Internet-technologie, toezicht en de rol van IT-auditors bij financiële instellingen

Mw. B. Beugelaar RE RA

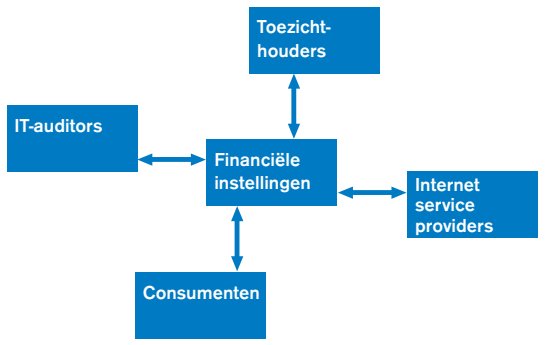
**Door zowel De Nederlandsche Bank (DNB) als de Stichting Toezicht Effectenverkeer (STE) is regelgeving opgesteld ten aanzien van het aanbieden van diensten aan cliënten door middel van Internet.
Dit artikel bevat een beschrijving van de door de toezichthouders gestelde eisen ten aanzien van Internet. Tevens worden hierbij de verschillen en overeenkomsten in regelgeving tussen beide toezichthouders toegelicht en wordt een evaluatie van de betreffende regelgeving beschreven.**

Inleiding

Het verlenen van financiële diensten via Internet is een ontwikkeling die zich niet meer weg laat denken binnen de huidige maatschappij. De variëteit in de soort van dienstverlening neemt toe naarmate op het gebied van de informatietechnologie ook steeds meer mogelijkheden aanwezig zijn. Momenteel worden via Internet onder meer financiële diensten aangeboden voor het uitvoeren van betalingsopdrachten, het opvragen van informatie omtrent financiële diensten en het afsluiten van effectenorders.
Een nog verdergaande vorm is het opzetten van een Internet-bank. Hiervoor geldt dat deze Internet-bank via een website diverse financiële diensten aanbiedt zonder dat zij fysiek in het betreffende land gevestigd is. Met name voor instellingen die het streven hebben om diensten over de landsgrenzen heen aan te bieden zou deze vorm van Internet-banking uitkomsten kunnen bieden, zonder dat dit extra kosten van huisvesting met zich meebrengt. Duidelijk zal zijn dat dergelijke activiteiten ook van invloed zijn op de rol die de toezichthouders spelen en de rol die de IT-auditor daarbij kan vervullen. Toezichthouders hebben derhalve ook niet stil gezeten en door hen zijn regelgeving en beleidsregels opgesteld die betrekking hebben op het inzetten van nieuwe technologieën en media door financiële instellingen. In dit artikel zal een overzicht en evaluatie worden gegeven van de beschikbare regelgeving met betrekking tot het gebruik van Internet, de rol van de toezichthouders en van de IT-auditor.

Veranderingen in regelgeving als gevolg van Internet-technologie

Het gebruik van Internet betekent veelal dat landsgrenzen vervagen en daardoor ook niet duidelijk is welke wetgevingsaspecten van toepassing zijn. Om financiële diensten aan te kunnen bieden geldt in Nederland dat een financiële instelling in het bezit moet zijn van een vergunning van De Nederlandsche Bank (DNB). Dergelijke instellingen vallen onder het toezichtsregime van DNB. In de situatie van een Internet-bank zou in feite hetzelfde moeten gelden, afhankelijk van de regels van de centrale bank in een bepaald land. Echter, indien een Internet-bank zich vestigt in een land waar de toezichthouder minimale eisen stelt ten aanzien van de afgifte van een vergunning voor activiteiten, dan zouden daar voor cliënten risico's uit voort kunnen vloeien als malafide organisaties participeren in de Internet-bank. Deze risico's zijn ook onderkend door DNB, die hiertoe Beleidsregels Media WtK 1992 heeft uitgevaardigd. Wat DNB onder het begrip media verstaat, wordt toegelicht in de paragraaf 'Aanwezige regelgeving'. Kort samengevat stelt DNB in de beleidsregels dat een vergunning vereist is indien het bedrijf van kredietinstelling via media wordt uitgeoefend in of vanuit Nederland, ongeacht in welk land het via media actief is. De beleidsregels zijn derhalve van toepassing op een in Nederland gevestigde Internet-bank of een buitenlandse bank die diensten aanbiedt op de Nederlandse markt.
Een ander vraagstuk betreft de situatie in hoeverre de belangen van Nederlandse consumenten die gebruikmaken van een 'buitenlandse' Internet-bank, worden beschermd. Hierop wordt in de beleidsregels geen antwoord gegeven, waardoor leemten kunnen ontstaan in de bescherming van consumenten tegen aangeboden diensten. Denk daarbij aan het voorbeeld van malafide Internet-banken die zich vestigen in landen waar minimaal tot geen toezicht van een centrale bank van toepassing is.
Concluderend kan worden gesteld dat de huidige regelgeving vooralsnog niet voorziet in het op de hoogte stellen van consumenten inzake het toepasselijke toezichtsregime op Internet-banken, alsmede de kwaliteit daarvan. Bij het informeren van consumenten ten aanzien van de integriteit van de door een Internet-bank aangeboden financiële diensten kan de IT-auditor een rol spelen. Door de IT-auditor zou een 'kwaliteitscertificaat' afgegeven kunnen worden die een oordeel geeft over de uitingen van een bancaire instelling op Internet. Dit kwaliteitscertificaat zou waarborgen kunnen bieden betreffende bijvoorbeeld de integriteit en authenticiteit van de via de Internet-bank aangeboden financiële diensten. De consument kan hieraan meer zekerheden ontlenen.



