6.3 Invoering van ISO 17799: een succesvolle aanpak

Wie kent de norm ISO 17799 niet? Het succes van deze bekende leidraad voor invoering van informatiebeveiliging is de afgelopen jaren sterk toegenomen. De vernieuwde versie van de 'Code of Practice for Information Security Management', ook bekend als de BS7799 en in het Nederlands vertaald naar de Code voor Informatiebeveiliging, is in 2000 uitgekomen als ISO-standaard onder de naam ISO/IEC 17799-1: 2000. Dit feit is voor nog meer organisaties een aanleiding geweest om informatiebeveiliging op basis van deze standaard te willen implementeren binnen hun organisatie.
Dit artikel beschrijft ervaringen van een internationaal invoeringstraject van deze ISO-standaard. Het geeft inzicht in een aantal factoren die het succes van een implementatie bepalen.

Auteur: **Aart Bitter** *is werkzaam bij Inter Access B.V. als adviseur op het gebied van informatiebeveiliging. Hij houdt zich vooral bezig met het adviseren van bedrijven over informatiebeveiliging, veelal met het uitvoeren van risicoanalyses en op basis van de ISO 17799-standaard. Voor reacties: Aart.Bitter@interaccess.nl.*

Inleiding

Ondanks de stagnatie van de economische groei in de afgelopen jaren is het onderwerp 'Informatiebeveiliging' een blijvend agendapunt gebleken bij organisaties. Niet bij alle organisaties heeft dit al geleid tot een concrete investering in de vorm van een beleid voor informatiebeveiliging. Het belang van informatiebeveiliging wordt echter onderkend waardoor organisaties zogezegd 'in de startblokken' staan om een implementatie uit te voeren. De wijze waarop men een dergelijke implementatie moet aanpakken, is nog niet altijd even duidelijk. Wellicht een reden waarom men nog even op het startblok blijft staan.

Dit artikel beschrijft een internationale implementatie van informatiebeveiliging op basis van de nieuwe ISO-standaard ISO/IEC 17799. Allereerst zal de omgeving van dit traject worden geschetst. Vervolgens zal de aanpak van deze implementatie worden beschreven. Deze aanpak is een gestandaardiseerde aanpak en hierbij zullen de succesfactoren en 'lessons learned' worden aangegeven. In de conclusie van dit artikel zal worden samengevat welke wijze onderdelen van de aanpak het uiteindelijke succes van de implementatie bepalen.

Het speelveld

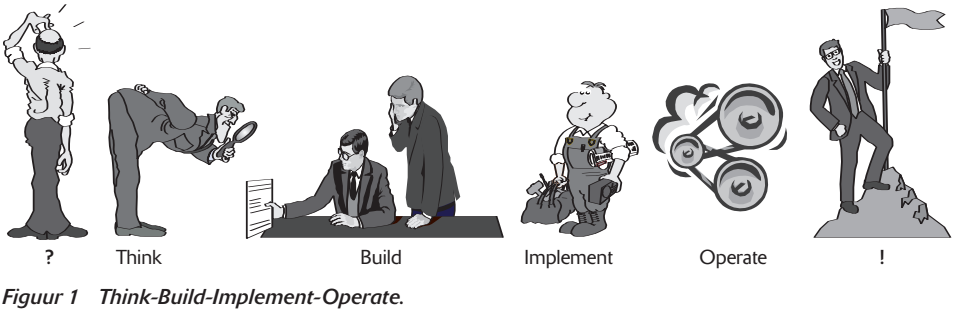
Het informatiebeveiligingstraject speelt zich af binnen een van oorsprong Nederlandse financiële instelling. Deze bestaat uit een Holding-

