8.5 Information security governance

Casus bij financiële instellingen

Na 'corporate governance' en 'IT-governance' duikt binnen (Nederlandse) organisaties het begrip 'information security governance' op. Iedereen 'moet aan de governance'. Maar wat is governance, en wat is dan de betekenis van information security governance?
En onherroepelijk rijst de vraag: hoe implementeren we information security governance? De auteur geeft een inleiding in het begrip 'information security governance', een uitleg van een information security governance-model en een beschrijving van een aanpak om information security governance werkend te maken en te houden.

Auteur:

Aart Bitter is adviseur op het gebied van informatie-beveiliging en is werkzaam bij Inter Access B.V.
E-mail:
aart.bitter@interaccess.nl.

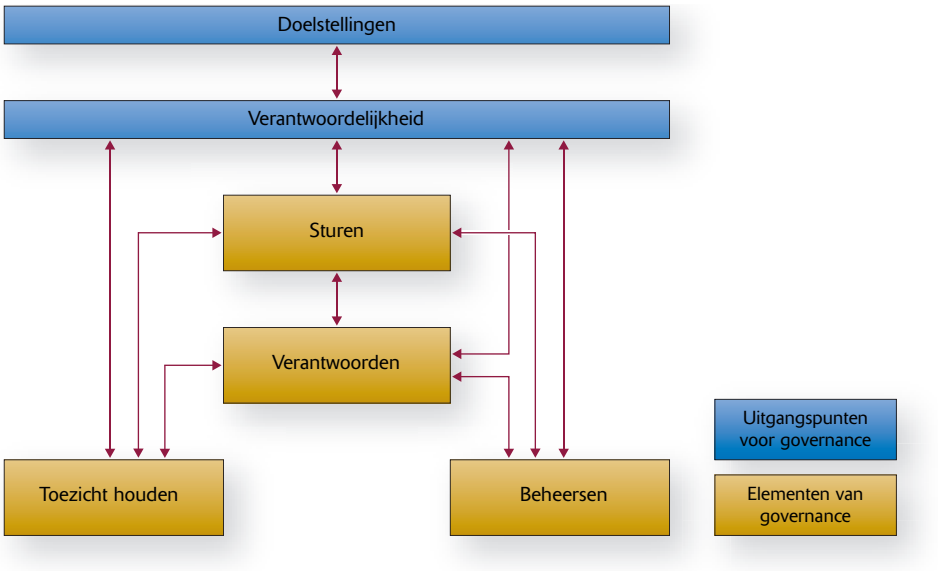
Het begrip 'governance' is al enige tijd nadrukkelijk aanwezig binnen veel organisaties. Veelal is de aanleiding de verplichting van deze organisaties om te voldoen aan de Sarbanes-Oxley-wetgeving (of een van de soortgelijke gedragscodes zoals Turnbull of Tabaksblat). Maar vaak is het begrip zonder deze verplichting 'binnengekomen'. 'Governance' is een algemeen begrip geworden: men spreekt onder andere over corporate governance, IT-governance en information security governance. En vooral die laatste combinatie spreekt de information security-professionals aan. Maar wat verstaan we dan onder information security governance en wat kunnen en/of moeten we ermee?

GOVERNANCE

Onder governance wordt in algemene zin verstaan het 'in control zijn' van een organisatie. Dit wordt bereikt door de strategie en de bedrijfsdoelstellingen van een organisatie op elkaar af te stemmen en door te vertalen naar bedrijfsactiviteiten. Daarin dient eenieder binnen de organisatie zijn verantwoordelijkheid te nemen om de juiste handelingen te verrichten conform interne en externe richtlijnen, waarbij het topmanagement de eindverantwoording draagt. Onder governance valt expliciet ook het op een open wijze communiceren en verantwoording afleggen. Uiteindelijk is het resultaat van governance dat de activiteiten op het gebied van sturen, beheersen, toezicht houden en verantwoorden onderling in balans zijn en in overeenstemming zijn met de doelstellingen van de organisatie.