Figuur 1. Betrokken partijen bij het verlenen van diensten via Internet.

Gesteld kan worden dat bij het handeldrijven via Internet diverse partijen betrokken kunnen zijn. Zie figuur 1. Deze partijen vervullen alle een bepaalde rol. De financiële instellingen bieden via websites financiële diensten aan consumenten aan. Om dit te kunnen doen maken zij gebruik van de diensten die door Internet service providers worden aangeboden. Met deze service providers dienen contractueel afspraken te worden gemaakt omtrent onder meer de gewenste beschikbaarheid en performance van bijvoorbeeld een website. De toezichthouders hebben een rol in het kader van het houden van toezicht uit hoofde van de regelgeving. IT-auditors kunnen vanuit verschillende aandachtsgebieden een functie vervullen. Zij kunnen adviserend en uitvoerend optreden bij het formuleren van de wensen en eisen die mede vanuit het oogpunt van beveiliging aan een website of webapplicatie naar voren worden gebracht c.q. dienen te worden gesteld. Daarnaast worden zij uit hoofde van regelgeving geacht een verklaring te geven omtrent opzet en werking van de betrokken systemen en administratieve organisatie van bijvoorbeeld beursorderlijnen via Internet. Op dit laatste wordt in de hiernavolgende paragrafen nog nader ingegaan.

Aanwezige regelgeving

Bij financiële instellingen wordt toezicht uitgeoefend door DNB en/of de Stichting Toezicht Effectenverkeer (STE). Beide toezichthouders hebben onderkend dat de tot voor kort geldende regelgeving niet voorzag in het inspelen op nieuwe ontwikkelingen in elektronisch zakendoen zoals die binnen de financiële instellingen plaatsvonden. Derhalve hebben zij nieuwe regelgeving opgesteld. Dit artikel zal met name ingaan op de door DNB en de STE opgestelde regelgeving betreffende Internet.

Door toezichthouders is als gevolg van het groeiend gebruik van Internet (onder meer in het effectenverkeer) de in tabel 1 vermelde regelgeving opgesteld.

Tabel 1. Regelgeving door toezichthouders inzake Internet.

DNB	STE
* Beleidsregels Media WtB * Beleidsregels Media WtK 1992	* Beleidsnotitie 99-0003 inzake het Internet in relatie tot het toezicht op het effectenverkeer in Nederland. Deze regelgeving dient gerelateerd te worden aan de Wte 1995, Bte 1995 en de Nadere Regeling toezicht effectenverkeer 1999 (NR 1999)

In de volgende paragrafen zal deze regelgeving worden toegelicht.

Door DNB opgestelde Beleidsregels Media WtB en Media WtK 1992

Door DNB zijn beleidsregels opgesteld waarin aangegeven is dat een vergunning vereist is indien het bedrijf van kredietinstelling via media wordt uitgeoefend in of vanuit Nederland, ongeacht in welk land het via media actief is (Beleidsregels Media WtK 1992).
Ook zijn voor de beleggingsinstellingen bepalingen opgenomen in welke situaties beleggingsinstellingen over een vergunning dienen te beschikken indien zij gebruikmaken van Internet of andere media (Beleidsregels Media WtB).

Onder de term media wordt door DNB verstaan 'Internet, telefoon, televisie, fax en andere elektronische communicatiemiddelen, alsmede kranten, tijdschriften, direct mail, folders en andere papieren communicatiemiddelen'.
Onder de term Internet wordt in deze beleidsregels verstaan 'de verscheidene methoden om informatie elektronisch te distribueren, waaronder het World Wide Web, bulletin boards, e-mail, personal broadcast network en push-media'.
Geconcludeerd kan worden dat het begrip media zeer ruim gedefinieerd is en derhalve op velerlei wijzen van aanbieden van diensten van toepassing is.

