidenten zoals virussen, diefstal en verlies.

De Gouden Regels worden onder andere tijdens beveiligingsbewustzijnactiviteiten, cursussen en IB-contactmomenten[16] voor IB-coördinatoren[17] vaak gecommuniceerd.

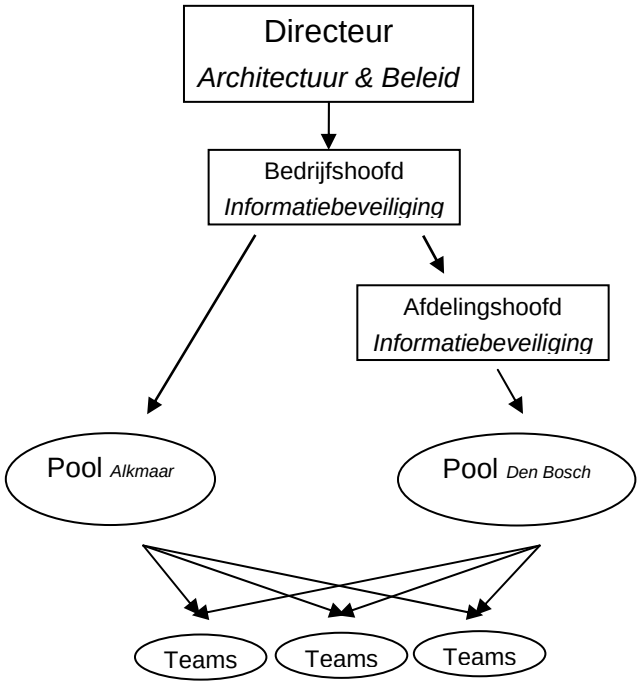
Er zijn twee IB-vestigingen, te weten in Alkmaar en Den Bosch (zie Figuur 4). De diensten verschillen per vestiging. In Alkmaar houdt men zich bijvoorbeeld bezig met de aandachtsgebieden *'speciale (advies) onderzoeken SNS REAAL IT'*, *'cybercrime'* en *'begeleiding bij audits'*. In Den Bosch bijvoorbeeld met *'beveiligingsbewustzijn'*, *'Security monitoring'* en *'certificering (ISO 27000)'*. Het aantal fte[18] van het bedrijfsonderdeel IB bedraagt 19,7.

[15] Bron: 7 Gouden regels van Informatiebeveiliging van SNS Bank

[16] Een middag georganiseerd door IB. Tijdens deze middag zijn er presentaties over allerlei ontwikkelingen die te maken hebben met de taken en verantwoordelijkheden van de IB-coördinatoren.

[17] Per bedrijfsonderdeel wordt een medewerker aangesteld die een aantal taken en verantwoordelijkheden op zich neemt met betrekking tot informatiebeveiliging. Deze taken en verantwoordelijkheden worden vastgesteld door IB.

[18] Dit staat voor full time employee, dit betekent het aantal medewerkers geteld in uren. Dus als er twee medewerkers 18 uur per week werken en een volledige werkweek is 36 uur dan is dat 1 fte.



Figuur 4 Het organogram van het bedrijfsonderdeel Informatiebeveiliging[19]

In 1997 is de SNS groep formeel gefuseerd met de REAAL groep. In de afgelopen jaren zijn reeds diverse bussiness-bedrijfsdelen[20] geïntegreerd. In 2009 is men begonnen met de integratie van de verschillende IT onderdelen; REAAL IT en SNS IT, dat is op dit moment in 2010 in volle gang is. Zo ook bij het bedrijfsonderdeel IB. De focus van veel activiteiten in 2010 ligt op de integratie van de SNS en REAAL IB afdelingen en het behalen van synergievoordelen[21]. De integratieactiviteiten worden in diverse projecten uitgevoerd. De realisatie wordt gemonitord. Hierbij worden werkzaamheden zoveel mogelijk gestroomlijnd om kostenverlaging te realiseren. Men richt zich daarbij op het standaardiseren van werkwijzen, standpunten en op te leveren producten.

[19] Bron: Structuur afdeling Informatiebeveiliging 1.1

[20] Bedrijfsdelen aan de business kant; m.a.w. bedrijfsdelen die

[21] Het voordeel dat kan optreden als bedrijven fuseren doordat er minder overheadkosten zijn en er efficiënter kan worden gewerkt.

3. De opdracht

In dit hoofdstuk worden alle details van de opdracht beschreven. In de aanleiding en probleemstelling wordt de beginsituatie uitgelegd en met behulp van de doelstelling de gewenste eindsituatie. Daarna wordt de exacte opdrachtomschrijving gegeven en wordt beschreven welke wijzigingen er in de opdrachtomschrijving tijdens dit project zijn aangebracht. Op het einde van dit hoofdstuk wordt de gehanteerde methodiek beschreven, deze methodiek is de standaard die binnen SNS REAAL wordt gebruikt.

3.1. Achtergrond

Bij SNS REAAL is informatiebeveiligingsbewustzijn een belangrijk thema. Hierbij zijn kennis, houding en gedrag van de regels van informatiebeveiliging van belang. Als bank- en verzekeringsbedrijf vindt SNS REAAL het belangrijk dat er geen vertrouwelijke informatie op straat komt. Als er geen of in onvoldoende mate beveiligingsbewustzijn bestaat dan loopt het concern overmatige risico's die kunnen leiden tot ernstige (financiële) schade.
Het bedrijfsonderdeel Informatiebeveiliging houdt zich al jaren bezig met het verhogen van het beveiligingsbewustzijn. IB is van mening dat dit een continu proces is, waar aan gewerkt moet blijven worden

3.2. Aanleiding van de opdracht

In het verleden zijn meerdere activiteiten en projecten met betrekking tot informatiebeveiligingsbewustzijn uitgevoerd. Deze activiteiten en projecten hebben tot middelen en campagnes ter verhoging van het beveiligingsbewustzijn geleid. Dit project borduurt verder op de wens om het proces Informatiebeveiligingsbewustzijn naar een hoger volwassenheidsniveau[22] te brengen om zo de efficiëntie en meetbaarheid te verhogen.

[22] Het volwassenheidsniveau geeft aan hoe goed/professioneel een organisatie of proces is georganiseerd.

3.3. Probleemstelling

Binnen SNS REAAL wordt vanwege het indammen van IT risico's veel aandacht besteed aan informatiebeveiligingsbewustzijn. Een netwerk van ongeveer 100 IB-coördinatoren verspreid over de organisatie functioneren als eerste aanspreekpunt m.b.t. informatiebeveiliging. Het bedrijfsonderdeel IB ondersteunt hen daarbij. Het huidige proces Informatiebeveiligingsbewustzijn voldoet aan alle standaarden; toch wil SNS REAAL naar een nog hoger niveau. De vraag luidt dan ook:

'Waar liggen voor SNS REAAL de kansen om het proces informatiebeveiligingsbewustzijn efficiënt en meetbaar over het hele concern in te richten?'.

3.4. Doelstelling

Tijdens dit project moet duidelijk worden waar voor SNS REAAL kansen liggen om het proces Informatiebeveiligingsbewustzijn meer volwassen te maken. Daarnaast moet er een geschikt model gekozen worden om het volwassenheidsniveau aantoonbaar te kunnen maken.
Door het uitwerken van deze kansen zal het proces Informatiebeveiligingsbewustzijn aan het einde van dit project op een hoger volwassenheidsniveau functioneren. Dit wordt onder andere bereikt door het bouwen van één centrale site, hierop moeten alle materialen m.b.t. het onderwerp informatiebeveiligingsbewustzijn binnen SNS REAAL gepost kunnen worden.

Samenvattend moet dit project opleveren:

- een onderzoeksrapport met conclusies en aanbevelingen die beschrijven waar voor SNS REAAL de kansen liggen en wat het geschikte volwassenheidsmodel[23] is om te hanteren;
- één centrale site waarop alle materialen effectief en efficiënt kunnen worden gepubliceerd;
- het proces Informatiebeveiligingsbewustzijn dat op een nog hoger volwassenheidsniveau functioneert.

[23] Een volwassenheidsmodel is een hulpmiddel om de volwassenheid van een organisatie te beoordelen en om de aandachtsgebieden te bepalen aan de hand waarvan de volwassenheid van die organisatie vergroot kan worden. (Bron: Sogeti)

3.5. Opdrachtomschrijving

Maak duidelijk waar voor SNS REAAL de kansen liggen om het proces Informatiebeveiligingsbewustzijn naar een nog hoger volwassenheidsniveau te brengen en zorg dat dit meet- en aantoonbaar wordt met behulp van een geschikt volwassenheidsmodel.

Werk alle kansen beschreven in de conclusies en aanbevelingen uit het onderzoek, zo ver als mogelijk binnen de grenzen van dit project, uit. Er moet een (op basis van Project Management overwegingen) beargumenteerde keuze gemaakt worden tussen kansen die niet en die wel uitgewerkt worden.

Integreer de drie bestaande IB sites naar één centrale site.

3.6. Op te leveren producten

De resultaten (de op te leveren producten) die bereikt dienen te worden zijn:

- projectplan;
- onderzoekopzet;
- rapport onderzoek;
- centrale IB site op ID (is centrale SharePoint site in gebruik binnen SNS REAAL);
- middelen te bevordering van het beveiligingsbewustzijn;
- testverslag;
- ondersteunende documentatie IB-coördinatoren;
- presentaties:
    - IB-coördinatordag;
    - oplevering resultaten;
    - afstudeerzitting.
- eindscriptie project.

3.7. Opdrachtwijziging

De opdracht is eenmaal gewijzigd, dit is in de tweede week van het project gebeurd. De opdrachtgever kon zich niet vinden in de opdrachtomschrijving zoals deze was opgesteld ter voorbereiding van dit project.

Oude opdrachtomschrijving

Probleemstelling

SNS REAAL-medewerkers zijn zich niet in voldoende mate bewust van de risico's die er verbonden zijn aan het niet in acht nemen van de informatiebeveiligingsvoorschriften. Doordat men deze voorschiften te lichtzinnig opvat dan wel doordat deze voorschriften niet bekend zijn ontstaat er een risico dat het BIV niveau van de informatie te laag wordt.

Doelstelling

Medewerkers moeten bewust worden van het belang van een zorgvuldige toepassing van de regels en procedures van informatiebeveiliging. Om dit vast te kunnen stellen moeten beveiligingsbewustzijnaspecten meetbaar worden gemaakt.

Opdracht

Uitwerking van Minerva en e-learning[24] aspecten voor alle IB-coördinatoren voor geheel SNS REAAL. Opzetten van beveiligingsbewustzijncampagne en hoe de IB-coördinator hierbij te ondersteunen zodat hij/zij dit decentraal kan uitvoeren. Ontwikkelen van testmethode voor awareness.

3.7.1. Motivatie wijziging

Het niveau van het beveiligingsbewustzijn bevindt zich al op een hoog niveau. Dit project is dan ook gestart om het bewustzijnniveau en het volwassenheidsniveau van het proces naar een nog hoger niveau te tillen. Om dit te bereiken was het opstellen van een compleet nieuwe beveiligingsbewustzijncampagne, omdat er al een campagne bestaat, niet nodig. Wel moest met de verkregen inzichten duidelijk worden hoe SNS REAAL het proces Informatiebeveiligingsbewustzijn efficiënt en meetbaar kon inrichten.

3.7.2. Ontstane problemen

Het projectplan moest in lijn zijn met de nieuwe opdrachtomschrijving, hierin zijn daarom een aantal wijzigingen aangebracht. Dit had geen grote gevolgen voor de rest van het project, omdat het project zich nog in de initiatie- en definitiefase bevond.

[24] Elke leervorm die gebruik maakt van een computernetwerk voor distributie, communicatie over en weer en facilitering.

3.8. Gehanteerde methodiek[25]

In de huidige tijd volgen veranderingen in de markt elkaar in een steeds sneller tempo op. Wil SNS REAAL blijven voldoen aan de eisen en behoeften van haar omgeving dan moet ze inspringen op deze veranderingen. De tijd waarin veranderingen ad hoc kunnen worden geïmplementeerd is voorbij. Werkzaamheden worden daarom op een projectmatige wijze uitgevoerd. Binnen SNS REAAL is PMW Professional (zie Figuur 5) de standaard voor het beheer van projecten. Deze methodiek is geschikt voor alle soorten en maten projecten en is analoog aan de PRINCE2[26] methode. Met behulp van PMW professional zijn een aantal samenhangende activiteiten geformuleerd waarbij het doel centraal staat.

Figuur 5 Het logo van PMW Professional.

Door PMW Professional te hanteren wordt binnen SNS REAAL op een gestandaardiseerde manier gewerkt, dit verbetert de communicatie enorm. Met deze methodiek bereikt een project verder ook:

- een gecontroleerde en georganiseerde start-, midden- en eindfase;
- regelmatige controle op de voortgang aan de hand van de planning;
- automatische managementcontrole op afwijkingen van het plan;
- informeren van betrokkenen op de juiste momenten en plaatsen gedurende het project;
- goede communicatiekanalen tussen het project, projectmanagement, en de rest van de organisatie.

Naast een projectmanagementmethodiek beschrijft PMW Professional ook een vooronderzoek- en programmamanagement methodiek. Voor dit project is alleen gebruik gemaakt van een aantal templates en de fasering van de projectmanagementmethodiek.
In de volgende paragraaf is deze fasering vertaald naar de aanpak die is gebruikt om te komen tot de gewenste eindsituatie van dit project.

[25] Bron: http://SharePoint.bank.local/sites/200807032/default.aspx

[26] PRINCE2 is een gestructureerde methode voor projectmanagement.

4. Definitie- en initiatiefase: Plannen is vooruitzien

In dit hoofdstuk worden de activiteiten en resultaten uit de eerste fase van dit project beschreven. Tijdens deze fase is een concrete beschrijving gemaakt van de probleem- en doelstelling en de daaropvolgende opdracht. Op basis van deze beschrijvingen is een projectplan geschreven; dit document bevat onder andere een planning, een beschrijving van de projectorganisatie en allerlei beheermechanismen. Hiermee kon op een gecontroleerde manier naar het gewenste eindresultaat gewerkt worden. In deze fase is ook een plan gemaakt voor het uitvoeren van het onderzoek, tijdens dit onderzoek moest kennis worden verworven, waarmee duidelijk werd waar voor SNS REAAL kansen liggen om het proces Informatiebeveiligingsbewustzijn effectief en meetbaar over het hele concern in te richten.

4.1. Projectopdracht afbakenen

Tijdens de sollicitatieprocedure voor dit project is met de beschikbare kennis over de huidige situatie binnen en de eisen en behoeften van SNS REAAL een opdrachtomschrijving geschreven. Deze omschrijving bleek tijdens de eerste projectweken niet voldoende aan te sluiten op de werkelijke behoeften van SNS REAAL (zie hoofdstuk 3 voor de oude en nieuwe opdrachtomschrijving). De volwassenheid van het proces en het beveiligingsbewustzijn van de medewerkers is reeds op een voldoende niveau. De reden voor het opstarten van dit project is om het volwassenheidniveau meet- en aantoonbaar te maken en waar mogelijk te verhogen. Het indirecte doel is daarbij natuurlijk ook om het beveiligingsbewustzijn over het hele concern te verbeteren. SNS REAAL is een bedrijf dat altijd naar verbetering en vooruitgang streeft. Alleen het beste is goed genoeg, daar sluit de nieuwe opdrachtomschrijving dan ook beter op aan.

Tijdens het schrijven van de eerste opdrachtomschrijving was ook niet bekend dat de informatieverstrekking onder andere via drie verschillende sites verliep. Dit was geen efficiënte manier van werken. Gezien het doel van dit project moesten ook de drie sites in één centrale site worden geïntegreerd.

Bij de start van het project was nog niet duidelijk hoeveel tijd het bouwen van de centrale site op ID in beslag zou nemen, daarom kon niet worden gegarandeerd dat alle aanbevelingen uitgewerkt konden worden. Met betrekking tot het uitwerken van de aanbevelingen is de opdrachtomschrijving daarom enigszins vrijblijvend gebleven.

4.2. Projectplan schrijven

Het projectplan had in conceptvorm de vorm en naam van een Project Initiation Document (PID). Bij SNS REAAL wordt echter gebruik gemaakt van een ander formaat; qua opbouw lijken deze documenten veel op elkaar. PID is afkomstig uit de PRINCE2 methodiek en het projectplan uit de PMW Professional methodiek, een methodiek afgeleid van PRINCE2. Omwille van de consistentie en de herkenbaarheid binnen SNS REAAL is besloten om het op te bouwen als een projectplan (zie bijlage A).

Het projectplan is opgedeeld in drie hoofdfasen: de definitie- en initiatiefase, de uitvoeringsfase, en de afsluitingsfase. De voortgang van de activiteiten in deze fases is door de opdrachtgever in samenwerking met de projectleider, bedrijfsbegeleiders en stagedocent van Fontys bewaakt. De drie hoofdfases zijn op hun beurt in deelfases opgedeeld:

1. definitie- en initiatiefase:
    a. projectopdracht afbakenen;
    b. projectplan schrijven;
    c. onderzoek voorbereiden.
2. uitvoeringsfase:
    a. onderzoek beveiligingsbewustzijn uitvoeren;
    b. onderzoek afsluiten;
    c. (deel van) aanbevelingen onderzoek implementeren;
        i. integreren van de drie sites in ID;
        ii. opstellen procesbeschrijving Informatiebeveiligingsbewustzijn;
        iii. middelen ter verhoging van het beveiligingsbewustzijn ontwerpen;
    d. pilot[27] meting beveiligingsbewustzijn houden;
        i. meting beveiligingsbewustzijn uitvoeren;
        ii. testverslag schrijven (inclusief advies).
3. afsluitingsfase:
    a. afstudeerscriptie schrijven;
    b. afrondende presentaties houden.

[27] Een test waarbij een programma of apparaat voor een tijdje in productie (werkomgeving) wordt gebruikt, zodat de eventuele gebreken/bugs achterhaald worden.

4.3. Onderzoek voorbereiden[28]

SNS REAAL wilde met dit project onder andere kennis over de huidige markt van middelen ter verhoging van het beveiligingsbewustzijn krijgen. Duidelijk moest worden of en hoe deze middelen kunnen bijdragen bij het verhogen van het beveiligingsbewustzijn. Daarnaast moest een geschikt volwassenheidsmodel gevonden worden om het proces Informatiebeveiligingsbewustzijn te kunnen beoordelen. Om een oordeel te kunnen geven wat SNS REAAL nodig heeft was het ook van belang dat onderzocht werd hoe de huidige organisatie omtrent beveiligingsbewustzijn was. Literatuur over informatiebeveiliging onderzoeken was niet nodig, kennis over dit onderwerp is binnen IB genoeg kennis beschikbaar.

Ter voorbereiding op het onderzoek is een plan (zie externe bijlage B) gemaakt, de onderzoeksopzet. Dit plan beschrijft hoe er een antwoord kan worden verkregen op de hoofdvraag: *'Waar liggen voor SNS REAAL de kansen om het proces Informatiebeveiligingsbewustzijn efficiënt en meetbaar over het hele concern in te richten?'*.

Het antwoord op de hoofdvraag was nogal complex. Daarom is deze vraag in deelvragen opgesplitst. Elk antwoord op een deelvraag droeg zijn steentje bij aan het beantwoorden van de hoofdvraag. De deelvragen waren:

1. Wat is informatiebeveiligingsbewustzijn?
2. Hoe wordt informatiebeveiligingsbewustzijn bewerkstelligd?
3. Hoe kunnen aspecten van informatiebeveiligingsbewustzijn meetbaar gemaakt worden?
4. Welke modellen bestaan er om het volwassenheidsniveau van een proces vast te stellen?
5. Welk model is het beste geschikt om het volwassenheidsniveau van het proces Informatiebeveiligingsbewustzijn binnen SNS REAAL vast te stellen?
6. Hoe is het proces informatiebeveiligingsbewustzijn op dit moment ingericht en welke middelen worden hiervoor gebruikt?
7. Wat zijn de ervaringen met reeds gebruikte middelen?
8. Welke criteria zijn van toepassing bij de keuze van middelen voor informatiebeveiligingsbewustzijn?
9. Welke middelen voor informatiebeveiligingsbewustzijn zijn er op de markt, op basis van welke principes werken deze en hoe verhouden ze zich tot elkaar?
10. Welke van deze middelen passen het beste bij SNS REAAL?

[28] Bron: Piet Verschuren, Hans Doorewaard: Het ontwerpen van een onderzoek (derde druk 2004)

De deelvragen droegen niet alleen bij om structuur aan te brengen in het onderzoek, maar ook in het onderzoekrapport. Bovendien verkleinden de deelvragen de kans dat belangrijke zaken over het hoofd werden gezien.

