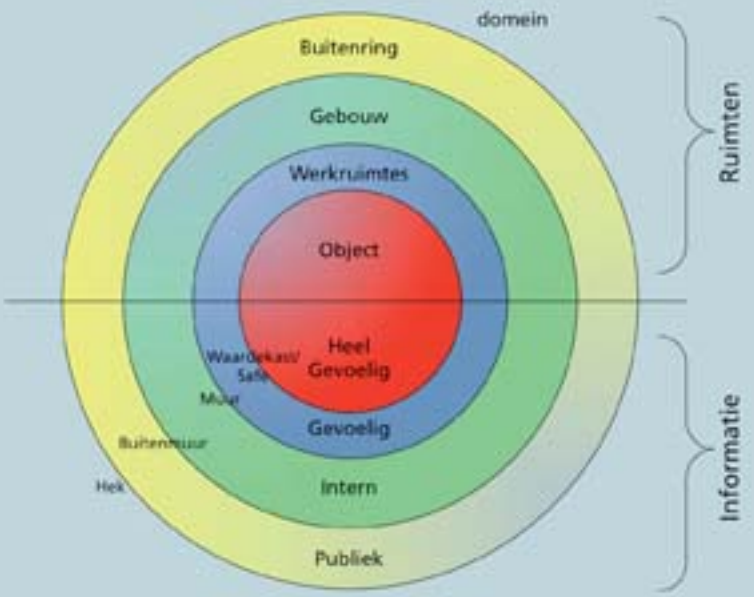
BEST PRACTICE

# Basiskennis informatiebeveiliging

## op basis van ISO27001 en ISO27002




Hans Baars
Jule Hintzbergen
Kees Hintzbergen
André Smulders

Van Haren Publishing

Basiskennis informatiebeveiliging op basis van ISO27001 en ISO27002

## Andere uitgaven bij Van Haren Publishing

Van Haren Publishing (VHP) is gespecialiseerd in uitgaven over Best Practices, methodes en standaarden op het gebied van de volgende domeinen:

- IT-management,
- Architecture (Enterprise en IT),
- Business management en
- Projectmanagement.

Deze uitgaven worden uitgegeven in verschillende talen in series, zoals *ITSM Library*, *Best Practice, IT Management Topics* en *I-Tracks.*

Van Haren Publishing biedt een groot aanbod aan whitepapers, templates, gratis e-books, docentenmateriaal etc. via de **VHP Freezone**: freezone.vanharen.net

VHP is tevens de uitgever voor toonaangevende instellingen en bedrijven, onder andere: ASLBiSL Foundation, CA, Centre Henri Tudor, Gaming Works, Getronics, IACCM, IAOP, IPMA-NL, ITSqc, NAF, Ngi, PMI-NL, PON, Quint, The Open Group, The Sox Institute

Onderwerpen per domein zijn:

**IT (Service) Management / IT Governance**
ASL
BiSL
CATS
CMMI
COBIT
ISO 17799
ISO/IEC 27001
ISO/IEC 20000
ISPL
IT Service CMM
ITIL® V3
ITSM
MOF
MSF
SABSA

**Architecture (Enterprise en IT)**
Archimate®
TOGAF™
GEA®

**Business Management**
EFQM
eSCM
ISA-95
ISO 9000
OPBOK
SixSigma
SOX
SqEME®

**Project-, Programma- en Riskmanagement**
A4-Projectmanagement
ICB / NCB
MINCE®
M_o_R®
MSP™
*PMBOK® Guide*
PRINCE2™

Voor een compleet overzicht van alle uitgaven, ga naar onze website: www.vanharen.net en freezone.vanharen.net voor whitepapers, templates, gratis e-books, docentenmateriaal etc.

# Basiskennis informatiebeveiliging

## op basis van ISO27001 en ISO27002

**Hans Baars**
**Jule Hintzbergen**
**Kees Hintzbergen**
**Andre Smulders**

Van Haren PUBLISHING

# Colofon


| | |
|---|---|
| Titel: | Basiskennis informatiebeveiliging op basis van ISO27001 en ISO27002 |
| Auteurs: | Jule Hintzbergen, Kees Hintzbergen, André Smulders, Hans Baars |
| Reviewers: | Engelstalige versie:<br>Norman Crocker (Cronos Consulting)<br>Steven Doan (Schlumberger, USA)<br>James McGovern (The Hartford)<br>Prof. Pauline C. Reich (Waseda University School of Law)<br>Bernard Roussely (Cyberens Technologies & Services)<br>Tarot Wake (Invictus Security) |
| Uitgever: | Van Haren Publishing, Zaltbommel, www.vanharen.net |
| ISBN: | 978 90 8753 567 4 |
| Druk: | Eerste druk, eerste oplage, maart 2011<br>Eerste druk, tweede oplage, oktober 2013 |
| Redactie en zetwerk: | CO2 Premedia, Amersfoort |
| Copyright: | © Van Haren Publishing, 2011 |

Voor verdere informatie over Van Haren Publishing, e-mail naar: info@vanharen.net.

