Fontys Hogeschool ICT

SNS Bank

SNS IT aantoonbaar 'In Control' door ISO27001 certificering

Van BS7799-2 norm naar nieuw beheerproces voor Informatiebeveiliging: ISO27001

Afstudeerscriptie

Uitgebracht aan	Dhr. Ben van Zuijlen, Dhr. John Verkooijen, Dhr. Gerd Damen (SNS Bank) Dhr. Adri Cornelissen, Marco Dorenbos (Fontys) Dhr. W.A. van den Bosch (extern deskundige) Fontys afstudeerstagebureau
Datum	12 juni 2009
Bedrijf	SNS Bank
Bedrijfsonderdeel	SNS IT
Afdeling	Informatiebeveiliging & Controle
Project	Interne Certificering volgens ISO27001
Opdrachtgever	Ben van Zuijlen
Opdrachtnemer	Paul Welles
Plaats	's-Hertogenbosch
Versie	1.0
Auteur	Paul Welles

Titelpagina

Naam stageverlenende instelling:	SNS REAAL - SNS Bank - SNS IT
Afdeling:	Informatiebeveiliging & Controle (IB&C)
Bezoekadres:	Pettelaarpark 120, 5201 DZ Den Bosch
Postadres:	Postbus 70053
Telefoonnummer:	073-6833333
Faxnummer:	073-6833600
Naam bedrijfsbegeleiders:	Dhr. John Verkooijen/Dhr. Gerd Damen
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. Adri Cornelissen
Naam 2de afstudeerstagedocent:	Dhr. Marco Dorenbos

Naam stagiair:	Paul Welles
Studentnummer:	2074835
Adres:	Horsterweg 88
Postcode/Woonplaats:	5971 NG Grubbenvorst
E-mailadres:	paul.welles@sns.nl
Telefoonnummer:	06-13457917
Stageperiode:	2 februari 2009 t/m 26 juni 2009

Voorwoord

In het kader van mijn afstudeerstage voor de opleiding Bedrijfskundige Informatica heb ik deze scriptie mogen schrijven. Dit document bevat de uitwerking van de afstudeeropdracht die ik heb uitgevoerd bij de SNS Bank, grootbank in financiële dienstverlening, te 's-Hertogenbosch, van 2 februari 2009 t/m 26 juni 2009.

De opdracht die ik heb uitgevoerd betreft het ontwikkelen van een methodiek om organisatie-onderdelen van SNS IT intern te kunnen certificeren volgens de ISO 27001 standaard. Deze standaard beschrijft het beheerproces om te komen tot een ingevuld Information Security Management System (ISMS). Daarnaast wordt in het certificeringstraject ook gesteund op de ISO27002 standaard die een aantal concrete informatiebeveiligingsmaatregelen bevat waaraan de bedrijfsdelen binnen SNS IT dienen te voldoen. Op basis hiervan kunnen organisatieonderdelen aantonen 'In Control" te zijn op het gebied van beheersings van informatiebeveiligings-risico's. Naast de ontwikkeling van de methodiek behoorde ook een pilotfase tot de opdracht. Tijdens deze pilot werd de ontwikkelde methodiek getest en doorliep een specifiek bedrijfsonderdeel van SNS IT het gehele interne certificeringstraject.

Mede via deze weg wil ik allereerst mijn opdrachtgever en afdelingshoofd IB&C, dhr. Ben van Zuijlen, bedanken 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 Bank. Daarnaast wil ik hem, maar ook mijn stagebegeleiders dhr. John Verkooijen en dhr. Gerd Damen, bedanken voor de begeleiding en de ondersteuning tijdens mijn afstudeerperiode, evenals voor de terugkoppeling op al mijn gerealiseerde mijlpaalproducten.

Verder wil ik graag dhr. Robert Lauwen, dhr. Kees van Maaren, dhr. Leon Kers, dhr. Roland Molier, dhr. Job Joosten en dhr. Rutger Schulte van afdeling IB&C alsook de mensen van bedrijfsonderdeel Relatiebeheer en andere medewerkers van afdelingen met wie ik tijdens mijn afstudeerperiode heb samengewerkt c.q. te maken heb gehad, bedanken voor hun ondersteuning en inzet m.b.t. het door mij uitgevoerde project. Ook aan de lezers van mijn scriptie ben ik dank verschuldigd voor hun feedback.

Mijn laatste dankwoord gaat uit naar de Fontys Hogeschool ICT, en in het bijzonder naar dhr. Adri Cornelissen en dhr. Marco Dorenbos, die mijn afstuderen hebben begeleid vanuit de opleiding Bedrijfskundige Informatica.

Tot slot wens ik de SNS Bank, en in het bijzonder SNS IT en afdeling IB&C, veel succes in de toekomst en ik ben ervan overtuigd dat er met de nieuwe certificeringmethodiek een basis is gelegd om alle bedrijfsonderdelen van SNS IT op een efficiënte wijze intern te kunnen certificeren.

's-Hertogenbosch, 12 juni 2009,

Paul Welles
Bedrijfskundige Informatica
Fontys Hogeschool ICT

Inhoudsopgave

Samenvatting **5**

Summary **6**

Verklarende woordenlijst **7**

1. Inleiding **8**

2. Het bedrijf **9**

2.1. SNS REAAL 9

2.2. SNS Bank 9

2.3. SNS IT 10

2.4. Afdeling Informatiebeveiliging & Controle 10

3. De opdracht **14**

3.1. Aanleiding van de opdracht 14

3.2. Probleemstelling 14

3.3. Projectdoelstelling 15

3.4. Toelichting op de projectdoelstelling 15

3.5. De gewenste situatie 16

3.6. Concrete opdrachtomschrijving 18

4. Raamwerk van het project **19**

4.1. Pilotfase certificering 19

5. Methoden en werkwijzen **20**

5.1. Project Matig Werken - Professional (PMW-P) 20

5.2. PDCA-cyclus 21

5.3. ISRAC 24

5.3.1. Business Impact Analyse *24*

5.3.2. Threats and Vulnerability Assessment *25*

5.3.3. List Of Controls *25*

6. Definitie -en initiatiefase: Literatuuronderzoek ISO27000 ..... **26**

6.1. BS17799 versus ISO27000 26

6.2. Conclusies en aanbevelingen uit het onderzoek 27

7. Ontwerpfase: ISMS Toolkit **28**

7.1. Procesbeschrijving ISMS 28

7.2. Procedurebeschrijving intern certificeren 29
7.3. Controlebrief 29
7.4. Business Impact Analyse 29
7.5. Overzicht beleidsdocumenten 30
7.6. Vragenlijst IB-activiteiten 30
7.7. IB-Jaarplan 31
7.8. Beoordeling beveiligingsbewustzijn 31
7.9. Beoordeling afhandeling actiepunten 32
7.10. Documentkwaliteit 32
7.11. Controlerapport 34
7.12. ISO27001 certificaat 35
7.13. Presentatie introductie ISO2700X 35
7.14. Workshop ISMS 35
7.15. Presentatie afdelingsoverleg 36
8. Implementatie en testfase: Certificeringproces Relatiebeheer 37
8.1. Relatiebeheer 37
8.2. Informeren van het management Relatiebeheer 38
8.3. Introductie ISO27000 bij Relatiebeheer 38
8.4. Uitvoering workshop ISMS 38
8.5. Risicoanalyse m.b.v. ISRAC 38
8.6. Actie –en verbeterpunten 39
8.7. Presentatie overleg Relatiebeheer 39
8.8. Controlerapportage 39
8.9. Uitreiking ISO27001 certificaat 40
9. Conclusies en aanbevelingen 41
Evaluatie 42
Literatuurlijst 43
Bijlagen 44
A Projectplan 45
B Samenvatting bijstuurmomenten 59

Samenvatting

De afdeling Informatiebeveiliging & Controle van het bedrijfsdeel SNS IT, de IT afdeling van de financiële dienstverlener SNS Bank, heeft de afgelopen jaren zorg gedragen voor de interne certificering van SNS IT volgens BS7799-2. Dit is een internationale norm voor Informatiebeveiliging (IB) waaraan SNS Bank wil voldoen. Omdat er sinds het jaar 2007 een nieuwe standaard voor Informatiebeveiliging is ontwikkeld, namelijk ISO27001, is er aanleiding geweest voor SNS Bank om de overstap te maken naar deze nieuwe norm. Ook het tijdens het project geschreven literatuuronderzoek heeft hier een bevestigende rol in gespeeld. Beide normen beschrijven het proces om te komen tot een Information Security Management System (ISMS). Het ISMS is een management systeem dat een aantal beleidsonderdelen bevat, welke zich bezighouden met information security management. De belangrijkste 'key' van het ISMS voor SNS Bank is het ontwerpen, implementeren en onderhouden van een samenhangend pakket van processen en systemen voor het effectief beheren van de toegankelijkheid van informatie en daarnaast ook het minimaliseren van informatiebeveiligingsrisico's. In ISO27002, de concrete invulling van de ISO27001, staan 133 beheersmaatregelen beschreven op het gebied van informatiebeveiliging.

Het management is eindverantwoordelijk voor de informatiebeveiliging van het betreffende bedrijfsonderdeel van SNS IT. Per afdeling is er een IB-coördinator benoemd welke het management en de medewerkers ondersteunt m.b.t. de communicatie en naleving van het informatiebeveiligingsbeleid.

Tijdens het uitvoeren van het afstudeerproject 'Interne Certificering volgens ISO27001' is een nieuwe certificeringmethodiek ontwikkeld, wat binnen SNS IT de 'ISMS Toolkit' wordt genoemd. Deze toolkit is ontwikkeld zodat de bedrijfsonderdelen van SNS IT dit als hulpmiddel kunnen gebruiken voor de invulling van hun eigen ISMS. In de ISMS Toolkit is een procesbeschrijving van het beheer van het ISMS opgenomen, waarin staat hoe SNS REAAL haar risico's op het gebied van informatiebeveiliging beheerst. Daarnaast maakt een procedurebeschrijving van de certificering deel uit van de ISMS Toolkit. Verder is er een aantal templates ontwikkeld waarmee de invulling van het ISMS kan worden gerealiseerd.

De certificeringmethodiek is vervolgens getest en met succes uitgevoerd in een pilotfase bij het bedrijfsonderdeel Relatiebeheer van SNS IT. Hieruit kan geconcludeerd worden dat de templates uit de ISMS Toolkit primaire hulpmiddelen zijn en dat deze de meest belangrijke elementen zijn voor de totstandkoming van het ISMS. De bevindingen en resultaten van de pilotfase zijn in een controlerapport verwerkt, welke is ondertekend door het bedrijfshoofd van het bedrijfsonderdeel Relatiebeheer. Daarmee verklaart men dat het voldoet aan de eisen zoals die gesteld zijn in ISO27002. Door middel van het intern uitgereikte ISO27001 certificaat kan Relatiebeheer overleggen dat het aantoonbaar 'In Control' is op het gebied van Informatiebeveiliging.
Op basis van het bovenstaande verdient het de aanbeveling om de nieuwe certificeringmethodiek te blijven gebruiken voor alle bedrijfsonderdelen van SNS IT. Tot slot is het aanbevolen om de nog te publiceren ISO-reeksen nauwlettend in de gaten te houden, voornamelijk ISO27015, welke gespecificeerd wordt voor financiële dienstverleners.

Summary

The Information Security & Audit department of SNS IT, the IT division of the financial service provider SNS Bank, has in recent years ensured the internal certification according to BS7799-2. This is a international norm for Information Security which SNS Bank wishes to comply. Because since the year 2007 a new standard for Information Security has been developed, ISO27001, it was a reason for SNS Bank to make the transition to this new standard. The research based on literature was affirmative on this matter. The BS7799-2 standard is so outdated that SNS IT is no longer detectable 'In Control'.

ISO27002 is a norm which is a completion of ISO27001 and consists of 133 specific security measures in the field of Information Security. Both standards describe the process to establish an Information Security Management System (ISMS). The ISMS is a management system that contains a number of policies, which are concerned with information security management. The main key of the ISMS for SNS Bank is to design, implement and maintain a coherent set of processes and systems to manage the accessibility of information effectively and also to minimize information security risks.

During the implementation of the project 'Internal Certification according to ISO27001' a new certification methodology is developed, which is called the 'ISMS Toolkit'. This toolkit is designed so that SNS IT departments can use this tool for implementing their ISMS. The ISMS is built according the Plan-Do-Check-Act cycle. The persistence of this 'cycle' will ensure the continuous planning, implementation, monitoring and adjusting of the ISMS and forces the IS coordinators to keep the ISMS up to date. Each department of SNS IT has its own IS coordinator assigned, which is responsible for the communication and compliance of the information security policy in his/her own department.

The ISMS Toolkit features a process description of the ISMS, which describes how SNS REAAL controls their risks in the field of information security. In addition, there is a procedure describing the internal certification process of the ISMS Toolkit. There are also a number of templates developed so that the completion of the ISMS can be realized.

The new certification method is tested and is successfully implemented in a pilot in the department Relatiebeheer of SNS IT. There can be concluded that the templates from the ISMS Toolkit are primary tools and that it contains the most important elements for the establishment of the ISMS. The findings and results of the pilot are set in an audit report, signed by the holder of Relatiebeheer.

Relatiebeheer has stated that it meets the requirements as mentioned in ISO27001. By showing the ISO27001 certificate, Relatiebeheer can prove that it is 'In Control' in the field of Information Security.

Based on the foregoing, it is recommended that SNS IT keeps using the new certification methodology for certifying all departments of SNS IT. Finally, it is recommended to monitor the ISO standards which still have to be published. Especially ISO27015, which specifies information security for banks.

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.

AAP, 32
Account Management, 37
Architectuur, 10
Audits, 11
Aware, 12
Best practices, 11
BIA, 24, 29
BIV, 19, 35
BS17799, 16
BS7799-1, 15
BS7799-2, 15
Certificeringsaudit, 26
Code voor Informatiebeveiliging, 8
Core business, 10
DS, 10
Flexwerkplekken, 13
IB, 5
IB-jaarplan, 30
Informatiebeveiliging & Controle, 10
Information Security Management System, 15
IS, 10
ISMS, 15
ISMS Toolkit, 28
ISO 27000, 8
ISO 27015, 27, 41
ISO27001, 5
ISO27002, 5
ISRAC, 16
KKM, 10
Literatuuronderzoek, 24
LOC, 25
Ontwikkeling, 10
PDCA-cyclus, 21
Pilot, 27
PMW-P, 20
RACI, 29
Relatiebeheer, 10
Security management rapportages, 11
Security monitoring, 11
Servicedesk, 37
SLA's, 37
SLM, 37
SNS Bank, 9
SNS IT, 8, 10
SNS REAAL, 9
SPOK, 33
Telethuiswerken, 13
Templates, 5
TVA, 25

1. Inleiding

“Gezond verstand, gezond geweten”

Informatie is tegenwoordig het belangrijkste bezit van organisaties. Zonder de benodigde en juiste informatie is het niet mogelijk om bedrijfsprocessen goed te laten verlopen. Immers, als een bedrijfsproces geen informatie als input heeft, zal het proces stil liggen. Omdat niet ieder individu bevoegd is bepaalde informatie in te zien, te muteren en/of te verwijderen, is het belangrijk dat de informatie beveiligd wordt. Want informatie deel je, maar niet met iedereen. Bij de SNS Bank is dit belangrijk, omdat het financiële gegevens bezit van duizenden klanten en leveranciers, maar bijvoorbeeld ook informatie bezit over kritische processen en informatiesystemen.

De SNS Bank heeft een speciale afdeling ‘Informatiebeveiliging & Controle’ (IB&C) in het leven geroepen om de handhaving en naleving van de door haar opgestelde regels en eisen m.b.t. informatiebeveiliging te bewaken. IB&C geeft ook beveiligingsadviezen en voert controles uit. Verder streeft men naar het ‘naar een hoger niveau tillen’ van het beveiligingsbewustzijn: gezond verstand, gezond geweten.

Sinds 2007 is SNS IT, bedrijfsonderdeel van de SNS Bank, gecertificeerd volgens de internationale standaard voor Informatiebeveiliging. In deze standaard, de British Standard 7799-1 (BS7799-1), staat het proces beschreven welke eisen stelt aan informatiebeveiliging en waar SNS Bank aan wil voldoen. De huidige standaard kan echter wegens veroudering niet voldoen aan de eisen op het gebied van informatiebeveiliging. Om de beveiliging naar een hoger niveau te tillen is de overstap gemaakt naar de ‘nieuwe’ Code voor Informatiebeveiliging. Deze nieuwe norm heet ‘International Organization for Standardization 27002’ (ISO 27002) en bestaat uit verschillende beheersingsmaatregelen.

Vanwege de plannen voor implementatie van deze nieuwe norm, is er een ‘pilot’ uitgevoerd waarbij één bedrijfsonderdeel succesvol is gecertificeerd volgens ISO 27001, waarin het beheerproces is beschreven. Deze pilot is de basis van alle certificering- trajecten die dit jaar gaan plaatsvinden binnen SNS IT. Voordat de pilot van start is gegaan, was het zaak om een nieuwe certificeringmethodiek te bedenken, de zogenaamde ISMS Toolkit, waarbij de nadruk sterk ligt op documentatie en de totstandkoming van het Information Security Management System (ISMS). Het ISMS is bedoeld om kritische processen en systemen binnen organisaties vast te stellen, te implementeren en uit te voeren, te controleren en te beoordelen en bij te houden en te verbeteren op het gebied van informatiebeveiliging. Door het documenteren van het ISMS wordt de kans op beveiligingsrisico’s kleiner en de impact teruggedrongen.

Hoofdstuk 2 bevat informatie over SNS Bank, maar in het bijzonder over SNS IT en de afdeling IB&C. Hoofdstuk 3 bespreekt de details over de opdracht en het uitgevoerde project, maar ook de opgeleverde eindproducten. Hoofdstuk 4 haakt in op het projectraamwerk. In hoofdstuk 5 worden de gebruikte methoden en werkwijzen beschreven. Hoofdstuk 6 vertelt over het uitgevoerde literatuuronderzoek in het kader van ISO27000. In hoofdstuk 7 wordt de certificeringmethodiek besproken, terwijl hoofdstuk 8 het uitgevoerde certificeringproces van bedrijfsonderdeel Relatiebeheer beschrijft. Hoofdstuk 9 geeft tot slot de bevindingen weer in de vorm van conclusies en aanbevelingen.

