



CIO Platform Nederland
Informatie Beveiling



Informatie Beveiling
Resultaat van de CIO Interest Group

Onderwerpen:
Informatiebeveiling in control
Security awareness
Identity en Access management

Tweede publicatie van het CIO Platform Nederland
Juni 2007

Van de voorzitter

Dit is de tweede publicatie van het CIO Platform Nederland. Dit platform is een onafhankelijke vereniging van CIO's en ICT directeuren van de grote bedrijven in Nederland.

Binnen ons platform zijn diverse werkgroepen, de CIO Interest Groups (CIGs), actief om verschillende, voor de CIO interessante onderwerpen, uit te diepen en hierover aan de leden van het CIO Platform verslag te doen.

De algemene informatie, zoals dit rapport, stellen wij graag publiekelijk beschikbaar. In het geval van dit rapport is veel input beschikbaar gekomen van de leden en als best practice in deze publicatie gebundeld.

Onze eerste uitgave, de publicatie over Human Resource Management, is een eindrapport met daarin het resultaat van de werkzaamheden van de werkgroep *It-HRM* in 2005, gebaseerd op de aanzet uit 2004. Deze uitgave is op aanvraag gratis beschikbaar.

Deze tweede publicatie gaat in op het onderwerp informatiebeveiliging.

Bestuurders krijgen de laatste jaren zeer expliciet de verantwoordelijkheid voor risicobeheersing toebedeeld. Denk bijvoorbeeld aan de Code Tabaksblat en Sarbanes Oxley. Binnen risicobeheersing vormt het beveiligen van Informatie een cruciaal onderdeel.

Dit document bevat als eerste een overkoepelende beschrijving over de beheersing van informatiebeveiliging onder de titel: "Informatiebeveiliging in Control". Vervolgens een verdere detaillering van twee actuele onderdelen van informatiebeveiliging: "Security Awareness" en "Identity & Access management."

Ook is er een toolbox samengesteld uit de best practices van de deelnemende leden met concreet bruikbare zaken van voor een Security Awareness campagne. Deze toolbox is alleen voor de leden van het CIO Platform beschikbaar.

De deskundige inbreng van vertegenwoordigers van de leden heeft deze publicatie mogelijk gemaakt en levert een goed inzicht voor de CIO op genoemde gebieden. Graag bedank ik ze dan ook voor hun inbreng bij de totstandkoming van deze publicatie.

Namens het bestuur,



Peter Hagedoorn (CIO Océ)
Voorzitter CIO Platform Nederland.

Inhoud

1	Informatiebeveiliging in control	4
1.1	Managementsamenvatting	4
1.2	Probleemstelling	4
1.3	Definitie "In control" voor Informatiebeveiliging	4
1.4	Waarom "in control"?	4
1.5	Conclusie met betrekking tot regelgeving	7
1.6	Noodzakelijke processen en structuren	7
1.7	Hulpmiddelen	11
2	Security Awareness	19
2.1	Het proces	19
2.2	De aanpak	21
2.3	De IB Toolbox Awareness	23
3	Identity en Access Management	25
3.1	Inleiding	25
3.2	I&AM begrippen en uitgangspunten	25
3.3	De Business Case van I&AM	28
3.4	Aanbevelingen bij I&AM	30
3.5	De stand van zaken van I&AM bij de deelnemende organisaties	31
4	Samenstelling CIG	33

1 Informatiebeveiliging in control

1.1 *Managementsamenvatting*

Er is (nog) geen algemeen aanvaarde norm voor het vaststellen van het “in control” zijn op het volledige spectrum van informatiebeveiliging. Analyse van praktijkervaringen en standaarden op deelgebieden laten echter al wel een zekere consensus zien over de onderwerpen waar in ieder geval aandacht moet worden besteed:

- Zorg ervoor dat de voor informatiebeveiliging relevante processen ingericht worden in de organisatie;
- Zie toe op de werking van deze processen door terugkoppeling van de key performance indicators;
- Zorg ervoor dat alle voor informatiebeveiliging relevante aspecten zijn genormeerd door het beveiligingsbeleid te baseren op de ISO 17799;
- Zorg ervoor dat specifieke eisen van de branche en omgeving waarin geopereerd worden hun weerslag hebben in een concretisering van de abstracte standaarden uit de ISO 17799 naar een bedrijfseigen beleid met concrete maatregelen per standaard;
- Zorg ervoor dat de verschillen in beveiligingseisen van bedrijfsprocessen via classificatie hun weerslag hebben in de maatregelen in applicaties en infrastructuur.

In de navolgende paragrafen wordt hier nader op ingegaan.

1.2 *Probleemstelling*

Veel bedrijven worden geconfronteerd met het vraagstuk om aan te tonen dat ze “in control” zijn. De informatiebeveiligers krijgen op hun beurt de vraag aan te tonen dat de organisatie “in control” is op het gebied van informatiebeveiliging. In dit document wordt, op basis van “best practices” uitgewerkt wanneer een organisatie “in control” is van de informatiebeveiliging¹.

Deze uitwerking heeft een meerledig doel:

- Het ondersteunen van de CIO bij het inrichten van de beveiligingsorganisatie en het toezien op de werking van deze organisatie;
- Het bieden van een marktconforme norm voor de inrichting van het informatiebeveiligingsproces ten behoeve van informatiebeveiligingsfunctionarissen;
- Het bieden van een de-facto marktstandaard als norm voor het toetsen van het “in control” zijn.

1.3 *Definitie “In control” voor Informatiebeveiliging*

Een organisatie is “in control” voor informatiebeveiliging als informatiebeveiliging aantoonbaar beheerst wordt tot op een niveau wat van een organisatie verwacht mag worden. Dit niveau wordt bepaald door de navolgende criteria:

- Eisen gesteld door de organisatie zelf (kan vertaling zijn van klanteisen);
- Risico's in de betreffende branche;
- De stand van de beveiliging (afweging (rest)risico versus acceptabele kosten);
- Eisen gesteld door wetgeving en regelgeving van toezichthouders.

1.4 *Waarom “in control”?*

Externe regelgeving is veelal de aanleiding om zich te buigen over het “in control” vraagstuk. De behoefte hiertoe zou echter zijn basis moeten vinden in de interne wens tot kwaliteitsbeheersing. Achtereenvolgens wordt op beide aspecten nader ingegaan.

¹ NB: “In Control” voor informatiebeveiliging is een onderdeel van het “In Control” vraagstuk dat betrekking heeft op beheersing van processen.

1.4.1 Eisen vanuit de eigen organisatie

Iedere organisatie kent interne regelgeving en procedures die een bepaald niveau van kwaliteit nastreven. De diepgang hiervan en de toetsing op de naleving is een management verantwoordelijkheid. De financiële audit is veelal een van de bestaande drijfveren om het kwaliteitsniveau van processen in kaart te brengen. Dit als gevolg van het feit dat de juistheid en volledigheid van financiële gegevens in moderne ICT gedreven organisaties niet aangetoond kan worden zonder te steunen op de kwaliteit van de gegevensverwerkende processen.

Verder zal de diepgang van regelgeving en procedures worden bepaald door de typologie van de organisatie. Binnen financiële instellingen zullen andere normen worden gehanteerd voor het "in control" zijn, dan binnen een handelsbedrijf of productiebedrijf. Ook binnen een typologie kunnen aanzienlijke verschillen bestaan.

De verantwoordelijkheid voor de betekenis van het "in control" zijn ligt in eerste instantie bij de leiding van de organisatie en werkt top down naar het management en de medewerkers. Algemene eisen zijn moeilijk te formuleren. De externe eisen komen vooral vanuit de financiële wereld en kennen een zekere algemeenheid dat procedures moeten zijn gedocumenteerd en de werking er van getoetst moet worden. Deze algemene eisen zien we nu ook terug gaan komen in niet financiële processen.

Ook in situaties waarbij delen van de (ICT) dienstverlening zijn uitbesteed blijven de in deze nota genoemde aspecten van kracht. De verantwoordelijkheid voor risicobeheersing kan immers niet uitbesteed worden. Wel kan het zo zijn dat de informatie die noodzakelijk is voor het aantonen van de beheersing (zoals Key Performance Indicators) afkomstig is van de outsourcingpartner.

1.4.2 Eisen gesteld door wetgeving en regelgeving van toezichthouders

Elke organisatie dient te beschikken over een proces dat relevante wet- en regelgeving vertaalt naar de organisatie. Bij wetgeving kan gedacht worden aan Wet Bescherming Persoonsgegevens (WBP) en Wet op de Computer Criminaliteit (WCC). Daarnaast zijn er diverse (fiscale) wetten die eisen opleggen voor bewaartermijnen van gegevens.

Drie belangrijke bronnen van regelgeving die de laatste jaren veel aandacht hebben gehad zijn de Sarbanes Oxley Act (SOX), de Regeling Organisatie en Beheersing (ROB) en Basel II. Het zijn regelingen die de lat qua 'in control' zijn voor bedrijven hoger hebben gelegd. Daarmee wordt ook de lat voor informatiebeveiliging verhoogd, of in ieder geval wordt dat zo gevoeld. Een substantieel deel van de bedrijven in Nederland geeft zelfs aan dat toenemende regelgeving de belangrijkste drijfveer is om meer aan Informatiebeveiliging te doen.

Naast bovengenoemde regelgeving is op 1 januari 2004 de Nederlandse corporate governance code in werking getreden. De aanbevelingen van deze gedragscode, ook wel bekend als de code Tabaksblat, spitsen zich toe op het functioneren van de leden van de raad van bestuur, de macht van commissarissen en de invloed van aandeelhouders. De code kent geen inhoudelijke uitwerking op het vlak van interne beheersing en control maar schrijft wel voor dat beursgenoteerde ondernemingen zich in hun jaarverslag uitspreken over de werking van het interne risicobeheersings- en controlesysteem. De behandeling van deze regelgeving in dit document is daarom beperkt tot het vermelden dat het een extra aanleiding kan zijn om aandacht te besteden aan aantoonbaarheid van risicobeheersing en daarmee ook informatiebeveiliging.

Sarbanes-Oxley Act

De Sarbanes-Oxley Act werd in 2002, direct na het grote financiële schandaal rondom Enron (boekhoudkundige fraude), aangenomen om frauduleuze praktijken binnen beursgenoteerde organisaties tegen te gaan. Alle in de V.S. aan de beurs genoteerde organisaties dienen te voldoen aan de Sarbanes-Oxley reglementen.

Handelspartners van de aan de SOX voldoende ondernemingen worden ook meegezogen in deze stroom: de informatieprocessen van handelspartners worden immers gekoppeld. Feitelijk stelt SOX daarmee haar eisen ook aan deze ondernemingen.

SOX is grotendeels gefocust op de accuraatheid van de financiële processen binnen organisaties en de controlemaatregelen hieromtrent. Het management moet 'in control' zijn, wat betekent dat processen beschreven dienen te zijn inclusief de beheersingsmaatregelen binnen de processen. Het management dient een structuur op te zetten om de werking van de beheersingsmaatregelen te beoordelen.

De financiële gegevens van organisaties moeten betrouwbaar (juist en volledig) zijn. Het genereren van deze gegevens moet nauwkeurig geschieden en een acceptabele industriestandaard weerspiegelen.

Om de betrouwbaarheid te waarborgen dient er nauwlettend gekeken te worden naar de kritische financiële systemen. Alle activiteiten rondom deze systemen dienen gelogd te worden, zodat rapportages gegenereerd kunnen worden. Op deze manier is de aantoonbaarheid van het 'in control' zijn gewaarborgd.

SOX stelt dan ook eisen op onderdelen van de informatiebeveiliging. Veelal worden die echter al gedekt door het vigerende informatiebeveiligingsbeleid, zeker als dat beleid gebaseerd is op een uitgebreide standaard zoals de ISO17799. Zaken die dan wellicht in het kader van SOX nog extra aandacht behoeven zijn de aantoonbaarheid (o.a. archivering) en de onafhankelijke waarborging.

ROB

De Regeling Organisatie en Beheersing, uitgegeven door De Nederlandsche Bank heeft tot doel richtlijnen en aanbevelingen te geven voor de organisatie en beheersing van bedrijfsprocessen bij financiële instellingen. Uitgangspunt hierbij is dat instellingen verantwoordelijk zijn voor een zodanige organisatie en beheersing van bedrijfsprocessen, dat daarmee wordt voorzien in een beheerste en integere bedrijfsvoering. Hoewel informatiebeveiliging betrekking heeft op de complete organisatie ligt het voor de hand om eerst te kijken naar wat de ROB zegt over het IT risico. Binnen de ROB wordt dat overigens gezien als een zelfstandig risico, terwijl het meestal (b.v. Basel II) deel uitmaakt van het operationeel risico. De ROB geeft daarbij vier artikelen (54 t/m 57) die voor het IT risico het meest van belang zijn.