maatschappij, gevestigd in Nederland, met een 20-tal door Europa gevestigde resultaatverantwoordelijke business units. In deze buitenlandse business units werken tot ca. 200 medewerkers. Alle business units hebben een lokaal netwerk dat lokaal onderhouden wordt. Elke lokale IT-afdeling bestaat uit een groep van 3 tot 15 medewerkers. In een enkel geval is de lokale IT geoutsourcet.
Het lokale netwerk is gekoppeld aan een Wide Area Network (WAN), dat weer toegang geeft tot centrale systemen. De holding heeft ook een IT-afdeling die de buitenlandse business units ondersteunt bij hun beheer van de infrastructuur. Daarbij ligt de nadruk op het gebruik van het WAN. De holding heeft hierbij onderkend, dat risico's met betrekking tot informatiebeveiliging beheerst moeten worden. Deze risico's komen voort uit de businessprocessen, de informatievoorziening en de IT-infrastructuur. Er is een bedrijfsbreed programma gestart, om informatiebeveiliging in te voeren binnen de holding en de afzonderlijke business units. Op centraal niveau heeft men gekozen voor de ISO 17799-standaard voor het implementeren van de beveiligingsmaatregelen.

Om de totale beveiliging van het WAN en ieder aangesloten LAN te waarborgen is en blijft iedere business unit zelf verantwoordelijk voor het beveiligen van de lokale informatievoorziening. De holding zal vanuit het informatiebeveiligingsprogramma de business units ondersteunen met het implementeren van maatregelen door de inzet van een Security Consultant.

De aanpak

Informatiebeveiligingstrajecten zijn veelal complexe gebeurtenissen die binnen de organisatie op veel aandachtsgebieden betrekking hebben. In de praktijk is gebleken, dat een projectmatige aanpak met deadlines, mijlpalen, resourceplanning en andere bij projecten noodzakelijke aandachtspunten, noodzakelijk is. In het afgelopen project hebben we gebruik gemaakt van de binnen Inter Access gehanteerde 'Think – Build – Implement – Operate' aanpak (zie figuur 1). Deze aanpak zorgt ervoor, dat we achtereenvolgens duidelijk de doelstellingen en randvoor-

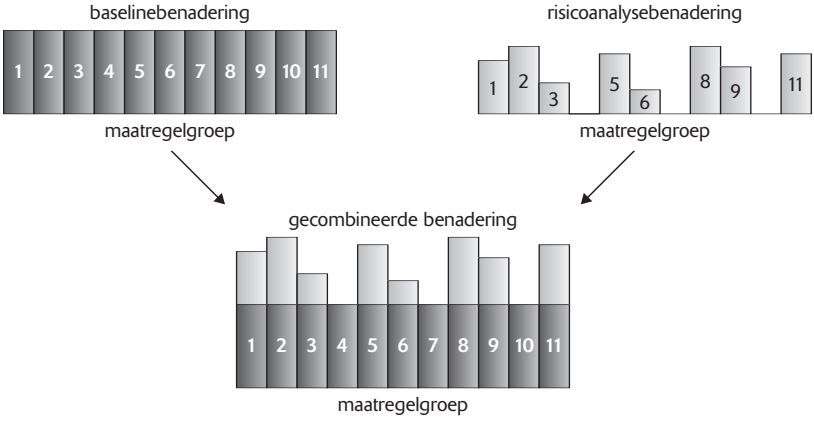


Figuur 1 Think-Build-Implement-Operate.

waarden van het implementatietraject vaststellen, de ondersteunende hulpmiddelen bouwen, de daadwerkelijke implementatie uitvoeren en als laatste stap zorgen dat de geïmplementeerde maatregelen procesmatig geborgd blijven in de organisatie.

