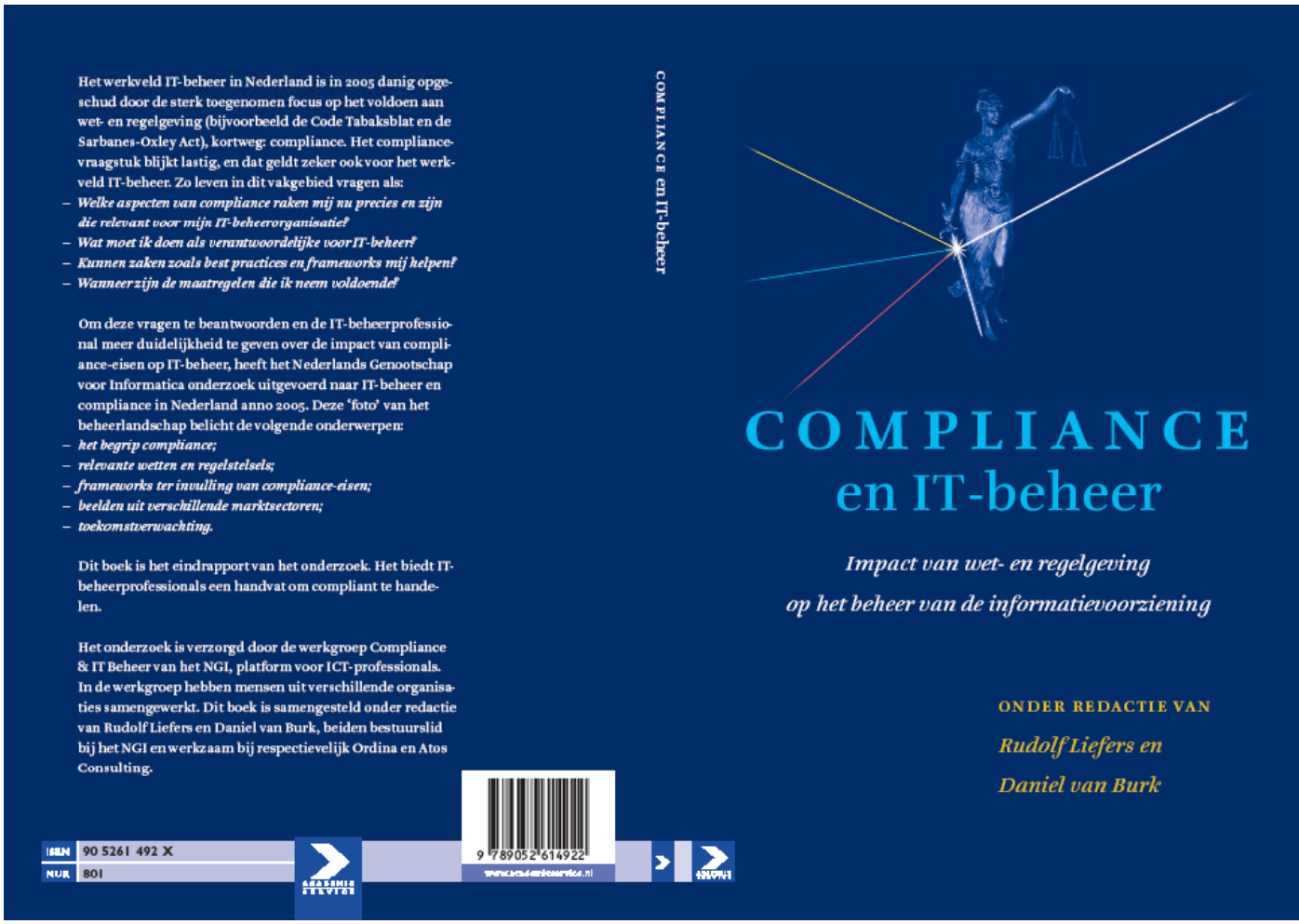
Onderstaand artikel is de bijdrage van Hans Keller aan het boek:

Compliance en IT Beheer 2006
Impact van wet- en regelgeving op het beheer van de informatievoorziening

Een verkenning van de actuele situatie van de impact die wet- en regelgeving hebben op het IT Beheer werkveld. Dit rapport is opgesteld door de werkgroep ‘Compliance & IT Beheer’ onderdeel van NGI afdeling Beheer, onder redactie van Rudolf Liefers en Daniel van Burk.