Voor het beantwoorden van de vragen is gekozen voor een combinatie van onderzoekstrategieën. Dit is een combinatie van een casestudy en een bureauonderzoek. Bij een bureauonderzoek worden gegevens verzameld en verwerkt tot bruikbare informatie. De gegevens die verzameld worden zijn afkomstig van bestaande onderzoeken en/of informatiebronnen.
Bij een casestudy wordt geprobeerd om een diepgaand inzicht te krijgen in één of enkele tijdruimtelijk begrensde objecten of processen. Deze objecten of processen kunnen zijn een organisatie, een bedrijf, de totstandkoming van een bepaalde wet, de locatiekeuze van een stortplaats, enzovoort. In dit geval is het object het proces Informatiebeveiligingsbewustzijn bij SNS REAAL

Het onderzoek is als volgt ingericht:

- een bureauonderzoek, waarmee inzicht gekregen moest worden over:
    - wat beveiligingsbewustzijn is (deelvraag 1);
    - hoe beveiligingsbewustzijn gecreëerd kan worden (deelvraag 2);
    - hoe en wat van beveiligingsbewustzijn meetbaar kan worden gemaakt (deelvraag 3);
    - welke volwassenheidsmodellen er bestaan en of en hoe deze toepasbaar zijn voor het bepalen van het niveau van het proces Informatiebeveiligingsbewustzijn (deelvragen 4 en 5);
- een casestudy, waarmee duidelijk moest worden:
    - hoe het huidige proces is georganiseerd en met welke middelen (deelvragen 6 en 7);
    - welke middelen er op de markt zijn en welke eisen SNS REAAL aan middelen ter verhoging van het bewustzijn stelt (deelvragen 8 en 9);
    - welke middelen passen het beste bij SNS REAAL (deelvraag 10).

5. Uitvoeringsfase Deel I: Het Onderzoek

In dit hoofdstuk worden de deelvragen uit het onderzoek behandeld. Na elke paragraaf wordt kenbaar gemaakt welke deelvraag daarmee is beantwoord. Op het einde wordt in de conclusie en aanbevelingen van het onderzoek ingegaan op de hoofdvraag. Hier wordt kenbaar gemaakt welk deel van de doelstelling is voltooid

5.1. Beveiligingsbewustzijn onderzoek

Het onderzoek heeft geleid tot veel nieuwe kennis voor zowel de projectleden als voor SNS REAAL. Hierover is een rapport geschreven waarin alle deelvragen apart worden behandeld (zie externe bijlage C). In de conclusie en aanbevelingen van het rapport wordt ingegaan op de hoofdvraag. Binnen deze scriptie is besloten om alleen de belangrijke punten uit het rapport te beschrijven.

5.1.1. Informatiebeveiligingsbewustzijn

Vaak wordt vanuit gegaan dat met het invoeren van organisatorische en technische maatregelen de informatiebeveiliging goed is geregeld; dat is echter meestal niet het geval. Voor deze maatregelen en de noodzaak ervan moet bij elke medeweker bewustzijn worden gecreëerd, of te wel informatiebeveiligingsbewustzijn.

'Informatiebeveiligingsbewustzijn[29] *is de mate waarin elke medewerker de volgende punten begrijpt:*

- *het belang van informatiebeveiliging voor de organisatie;*
- *het niveau van informatiebeveiliging dat voor de organisatie noodzakelijk is en er ook naar handelt.'*

Om tot het noodzakelijke niveau van informatiebeveiliging te komen moet het aandeel van medewerkers niet worden onderschat. Het creëren van informatiebeveiligingsbewustzijn zal daarom altijd belangrijk zijn bij het op peil houden dan wel verhogen van het niveau.

Voor het verhogen van dit niveau bestaan vele middelen. Een effectief middel richt zich op drie dimensies:

- **kennis**: wat weet een persoon? (d.m.v. interne of externe opleidingen);
- **houding**: wat voelen ze voor het onderwerp? (door het belang duidelijk te maken);
- **gedrag**: wat doen ze? (d.m.v. herhaalde oefening en training).

[29] Bron: Caroline Neys: It'ers, regels en security awareness (2010)

Door alle drie de dimensies bij medewerkers naar een zo hoog mogelijk niveau te brengen stijgt het beveiligingsbewustzijn.

Gedrag is uiteindelijk de belangrijkste dimensie. Hieruit kunnen, door het niet uitvoeren van de regels, beveiligingsincidenten[30] of -risico's ontstaan. Maar zonder weet te hebben van het bestaan van deze regels (voortvloeiend uit de kennis) of de wil om ze ook te volgen (houding) komt er van het juiste gedrag weinig terecht.

Deelvraag (✓ = vraag is beantwoord)									
1 ✓	2 ✓	3	4	5	6	7	8	9	10

Met het bepalen van wat beveiligingsbewustzijn is en hoe dit beveiligingsbewustzijn gemeten kan worden, zijn de deelvragen 1 en 2 beantwoord.

Deelvraag 1: 'Wat is informatiebeveiligingsbewustzijn?'
Deelvraag 2: '*Hoe kunnen aspecten van informatiebeveiligingsbewustzijn meetbaar gemaakt worden? '*

5.1.2. Meten van beveiligingsbewustzijn

SNS REAAL wil aantoonbaar 'in control' zijn, zo ook op het vlak van beveiligingsbewustzijn. Dit kan men alleen bereiken door metingen uit te voeren. Informatiebeveiligingsbewustzijn is echter een breed kwalitatief begrip. Breed omdat het vele aspecten heeft en kwalitatief omdat het niet altijd even tastbaar is en niet één, twee, drie met cijfers is te beschrijven. Dit maakt het lastig meetbaar. Toch bestaan er meerdere methodieken om beveiligingsbewustzijn meetbaar te maken. Een selectie is gemaakt uit de beschikbare methoden:

- mystery guest;
- face-to-face interviews;
- online ib-peiling (m.b.v. enquêtes).

Mystery guest

Wetende hoe medewerkers geïnstrueerd zijn, wat de Gouden regels zijn en wat in de gedragscode en handboeken staat, zal een mystery guest op locaties door de kantoren 'sluipen'. Op basis van een vooraf opgestelde checklist wordt gelet op 'incidenten' die duiden op een tekort aan bewustzijn. Zoals stoelen die toegangsdeuren tegen de regels in open houden, desktops die niet vergrendeld zijn, waardevolle zaken die op bureaus slingeren (pasjes, PDA's, gevoelige documenten), informatie aanwezig op whiteboards en geprinte informatie bij printers en faxmachines. Dit vergt een scherp oog en een turflijst of een goed geheugen. De fotocamera is hierbij een uitstekend hulpmiddel.

De belangrijkste kenmerken van deze methodiek zijn:

- maakt kwetsbaarheid van de organisatie zeer concreet en zichtbaar;

[30] Een beveiligingsincident is een gebeurtenis die een bedreiging vormt of kan vormen voor de vertrouwelijkheid, betrouwbaarheid of beschikbaarheid van gegevens.

- kort tijdsbestek/veel resultaat;
- verregaande sociale vaardigheden vereist bij mystery guest;
- moet goed getraind zijn;
- resultaat kan subjectief zijn;
- wordt uitgevoerd door een externe persoon.

Face-to-face interviews

Via voorbereide vraaggesprekken is te achterhalen hoe medewerkers tegen informatiebeveiliging aankijken, wat ze er onder verstaan, hoe ze in bepaalde omstandigheden handelen en hoe ver hun kennis van het informatiebeveiligingsbeleid en de daaruit afgeleide regels en richtlijnen van de organisatie strekt.

De belangrijkste kenmerken van deze methodiek zijn:

- interactief, de interviewer kan inspelen op zaken die naar voren komen;
- smaakbepaling, de interviewer kan een juist gevoel krijgen over hoe medewerkers over bepaalde zaken denken;
- kan goed gecombineerd worden met andere soorten metingen;
- bewerkelijk;
- beter geschikt voor een kleinschalig onderzoek;
- sterk afhankelijk van vaardigheden interviewer;
- sterk afhankelijk van het niveau van de ondervraagden;
- bij voorkeur uitgevoerd door een externe persoon.

Online ib-peiling

Een derde wijze waar goede ervaringen mee zijn, is het meten van bewustzijn via online ib-peilingen. Hierbij wordt een digitale vragenlijst speciaal geprepareerd en 'losgelaten' op een doelgroep of op alle medewerkers binnen de organisatie.

De belangrijkste kenmerken van deze methodiek zijn:

- web-based[31] vragenlijst;
- na start is vragenlijst niet meer te wijzigen;
- formulering/opbouw vragenlijst moet perfect zijn, dit is lastig;
- veel waardevolle informatie;
- kan extra informatie achterhalen door anonieme deelname;
- geen externe (organisatie) nodig.

[31] Web-based is een term om software aan te duiden die via het internet of een intranet werkt.

De kwaliteit van de vragenlijst is zeer belangrijk, deze moet absoluut goed zijn. Er is maar één gelegenheid om hem op te stellen. Als de meting loopt, is de vragenlijst niet meer te wijzigen. Bij het opstellen moet gelet worden op de aspecten kennis, houding en gedrag. Maar ook op een goede balans. Een te eenzijdige vragenlijst geeft een te eenzijdige uitspraak. Enerzijds is het goed om te toetsen of medewerkers bepaalde zaken snappen (en dus bewust zijn van), maar anderzijds is ook relevant wat zij in bepaalde omstandigheden zouden doen.

5.1.3. Opbouw meetinstrument beveiligingsbewustzijn

Naast de voorgaande methoden over de manier van meten van beveiligingsbewustzijn bestaan er ook nog voorbeelden voor het opbouwen van een meetinstrument. In het onderzoek zijn twee van dit soort modellen naar voren gekomen. Het eerste model dat beschreven wordt is te gebruiken bij een mystery guest en face-to-face interviews, het tweede model is juist geschikt voor een online ib-peiling.

Information Security Competence Maturity Model[32]

Het Information Security Competence Maturity Model beschrijft een viertal niveaus waarin het beveiligingsbewustzijn van een medewerker zich kan bevinden. Dit model is vooral geschikt voor gebruik bij een mystery guest en een face-to-face interview, want met het stellen van vragen en het observeren van bepaalde situaties kan beoordeeld worden op welk niveau men zit. Omdat bij een online ib-peiling geen observaties mogelijk zijn is dit model een stuk lastiger om toe te passen.

Per niveau is aangegeven waar een medewerker aan moet voldoen om tot een bepaald niveau te horen. Zo is het mogelijk voor een interviewer of mystery guest om gerichte vragen te stellen of op bepaalde zaken te letten om te bepalen op welk niveau een medewerker zich bevindt. Bij een laag beveiligingsbewustzijn zijn medewerkers zich er meestal niet van bewust dat ze fouten maken (onbewust onbekwaam). Bij de eerste trainingen voor beveiligingsbewustzijn is het doel om medewerkers bewust te maken van het feit dat zij incidenten veroorzaken of veroorzaakt hebben en waarom zij deze incidenten veroorzaken (bewust onbekwaam). Nadat medewerkers zich hiervan bewust zijn, kan begonnen worden met het aanleren van het juiste gedrag. Medewerkers moeten zich bewust worden van de risico's van hun gedrag en moeten handelen volgens het aangeleerde juiste gedrag. (bewust bekwaam). Op het hoogste niveau van beveiligingsbewustzijn is het veilig handelen van de medewerker een regulier onderdeel van zijn gedrag. Hij handelt in overeenstemming met wat hem geleerd is en is in staat om dit ook in andere situaties toe te passen (onbewust bekwaam). Voor de kenmerken van alle niveaus zie Tabel 1.

[32] Bron: Kerry-Lynn Thomson, Rossouw von Solms: Towards an Information Security Competence Maturity Model (2006)

Nr	Niveau	Kenmerken
1	Onbewust onbekwaam	• Medewerkers zijn zich niet bewust van de rol die zij (zouden moeten) spelen bij informatiebeveiliging. • Medewerkers zijn zich niet bewust van hun ineffectiviteit bij informatiebeveiligingsactiviteiten. • Verandering van gedrag op dit niveau is niet verstandig, omdat medewerkers de baten nog niet inzien. • Medewerkers zien informatiebeveiliging als hinder voor hun werk en hebben 'workarounds' om informatiebeveiliging maatregelen te omzeilen.
2	Bewust onbekwaam	• Een effectieve informatiebeveiligingscampagne moet medewerkers hebben geïnformeerd. • Deze campagne moet medewerkers helpen te begrijpen waarom zij informatiebeveiliging serieus moeten nemen en wat voor baten een goede uitvoering heeft. • In het ultieme geval moet deze campagne medewerkers voorbereiden voor het veranderen van hun houding t.o.v. informatiebeveiliging.
3	Bewust bekwaam	• Medewerkers zijn bekend met hun rol en verantwoordelijkheden bij een goede werking van informatiebeveiliging. • Ze zien de voordelen van het beveiligen van de informatie 'bezittingen'. • Medewerkers realiseren zich dat informatiebeveiliging niet alleen maar belangrijk is voor henzelf maar ook voor de organisatie. • Medewerkers zijn bewust bezig met informatiebeveiliging. • Medewerkers realiseren zich wat nodig is om tot niveau 4 te komen.
4	Onbewust bekwaam	• Ze hebben verstand van en zijn ervaren in informatiebeveiliging. • Medewerkers handelen onbewust naar de activiteiten opgesteld volgens de visie over informatiebeveiliging van het management. • De activiteiten zijn onderdeel van het gedrag van de medewerker en daarom onderdeel van de cultuur.

Tabel 1 Bewustzijnniveaus uit het Information Security Competence Maturity Model.

Prototype ter meting van informatiebeveiligingsbewustzijn[33]

Het volgende prototype is van toepassing op een online ib-peiling, omdat hierbij wordt gewerkt met vastgestelde vragen en antwoorden. Het gebruik van een vastgestelde vragenlijst en antwoorden is bij een face-to-face interview of het bezoek van een mystery guest geen meerwaarde. Omdat men zich precies aan de vragenlijst en voorgekauwde antwoorden moet houden worden de voordelen van het gebruik van een face-to-face interview en de mystery guest, het kunnen inspelen op situaties, geblokkeerd.

Het 'Prototype ter meting van informatiebeveiligingsbewustzijn' beschrijft de soort vragen die moeten worden gesteld bij een meting. Daarnaast geeft het uitleg over hoe dit vertaald moet worden tot een score.

Na onderzoek van Kruger en Kearney hebben zij een prototype beschreven voor de opbouw van een beveiligingsbewustzijnsmeetinstrument. Hierbij worden 35 vragen gesteld die ingaan op de kennis, houding en gedrag van medewerkers. Per aspect richt hun model zich verder op zes verschillende gebieden. De 'zes kritische risicogebieden' zoals zij het noemen. Het gaat om de volgende gebieden:

- altijd voldoen aan het bedrijfsbeleid;
- houd wachtwoorden en persoonlijke identificatienummers geheim;
- gebruik e-mail en het internet met zorg;
- wees voorzichtig bij het gebruik van mobiele apparatuur;
- meld incidenten zoals virussen, diefstallen en verliezen;
- wees u ervan bewust dat menig actie ingrijpende gevolgen kan hebben.

Deze zes gebieden zijn bij toepassing van deze methodiek bij SNS REAAL goed te vervangen door de 7 Gouden regels

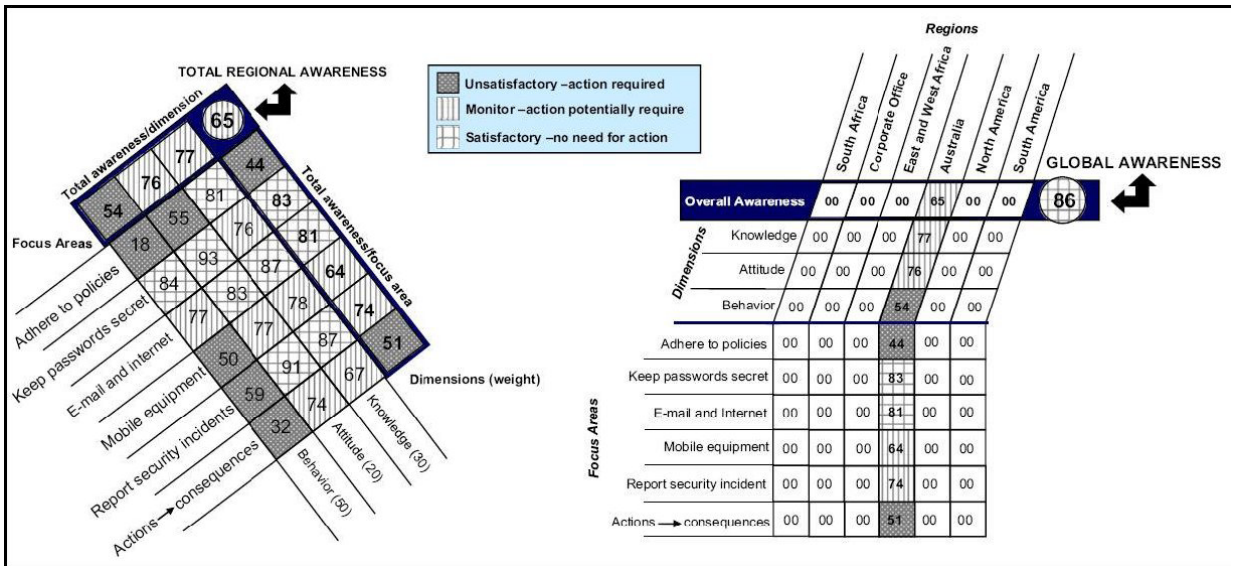
De belangrijkste kenmerken van dit model zijn:

- zeer gedetailleerd resultaat, zowel in de breedte als in de diepte;
- complex(er) om op te zetten;
- kost veel tijd om wegingen te bepalen;
- hoge herbruikbaarheid;
- makkelijk te gebruiken.

[33] Bron: H. A. Kruger, W.D. Kearney: A prototype for assessing information security awareness (2006)

In Figuur 5 is een voorbeeld gegeven van de uitkomst van een meting. In de linker tabel staan op de linker diagonale lijnen de zes kritische risicogebieden en op de rechter diagonale lijnen de drie dimensies (kennis, houding en gedrag). De linker tabel gaat over de scores van een vestiging. De getallen in de vakjes gaan over het percentage medewerkers dat een vraag correct heeft beantwoord. Als dit vakje op de kruising ligt tussen de linker diagonale rij 'Adhere to policies' (altijd voldoen aan het bedrijfsbeleid) en de rechter diagonale rij 'Behaviour' (gedrag), dan blijkt dat 18% van de ondervraagden de gedragsvra(a)g(en) met betrekking tot het altijd voldoen aan het bedrijfsbeleid goed heeft beantwoord.
In de bovenste linker diagonale rij 'Total awareness/dimension' (totale beveiligingsbewustzijn per dimensie) wordt per dimensie het percentage goed beantwoorde vragen berekend. In de bovenste rechter diagonale rij 'Total awareness/focus area' (totale beveiligingsbewustzijn per kritisch risicogebied) wordt per risicogebied het percentage goed beantwoorde vragen berekend.
Zoals eerder is gemeld zijn niet alle dimensies even belangrijk, daarom heeft iedere dimensie voor het berekenen van de (totale) score(s) een weegfactor. De weegfactor voor gedrag is 0,5, voor houding 0,2 en voor kennis 0,3. Hiermee kan per risicogebied de score berekend worden maar ook de totale score van het beveiligingsbewustzijn, de totale score wordt in het bovenste vakje berekend.

In de rechter tabel in Figuur 6 kan met behulp van de berekende scores uit de rechter tabel een overzicht gemaakt worden van alle vestigingen. Zo is duidelijk te zien waar al dan niet risico's worden gelopen met betrekking tot beveiligingsbewustzijn.



Figuur 6 De uitkomst van een informatiebeveiligingsbewustzijnmeting zoals deze eruit ziet na het onderzoek van Kruger en Kearney.

Deelvraag (✓ = vraag is beantwoord)									
1 ✓	2 ✓	3 ✓	4	5	6	7	8	9	10

Met het bepalen van hoe een meting kan worden gehouden (paragraaf 5.1.2), en hoe deze kan worden opgebouwd (paragraaf 5.1.3) is deelvraag 3 beantwoord.

Deelvraag 3: 'Welke modellen bestaan er om het volwassenheidsniveau van een proces vast te stellen?'

5.1.4. Volwassenheid van het proces

SNS REAAL beschikte nog niet over een volwassenheidsmodel voor het proces Informatiebeveiligingsbewustzijn. Om beter zicht te hebben op hoe goed het proces is georganiseerd en presteert was de wens voor een dergelijk model aanwezig.
Tijdens het onderzoek kwamen de Security Awareness Maturity Tables[34] (SAMT) van ISACA[35] als het meest geschikte model naar voren (zie externe bijlage C). De alternatieven waren het COBIT Generic Maturity Model (volwassenheid IT-beheeromgeving), het Capability Maturity Model (volwassenheid softwareontwikkeling), het OMG Business Process Maturity Model (volwassenheid van processen binnen een procesgeoriënteerde organisatie) en een model gemaakt door Ronald van Erven (volwassenheid van de organisatie betreffende informatiebeveiliging). Maar geen van de alternatieven sloot zo goed aan als de SAMT tabellen.
De SAMT tabellen gaan over het bepalen van het volwassenheidniveau van verschillende vlakken binnen een proces Informatiebeveiligingsbewustzijn. Deze vlakken zijn het beveiligingsbewustzijn binnen de organisatie, het programma ter bevordering van beveiligingsbewustzijn, de organisatie van het proces, de inhoud van het programma, de communicatie door het proces en het aangeboden materiaal ter bevordering van het beveiligingsbewustzijn. Al deze tabellen samen geven het volwassenheidsniveau van het hele proces Informatiebeveiligingsbewustzijn.