Een belangrijke vraag die vanuit de regelgeving beantwoord dient te worden is of een instelling op de Nederlandse markt actief is. Het antwoord op deze vraag hangt af van de vraag of de door middel van media uitgeoefende activiteiten op inwoners van Nederland zijn gericht.
Door zowel DNB als de STE worden de hiernavolgende indicatoren gehanteerd om te bepalen of de door middel van Internet uitgeoefende activiteiten op inwoners van Nederland zijn gericht:
* het niet gebruiken van disclaimers of een gebrekkige handhaving daarvan;
* het niet opnemen van een lijst van landen waarop de activiteiten uitdrukkelijk zijn gericht, of de gebrekkige handhaving daarvan;
* het gebruik van Nederlands als voertaal bij de activiteiten;
* adressering (bijvoorbeeld via e-mail) aan ingezetenen van Nederland;
* informatieverschaffing over het Nederlandse fiscale regime;
* informatieverschaffing over een buitenlands fiscaal regime ten opzichte van Nederland;
* verwijzingen naar of informatieverschaffing over Nederlandse wetten;
* 'hyperlinks' op Internet waarmee de gebruiker naar een website wordt geleid waar effectendiensten worden aangeboden dan wel verricht.

Bovenstaande wordt door DNB en de STE per situatie bepaald. Een financiële instelling dient derhalve voor zichzelf vast te stellen welke indicatoren van toepassing zijn om te kunnen vaststellen of de beleidsregels op haar van toepassing zijn.

Evaluatie van de door DNB opgestelde beleidsregels

Opvallend is dat de regelgeving van DNB alleen ingaat op de formele aspecten van regelgeving, dat wil zeggen het beschikken over een vergunning indien de activiteiten vanuit Nederland worden aangeboden dan wel indien zij op de inwoners van Nederland zijn gericht. De regelgeving stelt geen eisen aan de wijze waarop de geautomatiseerde informatiesystemen en de maatregelen van AO/IC rondom Internet-toepassingen dienen te worden opgezet.
Door DNB is in 1988 het Memorandum omtrent de betrouwbaarheid en continuïteit van geautomatiseerde gegevensverwerking in het bankwezen uitgevaardigd. Dit Memorandum gaat echter niet expliciet in op de eisen die gesteld dienen te worden aan Internet-toepassingen. In de tijd waarin het Memorandum werd opgesteld, waren de bedrijfssystemen van banken veelal nog afgeschermd van de buitenwereld (zogenoemde gesloten systemen). Daarbij speelt tevens dat sinds het uitbrengen van het Memorandum in 1988 daarin overigens geen aanpassingen meer zijn aangebracht. Wel wordt in het Memorandum reeds ingegaan op de ontwikkeling van het via datacommunicatie aanbieden van transacties door derden en de in opkomst zijnde integratie met de geautomatiseerde systemen. De connectie van bedrijfssystemen met de buitenwereld via Internet brengt echter nieuwe risico's met zich mee die de betrouwbaarheid en continuïteit van financiële instellingen kunnen beïnvloeden.
Het Memorandum bevat een aantal algemene uitgangspunten ten aanzien van de te treffen maatregelen van beveiliging en continuïteit van de geautomatiseerde gegevensverwerking. Deze uitgangspunten worden door DNB als richtinggevend betiteld. Voor wat betreft datatransmissie met behulp van communicatienetwerken is aangegeven dat gevoelige informatie tijdens transport tegen ongeautoriseerd raadplegen of veranderen beveiligd dient te zijn. Dit is een uitgangspunt dat onverkort van toepassing verklaard kan worden op kritieke Internet-transacties. Aan de door een financiële instelling te treffen technische maatregelen worden in het Memorandum echter geen concrete eisen ten aanzien van de beveiliging en continuïteit gesteld, aangezien DNB niet de intentie heeft gehad om dit gedetailleerd voor te schrijven. De wijze van technische inrichting van de (Internet-)systemen wordt door DNB overgelaten aan het verantwoordelijke management. De vraag doet zich hierbij echter voor in welke mate het Memorandum met algemene eisen ten aanzien van betrouwbaarheid en continuïteit nog actueel is gelet op de veranderende inzet van informatietechnologie binnen de financiële wereld en de snelheid waarmee veranderingen plaatsvinden. Aspecten zoals 'time-to-market' spelen een steeds belangrijker rol bij financiële instellingen, waardoor het risico bestaat dat bepaalde waarborgen die normaliter aanwezig waren in het traject van ontwikkelen, implementeren en beheren van applicaties, besturingssystemen en netwerken als hinderlijk worden ervaren en niet voldoende aandacht krijgen, met alle risico's van dien.