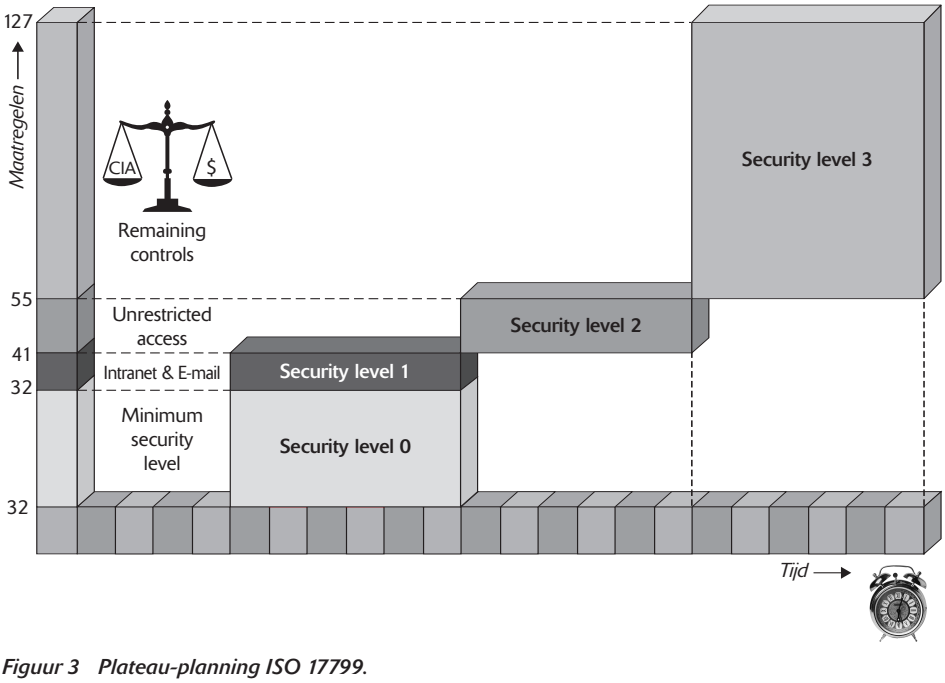
Think

In de Think-fase is het van belang om allereerst de doelen en randvoorwaarden van de implementatie te definiëren. In eerste instantie lijkt het doel: '*Implementeer alle informatiebeveiligingsmaatregelen uit de ISO 17799 bij alle business units*' weinig discussie en open einden te hebben. Bij nadere beschouwing blijkt er daarbij toch een onderwerp te zijn, dat vroeg of laat aan de orde komt, namelijk 'risicoanalyse'.
In het algemeen kan men stellen, dat het implementeren van informatiebeveiliging op twee verschillende manieren kan plaatsvinden, namelijk volgens de zogenoemde 'baselinebenadering' en volgens de 'risicoanalysebenadering'. Bij de baselinebenadering wordt gekozen voor de implementatie van een vaste set van beveiligingsmaatregelen. Bij de risicoanalysebenadering worden de maatregelen geselecteerd op basis van het uitvoeren van een risicoanalyse. Hoewel een implementatie van ISO 17799 een zogenoemde 'security-baselinebenadering' is, wordt in de ISO-standaard zelf het uitvoeren van een risicoanalyse verondersteld. In de Think-fase is het van belang vast te stellen, op welke wijze de organisatie met risicoanalyses omgaat en wat de relatie met het ISO 17799-implementatietraject is.
In de praktijk zien we steeds vaker, dat een combinatie van baselinebenadering en risicoanalyse wordt gekozen. Door een combinatie van beide benaderingen wordt in eerste instantie een vastgestelde set maatregelen geïmplementeerd. Vervolgens wordt voor een aantal specifieke systemen of bedrijfsprocessen een aparte risicoanalyse uitgevoerd om te komen tot aanvullende maatregelen. In figuur 2 wordt dit weergegeven.



Figuur 2 Baseline versus risicoanalyse.

In relatie tot de implementatie van ISO 17799 is er nog een alternatieve mogelijkheid. Daarbij wordt de risicoanalyse uitgevoerd voordat de maatregelen uit de ISO-standaard worden geïmplementeerd. De analyse kan zich bijvoorbeeld richten op de generieke infrastructuur, op generieke bedrijfsprocessen of centrale informatiesystemen. Op basis van de geïdentificeerde risico's worden de maatregelen uit de ISO-standaard vervolgens verdeeld naar beveiligingsniveaus.
In onze praktijksituatie is de risicoanalyse gericht op het gebruik van de (generieke) infrastructuur (het Wide Area Network) en zijn uiteindelijk vier beveiligingsniveaus vastgesteld. Elke 'Security Level' bevat een aantal maatregelen uit de ISO-standaard. 'Security Level 0' wordt beschouwd als een minimum beveiligingsniveau, waaraan iedere business unit dient te voldoen. Security Level 1 is noodzakelijk zodra een business unit van beperkte faciliteiten van het WAN gebruik wil maken (bijvoorbeeld e-mail en intranet). Security Level 2 geeft onbeperkte toegang tot het WAN. Security Level 3 zijn de resterende maatregelen uit de ISO-standaard, die de 127 maatregelen uit de standaard completeren en ISO-compliance mogelijk maken.
Het vaststellen van beveiligingsniveaus sluit perfect aan bij het faseren van de projectaanpak. Het is hierdoor namelijk probleemloos mogelijk om een soort plateauplanning op te stellen van 'Security Levels' (zie figuur 3) die op sequentiële momenten in de tijd binnen de organisatie geïmplementeerd kunnen worden.