# Woord vooraf

Aan het woord beveiliging (security) kleeft van nature een negatief gevoel. Beveiliging wordt uiteindelijk alleen toegepast als daar een reden voor is, namelijk wanneer er risico's bestaan dat dingen niet zullen gaan zoals ze moeten gaan. In dit boek worden veel onderwerpen over informatiebeveiliging op een zo eenvoudig mogelijke manier besproken, want informatiebeveiliging is ieders verantwoordelijkheid, hoewel veel mensen zich dat vaak niet realiseren.

Beveiliging is niet nieuw, de bron van informatiebeveiliging ligt al vele eeuwen achter ons. De Egyptenaren bijvoorbeeld, gebruikten niet-standaard hiërogliefen bij het graveren van hun monumenten. En de Romeinen vonden de zogenoemde Ceasar Cypher uit om berichten te versleutelen. Ook de fysieke beveiliging is al heel oud. Denk aan de oude kastelen en verdedigingswallen als de Chinese muur, maar ook aan de sloten op kasteeldeuren en boekenkisten. De laatste jaren wordt bij fysieke beveiliging steeds meer ICT-technologie toegepast. Voorbeelden zijn fysieke toegangscontrolesystemen en (IP-)camerasystemen.

De eerste versie van dit boek dateert uit 2007 en werd door EXIN gebruikt als studiemateriaal. Maar het boek is ook bedoeld voor iedereen die iets met informatiebeveiliging te maken heeft en voor diegenen die gewoon wat meer kennis over dit onderwerp willen opdoen. Eind 2009 verscheen de Engelstalige versie van het boek, waarin een groot aantal verbeteringen zijn doorgevoerd. Deze grondig herziene versie van het oorspronkelijke boek ligt nu voor je, en vormt een goede basis als je een verdere studie binnen dit vakgebied wilt gaan doen.

**Wat vind je in dit boek?**
We starten met een introductie en begripsvorming, dit is de basis: de fundamentele principes waarop informatiebeveiliging en risicomanagement zijn gebaseerd.

Daarna bespreken we de onderwerpen: architecturen, processen en informatie. Inzicht in deze onderwerpen is nodig om IT-beveiliging te begrijpen. Vervolgens gaan we dieper in op risico's, dreigingen en de beveiligingsmaatregelen die genomen kunnen worden om die risico's en dreigingen te managen.

Bedrijfseigendommen worden bediscussieerd. Wat zijn dat en hoe moeten die worden onderhouden?

In de verdere hoofdstukken gaan we in op de (IT-)beveiligingsmaatregelen. Eerst benoemen we de fysieke beveiligingsmaatregelen, en die beginnen bij de deur. Want daar komen mensen het gebouw binnen. Als tweede punt bespreken we de technische IT-aspecten die te maken hebben met beveiliging, zoals encryptie. En vervolgens gaan we in op organisatorische beveiligingsmaatregelen. Waar nodig gaan we dieper in op de technische beveiligingsmaatregelen die noodzakelijk zijn om de organisatorische beveiligingsmaatregelen uit te kunnen voeren.

Als laatste beschrijven we de communicatie- en operationele procedures die noodzakelijk zijn voor een effectief risicomanagement binnen een organisatie.

Ook geven we wat informatie over wet- en regelgeving. De oorspronkelijke uitgave in het Engels is de bron voor deze uitgave, wat betekent dat we niet alleen op de wetgeving in Nederland en België ingaan. Er zijn veel boeken geschreven over wet- en regelgeving, en ook op internet vind je enorm veel bronnen die in dit onderwerp zijn gespecialiseerd.

Dit boek wordt aanbevolen als studieboek voor het examen Information Security Foundation based on ISO/IEC 27002 van EXIN. Je kunt de Information Security examens doen op Foundation, Advanced en Expert niveau. Op het Expertniveau word niet alleen je kennis van de ISO/IEC 27002 geëxamineerd, maar ook je kennis van de ISO/IEC 27001.

De organisatie van Informatiebeveiliging Professionals in Nederland (PvIB) beveelt dit boek aan als een goede start in de wereld van informatiebeveiliging. Het is een boek dat je gelezen moet hebben!
Fred van Noord, voorzitter PvIB.
www.pvib.nl

# Inhoudsopgave

# Over de auteurs

De auteurs zijn allen lid van het Platform voor Informatiebeveiliging en stellen zich tot doel het vakgebied informatiebeveiliging toegankelijker te maken voor zowel informatiebeveiligingspecialisten als voor managers en medewerkers van organisaties die er net mee beginnen.