Die vragen om:

- Helder geformuleerde beleidsuitgangspunten ter beheersing van IT risico's;
- Het op systematische wijze uitvoeren van analyse van IT risico's;
- Het zorgdragen voor de uitwerking en implementatie van de beleidsuitgangspunten ter beheersing van IT risico's in zichtbare organisatorische en administratieve procedures en maatregelen, welke geïntegreerd zijn in de IT processen en de dagelijkse werkzaamheden van alle relevante geledingen. Tevens wordt voorzien in een systematisch toezicht op de naleving daarvan;
- Het zorgdragen voor specifieke maatregelen die een afdoende beveiliging van de informatie en de continuïteit van de IT waarborgen.

Meer dan in SOX ligt de nadruk op IT risico's, risicoanalyses en het omgaan daarmee binnen processen. Maar daarnaast komen de eisen vanuit SOX ook terug. Voor een belangrijk deel lijken SOX en de ROB dan ook overlappend.

Basel II

Basel II is opgesteld door de centrale banken wereldwijd, onder toezicht van het Basel Committee on Banking Supervision (BCBS). Deze vernieuwde overeenkomst tussen banken, ingaande per 2007, heeft ten doel om een eensluidende visie te creëren met betrekking tot risicomanagement. Basel II is dus niet van toepassing op andere soorten bedrijven.

Het comité van Basel is opgericht in 1974. Mede door de internationalisering was destijds de concurrentie tussen bancaire instellingen verhevigd. In de jaren tachtig zette dit verder door en werd als gevolg van deze concurrentie steeds minder eigen vermogen in relatie tot de

verstrekke kredieten aangehouden. Deze verslechterende solvabiliteit leidde tot hoge risico's. Toezicht en afspraken waren noodzakelijk om de financiële markten te beschermen. Het eerste kapitaalakkoord van Basel van 1988 werd met dit doel opgesteld. Het in 1988 opgesteld kapitaalakkoord is in 2001 enigszins aangepast. Het is de bedoeling dat Basel II op 1-1-2007 geëffectueerd wordt. Voor banken die kiezen voor een meer geavanceerde benadering van dit soort risicomanagement geldt een latere invoeringsdatum (1-1-2008). De Basel regels worden in onze nationale wetgeving verankerd door opname in de WTK.

Eén van de gevolgen van het kapitaalakkoord van Basel zal zijn dat banken op een meer frequente basis de risico's van hun cliënten kwantificeren. Cliënten zullen hierdoor vaker worden verzocht om inzicht in de financiële situatie te verschaffen.

Basel II pakt drie soorten risico's aan, namelijk

- Kredietniveau: uitgeleend geld dat mogelijk niet terugvloeit;
- Marktniveau: koersveranderingen;
- Operationeel niveau: risico's met betrekking tot interne processen.

Deze verschillende risico's kennen meerdere benaderingen, welke in Basel II gedefinieerd zijn. Met betrekking tot informatiebeveiliging is het laatste risico interessant: operationeel niveau. Doel is om inzicht te geven in de financiële risico's die voortvloeien uit het operationeel risico en in welke mate er daarom een financiële reservering ter compensatie van dit risico noodzakelijk blijft.

Het Basel II akkoord geeft verder niet expliciet aan welke beveiligingsmaatregelen er getroffen dienen te worden. Wel vraagt bijvoorbeeld de eis naar risico statistiek om een zogenaamde Loss database. In deze Loss database worden schades en bijna schades vastgelegd. Naar aanleiding van deze statistiek kunnen dan maatregelen genomen worden.

Het implementeren van een goede beveiliging kan er voor zorgen dat een organisatie een lager operationeel risico kent. Dit leidt ertoe dat een minder hoog reserveringspercentage vrij gehouden dient te worden voor noodgevallen. Dit geldt valt vrij voor andere doelen.

Basel II legt informatiebeveiligers dus grote aandacht voor risico's op. Niets nieuws dus. Wel dient er meer gemeten te worden en dienen opgetreden (bijna) risico's onderzocht te worden en dient er aantoonbaar op gereageerd te worden.

Basel heeft enige overlap met de ROB. Alleen richt de ROB zich op meer soorten risico's dan Basel. En Basel werkt voor de drie soorten risico's die het bespreekt in meer detail uit hoe daarmee omgegaan dient te worden.

1.5 Conclusie met betrekking tot regelgeving

Hoewel iedere regeling zoals bovenstaand betoogt wel bepaalde nieuwe aspecten toevoegt is er zeker geen sprake van een revolutie voor bedrijven die al een beveiligingsbeleid gebaseerd op ISO 17799 nastreefden. Wel is het zo dat auditors meer handvatten hebben via de grotere aantoonbaarheid die gevraagd wordt. Omdat de drie regelingen beleid formuleren en geen maatregelen daaraan koppelen zie je dat, onder druk van auditors en de publiciteit, er sprake is van 'maatregelinfatie'. Wat vandaag voldoet, voldoet morgen al niet meer. De lat komt daarmee steeds hoger te liggen, terwijl daar feitelijk geen redenen voor zijn.

1.6 Noodzakelijke processen en structuren

In de navolgende paragrafen worden processen en structuren die noodzakelijk zijn om "in control" te zijn op het gebied van informatiebeveiliging op hoofdlijnen uitgewerkt. Bestaande beheermodellen en standaarden kunnen helpen bij het verder invullen (Classificatiemodel, ISO 17799 en ITIL) en aantoonbaar maken (CobiT, ISF) van de kwaliteit van deze processen.

Per onderwerp wordt tevens aangegeven welke key performance indicatoren gehanteerd kunnen worden om een adequate terugkoppeling te krijgen over de werking.

1.6.1 Beleid

Informatiebeveiliging

Beleid op het gebied van Informatie beveiliging kent vele gradaties. De organisatie dient te beschikken over een informatiebeveiligingsbeleid en -baseline die gebaseerd zijn op een algemeen geaccepteerde standaard zoals de ISO 17799. "Gebaseerd zijn" betekent dat alle in de ISO standaard genoemde relevante standaarden vertaald moeten worden in concrete normen (maatregelen) die noodzakelijk zijn gezien de branche en omgeving waarin het bedrijf opereert.

De mate van beveiliging is in eerste instantie een business aangelegenheid. Dit betekent dat de organisatie dient te beschikken over een methode om op eenduidige manier een beveiligingsnorm te specificeren. Classificatie is een hulpmiddel om ervoor te zorgen dat men, zonder details te kennen of beschrijven, een eenduidige keuze kan maken voor een pakket van beveiligingsmaatregelen.

Voor specifiek aandachtsgebieden of doelgroepen dient men te beschikken over detailbaselines. Deze hebben vaak een meer technische achtergrond en zijn een vertaling van de beveiligingsnorm in meer specifieke maatregelen. Denk bijvoorbeeld aan baselines voor besturingssystemen.

Mogelijke KPI's:

- Niveau van formele accordering en communicatie van informatiebeveiligingsbeleid.
- Actualiteit van het informatiebeveiligingsbeleid.
- Percentage van de platformen waarvoor een beveiligingsbaseline is opgesteld.
- Frequentie van de toetsing aan de beveiligingsbaseline.

Risicomanagement

De organisatie dient te beschikken over beleid ten aanzien van risico's;

- Wie is verantwoordelijk voor risico's;
- Welke risico's zijn in het algemeen acceptabel (risk appetite);
- Wie mogen risico's accepteren.

Mogelijke KPI's:

- Actualiteit risicobeleid;
- Risk appetite;
- Aantal FTE's op het gebied van risico management;
- Tijd die besteed wordt aan risico management per organisatie onderdeel.

1.6.2 Organisatie

Verantwoordelijkheden

Verantwoordelijkheden voor informatiebeveiliging moeten eenduidig belegd zijn:

- Business bepaalt hoogte beveiligingsniveau:
 - Classificatie van bedrijfsprocessen en informatiesystemen. Deze classificatie is gebaseerd op het belang van het bedrijfsproces en bepaalt de hoogte van het pakket van beveiligingsmaatregelen.
- De (ICT) organisatie realiseert het beveiligingsniveau:
 - Verankeren van informatiebeveiliging in bedrijfsprocessen;
 - Aantoonbaar maken van gerealiseerde classificatie in applicaties;
 - Aangeven van maximale classificatie van generieke ICT producten.
- Controlefunctie op verschillende 3 niveaus zijn belegd:
 - Zelfcontrole door uitvoerenden;
 - Interne kwaliteitscontrole binnen eenheden;
 - Rol van de interne- en externe toezichthouder.

De (eind)gebruiker is verantwoordelijk voor het waarborgen van de beveiliging van informatie in de omgang met informatie.

De mate waarin invulling gegeven wordt aan deze verantwoordelijkheden is sterk afhankelijk van het beveiligingsbewustzijn van deze partijen. Het is daarom veelal wenselijk om, toegespitst op deze verantwoordelijkheden, een beveiligingsbewustzijnsprogramma uit te werken.

Mogelijke KPI's:

- Percentage relevante functiebeschrijvingen waarin verantwoordelijkheden voor informatiebeveiliging zijn belegd;
- Dekkingsgraad (% medewerkers) van bewustzijnsprogramma.

Security Officer

De organisatieonderdelen dienen te beschikken over een eenduidig aanspreekpunt voor beveiliging. Security officers staan opgesteld om business en ICT te ondersteunen bij de invulling van hun verantwoordelijkheden en toe te zien op tijdige invulling van de verbeteringen.

- Informatie security officer rol dient belegd te zijn binnen de verschillende organisatieonderdelen. Binnen deze onderdelen kunnen ze het beste in een onafhankelijke (staf) positie opgehangen worden;
- Informatie security officers van organisatieonderdelen hebben gestructureerd overleg ten synergie te bereiken en adequaat in te kunnen spelen op onderdeeloverstijgende vraagstukken.

De mate van (de)centralisatie van deze rol of functie is sterk afhankelijk van de structuur van de organisatie. In het algemeen is het verstandig om deze functie op te hangen op een punt in de organisatie waar belangrijke besluitvormingstrajecten samen komen.

Mogelijke KPI's:

- Percentage organisatieonderdelen waarin informatiebeveiligingsrol is belegd;
- Frequentie waarmee (top) management zich bezig houdt met informatie beveiliging;
- Frequentie van overleg tussen informatiebeveiligingsfunctionarissen.

1.6.3 Proces

Beveiligingsplan

Elk organisatieonderdeel stelt periodiek (jaarlijks) een beveiligingsplan op met daarin een opsomming van de beveiligingsactiviteiten van het onderdeel die noodzakelijk zijn om te voldoen aan het informatiebeveiligingsbeleid. Dit plan vormt de basis voor de bewaking van de voortgang van de activiteiten.

Deze basis wordt gedurende het jaar aangevuld met:

- Verbeteracties die volgen uit incidenten;
- Verbeteracties die volgen uit audits;
- Verbeteracties die volgen uit anderszins gesignaleerde risico's.

Mogelijke KPI's:

- Percentage van bedrijfsonderdelen dat beveiligingsplan heeft opgesteld;
- Percentage van de geplande verbeteracties ten opzichte van gerealiseerde verbeteracties;
- Frequentie van de rapportage over de verbeteracties;
- Percentage van de bekende verbeteracties uit incidenten, audits etc., dat niet in het jaarplan is opgenomen.

Classificatie

De bedrijfsprocessen en systemen worden geclassificeerd volgens een standaard opgesteld classificatie systeem. Bij het classificeren worden zowel de intrinsieke waarde van de

informatie evenals het belang dat derden kunnen hebben bij het beïnvloeden of inzien van deze informatie, meegenomen.

Mogelijke KPI's:

- Percentage van bedrijfsprocessen dat is geclassificeerd;
- Percentage van de informatiesystemen dat is geclassificeerd;
- Percentage van de ICT-producten dat is geclassificeerd.

Risico analyse

De (ICT-)organisatie dient te beschikken over een methode voor het vertalen van een door de business bepaalde norm naar maatregelen.

Hiervoor zijn twee instrumenten geschikt:

- Baselinecontrole met maatregelen gegeven classificatie en/of businessseisen;
- Risicoanalyse methode voor bepalen maatregelen gegeven een classificatie en/of business vereisten.

De eerste methode is efficiënter maar niet altijd mogelijk omdat voor sommige situaties geen relevante baselines beschikbaar zijn.

