de Berlaimontlaan 14 – BE-1000 Brussel
tel. +32 2 221 45 44 – fax + 32 2 221 31 38
ondernemingsnummer: 0203.201.340
RPR Brussel
www.nbb.be

BanqueNationaleBank DE BELGIQUE VAN BELGIË
Eurosystem

Circulaire

Brussel, 18 december 2015

Kenmerk: NBB_2015_32

uw correspondent:
Gino Thielemans
tel. +32 2 221 45 44 – fax +32 2 221 31 38
Gino.thielemans@nbb.be

Aanvullende prudentiële verwachtingen op het vlak van de operationele bedrijfscontinuïteit en beveiliging van systeemrelevante financiële instellingen

Toepassingsveld

Systeemrelevante financiële instellingen naar Belgisch recht als bedoeld in artikel 3, 29° van de wet van 25 april 2014 betreffende het statuut en het toezicht op kredietinstellingen, en artikel 36/3, §2 van de organieke wet[1]*.*

Samenvatting/Doelstelling

Toelichting verstrekken aan de systeemrelevante financiële instellingen over de verwachtingen van de Nationale Bank van België (NBB) op het vlak van hun operationele bedrijfscontinuïteit en beveiliging.

Geachte mevrouw
Geachte heer

1. Verantwoording

Systeemrelevante financiële instellingen dienen bijzondere zorg te besteden aan de continuïteit van hun dienstverlening en de veiligheid van hun bedrijfsvoering gelet op:

- hun kritieke rol in het financieel systeem en hun groot maatschappelijk belang;
- het feit dat ze, juist omwille van hun systemisch karakter en/of hun grote zichtbaarheid en naambekendheid, potentieel bevoorrechte doelwitten vormen van zowel externe als interne kwaadwilligen (criminelen, terroristen ...).

[1] Conform artikel 36/3, §2 van de organieke wet, bepaalt de Bank onder de financiële instellingen bedoeld in artikel 36/2, met uitzondering van de kredietinstellingen, welke als systeemrelevant moeten worden beschouwd, en brengt ze deze instellingen hiervan op de hoogte.

2. Inleiding

Deze circulaire beoogt de systeemrelevante financiële instellingen duidelijkheid te verschaffen over de aanvullende prudentiële verwachtingen van de NBB op het vlak van hun operationele bedrijfscontinuïteit en beveiliging. Ze vervangt de richtlijnen van het vroegere Comité voor Financiële Stabiliteit (CFS) van 20 oktober 2004 op het vlak van de bedrijfscontinuïteit voor de systeemrelevante banken.

De circulaire vormt een aanvulling op de navolgende bestaande circulaires:

- PPB 2005/2 inzake de gezonde beheerpraktijken op het vlak van de bedrijfscontinuïteit;
- PPB 2004/5 en PPB-2006-1-CPA over de gezonde beheerpraktijken bij uitbesteding;
- CBFA_2009_17 inzake financiële diensten via het Internet;

en moet samen met de voormelde bepalingen worden gelezen en nageleefd. Afwijkingen ervan dienen aan de NBB te worden toegelicht ("comply or explain")[2].

De systeemrelevante financiële instellingen die als kritieke infrastructuur eveneens onder "oversight" vallen, dienen naast de prudentiële verwachtingen in deze circulaire ook te voldoen aan de "oversight"-verwachtingen ter zake.

3. Toepassingsgebied

A. Ratione personae

De gezonde beheerpraktijken in deze circulaire zijn van toepassing op de systeemrelevante kredietinstellingen, verzekeringsondernemingen en betalingsinstellingen naar Belgisch recht.

B. Ratione materiae

Deze circulaire beoogt de gepaste bescherming van de kritieke activiteiten, diensten en middelen (gebouwen, activa, toepassingen, gegevens …) van de systeemrelevante financiële instellingen tegen onomkeerbare operationele schade of langdurige verstoringen, ongeacht of de oorzaak menselijk (pandemie, kwaadwillige daden, …) dan wel technisch van aard is (pannes, vernietiging of beschadiging van kritieke gebouwen of middelen, ...).

De circulaire is van toepassing op de kritieke diensten, middelen en functies waarvan de verstoring of vernietiging:

a) de goede werking van het financiële systeem in gevaar kan brengen, vanwege hun operationeel belang voor de centrale financiële infrastructuren voor betalingsverwerking, -verrekening en -vereffening van effectentransacties en/of voor de werking van gereglementeerde financiële markten (hierna "systeemrelevante kritieke activiteiten, diensten en middelen" genoemd);
b) de interne bedrijfsvoering ernstig kan verstoren en onderbrekingen in de dienstverlening kan veroorzaken, maar met weinig of geen gevolg voor de goede werking van de centrale financiële infrastructuren voor betalingsverwerking, -verrekening en -vereffening van effectentransacties en/of voor de werking van gereglementeerde financiële markten (hierna "interne kritieke activiteiten, diensten en middelen" genoemd).

Behoudens een expliciet onderscheid dient te worden gemaakt tussen de hiervoor vermelde "systeemrelevante" en "interne" kritieke activiteiten, diensten en middelen, zal deze circulaire het meer algemene en overkoepelende concept van "kritieke activiteiten, diensten en middelen" aanwenden.

[2] Deze circulaire en de andere vermelde circulaires worden door de NBB ook als leidraad gehanteerd tegenover instellingen onder prudentieel toezicht voor haar wettelijke toezichtsopdracht in het kader van de wet van 1 juli 2011.

De prudentiële verwachtingen ten aanzien van de voorbereiding en de opmaak van herstelplannen en afwikkelingsplannen overeenkomstig respectievelijk de artikels 108 t.e.m. 116 en 226 t.e.m. 232 van de wet van 25 april 2014, vallen buiten het toepassingsgebied van deze circulaire.

Vermits de NBB niet bevoegd is voor het toezicht op de naleving van de privacy- en/of de databeschermingswetgevingen, vallen de specifieke veiligheids- en confidentialiteitsbepalingen in de privacy- en/of de databeschermingswetgevingen buiten het toepassingsgebied van deze circulaire.

De gezonde beheerpraktijken slaan waar toepasselijk, op de:
- centrale en decentrale bedrijfseenheden en gebouwen;
- ondersteunende (groeps)functies;
- centrale en decentrale IT-systemen, gegevensbanken en toepassingen;
- uitbestedingen binnen de groep en / of met externe tegenpartijen.

die kritieke activiteiten, diensten en/of middelen leveren aan systeemrelevante kredietinstellingen, verzekeringsondernemingen en betalingsinstellingen naar Belgisch recht.

4. Gezonde beheerpraktijken

a. Algemene omkadering

1. Strategie, beleid en risicoanalyse

Het directiecomité is verantwoordelijk voor de uitwerking van een strategie en een beleid om de veiligheid[3] en de continuïteit van haar kritieke activiteiten, diensten en middelen op adequate manier te vrijwaren. Hierbij maakt de instelling op het vlak van de beveiliging een duidelijk onderscheid tussen de fysieke en logische beveiliging (cf. hoofdstuk 4.C). Waar mogelijk en gepast maakt de instelling hierbij gebruik van internationaal erkende gezonde beheerpraktijken en/of standaarden[4].