De zes tabellen beschikken allemaal over vijf niveaus. Deze niveaus van een lage volwassenheid tot een hoge volwassenheid zijn 'initieel/ad hoc', 'herhaaldelijk maar intuïtief', 'gedefinieerde processen', 'beheerst en meetbaar' en 'geoptimaliseerd'. Binnen deze niveaus en per tabel zijn allerlei kenmerken beschreven waaraan het proces moet voldoen wil het op een bepaald niveau zitten.

Met behulp van deze tabellen kan bepaald worden hoe volwassen het proces Informatiebeveiligingsbewustzijn is, daarnaast biedt het handvaten om het proces te verbeteren. Daarom zijn de SAMT van ISACA het meest geschikt om het volwassenheidsniveau van het proces Informatiebeveiligingsbewustzijn te bepalen.

[34] Bron: Tim Wulgaert (ISACA): Security Awareness: Best practices to serve your enterprise (2005)

[35] De Information Systems Audit and Control Association (ISACA) is een Amerikaanse beroepsvereniging van IT-auditors en informatiebeveiligers.

Deelvraag (✓ = vraag is beantwoord)									
1 ✓	2 ✓	3 ✓	4 ✓	5 ✓	6	7	8	9	10

Met het bepalen van welk volwassenheidsmodel het meest geschikt is voor het proces Informatiebeveiligingsbewustzijn zijn de deelvragen 4 en 5 beantwoord.

Deelvraag 4: 'Welke modellen bestaan er om het volwassenheidsniveau van een proces vast te stellen?'
Deelvraag 5: 'Welk model is het beste geschikt om het volwassenheidsniveau van het proces Informatiebeveiligingsbewustzijn binnen SNS REAAL vast te stellen?

5.1.5. De huidige situatie bij SNS REAAL

Bij het onderzoeken van de huidige situatie kwamen een aantal punten naar voren. In de toenmalige situatie bestond geen vastgelegd en gedocumenteerd proces Informatiebeveiligingsbewustzijn. Wel waren een aantal zaken afgesproken, vastgelegd en beschikbaar. Deze zaken worden hieronder beschreven.

Campagne

In 2007 is door Reinate Gijsberts (afstudeerster) een beveiligingsbewustzijncampagne voor het bedrijfsonderdeel informatiebeveiliging ontwikkeld. Onderdeel van deze campagne is een gedetailleerde planning die tot september 2009 liep.
De planning is gedeeltelijk gevolgd zoals het lanceren van een e-learning module, artikelen plaatsen op Delphi (intranet[36]-site), presenteren van de 7 Gouden regels en cursussen en contactmomenten houden voor de IB coördinatoren. Helaas zijn de meeste activiteiten slechts gedeeltelijk of niet uitgevoerd.

Contactmomenten

Bij de oude gang van zaken werd vastgesteld dat er 24 beveiligingsbewustzijn contactmomenten waren. Van deze 24 momenten stonden de soort activiteiten grotendeels vast en werden ze over het jaar heen uitgevoerd.

Gedocumenteerd

Een aantal zaken lagen formeel vast, bijvoorbeeld dat John Verkooijen (adviseur Informatiebeveiliging) de eindverantwoordelijke was voor informatiebeveiligingsbewustzijn en wie de betreffende IB-coördinatoren waren. Ook was beschreven wat de taken van alle verschillende belanghebbenden waren. Er bestond echter geen document met een complete procesbeschrijving.

Middelen

Uit een opsomming van alle beschikbare middelen werd duidelijk welke soorten middelen er op dat moment beschikbaar waren. De ervaringen met deze middelen zijn te vinden in het onderzoekrapport (zie externe bijlage C):

[36] Een intranet is een intern netwerk binnen een organisatie.

- artikelen voor alle medewerkers;
- brieven aan het management en directie;
- campagnes;
- checklisten;
- (beleid)documenten;
- e-learning module(s);
- enquête(s);
- films;
- folder/flyers;
- give-aways;
- intranet;
- meetinstrument(en);
- nieuwsbrieven;
- presentaties;
- quizzen;
- rapportages (vooral voor het management en directie);
- strips;
- SharePoint[37];
- tafelkaarten;
- workshops.

Intranet/SharePoint

De communicatie verliep d.m.v. van drie verschillende sites, namelijk via Minerva (SharePoint), Delphi (intranet) en ID (Sharepoint). Door het gebruik van drie sites was de communicatie dan ook inefficiënt en ineffectief te noemen, dit is geen ideale situatie.

Deelvraag (✓ = vraag is beantwoord)									
1 ✓	2 ✓	3 ✓	4 ✓	5 ✓	6 ✓	7 ✓	8	9	10

Met het beschrijven van de huidige situatie en het rapporteren van de ervaringen met de huidige middelen zijn de deelvragen 6 en 7 beantwoord.

Deelvraag 6: 'Hoe is het proces Informatiebeveiligingsbewustzijn op dit moment ingericht en welke middelen worden hiervoor gebruikt?'
Deelvraag 7: 'Wat zijn de ervaringen met reeds gebruikte middelen?'

[37] SharePoint is een platform van Microsoft dat dient als een raamwerk voor het opzetten van een website voor informatie-uitwisseling en online samenwerking binnen een groep of organisatie, zoals dat vaak op een intranet gebeurt.

5.1.6. Criteria voor middelen ter verhoging van het beveiligingsbewustzijn

Tijdens het onderzoek zijn bijna honderd nieuwe middelen naar voren gekomen die gebruikt kunnen worden om het beveiligingsbewustzijn te verhogen. Niet alle middelen zijn even interessant om te gebruiken, dit geldt ook voor bestaande middelen binnen SNS REAAL. Daarom zijn een drietal criteria, bedacht voor en afgestemd op de organisatie, opgesteld waaraan een middel moet voldoen om interessant te zijn om te gebruiken.

- Kostenefficiënt te gebruiken:
  - lage 'out of pocket'[38]-kosten;
  - is met zo min mogelijke tijd en inspanning van een informatiebeveiliging medewerker of IB-coördinator in te zetten;
  - doorlooptijd is zo kort mogelijk, het mag de doelgroep niet te veel tijd kosten.

- Effectief en breed inzetbaar:
  - met enige aanpassing bruikbaar op meerdere onderwerpen;
  - zoveel mogelijk meetbare resultaten bij het verhogen van het beveiligingsbewustzijn.

- Hoge acceptatiegraad door doelgroepen:
  - het mag voor de medewerkers geen lastig middel zijn om te 'ondergaan';
  - het moet voor de IB-coördinator niet te moeilijk zijn om het gewenste resultaat te behalen of het middel bruikbaar te houden.

Deelvraag (✓ = vraag is beantwoord)

1 ✓	2 ✓	3 ✓	4 ✓	5 ✓	6 ✓	7 ✓	8 ✓	9	10

Met het opstellen van criteria voor nieuwe middelen is deelvraag 8 beantwoord.

Deelvraag 8: 'Welke criteria zijn van toepassing bij de keuze van middelen voor informatiebeveiligingsbewustzijn?'

5.1.7. Overzicht van alle nieuwe middelen

Alle nieuwe middelen zijn tijdens het onderzoek beoordeeld op de bruikbaarheid binnen SNS REAAL. Door gebruik te maken van de eerder gestelde criteria is beoordeeld welke middelen het meest geschikt zijn om binnen SNS REAAL te gebruiken, hiervan is een overzicht gemaakt. Dit overzicht is later in dit project gebruikt bij de keuze over het al dan niet uitwerken van bepaalde middelen.

[38] De kosten die bijvoorbeeld aan het kopen van een product verbonden zitten, m.a.w. het prijskaartje.

Deelvraag (✓ = vraag is beantwoord)									
1 ✓	2 ✓	3 ✓	4 ✓	5 ✓	6 ✓	7 ✓	8 ✓	9 ✓	10 ✓

Met het opstellen van een overzicht van alle nieuwe middelen zijn de deelvragen 9 en 10 beantwoord.

Deelvraag 9: 'Welke middelen voor informatiebeveiligingsbewustzijn zijn er op de markt, op basis van welke principes werken deze en hoe verhouden ze zich tot elkaar?'
Deelvraag 10: 'Welke van deze middelen passen het beste bij SNS REAAL?'

5.2. Conclusie en aanbevelingen onderzoek

Het onderzoek is uitgevoerd omdat de volgende vraag voor het verbeteren van het proces Informatiebeveiligingsbewustzijn beantwoord moest worden:

'Waar liggen voor SNS REAAL de kansen om het proces Informatiebeveiligingsbewustzijn efficiënt en meetbaar over het hele concern in te richten?'

Als naar de oude situatie van het proces Informatiebeveiligingsbewustzijn wordt gekeken ontbraken er nog een aantal belangrijke zaken waardoor het een onvoldoende efficiënt en beperkt meetbaar ingericht proces was. Meerdere middelen ter verhoging van het bewustzijn bestonden, maar qua beschikbaarheid viel nog veel resultaat te halen. Het bestaan van drie verschillende sites, waarop voor de IB-coördinator, een normale medewerker met extra verantwoordelijkheden, redelijk ongeorganiseerd middelen ter verhoging van het bewustzijn waren geplaatst, zorgde ervoor dat de sites voor een aantal verbeteringen vatbaar waren. Daarnaast waren veel beschikbare middelen verouderd, daarom moest een keuze worden gemaakt of ze nog up-to-date waren en of ze nog pasten in het uniforme beeld dat IB wil uitdragen.
Een belangrijke factor bij het efficiënt en effectief kunnen sturen van een proces is dat het proces vastgelegd en daardoor bekend is. In de oude situatie bestond geen document die het proces beschreef, maar een aantal losse documenten die een deel van het proces betreffende Informatiebeveiligingsbewustzijn beschreven, dit was op zijn minst onhandig te noemen.

Om deze reden is aan het einde van het onderzoek een aantal aanbevelingen gedaan richting SNS REAAL, en in het bijzonder aan het bedrijfsonderdeel Informatiebeveiliging:

1. Procesbeschrijving maken:
a. voor het proces Informatiebeveiligingsbewustzijn:
i. simpel en duidelijk;
ii. waarin de principes van onderstaande aanbevelingen 2 t/m 5 zijn opgenomen.

2. Standaardiseren:
a. de Security Awareness Maturity Tables gebruiken om het volwassenheidsniveau van het proces Informatiebeveiligingsbewustzijn te bepalen en verhogen.

3. Verbeteren proces:
a. het proces Informatiebeveiligingsbewustzijn verbeteren aan de hand van de Security Awareness Maturity Tables, en door:
i. structureel jaarlijks voor het begin van een nieuw kalenderjaar een planning te maken voor het verhogen van het beveiligingsbewustzijnsniveau, in deze planning contactmomenten en inzet van bewustzijnsmiddelen in te plannen;

4. Meten is weten:
a. één of meerdere doelgroep specifieke (online) enquêtes/vragenlijsten opstellen om het beveiligingsbewustzijnsniveau te kunnen meten;
b. de (online) enquêtes/vragenlijsten opbouwen volgens het 'Prototype ter meting van informatiebeveiligingsbewustzijn'
c. de (online) enquêtes/vragenlijsten zo opbouwen dat ze met enige aanpassing toepasbaar zijn voor meerdere onderwerpen;
d. bij face-to-face interviews of de inzet van een mystery guest resultaten verwoorden in de niveaus beschreven in het Information Security Competence Maturity Model;
e. jaarlijks het beveiligingsbewustzijnsniveau t.o.v. het gewenste beveiligingsbewustzijnsniveau analyseren, bij negatieve discrepanties maatregelen treffen.

5. Middelen ter verhoging van het beveiligingsbewustzijn:
a. een schifting maken in de huidige beschikbare middelen ter verhoging van het bewustzijn op:
i. actualiteitsgehalte;
ii. ervaringen IB-medewerkers, IB-coördinatoren en managers.

	b. lijst van middelen ter verhoging van het bewustzijn verrijken met nieuwe middelen;
	c. alle huidige middelen aanpassen en alle nieuwe middelen maken in de huisstijl van SNS REAAL;
	d. de drie sites samen integreren tot één site op ID, daarbij letten op:
	i. de verschillende doelgroepen;
	ii. eenduidige overzichtelijke opslag.

Deel van de doelstelling (✓ = deel is beantwoord)		
1/3 ✓	2/3	3/3
Met het afronden van het onderzoekrapport is het eerste deel van de doelstelling van dit project behaald. Het eerste deel van de doelstelling is: *'Tijdens dit project moet duidelijk worden waar voor SNS REAAL kansen liggen om het proces Informatiebeveiligingsbewustzijn meer volwassen te maken. Daarnaast moet er een geschikt model gekozen worden om het volwassenheidsniveau aantoonbaar te kunnen maken…'*		

6. Uitvoeringsfase Deel II: De Sites

In dit hoofdstuk wordt de integratie van de drie sites naar één centrale site op ID beschreven. Op het einde zal met een soortgelijke tabel als bij de deelvragen kenbaar worden gemaakt welke aanbeveling is uitgewerkt en welk delen van de doelstelling zijn voltooid.

6.1. Integreren naar één centrale site

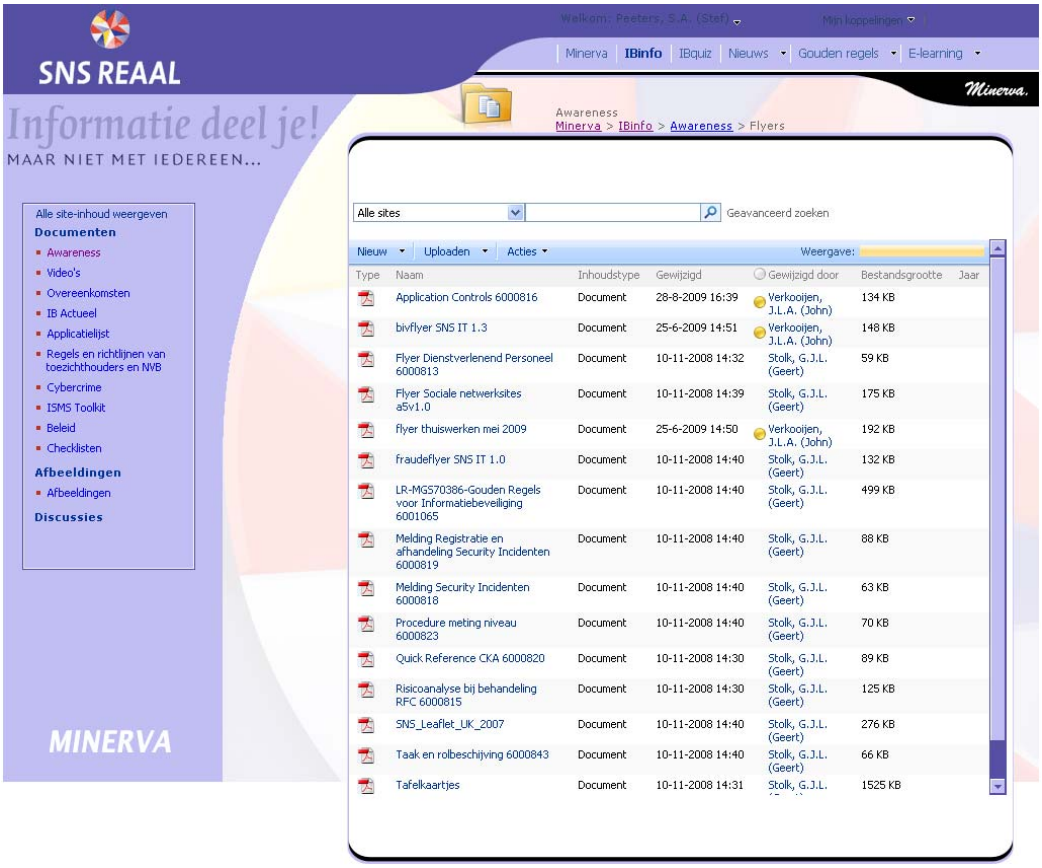
Voor de start van dit project verliep een deel van de communicatie van het bedrijfsonderdeel Informatiebeveiliging via drie sites. Uit het onderzoek bleek dat dit geen efficiënte manier van werken is. Daarom werd al snel duidelijk dat dit tot één centrale site geïntegreerd moest worden. De drie sites waren Delphi (intranet), Minerva (SharePoint) en ID (SharePoint).

6.1.1. Voor de integratie

Delphi was de oude intranet site van SNS REAAL (zie Figuur 7). Hierop konden alle organisatie- en bedrijfs(onder)delen hun algemene informatie plaatsen. Ook bood Delphi de mogelijkheid om allerlei actuele informatie, zoals een nieuwsbrief, te tonen.
Heel de site was voor alle medewerkers binnen SNS REAAL toegankelijk. Dit had als nadeel dat je vertrouwelijke informatie niet via dit medium kon verspreiden, want informatie en kennis alleen voor bepaalde doelgroepen beschikbaar stellen was niet mogelijk. Aan het onderhouden van de site, m.a.w. het plaatsen van nieuwe informatie, was een nadeel verbonden: dit verliep via een sitebeheerder. Het was niet mogelijk voor organisatie- en (bedrijfs)onderdelen om zelf hun site te onderhouden, simpel en snel aanpassen was dus niet mogelijk. Daarnaast was door de jaren heen de uitstraling van de site sterk verouderd.

Figuur 7 Een screenshot van de intranetsite Delphi.

Minerva was de oude SharePoint site van het bedrijfsonderdeel Informatiebeveiliging (zie Figuur 8). Hierop kon men allerlei informatie en kennis delen die voor de medewerkers en IB-coördinatoren van SNS REAAL interessant waren. Zo bood Minerva de mogelijkheid om gesorteerd op soort middelen ter verhoging van het beveiligingsbewustzijn, beleidsdocumenten en handige tools voor IB-coördinatoren te plaatsen. Daarnaast was in Minerva een aantal e-learning modules ingebouwd, hiermee kon Informatiebeveiliging het beveiligingsbewustzijn onder medewerkers verhogen. In tegenstelling tot Delphi was het binnen Minerva wel mogelijk om bepaalde documenten alleen voor bepaalde doelgroepen beschikbaar te maken. IB had Minerva zelf in beheer, ze konden de site dus aanpassen aan hun eigen wensen en eisen. Daarom was het onderhoudstechnisch een goede site.



Figuur 8 Een screenshot van de SharePoint site van IB.

ID is de nieuwste SharePoint-omgeving van heel SNS REAAL (zie Figuur 9). SNS REAAL is één concern. Daarom is gekozen voor één SharePoint omgeving met één design en één structuur. Met de nieuwe site heeft elke medewerker zelf de regie over het ophalen en aanbieden (push & pull) van informatie en kennis: ‘power to the people’ staat centraal. Er wordt uitgegaan van openbaarheid van informatie en werken met organisatiebrede kennisdeling. Elk organisatie- en (bedrijfs)onderdeel kan zelf informatie en documenten plaatsen en heeft dus de mogelijkheid om al hun kennis met de organisatie te delen. Daarnaast is het mogelijk informatie en kennis alleen voor bepaalde groepen beschikbaar te maken. Zo kunnen werkgroepen met behulp van ID efficiënter samenwerken.

Figuur 9 Een screenshot van de SharePoint omgeving van SNS REAAL.

ID is organisatiebreed geïmplementeerd om over het hele concern informatie- en kennisdeling mogelijk te maken. Daarvoor is het een vereiste dat alle intranet en SharePoint sites binnen SNS REAAL overgaan naar ID; de directie heeft deze overgang verplicht gesteld. Een van de projectresultaten is derhalve het integreren van de centrale site van IB binnen ID.

6.1.2. De centrale site: de voorbereiding

Voordat gestart werd met het realiseren van deze integratie binnen ID moest er geïnventariseerd worden welke informatie en kennis op dat moment op Delphi en Minerva stond.

Op Delphi stond veel verouderde informatie zoals oude artikelen en nieuwsbrieven. Dit hoefde niet verwerkt te worden op ID. Wat wel interessant was om te verwerken was een grote hoeveelheid aan algemene informatie, zoals beschrijvingen wat informatiebeveiliging is en hoe medewerkers daaraan mee kunnen werken. ID biedt de mogelijkheid om wiki-pagina's aan te maken, deze pagina's zijn bedoeld om met een simpele HTML-pagina informatie en kennis te delen. Dit is een ideale manier om deze algemene informatie beschikbaar te maken op ID.

Minerva was zoals eerder gemeld de SharePoint site. Hierop waren vooral veel middelen ter verhoging van het beveiligingsbewustzijn, beleidsdocumenten en handige tools voor IB-coördinatoren te vinden. Deze middelen konden ook op ID geplaatst worden.

6.1.3. De centrale site: de eerste versie

In het begin was het vooral noodzaak om de informatie en kennis van Delphi in ID te verwerken. Delphi zou binnen afzienbare tijd worden gesloten. Alles wat nog op Delphi stond zou verloren gaan als dit niet op tijd werd veiliggesteld. De eerste versie was zeer simpel maar overzichtelijk (zie Figuur 10).