Figuur 3 Plateau-planning ISO 17799.

Het is verder van belang om in deze Think-fase aandacht te schenken aan:

- *Afhankelijkheden met andere projecten*
  Hierbij worden niet alleen security-gerelateerde projecten bedoeld, maar dient ook gedacht te worden aan bijvoorbeeld projecten die aanspraak maken op dezelfde resources. Als specifiek security-gerelateerd project willen we hierbij nog Business Continuity Management aanvoeren. Dit onderwerp is al binnengedrongen bij de meeste ondernemingen. Vaak is er al een start gemaakt met het invullen van dit onderwerp volgens een bepaalde methodiek of aanpak. Het onderwerp Business Continuity Management is ook onderdeel van ISO 17799. Gezien de complexiteit en het belang van het onderwerp is het gewenst de aparte aanpak of methodiek te volgen, die al is gedefinieerd binnen de organisatie.

- *Bepalen van implementatie- & projecthulpmiddelen (Dashboard, Toolkit, Reports)*
  Voor de implementatie van informatiebeveiliging is het zaak zowel de te implementeren beveiligingsmaatregelen als ook de voortgang van het traject zo snel en helder mogelijk zichtbaar te maken voor de gehele organisatie. Zie apart kader.

- *(Project) governance*
  De ISO-17799-implementatie wordt projectmatig uitgevoerd. Dat houdt in dat het informatiebeveiligingsproject zich zal moeten conformeren aan de door de organisatie gevolgde projectmanagementmethodiek. De bestaande projectinitiatie, -rapportage en -besluitvorming dienen in acht te worden genomen.

- *(Management) commitment*
  Essentieel voor het in gang zetten en tot een goed einde brengen van een informatiebeveiligingsproject is een duidelijk zichtbaar *commitment* van het management. De verantwoordelijkheden door de organisatie heen dienen helder te zijn vastgesteld en uitgedragen. Alleen hierdoor is het mogelijk om informatiebeveiliging organisatiebreed te besturen en beheersen. Een raamwerk voor dit mechanisme vatten we samen onder de noemer 'Information Security Governance' en in de Operate-fase zullen we hier nog kort op terugkomen.

- *Sponsor*
  Naast het formeel beleggen van taken, bevoegdheden en verantwoordelijkheden van informatiebeveiliging dient gedurende het project een sponsor aanwezig te zijn. Deze sponsor is de verantwoordelijke persoon voor het promoten en dragen van het project.