Het directiecomité ziet toe op de invulling en de effectiviteit van het risicobeheer, de genomen voorzorgsmaatregelen en interne controles. Ze beschikt hiervoor over een beveiligingsplan en aangepaste rapportering, waarin bijzondere aandacht wordt besteed aan de risicoanalyse van de kwetsbaarheden en bedreigingen, en de door de onderneming geplande maatregelen.

Minstens jaarlijks brengt het directiecomité verslag uit aan de raad van bestuur over de werking en doeltreffendheid van de strategie, het beleid en het plan om de operationele veiligheid en de continuïteit van haar kritieke activiteiten, diensten en middelen op adequate wijze te vrijwaren.

De raad van bestuur en het directiecomité beschikken over de nodige expertise om hun toezichtstaken uit te voeren, of laten zich hiervoor bijstaan door (interne of externe) experten.

De strategie, het beleid en het beveiligingsplan verschaffen minimaal duidelijkheid met betrekking tot:
a) de doelstellingen (risicotolerantie) van de onderneming inzake de beveiliging (fysiek en logisch) en de continuïteit van haar kritieke activiteiten, diensten en middelen;
b) de interne “governance”, met bijzondere aandacht voor de beleidsvormende en toezichthoudende organen en processen, en de rollen en verantwoordelijkheden van alle betrokkenen;
c) de geldende rapporteringlijnen en –verwachtingen;

3 De veiligheid omvat eveneens de bescherming van de integriteit van kritieke gegevens en toepassingen.

4 Bijvoorbeeld de standaarden inzake de informatiebeveiliging (ISO 27001/27015, …) en de bedrijfscontinuïteit (ISO 22301, …).

d) de toegepaste classificatiecriteria en -aanpak voor de identificatie van kritieke activiteiten, diensten en middelen;
e) de voorziene vormings- en/of sensibiliseringsmaatregelen (cf. punt 5 hierna);
f) het gevolgde beleid en de interne controlevereisten bij de uitbesteding van kritieke activiteiten, diensten en middelen;
g) de organisatie van meldpunten voor opgemerkte onregelmatigheden en/of verdachte gebeurtenissen door interne medewerkers of externe partijen (cliënten, leveranciers, …).

Hierbij dient de interne auditfunctie periodiek:

- de correcte invulling en de doeltreffendheid van de vastgelegde strategie, het beleid en het beveiligingsplan, alsook de kwaliteit van de uitgevoerde risicoanalyse en risicorapportering te testen.
- verslag uit te brengen over dit onderwerp bij het auditcomité.

2. <u>Beheer van de IT complexiteit en kwetsbaarheid</u>

De instelling beschikt over een aangepaste “governance” om de complexiteit van haar IT systemen beheersbaar te houden en te voorkomen dat de complexiteit van de IT systemen een adequaat beheer van de operationele veiligheid en continuïteit van de kritieke activiteiten, diensten en middelen in het gedrang brengt.

De onderneming legt in dit kader de verantwoordelijkheden en processen vast die moeten instaan voor de nodigde technologische en architecturale keuzes vanuit een ondernemingsperspectief op de korte en de lange termijn. Deze keuzes worden vervolgens vertaald en gecommuniceerd onder de vorm van gepaste technische standaarden en richtlijnen die dienen te worden nageleefd. Waar mogelijk en gepast maakt de instelling hierbij gebruik van internationaal erkende gezonde beheerpraktijken en/of standaarden[5]. Afwijkingen van deze standaarden en richtlijnen maken het voorwerp uit van een gepast validatieproces.

Om de IT-complexiteit te beheren beschikt de instelling ook over een volledige en betrouwbare (gecentraliseerde, gedecentraliseerde of gefedereerde) inventaris van alle IT- en configuratiecomponenten (i.e. een “Configuration Management Database” of CMDB), die haar o.a. toelaat om vanuit veiligheids- of bedrijfscontinuïteitsoogpunt, tijdig de benodigde:

- "software"- en "hardware"-verbeteringen en rechtzettingen (“patches) door te voeren voor alle betrokken componenten; en
- verouderde technologieën te vervangen of te actualiseren (“upgrades”).

De instelling beschikt ook over formele processen om:

a) alle IT-, configuratie-, en architectuurcomponenten, die aan het einde van hun levensduur zijn of komen, proactief te identificeren en tijdig af te bouwen; en
b) software-rechtzettingen (i.e. “patches”) te bekomen, te testen en te ontplooien op basis van hun kritieke karakter en ontbrekende software-rechtzettingen op te volgen en te prioriteren over alle omgevingen;

met als doel de operationele veiligheid en continuïteit van de kritieke activiteiten, diensten en middelen te verzekeren en in stand te houden.

Verouderde IT-componenten, te lang uitgestelde kritieke software-rechtzettingen en onaangepaste technologieën en/of architecturen die de operationele veiligheid en continuïteit van de kritieke activiteiten, diensten en middelen rechtstreeks of onrechtstreeks in het gedrang brengen, worden tijdig gerapporteerd aan het hoger management en worden opgenomen in de jaarlijkse rapportering naar het directiecomité met als doel, de nodige correctieve aanpak en/of maatregelen op te nemen in het beveiligingsplan.

5 Bijvoorbeeld standaarden inzake “enterprise”-architectuur (TOGAF, ISO 42010, SABSA, …).

3. Risicoanalyse en goedkeuring

De instelling beschikt over formeel gestructureerde processen voor de analyse en goedkeuring van de operationele veiligheids- en continuïteitsrisico's van (minstens) haar kritieke activiteiten, diensten en middelen, die samengaan met en/of voortvloeien uit:

- belangrijke wijzigingen in de bedrijfsvoering (bv. nieuwe producten, diensten, externe dienstverleners of organisatiemodellen);
- de invoering van nieuwe technologieën en/of architecturen;
- belangrijke nieuwe bedrijfsinvesteringen en/of -projecten.

Hierbij wordt naast de traditionele financiële en commerciële kosten-batenanalyse, ook een risicoanalyse uitgevoerd betreffende de impact op de operationele veiligheid en de continuïteit van op zijn minst de kritieke activiteiten, diensten en middelen, met bijzondere aandacht voor de reputatie van de onderneming, het cliëntenvertrouwen, de goede werking van het financieel systeem en de legale en maatschappelijke gevolgen.

Bij de aanschaf van oplossingen of diensten, die belangrijk zijn (of zullen worden) voor de veiligheid en/of continuïteit van de kritieke activiteiten, diensten en middelen, wordt in het selectie- en aankoopproces nagegaan of aan de interne veiligheids- en continuïteitsvereisten van het (i) betrokken lijnmanagement, (ii) de (onafhankelijke) operationele risicobeheersfunctie op ondernemingsniveau en (iii) het (interne) audit departement[6] wordt voldaan. Waar mogelijk en gepast maakt de instelling hierbij gebruik van internationaal erkende gezonde beheerpraktijken en/of standaarden[7]. Het bekomen van onafhankelijke certificaten, het (laten) uitvoeren van verificaties op de broncode, penetratietesten en kwetsbaarheidsanalyses, vormen hierbij nuttige hulpmiddelen[8].

4. Screening van personen en tegenpartijen

De instelling hanteert een aangepast proces dat in overeenstemming is met de relevante reglementering en wetgeving (bijvoorbeeld privacy- en databeschermingswetgevingen) voor de screening van de betrouwbaarheid en integriteit van interne medewerkers en externe partijen die door hun taken of opdrachten over belangrijke of gevoelige beheers- en/of toegangsrechten beschikken tot de kritieke activiteiten, diensten en middelen.