2. Het bedrijf

"Zo kan het ook"[1]

Dit hoofdstuk zal ingaan op het bedrijf waar het project is uitgevoerd, hoe de structuur van het bedrijf eruit ziet en hoe de afdeling Informatiebeveiliging & Controle is opgebouwd en functioneert. Verder wordt ook informatie verstrekt over de werkomgeving en de Gouden Regels in het kader van Informatiebeveiliging.

2.1. SNS REAAL

SNS REAAL is een financiële dienstverlener voor de particulier en het Midden -en Klein Bedrijf (MKB) in Nederland. SNS REAAL heeft een lange historie in de Nederlandse samenleving en is voortgekomen uit verschillende regionale spaarbanken en diverse verzekeringsmaatschappijen, die van oorsprong verdeeld waren over twee aparte concerns: SNS Bank en REAAL Verzekeringen. SNS REAAL is met een balanstotaal van € 124 miljard en 7.500 medewerkers (fte's) een van de grote bank-verzekeraars van Nederland. Tot SNS REAAL behoren ook diverse verkooplabels die op een specifieke markt werkzaam zijn: ASN Bank, BLG Hypotheken, SNS Regio Bank, Proteq, SNS Property Finance, SNS Securities, SNS Assurantiën, SNS Asset Management en Route Mobiel.

2.2. SNS Bank

De geschiedenis van SNS Bank gaat terug tot in de 19e eeuw. SNS staat voor Samenwerkende Nederlandse Spaarbanken REAAL. In 1817 werd de eerste Nederlandse spaarbank opgericht. Sparen was toen vooral een middel om de zelfredzaamheid van Nederlanders te bevorderen. Die zelfredzaamheid staat ook nu nog centraal bij SNS Bank. SNS Bank is onderdeel van SNS REAAL. SNS Bank is gevestigd in Utrecht (hoofdkantoor) en 's-Hertogenbosch (zie figuur 2).

Met circa 3.200 medewerkers behoort SNS Bank tot de top 5 van banken in Nederland. Spaarbanken zijn oorspronkelijk de banken waar individuele burgers hun geld onderbrachten. Een spaarbank gebruikte dat geld dan eventueel weer voor het verstrekken van hypotheken. Tegenwoordig zijn er niet veel echte spaarbanken meer. De oorzaak hiervan is dat deze banken zich hebben samengevoegd en hun dienstenaanbod vergroot hebben.

[1] Bron: slogan SNS Bank

2.3. SNS IT

De afdeling SNS IT is onderdeel van SNS Bank en verzorgt met ruim 400 medewerkers de IT-dienstverlening binnen SNS Bank. Het onderdeel SNS IT bestaat uit verschillende bedrijfsonderdelen, dat naast de stafafdelingen Informatiebeveiliging & Controle, Kennis, Kwaliteit en Management (KKM), Programma Management en het Secretariaat ook de bedrijfsonderdelen Architectuur, Infrastructuur Services (IS), Ontwikkeling, Datacenter Services (DS) en Relatiebeheer heeft (zie figuur 1).

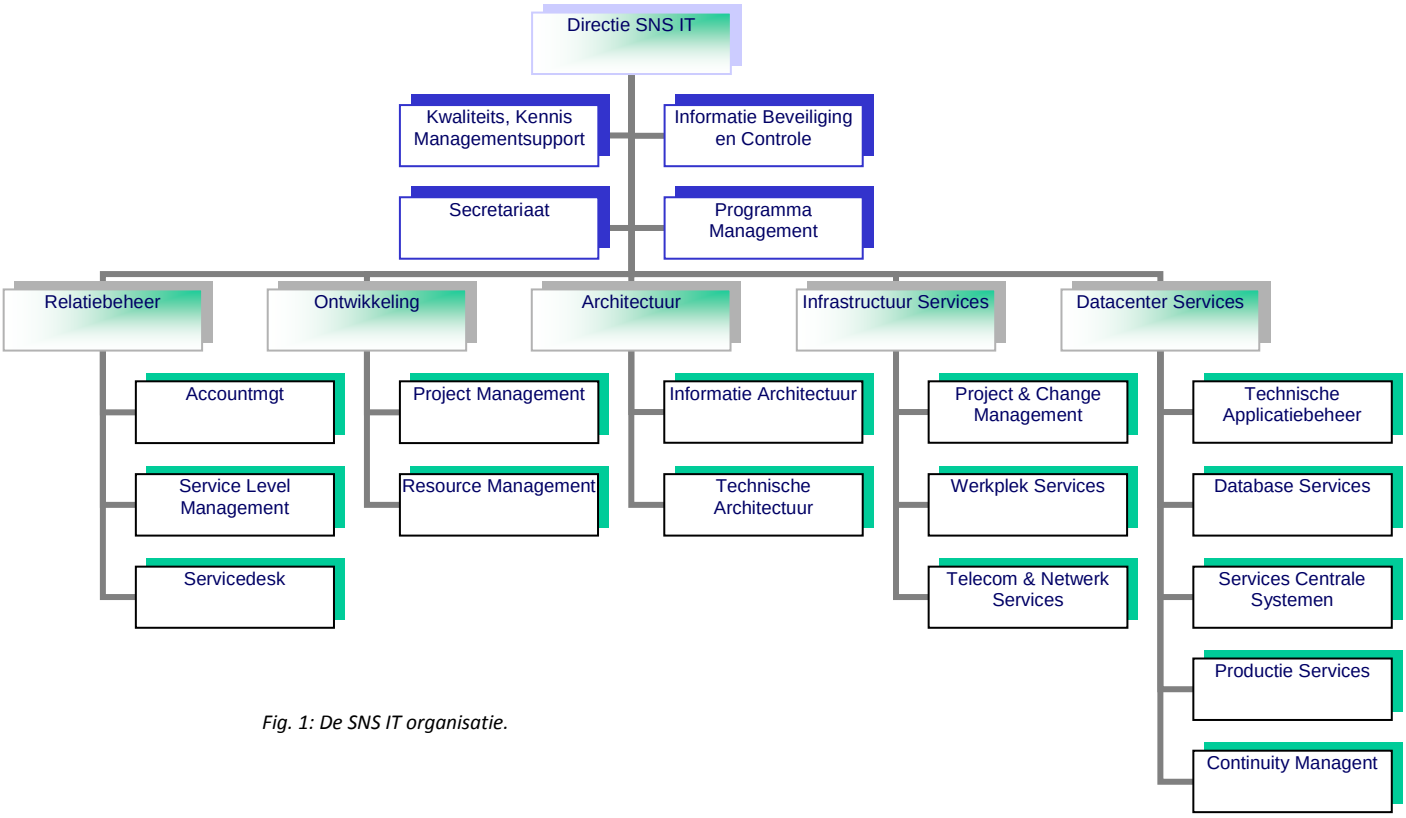


Fig. 1: De SNS IT organisatie.

2.4. Afdeling Informatiebeveiliging & Controle

De afdeling IB&C is één van de stafafdelingen van SNS IT en heeft als 'core business[2]' het toepassen, waarborgen en onderhouden van informatiebeveiliging en het hierin ondersteunen van SNS Bank en SNS REAAL. Informatiebeveiliging is voornamelijk gericht op het beheersen van het risico dat bedrijfsprocessen en informatievoorziening onvoldoende integer, niet continu of onvoldoende beveiligd worden ondersteund door IT[3].

[2] De kernactiviteiten van een onderneming (smal assortiment). De onderneming beperkt zich tot die taken waarin men goed is en waarmee winst valt te behalen (Bron: http://www.computerwoorden.nl/direct--19194--Core%20business.htm).

[3] Bron: informatiemap 'nieuwe medewerkers SNS Bank'

IB&C stelt beheersdoelstellingen en beheersmaatregelen op volgens normen die staan beschreven in de code van de ISO 27000 reeks. Dit is een set van 'best practices' die wordt ingevuld in de informatiebeveiligings- structuur van SNS REAAL en SNS Bank. Best practice gaat er van uit dat er een techniek, methode, proces, activiteit of beloningmethodiek is die effectiever is om een bepaald resultaat te halen dan enige andere techniek, methode, etc. Bij het concept Best Practice staat praktijkervaring centraal. Het uitgangspunt is dat met de juiste processen, controles en tests een project uitgevoerd kan worden met minder problemen, minder onvoorziene complicaties en betere eindresultaten.

Fig. 2: Vestiging SNS Bank 's-Hertogenbosch. Hier bevinden zich de bedrijfsdelen SNS IT en Asset Management.

De afdeling verleent een aantal diensten en voert activiteiten uit die onderscheiden worden op het gebied van advies en controle. Adviesdiensten zijn bijvoorbeeld het opstellen van beleid en voorschriften, het geven van op maat gemaakte beveiligingsadviezen, het ondersteunen van activiteiten om het beveiligingsbewustzijn binnen SNS op het gewenste niveau te brengen en te houden, het uitvoeren van risicoanalyses voor IT en het opstellen van security management rapportages[4].

De 'controlekant' van de afdeling heeft het uitvoeren van audits[5] en beveiligingscontroles, het onderzoeken van security incidenten en security monitoring [6] in haar takenpakket.
IB&C heeft inclusief de leidinggevende in totaal 9 medewerkers in dienst. In figuur 3 is het organigram van de SNS IT-directie weergegeven, waar afdeling IB&C ook in vertegenwoordigd is:

[4] Rapportage waarin beschreven staat hoe het security management proces is ingericht. Daartoe vindt een beoordeling plaats voor vier belangrijke aspecten van security management, namelijk het beveiligingsniveau, beveiligingsbewustzijn, bedrijfscontinuïteit en de afhandeling van verbeterpunten.

[5] Beoordelingen van de automatisering van de organisatie en de organisatie van de automatisering.

[6] Actieve controle van beveiligingsinstellingen en passieve controle (achteraf) van onder meer loginformatie.

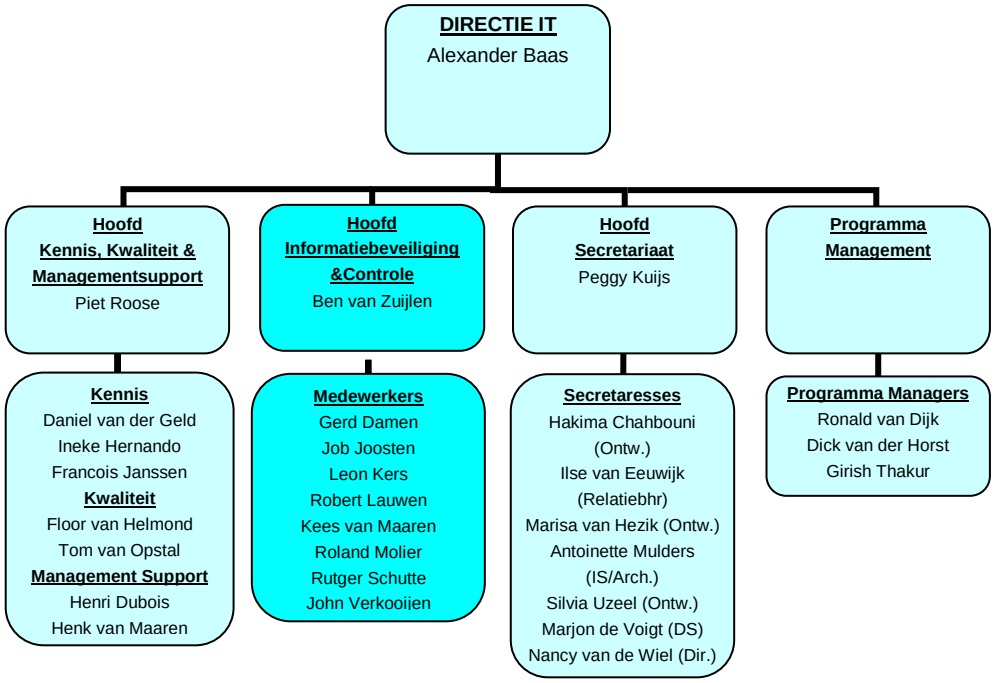


Fig. 3: organigram IT-directie. De afdeling IB&C is hierbij uitgelicht.

Zoals in figuur 3 te zien is, is de afdeling IB&C samen met de afdelingen KKM, het Hoofdsecretariaat en Programmamanagement vertegenwoordigd in de personen van respectievelijk dhr. Ben van Zuijlen, dhr. Piet Roose en mw. Peggy Kuijs. Dit zijn de verschillende afdelingshoofden. Hieronder werken momenteel 26 medewerkers (exclusief stagiairs). Alle afdelingen bevindingen zich in dezelfde ruimte op de 2de verdieping van het SNS gebouw in 's-Hertogenbosch, met uitzondering van Programma Management.

Afdeling IB&C maakt het management, de leidinggevenden en de medewerkers van SNS Bank 'aware[7]' van het feit dat de regels voor informatiebeveiliging nageleefd dienen te worden. Dit doet men onder andere aan de hand van de 7 gouden regels van Informatiebeveiliging:

Gouden Regels voor Informatiebeveiliging[8]

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.

[7] Engelse benaming voor Bewustwording

[8] Bron: 7 gouden regels van Informatiebeveiliging van SNS Bank

Deze Gouden Regels worden ondermeer tijdens awareness-sessies, IB-cursussen en contactmiddagen voor IB-coördinatoren veel gecommuniceerd.

De zogenaamde ‘flexwerkplekken’ (zie fig. 4) en het ‘telethuiswerken’ zorgen ervoor dat er overal gewerkt kan worden. Hierdoor worden medewerkers van de SNS werkplekonafhankelijk. Dat geeft enorm veel flexibiliteit.

Fig. 4: de flexwerkplekken bij SNS IT.

Door het gebruik van flexwerkplekken kunnen medewerkers op alle plekken in het gebouw werken met de voor hun beschikbare informatiesystemen (op basis van autorisaties). Het ‘telethuiswerk-concept’ is ontwikkeld zodat er een flexibele werkomgeving kan worden gecreëerd, dus ook in de thuisomgeving. Met behulp van smartcards kunnen medewerkers vanuit thuis inloggen op de informatiesystemen en terminal servers [9]van SNS Bank. Afdeling IB&C ziet informatiebeveiliging dan ook als een van de belangrijkste pijlers voor de flexibilisering van (telethuis)werken en bedrijfsprocessen.

Fig. 5: de Smartcard die binnen SNS REAAL sinds een jaar officieel in gebruik is genomen. De Smartcard kan gebruikt worden op de werkplek (fat clients en notebooks), alsook voor het telethuiswerken. Het is nu ook nog mogelijk om via het Windows inlogscherm aan te loggen; in de nabije toekomst wordt deze Smartcard echter volledig ingevoerd, zowel voor logische als fysieke toegangsbeveiliging.

[9] Een terminal server is een gespecialiseerde computer die om kan gaan met meerdere communicatiekanalen tegelijkertijd.

3. De opdracht

Beheersing van beveiligingsrisico's

Dit hoofdstuk beschrijft alle aspecten die betrekking hebben op het uitgevoerde project. De aanleiding van de opdracht en de concrete probleemstelling worden besproken, evenals het doel van het project. Vanuit deze onderwerpen wordt er ingegaan op de gewenste situatie inclusief de op te leveren eindproducten en de concrete opdrachtomschrijving.

3.1. Aanleiding van de opdracht

Omdat de bedrijfsonderdelen binnen SNS Bank gecertificeerd zijn volgens BS7799-2, is het belangrijk dat er wordt onderzocht waarom de overstap naar ISO27001 nodig is. Uit het opgestelde literatuuronderzoek (zie externe bijlage XX) is de conclusie getrokken dat de huidige BS 17799 vervangen dient te worden door de nieuwe ISO 27000 norm. De reden hiervoor is dat de BS 17799 zodanig verouderd is dat de SNS Bank niet 100% voldoet aan de beheersingsmaatregelen zoals die staan beschreven in de nieuwe norm. Door deze veroudering zouden de beheers- en beveiligingsmaatregelen niet meer up to date kunnen zijn.

3.2. Probleemstelling

Als het informatiebeveiligingsbeleid van de SNS Bank niet voldoet aan de ISO 27000 norm, dan kan dit problematisch zijn omdat de SNS Bank een financiële dienstverlener is, welke gevoelige en betrouwbare informatie bezit van haar medewerkers, klanten, leveranciers en andere (externe) partijen. De gevolgen zullen niet te overzien zijn als vertrouwelijke of kritische informatie die bedoeld is voor intern gebruik op straat komt te liggen. De SNS Bank verliest dan haar imago en dus ook haar klanten. Hieruit volgt dan ook de volgende probleemstelling:

De huidige informatiebeveiligingsnorm BS7799-2 is verouderd waardoor SNS IT niet aantoonbaar 'In Control' zou kunnen zijn, wat een verhoogde kans op beveiligingsrisico's tot gevolg kan hebben. De werkelijke situatie zou afbreuk kunnen doen aan de doelen 'Blijf betrouwbaar' en 'Verhoog de kwaliteit' uit het Operationeel Plan van 2009, welke is opgesteld door de directie van SNS IT.

3.3. Projectdoelstelling

De projectdoelstelling luidt als volgt:

Het ontwikkelen van een methodiek waarmee het “In Control” zijn van een bedrijfsdeel van SNS IT middels interne certificering ISO27001 aantoonbaar kan worden gemaakt.

3.4. Toelichting op de projectdoelstelling

Om de gevolgen die in paragraaf 3.2 genoemd zijn te voorkomen, worden de beheersingsdoelstellingen –en maatregelen volgens ISO 27001 ingevoerd en nageleefd. Bij de SNS Bank is er tijdens dit project inhoudelijk aandacht geschonken aan ISO 27001 en ISO 27002. Het 1ste deel is in hoofdlijnen de vervanging van de oude BS7799-2 norm, waarbij er speciale aandacht wordt geschonken aan het Information Security Management System (ISMS). ISO27001 beschrijft dus het proces om te komen tot een ingevuld ISMS.

Een ISMS bevat een aantal beleidsonderdelen, die zich bezighouden met information security management. De belangrijkste ‘key’ van het ISMS voor SNS Bank is het ontwerpen, implementeren en onderhouden van een samenhangend pakket van processen en systemen voor het effectief beheren van de toegankelijkheid van informatie en daarnaast ook het minimaliseren van informatiebeveiligingsrisico's.

Dit systeem is ervoor om directie en lijnmanagement, maar ook om interne en externe betrokkenen uitleg te geven over de werking van risicodekkende beheersmaatregelen. De bewijzen van werking worden in het ISMS opgeslagen en toegankelijk gemaakt voor de personen die de bevoegdheid dienen te hebben om deze bewijzen in te zien en te raadplegen.

De ISO 27002 norm, voorheen de BS7799-1 norm genoemd, schetst 133 potentiële maatregelen, die kunnen worden uitgevoerd met inachtneming van de aanwijzingen die in ISO 27001 zijn beschreven. Op deze manier wil de SNS Bank haar informatiebeveiliging naar een hoger niveau tillen.

