De Nederlandsche Bank N.V. mei 2011

Toetsingskader
Business Continuity Management
Financiële Kerninfrastructuur

Inhoud

Inleiding

In 2004 is het Toetsingskader Business Continuity Planning (BCP) opgesteld als kader voor banken en marktinfrastructuren. In 2006 heeft hier een aanvulling op plaatsgevonden in de vorm van een handreiking voor de invulling van de continuïteit van de menselijke factor voor kritieke systemen / bedrijfsprocessen. In 2010 is het kader herzien naar aanleiding van de verdere ontwikkeling van standaarden door standaardisatie organisaties[1], best practices in de markt en de ontwikkeling en herziening van normen die zijn opgesteld door financiële autoriteiten[2]. Deze laatste herziening heeft geleid tot het voorliggende Toetsingskader Business Continuity Management (BCM) Financiële Kerninfrastructuur (FKI)[3]. Dit kader sluit aan bij het onderdeel continuïteit in een aantal internationale toetsingskaders[4] van deze instellingen en committees en is opgesteld in aanvulling op deze internationale kaders omdat de FKI betalings- en effectenverkeer zowel financiële marktinfrastructuren (FMI's, zoals clearing- en settlementorganisaties) als banken omvat terwijl de internationale kaders een werking hebben voor of (een deel van) de FMI's of (een deel van) de banken.

De Nederlandsche Bank (DNB) en de Autoriteit Financiële Markten (AFM) hanteren dit Toetsingskader om vast te stellen in welke mate de normen hierin nageleefd worden door de instellingen die deel uitmaken van de Financiële Kerninfrastructuur (FKI). Het voldoen aan de normen in dit Toetsingskader Business Continuity Management FKI ontslaat instellingen niet van de verplichting te voldoen aan internationale toetsingskaders (zoals die van de BIS / IOSCO) waar deze van toepassing zijn op bijvoorbeeld specifieke systemen. Omdat de FKI deels bestaat uit instellingen die betaalsystemen cq effectenafwikkelsystemen aanbieden en deels uit instellingen die aan dergelijke systemen deelnemen, kan het zijn dat de aanbieders van systemen eisen stellen aan de deelnemers met betrekking tot beveiliging en business continuity. Deelnemers dienen hier alert op te zijn en aan dergelijke eisen te voldoen.

Business continuity heeft een relatie met enkele verwante vakgebieden: informatiebeveiliging, fysieke beveiliging, crisismanagement en meer in algemene zin (operational) risk management.

---

1 Zoals de BS 25999 van het British Standards Institute

2 Zoals de Europese Centrale Bank (ECB), het Committee on Payment and Settlements Systems (CPSS) van de Bank for International Settlements (BIS), de International Organization of Securities Commissions (IOSCO), het Basel Committee on Banking Supervision (BCBS) en het Joint Forum (een samenwerking tussen het BCBS, IOSCO en de International Association of Insurance Supervisors (IAIS)).

3 Onder het begrip FKI vallen die instellingen die verantwoordelijk zijn voor de belangrijkste transactiestromen en betaal- en effectenafwikkelsystemen in Nederland. Dit zijn zowel marktinfrastructuren als deelnemers aan deze infrastructuren.

4 CPSS *Core principles for systemically important payment systems,* CPSS/IOSCO *Recommendations for securities settlement systems*, CPSS/IOSCO *Recommendations for central counterparties,* BCBS / Joint Forum *High Level Principles for Business Continuity*, ECB *Business continuity expectations for systemically important payment systems*

In het business continuity proces dient rekening gehouden te worden met deze relaties en dienen beleid en maatregelen op elkaar aan te sluiten. Het onderwerp crisismanagement zal in de normen in dit Toetsingskader expliciet terugkomen, de overige verwante vakgebieden niet.

De financiële sector in Nederland kent enkele overlegstructuren die de hiervoor genoemde onderwerpen informatiebeveiliging, crisismanagement en business continuity instellingsoverstijgend behandelen. Voor business continuity is specifiek het Platform Business Continuity Vitale Infrastructuur Financiële sector (BC VIF) opgericht om beleidsmatige onderwerpen op het gebied van business continuity en bescherming vitale infrastructuren te bespreken en om ervaringen met elkaar te delen. In dit Platform bespreken de instellingen uit de FKI onder andere het gebruik van best practices en stellen ze gezamenlijke eisen aan kritieke service providers op. Met betrekking tot instellingsoverschrijdende operationele crises in het betalings- en effectenverkeer is het Tripartiete Crisismanagement Orgaan (TCO) ingesteld waarin DNB, AFM en het Ministerie van Financiën deelnemen. De instellingen uit de FKI zijn in deze crisismanagementstructuur vertegenwoordigd in een Consultatiegroep en drie Adviesgroepen.

