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

Circular

Brussels, 18 December 2015

Reference: NBB_2015_32

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

Additional prudential expectations regarding operational business continuity and security of systemically important financial institutions

Scope

Systemically important financial institutions governed by Belgian law as referred to in Article 3, 29°, of the Law of 25 April 2014 on the legal status and supervision of credit institutions, and Article 36/3, § 2, of the Organic Law[1].

Summary/Objectives

Provide an explanation to systemically important financial institutions about the expectations of the National Bank of Belgium (NBB) regarding their operational business continuity and security.

Dear Madam,
Dear Sir,

1. Rationale

Systemically important financial institutions should devote particular attention to the continuity of their services and the security of their operations, in the light of:

- their critical role in the financial system and their great social importance;
- the fact that, precisely because of their systemic character and/or their high visibility and strong reputation, they may be privileged targets for both external and internal persons with malicious intentions (criminals, terrorists, etc.).

[1] According to Article 36/3, § 2, of the Organic Law, the Bank must determine, among the financial institutions referred to in Article 36/2, with the exception of credit institutions, those that must be considered as system-relevant and must inform each one of these institutions.

2. Introduction

This circular aims to provide clarification to systemically important financial institutions on the additional prudential expectations of the NBB regarding their operational business continuity and security. It replaces the guidelines of the former Financial Stability Committee (FSC) of 20 October 2004 on business continuity for systemically important banks.

The circular complements the following existing circulars:

- PPB 2005/2 on sound management practices in respect of business continuity;
- PPB 2004/5 and PPB-2006-1-CPA on sound management practices for outsourcing;
- CBFA_2009_17 on financial services via the internet;

and must be read and complied with together with the aforementioned provisions. Any deviations should be explained to the NBB ("comply or explain")[2].

Those systemically important financial institutions which are considered to be critical infrastructures and therefore also fall under the Bank's oversight must, along with the prudential expectations set out in this circular, also fulfil the expectations under the oversight regulations.

3. Scope

A. Ratione personae

The sound management practices set out in this circular apply to systemically important credit institutions, insurance companies and payment institutions governed by Belgian law.

B. Ratione materiae

This circular concerns the adequate protection of critical activities, services and resources (buildings, assets, applications, data, etc.) of systemically important financial institutions against irreversible operational damage or lengthy disruption, irrespective of whether the cause is human (pandemic, malicious acts, etc.) or technical in nature (failures, destruction or damage to critical buildings or resources, etc.).

The circular covers the critical services, resources and functions of which the disruption or destruction may:

a) jeopardize the proper functioning of the financial system, because of their operational importance for the central financial infrastructures for payment processing, clearing and settlement of securities transactions and/or for the operation of regulated financial markets (hereinafter "systemically important critical activities, services and resources");
b) seriously disrupt the internal business management and cause discontinuities in the delivery of services, but has little or no effect on the proper functioning of the central financial infrastructures for the processing of payments, the clearing and settlement of securities transactions and/or for the operation of regulated financial markets (hereinafter "internal critical activities, services and resources").

[2] This circular and the other circulars mentioned are also used by the NBB as a guideline as regards institutions subject to prudential supervision for its statutory supervisory task under the Law of 1 July 2011.

Unless an explicit distinction needs to be made between the "systemically important" and the "internal" critical activities, services and resources, the circular will apply the more general and overarching concept of "critical activities, services and resources".

The prudential expectations regarding the preparation and drawing-up of recovery plans and resolution plans in accordance respectively with Articles 108 to 116 and 226 to 232 of the Law of 25 April 2014, fall outside the scope of this circular.

As the NBB is not competent to monitor compliance with privacy and/or data protection laws, the specific security and confidentiality related requirements in the privacy and/or data protection laws fall outside the scope of this circular.

Where relevant, the sound management practices concern:

- centralised and decentralised business units and buildings;
- support functions (at group level);
- centralised and decentralised IT systems, databases and applications;
- outsourcing within the group and/or with external counterparties;

that provide critical activities, services and/or resources to systemically important credit institutions, insurance companies and payment institutions governed by Belgian law.