Alle personen en partijen die toegang krijgen tot kritieke activiteiten, diensten en middelen dienen schriftelijk geïnformeerd te worden over de geldende interne beleidslijnen en vereisten met betrekking tot veiligheid.

5. Sensibilisering

Het directiecomité zorgt voor de uitwerking en uitvoering van een aangepast sensibiliseringprogramma voor alle interne en externe personen die een invloed kunnen hebben op, of een rol te vervullen hebben met betrekking tot de operationele veiligheid en de continuïteit van haar kritieke activiteiten, diensten en middelen.

6 Dit gelaagde model voor risicobeheersing wordt ook het "3 lines of defense" model genoemd.

7 Bijvoorbeeld internationale standaarden inzake software-kwaliteit (ISO 25010, …).

8 Het CREST raamwerk van het Verenigd Koninkrijk voor kwaliteitsvolle, gecontroleerde en "intelligence"-gedreven cyber beveiligingstesten is een voorbeeld ter zake.

Het sensibiliseringprogramma voorziet o.a. in informatie met betrekking tot:

a) de toepasselijke wetgevingen en reglementeringen en de geldende interne beleidslijnen, richtlijnen en standaarden;
b) de bestaande rollen en verantwoordelijkheden binnen de organisatie met aandacht voor de taken en verantwoordelijkheden van alle betrokkenen;
c) de bestaande operationele veiligheids- en continuïteitsdreigingen en de bijdrage van eenieder om deze binnen aanvaardbare perken te houden.
d) veiligheidsgericht denken (bijvoorbeeld over hoe niet verleid te worden door phishing emails).

Het sensibiliseringsprogramma voorziet in de nodige periodieke actualisering en opfrissing van de informatie en wordt systematisch georganiseerd voor nieuwe medewerkers en dienstverleners die toegang krijgen tot de kritieke activiteiten, diensten en middelen van de onderneming.

6. Incident- en probleembeheer

De instelling beschikt in het kader van haar proactieve risicobeheersing en de effectieve detectie, indijking en herstelling van incidenten met een (potentieel) grote impact op de operationele veiligheid en/of de continuïteit van haar kritieke activiteiten, diensten en middelen, over

- gepaste middelen en processen[9] om proactief de belangrijkste continuïteits- en veiligheidsdreigingen en –dreigingsscenario's te identificeren, die moeten worden beheerd en voorbereid met een bijzondere focus op de noodzakelijke preventieve maatregelen;
- vooraf vastgestelde interne detectie, notificatie-, classificatie-, escalatie- en beheersprocedures en –plannen voor incidenten;
- op voorhand samengestelde "incident respons"-teams[10], waarvan de leden over de nodige management, technische en praktische kennis beschikken om de incidenten die zich kunnen voordoen, te beheren en de schade en/of verstoring van de kritieke activiteiten, diensten en middelen tot een minimum te beperken;
- interne en externe communicatieprocessen en vooraf aangeduide communicatieverantwoordelijken, die gebruik maken van op voorhand voorbereide communicatieplannen en –boodschappen voor de incidenten die zichtbaar zijn voor de buitenwereld en/of een belangrijke impact hebben op cliënten, het publiek, haar medewerkers en/of andere externe stakeholders;
- processen en teams die instaan voor de ex post analyse van belangrijke incidenten[11] met als doel de belangrijkste oorzaken ervan op te sporen, te rapporteren en te remediëren om een herhaling van het incident te vermijden.

De NBB verwacht door de instelling tijdig en gepast geïnformeerd te worden van alle incidenten met een belangrijke impact op de operationele veiligheid en/of de continuïteit van haar kritieke activiteiten, diensten en middelen. De instelling voorziet hiervoor de nodige maatregelen in haar interne incidentescalatie-, communicatie- en beheerprocedures[12].

9 Waar veel financiële instellingen vroeger afzonderlijke processen aanwendden om de continuïteits- en veiligheidsrisico's te identificeren en te prioriteren, hanteren nu meer en meer instellingen een geïntegreerd "Bedrijfs Impact Analyse"-proces voor de belangrijkste continuïteits- en veiligheidsdreigingen.

10 Indien de beschikbare interne experten en/of expertise niet voldoende zijn, dienen proactief externe technische middelen, adviseurs en/of forensische experten geïdentificeerd te worden en betrokken te worden tijdens en/of volgend op een belangrijk incident.

11 Indien de beschikbare interne experten en/of expertise niet voldoende zijn, dienen proactief externe technische middelen, adviseurs en/of forensische experten geïdentificeerd te worden en betrokken te worden tijdens en/of volgend op een belangrijk incident.

12 Bij wijze van leidraad verwacht de NBB minimaal geïnformeerd te worden over de operationele continuïteits- en veiligheidsincidenten die conform de interne incidentescalatie- en beheerprocessen worden geëscaleerd tot op het hoogste operationeel incidentbeheersniveau of –comité.

b. Bedrijfscontinuïteit

1. Inventaris

De instelling houdt een inventaris bij van haar kritieke activiteiten, diensten en middelen, die regelmatig (bijvoorbeeld jaarlijks) wordt bijgewerkt en veilig wordt bewaard.

De inventaris omvat minimaal:

- een “mapping” van de middelen die noodzakelijk zijn voor de kritieke activiteiten en diensten;
- de locaties en uitwijklocaties van de kritieke activiteiten, diensten en middelen;
- de datum waarop de betrokken uitwijklocaties en -oplossingen het laatst werden getest door middel van productie-nooduitwijktesten (cf. punt 10 hierna), met een kopie[13] van het testverslag en een synoptische weergave van de bekomen testresultaten (bv. succesvol, beperkte verbeteringen benodigd, …);
- de contactlijsten[14] met de kritieke medewerkers, leveranciers, onderaannemers en hun vervangers. Hierbij wordt een onderscheid gemaakt tussen de medewerkers die rechtstreeks instaan voor de betrokken functies en de ondersteunende facilitaire, IT- of andere medewerkers.

2. Herstel- en hervattingsobjectieven

De instelling maakt bij de bepaling van de herstel-en hervattingsobjectieven voor haar kritieke activiteiten, diensten en middelen een onderscheid tussen de “systeemrelevante kritieke activiteiten, diensten en middelen” en de “interne kritieke activiteiten, diensten en middelen”[15].

a. De systeemrelevante kritieke activiteiten, diensten en middelen

De instelling hanteert voor haar systeemrelevante functies een herstel- en hervattingsobjectief (“*Recovery Time Objective” of RTO[16])* van twee uur[17]. Deze RTO is van toepassing op alle noodzakelijke bedrijfsonderdelen en –middelen vanuit een “end to end”-perspectief, en geldt bijvoorbeeld ook voor (cf. schema in bijlage 1):

- ✓ de belangrijkste "front end" aanvoer/distributiekanalen en hun bijbehorende “back offices” en “back office”-oplossingen;
- ✓ de gebruikte oplossingen en middelen voor de centralisatie van de verrichtingen en de gegevens vanuit de verschillende aanvoer/distributiekanalen;
- ✓ de centrale “back office”-functies en “back office”-oplossingen die zorgen voor de verwerking en het operationeel (risico)beheer van de verrichtingen en gegevens;
- ✓ de oplossingen en kanalen voor de uitwisseling van de verrichtingen en/of hun gegevens met de centrale betalings-, verrekenings - en vereffenings-infrastructuren en de gereglementeerde financiële markten;
- ✓ de belangrijkste informatiekanalen naar de betrokken cliënten en/of andere externe “stakeholders” (toezichthoudende autoriteiten, …) betreffende de uitvoering en/of de afwikkeling van de verrichtingen of verleende diensten.