In de rest van de tekst wordt ingegaan op de normen: (1) strategie en beleid ten aanzien van business continuity management, (2) business impact en risico analyses, (3) scenario's en maatregelen, (4) testen en monitoren, (5) beheer en onderhoud en tenslotte (6) crisismanagement en communicatie.

Normen Business Continuity Management FKI

1. Strategie / beleid

Iedere instelling moet een door de directie goedgekeurd business continuity beleid en business continuity plan (BCP) hebben[5]. Beleid en plan vormen een essentieel onderdeel van het overkoepelende operationeel risico management raamwerk van de instelling en moeten in lijn hiermee zijn. In het BCP zijn de kritieke bedrijfsprocessen en bijbehorende systemen geïdentificeerd en zijn de strategie, beleidsuitgangspunten en doelstellingen ten aanzien van de continuïteit van deze kritieke bedrijfsprocessen vastgelegd. De identificatie van de kritieke bedrijfsprocessen dient gebaseerd te zijn op een business impact analyse (BIA).

In het plan dient de maximaal acceptabele tijd dat bedrijfsprocessen en systemen niet kunnen functioneren te zijn opgenomen en te worden toegelicht. Deze tijd is bepalend voor de doelstelling ten aanzien van het herstellen van de processen en systemen (RTO: recovery time objective). Behalve de maximale uitvalsduur en bijbehorende hersteltijd dient ook vastgesteld te worden wat de doelstelling is met betrekking tot het maximale gegevensverlies (recovery point objective, RPO).
Er dient een analyse te worden gemaakt waarin een beschrijving wordt gegeven van mogelijke dreigingsscenario's die tot verstoring van de bedrijfsprocessen kunnen leiden, waarbij rekening wordt gehouden met zowel externe als interne dreigingen. Deze beschrijving omvat ook de maatregelen om te waarborgen dat de met de stakeholders afgesproken service levels (zoals vastgelegd in service level agreements, SLA's) gehaald worden. De maatregelen dienen gebaseerd te zijn op een risico analyse.

In het plan moet tevens aandacht zijn voor specifieke aspecten zoals de internationale dimensie van de organisatie en de consequenties van bijvoorbeeld outsourcing / offshoring. Waar instellingen deelnemen aan clearing- en/of settlementsystemen moet gerefereerd worden aan de eisen die door deze systemen aan haar deelnemers worden gesteld.

In het plan dient ook geïdentificeerd te worden aan welke nationale en internationale toetsingskaders en normen[6] voldaan moet worden.

Het actueel houden van het plan is een continu proces waarbij formele vaststelling periodiek (conform beleid) plaatsvindt en zoveel vaker als er ingrijpende wijzigingen zijn in de organisatie,

---

[5] Beleid en plan kunnen ook bestaan uit een stelsel van samenhangende documenten.

[6] Voorbeelden hiervan zijn de BIS CPSS en IOSCO principles en recommendations.

bedrijfsprocessen of systemen. Het business continuity management van een instelling dient beoordeeld te worden door een onafhankelijke partij zoals interne of externe auditor.

2. Business impact analyse / risico analyse

Business impact analyse / kritieke bedrijfsprocessen en systemen

Iedere instelling dient met behulp van een business impact analyse (BIA) vast te stellen wat de gevolgen zijn van gehele of gedeeltelijke uitval van een bedrijfsproces. Het resultaat van een dergelijke analyse is een inventarisatie van kritieke bedrijfsprocessen en systemen / resources. Daarbij dient niet alleen gelet te worden op de gevolgen van uitval voor de instelling zelf maar ook op de gevolgen voor het betalings- en/of effectenverkeer waar het betreffende proces / systeem onderdeel van uit maakt. De mate waarin andere instellingen afhankelijk zijn van het goed functioneren van het betreffende proces is mede van belang voor het bepalen van het kritieke gehalte. De business impact analyse dient actueel gehouden te worden en te worden uitgevoerd bij elk nieuw proces / systeem of belangrijke wijziging.

Risico analyse / scenario's en maatregelen

Iedere instelling dient een risicoanalyse te hebben gemaakt waarbij per kritiek proces / systeem wordt nagegaan waardoor het proces of systeem niet beschikbaar is en wat de oorzaak hiervan kan zijn. Voor deze dreigingsscenario's wordt vervolgens bepaald welke maatregelen genomen zijn respectievelijk genomen kunnen worden om het risico (kans en impact) te mitigeren. Tenslotte dient vastgelegd te worden welke restrisico's door de directie geaccepteerd zijn. Deze stappen zijn samengevat in tabel 1.