4. Sound management practices

A. General framework

1. Strategy, policy and risk analysis

The management committee is responsible for developing a strategy and a policy to adequately safeguard the security[3] and continuity of its critical activities, services and resources. As regards security, the institution should make a clear distinction between physical and logical security (see chapter 4.C). Wherever possible and appropriate, the institution makes use of internationally recognised sound management practices and/or standards[4].

The management committee should monitor the implementation and effectiveness of the risk management, of the precautionary measures which have been taken and of the internal controls. To this end, it should have a security plan and an appropriate reporting system which specifically address the risk analysis of vulnerabilities and threats, and the measures planned by the company.

The management committee should report at least annually to the board of directors on the operation and effectiveness of the strategy, policy and plan to adequately safeguard the operational security and continuity of its critical activities, services and resources.

The board of directors and the management committee should have appropriate expertise, or engage with (internal or external) experts to assist them, to perform their oversight responsibilities.

[3] Security also includes protecting the integrity of critical data and applications.

[4] For example standards on IT security (ISO 27001/27015, etc.) and business continuity (ISO 22301, etc.).

The strategy, policy and security plan at least provide clarification on:

a) the objectives (risk tolerance) of the company with regard to (physical and logical) security and the continuity of its critical activities, services and resources;
b) the internal governance, with particular attention for the policy-making and supervisory bodies and processes, and the roles and responsibilities of all persons involved;
c) the applicable reporting lines and expectations;
d) the classification criteria and approach used for the identification of critical activities, services and resources;
e) the training and/or awareness-raising measures provided for (see point 5 below);
f) the policy followed and the internal control requirements in case of outsourcing of critical activities, services and resources;
g) the provision of contact points where irregularities and / or suspicious events can be reported by internal staff or external parties (clients, suppliers, etc.).

In this respect, the internal audit function should periodically:

- test the correct implementation and effectiveness of the strategy, policy and security plan defined, and the quality of the risk analysis and risk reporting performed; and
- report on this matter to the audit committee.

2. IT complexity and vulnerability management

The institution should have an appropriate governance system in place in order to keep the complexity of its IT systems at a manageable level and to prevent the complexity of the IT systems from jeopardising the proper management of the operational security and continuity of critical activities, services and resources.

In this context, the company should define the responsibilities and processes for making the necessary technological and architectural choices from a company perspective, both in the short as well as in the long run. These choices should then be translated and communicated in the form of appropriate technical standards and guidelines which should be complied with. Wherever possible and appropriate, the institution makes use of internationally recognised sound management practices and/or standards[5]. Any deviations from these standards and guidelines must be subject to an appropriate validation process.

In order to manage IT complexity, the institution should also have a full and reliable (centralised, decentralised or federated) inventory of all IT and configuration components (i.e. a Configuration Management Database or CMDB), that allows it inter alia to manage and ensure:

- timely patching of all important software and hardware components from a security or business continuity point of view;
- timely replacement and/or upgrading of obsolete and/or outdated technologies.

The institution should also have formal processes in place to:

a) proactively identify and phase out in a timely manner all IT, configuration and architecture components that are or may become “End Of Life”; and
b) acquire, test, and deploy software patches based on criticality and track and prioritize missing patches across all environments;

in order to ensure and maintain the operational security and continuity of the critical activities, services and resources.

[5] For example standards on enterprise-architecture (TOGAF, ISO 42010, SABSA, etc.).

Outdated IT components, overdue unpatched high-risk vulnerabilities and inadequate technologies and/or architectures which may significantly (directly or indirectly) compromise the operational security and continuity of critical activities, services and resources, should be reported to senior management in a timely manner and should be included in the annual reporting to the management committee, so that the necessary corrective approach and/or measures can be included in the security plan.

3. Risk analysis and approval

The institution should have formally structured processes for analysing and approving operational security and continuity risks, (at least) for its critical activities, services and resources, associated with and/or arising from:

- significant changes in business operation (e.g. new products, services, external service providers or organisational models);
- the introduction of new technologies and/or architectures;
- major new business investments and/or projects.