13 Of een elektronische link.

14 Of een elektronische link.

15 Cf. de definities onder 3.B. “Ratione materiae”

16 RTO staat voor de nagestreefde tijdsdoelstelling voor het herstellen en hervatten van de dienstverlening na een incident.

17 De vermelde RTO van 2 uur geeft een indicatie van de door de instelling na te streven doelstellingen bij het ontwerpen, implementeren en testen van haar herstel- en hervattingsoplossingen voor haar systeemrelevante activiteiten en diensten. De herstel- en hervattingsmaatregelen van de instelling tijdens een incident dienen voldoende aangepast te zijn aan de specifieke context en de karakteristieken van het incident.

Aanvullend op het voorgaande dienen de “business”-gerelateerde herstel- en hervattingsplannen en procedures ook te anticiperen op, en voorzieningen te treffen voor het eventuele optreden van incidenten kort voor het uitvoeren van kritieke einde-dag vereffenings- en/of verrekeningsprocessen. Indien noodzakelijk en waar mogelijk kan dit een verlenging van de normale werkuren in de instelling en de betrokken vereffenings- en/of verrekeningsinfrastructuren vereisen.

In het geval de voorziene noodoplossingen dataverlies aanvaarden (i.e. een “Recovery Point Objective” (RPO) hoger dan nul), dient ook rekening te worden gehouden met de tijd die nodig is om alle voor de hervatting benodigde gegevens terug samen en beschikbaar te stellen.

In uitzonderlijke situaties waarbij de data integriteit ernstig is aangetast ondanks alle door de instelling genomen voorzorgsmaatregelen met betrekking tot continuïteit en veiligheid, als gevolg van bijvoorbeeld een menselijke fout, een IT-fout en/of een (cyber) veiligheidsincident, kan de instelling ervoor opteren prioriteit te geven aan:

- het herstellen van de benodigde data-integriteit;
- of, in het geval van (cyber) veiligheidsincidenten, om bewarende maatregelen te nemen met het oog op het gerechtelijke of forensische onderzoek van de feiten en de opsporing en vervolging van de kwaadwilligen;

alvorens de getroffen dienstverlening en/of bedrijfsvoering terug te hervatten.

b. Interne kritieke activiteiten, diensten en middelen

De instelling bepaalt haar herstel- en hervattingsdoelstellingen conform de algemeen geldende principes in de circulaire PPB 2005/2.

3. Medewerkers

De instelling beschikt over een strategie, plan en aanpak om ervoor te zorgen dat ze in alle gebeurlijke omstandigheden[18] over voldoende (interne en externe) medewerkers beschikt met de nodige kennis en ervaring, om de goede werking van haar kritieke activiteiten, diensten en middelen te vrijwaren.

Hierbij houdt ze rekening met diverse risicoscenario’s zoals:

- hoogoplopend en langdurig ziekteverzuim[19] ten gevolge besmettelijke en /of dodelijke ziekten (pandemierisico), en/of voedselvergiftiging;
- sociale onrust (stakingen, manifestaties, blokkering van toegangswegen,…);
- menselijke schade bij de mogelijke gehele of gedeeltelijke vernietiging of beschadiging van (kantoor)gebouwen;
- de mogelijke blootstelling van medewerkers aan toxische substanties (bv. blootstelling aan asbest of de nabijheid van chemische transporten en/of productiefaciliteiten);

De instelling zorgt voor een opvolgings- en/of vervangingsplan, voor de medewerkers die belangrijk zijn voor de goede werking van de kritieke activiteiten, diensten en middelen en door hun specifieke expertise en/of beperkte aantal, moeilijk kunnen worden vervangen.

De instelling actualiseert en evalueert haar strategie, plan en aanpak regelmatig (bijvoorbeeld jaarlijks), rekening houdend met de evoluties op het vlak van de interne organisatie en de bedreigingen.

[18] Behoudens daden van oorlog of daarmee vergelijkbare grootschalige geweldplegingen en vernielingen door kwaadwilligen (terroristen, …).

[19] Voortbouwend op de ervaringen en de uitgevoerde simulaties in de financiële sector in 2006 en 2007 met betrekking tot een mogelijke pandemie van bvb. de vogelgriep, wordt hierbij uitgegaan van een mogelijk langdurig ziekteverzuim van 40% van de medewerkers over een periode van 3 maanden.

4. Datacenters

De instelling ondersteunt (minstens) haar kritieke activiteiten en diensten[20] vanuit minstens twee datacenters, die optreden als elkaars uitwijkoplossing en die:

a) voldoende ver van elkaar zijn verwijderd en een afzonderlijk risicoprofiel hebben conform de circulaire PPB 2005/2. In regel houdt dit in dat de betrokken data centers niet binnen dezelfde stedelijke agglomeratie zijn gevestigd en minimaal 15 kilometer[21] van elkaar verwijderd zijn. De instelling mag van deze regel afwijken op voorwaarde dat ze een voldoende onderbouwde risico-analyse voorlegt aan de NBB, die aantoont dat de aangewende of geplande oplossing in een gelijkwaardig niveau van residueel risico voorziet.
b) qua capaciteit voldoende gedimensioneerd zijn om de kritieke activiteiten en diensten op een adequate wijze te ondersteunen binnen de vooropgestelde herstel- en hervattingstermijnen (RTOs). Hierbij wordt ook rekening gehouden met mogelijke langdurige pannes of continuïteitsproblemen (bv. de gehele of gedeeltelijke vernietiging van een datacenter) en het feit dat een aantal functies die in de eerste uren volgend op de verstoring of ramp niet als kritiek worden beschouwd, na verloop van enkele uren of dagen wel kritiek kunnen worden. De instelling beschikt in dit kader over de benodigde bijkomende capaciteit of beschikt minimaal over een robuust en voldoende gevalideerd plan om de capaciteit, voldoende snel en op een betrouwbare en veilige wijze uit te breiden om alle noodzakelijke functies adequaat te ondersteunen, rekening houdend met hun herstel- en hervattingstermijnen.

De instelling huisvest de noodzakelijke IT-infrastructuur en data voor haar kritieke activiteiten en diensten in voldoende fysiek en logisch beveiligde data centers, waarbij voorzien is in de nodige redundantie van vitale nutsvoorzieningen (elektriciteit, telecom, koeling, water…) in overeenstemming met de Tier 3-standaard of hoger[22].

Bij de inrichting van nieuwe datacenters voor de kritieke activiteiten en diensten zorgt de instelling er bovendien voor dat deze:

- voldoende ver verwijderd zijn van alle door de instelling gebruikte sites voor haar kritieke activiteiten, diensten en middelen, om te vermijden dat verschillende locaties door eenzelfde incident zouden worden getroffen;
- zodanig zijn ingericht en beveiligd, dat het aantal medewerkers dat toegang behoeft tot de datacenters en daarin gehuisveste IT-systemen voor de kritieke activiteiten en diensten, tot een minimum wordt beperkt

De instelling laat het gepaste redundantieniveau en de fysieke beveiliging van de betrokken data centers en de gehuisveste kritieke IT-systemen periodiek (bijvoorbeeld eens om de 5 jaar of aan de hand van een meerjarige auditcyclus) uitvoerig auditeren door een onafhankelijke deskundige partij.