TABEL 1. Stappen in een risico analyse

Waardoor is het proces niet beschikbaar	**Wat is de oorzaak**	**Welke maatregelen zijn genomen/ kunnen worden genomen**	**Welke restrisico's blijven er over**
Gehele of gedeeltelijke niet beschikbaarheid van (en/of): • Mensen • IT systemen[7] • Communicatie[8] • Gebouwen[9]	• Natuurrampen (brand, storm, aardbeving, overstroming, etc) • Technisch falen (hardware / software storingen, uitval elektriciteit, etc) • Organisatorisch falen (menselijke fouten, ziekte, etc) • Moedwillig menselijk handelen (sabotage, terrorisme, cyberaanvallen, etc)	Maatregelen onder te verdelen in: • Preventief • Detectief • Correctief • Respons	Lijst met geaccepteerde restrisico's

[7] Waaronder data / informatie.

Onderdeel van een dergelijke risico analyse is de identificatie van single points of failure, die niet alleen technisch van aard kunnen zijn maar ook betrekking kunnen hebben op een organisatieonderdeel of op de aanwezigheid van essentiële kennis bij slechts één of een paar medewerkers.

De risicoanalyse dient actueel gehouden te worden en te worden uitgevoerd bij elk nieuw proces / systeem of bij een belangrijke wijziging. De risico analyse dient tenminste jaarlijks geaccordeerd te worden door het management, ook indien er geen wijzigingen in processen of systemen hebben plaatsgevonden.

Afhankelijkheden van service providers / deelnemers

In de risico analyse dient expliciet aandacht geschonken te worden aan de afhankelijkheid van basisvoorzieningen (elektriciteit, gas, water, telecom, etc.) en externe service providers, welke specifieke risico's deze afhankelijkheid inhoudt voor de continuïteit van de kritieke processen en op welke wijze de continuïteit hiervoor is georganiseerd. In het BCP dient duidelijk te zijn vastgelegd welke afspraken gemaakt zijn met deze service providers, op welke wijze informatie over de maatregelen bij de service providers en de performance ten opzichte van de contractuele afspraken beschikbaar is en hoe waarborgen over implementatie en werking verkregen worden. Deze vastlegging kan ook in de vorm van een verwijzing naar de betreffende contracten en service level agreements (SLA's). Ook dient te zijn nagedacht over eventuele alternatieven om de continuïteit van kernvoorzieningen veilig te stellen.

De Financial Market Infrastructures (FMIs) zijn instellingen die clearing en settlement systemen beheren waaraan andere FMIs en/of financiële instellingen deelnemen of die andere infrastructurele diensten aanbieden. Dergelijke FMIs dienen in hun risico analyse ook expliciet aandacht te schenken aan de risico's die deelnemers aan hun systemen kunnen veroorzaken. Daarbij dienen aan deelnemers operationele eisen te worden gesteld, in overeenstemming met het belang van de deelnemers in het betreffende systeem.

3. Scenario's / maatregelen

De risico analyse levert een overzicht van de risico's en mitigerende maatregelen voor diverse scenario's op. Enkele aspecten dienen expliciet behandeld te worden.

---

8 Communicatievoorzieningen voor zowel spraak- als dataverkeer

9 Waaronder ook infrastructurele / facilitaire voorzieningen zoals energie, electriciteit en water.

Menselijke factor

In het business continuity plan dient transparant te worden gemaakt op welke wijze rekening is gehouden met de menselijke factor[10]. Deze dient zo min mogelijk een knelpunt te zijn bij het voortzetten van de bedrijfsprocessen en ondersteunende IT systemen en er dient beschreven te zijn of en hoe inzet van (andere) medewerkers na een calamiteit kan worden georganiseerd.

Maximale uitvalsduur

De maatregelen voor de diverse scenario's dienen er op gericht te zijn dat de kritieke bedrijfsprocessen en systemen binnen de gestelde RTO's kunnen worden hervat. De maximale uitvalsduur per proces dient overeen te stemmen met de afspraken die zijn vastgelegd in service level agreements. Voor bepaalde soorten processen (zoals clearing en settlement) moet rekening gehouden worden met mogelijke eisen van (inter)nationale toezichthouders.

Uitwijklocatie

Elke instelling dient met zijn kritieke processen en systemen te kunnen uitwijken van de primaire locatie naar andere locaties. De uitwijk kan op meerdere locaties geregeld zijn waarbij vaak een splitsing is aangebracht tussen ICT en business. De uitwijklocaties dienen een verschillend risicoprofiel te hebben ten opzichte van de primaire locatie. Bij het vaststellen van de maatregelen om te kunnen voldoen aan de maximale uitvalsduur dient rekening gehouden te worden met de duur van het besluitvormingsproces om uit te wijken. Ook de eventuele reistijd van medewerkers naar de uitwijklocatie dient meegenomen te worden in de berekeningen. In geval van uitwijk dienen herstelplannen te worden uitgewerkt. In deze herstelplannen worden de activiteiten beschreven die ondernomen moeten worden om na een verstoring terug te kunnen keren tot de reguliere bedrijfsvoering.