In het in figuur 1 geschetste governancemodel vormen de organisatiedoelstellingen het uitgangspunt op basis waarvan de verantwoordelijkheden (en daarmee de taken en bevoegdheden) binnen de organisatie vastgesteld dienen te worden. Om van governance te kunnen spreken dienen de volgende activiteiten te worden uitgevoerd:

- Sturen: zorgdragen dat tijdig en adequaat richting wordt gegeven aan het bereiken van de doelstellingen rekening houdend met de interne en externe richtlijnen en verplichtingen.
- Beheersen: een taak van eenieder in de organisatie om volgens de geldende afspraken en richtlijnen te handelen, te monito-



Figuur 1 *Governancemodel*

ren en bij te sturen om het gewenste resultaat te bereiken.
- Toezicht houden: periodiek nagaan of daadwerkelijk is voldaan aan de geldende afspraken en richtlijnen. Dit kan zowel door een interne auditafdeling als door een externe instantie worden uitgevoerd.
- Verantwoorden: er dient te worden gerapporteerd aan belanghebbenden over de bedrijfsvoering. Input van bovengenoemde overige aspecten is hierbij benodigd.

IT-GOVERNANCE

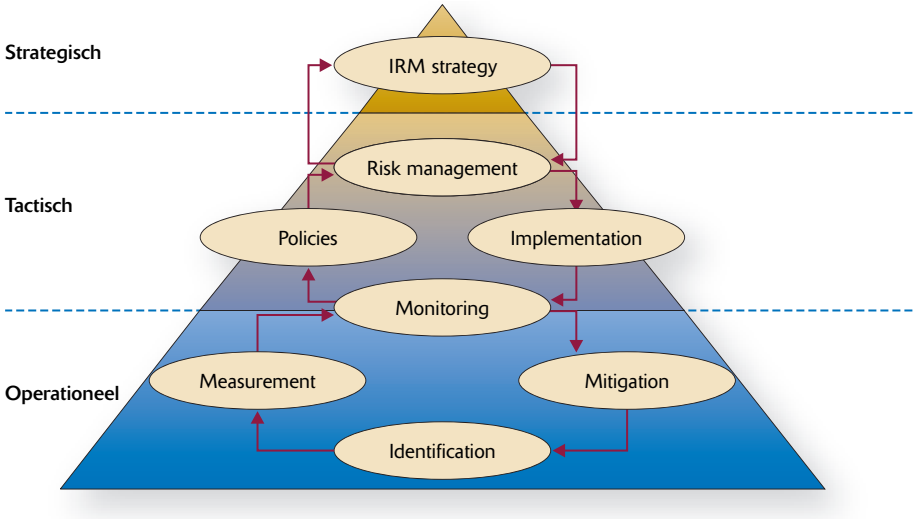
Er is een parallel te trekken naar IT en de wijze waarop organisaties het sturen, beheersen, toezicht houden en verantwoorden van informatie en IT-middelen uitvoeren. Informatie en IT-middelen dienen efficiënt te worden ingezet en benut; met andere woorden, men dient de juiste beslissingen te nemen ten aanzien van het investeren in en aanwenden van IT-middelen. Juiste informatievoorziening (beschikbaar gesteld door bijvoorbeeld technologische toepassingen) is uitermate belangrijk om te kunnen sturen en bijsturen.

Om als organisatie er zeker van te zijn dat in voldoende mate organisatiebreed aan informatiebeveiliging wordt gedaan, zouden organisaties het information security governance-concept moeten implementeren

Verantwoording afleggen over het besturen en beheersen van IT dient een onderdeel te zijn van het algemene governancemodel. Om de beheersing van IT te kunnen realiseren is het voor het management van belang dat het hierover juist wordt geïnformeerd. Hierbij kan worden gedacht aan de volgende informatie: effectiviteit en efficiency van (de inzet) van IT; naleving van relevante wet- en regelgeving op het gebied van IT; de betrouwbaarheid en continuïteit van IT.
In het bijzonder de laatste twee items kunnen worden gerelateerd aan een belangrijk deelaspect van IT, namelijk informatiebeveiliging. Informatiebeveiliging is het aspect dat voldoende mate van maatregelen waarborgt op het gebied van vertrouwelijkheid, integriteit en beschikbaarheid van de informatievoorziening. Om als organisatie er zeker van te zijn dat in voldoende mate organisatiebreed aan informatiebeveiliging wordt gedaan, zouden organisaties het information security governance-concept moeten implementeren.