In addition to the traditional financial and commercial cost-benefit analysis, a risk analysis should also be conducted of the impact on the operational security and continuity of at least the critical activities, services and resources, with particular attention for the company's reputation, customers' confidence, the proper functioning of the financial system and legal and social consequences.

When procuring solutions or services that are (or will become) important for the security and/or continuity of the critical activities, services and resources, the institution should check, during the selection and purchase process, whether the internal security and continuity requirements of the (i) business line management, (ii) the (independent) corporate operational risk management function and (iii) the (internal) audit department[6] are met. To this end, the institution makes use of internationally recognised sound management practices and/or standards, wherever possible and appropriate[7]. In this respect, it may be useful to obtain independent certificates and to perform or have performed verifications of the source code, penetration tests and vulnerability analyses[8].

4. Screening of persons and counterparties

The institution should use an appropriate process for screening the reliability and integrity of internal staff and external parties that by reason of their duties or assignments have important or sensitive administration rights and/or access rights to the critical activities, services and resources, that is compliant with all relevant regulations and legislation (e.g. privacy and the data protection laws).

All persons and parties who have access to critical activities, services and resources should be informed in writing of the applicable internal security policies and requirements.

[6] This layered risk management organisation model is often referred to as the "3 lines of defence".
[7] For example international standards on software quality (ISO 25010, etc.).
[8] For example the UK CREST framework to deliver controlled, tailored, intelligence-led cyber security tests.

5. Awareness-raising

The management committee should develop and implement an appropriate awareness-raising program for all internal and external persons who may influence or have a role to play in the operational security and continuity of its critical activities, services and resources.

The awareness-raising programme provides *inter alia* information regarding:

a) the applicable laws and regulations and the applicable internal policies, guidelines and standards;
b) the existing roles and responsibilities within the organisation, with due attention for the roles and responsibilities of all persons involved;
c) the existing operational security and continuity threats and everyone's contribution to keep them within reasonable limits;
d) security-based thinking (e.g. on how not to fall for phishing emails).

The awareness-raising programme provides for the necessary periodic updating and refreshing of the information and is systematically organised for new employees and service providers who have access to the critical activities, services and resources of the institution.

6. Incident and problem management

For the proactive risk mitigation, and the effective detection, containment, remediation and recovery of incidents with a (potentially) high impact on the operational security and/or continuity of its critical activities, services and resources, the institution should have adequate:

- resources and processes[9] in place to proactively identify the main continuity and security threats and threat scenarios that need to be managed and prepared for, with a special focus on the necessary preventative measures;
- pre-established internal incident detection, notification, classification, escalation and management processes and plans;
- previously selected incident response teams[10], the members of which have the necessary management, technical and practical knowledge in order to manage possible incidents and to minimise the damage and/or disruption of critical activities, services and resources;
- internal and external communication processes and pre-identified communication managers that make use of pre-established communication plans and messages for incidents that are visible to the outside world and/or have a significant impact on customers, the public, its staff and/or other external stakeholders;
- processes and teams responsible for conducting an ex post analysis of major incidents[11], with a view to identifying, reporting and remedying their main causes, in order to prevent any recurrence of the incident.

[9] Where formerly at the business side, many financial institutions used different processes to identify and prioritize the continuity and security risks, more and more institutions are now adopting (or are evolving towards) an integrated Business Impact Analysis process, where the business identifies and assesses the main continuity and security threats and threat scenarios for its business activities.

[10] When the available internal specialist resources and/or know-how are not sufficient, external technical sources, consultants and/or forensic specialists should be proactively identified and called upon during and/or following an important incident.

[11] When the available internal specialist resources and/or know-how are not sufficient, external technical sources, consultants and/or forensic specialists should be proactively identified and called upon during and/or following an important incident.

The NBB expects to be informed adequately and in a timely manner of all incidents with a major impact on the operational security and/or continuity of the critical activities, services and resources of the institution. In this respect, the institution should lay down the necessary measures in its internal incident escalation, communication and management procedures[12].

B. Business continuity

1. Inventory

The institution should keep an inventory of its critical activities, services and resources which is updated regularly (for example annually) and which is securely stored.