5. Telecomverbindingen

Omdat telecomverbindingen geregeld gepland en ongepland onbeschikbaar zijn door onderhouds- of herstellingswerkzaamheden en door pannes of incidenten (bv. leidingbreuken...), voorziet de instelling in voldoende redundante telecomverbindingen voor haar kritieke activiteiten en diensten. Dit geldt a fortiori voor telecomverbindingen die lange afstanden overbruggen, via meerdere landen lopen en/of een aaneenschakeling zijn van telecomverbindingen van meerdere telecomoperatoren.

[20] Voor de verwachtingen met betrekking tot de niet kritieke activiteiten, diensten en middelen verwijzen we naar de algemene bepalingen in de circulaire PPB 2005/2.
[21] De afstand van 15 kilometer dient enkel als een richtsnoer voor de ambitie die dient te worden nagestreefd door de instelling.
[22] Andere classificatiesystemen kunnen ook worden gehanteerd voor zover het redundantieniveau functioneel gelijkwaardig is.

In dit verband beschikt de instelling voor haar kritieke activiteiten en diensten over telecomverbindingen en -oplossingen die op een aantoonbare wijze (technische informatie en analyses, geografische beschrijving van de gebruikte telecomroutes, contracten …) voorkomen dat:

- een geplande of niet geplande onbeschikbaarheid van één telecomverbinding of –route aanleiding geeft tot een "single point of failure"[23] en/of een capaciteitstekort voor de ondersteuning van de kritieke activiteiten en diensten;
- problemen of pannes bij een enkele telecomaanbieder tot gevolg kunnen hebben dat de kritieke activiteiten en diensten geheel of gedeeltelijk buiten werking worden gesteld en/of niet langer over de voor hun goede werking benodigde telecomcapaciteit kunnen beschikken.

6. Werkplaatsen

De instelling zorgt ervoor dat de medewerkers die rechtstreeks of onrechtstreeks noodzakelijk zijn voor de goede werking van de kritieke activiteiten, diensten en middelen, beschikken over:

a) werkplaatsen en uitwijklocaties die voldoende fysiek beveiligd en logistiek uitgerust zijn, en enkel toegankelijk zijn via gepaste fysieke en logische toegangscontroles;

b) adequate oplossingen ingeval van mogelijke stroompannes (noodstroomvoorzieningen, …) die regelmatig (bijvoorbeeld jaarlijks) worden getest;

c) uitwijklocaties en –oplossingen, die voldoende ver verwijderd zijn van de normale werkplaatsen om niet door een zelfde incident of ramp te worden getroffen (cf. punt 9 hierna voor regionale incidenten of rampen). Indien uitwijkoplossingen worden gehanteerd zoals tele-werk, of het opsplitsen van meerdere medewerkers over vele verschillende kleinere locaties (vb. kantoren of agentschappen), voorziet de instelling in gepaste omkaderende werkings-, controle- en veiligheidsmaatregelen en -voorwaarden, om de daaruit voortvloeiende risico's voor de goede werking van de kritieke activiteiten en diensten binnen aanvaardbare perken te houden.

7. Back ups en gegevensopslag

De instelling zorgt ervoor dat haar technische opzet en de noodzakelijke componenten voor het nemen en het installeren van back ups en de opslag van kritieke gegevens, voldoende robuust, redundant en (fysiek en logisch) beveiligd zijn. Waar nodig voorziet de instelling ook in oplossingen om de consistentie van de gegevens te vrijwaren van logisch samenhangende toepassingen die gespreid zijn over verschillende systemen of oplossingen.

De instelling voert regelmatig testen uit om de bruikbaarheid en betrouwbaarheid van de back-up gegevens na te gaan.

8. "Denial of Service" (DOS)-aanvallen

De instelling beschikt over aangepaste maatregelen om de beschikbaarheid van haar kritieke activiteiten en diensten via het internet te verzekeren in het geval van cyberaanvallen die erop gericht zijn de toegang tot deze activiteiten en diensten te beletten of te verstoren ("Denial of Service"-aanvallen).

De genomen beschermende maatregelen op het vlak van de toepassingen en de netwerkverbindingen worden periodiek (bijvoorbeeld om de 3 jaar) getest om hun doeltreffendheid en efficiëntie te verifiëren en waar nodig bij te sturen.

[23] Een single point of failure is een potentieel risico veroorzaakt door een unieke afhankelijkheid in het design, de uitrol of de configuratie van een systeem of oplossing waarbij één probleem kan leiden tot het wegvallen van de volledige dienstverlening.

9. Noodvoorzieningen op grote afstand

De instelling voert een risicoanalyse uit met betrekking tot de kwetsbaarheid van haar kritieke activiteiten, diensten en middelen voor regionale rampen of incidenten, rekening houdend met de toepasselijke herstel- en hervattingsobjectieven (RTOs). Deze risicoanalyse wordt periodiek (bijvoorbeeld om de 3 jaar) geactualiseerd.

Waar nodig voorziet de instelling, rekening houdend met de vastgestelde kwetsbaarheden, de aard van de kritieke activiteiten en/of diensten en de potentiële impact op het financieel systeem, in bijkomende voorzorgsmaatregelen en/of uitwijk- en hersteloplossingen op grote afstand[24].

Voorbeelden van dergelijke bijkomende voorzorgsmaatregelen en/of uitwijk- en hersteloplossingen op het vlak van de datacenters en IT-systemen zijn:

- één of meerdere uitwijkdatacenters op grote afstand voor ten minste de kritieke activiteiten, diensten en middelen;
- één of meerdere herstelkopieën op grote afstand van de kritieke productie- en back up-gegevens, op basis waarvan de bedrijfsvoering, mogelijks met een beperkt doch aanvaardbaar verlies aan gegevens, terug kan worden hersteld en hervat.

Waar en voor zover noodzakelijk, gelet op de technologische beperkingen op grote afstand, voorziet de instelling in aangepaste herstel en hervattingsobjectieven (RTOs) voor de uitwijk van de kritieke activiteiten, diensten en middelen op grote afstand. De instelling informeert de Nationale bank van België indien ze tijdens haar risico-evaluatie vaststelt dat haar voorzorgs- en herstelmaatregelen op grote afstand niet toelaten om de herstel- en hervattingsobjectieven (RTOs) voor de systeemrelevante kritieke activiteiten, diensten en middelen (cf. punt 2.a hiervoor) na te leven.

10. Uitwijktesten

De instelling voert voor de kritieke activiteiten, diensten en middelen[25] periodiek (i.e. minimaal jaarlijks) productie-nooduitwijktesten uit voor de betrokken medewerkers en voor facilitaire en technische (IT-) systemen, waarbij de instelling op een adequate wijze aantoont dat:

a) ze de kritieke activiteiten, diensten en middelen op een gepaste en gecontroleerde manier kan overbrengen naar de voorziene uitwijkoplossingen en -locaties, en deze nadien kan terugbrengen naar de normale toestand. Hierbij is het van belang dat de uitwijkoplossingen, -plannen en -processen door alle betrokkenen voldoende gekend zijn en voldoende gedocumenteerd zijn om ook voldoende autonoom door minder ervaren medewerkers te kunnen worden uitgevoerd;
b) de voorziene uitwijkcapaciteit en -oplossingen volstaan om de kritieke activiteiten en diensten op een adequate wijze te ondersteunen. Hierbij dient de testperiode en/of de testduur zodanig te worden vastgelegd dat de uitwijkoplossingen tijdens de test niet enkel worden onderworpen aan lage of gemiddelde bedrijfsbelastingen (bv. tijdens een “bank holiday” of een verlengd weekend) maar ook (in de mate van het mogelijke) onderworpen worden aan hogere tijds- of seizoensgebonden piekbelastingen.
c) de gehanteerde uitwijkoplossingen voldoende betrouwbaar zijn voor de uitvoering van de kritieke activiteiten en het ter beschikking stellen van de kritieke diensten.