Door in beveiligingsbaselines maatregelen te relateren aan de classificatie wordt in detail vastgelegd welke maatregelen getroffen moeten worden bij een bepaalde classificatie. Dit kan nog verder worden geconcretiseerd door de standaard ICT-producten (werkplek, netwerk, hardwareplatformen etc.) te voorzien van een classificatie. Deze classificatie geldt als norm voor de maatregelen in de betreffende ICT-producten en tevens als maximale classificatie van de applicaties die de betreffende ICT producten gebruiken. Applicaties met een hogere classificatie kunnen dus alleen op de betreffende infrastructuur gebruikt worden indien additionele (applicatieve) maatregelen de lacunes compenseren dan wel restrisico's geaccepteerd worden. Een voorbeeld voor een classificatieschema is opgenomen in het laatste hoofdstuk.

Mogelijke KPI's:

- Percentage van applicaties met maatregelset op basis van baseline of risicoanalyse;
- Percentage van ICT producten met maatregelset op basis van baseline of risicoanalyse.

Risico management

In uitvoering heeft de organisatie:

- Inzicht in de (inherente) risico's. Dit zijn de risico's die gelden gegeven de aard van de bedrijfsvoering en de omgeving;
- Inzicht in de restrisico's. Dit zijn de risico's die het gevolg zijn van het onvolledig afdekken van de inherente risico's;
- Geregeld dat de risicodragers zich bewust zijn van en akkoord gaan met deze restrisico's.

Mogelijke KPI's:

- Aantal restrisico's in periode in relatie tot aantal processen en producten;
- Percentage formeel geaccepteerde restrisico's;
- Verliezen (loss data) die buiten de grenzen van risico-inschatting vallen.

Afhandelen afwijkingen

De organisatie beschikt over een proces voor het afhandelen van afwijkingen op de beveiligingsbaseline(s) en accepteren van de risico's die daaruit volgen.

Bij dit proces worden de navolgende gegevens vastgelegd:

- Reden afwijking;
- Risico als gevolg van afwijking;
- Compenserende maatregelen;
- Restrisico;
- Initiator en/of opdrachtgever;

- “Drager van risico” = acceptant;
- Datum en looptijd van acceptatie.

Mogelijke KPI's:

- Aantal openstaande afwijkingen (niet geaccepteerd en/of opgelost);
- Doorlooptijd afwijkingen.

Afhandelen schades

De organisatie beschikt over een proces voor het administreren van schades en bijna schades op het gebied van informatiebeveiliging die vallen boven een vastgestelde grenswaarde. Dit betreft situaties waarbij er een (bijna) inbreuk is geweest op het gebied van beschikbaarheid, integriteit en vertrouwelijkheid.

Mogelijke KPI's:

- Opvolging en doorlooptijd van gedefinieerde acties naar aanleiding van bevindingen;
- Percentage van beveiligingsincidenten met business impact;
- Percentage schades dat niet binnen gestelde tijd is afgehandeld;
- Ouderdomsanalyse van openstaande schades;
- Bedrag van afgehandelde schades.

1.7 Hulpmiddelen

1.7.1 Code voor Informatiebeveiliging (ISO 17799/27000)

De Code voor Informatiebeveiliging is de Nederlandse versie van de British Standard 7799, die later als ISO 17799 als internationale standaard voor informatiebeveiliging in organisaties is gepubliceerd. Deze standaard is de meest universeel geaccepteerde standaard voor informatiebeveiliging in de wereld. Het stelsel van standaarden wordt de komende jaren herzien in de nieuwe ISO 27000 serie.

De Code bestaat feitelijk uit twee delen: een norm en een code of practice. De code of practice is een overzicht van maatregelen en geeft als zodanig een handreiking voor de implementatie van beveiligingsmaatregelen in een organisatie. Tegen de norm kan men door een geaccrediteerde instelling worden gecertificeerd. Deze certificatie richt zich vooral op het management van informatiebeveiliging.

De Code (17799) kent de volgende elf hoofdstukken:

1. Beveiligingsbeleid
2. Beveiligingsorganisatie
3. Classificatie van beheer en bedrijfsmiddelen
4. Beveiligingseisen ten aanzien van personeel
5. Fysieke beveiliging en beveiliging van de omgeving
6. Beheer van communicatie en bedieningsprocessen
7. Toegangsbeveiliging
8. Ontwikkeling en onderhoud van systemen
9. Incident management
10. Continuïteitsmanagement
11. Naleving

In vergelijking met de hierna beschreven standaarden geeft de Code een waslijst aan te implementeren beveiligingsmaatregelen. Hierdoor is de Code bij uitstek geschikt voor het opstellen van een inhoudelijk beveiligingsprogramma. De Code is van alle standaarden dan ook het meest gedetailleerd.

1.7.2 CobiT

CobiT staat voor Control Objectives for IT and Related Technology. Het is ontwikkeld als een breed en generiek geaccepteerde standaard voor IT Governance en beheersmaatregelen voor IT. CobiT is het eerst gepubliceerd in 1996 en onlangs is versie 4.0 verschenen.

CobiT bestaat uit een aantal 'Good Practices' op het gebied van IT Governance. Deze zijn binnen vier domeinen verdeeld over 34 IT processen die voor elke organisatie herkenbaar zijn. Binnen de IT processen staan beheersdoelstellingen en bijbehorende maatregelen, prestatie-indicatoren en volwassenheidsniveaus centraal. Informatiebeveiliging is geïntegreerd binnen de structuur en opzet van CobiT. Daarnaast is informatiebeveiliging een apart IT proces (DS5 – Ensure Systems Security) waarbij de hierboven beschreven onderdelen in detail zijn uitgewerkt. De volwassenheidsniveaus voor informatie beveiliging zijn opgenomen in deze bijlage.

CobiT 4 hanteert daarbij expliciet de volgende vijf doelstellingen van IT Governance:

Strategic Alignment	Zorgen dat IT functie de organisatiedoelstellingen optimaal ondersteunt door het op elkaar afstemmen van organisatie- en IT beleid als ook processen.
Value Delivery	Zorgen dat de feitelijke uitvoering van IT processen de beoogde organisatiedoelstellingen oplevert
Resource Mgmt	Zorgen dat er optimaal wordt geïnvesteerd in IT resources en dat het maximale uit de aanwezige resources wordt gehaald
Risk Management	Zorgen dat risico's onderkend, geëvalueerd, gemitigeerd en gemonitord worden teneinde ze tot aanvaardbare omvang terug te brengen.
Performance Mgmt	Zorgen dat de IT functie bijgestuurd kan worden in de mate waarin het slaagt de beoogde organisatiedoelstellingen te realiseren door het meten van IT prestaties.

Aan de verzameling CobiT documenten is een Security Baseline toegevoegd. Deze baseline bestaat uit 39 stappen - feitelijk een assessment tool - die een organisatie kan hanteren om informatiebeveiliging te plannen en te organiseren. De stappen zijn afgeleid, respectievelijk een selectie van de voor informatiebeveiliging relevante beheersdoelstellingen van CobiT.

CobiT is zoals gezegd een raamwerk van good practices. In tegenstelling tot het hierna beschreven ITIL geeft CobiT primair aan *wat* er moet gebeuren. ITIL is daarentegen meer gericht op *hoe* een IT proces dient te worden ingericht.

Een sterk punt van CobiT is de toetsing door indeling van processen in volwassenheidsniveaus. Dit biedt de mogelijkheid om via een van nature subjectieve (zelf) controle toch een relatief objectieve weergave te geven van de processen.

De door CobiT gehanteerde volwassenheidsniveaus zijn:

0 Non-existent when

The organisation does not recognise the need for IT security. Responsibilities and accountabilities are not assigned for ensuring security. Measures supporting the management of IT security are not implemented. There is no IT security reporting and no response process for IT security breaches. There is a complete lack of a recognisable system security administration process.

1 Initial/ Ad Hoc when

The organisation recognises the need for IT security. Awareness of the need for security depends primarily on the individual. IT security is addressed on a reactive basis. IT security is

not measured. Detected IT security breaches invoke finger-pointing responses, because responsibilities are unclear. Responses to IT security breaches are unpredictable.

2 Repeatable but Intuitive when

Responsibilities and accountabilities for IT security are assigned to an IT security co-ordinator, although the management authority of the co-ordinator is limited. Awareness of the need for security is fragmented and limited. Although security-relevant information is produced by systems, it is not analysed. Services from third parties may not address the specific security needs of the organisation. Security policies are being developed, but skills and tools are inadequate. IT security reporting is incomplete, misleading or not pertinent. Security training is available but is undertaken primarily at the initiative of the individual. IT security is seen primarily as the responsibility and domain of IT and the business does not see that IT security is within its domain.

3 Defined Process when

Security awareness exists and is promoted by management. IT security procedures are defined and aligned with IT security policy. Responsibilities for IT security are assigned and understood, but not consistently enforced. An IT security plan and security solutions exist as driven by risk analysis. Reporting on security does not contain a clear business focus. Ad hoc security testing (e.g., intrusion testing) is performed. Security training is available for IT and the business but is only informally scheduled and managed.

4 Managed and Measurable when

Responsibilities for IT security are clearly assigned, managed and enforced. IT security risk and impact analysis is consistently performed. Security policies and practices are completed with specific security baselines. Exposure to methods for promoting security awareness is mandatory. User identification, authentication and authorisation are standardised. Security certification is pursued for staff who are responsible for the audit and management of security. Security testing is done using standard and formalised processes leading to improvements of security levels. IT security processes are co-ordinated with an overall organisation security function. IT security reporting is linked to business objectives. IT security training is conducted in both the business and IT. IT security training is planned and managed in a manner that responds to business needs and defined security risk profiles. KGIs and KPI's for security management have been defined but are not yet measured.

5 Optimised when

IT security is a joint responsibility of business and IT management and is integrated with corporate security business objectives. IT security requirements are clearly defined, optimised and included in an approved security plan. Users and customers are increasingly accountable for defining security requirements, and security functions are integrated with applications at the design stage. Security incidents are promptly addressed with formalised incident response procedures supported by automated tools. Periodic security assessments are conducted to evaluate the effectiveness of implementation of the security plan. Information on threats and vulnerabilities is systematically collected and analysed. Adequate controls to mitigate risks are promptly communicated and implemented. Security testing, root cause analysis of security incidents and proactive identification of risk are used for continuous process improvements. Security processes and technologies are integrated organisationwide. KGIs and KPI's for security management are collected and communicated. Management uses KGIs and KPI's to adjust the security plan in a continuous improvement process.

1.7.3 ITIL

ITIL is een verzameling van best practices voor IT-beheer gebaseerd op een procesmatige aanpak. ITIL bestaat uit een serie processen die gezamenlijk beheer ondersteunen. Een van die processen, het ITIL proces Security Management, geeft de structurele inpassing van beveiliging in de beheerorganisatie en dus binnen ITIL. Het doel van ITIL Security Management is tweeledig:

1. Het realiseren van de beveiligingseisen in het Service Level Agreement (SLA, de afspraken met de klant) en andere externe vereisten in andere contracten, wetgeving en eventueel intern of extern opgelegd beleid. Vaak betekent dit dat informatiebeveiliging betrokken is bij de totstandkoming van het SLA om te bewaken dat gemaakte afspraken realistisch zijn. Te hoge eisen veroorzaken veel kosten, te lage eisen veroorzaken veel risico's. Vervolgens zal informatiebeveiliging de eisen uit het SLA operationaliseren en trachten te zorgen voor implementatie in de IT organisatie. En er zal naar de klant terug gerapporteerd dienen te worden over de realisatie van de gestelde eisen.
2. Het realiseren van een basisniveau aan beveiliging. Dit is nodig om de eigen continuïteit van de beheerorganisatie te waarborgen, maar ook om te komen tot vereenvoudiging van het Service Level Management voor informatiebeveiliging. Immers, het beheer van een groot aantal verschillende service levels is veel complexer dan een beperkt aantal. Te denken valt aan een 'aanbod' niveau. Je kunt qua beveiliging drie basis niveaus aan de klant aanbieden. Bijvoorbeeld 'Basis', voor applicaties die qua vertrouwelijkheid, beschikbaarheid en integriteit niet hoog scoren. En daarnaast 'hoog' en 'zeer hoog'. Waarbij 'zeer hoog' bijvoorbeeld betrekking kan hebben op de beveiliging van processen als betalingsverkeer.

ITIL security management heeft relaties naar veel andere ITIL processen.

De belangrijkste zijn:

1. Incident management: Incidenten kunnen beveiligingsincidenten zijn en dienen in dat geval geanalyseerd te worden. De oorzaak van het incident of de zwakte in de beveiliging die het incident mogelijk maakte dient structureel weggenomen te worden.
2. Change management: Changes vormen veranderingen op de productieomgeving. Deze veranderingen kunnen zwaktes in de beveiliging veroorzaken. Security management richt zich op het voorkomen van nieuwe zwaktes via deze weg. Overigens is de betrokkenheid van beveiliging bij changes vaak meer effectief als beveiliging zo vroeg mogelijk in het proces wordt aangehaakt.
3. Configuration management: Als niet bekend is welke infrastructurele componenten beheerd worden is het vaak ook niet goed mogelijk om na te gaan welke bedreigingen of kwetsbaarheden er bestaan.
4. Service level management: Het is belangrijk om beveiliging de juiste plaats te geven in het SLA met de klant en daarover te rapporteren.