Hans Baars (CISSP, CISM) was van 1999 tot 2002 werkzaam als intern EDP-auditor bij het Korps Landelijke Politie Diensten (KLPD) te Driebergen. In 2002 werd hij adviseur integrale veiligheid bij het KLPD. Vanuit deze functie was hij medeverantwoordelijk voor de totstandkoming van het beveiligingsbeleid. Vanaf 2006 tot eind 2009 was hij werkzaam als security consultant. Gedurende die periode adviseerde hij overheids- en commerciële bedrijven over fysieke- en informatiebeveiliging. Van 2009 tot 2012 is hij als Chief Information Security Officer werkzaam geweest bij Enexis BV, een Gas- en Elektriciteit netwerkbeheerder in Nederland. Thans werkzaam als senior security consultant bij DNV KEMA met als specialisatie de energiesector en industriële controlesystemen.

Jule Hintzbergen (CISSP CEH) stapte in 1999 na 21 jaar voor het ministerie van Defensie gewerkt te hebben, over naar CapGemini als securityconsultant voor de publieke sector. Jule heeft meer dan 30 jaar ervaring in de IT en besteedt het overgrote deel van zijn werkzame tijd aan informatiebeveiliging. Hij heeft veel ervaring in verschillende vakgebieden zoals projectmanagement en informatiemanagement, fysieke en informatiebeveiliging en biometrie. Sinds 2003 is Jule gecertificeerd CISSP bij ISC(2) en sinds 2013 is hij gecertificeerd CEH (Certified Ethical Hacker).

Kees Hintzbergen is freelancer en beschikbaar voor interim en consultancy opdrachten binnen het vakgebied informatiebeveiliging. Kees heeft meer dan 25 jaar ervaring in de ICT en Informatievoorziening en werkt sinds 1999 in het vakgebied informatiebeveiliging. In 1998 heeft hij zijn AMBI-master gehaald op het gebied van Exploitatie en Beheer. Daarnaast heeft hij opleidingen gevolgd bij de Hogeschool van Amsterdam (HEAO-BI) en de Hogeschool Dirksen (System Engineer). Kees heeft veel ervaring binnen verschillende vakgebieden. Kees is sinds 2012 betrokken bij de oprichting van de Informatiebeveiligingsdienst voor Gemeenten. In deze opdracht heeft hij diverse adviezen gegeven, heeft hij meegewerkt aan de start-up van een sectorale CERT (voor gemeenten) en daarnaast is hij mede-auteur van de Baseline Informatiebeveiliging voor Gemeenten (BIG) in al zijn varianten.

André Smulders (CISSP) is senior informationsecurityconsultant bij TNO Informatie en Communicatie Technologie. Nadat André zijn studie Technology Management aan de Technische Universiteit van Eindhoven in 1996 afsloot, begon zijn carrière in het vakgebied innovatie en IT. Sinds 2000 heeft hij zich gespecialiseerd in informatiebeveiliging. In zijn huidige rol als consultant en programmamanager is hij betrokken bij informatiebeveiligingsprojecten variërend van een hoog technisch niveau tot aan het strategische niveau.

# Dankbetuiging

Dit boek is geschreven vanuit de visie dat een basisbegrip van informatiebeveiliging voor iedereen belangrijk is. We hebben geprobeerd veel informatie te verschaffen, zonder te gedetailleerd te zijn. De auteurs hebben het boek vanuit de Nederlandse context geschreven, zonder de internationale samenhang van informatiebeveiliging uit het oog te verliezen. Informatietechnologie kent immers geen grenzen.

Wij hebben dankbaar gebruikgemaakt van enkele reviewers die ons geheel vrijwillig hebben geholpen om dit boek nog beter te maken. Zij hebben onze teksten van waardevol commentaar voorzien. Wij willen hen dan ook graag onze dank betuigen. In alfabetische volgorde zijn dat:

Norman Crocker, Cronos Consulting, Silves, Portugal
Steven Doan, Schlumberger, Houston, Texas, USA
James McGovern, The Hartford, Hartford, Connecticut, United States
Prof. Pauline C. Reich, Waseda University School of Law, Tokyo, Japan
Bernard Roussely, Director, Cyberens Technologies & Services, Bordeaux, France
Tarot Wake, Invictus Security, Flintshire, United Kingdom

# 1 Introductie

Dit boek is bedoeld voor iedereen in een organisatie die basiskennis van informatiebeveiliging op wil doen. Kennis over informatiebeveiliging is belangrijk voor iedere medewerker. Het maakt geen verschil of je in een commercieel of een niet-commercieel bedrijf werkt. Elke organisatie heeft te maken met risico's.

Medewerkers moeten weten waarom zij in hun dagelijkse werkzaamheden beveiligingsvoorschriften na moeten leven. Lijnmanagers moeten kennis hebben van informatiebeveiliging omdat zij daarvoor binnen hun afdeling verantwoordelijk zijn. Deze basiskennis is ook belangrijk voor alle directieleden en zelfstandigen zonder personeel. Ook zij zijn verantwoordelijk voor het beschermen van de eigendommen en informatie die zij bezitten. Een bepaald gevoel van bewustwording is ook voor de thuissituatie belangrijk. Natuurlijk is deze basiskennis onontbeerlijk als je besluit van informatiebeveiliging, IT, of procesmanager je beroep te maken.