This inventory should include at least:

- a mapping of the resources which are required for the critical activities and services,
- the sites and fall-back sites for critical activities, services and resources;
- the date on which the fall-back sites and solutions were last tested by means of production emergency fall-back tests (see point 10 below), a copy[13] of the test report and a synoptic description of the test results obtained (e.g. successful, limited improvements required , etc.);
- the contact lists[14] of critical employees, suppliers, subcontractors and their alternates. In this respect, a distinction should be made between employees who are directly responsible for the functions involved and the supporting facilities and employees (IT or other).

2. Recovery and resumption objectives

In determining the recovery and resumption objectives for its critical activities, services and resources, the institution should make a distinction between the "systemically important critical activities, services and resources" and the "internal critical activities, services and resources"[15].

a. Systemically important critical activities, services and resources

For its systemically important functions, the institution should set a recovery and resumption objective (Recovery Time Objective or RTO[16]) of two hours[17]. This RTO should apply to all necessary business units and resources from an end-to-end perspective and should also apply for example to (see diagram in annex 1):

- ✓ the main front-end supply / distribution channels and the corresponding back offices and back-office solutions;
- ✓ the solutions and resources used for the centralization of the transactions and data from the various supply / distribution channels;

[12] As an indication, the NBB expects to be informed at least about the operational continuity and security incidents which are escalated to the highest operational incident management level or committee in accordance with the internal incident escalation and management processes.

[13] Or an electronic link.

[14] Or an electronic link.

[15] See the definitions under 3.B. "Ratione materiae"

[16] RTO is defined as the time objective pursued for recovering and resuming services after an incident.

[17] The RTO of 2 hours serves as an indication of the ambition that should be pursued by the supervised institution when designing, implementing and testing its recovery solution for its systemically important activities and services. The recovery and resumption actions to be undertaken by the institution during the incident should be adequately adapted to the specific context and the characteristics of the incident.

- ✓ the central back-office functions and back-office solutions for the processing and the operational (risk) management of transactions and data;
- ✓ the solutions and channels for the exchange of transactions and/or the corresponding data with the central payment, clearing and settlement infrastructures and regulated financial markets;
- ✓ the main information channels towards clients and/or other external stakeholders (supervisory authorities, etc.) concerning the execution and/or settlement of transactions or provided services.

Complementary to the foregoing, the business recovery and resumption plan and procedures should also anticipate on and prepare for the possible occurrence of incidents shortly before the execution of critical end-of-day settlement processes. If necessary and where possible, this may require the extension of normal working hours in the institution and the involved settlement infrastructure.

If the emergency solutions envisaged accept data loss (i.e. Recovery Point Objective (RPO) higher than zero), account should also be taken of the time required to reconstitute and make available all data required for the resumption.

In exceptional circumstances where the integrity of the data is seriously affected, despite all precautionary continuity and security measures taken by the institution, due, for example, to human error, an IT error and/or a (cyber) security incident, the institution may choose to give priority:

- to restoring the data integrity required;
- or, in case of (cyber) security incidents, to taking protective measures for the purposes of the criminal inquiries or the forensic investigation of the facts and the detection and prosecution of persons with malicious intentions;

before resuming the affected delivery of services and/or business operation.

b. Internal critical activities, services and resources

The institution should define its recovery and resumption objectives in accordance with the generally prevailing principles set out in Circular PPB 2005/2.

3. <u>Staff</u>

The institution should have a strategy, plan and approach to ensure that in all circumstances[18], it has sufficient (internal and external) staff at its disposal with the necessary knowledge and experience to safeguard the proper functioning of its critical activities, services and resources.

In this respect, it should take into account various risk scenarios, such as:

- a high rate of absenteeism and long-term absenteeism[19] due to infectious and/or fatal diseases (pandemic risk) and/or food poisoning;
- social unrest (strikes, demonstrations, roadblocks, etc.);

[18] Except for acts of war or similar large-scale assaults and destruction by people with malicious intentions (terrorists, etc.).

[19] Building on the experiences and simulations carried out in the financial sector in 2006 and 2007 with regard to a possible pandemic of for example bird flu, a possible long-term absenteeism of 40% of staff over a period of 3 months is assumed.