3.5. De gewenste situatie

Omdat de huidige situatie niet meer toereikend genoeg is vanwege de veroudering van en de niet up to date zijnde beheers- en beveiligingsmaatregelen volgens de oude BS17799 norm, wil SNS Bank overgaan op de interne certificering volgens de nieuwe ISO27001 norm.

De nieuwe certificering geeft het management waarborg dat de risico's ten aanzien van Informatiebeveiliging binnen het gecertificeerde bedrijfsonderdeel zijn beperkt tot een aanvaardbaar niveau.

Het proces van certificering volgens ISO 27001 heeft een iets andere opzet gekregen zoals die voorheen bij de BS7799-2 bestond. Allereerst worden alle beheersmaatregelen die in de Code voor Informatiebeveiliging zijn opgesteld gehanteerd bij elke afdeling (ISO 27002). Met behulp van de risicoanalyse tool 'ISRAC' (Information Security Risk Analysis and Compliance) van InfoSecure kunnen de bedrijfsonderdelen middels een self-assessment bekijken of ze voldoen aan de gestelde eisen. Hierna wordt er een hermeting gedaan, indien er actiepunten uit het self-assessment zijn voortgekomen.Aan alle maatregelen worden procentuele cijfers toegekend op basis van het al dan niet voldoen aan de gestelde eisen. Indien een beheersingsmaatregel onvoldoende scoort omdat de bedreigingen een te groot risico vormen, wordt deze maatregel als onvoldoende gewaardeerd en wordt dit als 'actiepunt' bestempeld. Alle actiepunten die voortkomen uit de meting, worden overgedragen aan het desbetreffende bedrijfshoofd van het bedrijfsonderdeel of de afdeling. Zij zijn daarmee dan ook eindverantwoordelijke voor de afhandeling, maar de IB-coördinatoren dienen zelf de actiepunten af te handelen. Deze actiepunten dienen binnen een vooraf bepaalde termijn de status 'afgehandeld' te krijgen, waarna dit ook gecontroleerd wordt.

Tot slot kan er worden overgegaan op certificering. Hiervoor dient wel het controlerapport, waarin de bevindingen en resultaten zijn geschreven, d.m.v. een managementrespons te worden goedgekeurd door het bedrijfshoofd van het te certificeren bedrijfsonderdeel. De bedrijfsonderdelen en/of afdelingen dienen zelf te zorgen dat de documentatie m.b.t. het ISMS up to date blijft. Controle vanuit de afdeling IB&C zal periodiek gaan plaatsvinden.

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

- Projectplan en detailplanning (bijlage A)
- Literatuuronderzoek ISO27000 (externe bijlage XX)
- Periodieke projectvoortgangsrapportages (externe bijlage XVI t/m XIX)
- Certificeringmethodiek, genaamd ISMS Toolkit, met daarin:
    - Procesbeschrijving ISMS (externe bijlage I) [10]
    - Procedurebeschrijving Intern certificeren volgens ISO2700x (externe bijlage II)
    - Template Controlebrief (externe bijlage III)
    - Template BIA Bedrijfsonderdeel X (externe bijlage IV)
    - Template IB Jaarplan bedrijfsonderdeel X 200X (externe bijlage V)
    - Template Vragenlijst IB activiteiten bedrijfsonderdeel X (externe bijlage VI)
    - Template Beoordeling beveiligingsbewustzijn (externe bijlage VII)
    - Template Overzicht beleidsdocumenten (externe bijlage VIII)
    - Template Beoordeling afhandeling actiepunten
    - Template Documentkwaliteit (externe bijlage IX)
    - Template Controlerapport ISMS bedrijfsonderdeel X (externe bijlage X)
    - Template Certificaat (externe bijlage XI)
    - Introductie Interne Certificering ISO 27001 (externe bijlage XII)
    - Workshop ISMS ISO27001 (externe bijlage XIII)
    - Afdelingspresentatie Interne certificering ISO 27001 (externe bijlage XIV)
- Eindpresentatie voor afdeling Informatiebeveiliging & Controle
- Eindpresentatie voor Fontys Hogeschool ICT
- Afstudeerscriptie

Met behulp van de nieuwe certificeringmethodiek zou het ISMS op een meer efficiënte manier van aanpak tot stand moeten worden gebracht, wat tijdsbesparing oplevert voor zowel de faciliterende afdeling IB&C als voor het te certificeren bedrijfsonderdeel. Door het gebruik van ISO27001 dient het beheerproces van het ISMS eenvoudiger en met meer structuur te worden opgezet, ingevoerd, onderhouden en bijgestuurd. Een overzichtstabel van de ISMS Toolkit is opgenomen in externe bijlage XV.

Door gewijzigde inzichten tijdens de uitvoering van het project komen de opgeleverde producten die hierboven genoemd zijn niet geheel overeen met de producten die zijn gedefinieerd in het Plan van Aanpak. Voor deze gewijzigde inzichten wordt verwezen naar het issuelog (samenvatting van de bijstuurmomenten), welke is opgenomen in bijlage B.

[10] Bij de producten 'Procesbeschrijving ISMS', de 'Template BIA' en de 'Template Controlerapport ISMS' is door de projectmanager een minder actieve rol gespeeld in de ontwikkeling daarvan omdat deze documenten mede op een hoger niveau zijn ontwikkeld en vanwege het feit dat de ontwikkeling van de 2 eerstgenoemde templates voor de aanvang van het project zijn gestart. Het controlerapport bevat echter wel onderwerpen die rechtstreeks uit de ISMS Toolkit komen.

3.6. Concrete opdrachtomschrijving

Het bedenken van een concrete invulling voor de ISO 27001 certificeringmethodiek op basis van beschikbare literatuur en middelen en voer deze voor een bedrijfsonderdeel uit. ISRAC (een binnen SNS gebruikte risicoanalysemethodiek) dient eventueel aangepast te worden t.b.v. de controle op documentatie. Na een pilotfase dient de geaccordeerde methodiek overgedragen te worden aan de afdeling IB&C, inclusief de eventueel daaruit voortkomende verbeteringen. De opdracht betrof het bedenken van een certificeringmethodiek voor de SNS Bank volgens het PDCA-principe voor de structurering van het security managementproces volgens ISO 27001. De opdracht is opgesplitst in twee delen, die overigens wel een sterke samenhang hebben:

1. ISO 27001-documentatie realiseren die gespecificeerd zal worden voor het Information Security Management System. Het doel hierbij is het vaststellen, uitvoeren, monitoren, evalueren, onderhouden en het verbeteren van het ISMS. Er wordt hierbij ook aandacht besteed aan de behoeftes en doelstellingen, de veiligheid, en de omvang en structuur van SNS Bank.
2. Hieraan zullen parallel de ISO 27002 beheersmaatregelen voor informatiebeveiliging aan gekoppeld worden. De 133 maatregelen die hierin beschreven staan, staan garant voor de gewenste beheersing volgens de aanwijzingen in ISO 27001. De werking van deze maatregelen zal worden geïdentificeerd en worden vastgelegd met behulp van een risico-evaluatie volgens de ISRAC methodiek.

4. Raamwerk van het project

In dit hoofdstuk wordt het raamwerk van het project uitgelegd. In dit raamwerk zijn alle zaken opgenomen die tijdens de uitvoering van het project aan de orde komen; de onderwerpen welke buiten de scope worden gelaten zijn hier dan ook niet beschreven en vallen buiten het projectraamwerk.

4.1. Pilotfase certificering

De pilotfase tijdens dit project zal zich puur toespitsen op de ISO 27001 certificering van het bedrijfsonderdeel Relatiebeheer. De overige bedrijfsonderdelen van SNS IT zullen conform de nieuwe certificeringmethodiek, die tevens gerealiseerd is tijdens dit project, gecertificeerd worden in het 3de en 4de kwartaal van 2009. Een kanttekening die hierbij geplaatst wordt is dat het bedrijfsonderdeel Architectuur, welke nog in 2008 volgens de BS7799-2 standaard is gecertificeerd, pas weer in 2010 aan de orde komt. Dit heeft als reden dat dergelijke certificeringen dusdanig veel tijd in beslag nemen dat het niet mogelijk is om alle bedrijfsonderdelen te certificeren binnen de duur van dit project. De certificering bij Relatiebeheer wordt ook gebruikt om eventuele verbeterpunten toe te passen voor de navolgende certificeringen en eventueel om de certificeringmethodiek bij te stellen.

Het projectraamwerk ziet er als volgt uit:

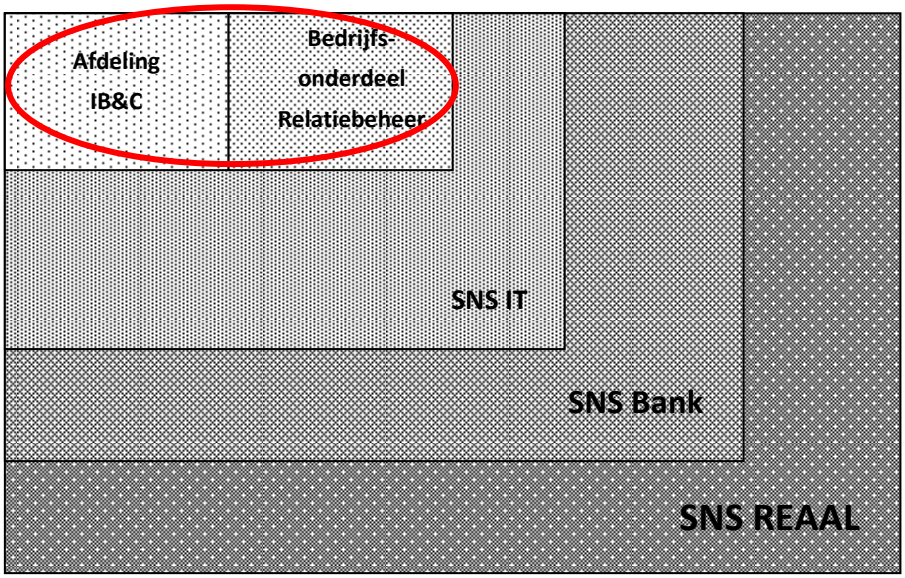


Fig 6: De scope van het project 'intern certificeren volgens ISO27001'.

De afdeling IB&C is hierbij de afdeling die het project tot uitvoer brengt. Bedrijfsonderdeel Relatiebeheer is het bedrijfsonderdeel welke in het 2de kwartaal van 2009 het certificeringproces zal gaan doorlopen. Meer informatie over Relatiebeheer is te vinden in hoofdstuk 8.

5. Methoden en werkwijzen

De gehanteerde methoden en werkwijzen tijdens het uitgevoerde project worden in dit hoofdstuk toegelicht en onderbouwd. Het betreft hier de methoden en werkwijzen die binnen SNS IT bekend zijn.

5.1. Project Matig Werken - Professional (PMW-P)

Veranderingen binnen de SNS Bank worden steeds ingrijpender en volgen elkaar steeds sneller op. Het stadium waarin werkzaamheden op een ad hoc wijze worden uitgevoerd, is voor een groot deel vervangen door de situatie waarin werkzaamheden in projectmatige vorm plaatsvinden. De methodiek PMW Professional is geschikt voor alle soorten en maten projecten en programma's. Met behulp van het PMW-P logo (figuur 7) wordt aangeduid dat documentatie volgens deze methode is opgebouwd en voldoet aan de eisen zoals PMW-P deze stelt.

Veel methoden presenteren projectmanagement in de vorm van een stap voor stap aanpak. In de praktijk is projectmanagement echter meestal niet een dergelijk proces. Kenmerkend voor PMW-P is dat deze procesbenadering de centrale plaats en de verzameling samenhangende activiteiten zijn die samen het doel nastreven.[11]

Fig. 7: het logo van PMW-P Professional.

PMW-P hanteert werkinstructies en templates voor projectdocumentatie. De op te leveren documentatie voor de SNS Bank zijn tijdens dit project grotendeels opgeleverd volgens de PMW-P methodiek, met uitzondering van het literatuuronderzoek en de ISMS templates. PMW-P maakt daarnaast gebruik van verschillende faseringen in een project:

- Projectaanvraag (aanvraag bij het management)
- Projectdefinitie[12] (projectvoorstel bij het management)
- Projectinitiatie (realisatie projectplan)
- Projectuitvoering (projectvoortgangsrapportages)
- Projectafsluiting (projecteindrapport)

[11] Bron: Q-systeem SNS Bank (http://sharepoint.bank.local/sites/200807032/default.aspx).

[12] De eerste 2 fases uit de PMW-P methodiek waren reeds uitgevoerd voordat het eigenlijke project van start is gegaan. Daarom wordt er in deze rapportage niet verder ingegaan op de projectaanvraag en projectdefinitie. Omdat de projectafsluiting volgens PMW-P voldoende raakvlakken heeft met deze rapportage is ook het projecteindrapport niet geschreven.

Door de bovenstaande beschreven methode te hanteren wordt er binnen SNS Bank op een gestandaardiseerde en uniforme manier gewerkt, wat het communicatieproces aanzienlijk verbetert. Daarnaast is het gebruik van standaard richtlijnen voordelig als men kijkt naar de uitvoering van projecten. Dit betekent dat belangrijke kernonderwerpen altijd aan bod komen binnen een project. Afwijkingen tijdens de uitvoer van dit project en die niet refereren aan deze projectmanagementmethode zijn weloverwogen genomen en zijn alleen met toestemming van de leidinggevende doorgevoerd.

5.2. PDCA-cyclus

Bij de realisatie van het ISMS, volgens de definitie in hoofdstuk 3, wordt er gebruik gemaakt van de Plan-Do-Check-Act[13] (PDCA) methode. Deze cirkel houdt in dat er allereerst een plan wordt opgesteld dat men wilt gaan uitvoeren. Vervolgens wordt het plan uitgevoerd in de Do-fase. In de Check-fase worden de resultaten die geboekt zijn vergeleken met de resultaten die in de verwachting lagen. Punten die niet overeenkomen worden bijgesteld in de 'Act-fase.

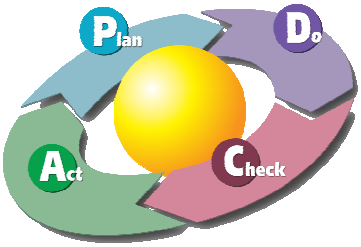


Fig. 8: de PDCA-cyclus in zijn elementaire vorm.

De PDCA-cyclus (figuur 8) is zodanig verweven in de stappen die ondernomen moeten worden om het ISMS te kunnen onderhouden, dat er een schema voor is opgesteld (figuur 9). De verschillende stappen zijn:

1. Het ISMS vaststellen (Plan)
2. Het ISMS implementeren & uitvoeren (Do)
3. Het ISMS controleren & beoordelen (Check)
4. Het ISMS bijhouden en verbeteren (Act)

[13] Bron: Boek 'Implementing Information Security – based on ISO27001 / ISO 17799

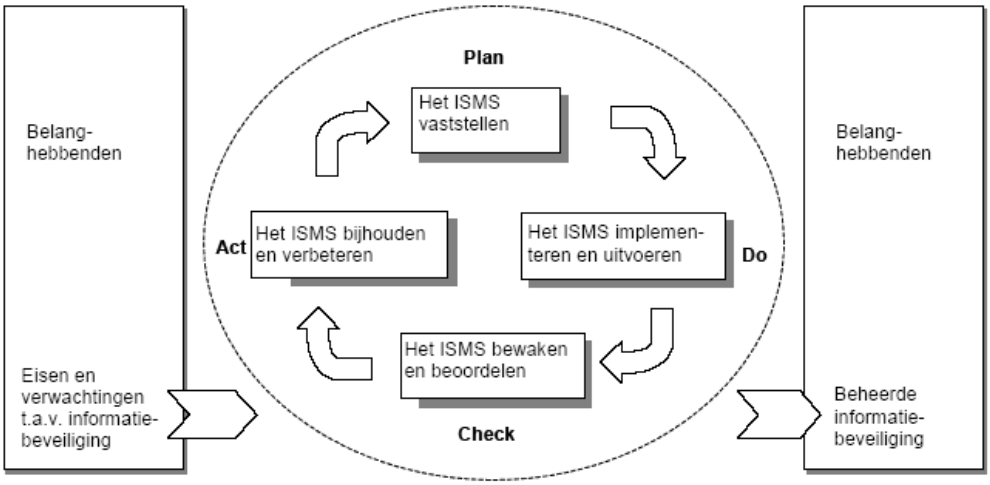


Fig. 9: de PDCA-cyclus geïntegreerd in het ISMS stappenplan.

Tijdens het vaststellen van het ISMS wordt bepaald wat binnen de scope van de certificering valt en welke bewust niet. Deze stap is uitermate belangrijk omdat er op deze manier een 'scope' wordt gecreëerd waarin staat vermeld wat het uit te voeren beleid is en wat dit beleid inhoudt. Daarnaast is het absolute noodzaak dat er in de scopebepaling wordt beschreven welke documentatie in het ISMS aanwezig dient te zijn en bij welke kritische processen en applicaties deze documentatie hoort. Verder spelen de fysieke locaties waar de bedrijfsonderdelen en afdelingen zich bevinden ook een grote rol. In het geval van een ernstige calamiteit dient er bijvoorbeeld een uitwijkmogelijkheid te zijn, waar uiteraard ook gebruik gemaakt kan worden van benodigde applicaties en waar de kritische processen door kunnen lopen.

Nadat de projectscope van het ISMS is vastgesteld wordt dit 'systeem' geïmplementeerd en uitgevoerd. De betreffende documentatie, de processen en de locaties worden gedetailleerd beschreven en de maatregelen hierbij worden op de locaties getroffen. Deze vastlegging en de getroffen maatregelen zorgen voor een stabiele werkomgeving.

Uiteraard worden er periodieke controles uitgevoerd op alle ISMS'en van de verschillende bedrijfsonderdelen. Door bijvoorbeeld nieuwe metingen uit te voeren met ISRAC (herhaalmetingen) kunnen nieuwe dreigingen en risico's blootgesteld worden en kunnen hier passende maatregelen bij gemaakt worden. Niet alleen de aanwezige documentatie en de kritische processen worden hierbij gecontroleerd, maar ook het awarenessniveau bij de IB-coördinatoren en de medewerkers zijn minstens zo belangrijk. Want alles begint bij de mens zelf. Door middel van het meten van het beveiligingsbewustzijnsniveau wordt er een 'check' gedaan op de dan huidige stand van gedrag, kennis en houding van de mensen die direct betrokken zijn bij het betreffende bedrijfsonderdeel of de betreffende afdeling. De IB-coördinatoren worden zelf bijvoorbeeld ook beoordeeld of zij hun taken goed uitvoeren op het gebied van informatiebeveiliging.