Uitwerking Dashboard, Toolkit, Reports

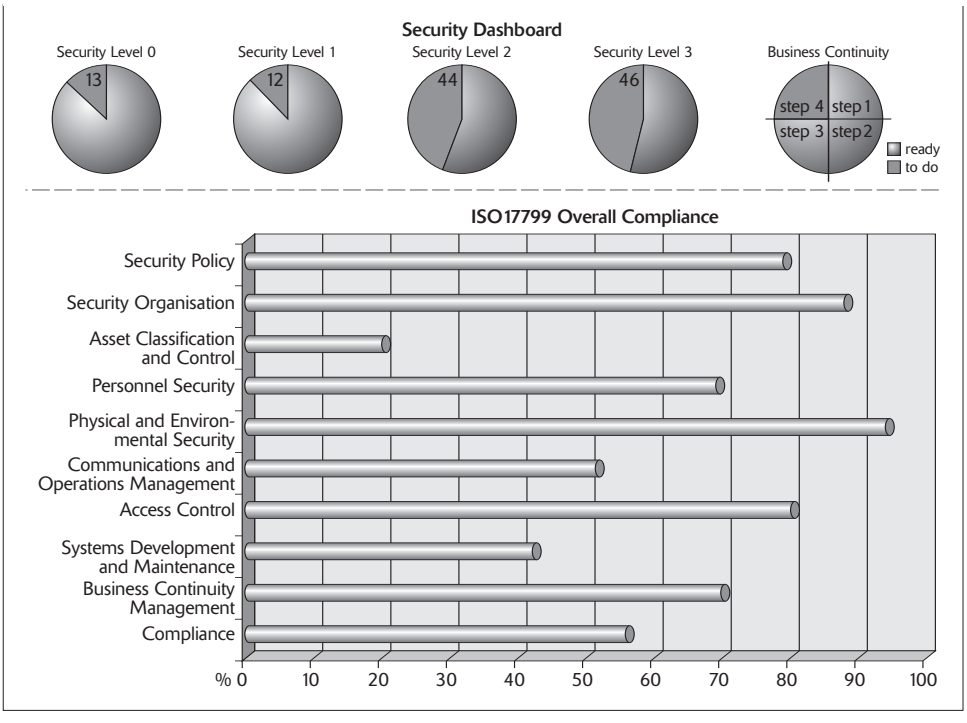
- Ten aanzien van de maatregelen hebben we afgelopen periode goede ervaringen opgedaan met de 'Security Toolkit'. Deze toolkit bevat een overzicht van alle maatregelen uit de te implementeren ISO 17799-standaard. Per maatregel is vastgesteld, welke concrete implementatiemogelijkheden de maatregel heeft. Bovendien geeft dit tijdens de implementatie invulling aan het onderwerp 'evidence'; ofwel welke concrete stukken 'bewijs' kunnen worden verzameld en aangeleverd in geval van een beoordeling van informatiebeveiligingsmaatregelen (bijv. EDP-audit)? De volgende figuur geeft een gedeelte van de Security Toolkit weer.

ISO17799 Security Toolkit

- 3.1.1 Information security policy document
  - Security Policy v1.0.doc
- 4.1.3 Allocation of information security responsibilities
  - Security Governance Model.doc
  - Presentation to joiners.ppt
  - Organisation Chart.ppt
  - Roles and Responsibilities of Application & IT Owners.doc
  - System supported by IT.xls
  - Information Techology Starter Pack.doc
- 4.2.1 Identification of Risks from Third Party Access
  - E-mail guidelines.doc
  - Guidelines use of passwords.doc
  - Internet Use Code of Conduct.doc
  - Non-Disclosure & Confidentiality Agreement Template.doc
- 4.3.1 Security Requirements in Outsourcing Contracts
  - SLA Framework.pdf
  - SLA Template.doc
- 5.1.1 Inventory of assets
- 5.2.1 Classification guidelines

De inhoud van de toolkit sluit verder aan bij de manier, waarop volgens ISO 17799 de security requirements van een organisatie moeten worden bepaald. In de eerste plaats geschiedt dat volgens de eerder genoemde risicoanalyse en afgeleide plateau-planning. Ten tweede is het van belang de relevante wet- en regelgeving in acht te nemen. Uit deze projectervaring blijkt, dat dit in een internationale omgeving van uitzonderlijk belang is. Niet alleen dient men hier de lokaal geldende wetgeving in kaart te laten brengen, vaak zijn ook Europese wetgeving en richtlijnen van belang zoals bijvoorbeeld in geval van grensoverschrijdend dataverkeer (bijv. gerelateerd aan encryptie of persoonsgegevens).
De toolkit sluit zowel aan bij de verscheidenheid aan Europese business units, met alle hun specifieke security requirements. De toolkit is bovendien zodanig opgezet, dat deze kan worden gebruikt door zowel de business units die hun eigen IT-beheren, als ook door de business units die hun IT geoutsourced hebben. Deze business units blijven uiteraard eindverantwoordelijk voor hun eigen informatiebeveiliging, maar kunnen steunen op een aantal formeel opgestelde overeenkomsten en beheercontracten met outsourcing-partners.