2 Compliance en haar belang

Er zijn veel juridische aspecten die op de een of andere manier direct of indirect IT raken. De organisatie dient te voldoen aan deze 'wet- en regelgeving'. Gezien het kader van de werkgroep (NGI, afdeling Beheer) en om het terrein in te perken gaat het onderstaande alleen over wet- en regelgeving die (direct of indirect) **invloed hebben op de inrichting en het beheer van IT-middelen**. Eisen aan functionaliteit (bijv. de aanwezigheid van een audittrail) zijn dus buiten beschouwing gelaten. Het overzicht beperkt zich niet tot Nederlandse wet- en regelgeving, maar bevat ook buitenlandse wet- en regelgeving, voor zover in Nederland opererende bedrijven hiermee te maken hebben of kunnen krijgen. (Voor een overzicht van (algemene) wet- en regelgeving, breder dan het IT-beheer willen we verwijzen naar 'IT-Recht, quick reference voor IT-auditors' van NOREA)

2.1 Definitie van compliance

Compliance is een beetje een modewoord, maar de inhoud is belangrijk. Hiermee wordt bedoeld "voldoen aan wet-en regelgeving". Een organisatie dient er derhalve zorg voor te dragen dat zij haar werkzaamheden uitvoert met in achtneming van wet- en regelgeving. Naast specifieke wet- en regelgeving is men ook gehouden om zich "als een goed huisvader" te gedragen. Dat betekent dat je ook behoort te doen wat in redelijkheid verwacht kan worden op basis van fatsoen, algemene kennis, etc. Daarmee raken we dan aan "corporate governance", zeg maar "behoorlijk bestuur". Met name wat "algemeen bekend" is, is hierbij van belang. Dan komen 'Code Tabaksblat', de 'Code voor informatiebeveiliging' e.d. in het vizier. Dit kan men typeren als zelfregulering. Hierbij zijn we uitgegaan van wet- en regelgeving waar in Nederland opererende organisaties mee van doen hebben. Dat is in de eerste plaats natuurlijk de Nederlandse wet- en regelgeving. De Europese wet- en regelgeving dient echter ook als zodanig aangemerkt te worden. Daarnaast hebben Nederlandse organisaties die een notering hebben aan de Amerikaanse beurs ook uitdrukkelijk te maken met de Amerikaanse wetgeving ten aanzien van het bestuur van de onderneming.

In de discussies over Compliance komt, mede naar aanleiding van de Sarbanes-Oxley Act (SOx), ook steeds nadrukkelijker het accent te liggen op de wijze van de uitvoering van het "behoorlijk bestuur", en/of de verantwoording daarover. Hierbij treden twee eisen op de voorgrond:

- het toepassen van een adequaat systeem ter borging van de daadwerkelijke uitvoering
- het daadwerkelijk toetsen van een dergelijk systeem (en daarmee ook "controleerbaar zijn" voor externen)

Definitie van Compliance voor dit boek

In de dagelijkse praktijk zijn vele definities en interpretaties van het begrip Compliance te vinden. De definitie van **Compliance** zoals deze in dit boek gehanteerd zal worden is:

- het voldoen aan wet-en regelgeving die op de organisatie van toepassing is
- het voldoen aan de gebruiken binnen de eigen branche
- het voldoen aan maatschappelijke normen
- op een gecontroleerde en controleerbare wijze.

2.2 Overzicht van wet- en regelgeving

Wie zich verdiept in wet- en regelgeving komt al snel tot de conclusie dat er een grote hoeveelheid aan wet- en regelgeving is waar organisaties mee te maken hebben. Een van de oorzaken hiervan is de hoge organisatiegraad van het maatschappelijk veld. Een willekeurige organisatie heeft al snel met een flink aantal spelers op haar veld te maken: overheden, brancheorganisaties, controlerende instanties. Daarbij is het niet toevallig dat ieder van de hier genoemde spelers in meervoudsvorm is genoemd. Bovendien, ieder van deze spelers maakt ook graag meerdere regelingen. En om de zaak te completeren zijn er ook nog de nodige organen die adviseren, normeren, certificeren, standaardiseren. Er is blijkbaar veel nodig om onze complexe maatschappij draaiende te houden.