INFORMATION SECURITY GOVERNANCE

Het doel van information security governance is om vanuit businessperspectief en -belangen te zorgen dat alle IT-activiteiten, -componenten, -systemen, -services en -processen en -procedures in lijn blijven met de eisen die voor de businessdoelen noodzakelijk zijn. Oftewel: op welke wijze moeten organisaties informatiebeveiliging besturen en beheersen zodat aan de eisen van de business, wetgeving en maatschappij kan blijven worden voldaan?
Om conform het algemene governancebegrip de gehele organisatie te betrekken bij information security governance, dient informatiebeveiliging integraal op strategisch, tactisch en operationeel niveau te worden ingevuld. Op ieder niveau zijn daarbij een aantal verschillende aspecten van belang:
- *Strategisch*. Richten (*alignment*): het bepalen van strategie, doelstellingen en beleid en het waarborgen (in control zijn) van informatiebeveiliging op directieniveau.
- *Tactisch*. Inrichten (*planning & implementation*): het bepalen van de normen en de wijze waarop de operationele handelingen en het monitoren van die handelingen wordt verricht.
- *Operationeel*. Verrichten (*measurement*): het uitvoeren van de specifieke securityhandelingen en het meten en controleren op operationeel niveau van deze handelingen.



Figuur 2 *Information security governance-model*

Deze aanpak voor information security governance is in figuur 2 samengevat.

We spreken van information security governance als informatiebeveiliging op alle drie de niveaus is geïmplementeerd. Alleen dan is een organisatie in staat informatiebeveiliging te besturen en beheersen, toezicht te (laten) houden op informatiebeveiliging(smaatregelen) en verantwoording af te leggen over de effectiviteit en efficiency van informatiebeveiliging. Door invulling van het information security governance-model levert informatiebeveiliging toegevoegde waarde aan de bedrijfsdoelstellingen, worden de onderliggende risico's gemanaged en wordt de overall performance gemeten.

IMPLEMENTATIE VAN INFORMATION SECURITY GOVERNANCE

Nu de achterliggende kaders en concepten van information security governance zijn beschreven, is het tijd een voorbeeld te schetsen van een implementatie van information security governance. Het voorbeeld is gebaseerd op een uitgevoerde opdracht om een information security governance-model te ontwerpen en te implementeren.

Het implementatietraject speelt zich af binnen een van oorsprong Nederlandse financiële instelling. Deze bestaat uit een holdingmaatschappij, gevestigd in Nederland, met een twintigtal over Europa verspreid gevestigde resultaatverantwoordelijke business units. De holding heeft hierbij onderkend dat risico's met betrekking tot de informatievoorziening beheerst moeten worden. Deze risico's komen voort uit de businessprocessen, de informatievoorziening en de IT-infrastructuur. Er is een organisatiebreed programma gestart om informatiebeveiliging in te voeren binnen de holding en de afzonderlijke business units. Men heeft gekozen voor de ISO 17799-standaard voor het implementeren van de beveiligingsmaatregelen.