Natuurlijk is het onmogelijk deze mensen er alleen voor te laten staan. Daarom organiseert de afdeling IB&C regelmatig awareness-sessies, informatiebeveiligingscursussen en contactmiddagen waarmee de noodzaak van het naleven van het informatiebeveiligingsbeleid haarfijn wordt uitgelegd (het awarenessniveau dient zeker niet te verslechteren) en de nieuwste ontwikkelingen bij SNS REAAL worden gecommuniceerd. Dit alles draagt bij aan een beter ISMS.

Om het ISMS up to date te houden, is het noodzakelijk om een nieuwe procedure te hanteren tegen om de actualiteit van het ISMS te borgen. Het is daarom belangrijk dat het ISMS wordt bijgehouden en waar nodig wordt verbeterd. Het verbeteren en bijsturen van het ISMS gebeurt op basis van een 2-jaarlijkse cyclus. Het totale stappenplan van het ISMS ziet er als volgt uit:

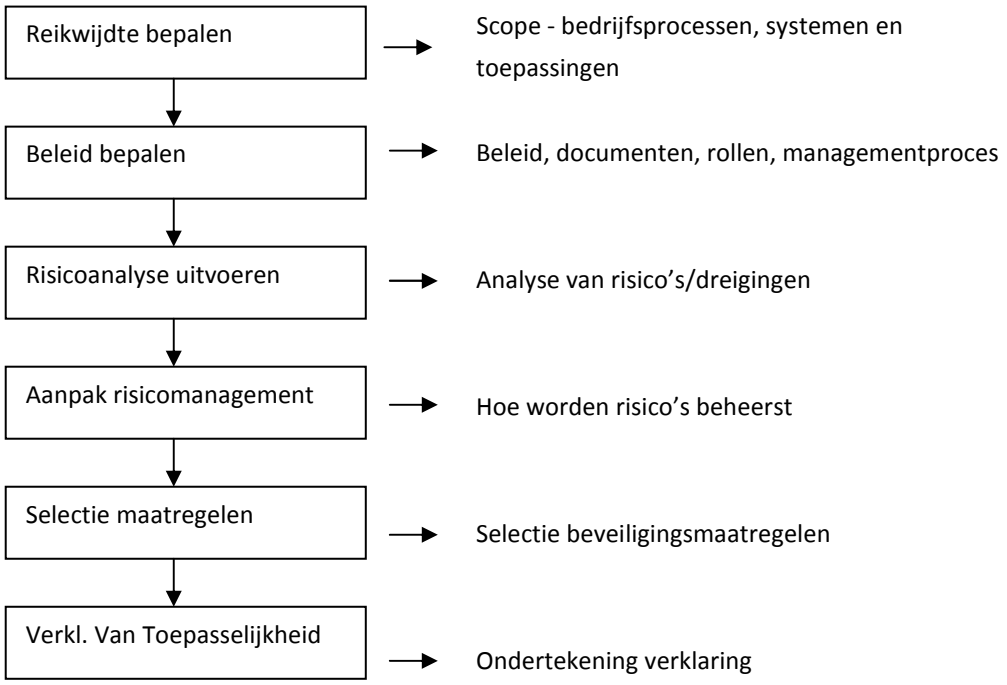


Fig. 10: Het ISMS stappenplan

Omdat SNS Bank intern wil uitstralen dat het veel belang hecht aan informatiebeveiliging, worden volgens een 2-jaarlijkse cyclus alle afdelingen (opnieuw) gecertificeerd volgens het beheerproces van het ISMS. Tot op heden was dit volgens BS7799-2, vanaf nu is dit de nieuwe ISO27001 standaard. Het concrete doel hiervan is om 'In Control' te blijven en om zo weinig mogelijk aan het toeval over te laten.

5.3. ISRAC

SNS analyseert de beveiligingsrisico's met behulp van de tool 'ISRAC[14]'. Deze methodiek bevat een self-assessment waaruit blijkt of de te certificeren bedrijfsonderdelen voldoen aan de beheersingsmaatregelen zoals die gesteld zijn in de ISO 27002 norm.

Deze ISRAC-sessies worden gedaan met alle IB-coördinatoren van het betreffende bedrijfsonderdeel dat gecertificeerd wil worden. De adviestak van de afdeling IB&C heeft hierbij 'slechts' een faciliterende en adviserende functie; het is immers een self-assessment.
Met behulp van drie maatstaven die in ISRAC gedefinieerd zijn worden de risico's beoordeeld. Deze maatstaven zijn de Business Impact Analyse (BIA), het Threats and Vulnerabilities Assessment (TVA), en de List of Controls (LOC).

De vragen die horen bij de BIA en de TVA worden gesteld in 3 verschillende categorieën, namelijk de Beschikbaarheid, de Integriteit en de Vertrouwelijkheid (BIV). De definities van deze drie categorieën zijn:

- **Beschikbaarheid:** geautoriseerde gebruikers hebben op de vereiste momenten tijdig toegang tot informatie en aanverwante bedrijfsmiddelen.
- **Integriteit:** de informatie heeft de vereiste betrouwbaarheid (volledigheid, juistheid) voor het gebruiksdoel;
- **Vertrouwelijkheid:** de informatie is alleen toegankelijk voor degenen, die hiertoe geautoriseerd zijn.

5.3.1. Business Impact Analyse

In de BIA, de eerste vragenlijst van ISRAC, worden middels het self-assessment vragen gesteld aan de IB-coördinator m.b.t. impact van de bedrijfsbeslissingen, de bedrijfsvoering, vertrouwen, juridische aspecten, wat risico's kunnen zijn waardoor extra kosten gemaakt moeten worden, enzovoorts. Dit wordt bepaald door de impact van bepaalde gebeurtenissen aan te geven. Voorbeeld: De impact bij het risico 'Foutieve beslissingen van het management' kan behoorlijke schade opleveren.

[14] Bron: ISRAC (http://israc.bank.local/index.php).

5.3.2. Threats and Vulnerability Assessment

Het TVA, het 2de onderdeel uit ISRAC, beschikt over een vragenlijst die ingaat op bedreigen zoals rampen, fysieke aanvallen, brand, continuïteit van kritische IT-componenten, zwakheden m.b.t. onjuiste informatie op websites, fysieke beveiliging, vertrouwelijkheid van systemen, enzovoorts. Door de kans aan te geven van het optreden van de dreiging kan er een risico-inschatting worden gemaakt. Voorbeeld: De kans dat iemand vergeet om het clear screen beleid [15]op te volgen, is vrij groot. Dit zou bijvoorbeeld dagelijks kunnen gebeuren.

De in het algemeen bekende formule treedt hier in werking:

R = K x I (Risico = Kans x Impact)

Door de kans van optreden van een risico te vermenigvuldigen met de impact die het risico zou kunnen veroorzaken komt men tot een risico-inschatting.

5.3.3. List Of Controls

In de LOC van ISRAC worden alle beheersingsmaatregelen uit ISO 27002 genoemd. Er dient hierbij aangegeven te worden of het bedrijfsonderdeel voldoet aan deze maatregelen, wat de kans van optreden is en of er eventuele opmerkingen zijn over bepaalde (slecht) toegepaste beheersingsmaatregelen. Voorbeeld: In het kader van 'beveiliging van personeel' wordt er onbewust niet juist toegezien op het gebruik van bedrijfsmiddelen. Een maatregel zou dan kunnen zijn om een awareness-sessie te houden bij de betreffende afdeling.

Door het bovenstaande in de LOC aan te geven kan de risicoanalyse uitgevoerd worden omdat de risicofactor al door de BIA en de TVA bepaald is.

De normering bij de LOC wordt aangegeven in percentages en is als volgt opgebouwd:

0 - 39%:	de maatregel is beschreven
40 - 69%:	de maatregel is beschreven en bekend
70 - 89%:	de maatregel is beschreven, bekend en gecommuniceerd
90 -100%:	de maatregel is beschreven, bekend, gecommuniceerd en onafhankelijk gecontroleerd

[15] Beleid dat aangeeft dat bij het verlaten van de werkplek het betreffende informatiesysteem vergrendeld dient te worden.

6. Definitie -en initiatiefase: Literatuuronderzoek ISO27000[16]

"One size fits all"[17]

Om meer kennis te vergaren over ISO27000 is er een literatuurstudie uitgevoerd om zodoende een beter beeld te krijgen over de verschillen tussen de BS17799 norm en de ISO27000 norm. Hieronder staan de normen van de Code voor Informatiebeveiliging uitgelegd, inclusief de aanwezige verschillen en de daaruit voortkomende conclusies en aanbevelingen.

6.1. BS17799 versus ISO27000

Voor de goede orde staat hieronder eerst de overgangsbenaming:

- BS17799 en ISO27000 zijn verzamelnamen voor alle BS- en ISO-reeksen op het gebied van Informatiebeveiliging;
- De oude norm 'BS7799-1' is de nieuwe 'ISO 27002' geworden;
- De oude norm 'BS7799-2' is de nieuwe 'ISO 27001' geworden.

De verschillen die aan het licht komen zijn aanzienlijk, doch zijn er ook overeenkomsten. De ISO27001 specificeert eisen voor het opstellen, uitvoeren en documenteren voor het Information Security Management Systems (ISMS). Verder worden er ook eisen beschreven die veiligheidscontroles specificeren. Dit kan worden afgestemd op de behoeften van SNS IT. Zodra een (onderdeel van) een organisatie intern is gecertificeerd volgens deze informatiebeveiligingsnorm, dient dit officieel als basis voor een certificeringsaudit die uitgevoerd wordt door een 3de partij. Een externe certificering is bij SNS Bank niet aan de orde.

De BS17799 definieert een proces om informatiebeveiliging te evalueren, te implementeren, te onderhouden en te beheren. De norm is bedoeld voor het gebruik als leidraad of als referentiedocument.

BS17799 is een adviserende informatiebeveiligingsnorm en dus niet een controleerbare norm zoals ISO 27000. Als men een organisatie wil certificeren volgens de code voor informatiebeveiliging, dan moet er gestreefd worden om ISO 27001 te hanteren.

Voor meer gedetailleerde informatie wordt verwezen naar het gehele literatuuronderzoek, dat te vinden is in externe bijlage XX.

[16] Bron: literatuurstudie_ISO27000_v1.0.doc

[17] Bron: http://www.computable.nl/artikel/ict_topics/security/2549644/1276896/nederland-veiliger.html

6.2. Conclusies en aanbevelingen uit het onderzoek

Omdat SNS IT 'In Control' wil zijn en alle bedreigingen en risico's (en de impact daarvan) wilt beperken tot een voor haar aanvaardbaar niveau, is het noodzakelijk dat er wordt overgegaan op de nieuwe ISO 27000 standaard. De norm richt zich op een doeltreffend beheer van informatiebeveiligingsincidenten, wat een belangrijke werkzaamheid is van de afdeling Informatiebeveiliging & Controle. Deze twee punten zijn kritische succesfactoren voor SNS IT.

Na uitvoerig onderzoek in dit project is er een zestal aanbevelingen gedaan richting SNS IT, en in het bijzonder aan afdeling Informatiebeveiliging & Controle.

1. SNS IT dient de overstap te maken van de huidige BS7799-2 norm naar de nieuwe ISO standaard voor Informatiebeveiliging: ISO27001.

2. Binnen één bedrijfsonderdeel van SNS IT dient een 'pilot uitgevoerd te worden waarbij er voor de eerste keer de certificering middels ISO27001 uitgevoerd wordt. Zo krijgt men een indruk in de 'nieuwe manier' van certificeren.

3. Voordat deze pilot van start gaat is het belangrijk dat de medewerkers van de betreffende bedrijfsonderdelen bewust worden gemaakt van de nieuwe manier van werken. Aanbevolen wordt om dit te doen d.m.v. workshops.

4. Aanbevolen wordt om de nieuwe ISO 27001 certificering te ondersteunen middels een nieuwe certificeringmethodiek, waarbij templates dienen te worden opgesteld om de documentatie van het ISMS te standaardiseren.

5. Verder verdient het de aanbeveling om eisen op het gebied van documenten en documentatiebeheer op te stellen, om zo een uniforme en eenduidige manier van werken te hanteren.

6. Om continu te kunnen voldoen aan de ISO-norm, wordt geadviseerd om alle ISO reeksen die relevant zijn voor de informatiebeveiliging van SNS Bank op te volgen. Het verdient speciale aandacht om informatie in te winnen over ISO 27015, wat naar alle waarschijnlijkheid de norm gaat worden voor de financiële dienstensector.

Het meer uitgebreide conclusie- en aanbevelingenhoofdstuk is eveneens te vinden in externe bijlage XX.

7. Ontwerpfase: ISMS Toolkit

“Zorgvuldig met informatie en middelen”

Een onderdeel van de projectopdracht was om een nieuwe methodiek te bedenken in het kader van het certificeringproces. Om dit proces zo goed en efficiënt mogelijk te kunnen laten verlopen, is hiervoor een hulpmiddel ontworpen, de zogeheten ’ISMS Toolkit’. In deze toolkit zit een procesbeschrijving van het ISMS, een procedure waarin het certificeringproces wordt beschreven en een aantal templates die door de verschillende bedrijfsonderdelen van SNS IT gebruikt dienen te worden om het ISMS in te kunnen vullen. Ook zijn er een aantal presentaties opgesteld die dienen voor rapportage aan de bedrijfsonderdelen die in het certificeringproces zitten en die daarnaast ook bedoeld zijn voor awareness bij het management en de IB-coördinatoren. Een compleet overzicht van de ISMS Toolkit is te vinden in externe bijlage XV. In dit hoofdstuk worden alle onderdelen uit de toolkit toegelicht.

7.1. Procesbeschrijving ISMS

In de procesbeschrijving van het ISMS wordt beschreven op welke wijze SNS REAAL risico’s op het gebied van Informatiebeveiliging beheerst. De basis voor deze beschrijving wordt gevormd door de ISO27001 norm. Alle activiteiten op het gebied van Informatiebeveiliging worden met behulp van deze beschrijving samengebracht.

Wanneer we wederom de PDCA-cyclus hanteren, wordt het duidelijk dat In de Plan-fase het ISMS wordt vastgesteld, wat betekent dat het toepassingsgebied van het ISMS bepaald wordt. Daarna wordt het beleid opgezet, waarin een aantal beleidsuitspraken worden gedaan. In de Plan-fase worden overigens ook doelstellingen, relevante processen en procedures t.b.v. risico management beschreven die in lijn zijn met de algemene beleidslijnen en doelstellingen van SNS Bank.

In de Do-fase wordt het ISMS geïmplementeerd en uitgevoerd. Hier wordt dus het gehele ISMS beleid wat is opgesteld in de Plan-fase uitgevoerd.

Tijdens de Check-fase worden de procesprestaties ten opzichte van het ISMS beleid, doelstellingen en ervaringen uit de praktijk beoordeeld en, voor zover van toepassing, gemeten. De resultaten die hieruit voortvloeien worden gerapporteerd aan management en directie.

In de Act-fase worden corrigerende en preventieve maatregelen genomen om het ISMS continue te verbeteren. Dit wordt gedaan op basis van interne audits en directiebeoordelingen.

Het wordt nu duidelijk hoe helder de stappen van het ISMS gestructureerd zijn verweven in de PDCA-cyclus en waarom er in dit rapport zoveel aandacht besteed wordt aan deze twee termen.

Voor een gedeeltelijke procesbeschrijving van het ISMS wordt verwezen naar externe bijlage I.

7.2. Procedurebeschrijving intern certificeren

In de procedurebeschrijving 'intern certificeren volgens ISO27001 is de gehele procedure opgenomen in het kader van het certificeringproces. Het doel van de procedure, de globale beschrijving van het proces, een gedetailleerde procedurebeschrijving en een RACI-matrix[i] (Responsible, Accountable, Consulted, Informed) vormen hierbij het uitgangspunt. Het RACI-model is een matrix die gehanteerd wordt om de rollen en verantwoordelijkheden van de personen die bij een project of lijnwerkzaamheden betrokken zijn weer te geven. Er wordt met deze matrix respectievelijk beschreven wie de uitvoerende werkzaamheden doet, wie eindverantwoordelijk is voor het uit te voeren project, bij wie er om advies gevraagd kan worden en wie er geïnformeerd dient te worden omwille van het project. Door deze taken, rollen en verantwoordelijkheden vast te leggen kunnen er geen onduidelijkheden ontstaan over de te volgen procedurestappen.

7.3. Controlebrief

Middels een controlebrief wordt het management van het te certificeren bedrijfsonderdeel op de hoogte gesteld van de ontwikkelingen die gaan plaatsvinden tijdens het certificeringproces. In de brief wordt de aanleiding van het project beschreven, wat dit betekent voor het bedrijfsonderdeel en een globale planning van de certificering. Het bedrijfshoofd dient akkoord te gaan met deze controlebrief.

7.4. Business Impact Analyse

De template 'BIA' is een document waarin wordt verwezen naar de gedocumenteerde bedrijfsprocessen, de locatie van het bedrijfsonderdeel en de applicaties, bedrijfsmiddelen, informatie en gebruikte technologieën van het bedrijfsonderdeel. Daarnaast wordt in dit document vastgesteld wat niet tot het toepassingsgebied van het ISMS behoort. Dit document wordt opgesteld om in één oogopslag te kunnen zien wat de meest kritische bedrijfsprocessen en applicaties zijn en wat binnen de scope van de certificering valt. De template BIA dient niet verward te worden met de BIA vragenlijst uit de risicoanalysetool ISRAC; toevalligerwijs is de naamgeving identiek.

7.5. Overzicht beleidsdocumenten

In de template 'Beleid' worden een aantal beleidsuitspraken gedaan waaraan bedrijfsonderdelen op het gebied van risicobeheersing dienen te voldoen. Een voorbeeld van een beleidsuitspraak is 'In stand houden en verhogen van beveiligingsbewustzijn wordt actief gestimuleerd'. IB-coördinatoren van bedrijfsonderdelen dienen er dus zelf voor te zorgen dat de medewerkers en leidinggevenden bewust worden op het gebied van informatiebeveiliging. Daarnaast wordt er in dit document een overzicht van beleidsdocumenten aangereikt die het beleid bepalen voor het betreffende bedrijfsonderdeel. Dit beleid kan op SNS REAAL niveau en/of op bedrijfsonderdeelniveau zijn.