Figuur 10 Het eerste wiki-menu op ID.

Door op een hyperlink te klikken kan men naar een volgende pagina gaan. Als bijvoorbeeld gekozen wordt voor ‘Informatiebeveiliging algemeen’ belandt men op de pagina waarop allerlei algemene zaken met betrekking tot informatiebeveiliging staan (zie Figuur 11).

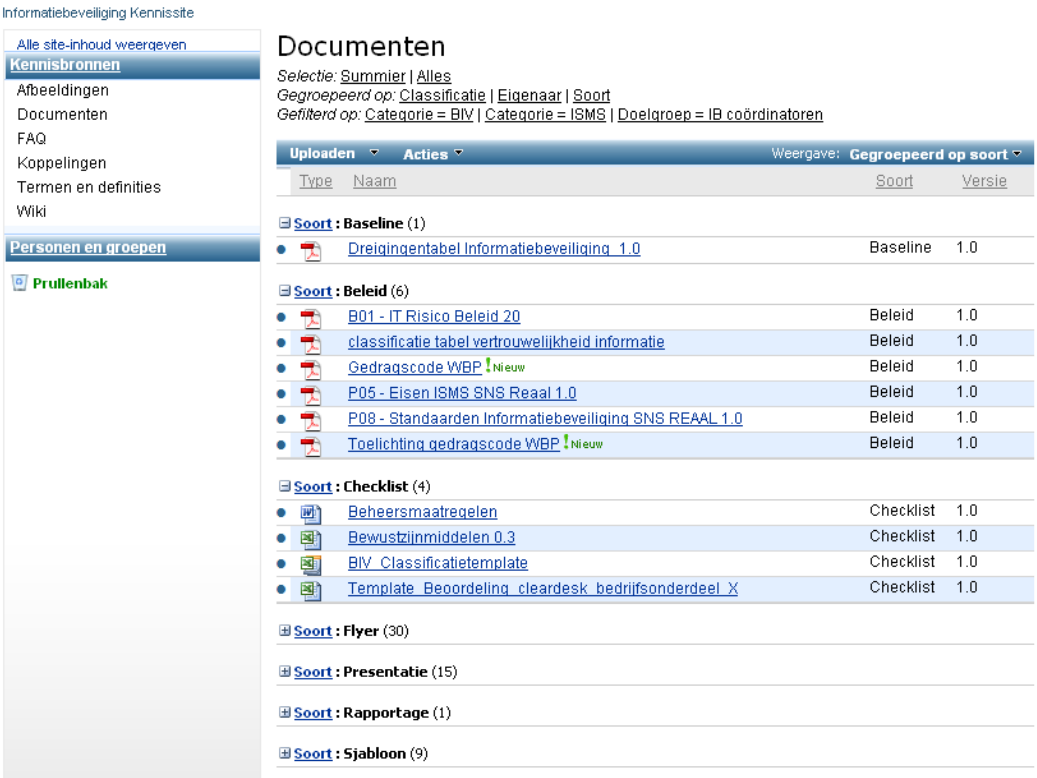
Figuur 11 ‘Algemene informatie’ op het wiki-deel.

Men kan dan doorklikken naar een volgend onderwerp, bijvoorbeeld ‘Wat is informatiebeveiliging?’ (zie Figuur 12).

Figuur 12 'Wat is informatiebeveiliging?' op het wiki-deel.

Alle middelen ter verhoging van het beveiligingsbewustzijn, beleidsdocumenten en handige tools voor IB-coördinatoren van Minerva moesten ook op ID een plaats krijgen. Deze middelen waren tijdens het onderzoek geïnventariseerd en beoordeeld op hun actualiteitsgehalte. Hiervan was een overzicht gemaakt. Hierin stonden ook middelen van de afdelingsschijf, dit is een locatie op de server waarop Informatiebeveiliging al haar documenten bewaard. Zodoende kon in één keer alle beschikbare middelen op ID geplaatst worden.

Binnen ID bestaat de mogelijkheid om alle documenten en bestanden overzichtelijk op één locatie te plaatsen, deze locatie heet 'Documenten' (zie Figuur 13). Hierop zijn alle beschikbare middelen geplaatst.
Bij het uploaden moet ook worden aangegeven wat voor soort document het is en wie de doelgroep is. Zo ontstaan specifieke overzichten voor meerdere doelgroepen. Alle middelen die in deze fase zijn toegevoegd behoorden tot de doelgroepen 'IB-coördinatoren' en/of 'Medewerkers SNS REAAL'.



Figuur 13 Documenten en middelen op ID.

De e-learning modules van Minerva zijn niet overgeplaatst naar ID. Deze modules waren ingebakken in Minerva, het overplaatsen zou niet onhaalbaar maar wel lastig zijn. Echter de belangrijkste reden om ze niet over te plaatsen was dat de modules niet meer actueel waren. SNS REAAL had in de afgelopen jaren door het bedrijf InfoSecure een aantal e-learning modules laten maken. Deze zijn op een internet server van SNS REAAL geplaatst en zijn via een wiki-pagina beschikbaar op ID (zie Figuur 14).

Figuur 14 Het e-learning menu op ID.

6.1.4. De centrale site: een nieuwe uitstraling

Nadat de eerste versie gereed was belandde het project in de volgende fase. De kennissite van ID moest er aantrekkelijk gaan uitzien. Als een medewerker van SNS REAAL op de site terecht komt moet voor hem meteen duidelijk worden waar voor hem de interessante informatie staat. Hij moet worden geprikkeld om verder te kijken. Daarom is er besloten om gebruik te maken van toepasselijke en kleurrijke plaatjes. Als men dan met de muis over een plaatje beweegt wordt een korte uitleg over dat onderwerp zichtbaar (zie Figuur 15).

Er ontstond echter weerstand tegen de nieuwe uitstraling. Voor het beheer van de IB site op ID zijn drie medewerkers van IB verantwoordelijk. Zij moeten toestemming geven voor wijzigingen op ID. Twee van de drie waren niet tevreden over de ontworpen plaatjes. Helaas hebben zij pas na het einde van dit project tijd om over een nieuwe uitstraling mee te denken. Daarom lag de verdere ontwikkeling van de kennissite op ID tot het einde van dit project stil. De voorlopige versie van de nieuwe uitstraling is om de IB-coördinatoren op de IB-coördinatordag in mei jl. toch een indruk te geven wel doorgevoerd.

Overige nieuwe ideeën voor de site zoals het plaatsen van een forum, het ontwikkelen van uploadmogelijkheden voor rapportages en jaarplannen van IB-coördinatoren, en het vereenvoudigen van plaatsen van nieuwe informatie door IB-medewerkers zijn daarom ook niet meer uitgewerkt.

Figuur 15 De nieuwe uitstraling van de kennissite Informatiebeveiliging op ID.

Deel van de doelstelling (✓ = deel is beantwoord)		
1/3 ✓	2/3	3/3 ✓

Met het integreren van de drie sites naar één centrale site op ID is het laatste deel van de doelstelling van dit project behaald en is aanbeveling 5.d uit het onderzoek uitgewerkt. Het laatste deel van de doelstelling is:

'…Dit wordt onder andere bereikt door het bouwen van één centrale site, hierop moeten alle materialen m.b.t. het onderwerp informatiebeveiligingsbewustzijn binnen SNS REAAL gepost kunnen worden.'

Aanbevelingen uit het onderzoek (✓ = aanbeveling is uitgewerkt)

1.	2.	3.	4.a.	4.b.	4.c.	4.d.	4.e.	5.a.	5.b.	5.c.	5.d. ✓

7. Uitvoeringsfase Deel III: Het Proces

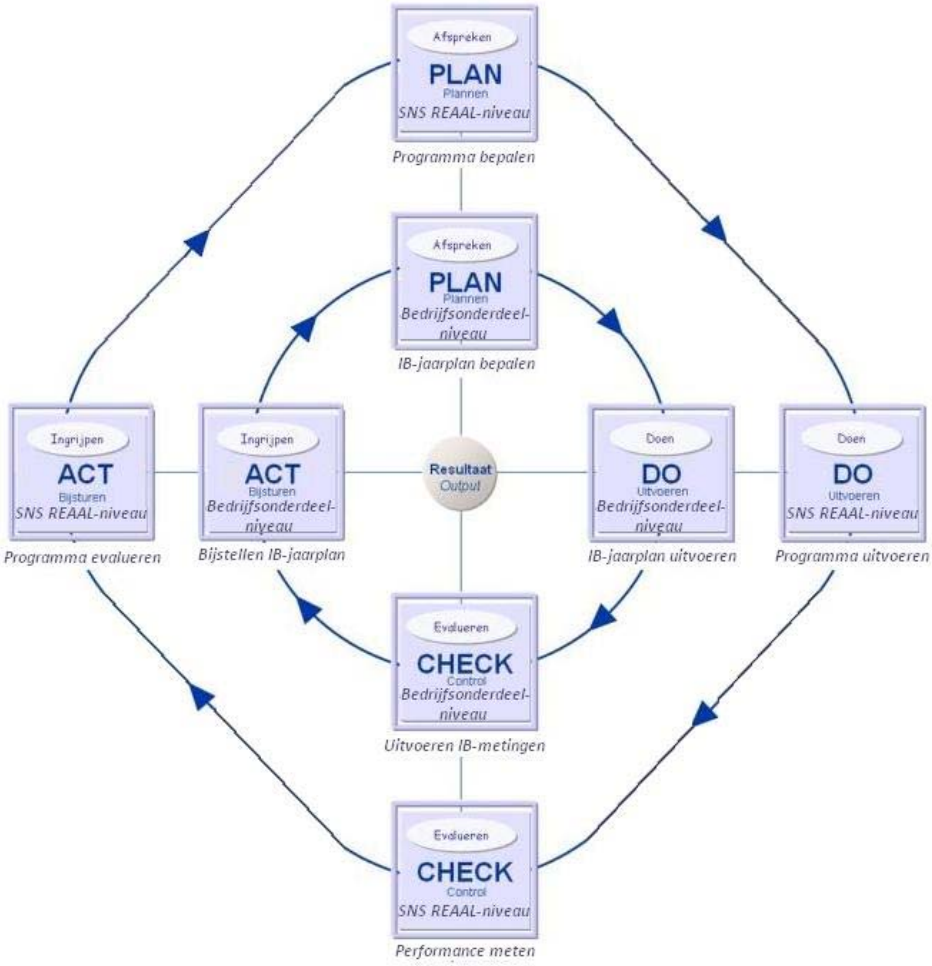
In dit hoofdstuk wordt de opgestelde procesbeschrijving beschreven. Op het einde zal wederom kenbaar worden gemaakt welke aanbevelingen zijn uitgewerkt en welk delen van de doelstelling zijn voltooid.

7.1. Opstellen van de procesbeschrijving

Bij het onderzoek kwam naar voren dat SNS REAAL nog niet over een procesbeschrijving van het proces Informatiebeveiligingsbewustzijn beschikte. Om het proces naar een hoger volwassenheid te brengen was dit een belangrijke stap. Hierin konden bepaalde eisen voor een volwassen proces worden vastgesteld en gedocumenteerd. Alle aanbevelingen die van toepassing waren op de procesbeschrijving zijn hierin dan ook verwerkt.

De procesbeschrijving (zie externe bijlage D) is opgedeeld in twee niveaus. Het eerste niveau is het SNS REAAL-niveau waarin alle activiteiten worden beschreven die verricht worden door het bedrijfsonderdeel Informatiebeveiliging. Het tweede niveau is het bedrijfsonderdeel-niveau waarin alle activiteiten worden beschreven die decentraal door de verschillende bedrijfsonderdelen worden uitgevoerd. De keuze voor deze deling is gemaakt om het overzichtelijker te maken, zo is duidelijk door wie welke activiteiten worden uitgevoerd. Het proces is op beide niveaus beschreven als een plan-do-check-act (PDCA)[39] cyclus (zie Figuur 16). Deze cyclus duurt één jaar.

[39] De cirkel beschrijft vier activiteiten die zorgen voor een betere kwaliteit. Het cyclische karakter garandeert dat er continu kwaliteitsverbetering is.



Figuur 16 Visuele uitleg beide niveaus van de PDCA-cyclus van het proces Informatiebeveiligingsbewustzijn.

7.1.1. Plan-fase

Het doel van deze fase is het opzetten van een goedgekeurd informatiebeveiligingsbewustzijn programma waaraan het management zijn commitment[40] wil geven. Daarnaast moet per bedrijfsonderdeel een goedgekeurd IB-jaarplan worden opgesteld. In beide plannen staan alle activiteiten voor het komende jaar beschreven. Bij het IB-jaarplan worden deze activiteiten door elke IB-coördinator decentraal ingevuld.

SNS REAAL-niveau

Op dit niveau begint het bedrijfsonderdeel Informatiebeveiliging met het analyseren van de discrepantie tussen het volwassenheidsniveau waarop het proces zich bevindt en waarop het wil zitten. Hieruit worden conclusies getrokken en aanbevelingen gemaakt voor het beveiligingsbewustzijn programma voor komend jaar. In het geval van een negatief verschil zal een tandje bijgezet moeten worden.

[40] Hoge mate van betrokkenheid.

Met behulp van de aanbevelingen uit de analyse wordt het programma voor komend jaar bepaald. Dit moet worden goedgekeurd door het afdelings- of bedrijfshoofd IB, zij zijn de procesbeheerder en -eigenaar en zijn zo 'in control' over wat het proces uitvoert. Dit is een kenmerk van een volwassen proces.
Daarnaast moet voor de effectiviteit van het programma commitment van het management zijn. Zonder commitment wordt het uitvoeren van een dergelijk programma lastig. In een organisatie als SNS REAAL ontstaan veel nieuwe plannen die medewerkers extra tijd kosten. Als al deze plannen klakkeloos worden uitgevoerd wordt het voor medewerkers lastig om nog aan hun dagelijkse werkzaamheden te komen. Om medewerkers niet te overspoelen met extra werk moet toestemming worden gegeven vanuit het management. Dit gebeurt door de noodzaak van een dergelijk programma door het management te laten onderstrepen, met andere woorden: er moet commitment vanuit het mamagement zijn.

Bedrijfsonderdeel-niveau

Per bedrijfsonderdeel wordt een IB-jaarplan gemaakt. Dit plan beschrijft de activiteiten die het komende jaar door de IB-coördinator en de desbetreffende leidinggevende worden uitgevoerd. Hiervoor bestaat een template IB-jaarplan waarin alle mogelijke activiteiten staan beschreven. De IB-coördinator moet een aantal zaken uit deze template kiezen en bepalen wanneer hij deze uitvoert. Ook het IB-jaarplan moet worden goedgekeurd door het management van het bedrijfsonderdeel.

7.1.2. Do-fase

Het doel van deze fase is om het niveau van informatiebeveiligingsbewustzijn op of boven het gewenste niveau te krijgen en daar ook te houden.

SNS REAAL-niveau

Het grootste deel van de tijd houdt IB zich bezig met het uitvoeren van het programma. Zij houden zich dan bezig met activiteiten zoals het opleiden van IB-coördinatoren, het realiseren van IB-contactmomenten, artikelen schrijven voor de IB-actueel (nieuwsbrief), rapporteren over het beveiligingsbewustzijnsniveau, etc.
Daarnaast moet het pakket aan middelen ter verhoging van het beveiligingsbewustzijn up-to-date gehouden worden. Dit houdt in dat verouderde middelen worden verwijderd van de kennissite op ID en wordt verrijkt met nieuwe middelen.
Tijdens deze fase biedt IB ook nog ondersteuning voor IB-coördinatoren en managers bij het verhogen of op peil houden van het beveiligingsbewustzijnsniveau.

Bedrijfsonderdeel-niveau

De IB-coördinatoren voeren door het jaar heen het IB-jaarplan uit. Zij houden zich dan bezig met activiteiten zoals het uitdelen van flyers, uitvoeren van clear desk/clear screen controles, metingen van beveiligingsbewustzijn uitvoeren, etc. Daarnaast fungeren zij voor managers en medewerkers als eerste aanspreekpunt betreffende informatiebeveiliging. En bieden zij ondersteuning zodat managers en medewerkers informatiebeveiliging kunnen realiseren.

7.1.3. Check-fase

Het doel van deze processtap is het meten van het beveiligingsbewustzijn nadat het programma en het IB-jaarplan zijn uitgevoerd. Met deze gegevens kan bekeken worden hoe goed het proces heeft gefunctioneerd.

SNS REAAL-niveau

Voor het meten van het beveiligingsbewustzijn zijn meetinstrumenten gemaakt. Deze meetinstrumenten moeten hiervoor gebruikt worden. Nadat een meting is voltooid moet deze geëvalueerd worden op de betrouwbaarheid van de gegevens, m.a.w. geeft het meetinstrument het juiste beeld. Deze evaluatie wordt in de volgende fase gebruikt.
Daarnaast wordt in deze fase gecontroleerd in hoeverre de KPI's[41] van het proces zijn behaald, KPI's als behaalde beveiligingsbewustzijnsniveaus en behaalde jaarplanning.

Bedrijfsonderdeel-niveau

Ook de IB-coördinator houdt zich bezig met meetinstrumenten. In de IB-halfjaarrapportage rapporteren zij samen met de leidinggevende over allerlei zaken omtrent informatiebeveiliging, zoals management commitment, kennis en houding van IB-coördinator, uitvoeren beveiligingsbewustzijnsactiviteiten, etc.
Ook voert de IB-coördinator een enquête onder hun leidinggevende of collega's uit, mits dit is vastgesteld in het IB-jaarplan. Met behulp van deze enquête kunnen zij aantonen dat het beveiligingsbewustzijn op een goed niveau is.

7.1.4. Act-fase

Het doel van deze processtap is het bepalen van in hoeverre het huidige niveau van beveiligingsbewustzijn en de volwassenheid van het proces voldoet aan het gewenste niveaus.

SNS REAAL-niveau

Als uit de evaluatie van de meting is gebleken dat deze niet het gewenste beeld geeft dan moet het meetinstrument mogelijk worden aangepast. Het kan voorkomen dat bepaalde vragen uit het meetinstrument niet meer up-to-date zijn. Daarnaast is het niet aan te raden telkens dezelfde vragen te stellen. Medewerkers kunnen hierdoor de vragen bewust positiever beantwoorden.

[41] Key performance indicators, zijn variabelen om prestaties van ondernemingen te analyseren.

In deze fase wordt ook nog geanalyseerd of de huidige beveiligingsbewustzijnniveaus voldoen. Samen met de KPI-rapportage uit de vorige fase worden hieruit conclusies en aanbevelingen geformuleerd voor het programma van volgend jaar.

Bedrijfsonderdeel-niveau

In deze fase wordt door de IB-coördinator alleen ingegrepen als blijkt uit de rapportage of enquêtes uit de vorige fase dat er iets niet goed gaat. In dat geval moet het IB-jaarplan worden aangepast.

7.1.5. Afronding procesbeschrijving

Op het moment van schrijven bevindt de procesbeschrijving zich nog in een concept status. De laatste versie moet nog door het afdelingshoofd worden beoordeeld, mogelijk is er dan nog feedback en zijn er kleine aanpassingen nodig.

Hierdoor loopt ook een ander plan enige vertraging op: het maken van een flyer. Om de IB-coördinator niet te overspoelen met een stortvloed aan voor hem grotendeels irrelevante informatie uit de procesbeschrijving, is besloten om een flyer op te stellen. In deze flyer zal met behulp van een visuele weergave kort en bondig uit worden gelegd wat precies zijn taken zijn en hoe hij deze kan uitvoeren. Voordat hieraan begonnen kan worden moet de procesbeschrijving echter de definitieve status hebben.

Deel van de doelstelling (✓ = deel is beantwoord)											
1/3 ✓			2/3 ✓			3/3 ✓					
Met het opstellen van de procesbeschrijving is het tweede (en daarmee alle delen) van de doelstelling van dit project behaald en is aanbeveling 1. uit het onderzoek uitgewerkt. Het tweede deel van de doelstelling is: *´…Door het uitwerken van deze kansen zal het proces Informatiebeveiligingsbewustzijn aan het einde van dit project op een hoger volwassenheidsniveau functioneren…´*											
Aanbevelingen uit het onderzoek (✓ = aanbeveling is uitgewerkt)											
1. ✓	2.	3.	4.a.	4.b.	4.c.	4.d.	4.e.	5.a.	5.b.	5.c.	5.d. ✓

8. Uitvoeringsfase Deel IV: Nieuwe Middelen

In dit hoofdstuk worden de nieuwe middelen beschreven. Als er een aanbeveling is uitgewerkt wordt dit kenbaar gemaakt.

8.1. Nieuwe middelen

Tijdens dit project zijn meerdere middelen ontwikkeld die het bedrijfsonderdeel Informatiebeveiliging kan inzetten bij het verhogen van het informatiebeveiligingsbewustzijn. Ook zijn er twee enquêtes en twee tools (door)ontwikkeld waarmee SNS REAAL efficiënt en meetbaar kan werken.