Beleidsregels STE inzake Internet-toepassingen

Door de STE worden in de 'Beleidsnotitie 99-0003 inzake het Internet in relatie tot het toezicht op het effectenverkeer in Nederland' (hierna verder aangeduid als Beleidsnotitie Internet) en de 'Nadere Regeling toezicht effectenverkeer 1999 (NR 1999)' meer expliciet eisen gesteld aan de geautomatiseerde gegevensverwerking en de maatregelen van AO/IC betreffende Internet-toepassingen.

Voor het van toepassing kunnen verklaren van de Beleidsregels Internet op een financiële instelling dient ook hier een antwoord te worden verkregen op de eerder in deze paragraaf genoemde indicatoren.

In deze subparagraaf wordt een uiteenzetting gegeven van de in de Beleidsnotitie Internet en de NR1999 opgenomen eisen ten aanzien van de administratieve organisatie en de beveiliging betreffende geautomatiseerde informatiesystemen.

Beheermaatregelen betreffende de geautomatiseerde systemen

Deze subparagraaf bevat de beheermaatregelen voor effecteninstellingen, met inbegrip van kredietinstellingen die het effectenbedrijf uitoefenen. De vereiste maatregelen betreffen uitsluitend de eisen die door de STE gesteld worden aan geautomatiseerde systemen en het via Internet aanbieden van effectendiensten. De overige eisen die binnen de organisatie van een effecteninstelling getroffen dienen te worden ten aanzien van de administratieve organisatie en interne controle moeten door de accountant worden beoordeeld. Voorbeelden hiervan betreffen de eisen die door de STE worden gesteld aan onder meer de inhoud van het emissieprospectus, de vermogensscheiding, de cliëntovereenkomst en gedragsregels. Derhalve zijn deze eisen in dit artikel niet verder uitgewerkt. De betreffende eisen zijn door de STE opgenomen in de NR 1999.

De betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking moet gewaarborgd zijn.

Als uitgangspunt geldt dat effecteninstellingen die gebruikmaken van geautomatiseerde gegevensverwerking zodanige maatregelen en procedures dienen te treffen dat de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking gewaarborgd is. De STE stelt in haar Beleidsnotitie Internet dat alvorens met de activiteiten via Internet gestart mag worden, de normen waaraan getoetst gaat worden vooraf ter goedkeuring aan de STE moeten worden voorgelegd. Deze normen zijn hierna verder uitgewerkt.

Onderstaande normen ten aanzien van de geautomatiseerde systemen zijn overgenomen uit de Beleidsnotitie Internet en de NR 1999 van de STE.

Nr.	Door effecteninstelling te treffen maatregelen uit hoofde van de NR 1999
	A. Problem- en change-managementprocedures
1.	De effecteninstelling dient over een adequate change-managementprocedure te beschikken die waarborgen biedt ten aanzien van de integriteit van de programmatuur en de automatiseringssystemen. Dit ter voorkoming dat ongeautoriseerde implementatie van nieuwe programmatuur en automatiseringssystemen plaatsvindt, dan wel ongeautoriseerde wijzigingen in bestaande programmatuur en systemen worden aangebracht.
2.	Maatregelen dienen aanwezig te zijn die waarborgen dat een scheiding aanwezig is tussen de ontwikkel-, test-/acceptatie- en productieomgeving ter waarborging van de betrouwbaarheid van de programmatuur en automatiseringssystemen.
3.	Maatregelen dienen aanwezig te zijn die waarborgen dat nieuw te implementeren modules door gebruikers worden getest alvorens zij in productie worden genomen.
4.	Een procedure dient aanwezig te zijn die voorziet in het detecteren, registreren, analyseren en oplossen van problemen die zich voordoen in het geautomatiseerde proces.
	B. Configuratiemanagement
1.	Procedures dienen aanwezig te zijn ter registratie van de in productie zijnde programmatuur en netwerkcomponenten. Deze procedures dienen ter bewaking dat de productieomgeving gebruikmaakt van de juiste programmatuur, stamgegevens en geprogrammeerde controles.
	C. Logische toegangsbeveiliging
1.	Procedures dienen aanwezig te zijn die waarborgen dat functiescheiding aanwezig is binnen de geautomatiseerde systemen, alsmede dat deze overeenkomstig de vastlegging volgens de competentietabellen heeft plaatsgevonden.
2.	Procedures dienen aanwezig te zijn ten aanzien van het registreren en toekennen van bevoegdheden aan medewerkers. Hierbij dient onder meer gedacht te worden aan het toekennen van bevoegdheden op basis van 'need to know' en 'need to have', alsmede een adequaat passwordbeheer en beheer van de competentietabellen.
3.	Het geautomatiseerde systeem dient te voorzien in geprogrammeerde controles die de juistheid van de ingevoerde gegevens toetsen op betrouwbaarheid. Tot deze controles behoren onder meer de bestaanbaarheidscontroles, redelijkheidscontroles en controles op doorlopende nummering.
	D. Fysieke toegangsbeveiliging
1.	Maatregelen dienen te worden getroffen die waarborgen dat de fysieke toegang tot de gegevensdragers en andere computerfaciliteiten is afgeschermd voor onbevoegden.
	E. Back-up, recovery en uitwijk
1.	De effecteninstelling dient te beschikken over een herstelprocedure die in geval van storingen en calamiteiten voorziet in handleidingen en procedures op basis waarvan de geautomatiseerde gegevensverwerking kan worden hersteld.
2.	Ten behoeve van de onderhoudbaarheid van de systemen dienen adequate documentatie en gebruikershandleidingen aanwezig te zijn en dienen deze onderhouden te worden.
3.	Procedures dienen aanwezig te zijn die voorzien in het maken van back-ups.
4.	Maatregelen dienen te zijn getroffen die voorzien in het kunnen uitwijken naar een andere locatie zodat de continuïteit in de geautomatiseerde gegevensverwerking gewaarborgd is.