7.6. Vragenlijst IB-activiteiten

In de vragenlijst over Informatiebeveiligingsactiviteiten worden een aantal vragen gesteld die te maken hebben met voldoende inzet bij de afdelingen op het gebied van informatiebeveiliging. Het gaat hier om vragen die gaan over het opstellen en naleven van het IB-jaarplan, de rol van de IB-coördinator, de naleving van de Gouden Regels en het beveiligingsbewustzijn. De betreffende IB-coördinatoren dienen de vragenlijst in te vullen. Per onderdeel zullen zij hierop beoordeeld worden d.m.v. de normen 'Slecht', Onvoldoende', Voldoende' en 'Goed'.

Beveiligingsbewustzijn management	
Goed	Er vindt actieve sturing op beveiligingsbewustzijn plaats
Voldoende	Beveiligingsbewustzijn wordt als belangrijk ervaren
Onvoldoende	Beveiligingsbewustzijn wordt niet als belangrijk ervaren
Slecht	Niet bekend / Niet zichtbaar
Naleving Gouden Regels (bv Clear Desk)	
Goed	Er wordt toegezien op naleving van de Gouden Regels
Voldoende	De Gouden Regels zijn bekend en worden nageleefd
Onvoldoende	De Gouden Regels zijn bekend
Slecht	De Gouden Regels worden niet nageleefd / Dit is niet bekend
Beveiligingsbewustzijnsactiviteiten	
Goed	Jaarlijks worden diverse awarenessactiviteiten uitgevoerd/vastgelegd
Voldoende	Jaarlijks worden diverse awarenessactiviteiten uitgevoerd
Onvoldoende	Jaarlijks worden nauwelijks awarenessactiviteiten uitgevoerd
Slecht	Er worden geen awarenessactiviteiten uitgevoerd / Dit is niet bekend
IB Cultuur (elkaar aanspreken)	
Goed	Men spreek elkaar regelmatig aan op IB aspecten
Voldoende	Men spreekt elkaar aan op IB aspecten
Onvoldoende	Men spreekt elkaar niet aan op IB aspecten
Slecht	Dit is niet bekend

Fig. 11: vragen beveiligingsbewustzijn, onderdeel van de vragenlijst IB-activiteiten.

7.7. IB-Jaarplan

In het IB-jaarplan wordt de goedkeuring verleend door het Management om IB-activiteiten uit te voeren. Vervolgens zal er een plan voor de behandeling van risico's geformuleerd worden. Aan de hand van deze risico's worden de beheersmaatregelen gekozen en geïmplementeerd. Periodiek zullen de gekozen maatregelen gecontroleerd worden op doeltreffendheid.

De bedrijfsonderdelen moeten zelf programma's voor training en bewustzijn implementeren om zo het niveau van beveiligingsbewustzijn op een zo hoog mogelijk niveau te houden.

Als er eventuele actiepunten zijn opgetreden na een meting, dan dienen deze bevindingen leiden tot aanpassingen in het IB-jaarplan. Daarbij is het absoluut noodzakelijk om continu te verbeterende, corrigerende en preventieve maatregelen te treffen en om middelen beschikbaar te stellen voor informatiebeveiliging. Afdeling IB&C zal periodiek controles uitvoeren op de zaken die zijn genoemd in de betreffende IB-jaarplannen.

7.8. Beoordeling beveiligingsbewustzijn

De medewerkers van het bedrijfsonderdeel dat gecertificeerd wordt, krijgen middels een digitale enquête de mogelijkheid om hun kennis, houding en gedrag ten aanzien van informatiebeveiliging te testen. De medewerkers krijgen een 21-tal vragen welke beantwoord dienen te worden. Deze vragen zijn veelal 'persoonlijk' van aard, wat wilt zeggen dat er situatiegerichte vragen gesteld worden zoals 'Wat doet u als u iemand niet het clear desk beleid ziet opvolgen?' Degene die de vraag beantwoordt kan kiezen uit verschillende antwoorden. Het antwoord wat voor de persoon in kwestie het meest voor de hand ligt (dus wat hij of zij ook echt zou doen) dient gekozen te worden.

De resultaten die voortkomen uit de enquête worden verwerkt in een excelblad, waar een beoordeling uit komt. Er wordt beoordeeld op de respons van de enquêtes en op het beveiligingsbewustzijn van de respondenten. Per bedrijfsonderdeel wordt een willekeurig aantal mensen van een bedrijfsonderdeel ondervraagd. Het gaat hier om 50% van de totale personeelsbezetting. Van deze 50% dient ook weer de helft van de medewerkers de enquête in te vullen, anders wordt het eindoordeel zonder pardon onvoldoende. In de eindbeoordeling wordt dit percentage meegenomen. Het beveiligingsbewustzijn wordt gemeten door de vragen op het gebied van kennis, houding en gedrag. Het gemiddelde hiervan bepaalt het eindcijfer. Deze beoordeling wordt aangegeven met een cijfer dat ligt tussen 1 en 10. Voor een template van de beoordeling van het beveiligingsbewustzijn wordt verwezen naar externe bijlage VII.

7.9. Beoordeling afhandeling actiepunten

Indien een bedrijfsonderdeel actiepunten krijgt toegewezen die voortkomen uit de ISRAC-meting, dan dienen de IB-coördinatoren van het bedrijfsonderdeel ervoor te zorgen dat minimaal 80% van deze actiepunten binnen een vooraf aangegeven termijn worden opgelost. Mochten de maatregelen niet adequaat zijn opgelost of is het percentage lager dan de gestelde norm, dan kan het bedrijfsonderdeel niet gecertificeerd worden. De actiepunten worden ingevoerd in de AAP-database (Audit Actie Punten). In deze database wordt een actiepunt voorzien van een nummer met bijbehorende letter dat aangeeft in welke categorie het actiepunt zich bevindt, een omschrijving van het actiepunt en een datum welke aangeeft voor wanneer het actiepunt opgelost dient te zijn.

7.10. Documentkwaliteit

Binnen de SNS Bank is het belangrijk dat er eisen gesteld worden aan de manier van documenteren. Door op een uniforme en eenduidige manier kennis te digitaliseren wordt de herkenbaarheid en bruikbaarheid van documenten en documentatie optimaal benut.

Binnen SNS Bank is documentatie op verschillende manieren ontsloten, bijvoorbeeld via sharepoint websites, het intranet, het Q-systeem en centrale netwerkschijven. Hierdoor wordt informatie onvoldoende toegankelijk omdat niet iedere medewerker bevoegd is voor toegang tot een bepaald medium. Door het gebruik van deze verschillende media ontstaat er veel redundante opslag en inconsistentie en het gevolg daarvan is dat de kwaliteit van de informatie onvoldoende wordt gewaarborgd.
ISO27001 schrijft voor dat er aan bepaalde eisen voldaan moet worden op het gebied van documentatie. Deze eisen zijn hieronder opgesomd.

- *Het acceptatie en goedkeuringsproces van het document.* Zodra de auteur van een bepaald document van mening is dat het klaar is om goedgekeurd te worden, dan wordt dit kenbaar gemaakt bij de directe leidinggevende van de medewerker. De leidinggevende doet een review op het rapport en geeft zo nodig aan waar welke aanpassingen doorgevoerd dienen te worden. Vervolgens wordt het document goedgekeurd en kan het worden opgenomen in het kwaliteitssysteem (Q-systeem).

- *Periodieke review.* Op het document dient een datum van schrijven zichtbaar te zijn. Er wordt als regel vastgesteld dat ieder bedrijfskritisch document dat onderdeel is van het ISMS periodiek een review krijgt. Deze maatregel wordt genomen om de documenten zo juist en actueel mogelijk te houden.

- *De controle op wijzigingen en revisie verwijzing.* Wijzigingen worden wederom gecontroleerd door de directe leidinggevende. Daarnaast is het ook van belang dat er een revisieverwijzing is opgenomen in het document. Door versiebeheer toe te passen kan er worden nagekeken welke documentatie er op welke datum is gewijzigd, verwijderd of toegevoegd en wie hier verantwoordelijk voor is.

- *Ontsluiting van de documenten.* Documenten dienen toegankelijk gemaakt te worden voor de personen die hier belang bij hebben en die hiervoor ook bevoegd zijn gesteld. Hierdoor ontstaat er tegelijkertijd een stukje logische functiescheiding, wat de informatiebeveiliging ten goede komt. Werkinstructies, procedurebeschrijvingen, procesbeschrijvingen, templates, enz. worden opgeslagen in het interne kwaliteitsysteem van SNS Bank, namelijk het Q-systeem. Dit heeft als voordeel dat documentatie op één centrale plaats is opgeslagen. Hierdoor hoeven er bijvoorbeeld ook niet onnodig bijlagen te worden verstuurd in de interne e-mail.

- *Leesbaarheid en identificatie.* Het is de bedoeling dat documenten herkend kunnen worden aan een unieke naamgeving in de bestandsnaam, dat eveneens in lijn is met de titel. Documenten kunnen zo eenvoudig worden teruggevonden en ontstaan er minder misverstanden. Daarnaast is het belangrijk dat de inhoud van het document onafhankelijk gelezen kan worden door directe collega's. Complexe technische literatuur dient omgezet te worden naar begrijpelijke en logische taal. Daarnaast wil SNS Bank voorkomen dat het zogenaamde 'SPOK's' (Single Point of Knowledge) in haar midden heeft. SPOK's zijn medewerkers die specifieke individuele kennis van bepaalde zaken hebben die niet gedocumenteerd is binnen SNS Bank. Bij het wegvallen van een dergelijke medewerker door wat voor oorzaak dan ook kan dit grote gevolgen hebben voor de organisatie.

- *Het gebruik van templates.* Door het gebruik van templates worden er twee duidelijke voordelen gecreëerd: een uniforme en gestandaardiseerde werkwijze en de kans dat belangrijke kerninformatie in documenten niet wordt vergeten. Omdat documentstructuren, opzetten, hoofdstuk- en paragraafindelingen al gedefinieerd zijn is de kans klein geacht dat belangrijke informatie niet wordt vergeten. Documenten worden op deze manier ook duidelijk herkend door mensen omdat zij zelf ook deze templates gebruiken om hun werkzaamheden uit te voeren.

- *Classificatie van de documentatie.* Door documenten te classificeren wordt het in één oogopslag duidelijk voor wie de informatie bedoeld is. Er dient op een andere manier met een document te worden omgegaan dat geclassificeerd is met 'sleutelmateriaal' dan een document dat gelabeld is met 'publieke informatie'. De verschillende classificaties in deze zijn: publieke informatie, interne informatie, vertrouwelijke informatie en sleutelmateriaal.

- *Identificatie van eventuele gebruikte externe bronnen.* Door bronnen aan te geven die gebruikt zijn om documentatie op te stellen wordt voorkomen dat onbevoegd gebruik wordt gemaakt van andermans werk. Lezers van de documenten kunnen op deze manier zien waar informatie vandaan komt, of het betrouwbaar is, of er verschillende bronnen gebruikt zijn en of de informatie überhaupt goed is overgenomen. Daarnaast bestaat de mogelijkheid om aanvullende informatie in de bronnen op te zoeken.

- *Document distributie.* Door een distributielijst in de documenten op te nemen creëert men een lijst van ontvangers van het document. Men weet dan voor wie het document geschreven is en wie het gelezen heeft.

- *De lifecycle van de documenten.* Door een datum van goedkeuring in het document op te nemen is het mogelijk om de levenscyclus van documenten up to date te houden. Nadat een bepaalde termijn verstreken is kan ervoor gekozen worden om het document inhoudelijk te herzien of te wijzigen.

- *Bewaartermijn van de documenten.* Door in het document aan te geven tot wanneer het document bewaard dient te worden voorkomt men onnodige dataopslag en, nog belangrijker, onjuiste informatie in het document zelf wegens veroudering.

De bovenstaande eisen die in de ISO-norm staan beschreven zijn niet uitputtend. De SNS Bank kan en mag deze lijst aanvullen naar eigen wens. De afdeling IB&C heeft daarom een checklist gemaakt dat als hulpmiddel dient om te controleren op documentkwaliteit. Bovenstaande zaken zijn in een korte vraagstelling opgenomen en het bedrijfsonderdeel wat gecheckt wordt op documentkwaliteit kan hierdoor verantwoording afleggen. De ingevulde checklists (met de uitkomst slecht, onvoldoende, voldoende of goed, worden ter bewijslast gearchiveerd.

De uniforme vastlegging van documentatie zorgt voor aanzienlijke kostenbesparingen doordat er efficiënter gecommuniceerd kan worden. Daarnaast worden bedrijfsprocessen hierdoor beter beheerst en zijn ketens binnen SNS minder afhankelijk van SPOK's. Een bijkomend voordeel is dat taken hierdoor makkelijker overgedragen kunnen worden en dat het opleiden van nieuwe medewerkers efficiënter verloopt.

7.11. Controlerapport

Na de verschillende controles en metingen wordt het controlerapport opgesteld. In het controlerapport worden allereerst de bevindingen en aanbevelingen gepresenteerd aan de opdrachtgever. Hierin wordt het risicoprofiel aangegeven door middel van de belangen 'Hoog', 'Midden' en 'Laag'. Ook wordt hier een oordeel over gegeven waarbij er gebruik gemaakt wordt van de statussen 'Goed', 'Voldoende', 'Onvoldoende' en 'Slecht'. Het management van het bedrijfsonderdeel geeft aan dat het akkoord gaat met deze bevindingen en aanbevelingen.

Vervolgens wordt het object van het onderzoek aangegeven. Dit is dus de reikwijdte van het project. Daarna wordt er per specifiek risico aangegeven wat het belang daarbij is en wat de gevolgen kunnen zijn bij het optreden van het risico.

7.12. ISO27001 certificaat

Zodra de certificering nagenoeg ten einde is dient het bedrijfshoofd van het bedrijfsonderdeel de Verklaring van Toepasselijkheid te ondertekenen. Deze verklaring houdt in dat het bedrijfshoofd akkoord is met inhoud van het controlerapport en de uitgevoerde certificering, en dus ook met het ISMS. De Verklaring van Toepasselijkheid is opgenomen in het controlerapport. De laatste stap is de uitreiking van het certificaat, waarmee aantoonbaar gemaakt kan worden dat het bedrijfsonderdeel gecertificeerd is volgens ISO27001. Het certificaat zal worden ondertekend door het afdelingshoofd van de afdeling Informatiebeveiliging & Controle. Een ztemplate van het ISO27001 certificaat is opgenomen in externe bijlage XI.

7.13. Presentatie introductie ISO2700X

De introductie over ISO27001 en ISO27002 wordt gehouden voor het management van het bedrijfsonderdeel dat gecertificeerd gaat worden. Er wordt informatie gegeven over wat kritische risico's en dreigingen kunnen zijn en waarom informatiebeveiliging toegepast dient te worden binnen SNS Bank. Ook wordt het beheerproces van ISO27001 uitgelegd en worden de beheersingsmaatregelen uit ISO27002 onder de loep genomen om op die manier aan te geven dat de set van maatregelen gebaseerd is op BIV (Beschikbaarheid, Integriteit en Vertrouwelijkheid).

Vervolgens worden de doelstellingen van de certificering uitgelegd en wat het stappenplan van het ISMS is en hoe het verdere certificeringproces eruit ziet, welke voorwaarden hiermee gemoeid zijn en de bijbehorende planning. Deze introductie wordt gehouden omdat het belangrijk is dat het management betrokkenheid toont bij het project en dat het inziet waarom het noodzakelijk is om deze certificering uit te voeren.

7.14. Workshop ISMS

De Workshop ISMS wordt gegeven aan de IB-coördinatoren (en eventueel het management) en geeft informatie over de te nemen stappen tijdens de workshop (reikwijdte bepalen, beleid bepalen, risicoanalyse uitvoeren), maar ook het vervolg van het certificeringproces (de aanpak van risicomanagement, het selecteren van maatregelen en de Verklaring van Toepasselijkheid). Tijdens deze workshop worden dus de stappen van het ISMS doorlopen en ingevuld.

Het geven van deze workshop heeft als voordeel dat de IB-coördinatoren worden voorbereid op de certificering en dat ze wat meer gevoel krijgen bij hetgeen van ze wordt verwacht, waardoor het proces sneller zal gaan verlopen.

7.15. Presentatie afdelingsoverleg

De presentatie tijdens het afdelingsoverleg bij het bedrijfsonderdeel dat gecertificeerd gaat worden is puur bedoeld om de dan huidige status van de ISMS voortgang te bespreken. Hierin wordt vermeld welke actiepunten er zijn opgetreden, wat de status is van die actiepunten en wat de status van het beveiligingsniveau is. Daarna wordt vermeld wat de vervolgacties en eventuele andere aandachtspunten zijn.
Hieronder in figuur 12 zijn de 15 ISMS Toolkitproducten in een schematisch overzicht weergegeven:

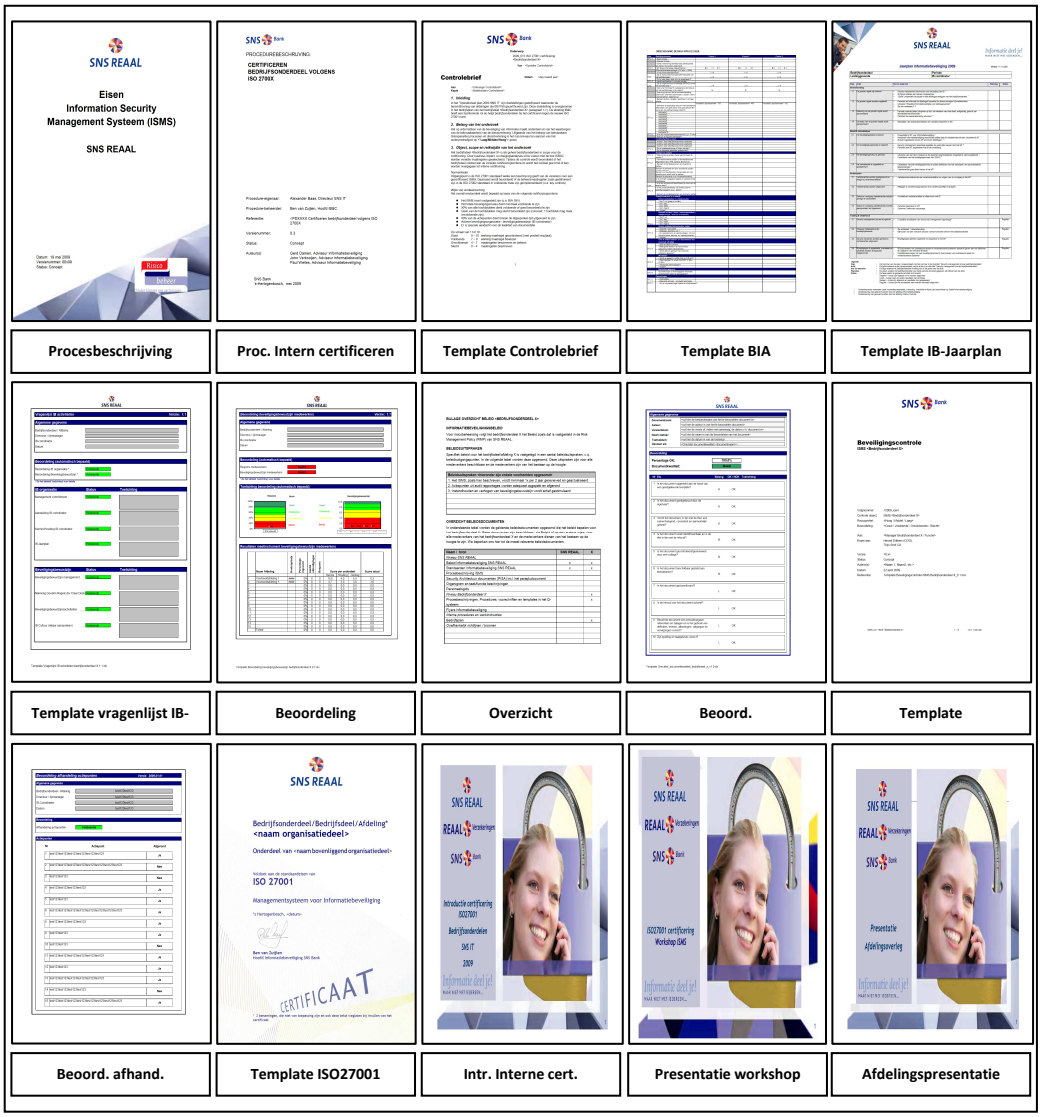


Fig. 12:Overzicht van de nieuwe certificeringmethodiek: de ISMS Toolkit.