Omdat ITIL gericht is op beheer zal het adviseren op het gebied van systeemontwikkeling en de projecten die zich daar op richten daar geen onderdeel van uitmaken, behalve via change management. Er zijn dan ook relaties vanuit beveiliging naar andere processen dan ITIL processen.

1.7.4 Classificatie

De bedrijfsprocessen dienen te beschikken over een methode om op eenduidige manier een beveiligingsnorm te specificeren. Classificatie is een hulpmiddel om ervoor te zorgen dat men, zonder details te kennen of beschrijven, een eenduidige keuze kan maken in voor een pakket van beveiligingsmaatregelen.

Bij het classificeren worden zowel de intrinsieke waarde van de informatie evenals het belang dat derden kunnen hebben bij het beïnvloeden of inzien van deze informatie, meegenomen.

Classificatie van bedrijfsprocessen en/of informatiesystemen

Het niveau van beveiliging dient in overeenstemming te zijn met de waarde en de (intrinsieke) risico's van het te beveiligen object en te voldoen aan de wettelijke voorschriften. Indien er meer beveiligingsmaatregelen zijn getroffen dan noodzakelijk is, leidt dit tot onnodig hoge kosten. Indien er minder maatregelen zijn getroffen dan noodzakelijk leidt dit tot onaanvaardbare risico's.

De businessafdelingen zijn, als eigenaar van de gegevens, verantwoordelijk voor het bepalen van het niveau van de beveiliging. Zij beschikken echter in veel gevallen niet over inhoudelijke kennis van beveiligingsmaatregelen.

Het classificeren van informatie is een instrument om businessafdelingen eenduidig het niveau van de beveiliging te laten specificeren zonder dat ze over inhoudelijke kennis van de beveiligingsmaatregelen hoeven te beschikken.

Hierbij zijn er twee methoden die gevolgd kunnen worden:

- Bedrijfsprocessen te classificeren en de systeemclassificatie als een afgeleide van de procesclassificatie te zien;
- Direct de systemen te classificeren op basis van de aard van de informatie die ze verwerken.

Aangezien beide methoden leiden tot geclassificeerde informatie is er geen voorkeur voor een van deze methoden. Bij bedrijven die kiezen voor procesclassificatie ziet men, onder invloed van bedrijfsprocesoverschrijdende informatiesystemen, steeds vaker dat sommige gegevens apart geclassificeerd worden.

De classificatie van applicaties is in beide gevallen afgeleid van de gegevens die door de applicatie verwerkt worden.

Classificatie van ICT producten

Door in beveiligingsbaselines maatregelen te relateren aan de classificatie wordt in detail vastgelegd welke maatregelen getroffen moeten worden bij een bepaalde classificatie. Dit kan nog verder worden geconcretiseerd door de standaard ICT-producten (werkplek, netwerk, hardwareplatformen etc.) te voorzien van een classificatie. Deze classificatie geldt als norm voor de maatregelen in de betreffende ICT-producten en tevens als maximale classificatie van de applicaties die de betreffende ICT-producten gebruiken. Applicaties met een hogere classificatie kunnen dus alleen op de betreffende infrastructuur gebruikt worden indien additionele (applicatieve) maatregelen de lacunes compenseren dan wel restrisico's geaccepteerd worden. Een voorbeeld voor een classificatieschema is opgenomen in het laatste hoofdstuk.

Op een lager niveau kunnen (ICT) processen gegevensstromen faciliteren die indirect een gevolg zijn van een commercieel product of dienst. In dat geval wordt de BIV-code voorgeschreven door de kwaliteitseisen die aan de verwerking worden gesteld. Deze zijn vastgelegd in bijvoorbeeld Service Level Agreements.

Dit suggereert dat maatregelen getroffen worden als "maatwerk" voor een specifieke klant of applicatie. In de praktijk worden infrastructurele componenten veelal geleverd als standaardproduct. In dat geval is het verstandig om deze standaard-producten ook te voorzien van een classificatie volgens het zelfde classificatiemodel

Deze classificatie geldt als norm voor de maatregelen in de betreffende standaard ICT-producten en is tevens als maximale classificatie van de applicaties die de betreffende ICT-producten gebruiken. Applicaties met een hogere classificatie kunnen dus alleen op de betreffende infrastructuur gebruikt worden indien additionele (applicatieve) maatregelen de lacunes compenseren dan wel restrisico's geaccepteerd worden.

Door in beveiligingsbaselines maatregelen te relateren aan de classificatie wordt in detail vastgelegd welke maatregelen getroffen moeten worden bij een bepaalde classificatie. Beheerders van de standaardproducten kunnen zo eenvoudig aflezen welke maatregelen getroffen moeten worden in hun producten.

Classificatiemodel

Bij classificatie wordt veelal de norm voor de aspecten Beschikbaarheid, Integriteit en Vertrouwelijkheid apart geclassificeerd. De classificatie wordt daarom wel aangeduid met de BIV-code (in het Engels veelal CIA of AIC).

Het is daarom van belang dat het vereiste beveiligingsniveau (norm) eenduidig gespecificeerd wordt.

Dit geschiedt veelal door middel van een classificatie naar drie kwaliteitsaspecten:

- beschikbaarheid;
- integriteit;
- vertrouwelijkheid.

Deze begrippen worden hierbij in ruime zin uitgelegd. Integriteit omvat daarom de aspecten "juistheid", "tijdigheid", "volledigheid", "geoorloofdheid" en "onloochenbaarheid". Controleerbaarheid is een afgeleid aspect van alle drie in de classificatie opgenomen kwaliteitsaspecten.

De classificatie wordt uitgedrukt in de zogenaamde BIV-code, een code van drie cijfers. Het eerste cijfer geeft de norm voor beschikbaarheid, het tweede voor integriteit en het derde voor vertrouwelijkheid. Elk van de kwaliteitsaspecten kent meerdere niveaus.

Een voorbeeld voor een indeling in niveaus is:

Beschikbaarheid

- 3 - Bij incidenten (kleine verstoringen) is onbeschikbaarheid van informatie tot maximaal 2 uur toelaatbaar. Bij ernstige calamiteiten uitval tot maximaal 1dag. (Apparatuur is dubbel uitgevoerd op meerdere locaties. In geval van storingen of calamiteiten wordt automatisch overgeschakeld op redundante apparatuur.)
- 2 - Bij incidenten (kleine verstoringen) is onbeschikbaarheid van informatie tot maximaal 8 uur toelaatbaar. Bij ernstige calamiteiten is uitval tot enkele dagen toelaatbaar. (Gegevens worden veiliggesteld op meerdere locaties. In geval van calamiteiten kan binnen enkele dagen worden beschikt over vervangende apparatuur.)
- 1 - Bij incidenten (kleine verstoringen) is onbeschikbaarheid van >24 uur tot enkele dagen toelaatbaar. Bij een ernstige calamiteit is uitval tot enkele weken acceptabel. (Gegevens worden veiliggesteld op meerdere locaties.)

Integriteit

- 3 - Indien de informatie onjuist, onvolledig of niet tijdig is, loopt de organisatie zeer grote schade. Voorbeelden zijn (onherroepbare) financiële transacties en publieke website.
- 2 - Indien de informatie onjuist, onvolledig of niet tijdig is, loopt de organisatie grote schade. Klantinformatie, financiële transacties die zonder (imago) schade teruggedraaid kunnen worden.
- 1 - Onjuiste, onvolledige of niet tijdige informatie leidt tot geringe schade.

Vertrouwelijkheid

- 3 - Geheime informatie. Informatie die, indien deze openbaar wordt, de organisatie ernstige schade kan berokkenen. Informatie die alleen toegankelijk mag zijn voor een zeer kleine groep mensen zoals medische informatie, geheime sleutels, pincodes en wachtwoorden.

- 2 - Vertrouwelijke informatie. Informatie die, indien deze openbaar wordt, de organisatie direct of indirect schade kan berokkenen. Informatie die alleen toegankelijk mag zijn voor een beperkte groep zoals klantinformatie en transactie informatie.
- 1 - Interne informatie. Informatie beschikbaar voor alle medewerkers van de organisatie. Bekend worden van deze informatie buiten organisatie leidt tot geringe schade. Informatie die niet in een van deze klassen van vertrouwelijkheid valt is informatie die vrij beschikbaar is. Uit praktische overwegingen wordt deze informatie soms aangeduid met V=0.

Ter illustratie wat voorbeelden van mogelijke classificaties op basis van dit model:

- Betalingsverkeer proces van bank = 332;
- Procesbewaking chemische industrie = 321;
- Telebankierensysteem = 332;
- Klantinformatiesysteem = 322;
- Publieke website = 320;
- Elektronisch patiëntendossier = 223;
- Intern WAN netwerk = 322;
- Interne mail = 222;
- Internet mail = 111;
- Hardware platform = 222 of 322 (afhankelijk van optie hoge beschikbaarheid).

1.7.5 Toetsingsinstrumenten

Er zijn diverse tools beschikbaar, al dan niet in combinatie met af te nemen consultancy diensten, om toetsingen uit te voeren van de status van informatiebeveiliging. De focus van de tools varieert van processen inclusief de risicobeperkende control selectie (BiZZdesign RiskManager®) tot aan de accountancy benadering specifiek voor de Nederlandse markt (Tabaksblat, Basel II en SOx) in het Global Risk Management Tool (GRMT) van Deloitte gericht op aantoonbaarheid en audit.

Navolgend wordt nader ingegaan op een algemeen beschikbare varianten (ISF) die gratis is voor organisaties die lid zijn van het ISF en een bedrijfseigen methode "Assessment Informatiebeveiliging".

ISF hulpmiddelen en ISF Health Check.

Het ISF heeft meerdere werkgroepen en projecten lopen en maakt wereldwijd gebruik van vertegenwoordigingen uit velerlei businesssectoren en regio's. Partijen die buiten details en afwijkingen door lokale wetgeving of specifieke business allen met hetzelfde probleem worstelen. "*Hoe beveilig ik optimaal (effectief / efficiënt) en hoe zorg ik dat de beveiliging als proces geborgd en aantoonbaar is.*" Ofwel hoe zorg ik dat ik als organisatie aantoonbaar "in control" ben.

Het ISF heeft momenteel activiteiten lopen op twee relevante gebieden:

- Aanpak, beschrijving en optimalisatie van de risicoanalyse en control selectie: Information Risk Assessment Method (IRAM);
- Programma Metastandaard:
Het inventariseren en verzamelen van "controls" afkomstig uit wetten, normen en standaarden per line of business en regio (wereldwijd) om deze in een grote database te zetten. Vervolgens kan, via één dynamische vragenlijst, een toetsing uitgevoerd worden naar al deze normen. Semi-automatische rapportage op het gewenste aandachtsgebied of standaard is vervolgens mogelijk.

ISF Security Health Check (SHC)

Op dit moment is in samenhang met beide trajecten IRAM en Metastandaard al gebruik te maken van een Excel sheet die de gebruiker in staat stelt om via de Security Health Check (SHC) te laten rapporteren over de status tegen meerdere normen en standaarden. Zo is nu al rapportage van de status van inrichting tegen de ISO17799:2000, de ISO17799:2005, CobiT 3, FIRM en GAISP mogelijk.

Informatiebeveiliging in control

In de SHC zijn ter beoordeling ook bladen met alle mogelijk cross references opgenomen. Na invulling van de huidige versie van de Security Health Check zijn de resultaten ervan tweeledig toepasbaar:

- Als rapportage in het kader van het "in control" statement voor de beschikbare normen en standaarden;
- Als input voor de IRAM waarbij de health check iets zegt over mogelijke kwetsbaarheden als gevolg van al dan niet op orde zijnde controls.