Additionele beveiligingseisen in het kader van het effectenverkeer via Internet

Naast de bovengenoemde eisen betreffende de geautomatiseerde gegevensverwerking uit hoofde van de NR 1999 gelden voor wat betreft de Internet-toepassingen de hierna volgende additionele beveiligingseisen ten aanzien van de Internet-transacties.

Nr.	Door effecteninstelling te treffen maatregelen uit hoofde van de Beleidsnotitie Internet
1.	Maatregelen dienen te worden getroffen die de vertrouwelijkheid van de door cliënten aangeleverde transacties via Internet, alsmede hun privacy waarborgen.
2.	Maatregelen dienen te worden getroffen ter waarborging van de identificatie en authenticatie van de cliënten en de door hen uitgevoerde transacties.
3.	Maatregelen dienen te worden getroffen ter preventie van het kunnen ontkennen van een aangegane transactie door cliënten.

Organisatorische maatregelen betreffende het effectenverkeer via Internet
Aanvullend dienen binnen de organisatie de volgende organisatorische maatregelen te worden getroffen.

Nr.	Door effecteninstelling te treffen maatregelen uit hoofde van de Beleidsnotitie Internet
1.	Eerste identificatie van de cliënt en het afsluiten van een cliëntovereenkomst mogen niet exclusief via Internet plaatsvinden. De cliëntovereenkomst dient te zijn voorzien van een originele handtekening en datum en dient in originele vorm te worden bewaard en mag dus niet uitsluitend op elektronische wijze worden bewaard.
2.	De effecteninstelling dient de cliënten onder meer via haar website te informeren omtrent de getroffen beveiligingsaspecten en -eisen.
3.	De cliënt dient toestemming te verlenen voor het gebruik van Internet.
4.	Ten aanzien van het via Internet publiceren van advertenties geldt dat een effecteninstelling aan haar cliënten op passende wijze gegevens en bescheiden verstrekt die nodig zijn voor de adequate beoordeling van de door de effecteninstelling aangeboden diensten en de financiële instrumenten waarop deze diensten betrekking hebben.
5.	Aan cliënten dient een schriftelijke effectennota ter beschikking te worden gesteld.

Evaluatie van de STE-regelgeving inzake Internet

De door de STE opgestelde eisen zijn globaal geformuleerd en geven niet expliciet aan op welke wijze bepaalde aspecten dienen te worden ingericht, dan wel dat het zou gaan om algemene uitgangspunten. Dit brengt het probleem met zich mee dat deze eisen, voor zowel de financiële instelling als de IT-auditor, ruimte laten voor interpretatie. Derhalve blijkt in de praktijk dat het niet altijd eenvoudig is om op basis van deze regelgeving normen te definiëren.
De door financiële instellingen aan de STE ter goedkeuring voorgelegde normen zijn vaak meeromvattend op het gebied van beveiliging en continuïteit dan bovenstaande normen. Ook de STE zelf stelt in de praktijk meer geconcretiseerde normen die niet direct zijn terug te vinden in de Beleidsnotitie Internet en de NR 1999. Hierdoor ontstaat veel onduidelijkheid zowel bij de financiële instelling zelf als bij de IT-auditor. Als gevolg van deze onduidelijkheid wordt vertraging opgelopen met het op de markt brengen van de dienst omdat nog relatief veel tijd besteed moet worden aan de onderlinge afstemming van de opgestelde normen met die van de STE.