Aspecten waar rekening mee gehouden moet worden bij het bepalen van de risicoprofielen van de locaties zijn:

- de samenstelling en capaciteit van de infrastructuur moet voldoende zijn om in de uitwijklocatie de verwerking van de primaire locatie over te kunnen nemen voor kritieke processen;
- er moet in de uitwijklocaties tijdig voldoende personeel ingezet kunnen worden om binnen de maximale uitvalsduur de verwerking voort te zetten;
- bij de afstand tussen en toegang tot de locaties dient rekening gehouden te worden met kans op verkeersopstoppingen, versperring door natuurrampen (die beide locaties tegelijk kunnen treffen) en de tijd die nodig is om van de ene naar de andere locatie te komen;
- verstoringen in de basisvoorzieningen (energie, elektriciteit, water, telecommunicatie) dienen waar nodig opgevangen te kunnen worden dan wel dient de kans van optreden tot een geaccepteerd niveau te worden gemitigeerd.

---

10 NB: dit toetsingskader gaat niet over de emergency response plannen die er op gericht zijn om personeel in veiligheid te brengen in geval van een calamiteit.

4. Testen / monitoren

De continuïteitsmaatregelen in het BCP dienen regelmatig getest te worden. Daaronder valt ook het testen van de uitwijk van processen en systemen uitgaande van verschillende scenario's waaronder grootschalige verstoringen en switch van primaire naar secundaire site. Het gaat hierbij om het testen van zowel de uitwijk van ICT-systemen als van de business processen. Service providers dienen regelmatig betrokken te worden bij dergelijke testen en, voor FMIs, ook kritieke deelnemers. Afhankelijk van het belang van het bedrijfsproces en het systeem dienen de maatregelen minimaal eenmaal per jaar getest te worden. De resultaten van de testen dienen vastgelegd te worden in rapportages waarin vastgestelde tekortkomingen en aandachtspunten worden verwoord waarbij een éénduidige probleemeigenaar en oplostermijn wordt vastgesteld. Het BCP dient een testkalender te bevatten waarin de planning van de testen is opgenomen en waarin een procedure is beschreven op welke wijze de resultaten van de tests verwerkt worden in het BCP.

De instellingen dienen een incident managementproces (detecteren, escaleren, analyseren en monitoren van incidenten) te implementeren. Incidenten kunnen immers ook een indicator zijn dat maatregelen aangepast dienen te worden.

5. Beheer en onderhoud

Business continuity is een verantwoordelijkheid van de proceseigenaar en de instelling dient de verantwoordelijkheid voor business continuity management expliciet in de lijn te hebben belegd. Er dient voldoende capaciteit beschikbaar gesteld te worden om deze verantwoordelijkheid in te vullen. Deze business continuity organisatie dient vastgelegd te zijn met een duidelijke beschrijving en afbakening van de taken ten aanzien van het beheer en onderhoud van het business continuity plan.

Een onderdeel van het onderhoud betreft het volgen van de ontwikkelingen op het gebied van nationale en internationale standaarden en toetsingskaders, van (internationale) wetgeving en van wijzigingen in de organisatie en in service level agreements.

6. Crisismanagement en communicatie

Iedere instelling dient over een crisismanagementorganisatie met voldoende mandaat te beschikken om in geval van een operationele calamiteit besluiten te kunnen nemen en maatregelen in werking te kunnen stellen. De crisismanagementorganisatie wordt aangestuurd door de directie. Deze organisatie, inclusief de hierbij behorende plannen en procedures, dient helder te zijn vastgelegd.

Iedere instelling dient een communicatieplan te hebben over de wijze waarop in geval van een calamiteit de communicatie naar alle stakeholders zo adequaat mogelijk kan worden georganiseerd. Tot de stakeholders behoren in ieder geval klanten, medewerkers, de andere instellingen van de FKI, toezichthouders en pers.

De crisismanagementorganisatie, procedures en communicatieplannen van de individuele instellingen dienen aan te sluiten op de organisatie, procedures en afspraken in het kader van het operationele sectorcrisismanagement zoals dat geldt voor de financiële kerninfrastructuur.

De crisismanagementorganisatie, procedures en communicatieplannen van de individuele instellingen dienen periodiek (conform het gestelde beleid) maar tenminste eenmaal per jaar getest te worden. De resultaten van de testen dienen vastgelegd te worden in rapportages waarin vastgestelde tekortkomingen en aandachtspunten worden verwoord waarbij een éénduidige probleemeigenaar en oplostermijn wordt vastgesteld. Op sectorniveau dient dit tenminste eenmaal per drie jaar te gebeuren met deelname van alle tot de FKI behorende instellingen.