8. Implementatie en testfase: Certificeringproces Relatiebeheer

“Bedrijfsonderdeel Relatiebeheer aantoonbaar In Control door ISO 27000 certificering”

De nieuwe certificeringmethodiek (de ISMS Toolkit) is tijdens het project gebruikt in de pilotfase. In deze pilot is het bedrijfsonderdeel Relatiebeheer van SNS IT gecertificeerd volgens ISO27001. Hierbij is dus de volledige toolkit gebruikt. In dit hoofdstuk wordt kort aangegeven uit welke afdelingen het bedrijfsonderdeel Relatiebeheer bestaat en wat voor werkzaamheden er worden uitgevoerd. Vervolgens is het hele certificeringproces toegelicht.

8.1. Relatiebeheer

De pilotcertificering is uitgevoerd bij het bedrijfsdeel Relatiebeheer. Dit is de ICT Frontoffice voor SNS bank, banklabels en groepsstaven: één centraal aanspreekpunt voor ICT diensten en facilitaire diensten bankkantoren, voor definitie en kwaliteitsbewaking van ICT diensten en voor optimale Business – ICT Alignment. Binnen het bedrijfsdeel Relatiebeheer zijn de afdelingen Servicedesk, Account Management en Service Level Management (SLM) ingericht.

De Servicedesk en de Account Managers & Consultancy onderhouden het primaire contact met de gebruiker. Bij de Servicedesk worden verstoringen, klachten en vragen opgelost en verwerkt, dienstaanvragen worden behandeld, enzovoorts.

Afdeling Account Management denkt mee met de afnemers over innovatie kansen die informatietechnologie biedt ter ondersteuning van de bedrijfsstrategie. Account Management is een relatief ‘kleine’ afdeling.

De afdeling SLM is verantwoordelijk voor het definiëren van diensten en het bewaken van de kwaliteit van de ICT dienstverlening op het vlak van Exploitatie en Beheer. Er worden onder andere Service Level Agreements (SLA’s) opgesteld waarin afspraken staan met de business en de leveranciers.[18]

De betrokken personen bij de certificering van Relatiebeheer zijn het management, maar in een actievere rol de drie IB-coördinatoren van de drie afdelingen binnen Relatiebeheer. Met deze drie medewerkers is het gehele certificeringproces doorlopen.

[18] Bron: Intranet SNS Bank: Delphi

8.2. Informeren van het management Relatiebeheer

Tijdens de start van het certificeringproces bij bedrijfsonderdeel Relatiebeheer is het management voor de 1ste keer geïnformeerd over dit proces middels de controlebrief. De controlebrief is tijdens deze bespreking definitief geworden. Het management van Relatiebeheer heeft de controlebrief goedgekeurd en is daarmee eindverantwoordelijk geworden voor de certificering. Het management van Relatiebeheer besteedt de uitvoering echter uit aan de IB-coördinatoren van SLM, AM en de Servicedesk.

8.3. Introductie ISO27000 bij Relatiebeheer

Aan het begin van het certificeringproces bij bedrijfsonderdeel Relatiebeheer is het management geïnformeerd over dit proces. De projectmanager heeft uitgelegd wat het ISMS inhoudt, dat de reikwijdte en het ISMS samen met de IB-coördinator worden bepaald en hoe de risicoanalyse zal worden uitgevoerd. Deze 'awareness-sessie' wordt voor het management gehouden met als reden dat er een stuk commitment ontstaat bij het management. Het belangrijkste onderdeel voor het management is de planning van het proces. Deze is dan ook uitvoerig behandeld tijdens deze sessie zodat het management weet hoeveel tijd er met dit proces gemoeid is. De sessie is gehouden aan de hand van een leidende presentatie.

8.4. Uitvoering workshop ISMS

De workshop in het kader van het ISMS is gegeven aan de IB-coördinatoren van de afdelingen Service Level Management, Account Management en de Servicedesk. Aan de hand van een presentatie zijn de bedoelingen van de workshop uitgelegd. Tijdens deze sessie is de BIA ingevuld en is het overzicht van de beleidsdocumenten concreet gemaakt.

8.5. Risicoanalyse m.b.v. ISRAC

Nadat de workshop was uitgevoerd heeft de 1ste ISRAC-meting plaatsgevonden. Tijdens deze 3 uur durende sessie is samen met de IB-coördinatoren de BIA, de TVA en de LOC ingevuld. Uit praktijkervaring blijkt dat verschillende vragen op meerdere manieren interpretabel zijn en dat er daardoor soms verwarring kan ontstaan. Dit bleek ook bij de sessies bij bedrijfsonderdeel Relatiebeheer. Door samen door de vragen heen te gaan heeft de projectmanager de vragen verduidelijkt en gespecificeerd voor de IB-coördinatoren.

8.6. Actie –en verbeterpunten

De ISMS onderdelen of beveiligingsmaatregelen waarop een onvoldoende wordt gescoord, worden bestempeld als actiepunt. Deze eventuele actiepunten moeten door het bedrijfsonderdeel binnen een vooraf bepaalde termijn opgelost worden, zodat er een nieuwe meting kan plaatsvinden m.b.t. deze actiepunten.

De risicoanalyse inclusief de bevindingen met tegenmaatregelen zijn opgenomen in een controlerapport, speciaal bestemd voor de afdeling Relatiebeheer. Het bedrijfshoofd van het betreffende bedrijfsonderdeel dient akkoord te zijn met de inhoud van het controlerapport, wil de certificering afgerond worden.

Relatiebeheer heeft een relatief klein aantal actiepunten dat zij dient te verbeteren. Deze actiepunten kunnen wegens vertrouwelijkheidfactoren niet worden genoemd in deze rapportage.

8.7. Presentatie overleg Relatiebeheer

Tijdens deze presentatie zijn de actiepunten, oftewel de tekortkomingen op het gebied van Informatiebeveiliging, aan de orde gekomen. Er is tijdens deze sessie door middel van een presentatie toegelicht wat de actiepunten zijn, waarom deze actiepunten zijn ontstaan en welke tegenmaatregelen er hiervoor genomen dienen te worden. Op deze manier worden de medewerkers bewust dat er binnen hun bedrijfsonderdeel waarde wordt gehecht aan informatiebeveiliging en kunnen zij antwoord geven op de vraag ‘Waar is dat ISO27001 certificaat voor?’

8.8. Controlerapportage

In het controlerapport dat is opgesteld voor Relatiebeheer zijn een aantal belangrijke zaken terug te vinden, onder andere de resultaten en bevindingen, de invulling van het ISMS, de Verklaring van Toepasselijkheid en een actiepuntenlijst. Vanwege de vertrouwelijke informatie die in dit rapport is vastgelegd kunnen de genoemde onderwerpen niet in deze rapportage gepubliceerd worden.

8.9. Uitreiking ISO27001 certificaat

Door middel van het ISO27001 certificaat kan het bedrijfsonderdeel Relatiebeheer aantoonbaar maken dat het voldoet aan de ISO27001 standaard. De uitreiking van het certificaat is een officiële gelegenheid en dient aan het einde van de maand juni plaats te vinden bij Relatiebeheer. Normaliter wordt hier een kort artikel over geschreven en worden er foto's gemaakt van deze feestelijke gebeurtenis. Deze stukken worden vervolgens geplaatst op Delphi, het intranet van SNS Bank.


SNS REAAL

Bedrijfsonderdeel/Bedrijfsdeel/Afdeling*
<naam organisatiedeel>

Onderdeel van <naam bovenliggend organisatiedeel>

Voldoet aan de standaardeisen van
ISO 27001

Managementsysteem voor Informatiebeveiliging

's Hertogenbosch, <datum>

Ben van Zuijlen
Hoofd Informatiebeveiliging SNS Bank

CERTIFICAAT

* 2 benamingen, die niet van toepassing zijn en ook deze tekst weglaten bij invullen van het certificaat

Fig. 13: De template van het interne ISO27001 certificaat

Omdat deze rapportage reeds is opgeleverd voordat de certificaatuitreiking plaatsvindt, is de vastlegging van deze gebeurtenis niet meer opgenomen in deze rapportage.

9. Conclusies en aanbevelingen

“Informatie deel je! Maar niet met iedereen…”

Tot slot zijn er een aantal conclusies en aanbevelingen geformuleerd die tot stand gekomen zijn na het uitvoeren van het afstudeerproject.

Bij aanvang van het certificeringproject is er een literatuurstudie uitgevoerd, waar conclusies en aanbevelingen zijn beschreven: een belangrijke aanbeveling is om de nieuwe ISO 27001 certificering te ondersteunen m.b.v. de nieuwe certificeringmethodiek, waarbij templates worden opgesteld om de documentatie van het ISMS te standaardiseren; een andere aanbeveling betreft het stellen van concrete eisen op het gebied van document(atie) en beheer daarvan. Tenslotte wordt geadviseerd om alle nog te publiceren ISO 2700X reeksen nauwlettend in de gaten te houden waarbij vooral ISO 27015 centraal staat, wat de norm wordt voor de financiële dienstensector.

.

Tijdens de ontwikkeling van de nieuwe certificeringmethodiek (ISMS Toolkit), is gebleken dat de onderdelen uit deze toolkit belangrijke hulpmiddelen zijn om te komen tot een interne ISO27001 certificering. De presentaties die in de toolkit zijn opgenomen zijn goede hulpmiddelen gebleken om de in het ISMS opgenomen onderdelen toe te lichten aan management en medewerkers.

Deze ISMS Toolkit raakt drie belangrijke pijlers, namelijk meting, awareness en rapportage. De pijler ‘meting’ raakt daarbij de pijler ‘awareness’ omdat het beveiligingsbewustzijn onder de medewerkers en het functioneren van de IB-coördinatoren eenduidig is vastgelegd met behulp van de beschikbare templates uit de ISMS Toolkit. Dit draagt dus bij aan de SNS REAAL slogan ‘Gezond verstand, gezond geweten’. Daarnaast is de ‘Checklist documentkwaliteit’, waarbij eisen gesteld worden waaraan documenten dienen te voldoen, een krachtig hulpmiddel om documentatie op orde te houden. In de 3de pijler, rapportage, wordt m.b.v. een controlerapport vastgelegd wat de bevindingen en resultaten van de certificering zijn d.m.v. ingevulde ISMS Toolkit templates, waarmee het beoogde ISMS concreet gestalte heeft gekregen.

Tijdens het succesvol afgeronde certificeringproces bij het bedrijfsonderdeel Relatiebeheer is nadrukkelijk naar voren gekomen dat de presentaties en workshops worden gewaardeerd door het management en de IB-coördinatoren, wat betrokkenheid oplevert . Verder is gebleken dat het gebruik van de templates inzicht en ondersteuning biedt waardoor het certificeringproces efficiënter doorlopen kan worden. De afdeling IB&C doet zijn voordeel met de ISMS Toolkit doordat de opzet hiervan een eenvoudige vastlegging en samenstelling van het ISMS per bedrijfsonderdeel bewerkstelligt.

Het verdient absoluut de aanbeveling dat SNS IT gebruik blijft maken van de ISMS Toolkit om haar bedrijfsonderdelen intern te certificeren volgens ISO27001, waardoor zij ‘aantoonbaar In Control’ blijft. Want informatie deel je! Maar niet met iedereen…

Evaluatie

Tijdens mijn afstudeerstage bij SNS Bank heb ik veel ervaring opgedaan op het gebied van Informatiebeveiliging. Tijdens mijn opleiding heb ik enige raakvlakken gehad met dit onderwerp. Toch bleek het in de praktijk brengen van een project complexer dan dat ik me had voorgesteld.

Ik ben van mening dat ik meer praktisch inzicht heb verkregen (ook op basis van de theoretische ervaring die ik tijdens mijn opleiding heb opgedaan) doordat ik mezelf heb 'ingeleefd' in de opdracht. Omdat ik met verschillende collega's te maken had, ook buiten mijn eigen afdeling, zijn mijn sociale contacten verbeterd door veel samen te werken. Ook heb ik met regelmaat zelfstandig werkzaamheden uitgevoerd. Daarnaast vind ik dat ik veel inzet heb getoond bij de uitvoering van het project en ik heb daarbij sterk het gevoel dat ik een gestructureerde manier van werken heb kunnen hanteren. Tijdens mijn stage heb ik ontzettende veel geleerd, wat ik pas na een tijd besefte.

Tijdens de stage heb ik op verschillende 'niveaus' gewerkt. Daarmee wil ik zeggen dat ik heb nagedacht om te werken op een hoger niveau (bijvoorbeeld het maken van een procedurebeschrijving en planningen) en om werkzaamheden op een lager, gedetailleerder niveau uit te voeren (bijv. templates bouwen). Zoals in het verslag is beschreven, heb ik een belangrijke bijdrage geleverd aan de ISMS Toolkit die volledig is goedgekeurd, en in gebruik is genomen. Daarmee geeft SNS IT ook een signaal af dat de kwaliteit van mijn opgeleverde eindproducten als goed is gemarkeerd. Omdat de toolkit veel onderdelen bevat voor verschillende doeleinden op verschillende niveaus is de kwantiteit van mijn werkzaamheden naar mijn mening meer dan voldoende te noemen. Door bovenstaande verantwoording wil ik aangeven dat ik een prettig gevoel over heb gehouden aan mijn afstudeerstage.

Ik heb geleerd dat het niet altijd gaat zoals je zelf had ingepland of zoals je zelf zou willen. Doordat er altijd onvoorziene omstandigheden optreden of doordat er sprake is van gewijzigde inzichten tijdens de uitvoer van een project, loop je al gauw achter en dus was het achteraf zeer verstandig om uitloop in te plannen. Verder is het een goed leermoment dat niets vanzelf gaat en dat je zelf actief dient te zijn als je iets voor elkaar wilt krijgen. Daarbij hoort ook het ruim van tevoren inplannen van afspraken.

Ik heb met de afdeling Relatiebeheer veel contact gehad met het management en de IB-coördinatoren van deze afdeling. Omdat ik zelf graag initiatieven wilde nemen heb ik soms onderwerpen gecommuniceerd waarvan het beter was dat ik dit in overleg had gedaan met mijn stagebegeleiders. Voorbeeld: ik had de vragenlijsten die in ISRAC worden ingevuld naar de IB-coördinatoren verstuurd voordat de sessie begon. Naar mijn idee zou dit tijdwinst opleveren als zij deze vragenlijsten van tevoren zouden doorlezen en invullen. Omdat deze werkzaamheden nogal veel tijd in beslag nemen bij de IB-coördinatoren was dit een wens van mij die niet mogelijk was. Vragende blikken vanuit Relatiebeheer kwamen naar afdeling IB&C. Deze perikelen heb ik opgelost door de fout toe te geven en corrigerende acties per e-mail uit te voeren. Dit is dus een leermoment voor mij.
Tijdens mijn stage heb ik veel input en ondersteuning gehad van mijn stagebegeleiders op de momenten dat dit nodig was, maar ook van mijn andere collega's. Zonder hen had ik deze opdracht onmogelijk kunnen uitvoeren.

Literatuurlijst

1. Boeken

1.1. Calder, Allen, *A management Guide – Implementing Information Security – based on ISO 27001 / ISO 17799*, 1ste druk, Van Haren Publishing, ,2006

1.2. Gert Wijnen, Willem Renes, Peter Storm, *ProjectMatig Werken,* 8ste druk, A-D Druk Zeist, 1991

2. Stukken, documenten en naslagarchieven

2.1. Informatiemap 'nieuwe medewerkers SNS Bank'

2.2. Nederlandse norm 'NEN-ISO/IEC 27001 (nl) Informatietechnologie – Beveiligingstechnieken – Managementsystemen voor informatiebeveiliging – Eisen (ISO/IEC 27001:2005, IDT)

2.3. 7 gouden regels met voorbeelden.doc

2.4. Damen, Gerd, *eisen_0.3.xls*

2.5. Welles, Paul, *Literatuurstudie_ISO27000_v1.0.doc*, versie 1.0, 2009

2.6. VallentGoed, Alex; Damen Gerd; Goedemans, Ton; Verkooijen, John; Welles, Paul, *Procesbeschrijving ISMS_00_09*

3. Websites

3.1. Wikipedia Encyclopedie, Wikimedia Nederland, www.wikipedia.nl, http://nl.wikipedia.org/wiki/CIA_Triad

3.2. Wikipedia Encyclopedie, Wikimedia Nederland, http://nl.wikipedia.org/wiki/ISO/IEC_27001

3.3. Wikipedia Encyclopedie, Wikimedia Nederland, http://nl.wikipedia.org/wiki/Code_voor_Informatiebeveiliging

3.4. Digital Academic Repository , Universiteit van Amsterdam, medium voor wetenschappelijke publicaties, www.dare.uva.nl, http://dare.uva.nl/document/98555.