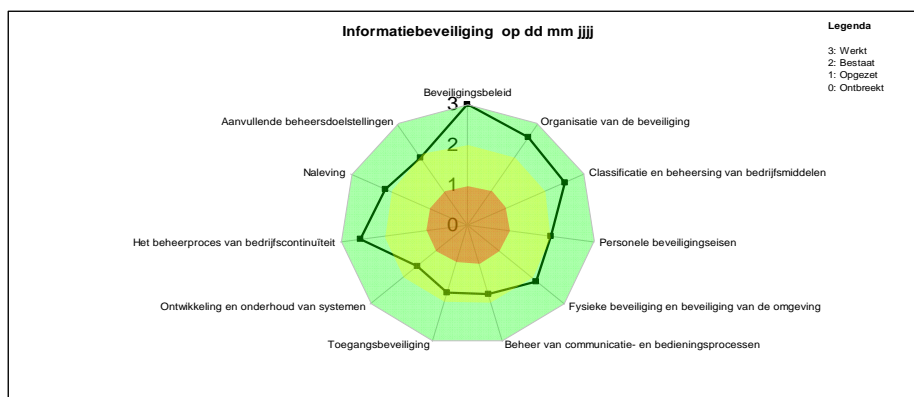
1.7.6 Assessment Informatiebeveiliging

Het doel van het Assessment Informatiebeveiliging is het beoordelen van de opzet, bestaan en werking van de aanwezige beheersmaatregelen conform de beheersdoelstellingen in het Beleid Informatiebeveiliging. Dit beleid is gebaseerd op de Nederlandse norm NEN-ISO IEC 17799, de Code voor Informatiebeveiliging en bestaat uit 125 beheersdoelstellingen. Op het moment dat alle doelstellingen aantoonbaar werken is 'In Control zijn' volledig behaald.

Voor het assessment is een sjabloon opgesteld waarbij elke unit op een eigen blad bij van toepassing zijnde doelstellingen die maatregelen vermeldt die zij zelf genomen heeft of gaat nemen. De ICT unit beoordeelt vrijwel alle 125 doelstellingen, voor overige units betreft het vaak minder doelstellingen, gemiddeld 77.

Per hoofdstuk uit het Beleid Informatiebeveiliging wordt op het voorblad per unit en totaal de gemiddelde score op de beoordeelde beheersdoelstellingen weergegeven. De score 0 betekent 'ontbreekt', 1 is 'opgezet', 2 is 'bestaat' en 3 staat voor 'werkt'. Bij opgezet kan vaak verwezen worden naar een instructie of een beleidsdocument, bij bestaan naar voorbeelden waaruit blijkt dat er volgens de instructie of het beleid wordt gewerkt en bij werking kan verwezen worden naar een controlerapport waaruit blijkt dat het bestaan structureel is. Waar de doelstellingen nog niet opgezet zijn, bestaan of werken, kan de planning in de kolommen 'wat', 'wie' en 'wanneer' aangegeven worden.

Op basis van deze planning wordt elk jaar een informatiebeveiligingsplan gemaakt. Elke unit vult ook een inventarisatie van bedrijfsprocessen in met daarop uitgevoerde risicoclassificaties, bedreigingen- en kwetsbaarheden analyses en daarbij behorende te nemen maatregelen als onderbouwing voor aanvulling op het basisbeveiligingsniveau.



Beheersdoelstellingen	Unit1	Unit2	Unit3	Unit4	Unit5	Bedrijf
% Gerapporteerd / Totaal (125)	100%	59%	50%	42%	22%	
% Gerapporteerd / Unitspecifiek (77)	100%	96%	81%	69%	35%	
Code Omschrijving						
3 Beveiligingsbeleid	3,0	3,0	3,0	3,0	3,0	3,0
4 Organisatie van de beveiliging	2,6	2,3	3,0	2,7	2,5	2,6
5 Classificatie en beheersing van bedrijfsmiddelen	2,3	2,3	3,0	2,7	0,0	2,5
6 Personele beveiligingseisen	2,6	1,0	1,7	1,8	2,7	2,0
7 Fysieke beveiliging en beveiliging van de omgeving	1,6	3,0	2,8	2,5	2,3	2,1
8 Beheer van communicatie- en bedieningsprocessen	1,9	1,1	2,3	1,6	2,3	1,8
9 Toegangsbeveiliging	1,9	1,1	2,0	1,9	1,0	1,7
10 Ontwikkeling en onderhoud van systemen	1,5	1,1	2,1	1,9	3,0	1,5
11 Het beheerproces van bedrijfscontinuïteit	2,6	2,2	2,6	2,2	3,0	2,5
12 Naleving	2,3	1,7	2,1	3,0	0,0	2,1
13 Aanvullende beheersdoelstellingen	2,0	3,0	2,0	2,0	3,0	2,0

2 Security Awareness

Het implementeren van het bewustwordingsproces rond informatiebeveiliging

2.1 Het proces

2.1.1 Wat is Awareness

Awareness zegt iets over het bewust zijn van risico's die er bestaan op het gebied van informatiebeveiliging. Bepaalde risico's kunnen worden beperkt met technische maatregelen. Maar veel risico's liggen in het handelen als onderdeel van menselijk gedrag.

De werkgroep Awareness binnen de CIO Interest Group Informatiebeveiliging heeft zich met name gericht op het aspect van menselijk gedrag. Hoe maak je medewerkers duidelijk, dat hun eigen gedrag voor een groot deel bepalend is voor de mate waarin risico's worden gelopen op het gebied van informatiebeveiliging.

De one-liner die wordt gehanteerd is daarom:

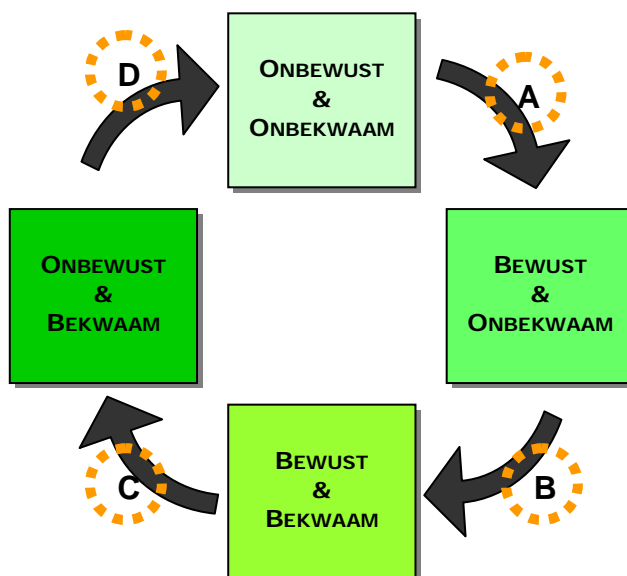
Wees bewust van jouw aandeel in informatiebeveiliging!

2.1.2 Doel van de werkgroep Awareness

De werkgroep heeft zich ten doel gesteld om een proces te beschrijven waarmee de bewustwording rond informatiebeveiliging bij medewerkers kan worden vergroot en tevens een gereedschapskist – de IB toolbox Awareness - samen te stellen, waarin voorbeelden zijn te vinden van hulpmiddelen ter ondersteuning van dit proces.

2.1.3 Leermodel van Maslow

Abraham Maslow onderscheidt in zijn leertheorie vier stadia die bij elk leerproces worden doorlopen om gedragsverandering te bereiken. Dit model is eveneens toepasbaar voor het creëren van bewustzijn en het afleren van onwenselijk gedrag op het gebied van informatiebeveiliging en zal als kapstok fungeren voor het communicatietraject.



Fase 1: onbewust onbekwaam

In het eerste stadium is men zich niet bewust dat men bepaalde vaardigheden mist of zelfs verkeerd gedrag vertoont.

Om gedragsverandering te bereiken is het noodzakelijk dat men zich bewust wordt dat het oude gedragspatroon niet (meer) voldoet én dat men overtuigd wordt van het nut van het gewenste gedrag.

A. Confronteren & motiveren

- Om medewerkers bewust te krijgen, is het belangrijk om ze te confronteren met de consequenties van hun gedrag.
- Om medewerkers gemotiveerd te krijgen, is het belangrijk om achtergrondinformatie bij het gewenste gedrag te geven. Het 'wat' en 'waarom'.

Fase 2: bewust onbekwaam

In deze fase treedt bewustwording op. Men mist nog steeds de gewenste vaardigheden maar weet het nu van zichzelf. Pas wanneer men openstaat voor nieuw gedrag kan begonnen worden met het aanleren van dit gedrag.

B. Instrueren

- Kenniscomponent: Het aanleren van de regels, procedures en processen rondom het gedrag.
- Vaardigheidscomponent: Het in praktijk brengen van het nieuwe gedrag.

Fase 3: bewust bekwaam

In deze fase is men bekend met het nieuwe gedrag, kent de waarde ervan en is in staat om het gedrag te vertonen, als men zich daarop concentreert. Het gedrag dient nu geautomatiseerd te worden.

Om nieuw gedrag eigen te maken is het belangrijk dat men herhaaldelijk geprikkeld wordt om dit gedrag te (blijven) vertonen en dat reflectie plaatsvindt op voortgang en resultaten.

C. Continuëren

- Afleren van ongewenst/verkeerd gedrag door herhaling van de boodschap.
- Uitwisseling van ervaringen/klankbord
- Reflectie op eigen voortgang en resultaten

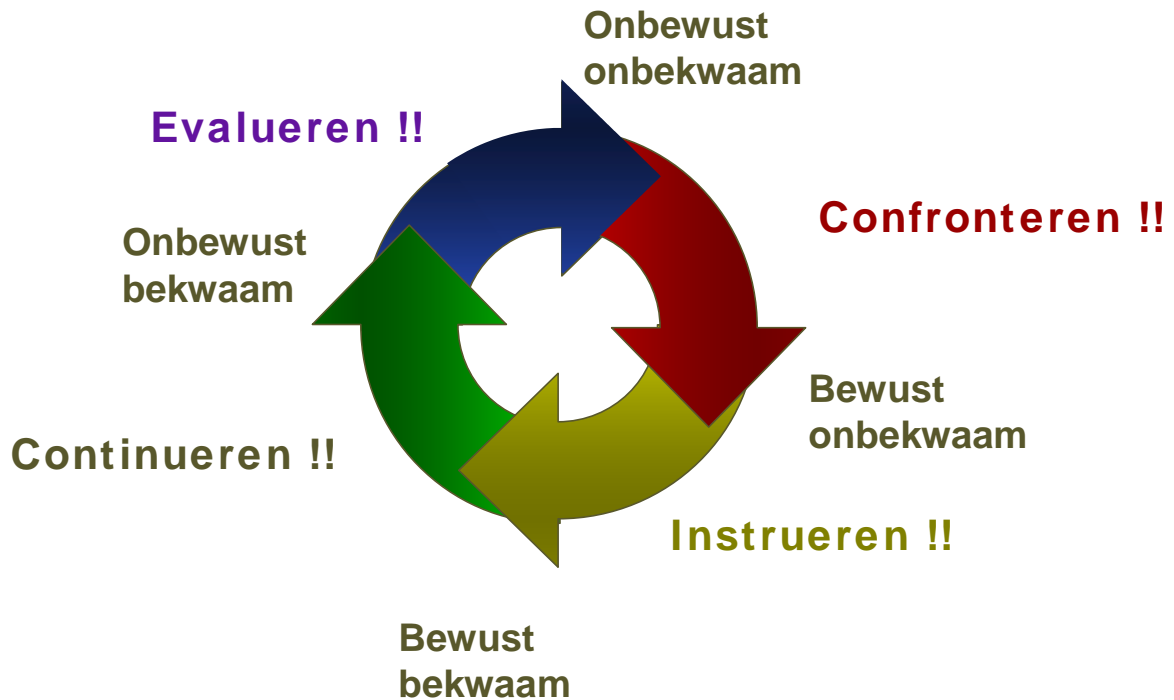
Fase 4: onbewust bekwaam

Men is onbewust bekwaam als het gewenste gedrag onderdeel is geworden van de persoon. Het nieuwe gedrag is ingesleten en geautomatiseerd. De opgedane kennis en vaardigheden kunnen vervolgens als basis dienen voor verdere ontwikkeling van de informatiebeveiliging.

D. Evalueren

- Meten van de resultaten
- Vaststellen (nieuwe) verbeterpunten

De figuur op de volgende pagina geeft de cyclus nog eens weer.



2.2 De aanpak

De aanpak van de bewustwordingscampagne bestaat uit een aantal stappen. De eerste stap is het vaststellen van het onderwerp of de onderwerpen die centraal worden gesteld. Het advies is, om hier het aantal onderwerpen beperkt te houden. Eén tot drie onderwerpen is prima.

Stap twee is het vaststellen van de afzonderlijke activiteiten in elke fase van bewustwording. In de navolgende paragrafen worden voorbeeld uitwerkingen beschreven.

Stap drie is het daadwerkelijk uitvoeren van deze activiteiten tot en met de evaluatie. Vervolgens kunnen voor nieuwe onderwerpen de hiervoor genoemde stappen worden herhaald.

2.2.1 Confronteren

In de fase van confronteren worden de medewerkers letterlijk geconfronteerd met het onbekwame gedrag, dat zij zelf vertonen. Dit confronteren kan op verschillende manieren:

Film

Met een film kan onbekwaam gedrag worden getoond. Daarbij kan gekozen worden voor de komische variant, de variant van de verborgen camera, de serieuze variant etc.