Het moge duidelijk zijn dat we in het korte bestek van deze publicatie ons sterk zullen beperken en zullen proberen de hoofdlijnen weer te geven. De belangrijkste beperking is dat alleen wet- en regelgeving is opgenomen die (direct of indirect) **invloed heeft op de inrichting en het beheer van IT-middelen**. Eisen aan functionaliteit (bijv. de aanwezigheid van een audittrail) zijn dus buiten beschouwing gelaten. Voor het overzicht is de volgende vraagstelling uitgewerkt:

- Wie zijn de spelers?
- Welke wet- en regelgeving hebben zij uitgevaardigd?
- Wat zijn de effecten voor het beheer van IT?

Het onderdeel ‘wie zijn de spelers?’ is in de eerstvolgende paragraaf (2.2.1) uitgewerkt. De twee andere vragen (welke wetten en de effecten voor beheer) zijn uitgewerkt in de tabel van de daaropvolgende paragraaf (2.2.2).

2.2.1 Spelers inzake wet- en regelgeving

Bij de spelers, die wetten en regels opstellen die betrekking hebben op organisaties, hebben we het volgende onderscheid gemaakt:

- *Overheden*: De opstellers van wet- en regelgeving bij uitstek.
- *Toezichthouders*: Toezichthouders zijn weliswaar geen wetgevende instanties, maar stellen regels op die gelden als voorwaarde voor hun goedkeuring. Door hun ‘macht’ om al dan niet goed te keuren hebben die regels feitelijk de zwaarte van wetgeving. Immers, als je de ‘goedkeuring’ niet krijgt heeft dat ernstige consequenties voor de uitoefening van de werkzaamheden van de organisatie.
- *Zelfregulering*: De regels van brancheorganisaties gelden veelal als norm binnen het maatschappelijk verkeer. In specifieke gevallen kan/mag je daar wel van afwijken, maar dan alleen op basis van een goede argumentatie.
- *Maatschappelijk* verkeer: Het maatschappelijk verkeer levert van zichzelf ‘normen’, die niet altijd rechtstreeks in wetten of regels zijn vastgelegd maar algemeen zijn geaccepteerd. De twee belangrijkste figuren zijn hierbij “handelen als goed huisvader” en “handelen als bekwaam vakgenoot”, twee figuren waaraan ieder in een bepaalde positie aan dient te voldoen. (zie verder de toelichting aan het einde van deze paragraaf).

In onderstaande tabel volgt een lijst met spelers die in het onderzoek van de werkgroep Compliance & IT beheer naar voren zijn gekomen. Dit is geen uitputtende opsomming, maar is bedoeld om een beeld te schetsen van de spelers die er ten aanzien van Compliance zijn.

Spelers m.b.t. Compliance	Karakter
Overheden	
Nederlandse wetgever - rijksoverheid - provinciale overheid - gemeentes - Zelfstandige Bestuurs-Organen (ZBO's)	Wet en regelgeving (verplichtend)
Europese Unie	Wetgeving (verplichtend), direct danwel indirect door middel van implementatie in de Nederlandse wetgeving
Mondiaal, bijv. VS, Japan, etc.	Wet en regelgeving (verplichtend) in landen waar men opereert, gevestigd is, of aan de beurs genoteerd.
Toezichthouders	
Inspecties	Vanuit de wet, aanvullende regels en richtlijnen
Algemene rekenkamer (een zg. Hoog College van Staat)	Eisen vanuit een controle-perspectief (alleen voor de overheid zelf) (dwingend adviserend)
Zelfstandige Bestuurs-Organen (ZBO's)[1]	ZBO's zijn binnen hun domein zowel regelgevend als controlerend. (vanwege hun wettelijke taak: verplichtend)
Europese commissie	Vanuit Europese wetgeving, aanvullende regels en richtlijnen
Overig	
Accountants	Eisen vanuit controleperspectief (dwingend adviserend)
Brancheverenigingen	Zelfregulering: Brancheverenigingen stellen doorgaans eisen t.a.v. kwaliteit en bedrijfsvoering. (Er zijn meer dan 100 brancheorganisaties) Adviserend (tamelijk dwingend karakter)
Internationaal, bijvoorbeeld Securities and Exchange Committee (SEC)	Eisen vanuit controleperspectief (dwingend adviserend)
Maatschappelijk verkeer: personen en organisaties	- Goed huisvaderschap; (Een maatschappelijk vereiste) - Redelijk handelend vakgenoot (Een maatschappelijk vereiste) Zie onderstaande toelichting.