- human casualties in case of total or partial destruction of or damage to (office) buildings;
- the possible exposure of staff to toxic substances (e.g. asbestos exposure or proximity of chemical transport and/or production facilities).

The institution should provide for a monitoring and/or replacement plan for employees who are crucial for ensuring the proper functioning of the critical activities, services and resources and who are difficult to replace due to their specific expertise and/or limited number.

The institution should regularly (for example annually) update and assess its strategy, plan and approach in the light of developments in internal organisation and threats.

4. Data centres

The institution should support (at least) its critical activities and services[20] from at least two data centres, which are each other's fall-back solution and which:

a) are located sufficiently far from each other and have separate risk profiles, in accordance with Circular PPB 2005/2. As a rule, this means that the data centres are not located within the same metropolitan area and are 15 kilometres[21] - or more - apart. The institution may derogate from this rule, provided that it submits to the NBB a duly substantiated risk analysis which demonstrates that the solution that is applied or planned provides an equivalent level of residual risk.
b) in terms of capacity, are sufficiently strong to adequately support its critical activities and services within the pre-established recovery and resumption periods (RTOs). In this respect, it also takes account of possible long-term failures or continuity problems (e.g. the total or partial destruction of a data centre) and of the fact that a number of functions that are not considered critical in the first hours following the disruption or disaster, may become critical after a few hours or days. The institution should have the necessary additional capacity or should at least have a robust and sufficiently validated plan to expand the capacity with sufficient speed and in a reliable and safe way, in order to adequately support all necessary functions, taking account of their recovery and resumption periods.

The institution should house the necessary IT infrastructure and data for its critical activities and services in data centres that are sufficiently secured, both physically and logically, and provide for the necessary redundancy of vital utilities (electricity, telecommunications, cooling, water, etc.) in accordance with the Tier 3 or higher standard[22].

The institution should also ensure that when opening new data centres for its critical activities and services, these data centres:

- are sufficiently far away from all sites used by the institution for its critical activities, services and resources, in order to avoid having different locations affected by the same incident;
- are designed and secured in such a way that the number of employees who must have physical access to the data centres and the IT systems for its critical activities and services that are housed in these data centres is kept to a minimum.

[20] For the expectations regarding non-critical activities, services and resources, please refer to the general provisions of Circular PPB 2005/2.
[21] The distance of 15 kilometres only serves as an indicator of the ambition that should be pursued by the institution.
[22] Other classification systems may also be used, provided that the redundancy level is functionally equivalent.

The institution should ensure that the appropriate redundancy level and the physical security of the data centres and the critical IT systems are subject to comprehensive audits, which should be carried out periodically (for example every five years or based on a multiannual audit cycle) by an independent expert party.

5. Telecom connections

As telecom connections are often subject to planned or unplanned unavailability, due to maintenance or repair work and failures or incidents (e.g. physical line ruptures, etc.), the institution should have sufficient redundant telecom connections for its critical activities and services. This applies in particular for long-distance telecom connections which pass through several countries and/or for chains of telecom connections delivered by different telecom operators.

For its critical activities and services, the institution should have telecom connections and solutions which avoid in a demonstrable manner (i.e. through technical information and analyses, geographical description of the telecom routes used, contracts, etc.) that:

- a planned or unplanned unavailability of one telecom connection or route causes a single point of failure[23] and/or a shortage of capacity to support the critical activities and services;
- problems or failures of one single telecom provider can cause the operation of critical activities and services to be suspended in whole or in part and/or result in the unavailability of the telecom capacity required for their proper functioning.

6. Workplaces

The institution should ensure that for staff that is directly or indirectly necessary for the proper functioning of critical activities, services and resources, it has:

a) workplaces and fall-back sites which are provided with sufficient physical security and logistical equipment and which are accessible only through appropriate physical and logical access controls;

b) adequate solutions in the event of power failures (emergency power supplies, etc.) which are tested regularly (for example annually);

c) fall-back sites and solutions which are sufficiently far away from the normal workplaces in order not to be affected by the same incident or disaster (see point 9 below for regional incidents or disasters). If fall-back solutions are used, such as telework, or the reallocation of various employees to various smaller locations (e.g. offices or agencies), the institution should lay down appropriate relevant operating, monitoring and security measures and conditions to ensure that any resulting risks to the proper functioning of the critical activities and services can be kept within reasonable limits.