- Ten aanzien van de rapportage kan er vaak gebruik worden gemaakt van bestaande projectrapportage-templates. Om de voortgang inzichtelijk te maken voor de gehele organisatie maken we gebruik van een zogenoemde 'Security Dashboard' (zie volgende figuur), dat in één overzicht de status en voortgang van het project weergeeft. Het 'Security Dashboard' is eveneens een waardevol hulpmiddel gebleken bij de periodieke rapportage door het management over informatiebeveiliging.



Build

In deze fase, die vooraf gaat aan de implementatie, wordt een aantal hulpmiddelen samengesteld. Deze zijn ondersteunend aan de implementatie, maar in veel gevallen kunnen deze hulpmiddelen ook blijven dienen na de daadwerkelijke implementatie. De meest sprekende voorbeelden zijn de 'Security Toolkit' en het eerder genoemde 'Security Dashboard'. Beide hebben hun waarde bewezen in en na de projectfasen. Op dit moment worden deze tools aangepast om ze te integreren in een modelleringstool voor business processen. Daarbij is het grote voordeel, dat een 'Information Security Management'-proces zal worden gedefinieerd in het kwaliteitshandboek (en daarmee in de operationele procesatlas). Op deze manier is het mogelijk om 'Information Security Management' als proces op te nemen in de dagelijks uit te voeren werkzaamheden.

Implement

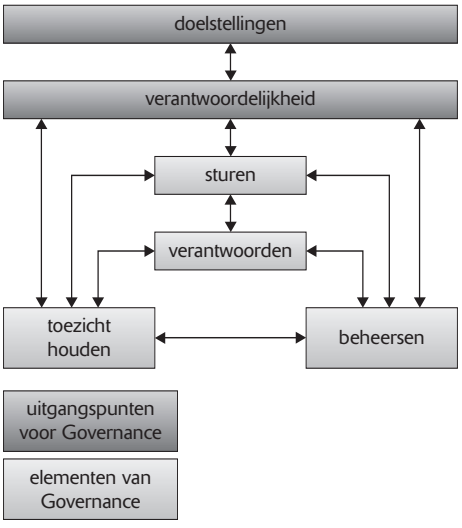
In deze fase vindt de invoering van informatiebeveiliging plaats. De allereerste constatering in deze fase is dat we te maken hebben met een complex veranderingstraject. En veranderingstrajecten dienen 'gemanaged' te worden. Een aantal organisatorische eigenschappen is zichtbaar zoals IT-processen, functieprofielen, Planning en Control en organisatiestructuur. Maar dat is slechts de top van de ijsberg. Niet direct zichtbare zaken van invloed binnen de organisatie zijn o.a. kennis en

kunde, gedrag, houding, politiek etc. En de manifestatie van dit alles bij elkaar heeft invloed op het uiteindelijke succes van een veranderingstraject. Er is daarmee een grote afhankelijkheid van de kennis, vaardigheden en ervaring van het implementatieteam. Grootste gewenste eigenschappen van het implementatieteam zijn kennis van processen, kunnen werken volgens een projectmanagementmethodiek, inlevingsvermogen in de mensen en cultuur en communicatieve vaardigheden. Alleen daarmee konden de business units op een adequate manier worden benaderd, kon een reële inschatting worden gemaakt van de omgevingsfactoren en konden de communicatiekanalen open worden gehouden om informatiebeveiliging onder de constante aandacht te houden. Zoals geïdentificeerd in vele verhandelingen over de implementatie van informatiebeveiliging binnen organisaties, vermelden we hier wellicht nog ten overvloede, dat 'awareness' een essentieel onderdeel van de implementatie dient uit te maken.