Toelichting

Goed huisvader

Er is niet zozeer een specifieke wettelijke definitie van "goed huisvaderschap" maar het is wel een juridisch figuur dat regelmatig in wetgeving wordt genoemd (zeker wanneer het gaat over het beheer van gelden of goederen), maar ook vaak een algemene werking heeft. Dergelijke terminologie, waaronder bijvoorbeeld ook termen

[1] (Een ZBO is een bestuursorgaan van de centrale overheid dat bij of krachtens de wet met openbaar gezag is bekleed en dat niet hiërarchisch ondergeschikt is aan de minister. Er zijn +/- 155 ZBO's)
Voorbeelden: Autoriteit Financiële Markten (AFM), Centrale organisatie Werk en Inkomen (CWI), College Bescherming Persoonsgegevens (CBP), College van Toezicht Auteursrechten en naburige rechten, De Nederlandsche Bank (DNB), Onafhankelijke Post- en Telecommunicatie Autoriteit (OPTA), etcetera

zoals 'redelijkheid en billijkheid' en 'zorgvuldigheid', valt dan ook onder het ongeschreven recht van het maatschappelijk verkeer. Ook in het kader van Tabaksblat en SOx komen deze termen vaak voor. Het betekend dat van bestuurders en directie verwacht mag worden dat ze de organisatie besturen "als goed huisvader", d.w.z. terughoudend, zonder (te) grote risico's, rekening houdend met alle belangen en besturen volgens de normen zoals die worden gehanteerd in het maatschappelijk verkeer.

Bekwaam vakgenoot
Het broertje (of zusje?) hiervan en voor het IT-beheer wellicht van groter belang is de figuur van de "de redelijk bekwaam en redelijk handelend vakgenoot". Op basis hiervan geldt dat een vakman/vakvrouw dient te handelen met zorg en voorzorg, overeenkomstig de stand van de kennis en kunde van zijn/haar vakgebied. Binnen de sector van het IT-beheer zou, als voorbeeld, op grond hiervan gesteld kunnen worden dat een beheerder of een beheerafdeling zorg dient te dragen voor adequate back-ups, ongeacht of hiertoe opdracht is gegeven aangezien het voorzien in een back-up faciliteit vanzelfsprekend geacht kan worden in het huidige maatschappelijk verkeer. (Het verdient uiteraard de voorkeur om dergelijke procedures vooraf duidelijk overeen te komen om discussie te voorkomen.) Naar het management-niveau betekent dit dat van een organisatie verwacht mag worden dat (ook) op het terrein van de IT een adequaat beheer plaatsvindt.

2.2.2 Wet- en regelgeving met impact op ICT van organisaties

In de onderstaande tabel is een overzicht gegeven van wet- en regelgeving waar je als IT Beheer organisatie aan hebt te voldoen. De meeste die genoemd zijn, zijn van toepassing op iedere organisatie, ongeacht de aard van je bedrijfsvoering of de doelstelling van de organisatie. Een aantal zijn specifiek voor een sector.

Het overzicht is als volgt opgebouwd:

Kolom: "Naam / soort wet":
Benaming van de betreffende wet

Kolom: "Soort eis":
Het blijkt dat, voor zover het de IT betreft de eisen vrijwel altijd liggen op het vlak van de beschikbaarheid, beveiliging of de integriteit. Vandaar deze onderverdeling. Als de eisen anders zijn, dan staan ze onder 'overig'. Vanzelfsprekend worden ook andere eisen gesteld (bijvoorbeeld de traceerbaarheid van transacties, maar die liggen op het applicatieve niveau en vallen daarmee buiten het kader van dit boek).