Een financiële instelling dient in principe primair zelf, op basis van een risicoanalyse, te bepalen welke risico's gelopen worden met Internet en welke beveiligingseisen en maatregelen van AO/IC als relevant worden ervaren om bepaalde financiële diensten via Internet aan te bieden. Het beveiligen dient dus niet alleen plaats te vinden omdat dit vanuit de regelgeving wordt geëist maar ook om eigen cliënten bepaalde waarborgen te bieden, bijvoorbeeld ten aanzien van hun privacy, of om de integriteit en continuïteit van de interne bedrijfssystemen te waarborgen. Daarom dient bij het uitwerken van de risicoanalyse en het definiëren van de eisen tevens rekening te worden gehouden met de intern geldende eisen ten aanzien van de beveiliging en continuïteit van Internet-toepassingen.
Zoals in de inleiding al gemeld, worden ook betaaldiensten reeds via Internet aangeboden, namelijk via de zogenoemde electronic-bankingapplicaties. Voor deze applicaties zijn door banken reeds eisen geformuleerd voor wat betreft de betrouwbaarheid en de continuïteit. Deze eisen zouden een goed uitgangspunt kunnen vormen bij het verder uitwerken van eisen voor Internet-toepassingen die effectentransacties verwerken.

De door de STE geformuleerde eisen zijn merendeels gericht op de beheerprocedures en de organisatorische maatregelen ten aanzien van de Internet-toepassing. De in tabel 2 opgenomen eisen kunnen in aanvulling op de door de STE geformuleerde eisen getroffen worden om een betrouwbare en continue Internet-IT-infrastructuur te realiseren:
1. de beveiliging van de IT-infrastructuur; dat wil zeggen het opstellen van eisen ten aanzien van de inrichting van de technische componenten bij Internet-toepassingen;
2. additionele beheerprocedures;
3. het uitwerken van een Internet-beveiligingsbeleid.

In figuur 2 is zichtbaar welke aandachtsgebieden door de STE reeds zijn uitgewerkt en welke additioneel door de effecteninstelling getroffen kunnen worden ter waarborging van de betrouwbaarheid en continuïteit van de Internet-toepassing.

Rol van de IT-auditor

De STE acht de beveiligingsaspecten met betrekking tot het via Internet aanbieden van effectendiensten dermate zwaarwegend dat voor de goedkeuring van een dergelijk systeem een onafhankelijke EDP-audit uitgevoerd dient te worden naar de opzet en de werking van de betrokken systemen en de administratieve organisatie, alsmede dat een verklaring hierover wordt afgegeven. Hiertoe dient de cliënt of de IT-auditor (in opdracht van de cliënt) op basis van de door de STE geformuleerde eisen een normenkader op te stellen en dit dient door de cliënt ter goedkeuring te worden voorgelegd aan de STE, alvorens met de nieuwe activiteit gestart mag worden. Indien een cliënt het normenkader zelf opstelt bevelen wij aan om dit normenkader af te stemmen met de onafhankelijke IT-auditor aan wie de opdracht verstrekt is om de verklaring af te geven.

Aangezien het bij veel financiële instellingen gaat om een nieuw op te zetten activiteit is het veelal nog niet mogelijk om direct een oordeel af te geven omtrent de werking van de betrokken systemen en de daarmee samenhangende organisatie. In eerste instantie zal een organisatie beschrijven op welke wijze de toepassing is opgezet en ingericht en welke AO/IC-maatregelen ter beheersing van de adequate werking van het systeem getroffen worden. De IT-auditor zal de aandacht dan ook richten op

1 Aandachtsgebieden van aanvullende eisen ten aanzien van de beveiliging en continuïteit van de IT-infrastructuur zijn onder meer:

A Opstellen van een configuratieoverzicht met de topologie van het netwerk.
B Fysieke beveiliging van computerruimten waar Internet-systemen zich bevinden.
C Opstellen van een beleid waarin aangegeven wordt welke Internet Services (zowel ingaand als uitgaand) toegestaan zijn.
D Het implementeren van filtering-regels op toegestaan verkeer via routers en firewall.
E Opstellen van security baselines ten aanzien van de IT-componenten.
F Opstellen van procedures ten aanzien van audit, logging en monitoring van kritieke netwerkcomponenten.

2 Additionele beheerprocedures kunnen onder meer getroffen worden met betrekking tot de volgende aandachtsgebieden:

A Procedures ten aanzien van Service level Management met cliënten, Internet service providers, leveranciers, de gebruikers- en IT-organisatie.
B Procedures ten aanzien van Security Management, bijvoorbeeld een Security Officer benoemen.
C Procedures ten aanzien van Availability Management, waaronder adequate back-up, recovery en uitwijkmaatregelen.
D Procedures ten aanzien van Operations Management; waaronder het monitoren van het operationeel zijn van de Internet-verbindingen.
E Procedures ten aanzien van Performance Management; waaronder het beoordelen van performance van netwerkcomponenten.