Iedereen heeft te maken met informatiebeveiliging, al is het maar met de beveiligingsmaatregelen die een organisatie genomen heeft. Deze beveiligingsmaatregelen zijn soms afgedwongen door wet- en regelgeving. Soms worden ze geïmplementeerd op basis van intern beleid. Neem als voorbeeld het gebruik van een wachtwoord op de computer. Vaak beschouwen we beveiligingsmaatregelen als lastig en overbodig. Ze kosten tijd en het is lang niet altijd duidelijk waartegen ze ons beschermen.

In informatiebeveiliging is het de truc om de gulden middenweg te vinden tussen een aantal aspecten:
- De kwaliteitseisen die een organisatie stelt aan zijn informatie.
- De risico's die geassocieerd worden met die kwaliteitseisen.
- De beveiligingsmaatregelen die genomen worden om die risico's af te dekken.
- Wanneer en op welke manier incidenten buiten de organisatie gerapporteerd worden.

## Wat is kwaliteit?

Kwaliteit betekent 'hoedanigheid' of, meer toegespitst, 'eigenschap'. Het woord is in die betekenissen ontleend aan het Latijnse *qualitas*. De meest neutrale definitie van kwaliteit is: het geheel van eigenschappen van een object, waarbij een object een ding, activiteit, persoon of concept kan zijn. Het begrip wordt daarnaast in engere, positieve zin gebruikt in de betekenis: '*goede* hoedanigheid of eigenschap', 'deugdelijkheid'. Zo spreekt men van een kwaliteitskrant, van waterkwaliteit en van sociale kwaliteit.

Eerst zul je als organisatie moeten bepalen wat je onder kwaliteit verstaat. Op het eenvoudigste niveau dient kwaliteit twee vragen te beantwoorden: 'wat wordt er gevraagd?' en 'hoe doen we het?' Vanzelfsprekend ligt de basis van kwaliteit altijd in het gebied van de werkprocessen. Aan de hand van kwaliteitsaspecten, zoals beschreven in de ISO 9000, en procesbeschrijvingen volgens het 'Total Quality Management' (TQM), specificeren, meten, verbeteren kwaliteitsprofessionals de processen, en indien nodig herontwerpen zij processen om er zeker van te zijn dat organisaties krijgen wat ze willen.

Er zijn net zoveel definities voor het woord kwaliteit als er kwaliteitsconsultants zijn, maar algemeen aanvaarde omschrijvingen komen voor in de volgende artikelen/boeken[1]:

- Voldoen aan eisen ('Conformance to requirements') – Crosby.
- Passend binnen het gewenste gebruik ('Fitness for use') – Juran.
- Het totaal van karakteristieken dat een entiteit draagt in zijn mogelijkheid om aan vastgestelde en onuitgesproken eisen te voldoen. - ISO 8402:1994.
- Kwaliteitsmodellen voor bedrijven zoals de Plan-Do-Check-Act cyclus en het INK-management model van het Nederlands Kwaliteits Instituut.

Het primaire doel van dit boek is om studenten voor te bereiden op het basisexamen informatiebeveiliging. Het boek is gebaseerd op de internationale standaard NEN-ISO/IEC 27002, ook bekend als de Code voor Informatiebeveiliging.

Docenten kunnen de informatie in dit boek gebruiken om de kennis van hun studenten te toetsen. Aan het eind van ieder hoofdstuk is een case opgenomen. Iedere case gaat in op de onderwerpen die in het desbetreffend hoofdstuk zijn behandeld en geven veel vrijheid in de wijze waarop de vragen beantwoord kunnen worden. Voorbeelden van recente incidenten zijn 'vertaald' naar de casestudie en verduidelijken de teksten in het boek.

De case start op een basisniveau en naar gelang we verder komen in het boek, groeit het niveau. De case is gebaseerd op boekhandel Springbooks. In het begin telt Springbooks enkele medewerkers en heeft ze beperkte informatiebeveiligingsrisico's. Per hoofdstuk zien we de boekhandel groeien en aan het eind is het een grote organisatie met 120 winkels en haar internetwinkel kent een uitgebreid assortiment. De risico's en dreigingen nemen met de groei van de winkelketen ook toe.

Dit boek is bedoeld om de verschillen tussen risico's en kwetsbaarheden uit te leggen en de beveiligingsmaatregelen die kunnen helpen om deze risico's en kwetsbaarheden zo veel mogelijk in te perken.

Door het algemene karakter van dit boek is het ook goed bruikbaar als materiaal voor een bewustwordingstraining of als naslagwerk tijdens een bewustwordingscampagne.

Dit boek is in eerste instantie gericht op profit- en non-profitorganisaties. Het is echter ook goed toepasbaar in de huiselijke situatie en voor kleine bedrijven (MKB) die geen eigen beveiligingsmedewerkers in dienst hebben. In het MKB is beveiliging meestal een (bij)taak voor een enkele medewerker.