Het totale implementatietraject verloopt in een aantal fasen. De eerste fase van de aanpak voor het implementeren van informatiebeveiliging op basis van de ISO 17799-standaard is eerder gepubliceerd in het *Informatiebeveiliging Jaarboek 2004/2005* [Bitter 2004]. Een van de conclusies is dat het borgen van informatiebeveiliging onlosmakelijk verbonden is met het implementeren van het information security governance-concept. Dit

governancemodel waarborgt het kunnen besturen en beheersen van informatiebeveiliging door de gehele organisatie 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.
De tweede fase van de aanpak richtte zich op de vervolgstap, namelijk het opzetten van een information security governance-model en dat uitrollen in een pilot binnen de holding en een van de business units. Dit alles om de bovengenoemde conclusie uit fase 1 in te vullen. De ervaringen uit de pilot zijn intussen geëvalueerd en zullen worden gebruikt voor de uiteindelijke organisatiebrede uitrol.
Ook voor dit gedeelte van de aanpak is weer gekozen voor een gestructureerd implementatietraject. Als model voor de implementatie is gebruikgemaakt van een gefaseerde aanpak met de fasen alignment, planning, implementation en measurement. De verschillende activiteiten per fase zijn in tabel 1 weergegeven.

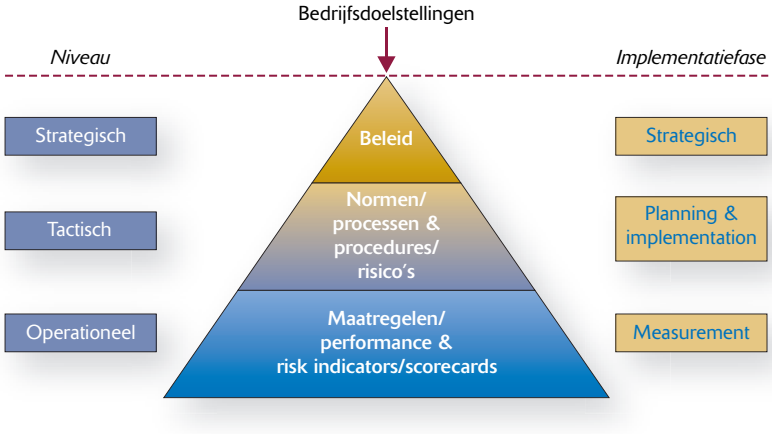
Met een gedeelte van de activiteiten was reeds een start gemaakt in het eerste gedeelte van het project. Door verdere uitvoering van deze implementatieaanpak kon het informatiebeveiligingsproces binnen het strategisch, tactisch en operationeel niveau verder worden ingevuld.

Strategisch niveau

Binnen de organisatie was reeds een onderdeel verantwoordelijk voor het strategisch beveiligingsbeleid. Dit strategisch beleid was afgestemd op de globale bedrijfsdoelstellingen. In deze organisatie gebeurt dat op het niveau van de raad van bestuur. Als startpunt heeft de organisatie in het verleden ervoor gekozen de ISO/IEC 17799 als baseline/best practice te implementeren door de gehele organisatie heen. Na de uitvoering van deze eerste stap (zie [Bitter 2004]) heeft men de strategie aangepast naar een meer 'risk-based' model. Hierbij staat een information risk management-strategie centraal. En daarmee wordt dan een mooie brug gevormd naar de risicoanalyse en het bijbehorende risicomanagementproces van het tactische niveau. Binnen de geschetste organisatie wordt dit tactische niveau ingevuld door de holdingmaatschappij.

Fase	Omschrijving	Activiteiten
Alignment	Het op elkaar afstemmen van interne & externe eisen en organisatorische doelstellingen	Beleid opstellen in lijn met vereisten vanuit wet- en regelgeving, klanteisen, interne eisen en overige belanghebbenden
Planning	Het inrichten van informatiebeveiliging	Het inrichten en trainen van de beveiligingsorganisatie Beveiligingseisen bepalen Het uitvoeren van een risicoanalyse Het opstellen van een informatiebeveiligingsplan
Implementation	Het implementeren van informatiebeveiliging	Implementatie van beveiligingsmaatregelen Het ontwikkelen van beveiligingsprocedures, -richtlijnen en documentatie Het trainen en opleiden van personeel
Measurement	Het toetsen van de mate waarin aan de eisen is voldaan	Bepalen van meetpunten en -instrumenten (Operationele) periodieke controles Toezicht (externe audits) Evaluatie: managementreview Verbeteracties (beslissingen) bepalen en doorvoeren