Kolom: "Karakter":
Hierbij is het volgende onderscheid gehanteerd:

Wet:	wettelijke verplichting waar je als organisatie aan hebt te voldoen (voorbeeld: bewaarplicht)
Regelgeving:	als je aanspraak wilt maken op rechten, dan moet je voldoen aan ... (voorbeeld: wil je rechten ontlenen aan de een of andere vorm van 'elektronische handtekening', dan moet aan bepaalde eisen zijn voldaan)
Advies:	heeft geen 'kracht van wet'. Echter, als het advies breed wordt toegepast wordt het wel een 'maatschappelijke norm'

Kolom "Consequenties IT-beheer"
Hierbij hebben we geprobeerd om op hoofdlijnen de belangrijkste consequenties voor het beheer van IT weer te geven.

Wet en regelgeving met impact op IT Beheer van organisaties						
Naam / soort wet	**Soort eis**				**Karakter**	**Consequenties IT beheer**
	beschikbaarheid	beveiliging	integriteit	overig		
Archiefwet 1995	bewaarplicht	beheer			wet	(1) Geldt voor archiefbescheiden in het algemeen. (2) De Archiefwet stelt algemene eisen aan het beheer van alle archiefbescheiden van de overheid
Burgerlijk Wetboek / Wetboek van koophandel			bewaar- en reproduceerbaarheidplicht		wet	(3) Hieraan kan alleen voldaan worden met een specifiek elektronisch archief. Een normale (systeem-)back-up zal doorgaans onvoldoende zijn. (4) Hoe langer hoe meer zal ook e-mail gerekend gaan worden tot de 'officiële' stukken. In rechtszaken nemen ze al vaak een zekere positie in. De eisen met betrekking tot de integriteit nemen dienovereenkomstig toe. (5) Wellicht moeten soms ook log-files hiertoe gerekend worden (6) Aandachtspunten: - aantoonbare authenticiteit - aantoonbaar ongewijzigd - toegankelijkheid (ondanks wijzigende technieken) (7) Voorwaarde: voldoende en beveiligde authenticatie
Belastingdienst			Bewaar- en reproduceerbaarheidplicht	eisen aan conversie	verplicht	Grotendeels hetzelfde als bovenstaande. (8) Conversie is apart aandachtspunt (vereist goedkeuring / instemming)
Wet elektronische handtekening		sleutels	niet manipuleerbaar, rechtens herleidbaar		regelgeving	(9) Naast adequate beveiliging zal een deugdelijke AO/IC van belang zijn voor rechtsgeldigheid. (10) Systemen waarbij de Administrator / Superuser / Root niet afgeschermd kunnen worden van de data zijn niet bruikbaar.
Wet computercriminaliteit (WCC)		adequate beveiliging			regelgeving	(11) Een, gegeven de aard van de organisatie, adequate beveiliging (12) Een groot deel van de 'criminaliteit' wordt gepleegd door de eigen medewerkers. Dus ook aandacht voor de 'interne beveiliging' (13) Logging en, logbestanden zijn van groot belang (14) In samenhang hiermee een goede identificatie (dus bijv. geen algemene gebruikers als 'guest' of 'user' ed)