3.5. Computerwoorden.nl, http://www.computerwoorden.nl/direct--19194--Core%20business.htm

3.6. Computable, http://www.computable.nl/artikel/ict_topics/security/2549644/1276896/nederland-veiliger.html

4. Webapplicaties intern

4.1. Q-systeem SNS Bank (http://sharepoint.bank.local/sites/200807032/default.aspx).

4.2. ISRAC (http://israc.bank.local/index.php).

4.3. Q- systeem: (http://sharepoint.bank.local/sites/q_systeem/Lists/Begrippenlijst/DispForm.aspx?ID=35&Source=http%3A%2F%2Fsharepoint%2Ebank%2Elocal%2Fsites%2Fq%5Fsysteem%2Fdefault%2Easpx).

4.4. Delphi Intranet (http://srgintranet.concern.srg/)

Bronnen die niet digitaal benaderbaar zijn en opgeleverde producten die bestemd zijn voor SNS Bank zijn op verzoek opvraagbaar bij de afdeling IB&C van SNS Bank.

Bijlagen

Dit afstudeerrapport bevat een tweetal bijlagen. De eerste bijlage (bijlage A) bevat het Plan van Aanpak, welke in de beginperiode van de afstudeerstage is geschreven en goedgekeurd. Verschillende hoofdstukken en/of paragrafen uit het afstudeerrapport corresponderen al dan niet direct met dit Plan van Aanpak. Bijlage B is een samenvatting van de bijstuurmomenten aan de hand van een 'Issuelog'. Het Issuelog is een binnen SNS IT veel gebruikte methode om gewijzigde inzichten en bijsturingen vast te leggen.

Uiteraard zijn er tijdens de uitvoer van het project aanzienlijk meer documenten opgeleverd dan de twee voornoemde. Vanwege de omvang van deze documentatie is hier een apart bijlagenverslag van gemaakt, wat de leesbaarheid van het afstudeerrapport bevordert en de complexiteit en omvang van dit afstudeerrapport vermindert. Het aparte bijlagenverslag bestaat uit de documentatie van de ISMS Toolkit, projectvoortgangsrapportages en het literatuuronderzoek. Hiervoor wordt doorverwezen naar het apart bijgeleverde document 'Eindproducten afstudeerstage SNS Bank Paul Welles'.

A Projectplan

Projectplan

Projectnaam	PP_Interne certificering volgens ISO27001
Projectcode	V2009IT11230_STAG_PW
Versie	1.0
Status	Definitieve versie
Datum	02-03-2009
Referentie	Template Projectplan_v1.1

Opdrachtgever	**Project manager**
Naam: Ben van Zuijlen	Naam: Paul Welles
Functie: Afdelingshoofd IB&C	Functie: Afstudeerder IB&C
Versie: 1.0	Versie: 0.93
Datum goedgekeurd: 2 maart 2009	Datum vastgesteld: 2 maart 2009

1ste Bedrijfbegeleider	**2de bedrijfsbegeleider**
Naam: John Verkooijen	Naam: Gerd Damen
Functie: Adviseur IB&C	Functie: Adviseur IB&C
Versie: 1.0	Versie: 1.0
Datum gezien	Datum gezien

1ste Afstudeerstagedocent	**2de Afstudeerstagedocent**
Naam: Adri Cornelissen	Naam: Marco Dorenbos
Functie: Afstudeerstagedocent Fontys	Functie: Afstudeerstagedocent Fontys
Versie: 1.0	Versie: 1.0
Datum akkoord:	Datum akkoord:

Versieblad

Versie	Status	Datum	Wijzigingen
0.1	Concept	02-02-2009	Eerste conceptversie, opzet en hoofdstukindeling
0.2	Concept	04-02-2009	Aanpassingen Indeling, invulling
0.3	Concept	05-02-2009	Aanpassingen J. Verkooijen verwerkt
0.5	Concept	11-02-2009	Aanpassingen J. Verkooijen, A. Cornelissen verwerkt
0.9	Concept	23-02-2009	Opmerkingen en aanpassingen G. Damen verwerkt
0.92	Concept	25-02-2009	Opmerkingen en aanpassingen J. Verkooijen, G. Damen verwerkt
0.93	Concept	26-02-2009	Opmerkingen en aanpassingen G. Damen, B. van Zuijlen verwerkt
1.0	Definitief	02-03-2009	Goedgekeurd door B. van Zuijlen

Distributieblad

Ontvangers	Functie
Ben van Zuijlen	Afdelingshoofd IB&C
John Verkooijen	Adviseur Informatiebeveiliging
Gerd Damen	Adviseur Informatiebeveiliging
Adri Cornelissen	1ste Stagedocent Fontys Hogeschool ICT
Marco Dorenbos	2de Stagedocent Fontys Hogeschool ICT

Gerefereerde documenten

Naam	Auteur	Versie	Datum
Bedrijfsplan Informatiebeveiliging & Controle 2009	Ben van Zuijlen	1.0	n.v.t.
Opdrachtomschrijving afstudeerstage SNS Bank	Paul Welles	1.0	22 december 2008
Beleid Informatiebeveiliging	Simon Greve, Ben van Zuijlen	0.91	12 januari 2009
Standaarden Informatiebeveiliging SNS Reaal	G. Damen, T. Goedemans, A. Vallentgoed, A. Verkooijen, J.	0.91	14 januari 2009
Schema voor Certificatie van Informatiebeveiliging op basis van ISO/IEC 27001	ECP.NL	4.0	4 november 2006
ISO 27001:2005	NEN/IEC/ISO	n.v.t.	n.v.t.

INHOUDSOPGAVE

SAMENVATTING **48**

1. PROJECTOPDRACHT **49**

1.1 PROJECTACHTERGROND 49
1.2 PROJECTDOELSTELLING 49
1.3 OPDRACHTFORMULERING 49
1.4 OP TE LEVEREN RESULTATEN 50
1.5 RANDVOORWAARDEN 50
1.6 UITGANGSPUNTEN 51
1.7 ACCEPTATIECRITERIA 51
1.8 KRITIEKE SUCCESFACTOREN (KSF) 51
1.9 RELATIES NAAR ANDERE PROJECTEN 51

2. PROJECTAANPAK **52**

2.1 PROJECTAANPAK 52

3. PROJECTORGANISATIE **53**

3.1 BESTURINGSMODEL 53
3.2 PROJECTGOVERNANCE 53
3.3 COMMUNICATIEPLAN 54
3.3.1 OVERLEGSTRUCTUREN 54
3.3.2 RAPPORTAGES 54

4. PLANNING **55**

4.1 ACTIVITEITENPLANNING PER FASE 55
4.2 MIJLPALENPLANNING 56
4.3 RESOURCEPLANNING 56

5. BEHEERSINGSMECHANISMEN **57**

5.1 TOLERANTIE 57
5.2 CHANGE MANAGEMENT 57
5.3 RISICOMANAGEMENT 57
5.4 KWALITEITSMANAGEMENT 57
5.5 TESTMANAGEMENT 58
5.5.1 TESTSCOPE 58
5.5.2 TESTSTRATEGIE 58
5.5.3 TESTOMGEVINGEN 58

1. SAMENVATTING

Dit document beschrijft het projectplan dat Paul Welles in het kader van zijn afstudeerwerk voor de opleiding Bedrijfskundige Informatica aan de Fontys Hogeschool te Eindhoven gaat uitvoeren. Deze afstudeerstage wordt uitgevoerd bij de afdeling Informatiebeveiliging & Controle van SNS IT (de automatiseringsafdeling van SNS Bank). Het project is erop gericht om een methodiek te ontwikkelen om een bedrijfsonderdeel van SNS Bank middels het interne certificeringtraject volgens de ISO27001 norm te kunnen realiseren. Deze certificering geeft het management waarborg dat de risico's ten aanzien van Informatiebeveiliging binnen het gecertificeerde bedrijfsonderdeel zijn beperkt tot een aanvaardbaar niveau. De ontwikkelde methodiek zal ook in pilot vorm worden getest bij een afdeling van SNS IT, zodat eventuele tekortkomingen in de ontwikkelde methodiek kunnen worden gecorrigeerd.

Voor de volledige opdrachtformulering en de concrete op te leveren projectresultaten wordt verwezen naar hoofdstuk 1.

De te verwachten tijdbesteding van Paul voor het project zal ongeveer 800 uur bedragen. Het project start in februari en loopt tot eind juni 2009. Aan het project zijn geen externe kosten verbonden zodat geen begroting maar een overzicht van te besteden uren in dit plan is opgenomen.

Het project wordt uitgevoerd conform de binnen SNS Bank gebruikte projectmanagement methodiek PMW Professional (kortweg PMW-P genoemd). Conform deze methodiek zal periodiek worden gerapporteerd over status en voortgang van het project.

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 'Beheersingsmechanismen' beschrijft de beheersmechanismen voor een succesvolle uitvoering van het project.

1. PROJECTOPDRACHT

1.1 Projectachtergrond

Eind 2002 is voor SNS Bank het informatiebeveiligingsbeleid vastgesteld door de Hoofddirectie en vastgelegd in het Handboek Informatiebeveiliging. Dit handboek is gebaseerd op de Britse standaard BS 7799-1:1999 en bevat een set van beveiligingsmaatregelen om de beveiligingsrisico's voor informatiesystemen te beperken tot een aanvaardbaar niveau. Om het beveiligingsniveau maar ook de interne beheersing van beveiligingsrisico's binnen afdelingen naar een hoger niveau te tillen is enkele jaren geleden binnen SNS IT besloten om afdelingen te gaan certificeren volgens BS 7799-2.

Binnenkort zal het beveiligingsbeleid binnen SNS vervangen worden door een nieuw Beleid Informatiebeveiliging, dat gebaseerd is op het meest recente ISO2700X normenkader. Het is daarom noodzakelijk om de certificeringmethodiek ook aan te passen volgens deze nieuwe standaard.

1.2 Projectdoelstelling

Het ontwikkelen van een methodiek voor certificering volgens ISO27001 waarmee het "in control" zijn van een bedrijfsdeel van SNS IT middels interne certificering ISO27001 aantoonbaar kan worden gemaakt.

1.3 Opdrachtformulering

Opdrachtgever is Ben van Zuijlen, afdelingshoofd Informatiebeveiliging & Controle. Gedelegeerde opdrachtgevers zijn John Verkooijen en Gerd Damen, adviseurs IB&C. De projectleider is Paul Welles, als afstudeerder werkzaam bij de afdeling IB&C.

Opdracht:

Bedenk op basis van beschikbare literatuur en middelen een concrete invulling voor de ISO 2700X certificeringmethodiek en voer deze voor een bedrijfsdeel uit. Pas indien nodig ISRAC (een binnen SNS gebruikte risicoanalysemethodiek) aan t.b.v. controle op documentatie. Draag na een pilotfase, en de eventueel daaruit voortkomende verbeteringen, de geaccordeerde methodiek over aan de afdeling IB&C.

Toelichting: De opdracht betreft het bedenken van een certificeringsmethodiek voor SNS volgens het PDCA-principe voor de structurering van het security managementproces volgens ISO 27001. De opdracht zal worden opgesplitst in twee delen, die overigens wel een sterke samenhang hebben:

1 ISO 27001-documentatie realiseren dat gespecificeerd zal worden voor het Information Security Management System. Het doel hierbij is het vaststellen, uitvoeren, monitoren, evalueren, onderhouden en het verbeteren van het ISMS. Er wordt hierbij ook aandacht besteed aan de behoeftes en doelstellingen, de veiligheid, en de omvang en structuur van SNS Bank.
2 Parallellopend zullen hier de ISO 27002 beheersmaatregelen voor informatiebeveiliging aan gekoppeld worden. De ca. 130 maatregelen die hierin beschreven staan, staan garant voor de gewenste beheersing volgens de aanwijzingen in ISO 27001. De werking van deze maatregelen zal worden geïdentificeerd en worden vastgelegd met behulp van een risico-evaluatie volgens de ISRAC methodiek.

1.4 Op te leveren resultaten

De op te leveren eindproducten van dit project in chronologische volgorde zijn:

1. Projectplan
2. Detailplanning
3. Literatuuronderzoek deel 1 en 2 (rapport).
4. Procesbeschrijving t.b.v. het Information Security Management System (ISMS)
5. Template Documentatiestandaard ISMS Q-systeem (= intern kwaliteitssysteem)
6. Projectvoortgangsrapportages (PVR's)
7. Template Controlerapport (risicoanalyse + advies)
8. Eindpresentatie SNS IT (IB)
9. Template ISO2700x certificaat
10. Eindpresentatie Fontys
11. Afstudeerscriptie

Alle resultaten zullen worden opgeleverd door Paul Welles al dan niet in samenwerking met de stakeholders. Voor de deadlines van de opleverdata wordt doorverwezen naar paragraaf 4.2 'Mijlpalenplanning'.

Bovenstaande eindproducten en activiteiten gelden alleen voor één specifiek bedrijfsonderdeel van SNS IT. Alle overige bedrijfsonderdelen kunnen conform de nieuwe methodiek worden gecertificeerd.

Voor meer gedetailleerde informatie wordt doorverwezen naar hoofdstuk 2 'Projectaanpak'.

1.5 Randvoorwaarden

Randvoorwaarden voor het slagen van het project zijn:

Randvoorwaarde	**Verantwoordelijk**
Voldoende resourcing beschikbaar vanuit SNS IT om mee te werken aan het project en benodigde informatie ter beschikking te stellen.	Afdeling IB&C en de te certificeren afdeling
Voldoende ondersteuning vanuit de SNS met betrekking tot eventuele vragen, feedback geven op documentatie en het tijd vrij maken voor besprekingen.	Bedrijfsbegeleiders SNS
Benodigde software voor de uitvoer van het project dient op de werkplek aanwezig te zijn. In het geval dat er toegang tot bepaalde systemen vereist is moet dit ook geregeld worden.	Afstudeerder voor aanvraag bij begeleiders. Begeleiders voor het verdere traject.
Begeleiders en opdrachtgever dienen op de hoogte te zijn van de voortgang van het project, om te kunnen bijsturen.	Afstudeerder
Terugkoppeling op documenten binnen 5 dagen.	Bedrijfsbegeleiders SNS

1.6 Uitgangspunten

Uitgangspunten voor dit project zijn:

Uitgangspunten
De certificering op basis van ISO27001 is een logisch vervolg op de BS7799.
De gehele opdracht dient uiterlijk te worden afgerond op 26 juni 2009

1.7 Acceptatiecriteria

Goedkeuring van opgeleverd(e) (eind)product(en) door de opdrachtgevers, te weten Ben van Zuijlen (afdelingshoofd IB&C) en Adri Cornelissen (afstudeerstagedocent Fontys Hogeschool ICT).

1.8 Kritieke Succesfactoren (KSF)

In onderstaande tabel heeft de opdrachtgever zelf aangegeven welke criteria (met daaraan gekoppeld een procentuele wegingsfactor) voor hem belangrijk zijn bij de uitvoering van dit project.

	(Klant)tevredenheidcriterium	Weging	Waardering
1	Het project wordt conform plan binnen budget en tijdsplanning opgeleverd	15%	
2	Uitgevoerd literatuuronderzoek	15%	
3	Certificeringsmethodiek (Procesbeschrijving ISMS, templates) is gedocumenteerd en integraal toepasbaar op bedrijfsonderdelen binnen SNS REAAL	30%	
4	Wijze waarop documentatie-eisen worden gemeten en vastgelegd	10%	
5	Een bedrijfsdeel heeft het hele certificeringtraject met succes doorlopen en certificeringdocumentatie is beschikbaar	20%	
6	Eindpresentatie	10%	
	Conclusie over het hele project		

1.9 Relaties naar andere projecten

Daar waar mogelijk wordt er samenwerking gezocht met het project “Key Controls SNS IT”. Dit kan de ISMS workshops betreffen. Daarnaast zal de output van dit project gebruikt worden in het project ‘ISO27001 interne certificering’, waar dhr. John Verkooijen projectleider van is.

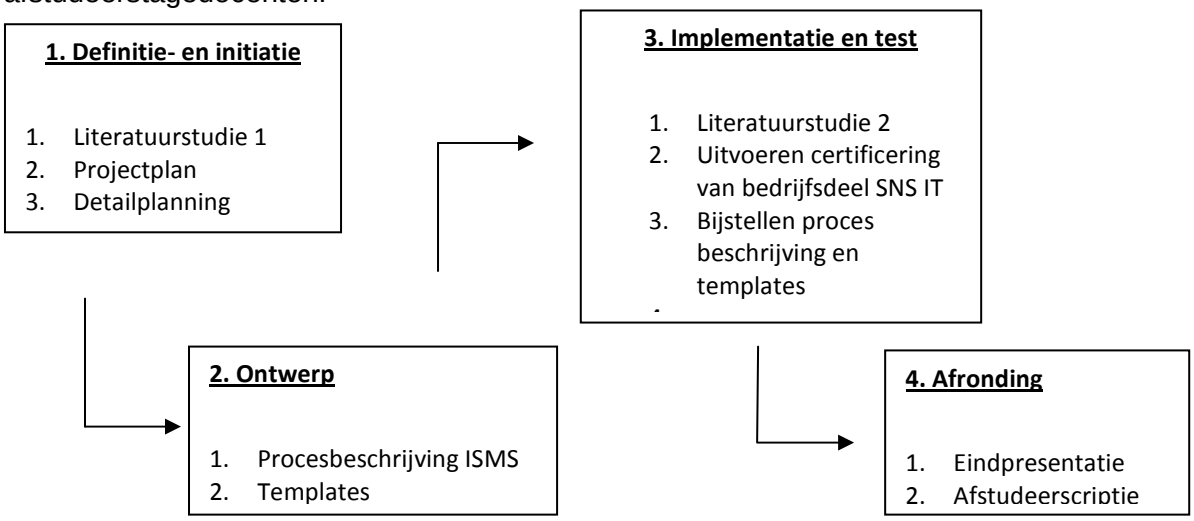
2. PROJECTAANPAK

2.1 Projectaanpak

In het nog te realiseren literatuuronderzoek wordt uitgelegd wat certificering op basis van de Code voor Informatiebeveiliging betekent en welke stappen ondernomen dienen te worden om een managementsysteem voor informatiebeveiliging (ISMS) op te zetten en te onderhouden. In deze paragraaf wordt dit alvast vertaald naar de aanpak om te komen tot een nieuwe certificeringsmethodiek en de certificering van één bedrijfsonderdeel binnen SNS IT.