8.1.1. Handleidingen

Tijdens het onderzoek zijn meerdere activiteiten naar voren gekomen die voor het proces Informatiebeveiligingsbewustzijn op beide niveaus interessant en leuk zijn om uit te voeren. Deze activiteiten dragen allen bij aan het verhogen van het beveiligingsbewustzijn.

Voor het uitvoeren van deze activiteiten zijn handleidingen geschreven. Aan de hand van deze handleidingen is het voor een medewerker van Informatiebeveiliging of een IB-coördinator makkelijker om deze uit te voeren. In deze handleiding wordt kort omschreven wat de activiteit inhoudt en het doel is. Daarna wordt ingegaan hoe men deze activiteit moet uitvoeren en waar op gelet moet worden.

Er zijn handleidingen (zie Figuur 17) geschreven voor:

- Korte doelgerichte sessies: in een kort tijdbestek meerdere keren per week/maand medewerkers kort inlichten over informatiebeveiliging.
- Story telling: vragen om ervaringen van medewerkers over bv. virussen, phishing, social engineering e.d. en deze verspreiden via SharePoint, een nieuwsbrief of een ander medium.
- Informatiebeveiligingsdag: roep een informatiebeveiligingsdag/week uit, plan tijdens deze dag meerdere activiteiten die te maken hebben met informatiebeveiliging.
- Rondetafelgesprekken: via begeleide gesprekken bij een bedrijfsonderdeel kunnen problemen worden getackeld en kan ervoor worden gezorgd dat de neuzen weer dezelfde kant op wijzen.

SNS REAAL

Informatie deel je!
MAAR NIET MET IEDEREEN...

Privé gerelateerde scenario's
Handleiding

Communicatierichting: Informeren
Doelgroep: Medewerkers
Korte omschrijving: Beveiligingsproblemen relateren aan onderwerpen die met privé zaken te maken hebben zodat ze beter in de gaten hebben wat het belang van informatiebeveiliging is.

Doel
Beveiligingsproblemen tastbaarder maken door ze te relateren aan onderwerpen die met privé zaken te maken hebben.

Aanpak
1. Stel het probleem vast, bv.: 'Beveiligingsincidenten worden niet gemeld bij de Servicedesk/Helpdesk.'.
2. Baseer hier een privé gerelateerd scenario op, bv.:'In uw huis wordt ingebroken.'.
3. Leg de overeenkomsten tussen het probleem en het privé scenario uit, bv.:'Op het moment dat bij u thuis wordt ingebroken wilt u dat dit in de toekomst wordt verkomen. Door de politie te bellen kan de dief gepakt en vervolgd worden hierdoor wordt de kans op herhaling bij de desbetreffende dief verkleind, daarnaast wordt een precedent geschept voor potentiële dieven. Ook kunt u de inbraak melden bij een beveiligingsbedrijf, zij kunnen dan uw huis controleren op zwakke plekken in de beveiliging en waar nodig uw huis extra beveiligen. Als u de inbraakpoging niet meldt bij de politie of bij een beveiligingsbedrijf wordt de kans op herhaling niet verkleind, en misschien zelfs vergroot, want dan is bekend hoe in uw huis kan worden ingebroken. Ditzelfde geld voor beveiligingsincidenten op uw werk.
Door een beveiligingsincident te melden bij de Servicedesk/Helpdesk hebben zij dezelfde mogelijkheden, ze kunnen de oorzaak aanpakken en waar nodig de beveiliging aanscherpen.'

Meer Informatie?
Neem contact op met de afdeling Informatiebeveiliging
John Verkooijen
Adviseur Informatiebeveiliging
T: 073-6833457
E: john.verkooijen@sns.nl
E: informatiebeveiliging@sns.nl

Wim Leenheer
Adviseur Informatiebeveiliging
T: 072-5487732
E: wim.leenheer@reaal.nl
E: informatiebeveiliging@reaal.nl

Intern | 4-5-2010 | Concept

Figuur 17 Voorbeeld van een handleiding.

- Posterwedstrijd: houd een informatiebeveiligingsposterwedstrijd.
- Chatsessies: medewerkers kunnen simpel vragen stellen over informatiebeveiliging d.m.v. een kort lijntje via Office Communicator met een medewerker van IB of een IB-coördinator.
- Brainstormsessies: houd brainstormsessies bij bedrijfsonderdelen over informatiebeveiliging.
- Jeopardy!: houd een quiz in de vorm van het Amerikaanse spelshowprogramma 'Jeopardy!'. Hierbij zijn antwoord en vraag omgedraaid.
- Privé-gerelateerde scenario's: beveiligingsproblemen relateren aan onderwerpen die met privézaken te maken hebben. Zodat medewerkers beter in de gaten hebben wat het belang van informatiebeveiliging is.

Met het schrijven van handleidingen voor activiteiten zijn de aanbevelingen 5.b. en 5.c. uit het onderzoek uitgewerkt.

Aanbevelingen uit het onderzoek (✓ = aanbeveling is uitgewerkt)

1. ✓	2.	3.	4.a.	4.b.	4.c.	4.d.	4.e.	5.a.	5.b. ✓	5.c. ✓	5.d. ✓

8.1.2. Informatiebeveiligingsquizen

Om informatiebeveiliging niet als eens saai onderwerp te gaan zien zijn een aantal informatiebeveiligingsquizen ontwikkeld. In een quiz worden zes meerkeuze en/of waar/onwaar vragen gesteld. Zo kan je medewerkers op een speelse manier bezig houden met informatiebeveiliging.

Voorbeeldvragen uit één van de quizen (het vetgedrukte antwoord is het juiste antwoord):

1. Welke van de volgende activiteiten worden gezien als verkeerd gedrag?

a) Het zenden van e-mailberichten om mensen te intimideren of lastig te vallen.

b) Het delen van wachtwoorden.

c) Delen of gebruiken van ongelicenseerde, copyrighteed software.

d) Spieken bij activiteiten van anderen op de computer.

e) Alle antwoorden zijn verkeerd gedrag.

2. Wachtwoorden met een lengte van 3 tot 5 karakters zijn sterk genoeg.

a) Onwaar.

b) Waar.

Met het schrijven van informatiebeveiligingsquizen zijn de aanbevelingen 5.b. en 5.c. uit het onderzoek uitgewerkt.											
Aanbevelingen uit het onderzoek (✓ = aanbeveling is uitgewerkt)											
1. ✓	2.	3.	4.a.	4.b.	4.c.	4.d.	4.e.	5.a.	5.b. ✓	5.c. ✓	5.d. ✓

8.1.3. Give-aways

Tijdens het onderzoek leek het interessant give-aways aan te schaffen. Give-aways zijn dingen, bv. een T-shirt of een zaklamp, met een informatiebeveiligingsboodschap erop vermeld. Dit is een manier om informatiebeveiliging onder de aandacht van de medewerkers te brengen. Tijdens het onderzoek was er echter niet genoeg tijd om een diepgaand marktonderzoek te houden naar give-aways. Toen hier later wel tijd voor was bleek al snel dat de investering die gemaakt moest worden om een aantal give-aways aan te schaffen, te groot was. Daarom is besloten om toch geen give-aways aan te schaffen.

8.1.4. Tipkaarten

Bij de 7 Gouden regels horen vierentwintig tips. Deze tips kunnen op kaartjes (A8 formaat) bij de Reproafdeling worden gedrukt (zie Figuur 18), om daarna uit te delen aan medewerkers. Als een IB-coördinator ziet dat bepaalde regels niet goed worden uitgevoerd, dan kan hij de daarbij horende tips uitdelen.

Figuur 18 Tipkaarten beschikbaar op ID om bij de Reproafdeling af te laten drukken.

Met het ontwerpen van tipkaarten zijn de aanbevelingen 5.b. en 5.c. uit het onderzoek uitgewerkt. Aanbevelingen uit het onderzoek (✓ = aanbeveling is uitgewerkt)											
1. ✓	2.	3.	4.a.	4.b.	4.c.	4.d.	4.e.	5.a.	5.b. ✓	5.c. ✓	5.d. ✓

8.1.5. Posters

Posters zijn goede middelen om het beveiligingsbewustzijn te verhogen. Met een aparte zin en/of een rare foto trekken zij de attentie van een passant. Door een (korte) uitleg wordt duidelijk welke boodschap de poster wil overdragen. Posters kosten de IB-coördinator weinig tijd en dragen bij aan de kennis van informatiebeveiliging. Ze kunnen hangen op plaatsen waar een medewerker voorbij loopt of moet wachten op iets of iemand, zoals bij de koffieautomaat of in de lift.

Voor SNS REAAL zijn twaalf nieuwe posters ontwikkeld voor zes voorbeelden van de posters zie Figuur 19, deze posters zijn voorgelegd aan de IB-coördinatoren. Aan hen is gevraagd om op- en/of aanmerkingen te geven, om zo de posters verder te kunnen doorontwikkelen. Daarnaast mochten de IB-coördinatoren hun top 3 doorgeven, zodat duidelijk werd welke posters de beste zijn. Deze informatie kan gebruikt worden bij het maken van nieuwe posters.
Helaas was er voor het afronden van deze scriptie nog geen tijd voor het verwerken van de op- en/of aanmerkingen en de top 3, daarom wordt hierover niets vermeld in deze scriptie.

Figuur 19 Een aantal voorbeelden van de nieuwe informatiebeveiligingsposters binnen SNS REAAL.

Met het ontwerpen van informatiebeveiligingsposters zijn de aanbevelingen 5.b. en 5.c. uit het onderzoek uitgewerkt.											
Aanbevelingen uit het onderzoek (✓ = aanbeveling is uitgewerkt)											
1. ✓	2.	3.	4.a.	4.b.	4.c.	4.d.	4.e.	5.a.	5.b. ✓	5.c. ✓	5.d. ✓

8.1.6. Stickers

Met behulp van onderstaande sticker is het mogelijk voor IB-coördinatoren om op kasten, whiteboards of elk ander object dat belangrijke informatie kan bevatten een sticker te plakken. Deze sticker vermeldt de boodschap 'Informatie deel je! Maar niet met iedereen…' (zie Figuur 20).

Figuur 20 De sticker 'Informatie deel je! Maar niet met iedereen...'.

Met het ontwerpen van stickers zijn de aanbevelingen 5.b. en 5.c. uit het onderzoek uitgewerkt.											
Aanbevelingen uit het onderzoek (✓ = aanbeveling is uitgewerkt)											
1. ✓	2.	3.	4.a.	4.b.	4.c.	4.d.	4.e.	5.a.	5.b. ✓	5.c. ✓	5.d. ✓

8.1.7. E-learning module

Nieuwe e-learning modules zijn nu simpel te maken. Een op PowerPoint gebaseerd programma Articulate Studio ’09 helpt je bij het maken van nieuwe modules over allerlei onderwerpen. Daarnaast biedt het de mogelijkheid om nieuwe quizen te maken. Na onderzoek bleek dat het bedrijfsonderdeel Kwaliteit & Kennis management voor dit programma een licentie heeft.
Dit programma is SCORM[42] compliant en voldoet dus aan de eisen om aan het leerportaal gekoppeld te worden.

8.1.8. Enquête voor medewerkers

Om de effectiviteit van het proces Informatiebeveiligingsbewustzijn te kunnen bepalen zijn meetinstrumenten een belangrijk middel. Binnen SNS REAAL bestaan hiervoor meerdere meetinstrumenten, bijvoorbeeld de enquête voor leidinggevenden (zie paragraaf 8.1.9). Om het niveau van het beveiligingsbewustzijn onder medewerkers te meten bestond al een online enquête. Een nadeel van deze enquête is dat niet alle vragen actueel zijn. Daarom is een nieuwe enquête ontwikkeld die over de 7 Gouden regels gaat. Met behulp van deze enquête kan bij de medewerkers door het stellen van 21 meerkeuzevragen het beveiligingsbewustzijn gemeten worden. Deze enquête is gebaseerd op de ‘Prototype ter meting van informatiebeveiligingsbewustzijn’ (zie paragraaf 5.1.3).

In de nieuwe enquête wordt per Gouden regel drie vragen gesteld over de drie dimensies (kennis, houding en gedrag). Voor een voorbeeld van de scorelijst na een meting zie Figuur 21. Bij een goed antwoord wordt een ‘1’ verwerkt in de scorelijst en bij een fout antwoord een ‘0’. Daarna kan met behulp van de score en de weegfactoren per dimensie worden berekend wat het beveiligingsbewustzijn is. Ook worden de scores per dimensie en gouden regel berekend. Zo is inzichtelijk op welke gebieden er wel of niet goed wordt gescoord en kan de inzet van middelen ter verhoging van het beveiligingsbewustzijn worden afgestemd op specifieke probleemgebieden.

[42] Is een verzameling standaarden en specificaties die bij e-learning kunnen worden toegepast. Het maakt de communicatie tussen de module en het leerportaal van SNS REAAL mogelijk.

Per dimensie	57%	86%	57%	63%	
Totale beveiligingsbewustzijn				63%	63%
Gouden regel 1	1	1	1		1
Gouden regel 2	0	1	1		0,7
Gouden regel 3	1	1	0		0,5
Gouden regel 4	0	0	1		0,5
Gouden regel 5	1	1	0		0,5
Gouden regel 6	1	1	1		1
Gouden regel 7	0	1	0		0,2
	Kennis (0,3)	Houding (0,2)	Gedrag (0,5)		Per regel

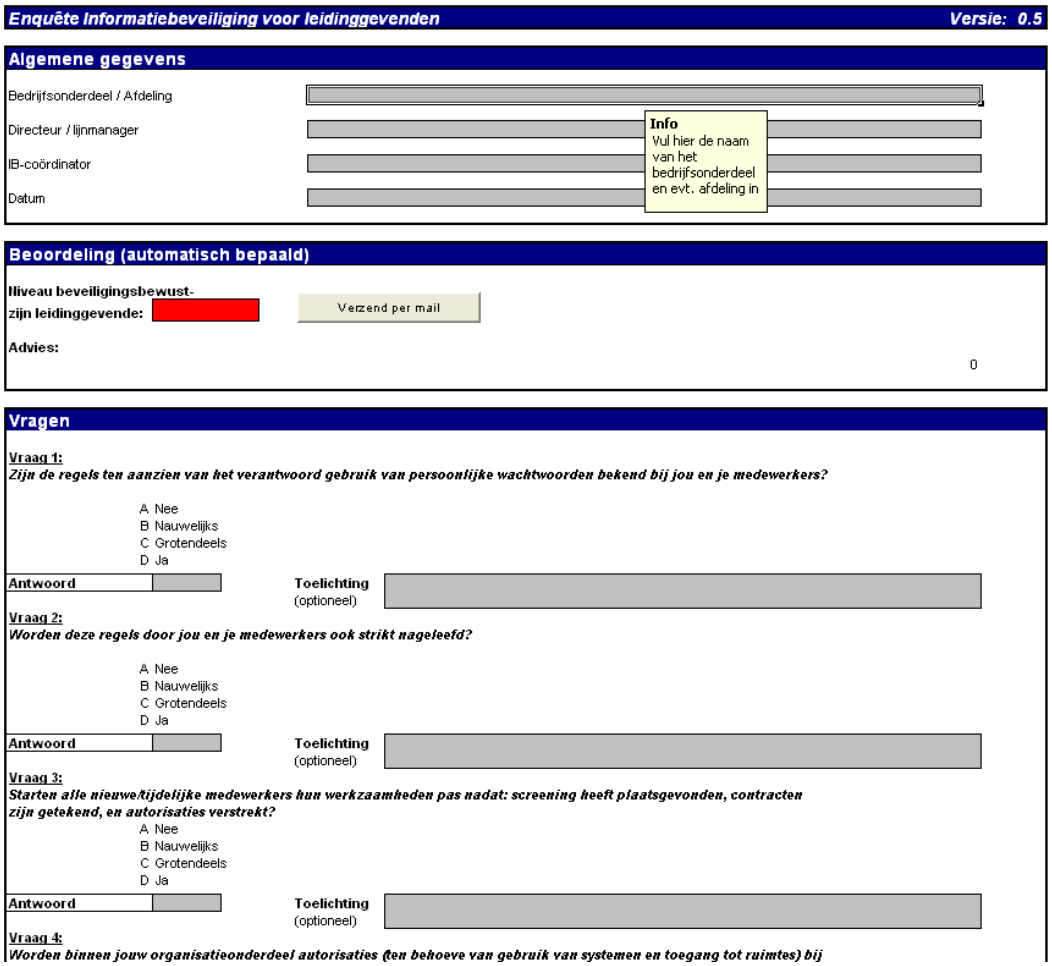
Figuur 21 Scores beveiligingsbewustzijn uit de enquête.

De bruikbaarheid van de enquête is getest d.m.v. het houden van een pilot meting. De pilot en het resultaat wordt in paragraaf 8.2 behandelt.

Met het ontwerpen van de enquête voor medewerkers zijn de aanbevelingen 4.a. t/m 4.c. uit het onderzoek uitgewerkt.										
Aanbevelingen uit het onderzoek (✓ = aanbeveling is uitgewerkt)										
1. ✓	2.	3.	4.a. ✓	4.b. ✓	4.c. ✓	4.d.	4.e.	5.a.	5.b. ✓	5.c. ✓	5.d. ✓

8.1.9. Enquête voor leidinggevende

De enquête voor leidinggevende is een enquête waarmee beoordeeld kan worden in welke mate een leidinggevende en zijn medewerkers invulling geven aan hun verantwoordelijkheid ten aanzien van informatiebeveiliging. Deze enquête bestond voorheen alleen in een papieren versie, nu bestaat de enquête ook in een digitale versie in Excel (zie Figuur 22). Dit heeft als voordeel dat de enquête simpel is in te vullen, met één druk op de knop via email kan worden verzonden en simpel op de afdelingschijf kan worden bewaard.



Figuur 22 De digitale versie van de enquête voor leidinggevenden.

8.1.10. Tool overzicht middelen ter verhoging van het beveiligingsbewustzijn

Met het Excel-bestand 'Beveiligingsbewustzijnmiddelen' is het mogelijk voor IB-coördinatoren en medewerkers van Informatiebeveiliging een overzicht van alle beschikbare middelen ter verhoging van het beveiligingsbewustzijn te krijgen. Door te filteren op één of meerdere onderwerpen kan men snel en simpel een geschikt middel kiezen om in te zetten bij het verhogen van het beveiligingsbewustzijn.

Filteren kan op:

- Communicatierichting, er zijn een aantal richtingen, dit zijn:
    - informeren, gecontroleerd eenrichtingsverkeer (bv. poster en flyers);
    - formeren, samenwerkingverbanden aangaan en afspraken maken;
    - dialogiseren en overreden, praten/discussiëren en overtuigen (bv. een onderwerp op de agenda van een werkoverleg plaatsen).
- Soort middel, bv. activiteiten, e-learning modules, presentaties, enquêtes, workshops.
- Doelgroep van het middel, het management moet bijvoorbeeld van andere zaken bewust worden gemaakt dan medewerkers.

- Of een middel voor een IB-coördinator geschikt is. Sommige middelen zoals het schrijven van een beleidsverantwoording kunnen niet door een IB-coördinator uitgevoerd worden. Toch kan het zeer handig zijn dat een IB-coördinator weet van het bestaan van een middel. Zo kan hij het middel desgewenst aanvragen bij het bedrijfsonderdeel Informatiebeveiliging.

Bij het creëren van deze tool is ook een schifting gemaakt in de huidige beschikbare middelen, hiermee is aanbeveling 5.a. uit het onderzoek uitgewerkt.										
Aanbevelingen uit het onderzoek (✓ = aanbeveling is uitgewerkt)										
1. ✓	2.	3.	4.a. ✓	4.b. ✓	4.c. ✓	4.d.	4.e.	5.a. ✓	5.b. ✓	5.c. ✓	5.d. ✓

8.1.11. Tool meting volwassenheidniveau

Uit gesprekken met de opdrachtgever kwam naar voren dat de Security Awareness Maturity Tables van ISACA te uitgebreid en daardoor tijdrovend zijn om te gebruiken. Daarom is voorgesteld om een tool te maken waarmee IB op een simpele manier kan beoordelen op welk volwassenheidsniveau het proces Informatiebeveiligingsbewustzijn zich bevindt.

De Security Awareness Maturity Tables bestaat uit 6 tabellen die op verschillende vlakken het volwassenheidsniveau van het proces meten. In deze tabellen staan meerdere kenmerken waaraan het proces moet voldoen om op een bepaald volwassenheidsniveau te zitten. Over het algemeen komt een kenmerk op alle niveaus voor. Bijvoorbeeld bij de tabel over de volwassenheid van het beveiligingsbewustzijn binnen de organisatie, hierin staat een kenmerk dat op alle niveaus terug komt, namelijk in hoeverre beveiligingsbewustzijn bij medewerkers aanwezig is. Het verschil tussen dit kenmerk op de verschillende niveaus is dat naarmate het proces op een hoger volwassenheidsniveau zit dit kenmerk uitgebreider is (zie Tabel 2).