Foto's

Met foto's kunnen ongewenste situaties helder in beeld worden gebracht. Vaak wordt het middel van foto gebruikt om fysieke situaties in het eigen bedrijf inzichtelijk te maken.

Workshops

De workshop gaat door de dialoog in op onbekwaam gedrag. De workshop is uitermate geschikt om de betrokkenheid van leidinggevenden te etaleren.

Publicaties

Publicaties in nieuwsmedia van herkenbare, maar ook vergelijkbare situaties als in het eigen bedrijf helpen de discussie aan te wakkeren over onbekwaam gedrag.

2.2.2 Instrueren

In de fase van instrueren draait alles om het verbeteren van onbekwaam gedrag. Daarbij is voorbeeldgedrag van onschatbare waarde. Commitment vanuit de top is noodzakelijk. Het instrueren kan op navolgende wijzen plaatsvinden:

Zeepkist sessies

Hier wordt de letterlijke betekenis bedoeld. Het vanaf de zeepkist verkondigen van de noodzaak om het gedrag aan te passen, ondersteunt met de nodige powerpoint presentaties. Maar hier kan ook creatief gebruik worden gemaakt van andere communicatiemiddelen, zoals de bedrijfsfilm.

Folders en nieuwsbrieven

Met de gedrukte media kan meer in detail, maar ook meer blijvend van aard, de noodzaak van de gewenste gedragsverandering worden onderbouwd.

Gouden regels

Als start, maar ook als reminder, is het plezierig de medewerkers te kunnen voorzien van de 10 gouden regels in het bedrijf. Beknopt, maar veelzeggend.

Gedragsregels

De gedragsregels beschrijven in detail en meer in juridische zin de regels waaraan medewerkers zich dienen te houden op het gebied van informatiebeveiliging.

De naleving

Om daadwerkelijk te kunnen vaststellen of gewenst gedrag ook wordt toegepast, is controle op naleving nodig. Daarbij is in de instructiefase de aanmoediging en bemoediging belangrijker dan de sanctie. Daarom kan van het naleven van gewenst gedrag een spel worden gemaakt, waarbij de best scorende medewerkers worden beloond.

Ondersteunend materiaal

Bij alle activiteiten in de fase van instrueren kan ondersteunend materiaal worden gebruikt in de vorm van posters, cartoons, bedrukte bekertjes, screensavers, leaflets, gadgets, etc.

2.2.3 Continueren

In de fase van continueren moet het veranderde gedrag dat in de vorige fase is bereikt, worden vastgehouden. Daarom moeten de activiteiten in deze fase zich richten op het actueel houden van het/de gekozen onderwerp(en).

Bereikte resultaten

Betrek de medewerkers bij het vaststellen van de bereikte resultaten door openheid te geven over de bereikte mate van naleving. Maak er een competitie van tussen organisatie onderdelen van het bedrijf bijvoorbeeld.

Risico's en sancties

Maak de medewerkers duidelijk dat het ernst is met de gewenste verbeteringen en spreek af welke risico's moeten worden beperkt en welke sancties worden gekoppeld aan het niet aanpassen van onbekwaam gedrag.

Maatregelen en acties

Stel vast op welke onderdelen van de campagne extra energie moet worden gezet en op welke manier acties worden ondernomen. Dit is dan een kort cyclisch programma.

Opfrisprogramma

Zorg dat voor het/de onderwerp(en) van de lopende campagne opfrisprogramma's worden gestart, zodat het actueel blijft onder de medewerkers. Hierbij kan gedacht worden aan E-learning programma's, nieuwsbrieven, nieuwe posters en screensavers etc.

2.2.4 Evalueren

In de fase van evalueren wordt vastgesteld wat is bereikt en welke vervolgacties nodig zijn.

Met en is weten

Door vooraf vast te stellen welke doelen men wil bereiken, kunnen ook op dat moment vragenlijsten worden gedefinieerd die inzicht geven in de mate van realisatie van deze doelen. Deze vragenlijsten moeten worden uitgezet en beantwoord.

Risico en impact analyse

De mate van realisatie van de gewenste doelen geeft ook zicht op de openstaande risico's. Risico's zullen moeten worden beoordeeld op hun impact voor de organisatie.

Vaststellen verbeterpunten

Uit de voorgaande twee acties kunnen de verbeterpunten worden vastgesteld. Deze verbeterpunten moeten in een volgende cyclus meegenomen worden.

Nieuwe onderwerpen en aandachtspunten

Naast de mogelijke verbeterpunten worden de nieuwe onderwerpen vastgesteld waarmee de cyclus opnieuw wordt doorlopen.

2.3 De IB Toolbox Awareness

2.3.1 Beschikbaarheid

De IB Toolbox Awareness is beschikbaar op een CD-ROM voor de deelnemers van de CIG Informatiebeveiliging van het CIO Platform Nederland.































2.3.2 Inhoud

De IB Toolbox Awareness bevat voorbeelden van in te zetten middelen ter ondersteuning van het bewustwordingsproces rond informatiebeveiliging. Elke organisatie vereist zijn eigen aanpak. Daarom is het niet mogelijk een complete gebruiksklare Toolbox te leveren. Deze Toolbox geeft wel de handvatten om een bedrijfsspecifieke Toolbox samen te stellen.

2.3.3 Eigendom

De inhoud van de Toolbox is geleverd door de deelnemers aan de CIG Informatiebeveiliging van het CIO Platform Nederland. Het materiaal is en blijft eigendom van de hierin vertegenwoordigde bedrijven. Wel is ingestemd met het ter inzage verstrekken van deze materialen aan de andere deelnemers van de CIG. Maakt u daarom op gepaste wijze gebruik van de inhoud van de Toolbox. (zie inhoudsopgave volgende pagina)

2.3.4 Inhoudsopgave IB Toolbox Awareness

- [-]  IB Toolbox Awareness
 - [-]  01 Confronteren
 -  01 Films
 -  02 Fotos
 -  03 Workshops
 -  04 Publicaties
 - [-]  05 ondersteunend materiaal
 -   Sprookje continuïteit-umcg
 - [-]  02 Instrueren
 -  01 Zeepkist sessies
 -  02 Folders en nieuwsbrieven
 -  03 Gouden regels
 -  04 Gedragsregels
 - [-]  05 Rode en Groene kaarten
 -  PGGM-versturen e-cards naar collega's
 -  Schiphol-Group
 - [-]  06 Ondersteunend materiaal
 -  Cartoons
 -  PGGM-Posters door medewerkers
 -  Posters
 - [-]  03 Continueren
 -  01 Resultaten van acties tonen
 -  02 Risicos en sancties
 -  03 Maatregelen en acties
 -  04 Opfrisprogramma
 - [-]  04 Evalueren
 -  01 Meten is weten
 -  02 Risico en impactanalyse
 -  03 Vaststellen verbeterpunten
 -  04 Nieuwe speerpunten programma

3 Identity en Access Management

3.1 Inleiding

Hoewel Informatiebeveiliging in de meeste organisaties als een belangrijk onderwerp wordt gezien, wil dat nog niet zeggen dat informatiebeveiliging daar overal ook in orde is. Corporate Information Officers (CIO's) trachten te komen tot een juist afdoende set van maatregelen, omdat zij steeds weer dienen te beargumenteren dat nieuwe investeringen noodzakelijk zijn om de beveiliging op een acceptabel niveau te krijgen. Volgens leveranciers daarentegen kan men nauwelijks ver genoeg gaan met het nemen van allerlei maatregelen op dit gebied. Om beter vast te stellen wat onder 'acceptabel' moet worden verstaan, hebben de CIO's en hun Corporate Information Security Officers (CISO's) van een aantal grote bedrijven en instellingen zich verenigd in de Werkgroep Informatiebeveiliging van het CIO-Platform Nederland. Ze beogen daarmee ervaringen uit te wisselen, te benchmarken en de state-of-the-art vast te stellen.

Dit hoofdstuk is geschreven door de binnen de Werkgroep opgerichte Subgroep Identity & Access Management (I&AM). Deze subgroep had de opdracht uit eigen ervaringen en uit een onder de overige leden van de Werkgroep te houden enquête de actuele stand van zaken van toegangsbeveiliging als onderdeel van informatiebeveiliging vast te stellen.

Ingevulde enquêtes zijn ontvangen van John Akkermans (Essent), René Backer (SVB), Jaap de Bie (NS), Hendrikus Beck (VGZ-IZA-Trias), Rob Bloemer (Telegraaf), Ron van den Bosch (UMCG), Luc Colaris (Océ), René Colsen (BAM), Frank van Delden (Schiphol), Cees Free (Fortis), Simon Greve (Reaal), Hans de Korte (Vopak), George Labrujere (Cordares), Bert de Man (Min. van Def.), Rob van Otterdijk (PGGM), Paul Samwel (Rabobank) en Reinier Versluis (Ahold),

3.1.1 Doel van dit hoofdstuk

Dit hoofdstuk zet uiteen wat Identification & Access Management (I&AM) is, voor wie het is en welk doel men er mee kan bereiken. Bovendien wordt de huidige stand van zaken bij de in het Platform verenigde bedrijven en instellingen in kaart gebracht. Aan de hand deze notitie kunnen de CIO's van het Platform vaststellen of en in welke mate hun Informatiebeveiliging vergelijkbaar is met collega-bedrijven en -instellingen, dan wel moet worden aangepast.

3.1.2 Opbouw van dit hoofdstuk

Dit hoofdstuk over I&AM is als volgt opgebouwd:

Paragraaf 4.1 bevat een inleiding en beschrijft het doel, de opbouw en de context van dit document.

Paragraaf 4.2 definieert en verklaart I&AM, beschrijft de bouwstenen waaruit het bestaat en de uitgangspunten bij het goed organiseren ervan.

Paragraaf 4.3 besteedt veel aandacht aan de rechtvaardiging, de business case, van I&AM.

Paragraaf 4.4 geeft richtlijnen en aanbevelingen over hoe met I&AM om te gaan en het concept in uw organisatie te implementeren.

Paragraaf 4.5 tenslotte geeft een inventarisatie van de stand van zaken rond I&AM van de aan het platform deelnemende bedrijven.

3.2 I&AM begrippen en uitgangspunten

Door een steeds verdergaande automatisering binnen bedrijven en het toenemende belang van beveiliging, worden de medewerkers in toenemende mate geconfronteerd met veelvuldig inloggen om zich toegang te kunnen verschaffen tot de diverse objecten (zoals systemen, applicaties en ook gebouwen) waarvoor zij zijn geautoriseerd. De situatie bij vele bedrijven kenmerkt zich enerzijds door een landschap met vele systemen, die iedere een eigen gebruikersadministratie en -autorisatie hebben en anderzijds met een grote mobiliteit van medewerkers. Dit kan tot gevolg hebben dat er nog steeds User ID's in gebruik zijn van personen die niet meer bij de organisatie werkzaam zijn of een andere functie hebben. Ook hebben medewerkers vaak meer autorisaties dan zij voor hun werk strikt nodig hebben.

Behalve dat het vervelend is om veelvuldig te moeten inloggen, levert het gebruik van meerdere wachtwoorden sneller beveiligingsincidenten op (wachtwoorden op memobriefjes e.d.) en wordt vaak de beheerder of helpdesk verzocht actie te nemen op een vergeten wachtwoord. Daarbij worden de autorisaties veelal decentraal en per object toegekend, wat eveneens een grote beheerlast met zich meebrengt.

3.2.1 Definitie van I&AM

Onder I&AM wordt hier verstaan het centraal beheren en controleren van identiteiten van gebruikers (natuurlijke personen en niet natuurlijke gebruikers zoals applicaties) en het toekennen van toegang tot informatie en objecten aan deze gebruikers.

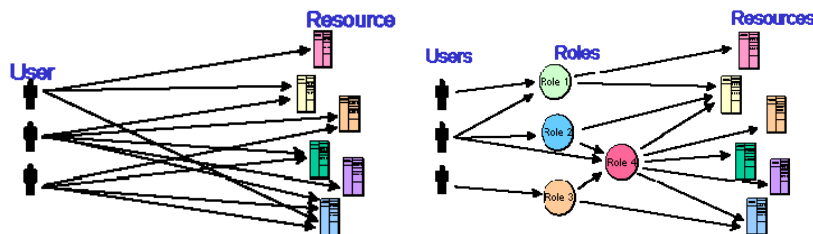
I&AM moet leiden tot een eenduidig georganiseerde toegang tot objecten en informatie op basis van toegekende autorisaties en het voorkomen van misbruik daarvan. Een I&AM programma heeft tot doel de bestaande processen en procedures voor toegang tot informatie en gebouwen te harmoniseren, de kwaliteit van deze processen en procedures te verbeteren en de registratie hiervan in te richten.