[24] Rekening houdend met de bestaande en in de nabije toekomst verwachte infrastructuur, de meteorologische, geografische en politieke context in West-Europa, moet “op grote afstand” worden begrepen als op een minimale afstand van 100 kilometer. De instelling mag van deze regel afwijken op voorwaarde dat ze een voldoende onderbouwde risicoanalyse voorlegt aan de NBB, die aantoont dat de aangewende of geplande oplossing in een gelijkwaardig niveau van residueel risico voorziet.

[25] Voor de verwachtingen met betrekking tot de niet kritieke activiteiten, diensten en middelen verwijzen we naar de algemene bepalingen in de circulaire PPB 2005/2.

De duurtijd van de productie-nooduitwijktesten voor de IT-systemen dient voldoende lang te zijn om representatieve besluiten te trekken met betrekking tot de vermelde doelstellingen in a, b) en c). De productie-nooduitwijktesten voor de medewerkers beslaan in regel één volledige werkdag of meer.

In het geval de voorziene noodoplossingen voor de kritieke activiteiten en diensten dataverlies aanvaarden (i.e. een “Recovery Point Objective” (RPO) hoger dan nul), dient ook de werkbaarheid en haalbaarheid van de procedures voor de recuperatie van de verloren gegevens binnen de vooropgestelde herstel- en hervattingsobjectieven op een gepaste wijze te worden getest en gevalideerd.

Bij in de tijd gefaseerde IT-productieuitwijktesten en uitwijkplannen, waarbij de IT-systemen van de niet kritieke activiteiten en diensten later worden heropgestart op de uitwijklocatie dan de IT-systemen van de kritieke activiteiten en diensten, verifieert en test de instelling dat de kritieke activiteiten en diensten adequaat blijven functioneren, in afzondering en in afwezigheid van de niet kritieke IT-systemen en toepassingen.

De instelling volgt een gefaseerd en projectmatig groeipad voor haar testen. De omvang en de complexiteit van de testen dient (waar en voor zover nodig) stelselmatig te worden verhoogd teneinde de vooropgestelde continuïteitsdoelstellingen te bereiken op een aantoonbare wijze, binnen een redelijke termijn.

11. Expertise en documentatie

De instelling beschikt over gepaste wettelijke en operationele oplossingen en waarborgen, om ervoor te zorgen dat ze zowel bij haar dagelijks beheer als bij incidenten en/of rampen, op een efficiënte en doeltreffende manier toegang heeft of krijgt tot de nodige expertise en/of technische en functionele documentatie van haar kritieke IT-systemen, toepassingen en gegevens.

c. Beveiligingsmaatregelen

1. "Defence in depth"-strategie

De instelling beschikt over een "defence in depth"-strategie voor haar logische en fysieke beveiliging, waarin de vroegere focus op de logische en fysieke perimeterbeveiliging wordt uitgebreid naar een bredere en diepgaandere beveiligingsaanpak, die steunt op meerdere complementaire en gedeeltelijk overlappende beveiligingslagen op fysiek vlak en doorheen de IT-systemen.

De verschillende beveiligingslagen hebben tot doel kwaadwillige daden te voorkomen en/of tijdig te detecteren, de mogelijke schade te beperken en/of beveiligingsincidenten beter te kunnen beheren. De kerngedachte hierbij is dat het falen van één verdedigingslijn gecompenseerd kan worden door één of meerdere andere verdedigingslijnen.

De instelling houdt in haar risicoanalyses en bij de ontwikkeling, implementatie en beoordeling van haar fysieke en logische beveiliging expliciet rekening met risicoscenario's waarbinnen kwaadwilligen er in geslaagd zijn de perimeterbeveiliging te doorbreken en/of te omzeilen (bv. via "social engineering") en zich toegang te verschaffen tot de interne bedrijfsgebouwen en IT-systemen.

2. Fysieke beveiliging

De fysieke beveiliging van de bedrijfsgebouwen en -middelen die aangewend worden voor de kritieke activiteiten en diensten, wordt centraal gecoördineerd en aangestuurd aan de hand van een veiligheidsstrategie en –politiek, aangevuld met de nodige processen en standaarden. De rollen en verantwoordelijkheden ter zake worden duidelijk toegewezen binnen de interne organisatie.

De instelling beschikt over een gepaste algemene toegangsbeveiliging en –controle, inclusief een permanente bewaking van de meest kritieke gebouwen, locaties[26] en middelen aan de hand van o.a. cameratoezicht en een modern inbraakalarmsysteem. De algemene beveiligingsmaatregelen worden waar nodig verder aangevuld met bijkomende beveiligingsmaatregelen (bv. bijkomende toegangscontroles) voor bepaalde kritieke activiteiten en/of locaties die omwille van hun aard extra gevoelig zijn (bv. de marktenzaal, de controlekamer voor de kritieke IT-systemen, datacenters, ...).

De permanente bewaking staat in voor de nodige preventieve en incidentgebonden contacten en samenwerking met de betrokken ordediensten (politie, …).

Het afdoend karakter van de fysieke beveiligingsmaatregelen maakt periodiek (bijvoorbeeld om de drie jaar) het voorwerp uit van gepaste audits.

3. Logische beveiliging

a. Perimeterbeveiliging

De instelling beschikt over een gecentraliseerd overzicht en veiligheidsbeheer van alle:

- websites, internettoepassingen (ook zogenaamde mobile apps) en netwerkverbindingen waarlangs derden zich toegang kunnen verschaffen tot de interne IT-systemen;

[26] Een locatie kan eveneens kritiek zijn wanneer ze kan worden gebruikt om zich logisch (bv. via netwerkconnecties, ….) toegang te verschaffen tot de kritieke activiteiten, diensten en middelen.

- toestellen en toepassingen (al dan niet beheerd door de instelling) die gemachtigd zijn om zich te verbinden met de interne IT-systemen;

De instelling beschikt ook over richtlijnen en oplossingen om:

- de ongeautoriseerde installatie van IT-componenten (bv. draadloze netwerken, ….) en/of toepassingen op te sporen, te voorkomen en/of te verbieden, die gebruikt kunnen worden om de perimeterbeveiliging te omzeilen en/of zich van buitenaf op een ongeautoriseerde manier toegang te verschaffen tot de interne IT-systemen.
- de in- en uitgaande communicatiestromen met externe partijen (professionele partners …) te beveiligen tegen en/of te controleren op onregelmatigheden die kunnen wijzen op veiligheidsincidenten;
- toe te zien op de gepaste beveiliging van de toestellen (draagbare computers, tablet computers, smartphones, ...) en toepassingen die geautoriseerd zijn om zich met de interne IT-systemen te verbinden van buiten en binnen de instelling, ongeacht of deze door de instelling worden beheerd of niet.