1 Initieel/Ad hoc	2 Herhaaldelijk maar intuïtief	3 Gedefinieerde processen	4 Beheerst en meetbaar	5 Geoptimaliseerd
Beveiligingsbewust-zijn is alleen present bij een klein aantal individuen.	Een laag niveau beveiligingsbewust-zijn is aanwezig binnen het grootste deel van de organisatie	Een laag niveau beveiligingsbewust-zijn is bij alle medewerkers aanwezig.	Volledige beveili-gingsbewustzijn bestaat bij mede-werkers. Ze zijn geïnformeerd en begrijpen de eisen en verantwoorde-lijkheden.	Volledige beveili-gingsbewustzijn bestaat bij medewerkers. Ze zijn geïnformeerd en hebben een geavanceerd en vooruitkijkend inzicht voor eisen en verantwoorde-lijkheden.

Tabel 2 Voorbeeld van kenmerken bij volwassenheid inhoud van het programma.

De tool voor meting van het volwassenheidniveau is zo opgebouwd dat door een combinatie van vraagstelling en antwoordmogelijkheden de juiste mate van volwassenheid van een kenmerk wordt bepaald (zie Figuur 23). Als alle antwoorden zijn ingevuld kan men zien wat het volwassenheidsniveau is op de verschillende vlakken en wat de totale volwassenheid is van het proces.

Niveau		Vraag 1: Het niveau van beveiligingsbewustzijn bij medewerkers is:
1	A	present bij een klein aantal individuen. **GA DOOR NAAR VRAAG 6**
2	B	van een laag niveau bij het grootste deel van de medewerkers. **GA DOOR NAAR VRAAG 6**
3	C	van een laag niveau bij alle medewerkers.
4	D	van een voldoende niveau, ze zijn geinformeerd en begreipen de eisen en verantwoordelijkheden.
5	E	van een voldoende niveau, ze zijn geinformeerd en hebben vooruitkijkend inzicht voor de eisen en verantwoordelijkheden.
Antwoord	E	

Figuur 23 Voorbeeldvraag uit de tool voor het meten van het volwasenheidsniveau.

Op het moment van schrijven bevindt de tool zich nog in een concept status. Er is nog geen mogelijkheid geweest om de tool voor te leggen aan de opdrachtgever. Daarnaast mist de huidige versie nog een functionaliteit die de projectgroep wil toevoegen. Deze functionaliteit moet duidelijk maken waarom op een bepaald vlak het niveau zo laag is. Zo kan men hierop bijsturen. Echter is het toevoegen

Door deze tool te baseren op de Security Awareness Maturity Tables is aanbeveling 2. uit het onderzoek uitgewerkt.											
Aanbevelingen uit het onderzoek (✓ = aanbeveling is uitgewerkt)											
1. ✓	2. ✓	3.	4.a. ✓	4.b. ✓	4.c. ✓	4.d.	4.e.	5.a. ✓	5.b. ✓	5.c. ✓	5.d. ✓

8.2. Pilot enquête beveiligingsbewustzijn

Voor het kunnen bepalen van de bruikbaarheid van de enquête beveiligingsbewustzijn (zie 8.1.8) bij medewerkers is besloten om een pilot uit te voeren. Tijdens deze pilot is bekeken of de vragen van het juiste niveau waren en of de scores overeenkwamen met de verwachtingen van de projectgroep.

De doelgroep van deze enquête was het bedrijfsonderdeel IB. Gevraagd is of zij de vragen wilden beantwoorden en feedback wilden geven. Hiermee kan het meetinstrument zo nodig worden verbeterd. Er is gekozen voor de medewerkers van IB omdat zij verstand hebben van de Gouden regels. Zij konden bepalen of de inhoud van de vragen en antwoorden juist was.

8.2.1. Verwachtingen vooraf

De enige verwachting was dat er een verval in de scores van de dimensies zou zijn. Hiermee wordt bedoeld dat de scores van de dimensies kennis, houding en gedrag opeenvolgend steeds een stukje lager zouden zijn (zie Figuur 24).

Score kennis > Score houding > Score gedrag ('>' betekent groter dan)

Figuur 24 Uitleg verwachting scores van de dimensies.

Dit werd verwacht omdat de doelgroep veel kennis heeft van informatiebeveiliging aangezien ze medewerker zijn van het betreffende bedrijfsonderdeel. De reden dat de score van de dimensie houding minder hoog zou zijn dan die van kennis is omdat er altijd wel regels bestaan waar een medewerker het niet mee is. Verwacht werd dat bij de dimensie gedrag de score het laagst zou zijn. Want ook al heeft een medewerker veel kennis over informatiebeveiliging en heeft hij een goede houding t.o.v. een regel dan kan het nog steeds gebeuren dat hij een regel (af en toe) niet uitvoert. Bijvoorbeeld omdat hij de regel vaak vergeet uit te voeren. Deze situaties kunnen opgeteld worden bij de gevallen waarin hij geen goede houding of geen kennis van een regel heeft en daarom een regel niet uitvoert.

8.2.2. Resultaat

De scores van de pilot kwamen overeen met de vooraf gestelde verwachtingen. Onder de 10 ondervraagden was de score voor de dimensie kennis het hoogst met een score van 90% goed beantwoorde vragen. Daarna had houding de tweede score met 84% goed beantwoorde vragen. De laagste score, was zoals verwacht te vinden bij de dimensie gedrag. Hierbij waren van de vragen 69% goed beantwoord. De totale score voor beveiligingsbewustzijn was 78%.

8.2.3. Feedback

De ondervraagden hebben feedback moeten geven op de enquête. Uit deze feedback werd duidelijk hoe bepaalde vragen geïnterpreteerd werden. Omdat de ondervraagden (medewerkers van IB) veel verstand hebben van informatiebeveiliging wisten zij wat bedoeld werd met een vraag. Als hun eerste interpretatie niet overeenkwam met waar de vraag werkelijk over ging dan hebben ze dit gemeld in hun feedback.

8.2.4. Conclusie

De enquête heeft een redelijk goed beeld gegeven over het beveiligingsbewustzijn van de doelgroep. De scores op de verschillende dimensies kwamen overeen met verwachte scores. Echter was op de dimensie gedrag de score wel heel laag. Dit is te verklaren met de opmerkingen van de ondervraagden. Hieruit bleek dat veel vonden dat bij één van de vragen over de dimensie gedrag het goede antwoord er niet tussen stond. Daarom hebben zij deze vraag niet kunnen beantwoorden en is het percentage met goed beantwoorde vragen lager.
Ongeveer de helft van de vragen moet net anders worden geformuleerd. Hierdoor wordt de kans op een verkeerde interpretatie bij officiële metingen verlaagd. Dit werk moet samen of door een medewerker van IB uitgevoerd worden, omdat binnen de projectgroep niet genoeg kennis van informatiebeveiliging aanwezig is om de vragen en antwoorden volledig in overeenstemming met de regels voor informatiebeveiliging te formuleren.

De scores uit de meting van de medewerkers van het bedrijfsonderdeel IB zijn hoogstwaarschijnlijk hoger dan die van een gemiddelde medewerker van SNS REAAL. Een gemiddelde medewerker heeft niet zoveel verstand van informatiebeveiliging. Hiermee moet rekening worden gehouden bij de inzet van dit meetinstrument. Want om te kunnen bepalen of het beveiligingsbewustzijn hoog genoeg is moet ook bekend zijn welk score daar bij past. Hiervoor zijn de scores van de medewerkers van IB geen goed referentiekader.

8.2.5. Advies

Voordat deze enquête kan worden ingezet moeten nog een aantal activiteiten worden uitgevoerd:

- de vragen en antwoorden waarop negatief commentaar is gemaakt moeten samen met of door een medewerker worden verbeterd;
- er moet een score (norm) worden bepaald waaraan een medewerker moet voldoen om beveiligingsbewust genoemd te worden.

8.2.6. Afronding enquête

Op het moment van schrijven is er nog geen tijd geweest om de enquête te verbeteren. Ook voor het opstellen van het testverslag is nog geen tijd geweest, daarom zal dit verslag geen onderdeel uitmaken van de bijlagen.

9. Afsluitingsfase

In dit hoofdstuk worden de activiteiten uit de laatste fase van het project beschreven, deze fase is nog niet afgerond. Er is een presentatie gehouden op de IB-coördinatordag over beveiligingsbewustzijn, er komt nog een presentatie waarin het project wordt opgeleverd en een afstudeerzitting waarin het project moet worden verdedigd.

9.1. Presentatie IB-coördinatordag

De IB-coördinatordag is één van de IB-contactmomenten. Hiermee leidt het bedrijfsonderdeel Informatiebeveiliging de IB-coördinatoren op. Daarnaast is het een ideale situatie voor het bedrijfsonderdeel IB en de IB-coördinatoren om elkaar beter te leren kennen. Doordat de coördinatoren vragen stellen en feedback geven kan Informatiebeveiliging de ondersteuning die ze bieden beter afstemmen.
De IB-coördinatordag wordt 2 keer per jaar gehouden. In de ochtend wordt een cursus gegeven voor nieuwe IB-coördinatoren, hierin worden de taken en verantwoordelijkheden uitgelegd. In de middag worden diverse presentaties gegeven, bijvoorbeeld over nieuwe ontwikkelingen die betrekking hebben op de taken en verantwoordelijkheden van de IB-coördinator.

Op de IB-coördinatordag van 24 mei 2010 is door projectlid Stef Peeters ook een presentatie gehouden. In deze presentatie is uitgelegd wat beveiligingsbewustzijn is en hoe de IB-coördinatoren het kunnen verhogen. De projectgroep heeft de IB-coördinatoren duidelijk gemaakt hoe zij met de tool ‘Beveiligingsbewustzijnmiddelen’ (zie 8.1.10) snel en simpel een keuze kunnen maken uit alle beschikbare middelen. Daarnaast is ingegaan op de nieuwe centrale kennissite op ID (zie 0), waar zij alle informatie, kennis en middelen kunnen vinden.

9.2. Oplevering project

Op 10 juni 2010 vindt er nog een oplevering van het project plaats. Tijdens deze oplevering wordt door de projectgroep een presentatie gehouden waarin het verloop van het project en de geboekte resultaten worden gepresenteerd. De resultaten zullen aan de hand van de doelstelling, opdracht en overige gemaakte afspraken zoals beschreven in het projectplan worden verantwoord.

9.3. Afstudeerzitting

Op 22 juni 2010 vindt de afstudeerzitting plaats. Tijdens deze zitting moet net zoals bij de oplevering van het project een presentatie worden gehouden waarin het verloop van het project en de geboekte resultaten worden gepresenteerd. Ook hier moeten de resultaten aan de hand van de doelstelling, opdracht en overige gemaakte afspraken zoals beschreven in het projectplan worden verantwoord. Daarna wordt door de examencommissie in het verdedigingsgesprek vragen gesteld over de gemaakte keuzes en geboekte resultaten.

10. Conclusies en aanbevelingen

Tot slot worden in dit hoofdstuk de conclusies en aanbevelingen geformuleerd die voortvloeien uit het project en haar doelstelling.

De doelstelling van het project was:

> 1) Tijdens dit project moet duidelijk worden waar voor SNS REAAL kansen liggen om het proces Informatiebeveiligingsbewustzijn meer volwassen te maken. Daarnaast moet er een geschikt model gekozen worden om het volwassenheidsniveau aantoonbaar te kunnen maken.
> 2) Door het uitwerken van deze kansen zal het proces Informatiebeveiligingsbewustzijn aan het einde van dit project op een hoger volwassenheidsniveau functioneren.
> 3) Dit wordt onder andere bereikt door het bouwen van één centrale site, hierop moeten alle materialen m.b.t. het onderwerp informatiebeveiligingsbewustzijn binnen SNS REAAL gepost kunnen worden.

1) Bij de start van de uitvoeringsfase is begonnen met het onderzoek, hieruit zijn aanbevelingen voortgevloeid voor het meer volwassen inrichten van het proces. Daarnaast is een volwassenheidsmodel aanbevolen, de Security Awareness Maturity Tables, dat het beste geschikt is voor het meten van de volwassenheid van het proces Informatiebeveiligingsbewustzijn.
2) Om het proces op het einde van het project op een hoger volwassenheidsniveau te kunnen laten functioneren is een procesbeschrijving opgesteld. In deze procesbeschrijving zijn kenmerken uit de Security Awareness Maturity Tables opgenomen die voorheen nog niet onderdeel waren van het proces.
3) De drie sites zijn geïntegreerd naar één centrale site, dit is gebeurd op ID. Daarbij is zoals aanbevolen na het onderzoek rekening gehouden met de verschillende doelgroepen voor de site en is eenduidige en overzichtelijke opslag van middelen mogelijk.

Desondanks wil de projectgroep hierbij graag een aantal aanbevelingen doen richting SNS REAAL en in het bijzonder aan het bedrijfsonderdeel Informatiebeveiliging:

- de nog niet uitgevoerde aanbevelingen of aanbevelingen die continu uitgevoerd moeten worden uitvoeren, dit zijn de aanbevelingen (zie paragraaf 5.2 voor uitleg) ‘2. Standaardiseren’, ‘3. Verbeteren proces’, ‘4.a. t/m 4.d. Meten is weten’ en ‘5.a. t/m 5.b. Middelen ter verhoging van het beveiligingsbewustzijn’;
- de nieuwe uitstraling van de centrale site op ID zo spoedig mogelijk verder afronden;
- afronden van de procesbeschrijving en hier een flyer over maken voor de IB-coördinatoren en beiden daarna in gebruik nemen;
- enquête beveiligingsbewustzijn verbeteren aan de hand van de resultaten uit de pilot;
- normen vaststellen voor de enquête beveiligingsbewustzijn.

Evaluatie

Op het moment dat ik deze opdracht op de website van SNS REAAL zag staan wilde ik deze opdracht al doen. In het bijzonder sprak het onderdeel beveiligingsbewustzijn in de opdracht mij erg aan. Ik heb mij altijd al geïnteresseerd in de manier waarop je gedrag van mensen op een positieve wijze kan beïnvloedden. De combinatie van dit en informatiebeveiliging, een onderwerp dat aansluit op mijn studie, maakte het een interessante opdracht.

Tijdens mijn studie had ik al kennisgemaakt met het onderwerp informatiebeveiliging, daarom had ik voordat ik begon al een beeld van waarmee ik te maken zou krijgen. Toch bleken de boeken en de colleges niet zo diep in te gaan op informatiebeveiliging als het op dit moment bij het bedrijfsonderdeel IB is georganiseerd. Maar dat is natuurlijk meer dan logisch bij een bedrijfsonderdeel dat al meerdere jaren bestaat en bijna 20 fte's in dienst heeft. Hierdoor heeft de tijd bij SNS REAAL voor veel nieuwe kennis gezorgd die ik goed kan gebruiken bij het vervolg van mijn (studie)loopbaan.

Ik heb geleerd om professioneler te werken. Dit zie ik terug in de opbouw en de manier van schrijven van mijn documenten en de uitvoering van mijn taken. Dit heb ik geleerd tijdens het schrijven van het project plan volgens de projectbeheermethodiek PMW Professional, het schrijven van de procesbeschrijving volgens de eisen van IB en de feedback die ik heb ontvangen tijdens het schrijven van mijn afstudeerscriptie.

Wekelijks had ik een voortgangsoverleg met mijn stagebegeleider John Verkooijen. In deze gesprekken maakte ik duidelijk wat ik die week had gedaan en wat mijn doelstellingen/taken voor de komende week waren. Doordat John Verkooijen zo exact wist hoe ik ervoor stond met het verloop van mijn afstudeerproject, kon hij waar nodig was op de juiste momenten bijsturen. Gelukkig heeft hij geen enkele keer hoeven ingrijpen. Dit spreekt denk ik voor de vaardigheden waarover ik beschik om een project tot een goed einde te brengen. Door de goede keuzes op de juiste momenten te maken in overleg met het stagebedrijf en in overeenstemming met de gestelde doelen van dit project.

Ik vind zorgvuldigheid en kwaliteit zeer belangrijk. De zorgvuldigheid waarmee een taak wordt uitgevoerd om niets aan het toeval over te laten en de kwaliteit die je hiermee bereikt. Dit is voor mij ook een valkuil. Door geen fouten te willen maken en altijd voor de hoogste kwaliteit te willen gaan, is het schrijven van de documenten wel een beetje vertraagd. Dit zie ik dan ook als een leermoment. Een document moet niet het doel zijn maar het middel. Ik ben me er ook van bewust dat dit een continu leerproces is waarin je alleen maar beter kan worden door het te blijven doen.

In de laatste fase van het project heb ik nog een presentatie gehouden voor vijftig IB-coördinatoren. Dit vond ik van te voren spannend. Maar hierdoor weet ik nu dat ik een presentatie kan houden voor een grote groep. Dit neemt voor de toekomst een groot stuk spanning weg.

Literatuurlijst

Boeken

1. Piet Verschuren, Hans Doorewaard, *Het ontwerpen van een onderzoek,* derde druk, LEMMA, 2004
2. Tim Wulgaert, *Security Awareness: Best practices to serve your enterprise*, eerste druk, Rolling Meadows, ISACA, 2005

Stukken, documenten en naslagarchieven

1. 7 Gouden regels van Informatiebeveiliging van SNS Bank
2. Bedrijfsplan Informatiebeveiliging 2010 v1.0
3. H. A. Kruger, W.D. Kearney, *A prototype for assessing information security awareness,* 2006
4. Caroline Neys, *It'ers, regels en security awareness,* 2010
5. Organogram ITC per 01-01-2010
6. Organogram SNS REAAL
7. Presentatie Architectuur en Beleid 10 november 2009
8. SNS REAAL financieel jaarverslag 2009
9. Structuur afdeling Informatiebeveiliging 1.1
10. Kerry-Lynn Thomson, Rossouw von Solms, *Towards an Information Security Competence Maturity Model*, 2006

Websites

1. http://nl.wikipedia.org/wiki/SNS_REAAL
2. http://www.snsreaal.nl/index.asp?NID=6545
3. http://www.snsreaal.nl/index.asp?NID=6562
4. http://SharePoint.bank.local/sites/200807032/default.aspx

Bijlagen

Dit document bevat als bijlage het projectplan. Uiteraard zijn er tijdens dit project meer documenten tot stand gekomen. Voor de leesbaarheid van dit document is gekozen om hier een apart bijlagenverslag van te maken.

De bijlage van deze scriptie is het:

A. Projectplan

Het bijlagenverslag bestaat uit:

B. Onderzoekopzet
C. Onderzoekrapport
D. Procesbeschrijving Informatiebeveiligingsbewustzijn

A: Projectplan

Projectplan

Projectnaam	Beveiligingsbewustzijn efficiënt en meetbaar ingericht bij SNS REAAL
Versie	1.2
Status	Definitief
Datum	15-4-2010
Referentie	Project plan 1.2.doc

Opdrachtgever	**Projectmanager**
Naam: Ben van Zuijlen	Naam: Stef Peeters
Functie: Afdelingshoofd IB	Functie: Afstudeerder
Datum goedgekeurd: 12-3-2010	Datum: 15-4-2010

1ste Bedrijfbegeleider
Naam: John Verkooijen
Functie: Adviseur IB
Datum gezien: 15-4-2010

1ste Afstudeerstagedocent	**2de Afstudeerstagedocent**
Naam: Rob van Stratum	Naam: Martin van de Rijt
Functie: Afstudeerstagedocent Fontys	Functie: Afstudeerstagedocent Fontys

Versiebeheer

Versie	Status	Datum	Opmerking
0.1	Concept	4-2-2010	Skelet PROJECTPLAN
0.2	Concept	5-2-2010	Eerste vorm projectafbakening
0.3	Concept	8-2-2010	
0.4	Concept	9-2-2010	
0.5	Concept	10-2-2010	Eerste complete conceptversie
0	Concept	12-2-2010	Opmerkingen Rob van Stratum verwerkt
0	Concept	18-2-2010	Opmerkingen John Verkooijen vewerkt
0.9	Concept	18-2-2010	Laatste conceptversie
1.0	Definitief	12-3-2010	Eerste definitieve versie
1.1	Definitief	22-3-2010	Gewijzigde planning en daarom ook 4.2 en 4.3
1.2	Definitie	14-5-2010	Wijzigingen Martin van de Rijt doorgevoerd.

Distributielijst

Naam	Functie
Rob van stratum	Stagedocent
John Verkooijen	Stagebegeleider
Ben van Zuijlen	Opdrachtgever
Martin van de Rijt	Stagedocent

Gerefereerde documenten

Naam	Auteur	Versie	Datum
Bedrijfsplan informatiebeveiliging 2010 v0.9.doc	Simon Greve, Ben van Zuijlen	0.9	18-01-2010
Structuur afdeling Informatiebeveiliging 1.1.ppt	Elvira Kas	1.1	Onbekend
Afstudeerstagebrochure_BI_voorjaar_2010.doc	Antonet Barten (stagebureau Fontys Hogeschool ICT)	Onbekend	Onbekend
NAVI_Begrippenkaders_definities_en_afkortingen.pdf	Nationaal Adviescentrum Vitale Infrastructuur	0.4	3-10-2008

INHOUDSOPGAVE

SAMENVATTING

Beveiligingsbewustzijn is een belangrijke maatregel om IT risico's te verlagen. Binnen SNS REAAL wordt hier reeds veel aandacht aan besteed. Daarnaast maakt men gebruik van een netwerk van IB-coördinatoren (+/- 100 personen), welke als deeltaak deze rol vervullen (4-8 uur per maand). Zij zijn voor de medewerkers m.b.t. informatiebeveiliging het eerste aanspreekpunt. Het bedrijfsonderdeel Informatiebeveiliging ondersteunt deze IB-coördinatoren met beveiligingsbewustzijn materialen, activiteiten, opleidingen etc.
Het goed ter beschikking stellen en het meet- en aantoonbaar maken van beveiligingsbewustzijn van medewerkers door de hele organisatie heen is de uitdaging van dit project.