7. Backups and data storage

The institution needs to ensure that its technical measures and the necessary components for making and restoring backups and storing critical data are sufficiently robust, redundant and secured (both physically and logically). Where necessary, the institution should also provide

[23] A single point of failure is a potential risk caused by a unique dependence of the design, deployment or configuration of a system or solution whereby one problem can lead to a complete failure to deliver services.

solutions to safeguard the data consistency of interdependent applications that are spread over different systems or solutions.

The institution should regularly carry out tests to assess the usefulness and reliability of the backup data.

8. Denial of Service (DOS) attacks

The institution should have in place adequate measures to ensure the availability of those of its critical activities and services which are provided through the internet in case of cyber-attacks aimed at preventing or disturbing access to these activities and services (Denial of Service attacks).

The protective measures which have been taken with regard to the applications and the network connections should be tested periodically (for example every 3 years), in order to verify their effectiveness and efficiency and make adjustments where necessary.

9. Remote site for regional disasters

The institution should carry out a risk analysis of the vulnerability of its critical activities, services and resources to regional disasters or incidents, taking account of the applicable recovery and resumption objectives (RTOs). This risk analysis should be updated periodically (for example every 3 years).

Where necessary, the institution should provide for additional precautions and/or fall-back and recovery solutions at a remote site, in the light of the vulnerabilities identified, the nature of the critical activities and/or services and the potential impact on the financial system[24].

Examples of such additional precautions and/or fall-back and recovery solutions for data centres and IT systems are:

- one or more fall-back data centres at a remote site, at least for the critical activities, services and resources;
- one or more recovery copies at a remote site of the critical production and backup data, which should allow business recovery and resumption, possibly with a limited but acceptable loss of data.

Where and to the extent necessary, considering the technological limitations at a remote site, the institution should define adequate recovery and resumption objectives (RTOs) in case of transfer of critical activities, services and resources to a remote site. The institution needs to inform the National Bank of Belgium if, further to its risk assessment, it finds that its remote precautionary and recovery measures do not enable it to comply with the recovery and resumption objectives (RTOs) for systemically important critical activities, services and resources (see point 2.a above).

[24] Considering the existing infrastructure and the infrastructure expected to be created in the near future, and the meteorological, geographical and political context in Western Europe, “at a remote site” must be considered to mean at a minimum distance of 100 kilometres. The institution may derogate from this rule, provided that it submits to the NBB a duly substantiated risk analysis which demonstrates that the applied or planned solution provides an equivalent level of residual risk.

10. Fall-back testing

For its critical activities, services and resources[25], the institution should periodically (i.e. at least annually) carry out production emergency fall-back tests for the staff concerned and for supporting and technical (IT) systems, and should adequately demonstrate that:

a) it can adequately and controllably transfer the critical activities, services and resources to the fall-back solutions and sites provided for, and that it can restore the normal situation afterwards. In this respect, it is important that the fall-back solutions, plans and processes are sufficiently known by all persons concerned and are sufficiently documented in order to ensure that less experienced staff can also carry out the tests sufficiently autonomously;
b) the fall-back solutions and capacity provided for are sufficient in order to adequately support the critical activities and services. The test period and/or test duration must be determined in such a manner as to ensure that during the testing the fall-back solutions are not only subject to low or medium business volumes (e.g. during a bank holiday or a long weekend) but also (to the extent possible) to higher time-limited or seasonal peak loads.
c) the fall-back solutions used are sufficiently reliable for exercising the critical activities and providing the critical services.

The duration of the production emergency fall-back tests for IT-systems should be sufficiently long to draw representative conclusions with regard to the objectives referred to in a), b) and c). The production emergency fall-back tests for the staff should as a rule last at least one full working day.