Na het lezen van dit boek heb je algemene kennis opgedaan over de onderwerpen waar informatiebeveiliging over gaat. Je weet ook waarom die onderwerpen belangrijk zijn en heb je kennis van de meest algemene concepten die gebruikt worden binnen de informatiebeveiliging.

1 http://syque.com/articles/what_is_quality/what_is_quality_1.htm

# 2 Case: Springbooks – een internationale boekhandel

## 2.1 Introductie

Om de theorie in dit boek te begrijpen, vertalen we die theorie naar de dagelijkse praktijk. We gebruiken daarvoor een case die gaat over boekhandel Springbooks. Deze case wordt in alle hoofdstukken gebruikt, en daarbij worden vragen gesteld die gerelateerd zijn aan de onderwerpen die in het hoofdstuk zijn behandeld.

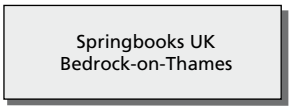
Figuur 2.1 De hoofdvestiging van Springbooks in Londen

In dit hoofdstuk beschrijven we de oprichting van de boekwinkel, de historie en groei die de boekwinkel doormaakte naar een internationaal bedrijf. Een organisatie die met haar tijd mee gaat en ook via internet boeken verkoopt. We hebben in deze case gekozen voor een fictief Engels bedrijf vanwege de bijzondere verhouding die het heeft met Europa, die ook zijn weerslag vindt in de organisatie van het bedrijf.

Springbooks werd opgericht in 1901. Gedurende haar groei tot een internationale organisatie met vestigingen door heel Europa moest zij zich constant aanpassen aan de veranderende omstandigheden. De belangrijkste en grootste veranderingen vonden plaats in de afgelopen 50 jaar, in de manier waarop met informatie wordt omgegaan. Iedereen zal begrijpen dat er grote verschillen zijn in de wijze waarop de processen gecontroleerd werden tijdens de oprichting in 1901, tot de eerste computers hun intrede deden in de jaren ’60 en ’70 van de vorige eeuw tot aan nu waar organisaties enorm afhankelijk zijn van geautomatiseerde systemen. ICT is een van de belangrijkste gereedschappen geworden voor Springbooks.

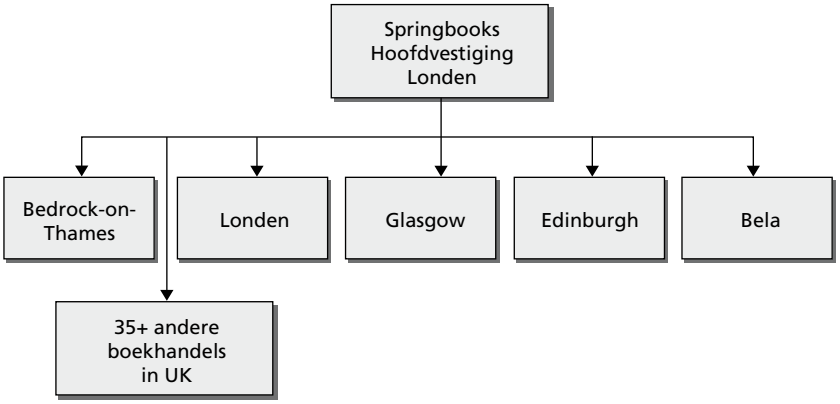
## 2.2 Springbooks

Springbooks Ltd. is een Europees opererende boekhandel. SB is een organisatie bestaande uit 120 boekhandels. De meeste daarvan opereren op franchisebasis. 50 Boekwinkels zijn eigendom van SB zelf.



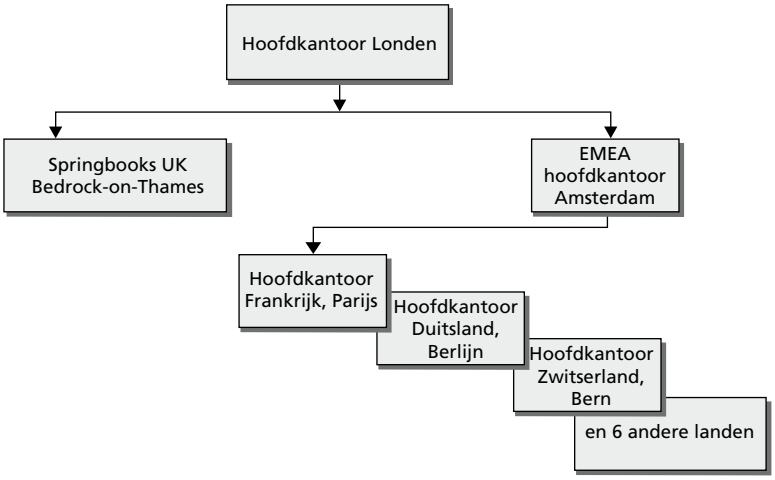

Figuur 2.2 Organisatieplaatje Springbooks 1901-1931

De eerste SB werd opgericht in 1901 in Bedrock-on-Thames, UK. Henry Spring opende een boekwinkel in een kleine winkel niet wetende dat zijn kinderen een mega winkelketen zouden gaan beheren.