De instelling beveiligt haar netwerkverbindingen, IT-systemen en toepassingen die rechtstreeks toegankelijk zijn van buitenaf en a fortiori via het internet, via een combinatie van meerdere, grotendeels complementaire beveiligingsoplossingen en -technieken zoals netwerk- en applicatieve "firewalls", inbraakdetectiesystemen (“intrusion detection”), “hardening”[27] van IT-systemen, aangevuld met veiligheidsbewuste IT-ontwikkelings- en -aankooppraktijken (cf. hierna).

b. Veiligheidsbewust ontwikkelingen en aankopen

De instelling beschikt binnen haar IT-ontwikkelings- en aankoopcyclus over een proces en methodologie om de veiligheidsrisico’s te bepalen van te ontwikkelen en/of aan te schaffen IT-oplossingen.

Hierbij wordt o.a. rekening gehouden met veiligheidsrisico’s die verband houden met:

- de gebruikte technische IT-platformen en ontwikkelingstalen (.net, java, MF/Cobol, etc.),
- de gevoeligheid van de ondersteunde functionaliteiten, de uitgevoerde verrichtingen en/of de gebruikte gegevens voor misbruiken;
- de gebruiks- en veiligheidscontext waarin de oplossing zal functioneren (al dan niet toegankelijk van buitenaf, externe web-toepassing of interne back office toepassing, …).

In functie van de hoogte van de bekomen veiligheidsrisico’s, hanteert de instelling aangepaste beveiligingsoplossingen en/of vereisten, die op een consistente, gecontroleerde en voldoende aantoonbare wijze (i.e. via eigen testen en/of adequate externe certificaties) dienen te worden nageleefd.

De instelling beschikt voor de ontwikkelingsactiviteiten in eigen beheer (al dan niet intern of extern ontwikkeld) over een formeel kader voor het veiligheidsbewust ontwikkelen dat alle ontwikkelaars eenduidig en duidelijk informeert over de toe te passen ontwikkelingspraktijken en -oplossingen, met aandacht voor de nodige kwaliteits- en veiligheidstesten (bijvoorbeeld verplichte geautomatiseerde kwetsbaarheids- en/of code-nazichten) voor de in productiestelling en de na te leven procedures en/of richtlijnen.

De instelling besteedt de nodige aandacht en middelen aan de vorming en sensibilisering van de diverse functies die betrokken zijn bij haar IT-ontwikkelings- en aankoopcyclus (analisten, ontwikkelaars, architecten, testers, risk management, …) en een rol te vervullen hebben inzake de adequate beveiliging van de ontwikkelde en/of aangekochte IT-oplossingen.

[27] Beveiligingstechniek waarbij de IT-systemen worden "ontdaan" van alle overbodige functies (stripping genoemd) en belangrijke applicaties zoveel mogelijk worden beveiligd.

Waar mogelijk en gepast maakt de instelling bij het voorgaande gebruik van internationaal erkende gezonde beheerpraktijken en/of standaarden[28].

c. Segmentering en afzondering

De instelling voorziet in de nodige fysieke en logische segmentering van haar interne IT-systemen, om:

- ervoor te zorgen dat een IT-veiligheidsincident of –probleem in één segment van de IT-systemen, zich niet ongehinderd en/of ongemerkt kan verspreiden naar de andere segmenten van de IT-omgeving
- de kansen op een tijdige opsporing te vergroten door gepaste preventieve en detectieve controles uit te voeren bij overgangen tussen de segmenten;
- de omvang van eventuele schade binnen financieel en operationeel aanvaardbare grenzen te houden.

De instelling beschikt ter zake over een goedgekeurde segmenteringspolitiek en aangepaste technische standaarden en oplossingen, die consequent worden toegepast. De segmenteringspolitiek en de bijbehorende technische standaarden leggen de criteria vast op basis waarvan de verschillende segmenten worden bepaald. Hierbij wordt bijvoorbeeld rekening gehouden met diverse aspecten zoals:

- de mate waarin bepaalde IT-systemen en/of toepassingen worden blootgesteld aan hoger dan gebruikelijke bedreigingen of beveiligingsrisico's, zoals bijvoorbeeld de DMZ's[29] en bureau-omgeving (desktop systemen, mobiele toestellen, …);
- de gevoeligheid van de ondersteunde bedrijfs- en/of IT-processen en/of de opgeslagen gegevens, voor bijvoorbeeld fraude, gegevensdiefstal, sabotage, ...;
- de logische samenhang van bepaalde IT-systemen en/of toepassingen, waardoor de betrokken IT-systemen een vergelijkbaar risico- en/of aanwendingsprofiel hebben en afwijkende handelingen, en/of gegevensstromen gemakkelijker kunnen worden opgespoord;
- de verhoogde kwetsbaarheid van een aantal IT-systemen en/of toepassingen omdat deze verouderd en/of niet voldoende "gepatcht" zijn of onvoldoende het voorwerp hebben uitgemaakt van veilige ontwikkelingstechnieken;
- het eventueel lagere beveiligingsniveau van de test- en ontwikkelingsomgevingen in vergelijking met de productieomgeving;
- de mogelijke proliferatie van veiligheidsincidenten ten gevolge van de gedeelde authenticatieoplossingen en -architecturen (bijvoorbeeld "Single Sign-on"[30], …).

Aansluitend en parallel hiermee, zorgt de instelling voor voldoende fysieke en logische afzondering van haar kritieke activiteiten, diensten en middelen, om ongeautoriseerde toegangen en misbruiken te voorkomen, te detecteren en/of binnen aanvaardbare proporties te houden.

[28] Bijvoorbeeld de "Open Web Application Security Project" (OWASP)-richtlijnen betreffende de beveiliging van software of internationale standaarden inzake software-kwaliteit (ISO 25010, …).

[29] Een gedemilitariseerde zone (DMZ) is een netwerksegment dat zich tussen het interne en externe netwerk bevindt.

[30] ''Single Sign-on"-oplossingen stellen eindgebruikers in staat om eenmalig in te loggen waarna automatisch toegang wordt verschaft tot meerdere applicaties en resources in het netwerk.

d. Sterke authenticatie en beheer van de toegangsrechten

Gebruikersnamen en paswoorden kunnen relatief gemakkelijk worden ontfutseld of gestolen waardoor deze niet volstaan voor de beveiliging van kritieke activiteiten, diensten en middelen die door hun aard (fraudegevoeligheid, hoge confidentialiteit en/of sensitiviteit, operationeel bedrijfskritiek karakter) bevoorrechte doelwitten vormen voor interne en externe kwaadwilligen. Voorbeelden hiervan zijn geprivilegieerde beheertoegangen tot kritieke of gevoelige IT-systemen, toepassingen en gegevens, alsook de toegangen tot fraudegevoelige betalingstoepassingen of betaalkaartgegevens. Voor deze laatste functies beschikt de instelling over sterke authenticatieoplossingen[31].

De instelling beschikt over een authenticatiebeleid waarin duidelijk wordt aangeven welke kritieke activiteiten, diensten en middelen gebruik moeten maken van sterke authenticatie oplossingen.

Daarnaast zorgt de instelling voor een efficiënt en kwaliteitsvol beheer van de toegangsrechten en ziet ze zorgvuldig toe op de correcte invulling en naleving van het “least privilege” en “need to know” principe.