Operate

In de Operate-fase steunen we uiteraard op het vele werk, dat in de implementatiefase is verricht. Echter een aantal essentiële zaken dient nog geregeld te worden om de implementatie 'succesvol' te maken. Enerzijds is dat het procesmatige karakter van een proces dat hier in gang gezet dient te worden. Een proces is immers een herhaalbaar iets, maar in deze fase is het van belang om het proces 'werkend te maken'. Ofwel hoe maken we Information Security een onderdeel van de dagelijkse bedrijfsvoering van een organisatie? Allereerst begint dat natuurlijk met het vanuit awareness of risicoanalyse duidelijk maken van het belang van informatiebeveiliging voor de organisatie. Als we ons project met veel communicatie en inlevingsvermogen hebben uitgevoerd, zal een groot gedeelte van dit belang van informatiebeveiliging voor een organisatie al zijn aangekomen bij de business unit manager. Verder hebben we in het kader van de implementatie al het onderwerp informatiebeveiliging en de maatregelen door de gehele organisatie heen aan de orde gesteld. Dat is dan meteen een goed startpunt, voor wat we steeds meer tegenkomen als Information Security Governance.
Dit concept is eigenlijk de waarborg voor het kunnen besturen en beheersen (en instandhouden) van informatiebeveiliging door een gehele organisatie heen. Een model voor (Security) Governance is in figuur 4 weergegeven.

We zorgen er hierbij voor, dat de informatiebeveiligingsactiviteiten in lijn blijven met de bedrijfsstrategie en relevante wet- en regelgeving. De systemen, processen, services en procedures worden hierop afgestemd. Nadat implementatie volgens voorgaande aanpak is uitgevoerd, is het van belang het onderwerp 'control' uit te werken. Daarbij kan enerzijds voor een groot gedeelte gesteund worden op het vaststellen van (taken, bevoegdheden en) verantwoordelijkheden en anderzijds op een ade-



Figuur 4 Information Security Governance.

quaat ingeregeld rapportagemechanisme. Als aansprekende uitwerking kan men hierbij denken aan het eerder genoemde Security Dashboard die verder kan worden geprofessionaliseerd tot een soort van 'Security Balanced Scorecard'. Dit alles dient om ervoor te zorgen, dat een organisatie 'in control' is en blijft van informatiebeveiliging.

Conclusies

De geschetste internationale implementatie van ISO 17799 heeft een groot aantal zaken aan het licht gebracht, die we kunnen beschouwen als belangrijke aandachtspunten voor toekomstige implementaties. Weliswaar zal een nieuwe versie van de ISO 17799-standaard naar verwachting medio 2004 zijn opwachting maken, maar implementatie blijkt voor een groot gedeelte 'mensenwerk' te zijn. Niet zo zeer de inhoud van de ISO-standaard is bepalend voor het succesvol zijn van de implementatie, maar des te meer de aanpak van deze implementatie. Eerste conclusie is dat een gestructureerde projectmatige aanpak de sleutel tot een succesvolle aanpak is. Niet alleen waarborgt de projectaanpak een heldere besluitvormingsstructuur binnen het project, ook kunnen de verantwoordelijkheden van informatiebeveiliging in de lijn worden belegd. De businessmanagers kunnen na het ontwikkelen van voldoende *commitment* als *accountable* worden aangewezen. Een gedegen projectmethodiek ondersteunt verder een fasering en adequate rapportage en dito besluitvormingsproces.

De tweede conclusie is dat het borgen van informatiebeveiliging onlosmakelijk verbonden is aan het implementeren van 'Information Security Governance'-concept. Dit governance-model waarborgt het kunnen besturen en beheersen van informatiebeveiliging door de gehele organi-

satie heen. Zonder een dergelijk concept is het moeilijk en waarschijnlijk zelfs onmogelijk om het informatiebeveiligingsproces werkend en continu draaiend in de organisatie te krijgen en te houden.

Literatuur

ISO/IEC 17799:2000, Code of Practice for Information Security Management

R. von Solms, Will baselines replace risk analysis?, in: *Proceedings of the IFIP/SEC Conference 'Information Security in Research and Business'*, 1997

Oud E.J., *Praktijkgids Code voor Informatiebeveiliging,* Academic Service, 2002

Inter Access, *Beheer en beveiliging,* Information Security Governance, white paper, 2003