Gerelateerde begrippen zijn:

- autorisatie: het verlenen van toegang tot objecten aan bepaalde personen;
- authenticatie (eigenlijk authenticatie): het aantonen door iemand van zijn/haar identiteit.

3.2.2 I&AM Bouwstenen

Een I&AM programma is er op gericht om bovengenoemde problematiek efficiënt en effectief aan te pakken door autorisaties centraal te administreren en geautomatiseerd door te voeren in de decentrale systemen. Vervolgens dient voor het Access Managementdeel te worden gezorgd voor koppeling van deze identiteiten aan autorisaties voor objecten. Dit wordt op de meest efficiënte wijze gerealiseerd door aan gebruikers op basis van hun functie rollen toe te kennen en vervolgens aan deze rollen bepaalde autorisaties te koppelen; ook wel **Role Based Access Control (RBAC)** genoemd. Door deze autorisatie centraal te registreren zijn audits gemakkelijk uit te voeren (auditeerbaar).



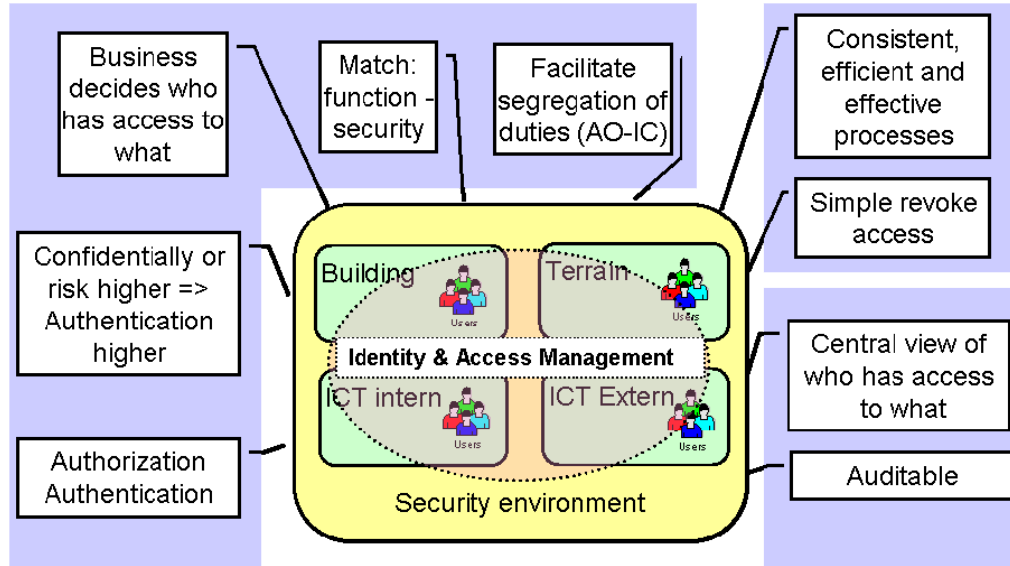
Figuur 1: Resultaat van RBAC

Met de inrichting van I&AM is het vervolgens mogelijk om bepaalde technieken toe te passen, die eerder genoemde ongemakken met wachtwoorden grotendeels verhelpen en de beveiliging doen toenemen. Zo wordt de mogelijkheid geboden om gebruikers zelf hun wachtwoord te laten wijzigen, indien zij dat zijn vergeten of als dat is verlopen; ook wel **Password Self Reset (PSR)** genoemd. Daarnaast kan een door de gebruiker gewijzigd wachtwoord automatisch worden overgebracht naar overige platformen en systemen; **Password Synchronisatie (PS)**. Om het aantal inlogmomenten drastisch in te perken kan nu ook worden gekozen voor **Single Sign-On (SSO)**; volgens Gartner: "One sign-on (logon) per user per session across multiple target systems". In praktijk wordt de inlog gedeeld door verschillende, maar niet door alle, objecten, waardoor de term **Reduced Sign-On (RSO)** vaak meer van toepassing is.

Genoemde concepten zijn toepasbaar voor 'normale' gebruikers, maar zeker ook voor ICT-medewerkers, om hun vaak zeer uitgebreide autorisaties te managen.

3.2.3 I&AM Uitgangspunten

Een I&AM programma dient te leiden tot een uniform, gestandaardiseerd proces van toegang op basis van rollen met toegangsregeling tot alle objecten en informatie op basis van een aantal uitgangspunten. Deze uitgangspunten zijn weergegeven in de volgende figuur en worden nader toegelicht.



Figuur 2: Security Policy

Uitgangspunt A: Security environment

- I&AM richt zich op gebouwen, terreinen, interne ICT-resources en externe ICT-resources.

Uitgangspunt B. Authorization/authentication

- Alleen gebruikers die daartoe geautoriseerd zijn krijgen toegang tot (niet publieke) informatie en objecten;
- Deze gebruikers dienen daartoe bekend en geadministreerd te zijn (bijvoorbeeld in het personeelsadministratiesysteem);
- Deze gebruikers zullen voorzien worden van de benodigde authenticatiemiddelen.

Uitgangspunt C. Confidentially or risk higher => authentication higher

- Alle gebruikers die gebruik maken van digitale informatie, anders dan publieke informatie, dienen zich te identificeren en authenticeren;
- De manier van authenticatie is afhankelijk van de mate van vertrouwelijkheid alsmede hoogte van afbreukrisico.

Als voorbeeld: personen die omgaan met vertrouwelijke informatie of informatie met een hoog afbreukrisico dienen zich door middel van een sterk authenticatiemiddel te identificeren, bijvoorbeeld met een crypto-card.

Uitgangspunt D. Business decides who has access to what

- Het toekennen van autorisatie geschiedt slechts door het daartoe bevoegd (lijn)management.

Uitgangspunt E. Match function - security

- Slechts die autorisaties mogen worden toegekend die voor het uitoefenen dan de functie/rol noodzakelijk zijn.

Uitgangspunt F. Facilitate segregation of duties (AO-IC, administrative organisation – internal control)

- In het kader van functiescheiding mogen er geen tegenstrijdige autorisaties worden toegekend aan één persoon/functie/rol.

Uitgangspunt G. Consistent, efficient and effective processes

- De relevante beheerprocessen, zoals het gebruikersbeheer en het autorisatiebeheer, worden consistent, efficiënt en effectief geïmplementeerd.

Uitgangspunt H. Simple revoke access

- Autorisaties moeten snel en eenvoudig ontnomen kunnen worden.

Uitgangspunt I. Central view of who has access to what

- Er dient vanuit één centraal punt zicht te zijn op wie toegang heeft tot welke objecten.

Uitgangspunt J. Auditable

- Identificaties en autorisaties moeten controleerbaar zijn, als ook de registratie van de individuele verrichte handelingen (logging).

3.3 De Business Case van I&AM

In algemene zin geeft de business case van een project de redenen aan waarom een project wordt opgestart. Het vormt de rechtvaardiging ervan in algemene termen en geeft een antwoord op vragen zoals:

- waarom wordt het project uitgevoerd;
- welke knelpunten worden erdoor verholpen;
- welke voordelen heeft het project voor de organisatie;
- in hoeverre draagt het project bij aan de bedrijfsdoelstelling;
- wegen de opbrengsten van het project op tegen de kosten ervan.

I&AM zorgt voor directe, vooral security-gerelateerde baten:

- het hebben en instandhouden van een adequaat beveiligingsniveau;
- het hebben en instandhouden van adequate interne controlemaatregelen, alsmede het aantoonbaar "in control" zijn;
- het voldoen aan verplichtingen die voortvloeien uit wet- en regelgeving;
- het beperken van het nadelige effect van trage of complexe mutatieprocedures;
- het verhogen van effectiviteit en efficiency van I&AM-gerelateerde processen en daarmee gepaard gaande mogelijke kostenbesparingen.

3.3.1 Enquêteresultaten

De onder de deelnemende bedrijven gehouden enquête geeft het beeld dat vrijwel iedereen op een of andere manier met I&AM bezig is en dat er plannen zijn om er verder mee te gaan. Hierbij worden door verschillende partijen verschillende business cases vermeld:

- Vanuit management: betere beveiliging:
 - men heeft een beter inzicht in de uitgegeven autorisaties (oa. door uitgebreide rapportagemogelijkheden);
 - men bereikt een meer toegesneden autorisatie;
 - RBAC is een must vanwege een onbeheersbare situatie die is ontstaan door het samenvoegingen van bedrijven;
 - I&AM activiteiten worden voorgeschreven vanuit de regelgeving;
 - sanering op reeds uitgegeven rechten wordt mogelijk;
 - role based access levert de mogelijkheid om tot een verantwoorde SSO te komen;
 - geen userid's en passwords op briefjes meer;
 - snel kunnen ontnemen van autorisaties.
- Sommige managers vinden dat bepaalde I&AM acties gewoonweg moeten, zonder dat er behoefte is aan een business case.
- Vanuit de controle afdeling:
 - de uitgegeven autorisaties kunnen eenvoudiger worden gecontroleerd;
 - verrichte handelingen kunnen achteraf worden getraceerd.
- Vanuit beheerders: eenvoudigere beheermogelijkheden:
 - autorisatie is gekoppeld aan de indienst-uitdienst procedure;

- versnipperde activiteiten op autorisatiegebied worden teruggedrongen;
- op het aantal FTE's dat met autorisatie bezig is wordt bespaard;
- door I&AM vanuit één bronsysteem uit te voeren, zijn er minder of geen redundante gegevens bij te houden;
- er zijn lagere kosten doordat er minder password resets nodig zijn;
- er zijn lagere kosten wanneer een password self-reset mogelijkheid wordt ingevoerd (medewerker zijn sneller weer aan het werk);
- Vanuit gebruikers: betere dienstverlening
 - men krijgt sneller toegang tot services;
 - er wordt voorkomen dat gebruikers ontevreden worden (morrend gespuis);
 - men heeft minder of geen wachtwoorden nodig; geen userid's en passwords op briefjes meer.

3.3.2 Kosten-baten analyse

In de enquêtes wordt veelvuldig gemeld dat er kostenbesparingen te verwachten zijn indien I&AM-gerelateerde processen effectiever en efficiënter worden uitgevoerd. De enquêtes bevatten echter geen financiële onderbouwing en geven dus geen antwoord op de vraag of en hoe de kosten die voor I&AM worden gemaakt, werkelijk worden terugverdiend.

3.3.3 Business cases per vorm/type I&AM

Bij de verschillende bouwstenen worden in de enquête de volgende kwalificaties toegekend:

Password Synchronisatie, Single Sign-On en Reduced Sign-On:

- + eenvoudiger beheer
- + besparing op het aantal FTE's dat met autorisatie bezig is
- + minder redundante gegevens over gebruikers bij te houden
- + lagere kosten door minder password resets
- + lagere kosten bij invoering van password self-reset (medewerkers zijn sneller weer aan het werk)
- ++ groter gebruikersgemak
- ++ gebruiker heeft geen of minder userid's en wachtwoorden; geen userid's en passwords op briefjes meer
- + gebruiker krijgt sneller toegang tot services
- + autorisaties kunnen snel worden ontnomen
- minder veilig, daardoor is een sterkere authenticatie en identificatie vereist

Role Based Access Control:

- + betere inzichtelijkheid van de uitgegeven autorisaties (oa. rapportage)
- + betere controleerbaarheid van de uitgegeven autorisaties
- + men bereikt een meer toegesneden autorisatie
- + men voldoet aan wet- en regelgeving
- + sanering van reeds uitgegeven rechten wordt mogelijk
- + basis om tot verantwoorde Single Sign-On te komen
- + verrichte handelingen kunnen worden getraceerd
- ++ veel eenvoudiger beheer
- ++ koppeling autorisatie aan indienst-uitdienst procedure
- ++ terugdringen van versnipperde activiteiten op autorisatiegebied
- ++ besparing op het aantal FTE's dat met autorisatie bezig is
- ++ door I&AM vanuit één bron systeem uit te voeren, zijn er minder of geen redundante gegevens
- ++ betere dienstverlening aan gebruiker
- ++ men krijgt sneller toegang tot services
- ++ autorisaties kunnen snel worden ontnomen
- het initieel toewijzen van de rollen en de daaraan gekoppelde autorisaties is zeer arbeidsintensief

ID-pas / token / biometrie voor fysieke en ICT toegang:

- + betere beveiliging
- + geen password resets meer
- + geen userid's en passwords op briefjes meer

- + eenvoudiger beheer
- + autorisaties kunnen snel worden ontnomen
- kosten voor verwerving en onderhoud van technische middelen

3.4 Aanbevelingen bij I&AM

Implementatie I&AM.