If the emergency solutions envisaged for critical activities and services accept data loss (i.e. Recovery Point Objective (RPO) higher than zero), the workability and feasibility of the procedures for recovering lost data within the pre-established recovery and resumption objectives (RTO), must also be tested and validated appropriately.

In case of phased IT production emergency fall-back testing and fall-back plans, where the IT systems of the non-critical activities and services are restarted later on the fall-back site than the IT systems of the critical activities and services, the institution should verify and test that the critical activities and services continue to function adequately in isolation and in the absence of the non-critical IT systems and applications.

For its tests, the institution should follow a phased growth path on a project basis. It should systematically increase the size and complexity of the tests (where and to the extent necessary) in order to demonstrably achieve the pre-established continuity objectives within a reasonable period of time.

11. Expertise and documentation

The institution should have appropriate contractual and operational solutions and safeguards to ensure that, both in its daily management and in case of incidents and/or disasters, it has or obtains access in an efficient and effective manner to the necessary expertise and/or technical and functional documentation of its critical IT systems, applications and data.

[25] For the expectations concerning non-critical activities, services and resources, please refer to the general provisions of Circular PPB 2005/2.

C. Security measures

1. Defence in depth strategy

The institution should have a defence in depth strategy for its logical and physical security, in which the former focus on the logical and physical security perimeter is extended to a broader and more in-depth approach to security, which relies on a number of complementary and partially overlapping security layers at the physical level and throughout the IT systems.

The different security layers are intended to prevent and/or detect malicious acts in a timely manner, minimise potential damage and/or better manage security incidents. The core idea is that the failure of one line of defence may be compensated for by one or more other lines of defence.

In its risk analyses and in developing, implementing and assessing its physical and logical security, the institution should explicitly take account of risk scenarios in which persons with malicious intentions have succeeded in breaking through and/or bypassing perimeter security (e.g. through social engineering) and in gaining access to the institution's buildings and IT systems.

2. Physical security

The physical security of buildings and resources used for critical activities and services, should be centrally coordinated and controlled by means of a security strategy and policy, complemented by the necessary processes and standards. In this regard, the roles and responsibilities should be clearly assigned within the internal organisation.

The institution should have an adequate general access security and control system, including continuous monitoring of the most critical buildings, sites[26] and resources, inter alia with video surveillance and a burglar alarm system. Where necessary, the general security measures are supplemented by additional security measures (e.g. additional access controls) for certain critical activities and/or sites which, by their nature, are more sensitive (e.g. the trading floor, the control room for critical IT systems, data centres, etc.).

The staff responsible for continuous monitoring should also maintain the necessary preventive and incident-related contacts and should cooperate with the security forces concerned (police, etc.).

The adequacy of the physical security measures should be subject to appropriate audits to be carried out periodically (for example every three years).

3. Logical security

a. Perimeter security

The institution should have a centralized view and security management of all:

- websites, internet applications (also the so-called mobile apps) and network connections through which third parties can have access to internal IT systems;
- devices and applications (whether or not administered by the institution) which are authorized to connect to the internal IT systems;

[26] A site can also be critical when it can be used to logically (e.g. via network connections, etc.) provide access to critical activities, services and resources.

The institution should also have guidelines and solutions:

- in order to detect, prevent and/or prohibit the unauthorized installation of IT components (e.g. wireless networks, etc.) and/or applications which can be used to bypass the security perimeter and/or to gain unauthorized access to the internal IT systems from outside.
- in order to secure and/or monitor the incoming and outgoing communication flows with external parties (professional partners, etc.) against / for irregularities that may be indicative of security incidents;
- in order to ensure appropriate protection of devices (portable computers, tablet computers, smartphones, etc.) and applications that are authorized to connect with the internal IT systems from outside and inside the institution, regardless of whether they are administered by the institution or not.

The institution should protect its network connections, IT systems and applications that are directly accessible from outside, in particular as regards the internet, through a combination of several, largely complementary security solutions and techniques such as network and applicative "firewalls", intrusion detection systems and hardening of IT systems[27], complemented by security-conscious IT development and procurement practices (see below).

b. Security-conscious development and procurement

The IT development and procurement cycle of the institution should include a process and methodology to determine the security risks of the IT solutions to be developed and/or purchased.