Hierbij:

- gebruikt de instelling authenticatiebeheersoplossingen waarbij de toegangsrechten van personen worden toegekend en beheerd in functie van de rollen en specifieke taken die deze personen vervullen, met inachtneming van de nodige functiescheidingen. De processen voor het tijdig aanpassen van de toegangsrechten bij de aanwerving, het vertrek of de interne overplaatsing van medewerkers krijgen hierbij bijzondere aandacht;
- beschikt elke toepassing, elk proces en elke gebruiker enkel over de strikt noodzakelijke privileges en toegangsrechten die nodig zijn voor de uitvoering van hun taken. Aldus dient bv. het gebruik van email en/of het surfen op het internet met een geprivilegieerd beheerdersprofiel zoveel als mogelijk worden vermeden.
- worden belangrijke en/of gevoelige geprivilegieerde beheertoegangen zoveel mogelijk op een gecontroleerde wijze toegekend en beperkt in de tijd (“Just In Time” of “Deny By Default Administration”), functioneel ingeperkt (“Just Enough Administration”) en onderworpen aan een aangepaste “logging” en “monitoring”.

e. Logs, audit trails en monitoring

Logs en audit trails zijn noodzakelijk om, in combinatie met geschikte monitoring- en onderzoeks-oplossingen, veiligheidsincidenten tijdig te kunnen opsporen en na de feiten alle kwaadwillige daden te kunnen reconstrueren en herstellen. De instelling beschikt daarom over adequate veiligheidslogs en -auditrails van haar IT-systemen en toepassingen, die op een afzonderlijke en voldoende beveiligde plaats worden aangelegd en bewaard om hun betrouwbaarheid te vrijwaren. De historiek van de te bewaren logs dient de effectiviteit van de instelling bij het detecteren van kwaadwillige activiteiten en/of aanvallen in beschouwing te nemen.

Daarnaast beschikt de instelling over een monitoringpolitiek, "real time" of "near real time" monitoring oplossingen en a posteriori onderzoeksoplossingen, die aangepast zijn aan de aard en de omvang van de bedreigingen en erop gericht zijn belangrijke beveiligingsincidenten zo snel mogelijk op te sporen met het oog op een efficiënte en doeltreffende incidentrespons.

[31] I.e. authenticatieoplossingen die minstens 2 van de navolgende elementen combineren: 1) iets dat alleen de gebruiker weet, 2) iets dat alleen de gebruiker heeft, 3) iets dat de gebruiker is (bijvoorbeeld biometrische gegevens), waarbij de verschillende elementen onderling onafhankelijk zijn en tenminste één element niet herbruikbaar is en niet ongemerkt kan worden gestolen. Ook de plaats waar de gebruiker zich bevindt (“where I am”) kan hierbij van belang zijn.

De instelling beschikt in dit verband minimaal over een aangepast operationeel monitoring- en analysesysteem voor beveiligingsalarmen en/of - incidenten die verband houden met:

- inbraakpogingen aan haar IT-perimeter;
- verdachte activiteiten in verband met haar meest gevoelige en/of kritieke systemen, toepassingen en gegevens die bevoorrechte doelwitten vormen voor interne en externe kwaadwilligen (bv. betalingstoepassingen, gevoelige betaalkaart of cliëntengegevens, kritieke IT-beheersconsoles en/of –toepassingen, …);
- verdachte uitgaande netwerkverbindingen en/of informatiestromen die mogelijks afkomstig zijn van kwaadwillige software, indringers en/of externe aanvallers met toegang tot de interne IT-systemen;
- de ongeautoriseerde aanmaak of aanwending van geprivilegieerde toegangsrechten.

Gelet op de aard van de betrokken veiligheidsrisico's en bedreigingen, en de specificiteit van de monitoringwerkzaamheden, zorgt de instelling voor voldoende personeel met een aangepaste opleiding om dergelijke incidenten op een permanente en continue basis op te volgen en te onderzoeken. De vastgestelde beveiligingsincidenten worden behandeld conform een vooraf goedgekeurd incidentescalatie- en incidentrespons proces.

De instelling voert ook periodiek gepaste aangekondigde en onaangekondigde testen uit, waarbij niet-geautoriseerde activiteiten en/of aanvalsscenario's worden gesimuleerd, met de bedoeling de doeltreffendheid van de monitoringoplossingen en de bijhorende escalatieprocedure voor incidenten te evalueren.

f. Kwetsbaarheidsopvolging en onafhankelijke testen

De instelling beschikt over geautomatiseerde oplossingen om de beveiligingskwetsbaarheden aan haar IT-perimeter en in haar interne IT-systemen regelmatig (bijvoorbeeld maandelijks) op te sporen en om de nodige correctieve maatregelen door te voeren.

De instelling laat ook periodiek (bijvoorbeeld om de drie jaar) uitgebreide veiligheidstesten doorvoeren, waarbij onafhankelijke deskundige specialisten de efficiëntie en de kwaliteit van de beveiliging nagaan door de ethische uitvoering van realistische aanvalsscenario's waarbij diverse aanvalsmethoden en –technieken worden aangewend. Voorbeelden van dergelijke aanvalsscenario's omvatten pogingen om:

- van buitenaf in te breken in de interne IT-systemen en gevoelige en/of kritieke verrichtingen uit te voeren en/of toegang te verkrijgen tot gevoelige en/of kritieke gegevens;
- van binnenuit door te dringen in de interne IT-systemen, vertrekkend van een gewone gebruikers werkpost of een interne netwerkpoort, met als doel gevoelige en/of kritieke verrichtingen uit te voeren en/of toegang te krijgen tot gevoelige en/of kritieke gegevens.

Indien en zolang de voorgaande grondige onafhankelijke experttesten belangrijke kwetsbaarheden aantonen van de perimeter en/of interne IT-beveiliging, zorgt de instelling ervoor dat deze testen regelmatig worden herhaald (bijvoorbeeld jaarlijks) om de vastgestelde tekortkomingen en de effectiviteit van de genomen correctieve maatregelen van nabij op te volgen en waar nodig bij te sturen.

4. Inwerkingtreding

De circulaire treedt in werking op 1 januari 2016. De NBB verwacht van de systeemrelevante instellingen dat zij hun bedrijfscontinuïteits- en veiligheidsbeleid en –oplossingen evalueren in de loop van de 6

maanden die volgen op de datum van inwerkingtreding van deze circulaire, en waar nodig bijsturen in het licht van de gezonde beheerspraktijken vermeld in deze circulaire.

Voor de aspecten die voor hun technische invulling en realisatie belangrijke organisatorische aanpassingen en termijnen voor tenuitvoerlegging vergen, stellen de betrokken instellingen een programma op om de vooropgestelde doelstellingen binnen een redelijke termijn – te beoordelen in het licht van de aard, schaal en complexiteit van hun bedrijf – te halen. Indien dit programma termijnen hanteert, die een periode van twee en een half jaar na de datum van inwerkingtreding van deze circulaire overschrijden, dient dit met de NBB te worden besproken. De voormelde spreiding van tenuitvoerlegging vormt geen beletsel voor de prudentiële beoordeling door de NBB van het bedrijfscontinuïteits- en veiligheidsbeleid op basis van de onderhavige beheerspraktijken.

Gelieve te noteren dat wij de commissaris(sen), erkend revisor(en) van uw instelling een kopie van deze circulaire bezorgen.

Jan SMETS
Gouverneur

Bijlage: 1