Om I&AM met een goede kans van slagen te kunnen implementeren, moet aan een aantal basisvoorwaarden worden voldaan. Allereerst is het van belang dat de brongegevens voor I&AM (persoon- en functiegegevens) centraal in een HR-systeem zijn vastgelegd om o.a. de integriteit van deze gegevens te kunnen waarborgen. Worden genoemde gegevens decentraal geadmistreerd (b.v. per afdeling of divisie), dan zal een deeloplossing het hoogst haalbare zijn.

Daarnaast dient voor RBAC de business (het lijnmanagement) de rollen met de daaraan te koppelen autorisaties vast te stellen. Dit is niet eenvoudig, zeker niet in een bijvoorbeeld door fusies en/of reorganisaties sterk wijzigende organisatie. Maar als dit eenmaal is gerealiseerd blijkt men juist wel veel flexibeler te kunnen omgaan met dergelijke veranderingen.

Tot slot is van belang het principe te hanteren van "de series of small successes", dus niet in één keer de gehele organisatie met al haar objecten in I&AM willen vangen, maar eerst met een goed afgebakend deel van de organisatie te starten.

De aanbevelingen bij een implementatie zijn:

Overtuig het topmanagement

- Veel wetgevingen zijn gericht op transparantie en het kunnen auditeren van processen, autorisaties en geautoriseerde gebruikers. Met een I&AM-programma (incl. de registratie wie wat kan, wie wat gedaan heeft, welke en door wie uitzonderingen zijn toegestaan) kan je daaraan voldoen. Het helpt het lijnmanagement dus om aan de wetgeving te voldoen en om aantoonbaar "in control" te komen;
- In elk groter bedrijf bestaan er meerdere processen voor user- en autorisatiemanagement. Bijna elke belangrijkere applicatie kent dit en vereist de nodige systeembeheercapaciteit, er worden fouten bij gemaakt en het wordt soms verwaarloosd. Het harmoniseren van deze processen kan, naast het verhogen van het niveau van beveiliging, kostenbesparend werken;
- Het toekennen van de vele afzonderlijke autorisaties maakt dat het operationaliseren van de autorisaties veel tijd kost. Is dat eenmaal goed geregeld dan werkt het uiteraard kostenbesparend indien personeel snel en correct aan de slag kan;
- Stel voor e.e.a. gefaseerd aan te pakken, een proof of concept of een pilot te laten plaatsvinden en geef aan dat er dus Go/No Go-beslismomenten worden ingebouwd.

Zoek medestanders

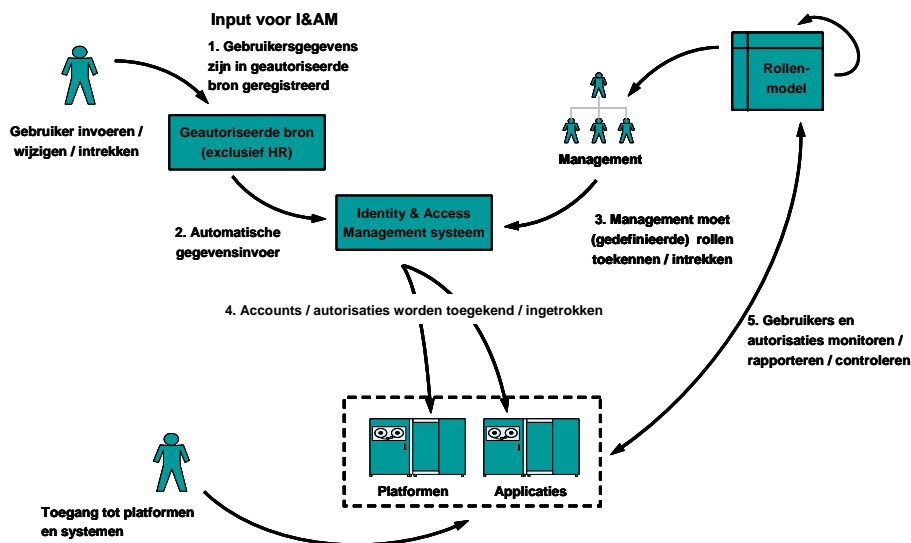
In het bedrijf zijn wellicht andere belanghebbende te vinden die baat hebben bij het inrichten van een efficiënt I&AM-proces en de registratie daarvan. Denk hierbij aan afdelingen zoals Risk Management, Internal Control en Audit en/of lijnmanagers met vaak wisselend personeel. Hierdoor zal het topmanagement sneller zijn overtuigd en zal de uitvoering van het programma soepeler verlopen.

Stel een I&AM beleid op

Het beleid maakt concreter wat men wil bereiken. In dit beleid worden bijvoorbeeld de uitgangspunten zoals onder paragraaf 2.3 (I&AM uitgangspunten) geformuleerd, maar ook de scope, de verantwoordelijkheden voor de processen (usermanagement, rolemangement, provisioning, de bronsystemen, bronregistratie, monitoring en control) voor de rollenindeling (in een RASCI-tabel), het strategisch, tactisch en operationeel niveau. Beschrijf daarnaast de definities, de doelgroepen, de doelsystemen, de te onderkennen typen rollen, etc.

Stel blueprints op

Bij een blueprint wordt vaak slechts gedacht aan de globale technische werking en infrastructuur. Wat veel belangrijker is een blueprint te hebben m.b.t. de organisatie en processen (t.b.v. het usermanagement, het rolemangement, de registratie) en wie de stakeholders en deelnemers binnen deze processen zijn. De volgende figuur geeft daar een voorbeeld van.



Deze processen dienen dus vooraf te zijn uitgewerkt en gedragen door de betrokkenen. Daarnaast dienen de te onderkennen typen rollen te worden vastgesteld, zoals de functionele rol (inkoper, magazijnmedewerker, etc.), de organisatorische rol (medewerker bedrijf c.q. afdeling), technische rollen (ICT-ers, etc.), specifieke rollen (telewerkers, leden OR, projectmedewerker). Aan personen kunnen uiteraard meerdere rollen worden toegekend.

De 80/20 regel is van toepassing: 80% van het werk is organisatorisch, 20% gaat over ICT.

Implementeer gefaseerd

De implementatiestrategie van het programma kenmerkt zich door een gefaseerde aanpak, gefaseerd qua doelsystemen, functionaliteit en doelgroepen en op de verificatie van het "I&AM"-concept door het uitvoeren van een tweetal Proofs-of-Concept. Zorg wel dat alle bronsystemen volledig op orde zijn

- Doelsystemen: begin met een of enkele van de belangrijkste applicaties zoals de financiële, de HR- en de klantsystemen. Laat (voorlopig) de minder belangrijke systemen en zeker de systemen die binnen enkele jaren worden uitgefaseerd (legacy) achterwege. Indien er een managementsysteem voor de fysieke toegang voor gebouwen en terreinen aanwezig is, onderzoek dan of er een koppelmogelijkheid bestaat. Zo ja, laat dit managementsysteem periodiek controleren of de hierin geregistreerde personen nog bekend zijn (via het I&AM-systeem in een van de bronsystemen zoals bijv. het HR-systeem);
- Functionaliteit: begin met (vooral nog) de benodigde generieke infrastructuur (organisatie, processen en technologie), inclusief de initiële uitrol van de organisatorische rol (medewerker bedrijf / afdeling) en enkele functionele rollen voor een beperkt aantal toepassingen;
- Doelgroepen: begin bij de doelgroep medewerkers/inhuurkrachten en laat "suppliers and partners" nog achterwege.
- *Aanpak: ga projectmatig te werk en stel daarvoor een goede projectorganisatie en met name een juiste stuurgroep samen (PRINCE II geeft hiertoe goede tips).*

3.5 De stand van zaken van I&AM bij de deelnemende organisaties

Door middel van de enquête is geïnventariseerd welke I&AM-activiteiten de deelnemende organisaties voltooid of onderhanden hebben en welke zij op de planning hebben staan.

3.5.1 Activiteiten

De activiteiten/concepten op het gebied van I&AM zijn onder te verdelen in drie categorieën:

- Voltooide activiteiten/concepten:
Single Sign On (2x), Password synchronisatie (3x), beperkt Rol Based Access Control (4x) en Reduced Sign On (met smartcard);
- Onderhanden activiteiten/concepten:
Single Sign On (2x), Password synchronisatie, Rol Based Access Control (5x), een proef met RBAC, definiëren van de rollen tbv RBAC, ID-passen voor fysieke toegang én 'ICT-toegang', en het inrichten van een Enterprise Directory gevoed door het HR-systeem;
- Geplande activiteiten/concepten:
Single Sign On (2x), inrichten van een portal om SSO te faciliteren, een studie naar SSO (2x), Reduced Sign On, Role Based Access Control (2x), het selecteren van een tool voor RBAC, en het inrichten van een Enterprise Directory (Active Directory).

3.5.2 Organisatie

Discussiepunt bij de invoering van I&AM is steeds: "wie is de trekker?" Organisaties laten deze rol graag bij de ICT-afdeling, terwijl actieve betrokkenheid van de Business, met name van de afdeling HR, onontbeerlijk is.

Van de geïnterviewde organisaties gaven acht aan dat P&O betrokken was, in vijf gevallen was dat niet zo.

3.5.3 Weerstand

In de enquêtes werden desgevraagd diverse problemen genoemd, waarmee men werd geconfronteerd bij de voorbereidingen en de uitvoering van I&AM-implementaties. Hier kunnen verschillende categorieën worden onderscheiden:

- Organisatorische problemen:
Geen rust in de organisatie, geen duidelijke strategie, geen goede mix van hoofdzaken en details, de organisatie van het 'beheer van de rollen' zelf;
- Praktische problemen:
Kwaliteit van data, (te) veel rollen, bijzondere groepen medewerkers, wegzakkend enthousiasme;
- Overige problemen:
Niet rond krijgen van de financiering, geen business case, prioriteitsstelling.

3.5.4 Tools

Bij de I&AM activiteiten van de deelnemende organisaties werden en worden diverse hulpmiddelen ingezet. Ook is men in twee gevallen nog op zoek naar het juiste product. De tools die worden genoemd zijn:

- IAM tool van SUN (2x)
- TIBCO
- Bhold
- Tivoli Identity Manager en Tivoli Access Manager
- DirX van Siemens
- Personeelssysteem
- Zelfbouw
- RBAC tool (zonder verdere aanduiding)
- Modellen in Excel
- Organogrammen

4 Samenstelling CIG

Elke CIG kent een vertegenwoordiger uit het bestuur van het CIO Platform Nederland en CIO van de leden als trekker.

De bestuursvertegenwoordiging van de CIG Informatiebeveiliging is Hennie Wesseling, CIO TNT Post. De trekker is Kees Jans, CIO van de Schiphol Group.

De bijeenkomsten worden georganiseerd en gemodereerd door de program director van het CIO Platform Nederland, Foppe Vogd.

De deelnemers aan de CIG Informatiebeveiliging en de samenstelling van de werkgroepen daarbinnen is als volgt:

CIG deelnemers

Bert de Man	Min. v Defensie	Luc Colaris	Océ
Dick Brandt	TNT Post	Lyzia van Iterson	Numico
Erik Pieters	Evean Groep	Martijn Dekker	AbnAmro
Evert Jan Evers	UMC Utrecht	Paul Samwel	Rabobank
Frank van Delden	Schiphol Group	Reinier Versluis	Ahold
Hans de Korte	Vopak	René Backers	SVB
Hans Kuiper	Stork	René Colsen	BAM
Hendrikus Beck	VGZIZA	Rob Bloemer	Telegraaf Media ICT
Hennie Wesseling	TNT Post	Rob van Otterdijk	PGGM
Jaap de Bie	NS	Ron van den Bosch	UMCG
Jan Helder	Belastingdienst CICT	Simon Greve	Reaal
Jan van de Wouw	Samas	Willem Knoop	Stork
John Akkermans	Essent	Foppe Vogd	CIO Platform
Kees Jans	Schiphol Group		

Werkgroep "In Control"

Paul Samwel, Rabobank (trekker)

Simon Greve, SNS Reaal

Reinier Versluis, Ahold

Luc Colaris, Océ

Klankbord:

Hendrikus Beck, VGZ/IZA

Willem Knoop, Stork

Piet Kalverda, PGGM

Werkgroep "Awareness"

Hendrikus Beck, VGZ/IZA

Jaap de Bie, NS

Rob Bloemer, Telegraaf Media ICT

Ron van den Bosch, UMCG (trekker)

Rob van Otterdijk, PGGM

Ondersteuning, Sonja Tien, junior ICT adviseur bij het UMCG.

Werkgroep "Identity & Access Management"

John Akkermans, Essent

René Colsen, BAM groep

Frank van Delden, Schiphol Group (trekker)

Bert de Man, Ministerie van Defensie