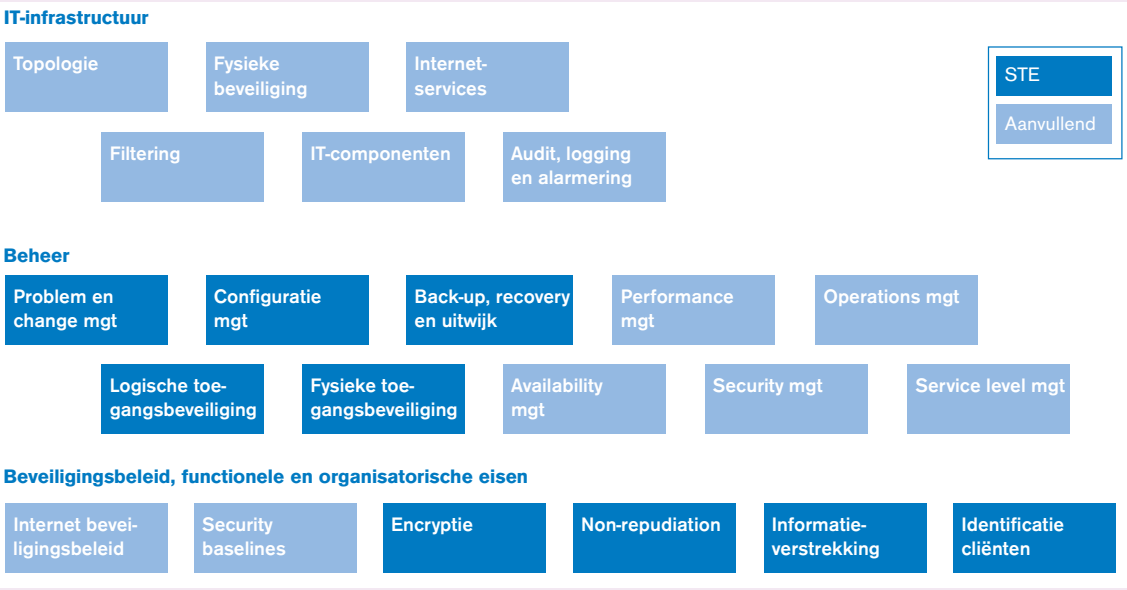
3 Aandachtsgebieden bij het uitwerken van het Internet-beveiligingsbeleid zijn onder meer:

A Uitwerken en onderhouden van een Internet-beveiligingsbeleid.
B Uitwerken van Security Baselines ten aanzien van de inrichting en implementatie van Internet-componenten.

Tabel 2. Aanvullende eisen.

hetgeen daaromtrent door de organisatie is beschreven (de opzet beoordelen). Pas in een latere fase, bijvoorbeeld bij een pilot waarbij ook enkele cliënten worden betrokken, kan een oordeel worden gegeven omtrent de werking van de systemen en de AO/IC-maatregelen. Echter in deze pilotfase is het systeem reeds operationeel en is de activiteit dus al gestart. In de regelgeving van de STE wordt in het geheel geen aandacht besteed aan dit probleem. Op welke wijze hiermee in de praktijk dient te worden omgegaan is dus niet geheel duidelijk vanuit de regelgeving. De Beleidsnotitie Internet behoeft ten aanzien van het afgeven van een verklaring omtrent de opzet en werking nog wel enige toelichting.

Hetzelfde is van toepassing voor de strekking van de door de IT-auditor af te geven verklaring. Binnen het vakgebied (IT-)auditing worden veelal de termen opzet, bestaan en werking gehanteerd bij het afgeven van een oordeel. In de Beleidsnotitie Internet wordt niet ingegaan op het aspect van bestaan. Onduidelijk is of dit begrip door de STE al dan niet bewust achterwege is gelaten. Voor het vormen van een oordeel dient over bovenstaande derhalve een nadere toelichting plaats te vinden. Bij het afgeven van een verklaring van via Internet aangeboden effectendiensten dient naar mijn mening in de verklaring voorzichtig te worden omgegaan met termen als 'voldoen aan STE-regelgeving'. Dit geldt in ieder geval zolang nog geen duidelijkheid bestaat omtrent de



Figuur 2. Aandachtsgebieden betreffende de betrouwbaarheid en continuïteit van Internet-toepassingen.

interpretatie van de regelgeving, dan wel door de STE nog geen goedkeuring heeft plaatsgevonden omtrent de wijze waarop het onderzoek uitgevoerd zal worden. In dergelijke gevallen is het aan te bevelen om in de verklaring aan te geven dat wordt voldaan aan algemeen geldende eisen ten aanzien van betrouwbaarheid en continuïteit.