Tijdens een onderzoek zal het vergroten van de kennis over beveiligingsbewustzijn centraal staan. Ook wordt tijdens dit onderzoek gekeken naar de huidige gang van zaken betreffende het verhogen van het beveiligingsbewustzijnsniveau.
De resultaten uit het onderzoek worden gebruikt als leidraad voor de rest van het project, namelijk voor de opzet van een nieuwe centrale intranetsite voor Informatiebeveiliging en voor het ontwerpen van (een) middel(en) t.b.v. beveiligingsbewustzijn.

Doel van dit document
De drie belangrijkste redenen voor gebruik van dit document zijn:

- om er zeker van te zijn dat het project een gezonde basis heeft voordat de Stuurgroep gevraagd wordt zich aan het project te committeren;
- om te dienen als basisdocument op grond waarvan de Stuurgroep en de Projectmanager de voortgang en wijzigingen kunnen toetsen en bewaken;
- om vragen betreffende geldigheid van het project tijdens de uitvoering ervan te kunnen beoordelen.

De leden van de Stuurgroep staan beschreven in paragraaf 3.1 'Besturingsmodel' en 3.2 'Projectgovernance'.

Het projectplan is als volgt ingedeeld:

- Hoofdstuk 1 Projectopdracht beschrijft het WAAROM, WAT en WAT NIET
- Hoofdstuk 2 Projectaanpak beschrijft het HOE
- Hoofdstuk 3 Projectorganisatie beschrijft het WIE en WAARMEE
- Hoofdstuk 4 Planning en begroting beschrijft het WANNEER en de UREN
- Hoofdstuk 5 Beheersmechanismen beschrijft de beheersmechanismen voor een succesvolle uitvoering van het project

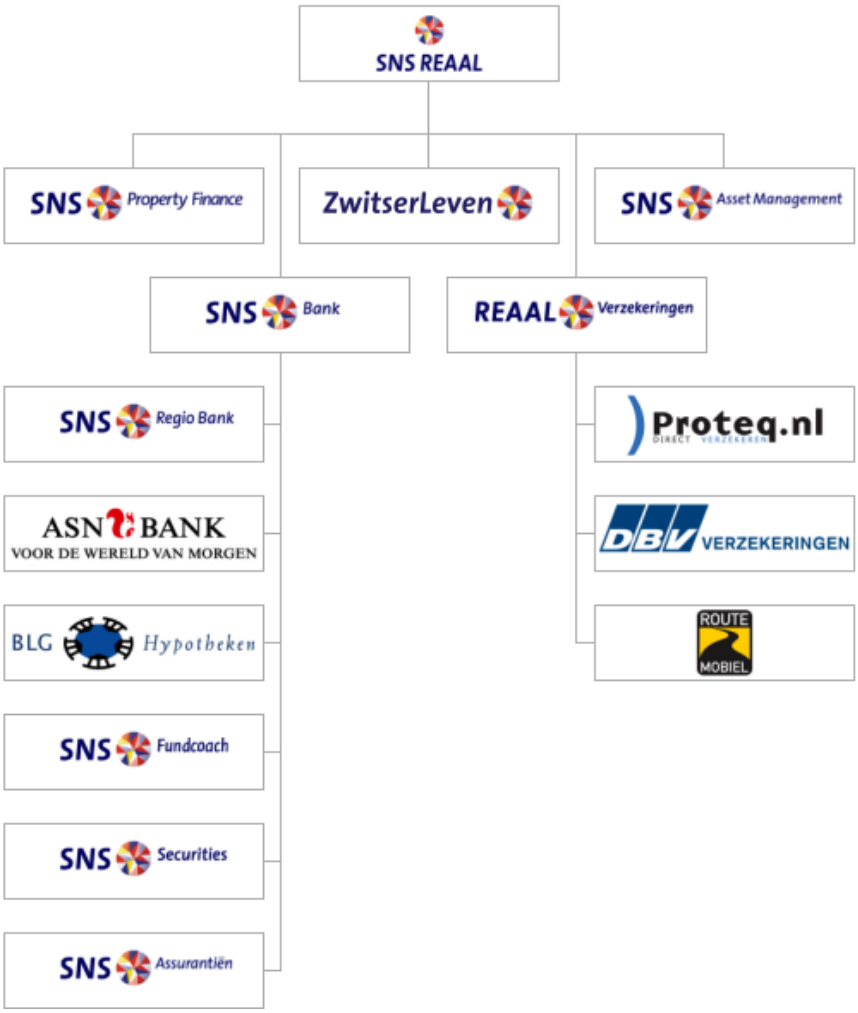
Projectopdracht

Projectachtergrond

Organisatie[43]

SNS REAAL is een Nederlandse financiële instelling op het gebied van verzekeren en bankieren die zich richt op de particuliere markt en het midden- en kleinbedrijf. De dienstverlening aan particuliere en zakelijke relaties vindt vooral plaats door SNS Bank en REAAL Verzekeringen. SNS Bank bedient haar klanten via eigen winkels, onafhankelijke intermediaris, regiokantoren, internet en de telefoon. REAAL Verzekeringen verkoopt haar producten en diensten uitsluitend via onafhankelijke intermediairs. SNS REAAL heeft ongeveer 6500 medewerkers op basis van volledige werktijd in dienst.
Tot SNS REAAL behoren ook diverse verkooplabels die op een specifieke markt werkzaam zijn:

- ASN Bank: Nederlands eerste zogenaamde duurzame bank
- BLG Hypotheken: hypotheekbank
- DBV Verzekeringen: levensverzekeringsmaatschappij
- Proteq: verzekeraar met direct distributiekanaal
- Route Mobiel
- SNS Asset Management: vermogensbeheerder voor institutionele beleggers
- SNS Property Finance: financierder vastgoed en participatieonderneming
- SNS Regio Bank: intermediair bank
- SNS Securities: effectenbedrijf
- Zwitserleven: pensioenverzekeraar



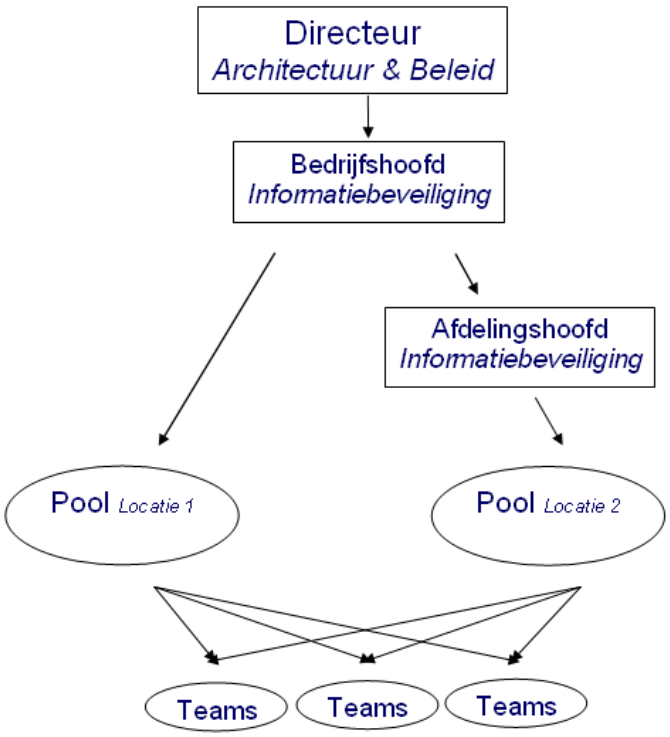
Figuur 25 Het organogram van SNS REAAL en haar verschillende onderdelen.
[44]

[43] http://nl.wikipedia.org/wiki/SNS_REAAL

[44] http://id/Organisatie/Pages/Default.aspx

Bedrijfsonderdeel[45]

Het bedrijfsonderdeel Informatiebeveiliging is gevestigd op twee vestigingen, namelijk Alkmaar en Den Bosch. De taken en diensten verschillen per vestiging. In 1997 is SNS formeel gefuseerd met REAAL, met het totaal integreren van de organisatie is men op dit moment nog bezig. Zo ook bij het onderdeel IB. Daarom komt in de strategie voor 2010 een aantal punten over het integreren van de twee afdelingen voor.



Figuur 26 Het organogram van de afdeling Informatiebeveiliging[46]

Aanleiding

In het verleden zijn meerdere activiteiten en projecten met betrekking tot informatiebeveiligingsbewustzijn uitgevoerd. Deze activiteiten en projecten hebben tot middelen en campagnes ter verhoging van het beveiligingsbewustzijn geleid. Dit project borduurt verder op de wens om het proces beveiligingsbewustzijn naar een hoger volwassenheidsniveau[47] te brengen om zo de efficiëntie en meetbaarheid te verhogen.

Projectprobleemstelling

Binnen SNS REAAL wordt in verband met het indammen van IT risico's veel aandacht besteed aan informatiebeveiligingsbewustzijn. Een netwerk van ongeveer 100 IB-coördinatoren functioneren als eerste aanspreekpunt m.b.t. informatiebeveiliging. Het bedrijfsonderdeel IB ondersteunt hen daarbij. Het huidige proces beveiligingsbewustzijn voldoet aan alle standaarden; toch wil SNS REAAL naar een nog hoger niveau. De vraag luidt dan ook:

[45] Bedrijfsplan informatiebeveiliging 2010 v0.9.doc

[46] Structuur afdeling Informatiebeveiliging 1.1.ppt

[47] Het volwassenheidsniveau geeft aan hoe goed/professioneel een organisatie of proces is georganiseerd.

'Waar liggen voor SNS REAAL de kansen om het proces informatiebeveiligingsbewustzijn efficiënt en meetbaar over het hele concern in te richten?'.

Projectdoelstelling

Tijdens dit project moet duidelijk worden waar voor SNS REAAL kansen liggen om het proces beveiligingsbewustzijn meer volwassen te maken. Daarnaast moet er een geschikt model gekozen worden om het volwassenheidsniveau aantoonbaar te maken.
Door het uitwerken van deze kansen zal het proces beveiligingsbewustzijn aan het einde van dit project op een hoger volwassenheidsniveau functioneren. Dit wordt onder andere bereikt door het bouwen van één centrale site, hierop moeten alle materialen m.b.t. het onderwerp informatiebeveiligingsbewustzijn binnen SNS REAAL gepost kunnen worden.

Kort gezegd moet dit project opleveren:

- een onderzoeksrapport met conclusies en aanbevelingen die beschrijven waar voor SNS REAAL de kansen liggen en wat het geschikte volwassenheidsmodel[48] is;
- één centrale site waarop alle materialen effectief en efficiënt kunnen worden gepubliceerd;
- het proces informatiebeveiligingsbewustzijn dat op een nog hoger volwassenheidsniveau functioneert.

Opdrachtformulering

Maak duidelijk waar voor SNS REAAL de kansen liggen om het proces beveiligingsbewustzijn naar een nog hoger volwassenheidsniveau te brengen en zorg dat dit meet- en aantoonbaar wordt met behulp van een geschikt volwassenheidsmodel.

Werk alle kansen beschreven in de conclusies en aanbevelingen uit het onderzoek, zo ver als mogelijk binnen de grenzen van dit project, uit. Er moet een (op basis van Project Management overwegingen) beargumenteerde keuze gemaakt worden tussen kansen die niet en die wel uitgewerkt worden.

Integreer de drie bestaande IB sites naar één centrale site.

Scope

Dit project moet binnen een tijdsbestek van 19 weken worden afgerond. Het eerste deel bestaat uit kenniswerving, dit gebeurt in de vorm van een onderzoek.
In het tweede deel wordt met behulp van de verworven kennis drie verschillende intranetsites geïntegreerd naar één centrale site op ID. Ook wordt in dit deel minimaal één middel uitgewerkt t.b.v. het verhogen van het beveiligingsbewustzijn.

[48] Een volwassenheidsmodel is een hulpmiddel om de volwassenheid van een organisatie te beoordelen en om de aandachtsgebieden te bepalen aan de hand waarvan de volwassenheid van die organisatie vergroot kan worden. (Bron: Sogeti)

In het derde deel van het project wordt een pilot uitgevoerd. Tijdens deze pilot wordt gecontroleerd of de meting voor beveiligingsbewustzijn gebruikt kan worden binnen SNS REAAL, dit is afhankelijk van het niveau van de vragen en de kwaliteit van de output.

Randvoorwaarden
Het literatuurrapport moet een praktijkgericht en goed rapport zijn, dit wil zeggen dat SNS REAAL stappen vooruit kan zetten met de getrokken conclusies. Ook moet dit document op een duidelijke en goed te lezen manier geschreven zijn.
De voorwaarde aan de centrale site op ID is dat deze marktconform is, het moet net zo goed of nog beter zijn dan wat er te vinden is in de markt. Ook moet de site interactieve onderdelen bevatten waarmee het beveiligingsbewustzijnniveau verhoogd kan worden.

Op te leveren resultaten

Om de resultaten smart (specifiek, meetbaar, acceptabel, realistisch en tijdsgebonden) te formuleren is gekozen om het project in fases op te delen.

Fase	**Periode (2010)**	**Duur (weken)**
Definitie- en initiatiefase	week 5 t/m 7	3
Uitvoering	week 7 t/m 21	15
Afronding	week 21 t/m 23	2

De volgende resultaten moeten tijdens dit project tot stand komen.

Resultaat	**Tijd**
Mini plan van aanpak (t.b.v. sollicitatie)	Definitie- en initiatiefase
Projectplan	Definitie- en initiatiefase
Rapport onderzoek	Uitvoeringsfase
Centrale IB site op ID	Uitvoeringsfase
Beveiligingsbewustzijnmiddel(en)	Uitvoeringsfase
Testverslag	Uitvoeringsfase
Ondersteunende documentatie IB-coördinatoren	Afrondingsfase
Eindscriptie project	Afrondingsfase

Resultaten die niet tot dit project horen:

- compleet geactualiseerde beveiligingsbewustzijncampagne.

Randvoorwaarden

Een randvoorwaarde is een zijdelingse beperking aan het project. Een randvoorwaarde stelt eisen aan het project die vanuit het project zelf niet kan worden beïnvloed.

Randvoorwaarde(n) voor het slagen van het project zijn:

Randvoorwaarde	**Verantwoordelijk**
• Bereidwillige medewerking van een representatief deel der IB-coördinatoren.	John Verkooijen
• Bereidwillige medewerking van medewerkers i.v.m. meting en uitvoeren pilot.	John Verkooijen
• Begeleiding door bedrijfsbegeleider (frequentie,	John Verkooijen

intensiteit).	
• Werkplek met pc, toegang tot internet en e-learning module(s).	John Verkooijen
• Beschikking hebben over middelen voor beveiligingsbewustzijncampagne.	John Verkooijen

Uitgangspunten

Uitgangspunten zijn die zaken die door het project als basis moeten worden meegenomen. Een uitgangspunt is iets waar het project niet omheen kan (lees: vertrekpunt).

Uitgangspunten
Het project dient uiterlijk te zijn afgerond op 10 juni 2010.
Er bestaan al meerdere beveiligingsmiddelen en -campagne(s).
Er is al allerlei kennis aanwezig binnen SNS REAAL m.b.t. beveiligingsbewustzijn.

Acceptatiecriteria

Om het project te kunnen beëindigen moeten de resultaten van dit project minimaal aan de volgende criteria voldoen:

- Een kwalitatief hoog onderzoekrapport met een duidelijke formulering en de aangedragen middelen moeten goed toepasbaar zijn binnen SNS REAAL;
- Een centrale Informatiebeveiliging site op ID die marktconform en interactief is;
- Één of meerdere goed werkend(e) beveiligingsbewustzijnmiddel(en).

Kritieke Succesfactoren (KSF)

	(Klant)tevredenheidcriterium	**Weging**	**Waardering**
1	Het project wordt conform plan binnen budget en tijdsplanning opgeleverd	10%	
2	Uitgevoerd onderzoek	20%	
3	Centrale intranet site	25%	
4	Werkend(e) beveiligingsbewustzijnmiddel(en)	25%	
5	Afstudeerscriptie	10%	
6	Eindpresentatie	10%	
	Conclusie over het hele project		

Relaties naar andere projecten

Integratie SNS Bank IB met REAAL verzekeringen IB.

Tijdens de fusie is gebleken dat er grote cultuurverschillen zijn tussen het bankdeel en het REAAL deel. Deze cultuurverschillen bestaan ook tussen de twee IB bedrijfsonderdelen. De relatie met dit project heeft hierbij vooral betrekking op de manier van communiceren. In dit stadium van het project is nog niet exact duidelijk waar de verschillen liggen. Wel is duidelijk dat de verschillen bestaan, om de effectiviteit van de beveiligingsbewustzijnmiddelen en campagne niet te verlagen is het daarom van essentieel belang dat hier rekening mee word gehouden.

Omtrainen van IB-functionarissen naar IB-coördinatoren.

Tot 1 januari 2010 verschilde de omschrijving van de IB-coördinatoren binnen het REAAL deel met die van het bankdeel. Binnen het REAAL deel werden ze functionarissen genoemd, was het takenpakket kleiner en lag de norm van het beveiligingsniveau lager. Dit alles is te herleiden uit het feit dat het bankdeel een andere kijk heeft op de beschikbaarheid, integriteit en

vertrouwelijkheid van informatie. Informatiebeveiligingsincidenten bij de bank brengen een veel grotere negatieve impact met zich mee. Daarom is besloten alle IB-functionarissen om te trainen tot IB-coördinatoren. Het gebruik van de beveiligingsbewustzijnmiddelen speelt hierbij een essentiële rol. Die moeten het bewustzijn creëren bij de IB-coördinatoren wat het belang is van een zorgvuldige toepassing van de regels en procedures van informatiebeveiliging. Ook moeten de ontwikkelde middelen voor hen bruikbaar zijn om het beveiligingsbewustzijn niveau bij hun afdeling of vestiging te verhogen.

PROJECTAANPAK

Projectaanpak

Voor het projectmanagement is gekozen voor de methodiek van PMW professional, omdat dit binnen SNS REAAL de standaard is. Deze methodiek is analoog aan de PRINCE2 methode[49]. Met behulp van PMW professional zijn een aantal samenhangende activiteiten geformuleerd waarbij het doel centraal staat. In deze paragraaf wordt dit vertaald naar de aanpak om te komen tot een gedegen onderzoek en een eenduidige intranet site.

Door gebruik te maken van PMW professional is er:

- Een gecontroleerde en georganiseerde start, midden en eindfase;
- Regelmatige controle op de voortgang a.d.h.v. de planning;
- Automatische management controle op afwijkingen op het plan;
- De betrokkenheid van (management en) aandeelhouders op de juiste momenten en plaatsen gedurende het project;
- Goede communicatiekanalen tussen het project, projectmanagement, en de rest van de organisatie.

Fasering

In het project zal er gebruik gemaakt gaan worden van drie hoofdfasen: definitie- en initiatiefase, uitvoeringfase en afsluitingsfase. De voortgang van de activiteiten in de bovengenoemde fases wordt bewaakt door de opdrachtgever in samenwerking met de projectleider, bedrijfsbegeleiders en stagedocent van Fontys. Hieronder volgt een gedetailleerde omschrijving van deze drie hoofdfasen:

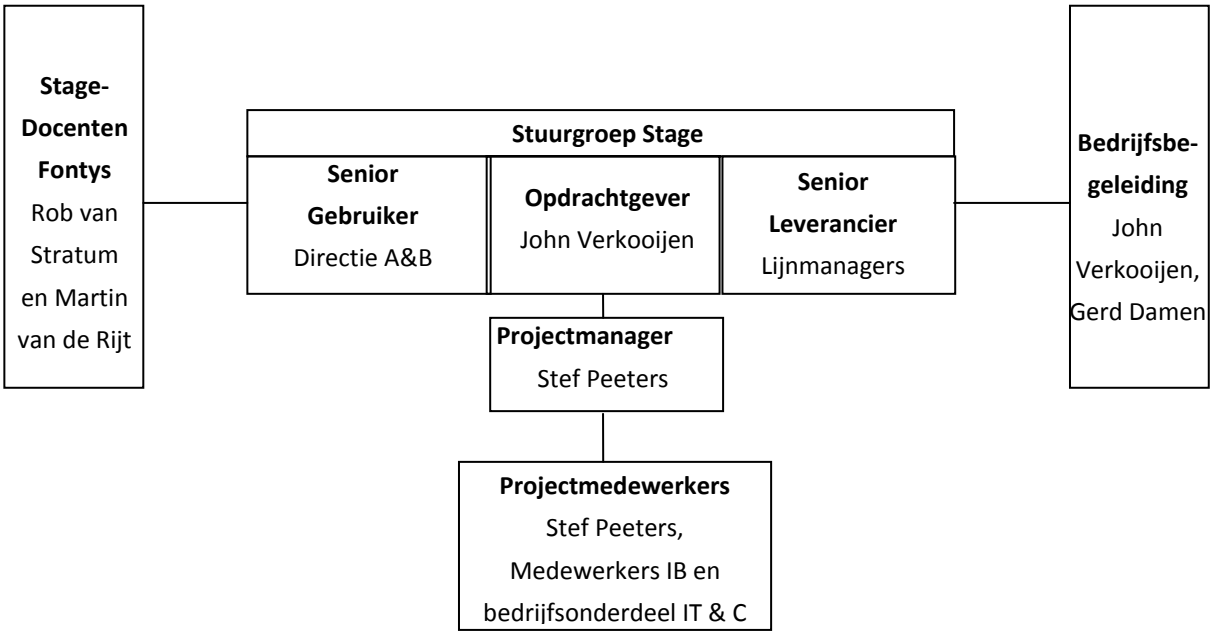
1. Definitie- en initiatiefase:
   - Projectopdracht afbakenen;
   - Projectplan maken;
   - Voorbereiden onderzoek.
2. Uitvoeringfase:
   - Onderzoek beveiligingsbewustzijn;
   - Conclusies trekken uit onderzoek;
   - Integreren van verschillende intranet sites in ID;
   - Ontwikkelen nieuwe beveiligingsbewustzijnmiddelen.
   - Pilot
   - Testverslag (inclusief advies)
3. Afsluitingsfase:
   - Afstudeerscriptie;
   - Presentatie.