Wet en regelgeving met impact op IT Beheer van organisaties						
Naam / soort wet	**Soort eis**				**Karakter**	**Consequenties IT beheer**
	beschikbaar-heid	beveiliging	integriteit	overig		
Wet bescherming Persoonsgegevens (WBP)		adequate be-veiliging	- melden - rechten geregi-streerde (inzage, correctie etc)	eisen aan uit-besteding	wet	(15) Extra nadruk op de AO/IC, zodat ook intern alleen de juiste personen met de juiste gegevens en de juiste bevoegdheden om kunnen gaan. (16) Extra nadruk op de rechten-structuur, waardoor beveiligingsmaatregelen tot op veldniveau kunnen worden doorgevoerd (17) Binnen veel organisaties (met name met MS-systemen) kan de systeembeheerder niet afgeschermd worden van de inhoud van de data. Op systeem-niveau komt men snel in strijd met de WPB (als er tenminste kritische gegevens worden verwerkt)
Databankenwet		doeltreffende voorzieningen			wet	(18) Beveiligingsmiddelen mogen een adequaat gebruik niet hinderen
Acountants-eisen / International Financial Reporting Standards (IFRS)		adequate be-veiliging	adequate integriteit	controleer-baarheid	regelgeving: voorwaarde voor controle	(19) Onbevoegde toegang tot systemen en bestanden (voor administraties die van belang zijn voor de controle) moet nagenoeg onmogelijk zijn (20) De automatiseringsomgeving en de systemen dienen de functiescheidingen binnen de organisatie af te (kunnen) dwingen (21) Systemen dienen ingericht te zijn op de uitvoering van controles (loggings, audi-trails, etc) (22) Adequate herstel- of reconstructie-mogelijkheden (van de administraties die voor de controle van belang zijn).
Tabaksblat / Nederlandse Corporate Governance Code, Sarbanes-Oxley (SOx)		controleerbaar en aantoon-baar voldoen aan eigen normen	controleer-baar en aantoon-baar vol-doen aan eigen nor-men		afhankelijk van situatie: verplicht of advies	(23) De belangrijkste kwaliteitsnormen dienen vastgelegd te zijn (24) Maatregelen voor beveiliging en integriteitshandhaving dienen te zijn gebaseerd op risico-analyse (25) De belangrijkste processen binnen een IT-afdeling dienen te zijn vastgelegd en te zijn voorzien van adequate maatregelen van controle (IT General Controls)
Wet elektronisch bestuurlijk verkeer					concept	(26) De wet is een aanvulling van de Awb en bevat regels over het verkeer langs elektronische weg tussen burger en bestuursorganen
Besluit voorschrift informatiebeveiliging rijksdienst 1994 (VIR)(ex art. 9 Besluit IVR 1990)		minimumei-sen voor be-leid			ministeriële regeling	(27) Op grond van VIR opstellen van een beleidsdocument informatiebeveiliging, informatiebeveiligingsplan. (28) De regeling stelt minimumeisen aan het te ontwikkelen beveiligingsbeleid binnen een ministerie. (29) Daarnaast stelt de regeling eisen aan de maatregelen die dit beleid in de praktijk moet brengen

Wet en regelgeving met impact op IT Beheer van organisaties						
Naam / soort wet	**Soort eis**				**Karakter**	**Consequenties IT beheer**
	beschikbaar-heid	beveiliging	integriteit	overig		
Wet bescherming Staatsgeheimen		informatiebe-scherming			wet	(30) Aanwijzen van verboden plaatsen ter bescherming van gegevens waarvan de geheimhouding is geboden in het belang van de staatsveiligheid
Wet elektronische handtekeningen	bewaarplicht	bewaring			wet	(31) De elektronische handtekening (EHT) heeft nu net als de handgeschreven handtekening wettelijke erkenning. De belemmeringen voor het vrije verkeer van diensten langs elektronische weg zijn hiermee weggenomen. (32) Bewaring en bewaartermijnen van EHT hebben betrekking op de elektronische handtekening zelf, de sleutel die is gebruikt, en vaak ook het gekwalificeerde certificaat. De bewaartermijn van de gegevens die de certificatie bewijzen varieert van min. 7 jaar (termijn AWR) tot het moment dat het (bewaar)belang van de bijbehorende informatie vervalt
Wet financiële dienstverlening (Wfd)			eisen aan de admini-stratieve organisatie		wet, van toe-passing op fi-nanciële dienstverle-ners zoals bijv. tussen-personen	(33) Indirect betekenen de eisen aan de administratieve organisatie dat dit ook voor de IT processen op orde moet zijn voor de relevante systemen
Nadere regeling gedragstoezicht ef-fectenverkeer (NRg 2002)	voorkomen van storingen en calamitei-ten	beveiliging van geauto-matiseerde gegevensver-werking	eisen aan de admini-stratieve organisatie en systeem van interne controle		regelgeving, van toepas-sing op effec-teninstellin-gen	(34) Art. 24 inzake administratieve organisatie en interne controle heeft als gevolg voor IT beheer dat voor relevante systemen ook de processen voor IT op orde moeten zijn. (35) Bijlage 4 onderdeel 27 gaat specifiek in op geautomatiseerde systemen. Er dient aandacht te zijn voor: • Beveiligingsmaatregelen • Functiescheiding • Business Continuity • Change control
Wet toezicht ver-zekeringsbedrijf (Wtv)			eisen aan de admini-stratieve organisatie en interne controle-procedures		wet, van toe-passing op verzekerings-instellingen	(36) Art. 70 van de Wtv. heeft als gevolg voor IT beheer dat voor relevante systemen ook de processen voor IT op orde moeten zijn