Figuur 2.3 Organisatie van Springbooks 1938

In 1938 was het bedrijf al gegroeid tot 40 winkels in alle belangrijke steden in het Verenigd Koninkrijk. Onmiddellijk na het einde van de Tweede Wereldoorlog opende SB boekwinkels in Amsterdam, Kopenhagen, Stockholm, Bonn, Berlijn en Parijs.




Figuur 2.4 Organisatie van Springbooks 1946-2011

Tegenwoordig heeft SB winkels in alle belangrijke steden van Europa. De Raad van Bestuur is gevestigd in het hoofdkantoor te Londen. Het Europese hoofdkantoor, een uitvloeisel uit de tijd dat het Verenigd Koninkrijk iets heel anders was, dan het verre Europa, is gevestigd in Amsterdam. Ieder land heeft een centraal kantoor dat in de hiërarchie onder het hoofdkantoor te Amsterdam staat. Amsterdam is verantwoording schuldig aan het hoofdkantoor te Londen. Hiermee is een goed georganiseerde organisatie ontstaan. Alle boekwinkels zijn verantwoording schuldig aan het landelijke centrale kantoor. De landelijke kantoren op hun beurt dragen zorg voor de bevoorrading van de winkels en regelen het leveren van internetbestellingen en de uitwisseling van internationaal verkochte boeken tussen de verschillende centrale vestigingen.

In 2000 werden plannen gemaakt om in 2010 'overzee' te gaan naar de Verenigde Staten, Canada, Australië and Nieuw Zeeland. De bankcrisis aan het eind van 2008 zorgde er echter voor dat men deze plannen tijdelijk moest opschorten, in afwachting tot een beter investeringsklimaat.
De bankcrisis had een serieus effect op de waarde van de aandelen van SB. Wanneer mensen moeten bezuinigen, doen ze dat het eerst op boeken, tijdschriften en kranten. Deze zaken vormen de kernactiviteiten van SB. Het gevolg was dan ook dat de waarde van aandelen SB zakte en het beter werd geacht om tijdelijk niet te investeren in nieuwe markten. De zoektocht naar nieuwe markten heeft echter wel geleid tot nieuwe plannen.

De Raad van Bestuur was erg ouderwets in zijn ideeën over hoe een bedrijf geleid moet worden. Internet, nee, dat was niet de manier om handel te drijven. Een onafhankelijk consultancybureau bracht echter het advies uit dat het beter was dat SB een on-linewinkel zou lanceren, waarin meer werd verkocht dan alleen boeken en tijdschriften. Er is nu een internetwinkel op het gebied van reizen, waarbij meteen reisboeken en –gidsen worden aangeboden. En op de wat langere termijn zullen ook consumentenelektronica, fotoapparatuur en andere consumentengoederen aangeboden gaan worden.

## Organisatie:

Londen:
In het Londense hoofdkantoor is de Raad van Bestuur gevestigd en de eindverantwoordelijke Chief Information Officer (CIO), Chief Financial Officer (CFO), Chief Procurement Officer (CPO) and Chief Executive Officer (CEO).

Ieder land heeft een centraal kantoor dat verantwoordelijk is voor de verkopen in dat land. In de Europese vestigingen is de 'land'directeur verantwoording schuldig aan de regionale directeur te Amsterdam.

Bedrock-on-Thames UK:
UK Directeur is verantwoordelijk voor de Engelse boekwinkels. Er is ook een UK-CIO, CEO, CFO en een Local Information Security Officer (LISO).

Amsterdam:
1 EU directeur (EU m.u.v. UK)

EU CIO, CEO, CFO, CPO, LISO en de Corporate Information Security Officer (CISO).
Springbooks heeft een informatiebeveiligingorganisatie die deels gecentraliseerd is. Het overkoepelende beveiligingsbeleid wordt voorgeschreven vanuit de Londense vestiging. ISO 27001 en ISO 27002 zijn de standaarden die in alle landen toegepast worden.

In Londen is de Chief Information Security Manager eindverantwoordelijk voor de informatiebeveiliging in de organisatie. Hij zorgt ervoor dat informatiebeveiliging deel uitmaakt van de dagelijkse werkprocessen van alle SB medewerkers.

De LISO's zijn er verantwoordelijk voor dat het bedrijf het beveiligingsbeleid uitdraagt binnen de landelijke organisatie en dat aan landelijke wet- en regelgeving wordt voldaan.