[49] http://sharepoint.bank.local/sites/200807032/default.aspx

PROJECTORGANISATIE

Besturingsmodel

Voor dit project is het volgende besturingsmodel van toepassing:



Projectgovernance

Rol	Wie	Taken, verantwoordelijkheden, bevoegdheden
Opdrachtgever	John Verkooijen	Managen van het project in relatie tot de overall doelen van SNS REAAL (IT).
Sr. Gebruiker	Directie A & B	Beschikbaar stellen resources en afname projectresultaten.
Sr. Leverancier	Lijnmanagers	Leveren medewerkers voor projectmanagement, uitvoering en ondersteuning.
Projectmanager	Stef Peeters	Planning, uitvoering en rapportage.
Projectmedewerkers	Stef Peeters, Medewerkers IB en Medewerkers bedrijfsdeel SNS IT&C	Uitvoeren projectactiviteiten
Stagedocent	Rob van Stratum, Martin van de Rijt	Ondersteuning leveren bij de uitvoering van het project indien dit gewenst is.
Bedrijfsbegeleiding	John Verkooijen Gerd Damen	Begeleiding student

Communicatieplan

Overlegstructuren
De status en voortgang van het project zal periodiek worden besproken in voortgangsoverleggen met de opdrachtgever. Alle op te leveren eindproducten zullen op nader te bepalen momenten worden besproken met de opdrachtgever en de stagedocent van Fontys.

Opdrachtgever/bedrijfsbegeleider
Met de bedrijfsbegeleider zal er wekelijks (d.m.v. een vergadering) de voortgang van het project besproken worden. Eventuele dringende vragen of knelpunten kan men ook buiten de wekelijkse vergaderingen aan de begeleider of opdrachtgever voorleggen. Voor de rest zal er met de opdrachtgever en bedrijfsbegeleider middels de volgende communicatiekanalen gecommuniceerd worden: verbale communicatie, e-mail en telefoon.

Stagedocent Fontys
De afstudeerbegeleider van Fontys zal twee keer tijdens het verloop van het project een bezoek brengen op locatie om de afstudeeropdracht te bespreken met de projectleider en de opdrachtgever/bedrijfsbegeleider. Verder zal er elke week een voortgangsmail naar de stagedocent van Fontys verstuurd worden. Dit zal door de projectleider (Stef Peeters) gedaan worden. Mochten er urgente vragen aan de afstudeerbegeleider zijn, dan bestaat er de mogelijkheid om deze per telefoon te vragen

Contactgegevens betrokkenen

Naam	**Functie**	**E-mailadres**	**Telefoonnummer**
John Verkooijen	Adviseur IB	john.verkooijen@sns.nl	073 683 3457
Gerd Damen	Adviseur IB	gerd.damen@sns.nl	073 683 3925
Ben van Zuijlen	Afdelingshoofd IB	ben.vanzuijlen@sns.nl	073 683 3261
Stef Peeters	Afstudeerder IB	stef.peeters@sns.nl	06 460 22 155
Rob van Stratum	Afstudeerdocent Fontys Hogeschool	r.vanstratum@fontys.nl	087 787 8624 06 24 50 63 41

Rapportages
Conform PMW-P zal periodiek een projectvoortgangsrapportage worden opgesteld.

PLANNING EN BEGROTING

Productplanning

Fase			
Activiteiten per fase	**Kalen-derweek nummer**	**Uitvoerder**	**Uren**
0. Algemeen			
Overige activiteiten week 5 t/m 7	Alle	Stef Peeters	29,5
Vrije dag in week 7	Alle	Stef Peeters	9
Feestdagen (alle behalve Hemelvaart)	Alle	Stef Peeters	45
Wekelijkse logboek sturen en doelstellingen formuleren	Wekelijks	Stef Peeters	9
Opstellen afstudeerscriptie (periodieke activiteit vanaf week 8 tot en met 21)	Wekelijks	Stef Peeters	28
Wekelijks voortgangoverleg met John Verkooijen	Wekelijks	Stef Peeters, John Verkooijen	4,5
1. Definitie- en initiatiefase			
Mini plan van aanpak (t.b.v. sollicitatie)	*0*	*Stef Peeters*	*3*
Definitieve probleemstelling definiëren	5, 6	Stef Peeters	6
Opstellen projectplan: • projectopdracht; • projectafbakening; • organisatiestructuur; • detailplanning; • projectbeheersing.	6	Stef Peeters	35
Voorbereiding onderzoek		Stef Peeters	
Uitwerken onderzoeksopzet, door vast te stellen: • doelstelling; • vraagstelling; • zoektermen; • zoeklocaties; • interview met (ervarings)deskundigen.	7	Stef Peeters	17
Evalueren en bijsturen projectplan, detailplanning.	7	Stef Peeters	1
2. Uitvoeringfase			
Uitvoering onderzoek			
Onderzoek houden	7 t/m 10	Stef Peeters	90
Afsluiting onderzoek			
Opstellen onderzoekrapport: • Data-analyse, alle verkregen data ordenen per deelvraag, bv. samenvatten interviews; • vraagstelling beantwoorden; • vergelijken van informatie op samenhang ; • conclusies trekken.	10	Stef Peeters	17
Evaluatie onderzoek	10	Stef Peeters	1
Uitloop onderzoek	11	Stef Peeters	33,25
Implementatie conclusie(s) onderzoek			

Alle gegevens, materialen van Delphi overplaatsen naar ID	12	Stef Peeters	6,25
Beschrijving centrale site op ID	12	Stef Peeters	9
Bouwen centrale site op ID	12	Stef Peeters	18
Ontwerpen test voor meting van beveiligingsbewustzijnniveau.	13	Stef Peeters	9
Middelen uitwerken om beveiligingsbewustzijn te verhogen (inclusief het maken van ondersteunende documentatie).	13 t/m 19	Stef Peeters	174,25
Pilot			
Pilot m.b.v. test voor meting beveiligingsbewustzijn	14 t/m 19	Stef Peeters	18
Afronding testfase • Verzamelen en evalueren van testresultaten • Maken testverslag (incl. advies)	20	Stef Peeters	28,75
Presenteren resultaten ib-coördinatoren Utrecht	21	Stef Peeters	9
Uitloop ontwerp- en realisatiefase	21	Stef Peeters	24,25
3. Afsluitingsfase			
Afronden afstudeerscriptie	22, 23	Stef Peeters	49,25
Evaluatie Project	23	Stef Peeters	2
Overige formaliteiten afhandelen	23	Stef Peeters	2
Presenteren aan stakeholders project	*24*	*Stef Peeters*	*9*
Effectief te besteden uren			**633**
Overige extra vrije uren			**54**
Totaal aantal uren			**687***

*De eis vanuit school gaat er vanuit dat de student 18 weken á 38 of 40 uur aan zijn afstudeerop-dracht werkt, tijdens deze periode heeft hij recht op 6 vakantie dagen. Dit komt neer op 636 werkuren bij een 38-urige werkweek en 672 uren bij een 40-urige werkweek[50].

Mijlpalenplanning

Fase	Mijlpaal	Geplande kalenderweek van oplevering	Toetsing
1	Mini plan van aanpak	0	John Verkooijen, Gerd Damen
1	Definitief projectplan	5	John Verkooijen, Gerd Damen, Ben van Zuijlen, Rob van Stratum (Fontys) en Martin van de Rijt (Fontys)
1	Definitieve probleemstelling	5	John Verkooijen, Gerd Damen, Ben van Zuijlen, Rob van Stratum (Fontys) en Martin van de Rijt (Fontys)
2	Onderzoek	10	John Verkooijen, Gerd Damen, Ben van Zuijlen
2	Beschrijving opbouw intranetsite ID	12	John Verkooijen, Gerd Damen, Ben van Zuijlen
2	Beschrijving test voor meting beveiligingsbewustzijnniveau	14	John Verkooijen, Gerd Damen, Ben van Zuijlen

[50] Afstudeerstagebrochure_BI_voorjaar_2010.doc

2	Beschrijving middel(en) ter verhoging beveiligingsbewustzijn	19	John Verkooijen, Gerd Damen, Ben van Zuijlen
2	Intranet site op ID	19	John Verkooijen, Gerd Damen, Ben van Zuijlen
2	Beveiligingsbewustzijnmiddel(en)	19	John Verkooijen, Gerd Damen, Ben van Zuijlen
2	Ondersteunende documentatie IB-coördinatoren	19	John Verkooijen, Gerd Damen, Ben van Zuijlen
3	Testverslag (incl. advies)	20	John Verkooijen, Gerd Damen, Ben van Zuijlen
4	Documentatie afronding project (eindpresentatie en afstudeerscriptie)	23	John Verkooijen, Gerd Damen, Ben van Zuijlen, Rob van Stratum (Fontys) en Martin van de Rijt (Fontys)

Resourceplanning

Benodigde resources/competenties	**2010**	**Uren totaal**
Stagiair afdeling IB	642	642
Stagebegeleider	63	63
Totaal	**705**	**705**

BEHEERSINGSMECHANISMEN

Tolerantie

Er is input van de afdeling IB gewenst m.b.t. de planning.

Change Management

Alle wijzigingen met een significante impact op scope, planning en te besteden uren worden door de projectmanager aan de stuurgroep Stage voorgelegd middels een bijgesteld projectplan.

Risicomanagement

Nr.	Risico beschrijving	Kans*	Impact**	Weging***	Maatregel	Eigenaar	Periode
R01	Beschikbaarheid medewerkers	6	6	36	Commitment Directie, bedrijfshoofd en afdelingshoofd	John Verkooijen	Heel project
R02	Langdurige ziekte	2	8	16	Uitvoer project overdragen	Stef Peeters	Heel project
R03	Het project is niet binnen de gestelde termijn afgerond	4	9	36	Per fase planning evalueren en eventueel bijstellen, wekelijks overleg	Stef Peeters	Heel project
R04	Gebrek aan coördinatie van mensen, middelen en activiteiten	4	6	24	Afdelingshoofd, stuurgroep Stage	John Verkooijen	Heel project
R05	Oorspronkelijke uitgangspunten en eisen veranderen (voortdurend) tijdens uitvoering van het project	4	8	32	Projectplan bijstellen	Stef Peeters	Heel project
R06	Meetbaarheid van sommige aspecten van beveiligingsbewustzijn is gecompliceerd of te tijdrovend.	8	8	64	Duidelijk melden aan opdrachtgever dat dit risico bestaat. Als dit probleem zich voordoet onmiddellijk melden bij opdrachtgever.	Stef Peeters	Laatste zes weken
R07	Fontys en SNS verschillen in	4	6	24	Vroegtijdig het projectplan	Stef Peeters	Eerste drie

	verwachtingspatroon				overleggen aan beide partijen zodat dit in overeenstemming met elkaar is		weken
R08	Te weinig tijd voor uitvoering project	7	5	35	Duidelijke planning opstellen, bij overschrijding planning onmiddellijk melden bij stagebegeleider.	Stef Peeters	Heel project
R09	Onduidelijke projectgrenzen	3	8	24	In de beginfase duidelijke afspraken vaststellen in projectplan.	Stef Peeters en John Verkooijen	Eerste drie weken
R10	Niet aan het project relevante werkzaamheden nemen te veel tijd in beslag	6	7	42	Duidelijke planning opstellen, weigeren van niet relevante werkzaamheden als daar geen tijd voor is.	Stef Peeters	Heel project
R11	Onervaren met binnen de organisatie gebruikte normen en technieken.	6	3	18	In de planning rekening houden met extra werk.	Stef Peeters	Heel project
R12	Kennisniveau of ervaringsniveau is te laag voor het goed afronden van dit project.	4	3	12	Genoeg tijd inplannen voor literatuurstudie.	Stef Peeters	Heel project
R13	Beschikbaarheid stagebegeleider te laag waardoor project niet goed verloopt.	3	7	21	Wekelijks een gesprek inplannen om voortgang van project te bespreken. Doet de situatie zich toch voor, contact opnemen met afdelingshoofd en eventueel andere	Stef Peeters en John Verkooijen	Heel project

					begeleiders aanvragen.		
R14	Opdracht/doelstelling uit het oog verliezen	4	6	24	Per week doelstellingen formuleren die bij de planning van die week passen om zo de planning te volgen.	Stef Peeters	Heel project

* Geeft de kans op een gebeurtenis, bij 1 is de kans nihil en bij 9 bijna zeker.

** Geeft de impact aan als van een gebeurtenis, bij 1 is de impact te verwaarlozen en bij 10 desastreus.

*** De weging is impact maal kans van een risico.

Kwaliteitsmanagement

Tussenproducten

Product	**Aspecten waarop getoetst gaat worden (kan >1 per product zijn)**	**Motivatie**
Projectplan	• Consistentie met opdrachtomschrijving • Aanwezigheid benodigde onderdelen • SMART-formulering van doelstellingen	• *Risico R03* • *Risico R07* • *Risico R08* • *Risico R09* • *Risico R10* • *Risico R11* • *Risico R12* • *Risico R14*
Literatuuronder-zoekopzet	• Doelstelling is relevant • Vraagstelling is relevant • Zoektermen en zoeklocaties zijn relevant • Doelgroepen / persona's zijn relevant	• *Risico R06* • *Risico R11* • *Risico R12* • *Risico R14*
Literatuuronder-zoekrapport	• Consistent met de doelstelling • Vraagstelling beantwoordt, zo niet moet er een geformuleerd zijn motivatie zijn • Verslagen over interviews met (ervarings)deskundigen zijn consistent met hun verhaal • Onderzoeksresultaten zijn relevant	• *Risico R06* • *Risico R12* • *Risico R14*
Beschrijving test beveiligingsbewustzijn niveau	• Meting op de goede aspecten • Breedte van dekkingsgebied test	• *Risico R06*

Eindproduct

De te toetsen aspecten worden op een groep gebruikers getest. De geselecteerde groep dient uit minimaal 10 personen te bestaan die voorkomen in de doelgroep. Voor de beschrijving van de doelgroep wordt verwezen naar het definitie document.

Product	Aspecten waarop getoetst gaat worden (kan >1 per product zijn)	Motivatie
Beschrijving middel(en) ter verhoging beveiligingsbewustzijn	• Betrouwbaar • Niet langdradig • Duidelijk en overzichtelijk • Bruikbaar binnen SNS REAAL	• *Risico R06* • *Risico R12* • *Risico R14*
Intranetsite op ID Beveiligingsbewustzijnmiddel(en)	• Ontwerp is overzichtelijk en functioneel • Middelen voldoen aan de gestelde criteria	• *Risico R14* • *Risico R14*

Proces-Kwaliteit

De kwaliteit wordt gewaarborgd door onder andere gebruik te maken van gerenommeerde methoden (PMW professional, Baronscourt), technieken(SharePoint) en principes (SMART, KOLB). Interne en externe begeleiders zullen de producten van de afstudeerder controleren. Hierdoor is de kans groter dat de beloofde kwaliteit ook waargemaakt wordt. Alle mijlpalen worden in concept versie gekeurd door beide interne begeleiders alvorens deze opgeleverd worden.

Proces	Aspecten waarop getoetst gaat worden (kan >1 per product zijn)	Motivatie
methodiek	• Fasering • Consistentie documentatie • Striktheid uitvoering	• *Ter structuur.* • *Risico R03* • *Risico R07* • *Risico R09* • *Risico R11* • *Risico R14*
planning	• Striktheid uitvoering planning • Uitloop	• *Risico R03* • *Risico R08* • *Risico R10* • *Risico R11* • *Risico R12* • *Risico R14*
Kennisver-werving	• Zelfstandigheid • Durft vragen te stellen	• *Risico R11* • *Risico R12*
Voortgang	• Rapportage geeft inzicht • Voortgangsgesprek geeft inzicht	• *Risico R06* • *Risico R13*
Reflectie	• Opmerken problemen of probleemgebieden • Ontstane situatie na wijziging projectkoers	• *Risico R05* • *Risico R06* • *Risico R12* • *Risico R14*

Configuration Management

Per dag dat er aan een document iets wordt gewijzigd wordt het versienummer met één tiende verhoogd. Elke keer als een interne of externe begeleider iets wijzigt wordt het versienummer met één honderdste verhoogd. Als een wijziging aan het document gemaakt is wordt dit aangegeven op de tweede pagina in de tabel versiebeheer. Definitieve documenten hebben een versie nummer met een heel getal, een voorbeeld:

Datum wijziging	Opmerking	Door	Versie
2-2-2010	Eerste concept versie	Stef Peeters	0.1
3-2-2010	Tweede concept versie	Stef Peeters	0.2
4-2-2010	Controle interne/externe begeleider	John Verkooijen	0.2.1
5-2-2010	Derde concept versie	Stef Peeters	0.3.1
7-2-2010	Controle interne/externe begeleider	Rob van Stratum	0.3.2
8-2-2010	Eerste definitieve versie	Stef Peeters	1.0

Bijlage A Verklarende woordenlijst

Woord	**Omschrijving**
Beschikbaarheid, integriteit en vertrouwelijkheid	Beschikbaarheid is de mate waarin informatie beschikbaar is voor de gebruiker en het informatiesysteem in bedrijf is op het moment dat de organisatie deze nodig heeft. Integriteit is de mate waarin de informatie actueel en zonder fouten is. Kenmerken van integriteit zijn de juistheid en de volledigheid van de informatie. Vertrouwelijkheid is de mate waarin de toegang tot informatie beperkt is tot een gedefinieerde groep die daar rechten toe heeft. Hieronder vallen ook maatregelen die de privacy beschermen. [51]
BIV	Zie omschrijving: *'Beschikbaarheid, integriteit en vertrouwelijkheid'.*
Beveiligingsbewustzijn	Beveiligingsbewustzijn is bewust zijn van de informatiebeveiligingbehoeftes en de hiervoor ontwikkelde voorschriften en procedures.
IB	Informatiebeveiliging
IB-coördinatoor	Zie omschrijving: *'Informatiebeveiliging-coördinatoor'*
Informatiebeveiliging-coördinatoor	Medewerkers buiten de informatiebeveiliging afdeling, die de verantwoordelijkheid hebben gekregen om het niveau van informatiebeveiligingsbewustzijn te meten en verhogen. Ook fungeren zij als aanspreekpunt voor andere medewerkers.
ID	Centrale intranetsite van SNS REAAL.
Informatiebeveiliging	Is het geheel van preventieve, detectieve, repressieve en correctieve maatregelen alsmede procedures en processen die de beschikbaarheid, exclusiviteit en integriteit van alle vormen van informatie binnen een organisatie of een maatschappij garanderen, met als doel de continuïteit van de informatie en de informatievoorziening te waarborgen en de eventuele gevolgen van beveiligingsincidenten tot een acceptabel, vooraf bepaald niveau te beperken. [52]
Informatiebeveiligingincidenten	Een (informatie)beveiliging incident is een enkele of serie van ongewenste of onverwachte gebeurtenissen welke een significante kans hebben op het veroorzaken van een ramp, het compromitteren van de

[51] http://www.ibpedia.nl/index.php?title=Basiskennis_-_Informatie%2C_bedrijfsdoelstellingen_en_kwaliteitseisen#Beschikbaarheid.2C_Integriteit_en_Vertrouwelijkheid

[52] http://nl.wikipedia.org/wiki/Informatiebeveiliging

	bedrijfsprocessen en een bedreiging vormen t.a.v. de beveiliging. [53]
Pilot	Een experiment waarbij gekeken wordt of een product naar behoren werkt.
Stakeholder	Een persoon of organisatie die belangen heeft in dit project.

[53] NAVI_Begrippenkaders_definities_en_afkortingen.pdf