Fasering

We onderscheiden in het project vier hoofdfasen. Dit is in onderstaande figuur weergegeven. De voortgang van het project in deze fasen wordt bewaakt door de opdrachtgever in samenwerking met de projectleider, bedrijfsbegeleiders en afstudeerstagedocenten.



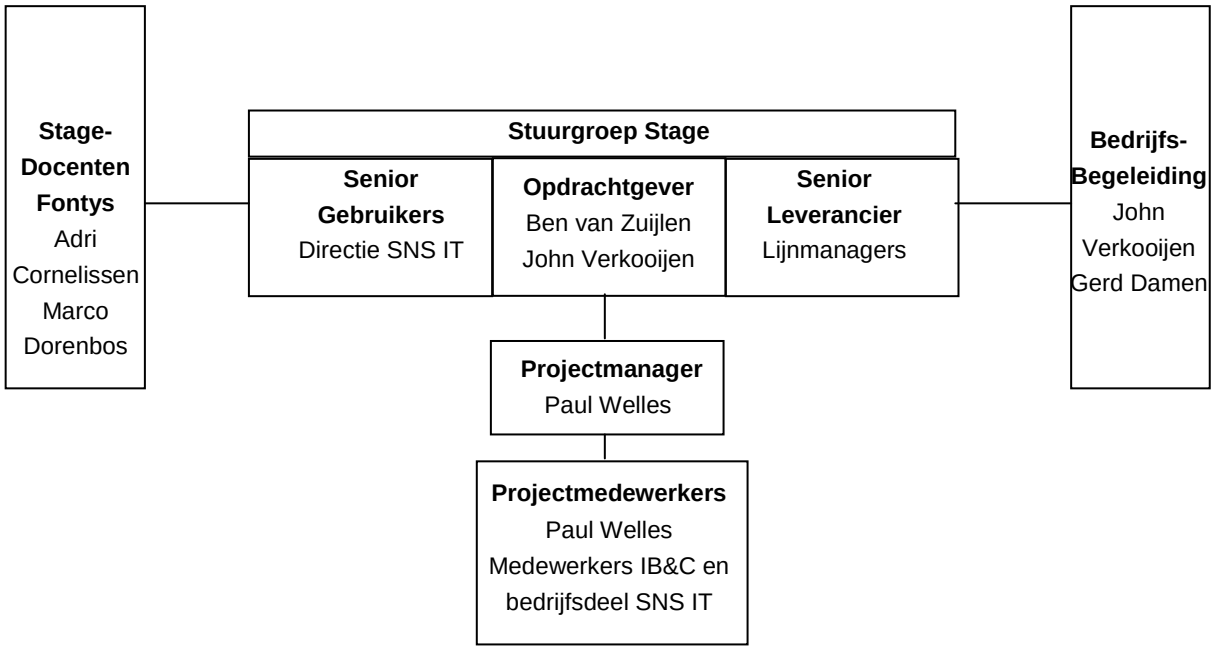
In de 1ste fase (definitie- en initiatiefase) wordt er om te beginnen onderzoek gedaan om kennis en vaardigheden op te doen zodat het project zo optimaal mogelijk kan worden uitgevoerd. Er wordt een literatuurstudie gedaan op basis waarvan een rapportage wordt opgesteld. Deze informatie is nodig voor het uitvoeren van de opdracht en het kunnen opstellen van het projectplan. In het projectplan staat ook de gedetailleerde planning van het project. Na goedkeuring kan worden gestart met de volgende fase.

In fase 2 (de ontwerpfase) wordt er allereerst begonnen met de procesbeschrijving van het ISMS inclusief de benodigde templates. Nadat deze procesbeschrijving is gerealiseerd, wordt er onder meer een ISMS documentatiestandaard opgesteld waarmee betrokkenen het ISMS continu kunnen controleren en bijstellen. Zodra de procesbeschrijving en templates zijn goedgekeurd kan gestart worden met de pilot om de methodiek in de praktijk te testen op een bedrijfsdeel binnen SNS IT. Na het doorlopen van het traject wordt de methodiek geëvalueerd en waar nodig bijgesteld en goedgekeurd door de opdrachtgever. De resultaten en bevindingen zullen worden opgenomen in ‘literatuurstudie 2’.In de 4de en laatste fase (de Afrondingsfase) zal het project worden afgerond. De resultaten van het project zullen worden gepresenteerd en in deze fase zal ook de afstudeerscriptie worden voltooid.

3. PROJECTORGANISATIE

3.1 Besturingsmodel

Voor het project is het volgende besturingsmodel van toepassing:



3.2 Projectgovernance

Rol	Wie	Taken, verantwoordelijkheden, bevoegdheden
Opdrachtgever	Ben van Zuijlen	Managen van het project in relatie tot de overall doelen van SNS (IT).
Sr. Gebruiker	Directie SNS IT	Beschikbaar stellen resources en afname projectdeliverables
Sr. Leverancier	Lijnmanagers	Leveren medewerkers voor projectmanagement, uitvoering en ondersteuning
Projectmanager	Paul Welles	Planning, uitvoering en rapportage.
Projectmedewerkers	Paul Welles, Medewerkers IB&C, Medewerkers bedrijfsdeel SNS IT	Uitvoeren projectactiviteiten
Afstudeerstagedocenten	Adri Cornelissen Marco Dorenbos	Ondersteuning leveren bij de uitvoering van het project indien dit gewenst is.
Bedrijfsbegeleiding	John Verkooijen Gerd Damen	Begeleiding student

3.3 Communicatieplan

3.3.1 Overlegstructuren

Het project wordt in termen van status en voortgang periodiek besproken in voortgangsoverleggen met de (gedelegeerde) opdrachtgever(s). Er zullen met de te certificeren afdeling ad hoc overleggen worden geïnitieerd. Alle op te leveren eindproducten zullen op nader te bepalen momenten worden besproken met de opdrachtgever en afstudeerstagedocenten.

3.3.2 Rapportages

Conform PMW-P zal periodiek een projectvoortgangsrapportage worden opgesteld.

4. PLANNING

4.1 Activiteitenplanning per fase

Fase			
Activiteiten per fase	**Week nummer**	**Uitvoerder**	**Uren**
1. Definitie- en initiatiefase			
Uitvoeren literatuurstudie	6, 7	Paul Welles	72
Opstellen literatuuronderzoek 1	8, 9	Paul Welles	15
Opstellen Projectplan	8, 9	Paul Welles	22
Opstellen Detailplanning 1.0	8, 9	Paul Welles	10
Maken opzet afstudeerscriptie	8	Paul Welles	12
Evalueren en bijsturen literatuurstudie, projectplan, detailplanning en afstudeerscriptie	9	Paul Welles	7
2. Ontwerpfase			
Opstellen procesbeschrijving ISMS m.b.v. PDCA-cyclus en te hanteren controlesheet	10, 11	Paul Welles	72
Opstellen/vernieuwen documentatie ISMS (Documentatiestandaard Q-systeem)	12, 13	Paul Welles	72
Borgen en bijsturen (voortgangsrapportage)	13	Paul Welles	18
Opstellen afstudeerscriptie (periodieke activiteit)	14	Paul Welles	36
Koppelen van ISO 27002 beheersingsmaatregelen aan de SNS REAAL implementatie van 27001-documentatie (literatuuronderzoek 2)	15, 16	Paul Welles	72
Opstellen afstudeerscriptie (periodieke activiteit)	17	Paul Welles	36
3. Realisatie- en testfase			
Uitvoeren pilot afdelingcertificatie	18 t/m 22	Paul Welles	72
Risico-analyse incl. geadviseerde verbetermaatregelen uitvoeren	18 t/m 22	Paul Welles	72
Opstellen controlerapport met resultaten t.o.v. beoogde resultaten m.b.v. ISRAC of advies	18 t/m 22	Paul Welles	36
Evalueren realisatie- en testfase	23	Paul Welles	24
4. Afrondingsfase			
Presenteren aan stakeholders (SNS, Fontys)	23, 24	Paul Welles	2
Template certificaat opstellen	23, 24	Paul Welles	8
Afronden afstudeerscriptie	23, 24	Paul Welles	35
Overige formaliteiten afhandelen	23, 24	Paul Welles	3
Activiteiten uitvoeren i.v.m. eventuele uitloop	25, 26	Paul Welles	72
Totaal aantal uren			**800**

De uitvoering en realisatie van alle activiteiten en eindproducten zullen al dan niet onder begeleiding geschieden van John Verkooijen en Gerd Damen. Verschillende activiteiten lopen parallel aan specifieke andere activiteiten, wat betekent dat meerdere activiteiten in hetzelfde tijdsbestek langs elkaar kunnen worden uitgevoerd.

4.2 Mijlpalenplanning

Fase	Mijlpaal	Geplande kalenderweek van oplevering	Toetsing
1	Definitief projectplan	9	Ben van Zuijlen, John Verkooijen, Gerd Damen
1	Detailplanning	9	Ben van Zuijlen, John Verkooijen, Gerd Damen
1	Literatuuronderzoek deel 1	10	John Verkooijen, Gerd Damen
2	Procesbechrijving ISMS	12	John Verkooijen, Gerd Damen
2	ISMS Documentatiestandaard (Q-systeem)	13	John Verkooijen, Gerd Damen
Overall	Projectvoortgang rapportages	periodiek	Ben van Zuijlen, John Verkooijen, Gerd Damen
2	Literatuuronderzoek deel 2	18	John Verkooijen, Gerd Damen
3	Controlerapport (risicoanalyse + advies)	24	John Verkooijen, Gerd Damen
4	Eindpresentatie aan stakeholders SNS	25	Ben van Zuijlen, John Verkooijen, Gerd Damen
4	Template ISO2700x certificaat	Einde van project, n.t.b.	Ben van Zuijlen, John Verkooijen, Gerd Damen
4	Projectafronding (afstudeerscriptie en eindpresentatie Fontys)	25	Adri Cornelissen, Marco Dorenbos, (Ben van Zuijlen)

Bij eventuele afwezigheid van dhr. John Verkooijen zullen de mijlpaalproducten getoetst worden door dhr. Gerd Damen.

Benodigde middelen
Er is geen specifieke externe kennis nodig, **€0, -** begroot.

De benodigde tooling, ISRAC is reeds in het bezit van de afdeling IB&C. Een nieuwe versie met significante verbeteringen wordt verwacht in het 1ste kwartaal van 2009.

4.3 Resourceplanning

Benodigde resources/competenties	***2009***	***Uren Totaal***
Afdeling IB&C	800	800
Te certificeren afdeling	38	38
	838	**838**

5. BEHEERSINGSMECHANISMEN

5.1 Tolerantie

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

5.2 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.

5.3 Risicomanagement

Nr.	Risico beschrijving	Weging	Maatregel	Periode
R01	Beschikbaarheid medewerkers	Midden	Commitment Directie, bedrijfshoofd en afdelingshoofd	Hele project
R02	Langdurige ziekte	Hoog	Uitvoer project overdragen	Hele project
R03	Het project is niet binnen de gestelde termijn afgerond	Hoog	Per fase planning evalueren en eventueel bijstellen	Hele project
R04	Gebrek aan coördinatie van mensen, middelen en activiteiten	Midden	Afdelingshoofd, stuurgroep Stage	Hele project
R05	Oorspronkelijke uitgangspunten en eisen veranderen (voortdurend) tijdens uitvoering van het project	Midden	Projectplan bijstellen	Hele project

5.4 Kwaliteitsmanagement

Voor de toetsing van de kwaliteit van de eindproducten wordt u doorverwezen naar de tabel die is weergegeven in paragraaf 4.2 ‘Mijlpalenplanning’. In de laatste kolom wordt de toetser getoond. Met behulp van de weeknummers zijn ook de toetsmomenten af te leiden.

De eisen die gesteld worden aan de opbouw van de eindpresentatie, voordracht en verdediging en afstudeerscriptie zijn vastgelegd in het document ‘ABC formulieren BI.doc’, te vinden in het interne dossier van de afdeling IB&C en in het archief van Fontys Hogescholen.

Eisen m.b.t. de eindproducten voor SNS Bank worden in samenspraak met de bedrijfsbegeleiders vastgesteld.

5.5 Testmanagement

5.5.1 Testscope

De eindproducten die zijn genoemd in paragraaf 1.4 behoren tot de testscope van dit project, evenals de activiteiten die uitgevoerd dienen te worden voor de realisatie van de eindproducten.

5.5.2 Teststrategie

Door middel van de pilot wordt er een bedrijfsdeel van SNS IT gecertificeerd en vormt dit ook de testbasis voor alle andere te certificeren afdelingen. De organisatie van de uit te voeren tests heeft de onderstaande structuur en volgorde:

1. Invullen documentstandaard ISMS i.s.m. IB-coördinator van de te certificeren afdeling
2. Eventuele aanpassingen van de beheersingmaatregelen in ISRAC
3. Self-assessment m.b.v. ISRAC door de IB-coördinator van de te certificeren afdeling
4. Controle/meting door IB&C (Paul Welles)
5. Testresultaten en bevindingen worden opgenomen in het controlerapport.
6. Eventuele actiepunten dienen te worden uitgevoerd
7. Na accordatie komt de betreffende afdeling in aanmerking voor certificatie.

5.5.3 Testomgevingen

In dit project wordt er gebruik gemaakt van één testomgeving. Dit is de te certificeren afdeling. De periode waarin deze testomgeving nodig is dient nog nader vastgesteld te worden. De benodigde testdata staan beschreven op het dan gerealiseerde standaarddocument ISMS. Ook wordt er met behulp van ISRAC het self-assessment uitgevoerd. Het aantal testers bestaat uit 2 personen: de manager van de betreffende afdeling en de afstudeerder die het project leidt. Daarnaast wordt er ondersteuning geboden door de bedrijfsbegeleiders van Paul Welles.

B Samenvatting bijstuurmomenten

Binnen SNS IT wordt gebruik gemaakt van een issuelog. In dit issuelog staan de gewijzigde inzichten die tijdens de projectvoortgang aan het licht komen. Middels dit issuelog wordt daarnaast verantwoording afgelegd en wordt aangegeven wie de eigenaar van het issue is, wat de prioriteit daarvan is en wat de oplossing voor het issue is.

Projectnaam	Interne certificering volgens ISO27001										
Projectcode	V2009IT11230_STAG_PW										
Datum	12-jun-2009										
Referentie	Template Issuelog_v1.0										
ID	**Omschrijving**	**DETAILS (inclusief mogelijke oplossing)**	**Update**	**Prioriteit**	**Eigenaar**	**Datum geopend**	**Ingediend door**	**Oplosdatum**	**Bijgestelde Oplosdatum**	**Status**	**Datum opgelost**
1	bijstellen opdracht + projectplan	opdracht is bijgesteld, vooral qua eindproducten en detailplanning	de eindproducten en overige inhoud zijn licht gewijzigd (zie pag. 12), daarnaast is de detailplanning drastisch gewijzigd (zie pag. 11).	hoog	Ben van Zuijlen	19-2-2009	Paul Welles	vrijdag 27 februari 2009	maandag 2 maart 2009	ter goedkeuring voorgelegd LG	maandag 2 maart 2009
2	switch van eindproducten	de template documentatiestandaard krijgt voorrang boven de procesbeschrijving van de ISMS template + controlesheet. De werkzaamheden en opleverdata worden dus eveneens omgeruild.	De data van oplevering worden hiermee ook geswitched: documentatiestandaard wordt in week 12 opgeleverd, procesbeschrijving ISMS in week 13.	midden	Ben van Zuijlen	4-4-2009	Paul Welles	4-3-2009	n.v.t.	goedgekeurd	4-3-2009
3	literatuuronderzoek 2 vervalt	Literatuuronderzoek 2 vervalt omdat dit niet nodig blijkt te zijn, de uren die vrijkomen worden besteed aan de realisatie van het ISMS. Bijstellen projectplan is niet nodig vanwege het daarvoor bestemde issuelog (dit document).	Akkoord gegeven door stagebegeleiders.	midden	Ben van Zuijlen	12-4-2009	Paul Welles	12-4-2009	n.v.t.	Projectplan versie 1.1ter goedkeuring voorgelegd aan LG	12-4-2009
4	Procesbeschrijving later opgeleverd dan gepland	De procesbeschrijving is door gewijzigde inzichten later opgeleverd dan gepland. Daarnaast zijn er templates voor het ISMS bijgekomen waardoor de controlesheet (tussenrapportage) hier onderdeel van is geworden.	De procesbeschrijving ligt ter inzage bij het afdelingshoofd.	laag	Ben van Zuijlen	20-3-2009	Paul Welles	8-4-2009	n.v.t.	ter goedkeuring voorgelegd LG	8-4-2009
5	Checklist kwaliteit documenteisen heeft meer tijd in beslag genomen dan ingepland.	Vanwege gewijzigde inzichten bij het afdelingshoofd IB&C en de stagebegeleiders, heeft de ontwikkeling en oplevering van de checklist vertraging opgelopen. Deze vertraging heeft geen invloed op de planning, omdat de tijd voor literatuuronderzoek 2 hiervoor gebruikt wordt.	Verschillende collega's van IB&C hebben de checklist gebruikt bij het beoordelen van documenten als test. De feedback die hieruit is voortgekomen is in de checklist verwerkt en vervolgens opgeleverd bij het afdelingshoofd.	laag	Ben van Zuijlen	27-3-2009	Paul Welles	16-4-2009	n.v.t.	ter goedkeuring voorgelegd LG	16-4-2009
7	Pilotfase certificering vangt in de eerste week van mei 2009 aan i.p.v. de laatste week van april 2009	Omdat de ISMS Toolkit (het hulpmiddel wat we nodig hebben voor en tijdens de certificering) niet eerder gereed is, wordt de pilotfase één week opgeschoven. Hier is rekening mee gehouden door twee uitloopweken in de detailplanning op te nemen.	De pilotfase gaat in week 20 van start	midden	Ben van Zuijlen	15-4-2009	Paul Welles	16-4-2009	8-5-2009	n.v.t.	8-5-2009
8	Uitreiking van het certificaat aan afdeling Relatiebeheer kan, indien er geen actiepunten zijn die voortkomen uit de meting, in juni 2009 plaatsvinden i.p.v. in december 2009.	Omdat de afstudeerstage half juni/eind juni 2009 zijn einde nadert, is het voor de afstudeerder beter dat de uitreiking van het certificaat al in juni gaat plaatsvinden i.p.v. in december. Dit is een extra deliverable wat wellicht al in juni opgeleverd kan worden. Indien er toch teveel actiepunten zijn wordt er van de oorspronkelijke situatie uitgegaan.		laag	Ben van Zuijlen	15-4-2009	Paul Welles	16-4-2009	n.v.t.	Niet gestart	