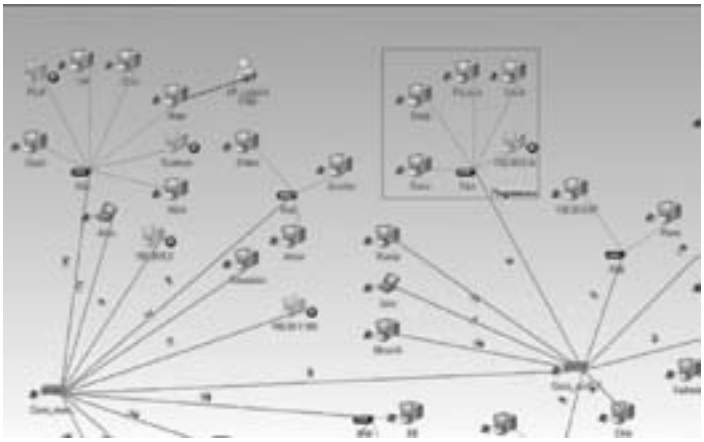
De LISO is ook verantwoordelijk voor de fysieke beveiliging van de SB-winkels en voor de bedrijfshulpverlening in de SB-winkels.

Iedere winkel kent een informatiebeveiligingsmedewerker. Dit is een medewerker met een opleiding op het gebied van informatiebeveiliging en bedrijfshulpverlening. Deze medewerker is verantwoordelijk voor de informatiebeveiliging in die winkel.

IT is centraal georganiseerd. Een Wide Area Network (WAN) verbindt alle winkels met elkaar. Het Springbooks WAN is een computernetwerk dat ervoor zorgt dat alle winkels internationaal met elkaar kunnen communiceren en dat zij van de centrale computervoorzieningen, zoals voorraadbeheer, gebruik kunnen maken. Dit is een verschil met het Local Area Network (LAN), waarop alle computers in een boekwinkel (binnen één enkel pand) zijn aangesloten.

Alle kassa's zijn aangesloten op het WAN. Ieder verkocht boek wordt aan de kassa gescand en de verkoop wordt onmiddellijk in de centrale database geregistreerd. Dit maakt het mogelijk om op ieder gewenst moment een overzicht te hebben van de actuele voorraad. Het bevoorraden van de winkels gebeurt op basis van de actuele verkoopcijfers. Zodoende kan SB ervoor zorgen dat goedlopende boeken altijd op voorraad zijn terwijl minder goed verkopende boeken snel leverbaar zijn.

Iedere medewerker heeft zijn eigen gebruikersnaam om in te loggen op het kassasysteem. Ieder verkocht boek wordt gekoppeld aan de verkoopmedewerker. In dezelfde database is veel klantinformatie aanwezig, zoals namen, adressen en creditcardinformatie.



Figuur 2.5 De WAN dataverbindingen tussen boekwinkels zoeken niet de kortste, maar de snelste route

Omdat in deze database klantinformatie is opgeslagen, is het zeer belangrijk dat men voldoet aan de nationale privacywetgeving, maar ook aan de interne beveiligingseisen. Onverwachte en ongeautoriseerde openbaarmaking van de vertrouwelijke informatie kan grote consequenties hebben voor het vertrouwen dat de klanten in Springbooks hebben.

# 3 Termen en definities

In dit hoofdstuk beschrijven we in het kort enkele belangrijke termen en definities met betrekking tot informatiebeveiliging. In appendix A is een uitgebreidere woordenlijst opgenomen.

**Bedrijfsmiddel**
Alles wat waarde heeft voor de organisatie
(ISO/IEC 13335-1:2004).

**Beschikbaarheid**
Beschikbaarheid waarborgt de betrouwbare en tijdige toegang tot data of computercapaciteit voor de medewerkers. Met andere woorden, beschikbaarheid garandeert dat de computersystemen beschikbaar zijn op het moment dat ze nodig zijn om de werkprocessen uit te kunnen voeren. Aanvullend hierop, betekent het voor de beveiligingsverantwoordelijke dat de beveiligingsmaatregelen die op computersystemen genomen zijn, ook daadwerkelijk naar behoren functioneren.[2] In hoofdstuk 4 komt dit onderwerp uitgebreid aan de orde.

**Vertrouwelijkheid**
De mate waarin de toegang tot informatie wordt beperkt tot een bepaalde groep gerechtigden, die inzage mag hebben in de data. Dit wordt ook wel exclusiviteit genoemd. Verlies van vertrouwelijkheid kan op veel manieren ontstaan, zoals het bewust verspreiden van gevoelige informatie over een bedrijf, of het onbewust lekken van informatie door fouten in autorisaties in applicaties of netwerkrechten.

**Beheersmaatregel**
Een middel om risico's te beheersen, waaronder beleid, procedures, richtlijnen, werkwijzen of organisatiestructuren, die administratief, technisch, beheersmatig of juridisch van aard kunnen zijn.
*Opmerking*: Beheersmaatregel wordt ook gebruikt als synoniem voor waarborging of tegenmaatregel.