Wet en regelgeving met impact op IT Beheer van organisaties						
Naam / soort wet	**Soort eis**				**Karakter**	**Consequenties IT beheer**
	beschikbaarheid	beveiliging	integriteit	overig		
Regeling Organisatie en Beheersing (ROB), De Nederlandse Bank	risico-analyse en maatregelen voor continuïteit dienstverlening			maatregelen om in geval van outsourcing in control te blijven	regelgeving, van toepassing op financiële instellingen die onder toezicht van DNB vallen	(37) Secties 2.5 en 2.6 stellen dat IT organisaties van financiële instellingen: • Beleid moeten hebben ten aanzien van de beheersing van IT- en outsourcingrisico's • Systematisch analyses moeten uitvoeren van IT- en outsourcingrisico's • Organisatorische en administratieve procedures moet hebben voor de beheersing van IT- en outsourcingrisico's • Specifieke maatregelen moet nemen voor de beveiliging en continuïteit van IT • Voldoende garanties moet hebben voor een beheerste operatie in geval van outsourcing • Moet beschikken over een SLA en de mogelijkheid moet hebben om een audit uit te voeren bij de dienstverlenende organisatie • Moet procedures hebben voor het toezicht op de dienstverlenende organisatie
Basel II	risicobeheersingsmaatregelen voor de continuïteit van de dienstverlening				regelgeving, van toepassing op kredietinstellingen	(38) Vanuit het Basel Committee zijn High-level principles opgesteld voor Business Continuity. Dit zijn zeven principes waarvan er zes van toepassing zijn op financiële instellingen en 1 op financiële autoriteiten.
Wet melding ongebruikelijke transacties (MOT)	bewaarplicht 5 jaar				wetgeving	(39) Gegevens omtrent meldingen van ongebruikelijke transacties dienen voor een periode van vijf jaar na de melding bewaard te blijven. Brengt dus eisen ten aanzien van backup en restore met zich mee.
De Code voor Informatiebeveiliging (BS 7799)		adequate beveiliging			advies	(40) Normenkader voor beveiliging van informatie, de facto standaard en daardoor voor veel bedrijven impliciete eis
Goed huisvaderschap	alle eisen 'in redelijkheid en billijkheid'	idem	idem	idem	maatschappelijke norm	(41) De eisen aan het IT-beheer dienen aan te sluiten bij wat in redelijkheid van haar verwacht mag
Redelijk handelend vakgenoot	alle eisen 'in redelijkheid en billijkheid'	idem	idem	idem	maatschappelijke norm	(42) De kwaliteit van het IT-beheer dient te voeldoen aan de (vigerende) normen van het vakgebied (dit betreft meer dan alleen de beveiliging en de integriteit, bijv. ook 'het bijhouden en implementeren van nieuwe technieken, als dat uit het oogpunt van vakmanschap vereist is')

Opmerkingen bij de genoemde wet- en regelgeving:
De wet- en regelgeving die voor IT Beheer organisaties gelden richten zich voornamelijk op de beschikbaarheid, beveiliging en/of de integriteit van de gegevens. Slechts in een beperkt aantal gevallen worden concrete normen gegeven. Deze betreffen dan voornamelijk de bewaarplicht. Alleen de belastingdienst stelt aanvullende regels met betrekking tot conversie.

Het ontbreken van concrete normen betekend niet dat er geen normen zijn. Gerefereerd moet worden aan twee algemene normen:
- gangbaar, in zijn algemeenheid en gangbaar binnen de eigen sector of branche (een algemene maatschappelijke norm (voorbeeld: back-ups)
- doeltreffend / adequaat gemeten naar het belang van het object (lees ‘het maatschappelijk’ belang) (dit ligt in het verlengde van het bovenstaande, maar kan situatiespecifiek zwaardere normen opleveren)