Samenvatting en conclusie

In dit artikel is een overzicht en evaluatie gegeven van de beschikbare regelgeving die door toezichthouders inmiddels is opgeleverd inzake Internet. Deze regelgeving is opgesteld als gevolg van de toenemende activiteiten van financiële instellingen op Internet. Zowel door DNB als door de STE is regelgeving op dit gebied ontwikkeld. Een belangrijke vraag die vanuit de regelgeving moet worden beantwoord, is of een instelling op de Nederlandse markt actief is. Het antwoord op deze vraag hangt af van de vraag of de door middel van Internet uitgeoefende activiteiten op inwoners van Nederland zijn gericht. In het artikel zijn enkele indicatoren opgenomen die door DNB en de STE gehanteerd worden bij het bepalen of de activiteiten op inwoners van Nederland gericht zijn.

Uit de evaluatie blijkt dat de door DNB ontwikkelde regelgeving op het gebied van Internet alleen de formele aspecten van regelgeving behandelt, dat wil zeggen het beschikken over een vergunning indien de activiteiten vanuit Nederland worden aangeboden dan wel indien zij op de inwoners van Nederland gericht zijn. Deze regelgeving stelt geen specifieke eisen aan de wijze waarop de geautomatiseerde informatiesystemen en de maatregelen van AO/IC rondom Internet-toepassingen dienen te worden opgezet. Eisen specifiek gericht op de beveiliging en continuïteit van Internet-toepassingen zijn (nog) niet geformuleerd. Ook het Memorandum DNB voorziet verder niet in concretere richtlijnen op het gebied van Internet.

De door de STE opgestelde regelgeving is in vergelijking met de DNB-regelgeving concreter uitgewerkt en daarnaast wordt een verklaring van een onafhankelijke IT-auditor geëist. De STE heeft eisen opgesteld ten aanzien van de algemene beheermaatregelen van systemen, additionele beveiligingseisen van systemen en AO/IC-maatregelen als gevolg van het gebruik van Internet. De door de STE opgestelde regelgeving laat echter ruimte voor interpretatie, waardoor het vormen van een oordeel door de IT-auditor in de praktijk bemoeilijkt wordt. Derhalve zijn in dit artikel aanvullende eisen geformuleerd die kunnen worden getroffen ter waarborging van de betrouwbaarheid en continuïteit van de Internet-toepassing. Om een verklaring te kunnen afgeven dient de IT-auditor te beschikken over een duidelijk stelsel van eisen. Gelet op bovenstaande is daarvan vanuit de STE nog geen sprake. De IT-auditor dient derhalve in nader overleg te treden met de STE om meer duidelijkheid te verkrijgen omtrent de te hanteren normen. Tevens dient door de STE meer duidelijkheid te worden verschaft ten aanzien van de gehanteerde begrippen opzet en werking. Van de IT-auditor wordt hierover een oordeel verwacht. Het vormen van een oordeel over de opzet van de betrokken systemen en administratieve organisatie van bijvoorbeeld beursorderlijnen via Internet zal in de praktijk niet direct een probleem opleveren. Het vormen van een oordeel omtrent de werking wel, aangezien het systeem hiertoe eerst operationeel dient te zijn, al dan niet in de vorm van een pilot met enkele cliënten.

Literatuur

Mr. Ch.E. Bethlem en mr. E.P.M. Joosen, *Internet banking vraagt meer van toezichthouders*, Bank- en Effectenbedrijf, oktober 1999.

Beleidsregels Media WtB, De Nederlandsche Bank.

Beleidsregels Media WtK 1992, De Nederlandsche Bank.

Nadere Regeling toezicht effectenverkeer 1999, STE.

Informatiememorandum over het gewijzigde besluit toezicht effectenverkeer 1995 en de daarop gebaseerde nadere regeling toezicht effectenverkeer 1999, STE, 26 januari 1999.

www.dnb.nl

www.ste.nl

Mw. B. Beugelaar RE RA is EDP audit manager binnen de unit Financiële Dienstverlening van KPMG EDP Auditors. Zij is verantwoordelijk voor het uitvoeren van diverse onderzoeken bij financiële instellingen, alsmede de daarmee samenhangende advisering. In die verantwoordelijkheid heeft zij onder meer ervaring opgedaan betreffende het toetsen aan regelgeving van toezichthouders en het adviseren van financiële instellingen omtrent de wijze van inrichting van de administratieve processen en de geautomatiseerde informatiesystemen.