**Risico**
Combinatie van de waarschijnlijkheid van een gebeurtenis en het gevolg ervan.

**Informatie**
Informatie is data die betekenis heeft voor de ontvanger van die informatie. Wanneer informatie in een computersysteem wordt opgeslagen, wordt daar meestal naar verwezen als data. Nadat de data is verwerkt, zal dit als informatie worden gezien.

**Informatieanalyse**
Informatieanalyse geeft een duidelijk beeld van hoe een organisatie met zijn informatie omgaat; hoe de informatie door de organisatie stroomt. In het Engels wordt dit 'flow' genoemd. Het Nederlandse woord informatiestroom is de beste benadering van de betekenis van het woord flow.

**Informatiemanagement**
Informatiemanagement beschrijft de wijze waarop een organisatie haar informatiestromen efficiënt plant, verzameld, organiseert, gebruikt en controleert. En informatiemanagement gaat ook over hoe de organisatie de informatie verspreidt en uitdraagt en de wijze waarop zij ervoor zorgt dat de waarde die de informatie in zich heeft ook ten volle benut wordt.

2 (The CISSP Prep Guide, Ronald L. Krutz / Russel Dean Vines).

**Faciliteiten voor het gebruik van informatie**
Iedere vorm van informatiesysteem, service of infrastructuur die gebruikt wordt om informatie op te slaan, te bewerken en te beheren en de fysieke middelen en locaties dienen daarvoor aanwezig te zijn.

**Informatiebeveiliging**
Het behouden van de vertrouwelijkheid, integriteit en beschikbaarheid van informatie. Daarbij kunnen ook andere eigenschappen, zoals authenticiteit, verantwoording, onweerlegbaarheid en betrouwbaarheid een rol spelen.

**Informatiebeveiligingsgebeurtenis**
De vastgestelde status van een systeem, dienst of netwerk die duidt op een mogelijke overtreding van het beleid voor informatiebeveiliging of een falen van beveiligingsvoorzieningen, of een tot dan toe onbekende situatie die relevant kan zijn voor beveiliging (ISO/IEC TR 18044:2004).

**Informatiebeveiligingsincident**
Afzonderlijke gebeurtenis of een serie ongewenste of onverwachte informatiebeveiligingsgebeurtenissen waarvan het waarschijnlijk is dat ze nadelige gevolgen voor de bedrijfsvoering hebben en een bedreiging vormen voor de informatiebeveiliging (ISO/IEC TR 18044:2004).

**Informatiebeveiligingsmanagement**
Alle gecoördineerde activiteiten die richting geven aan het beleid van een organisatie ten aanzien van risico's. Risicomanagement omvat normaal gesproken risicoanalyses, het nemen van beveiligingsmaatregelen, het accepteren van risico's tot een bepaald niveau en het communiceren van risico's binnen de organisatie (ISO/IEC Guide 73:2002).

**IT-voorzieningen**
Elk(e) systeem, dienst of infrastructuur voor informatieverwerking, of de fysieke locaties waarin ze zijn ondergebracht.

**Integriteit**
Integriteit gaat over de bescherming tegen ongeautoriseerde modificatie van (data in) software en hardware. Dit kan gebeuren door ongeautoriseerde en ongeautoriseerde medewerkers. Het gaat erom te waarborgen dat data betrouwbaar is.

**Beleid**
De formeel uitgesproken inrichting van informatiebeveiliging en de intentie van de directie hoe om te gaan met bedrijfsrisico's en de bescherming van de organisatie tegen informatiebeveiligingsrisico's.

**Risicoanalyse**
Systematisch gebruik van informatie om bronnen te identificeren en de risico's in te schatten (ISO/IEC Guide 73:2002).

**Risicobeoordeling**
Algeheel proces van risicoanalyse en risico-evaluatie (ISO/IEC Guide 73:2002).

**Risico-evaluatie**
Proces waarin het ingeschatte risico wordt afgewogen tegen vastgestelde risicocriteria om te bepalen in welke mate het risico significant is (ISO/IEC Guide 73:2002).

**Risicobeheer**
Gecoördineerde activiteiten om een organisatie sturing te geven en te bewaken met betrekking tot risico's (ISO/IEC Guide 73:2002)
*Opmerking*: Risicobeheer omvat doorgaans risicobeoordeling, risicobehandeling, risicoacceptatie en risicocommunicatie.

**Risicobehandeling**
Proces van keuze en implementatie van maatregelen om risico's te verlagen (ISO/IEC Guide 73:2002).
**Derde partij**
Persoon of entiteit die wat betreft de zaak in kwestie als onafhankelijk van de betrokken partijen wordt gezien (ISO/IEC Guide 2:1996).
**Bedreiging**
Potentiële oorzaak van een ongewenst incident dat een systeem of organisatie schade kan toebrengen (ISO/IEC 13335-1:2004).
**Kwetsbaarheid**
Zwakte van een bedrijfsmiddel of groep bedrijfsmiddelen die door een of meer bedreigingen kan worden benut (ISO/IEC 13335-1:2004).