Tabel 1 *Het implementatietraject*



Figuur 3 *Information risk management-proces.*

Tactisch niveau

Als voornaamste activiteit voor het onderliggende tactische niveau was het opstellen en uitvoeren van een risicomanagementproces benoemd. Het strategisch beleid resulteerde in tactisch beleid, vormgegeven door praktische 'policies' voor een bepaald aandachtsgebied. Een risicoanalysemethode zorgde voor de selectie van maatregelen. Op basis van deze risicoanalyse wordt op tactisch niveau binnen het risicomanagementproces een keuze gemaakt voor de maatregelen die men gaat implementeren. Opgestelde KRI's (*Key Risk Indicators*) en KPI's (*Key Performance Indicators*) vormen de basis voor het kunnen monitoren van de maatregelen en informatiebeveiliging. Na implementatie wordt het monitoren van de effectiviteit en efficiency van de maatregelen ingevuld door het operationele niveau. Na terugkoppeling en evaluatie hiervan is men op tactisch niveau in staat de normen (policies) aan te passen.

Operationeel niveau

Het monitoren van de maatregelen gebeurt op het operationele niveau, ofwel in deze situatie binnen de Europese business units. Uitgangspunt voor dit niveau zijn dan ook de geïmplementeerde maatregelen. Men meet vervolgens de effectiviteit van de maatregelen. Dat gebeurt enerzijds door een controle of de maatregelen nog steeds 'in place' zijn. Anderzijds zullen er KPI's en KRI's benoemd en gemeten worden, die een indicatie geven van de effectiviteit en efficiency van maatregelen. Een voorbeeld hiervan is het meten van bepaalde beveiligingsincidenten (bijvoorbeeld ongeautoriseerde toegang door derden), die een indicatie geven van de werking van een firewall of toegangscontrolesysteem. Deze resultaten worden beoordeeld en verder geëvalueerd op tactisch niveau, waar men kan besluiten tot het aanpassen van policies (bijvoorbeeld het verder aanscherpen van toegangscontrole of firewallinstellingen) en uiteraard ook tot het accepteren van restrisico's. Dit is dan weer het aangepaste normenstelsel, dat op operationeel niveau kan worden gemonitord.

Op basis van deze invulling van het information security governance-model is in figuur 3 het informatiebeveiligingsproces door alle drie de lagen heen weergegeven.

PILOT

Tijdens de pilot is de invulling van information security governance op de drie niveaus ondersteund door tooling. Er is aansluiting gezocht bij een business process management tool. Deze tool maakt het mogelijk processen, onderliggende risico's en genomen maatregelen vast te leggen en zo het information secu-

rity governance-model in te vullen. Tijdens de pilot is gebleken dat de tool bijdraagt aan de herkenbaarheid en consistentie van het informatiebeveiligingsproces binnen de drie niveaus.
In de tool is het informatiebeveiligingsproces ofwel het information risk management-proces beschreven. Dit proces is verder gedetailleerd naar de (deel)processen zoals deze eerder zijn ingevuld op basis van de ISO 17799-standaard. Om de risico's te kunnen benoemen zijn als eerste insteek de *control objectives* gekozen zoals die in de ISO 17799-standaard zijn benoemd. Deze controledoelstellingen zijn namelijk een op een gerelateerd aan een aantal risico's. Ook deze zijn vastgelegd en de geselecteerde en geïmplementeerde maatregelen zijn eveneens in de tool ondergebracht. Op deze manier is een complete vastlegging ontstaan van het informatiebeveiligingsproces binnen de organisatie, dat uiteindelijk uniform kan worden uitgerold binnen alle business units. Als laatste is gebruikgemaakt van de 'review-en-monitor'-functionaliteit van de tooling, die periodiek een aantal zogenaamde vragenlijsten (*assessments*) opstelt om het bestaan van de maatregelen te verifiëren. Aan alle beschreven processen (en dus aan iedere maatregel) is (role-based) een verantwoordelijke medewerker gekoppeld.
Vervolgens is in de pilot een volledige *assessment run* uitgevoerd, dat wil zeggen dat alle maatregelen minimaal één keer zijn getoetst op hun bestaan. De verantwoordelijke medewerker op operationeel niveau heeft deze assessments beantwoord en bijbehorend bewijsmateriaal aangeleverd. De security officer binnen de holding (het tactische niveau) beoordeelde de ingevulde assessments en het bewijsmateriaal en verifieerde de opgestelde policies en uitgevoerde risicoanalyse.

