

IT Risk Management for Financial Organisations

Dr. ir. Paul L. Overbeek RE
Paul.Overbeek@Ois-NL.EU

06-53786475



DNB

Rol

- Financiële stabiliteit
 - Gezonde economie en welvaart in Nederland.
 - Waardevaste Euro
 - Soepel en veilig betalingsverkeer
- **Toezicht op de soliditeit en betrouwbaarheid financiële instellingen**
 - Banken, Verzekeraars, Kredietinstellingen, Pensioenfondsen
 - Prudentieel: terughoudend
- (inter)nationale besluitvorming

Normen Toezicht DNB relevant voor IT

- Tot 1 jan 2007
 - Regeling Organisatie en Beheersing (ROB)
 - Toetsingkader Business Continuity Planning
- Sinds 1 jan 2007 is alleen de WFT verplicht
 - Dekt veel van de 'oude' ROB maar is nauwelijks normatief
 - WFT laat veel meer aan de AI (OTSI) over
- FIRM is de methode voor risico-analyse die DNB hanteert in haar toezicht
 - FIRM is niet verplicht, maar toont wel hoe DNB denkt

WFT en IT

- **Vanmiddag in detail**
- **Keuze van de aangesloten instelling (AI of OTSI voor Onder Toezicht Staande Instelling) is leidend**
 - Maar moet onderbouwd zijn
 - Risico management is verplicht
- **Zelf-regulering tenzij.**
 - Bankwet "...goede werking betalingsverkeer..."
 - Markt / AI's moeten zelf sound practices afspreken
 - Toezicht DNB is 'principle based'
- **Sound practices zijn:**
 - Normen / standaarden:
 - Core Principles for Payment Systems (BIS)
 - Recommendations for Securities Settlement Systems (BIS)
 - Electronic Money Schemes Security Objectives (ECB → BIS)
 - En nog steeds:
 - Regeling Organisatie en Beheersing (ROB)
 - Toetsingkader Business Continuity Planning
- **Samenvattend**
 - Risico management is verplicht
 - AI kiest sound practices
 - B.v. ROB, BCP en BIS core principles

Toetsingskader BCP

- Elke instelling heeft zijn eigen **business continuity plan** goedgekeurd door directie
- **Risicoanalyse** van kritische activiteiten en systemen (ICT en business)
- Aandacht voor continuïteit menselijke factor
- De interne **crisisorganisatie**
- Inventarisatie **single points of failure**
- Zo snel mogelijk voortzetten kritische processen en systemen
 - Uitwijkcentrum (risicoprofiel, warm-koud)
 - Testen van BCP-voorzieningen
- **Communicatieplan** voor alle stakeholders
- Ontwikkelen van een **business continuity plan** voor de gehele kerninfrastructuur



Autoriteit
Financiële Markten

Autoriteit financiële markten – 1/2

- Toezicht op het gedrag van de Nederlands financiële markten
- Consumenten:
 - Waarschuwingslijsten
 - De financiële bijsluiter
- Marktpartijen:
 - Wet financiële dienstverlening
 - Toezicht op accountants
 - Marktmisbruik
 - Reclame-uitingen
 - Toezicht op emissies
 - Toezicht op aanbieders beleggingsobjecten
- Registers



Autoriteit
Financiële Markten

Wet en regelgeving AFM 2/2

- Wet Identificatieplicht
- Gedragstoezichthouder gehele financiële marktsector.
 - Effectenwezen:
 - Wet toezicht effectenverkeer 1995
 - Wet giraal effectenverkeer.
 - Beleggingsinstellingen
 - Wet toezicht beleggingsinstellingen
 - kredietwezen
 - Wet op het consumentenkrediet.
 - Financiële Bijsluiter
- Toezicht op marktmisbruik, (voorkomen) voorwetenschap. manipulatie
- Melding Belang beursgenoteerde ondernemingen
- Anti-witwaswetgeving (MOT) / Sanctiewetgeving
- Vergunningen, sancties
- Vanaf 1 januari 2007: samengevat in WFT als gedragstoezicht
- Samenvattend AFM & IT risk management:
 - Het resultaat van 'gedragingen' valt onder toezicht
 - algemene en specifieke eisen aan inrichting IT-omgeving



Currence

- Brandowner van collectieve nationale betaalproducten als PIN, Chipknip, Acceptgiro en Incasso/Machtige
- Doel: marktwerking en transparantie met behoud van de kwaliteit en veiligheid
- Rules & regulations (minimumeisen):
 - Definitie rollen en eisen
 - Reglement: aanvraag-, beoordelings-, toekennings-, instandhoudingsprocedures voor de licenties en certificaten;
 - R&R bepalingen: organisatorische, procesmatige en operationele eisen per rol uit het rollenmodel
- Certificaat obv audit door accountant tegen het Currence auditprogramma
 - voorbeeld auditprogramma

Auditprogramma - hoofdlijn

- Organisatie
 - Geregistreerd bij DNB
 - **ROB**
 - Aantoonbaar voldoen aan alle eisen
 - Uitbesteden mag onder voorwaarden
 - Allerlei verplichtingen rond administratie en rapportage
- Proces
 - Aangaan van overeenkomsten
 - Plichten
 - **Controlerende** activiteiten
 - Productspecifieke eisen, b.v. cardlife-cycle
 - Fraudebeheersing
- Aantoonbaar voldoen aan eisen dmv jaarlijkse audit



BANK FOR INTERNATIONAL SETTLEMENTS

BIS 14 core principles

- **Bank for International Settlements**
 - Samenwerkingsverband tussen 'central banks'
 - Maakt internationale afspraken obv inbreng deelnemers
 - Die afspraken worden doorgaans later gecodificeerd
- **Principes voor risk management van de Bank of International Settlement**
 - Board / Management oversight (1-3)
 - Security controls (4-10)
 - Legal & Reputational risk management (11-14)



BANK FOR INTERNATIONAL SETTLEMENTS

Principles – BoD / Senior management

- **Principle 1: effective management oversight over the risks, including specific accountability, policies and controls to manage these risks.**
- **Principle 2: review and approve the bank's security control process.**
- **Principle 3: ongoing due diligence and oversight process for managing outsourcing and other third-party dependencies**



Principles – Security controls management 4-10

- Aim at:
 - 4. Authentication
 - 5. Non-repudiation
 - 6. Data and transaction integrity
 - 7. Segregation of duties
 - 8. Authorisation controls
 - 9. Maintenance of audit trails
 - 10. Confidentiality of key bank information



Principles – Legal / Reputational risk management 11-14

- Principle 11: Banks should ... provide adequate information to customers
- Principle 12: Accept and acknowledge applicable law
- Principle 13: ... effective capacity, **business continuity and contingency planning**
- Principle 14: appropriate **incident response** plans

- www.isf.org
- Coso/Cobit
- www.dnb.nl
- www.afm.nl
- www.bis.eu
- www.iaa.org
- www.ois-nl.eu