CONCLUSIES

De uitvoering van de pilot heeft plaatsgevonden op basis van een eerste invulling van het information security governance-model. Nog niet alle voor ogen zijnde functionaliteiten waren op dat moment opgenomen in het model (bijvoorbeeld de KPI's en KRI's), maar toch geeft de pilot een goed beeld van de aanpak en invulling van het model en zijn er enkele conclusies te trekken.
De eerste conclusie is dat zowel het strategisch, tactisch als operationeel niveau betrokken moet zijn bij de implementatie. Sturen, beheersen, toezicht houden en verantwoorden strekken zich uit door deze niveaus en taken, bevoegdheden en verantwoordelijkheden op het gebied van beveiliging zijn hier belegd. Zonder relatie naar het tactisch niveau ontbreekt de koppeling van maatregelen naar de oorspronkelijke risico's en processen en zonder strategische koppeling is er geen relatie naar bedrijfsdoelstellingen en geldende wet- en regelgeving.
De tweede conclusie is dat de geschetste gefaseerde aanpak voldoet om het governancemodel in te voeren. De benoemde activiteiten per fase verankeren het informatiebeveiligingsproces voldoende binnen de organisatie. Bovendien helpt de beschrijving van de processen en rollen om het bewustwordingsproces rondom informatiebeveiliging op gang te brengen. Het inzicht door medewerkers in hun rollen, taken, verantwoordelijkheden en bevoegdheden in relatie tot beveiliging nodigt uit tot dagelijkse betrokkenheid bij informatiebeveiliging.
De derde en laatste conclusie is dat de door de tool vereiste relatie proces-risico-maatregelen slechts een eerste invulling is, zeker in relatie tot de baselinebenadering van ISO 17799. De uiteindelijk relatie naar bedrijfsdoelstellingen komt hierdoor nog niet voldoende tot zijn recht. Mede daardoor is besloten om op korte termijn de risicoanalyse meer gewicht te geven. Nadrukkelijk zullen (uiteraard) de businessprocessen van de organisatie leidend zijn in deze analyse en kan hierdoor de relatie proces-risico-maatregelen beter worden aangesloten op het strategisch niveau.

LITERATUUR

[Bitter 2004] Bitter, A., 'Invoering van ISO 17799: een succesvolle aanpak', in: F.M. Kanters en W.J. Huurman (red.), *Informatiebeveiliging Jaarboek 2004/2005*, Sdu Uitgevers, 2005

Corporate Governance Task Force, 'Information Security Governance: A Call to Action', april 2004

Entrust, 'Information Security Governance: An essential element of Corporate Governance', april 2004

Inter Access, *Information Security Governance*, whitepaper en implementatieposter, april 2005.

ISO, BS 7799-2 Code of Practice for Information Security Management ISO, ISO/IEC 17799:2000 Code of Practice for Information Security Management

IT Governance Institute, 'Information Security Governance: Guidance for Boards of Directors and Executive Management', 2001

Ministerie van Financiën, *Handleiding Government Governance*, januari 2000

WEBSITES

www.itgi.org
www.cyberpartnership.org
www.interaccess.nl
www.isaca.org
www.entrust.com
www.bsa.org
europa.eu.int