In this respect, it should take account, inter alia, of security risks associated with:

- the technical IT platforms and development languages used (.net, java, MF / Cobol, etc.)
- the sensitivity to abuse of the supporting functionalities, the transactions performed and/or the data used;
- the operating and security context in which the solution will function (will it be accessible from outside or not, will it be an external web application or an internal back office application, etc.).

Depending on the severity of the security risks, the institution should use appropriate security solutions and/or requirements, which must be satisfied in a consistent, controlled and sufficiently demonstrable manner (i.e. through own tests and/or appropriate external certifications).

For in-house development activities (whether developed internally or externally), the institution should have a formal framework for safety-conscious development that informs all developers unambiguously and clearly about the development practices and solutions to be applied, including information on the necessary independent quality and security tests (e.g. mandatory automated vulnerability and/or code reviews) before launching into the production environment and the procedures and/or guidelines to be followed.

The institution should devote the necessary attention and deploy the necessary resources for training and awareness-raising for the various functions which are involved in its IT development and procurement cycle (analysts, developers, architects, testers, risk management, etc.) and have a role to play in the adequate protection of the IT solutions developed and/or purchased.

[27] Security measures which strip the servers of all superfluous dangerous functions and protect at-risk applications as much as possible.

Wherever possible and appropriate, the institution should to this end make use of internationally recognised sound management practices and/or standards[28].

c. Segmentation and isolation

The institution should provide for the necessary physical and/or logical segmentation of its internal IT systems, in order to:

- ensure that an IT security incident or problem in one segment of the IT systems cannot spread unhindered and/or unnoticed to other segments of the IT environment;
- increase the probability of an early detection by carrying out appropriate preventive and detective controls in case of spreading to other segments;
- keep the extent of any damage within acceptable financial and operational limits.

In this respect, the institution should have an approved segmentation policy and appropriate technical standards and solutions that are applied consistently. The segmentation policy and the relevant technical standards determine the criteria on the basis of which the various segments are determined. Various aspects are taken into account, such as:

- the extent to which certain IT systems and/or applications are exposed to threats or security risks which are more serious than usual, such as the DMZs[29] and office environment (desktop systems, mobile devices, etc.);
- the sensitivity of the supported business and/or IT processes and/or the data stored, for example to fraud, data theft, sabotage, etc.;
- the logical coherence between certain IT systems and/or applications, whereby the IT systems involved have a comparable risk and/or use profile and that abnormal acts and/or data streams can be detected more easily;
- the increased vulnerability of some IT systems and/or applications due to their obsolescence and/or to the fact that they are not sufficiently patched or have not been developed with sufficiently secure techniques;
- the possibly lower security level of the test and development environments as compared to that of the production environment;
- the potential proliferation of security incidents as a result of shared authentication solutions and architectures (for example Single Sign-on[30], etc.).

Subsequently, and in parallel, the institution should provide for an adequate physical and/or logical isolation of its critical activities, services and resources, in order to prevent or detect unauthorized access and abuses and/or to keep them within reasonable limits.

[28] For example the “Open Web Application Security Project” (OWASP) directives concerning the security of software or international standards on software quality (ISO 25010, etc.).
[29] A demilitarised zone (DMZ) is a network segment that is located between an internal and an external network.
[30] Single Sign-on solutions allow end users to log in once and subsequently receive automatic access to various applications and resources in the network.

d. Strong authentication and management of access rights

User names and passwords can be relatively easily extracted or stolen and therefore are not sufficient for protecting critical activities, services and resources which, by their nature (fraud sensitivity, high confidentiality and/or sensitivity, operational business-critical nature) are favoured targets for internal and external persons with malicious intentions. Examples of this include privileged administrator access to critical or sensitive IT systems, applications and data, and access to fraud-sensitive payment applications or payment card details. For the latter functions, the institution should have strong authentication solutions[31].

The institution should have an authentication policy which clearly indicates which critical activities, services and resources should use strong authentication solutions.

The institution should also ensure efficient and high-quality management of the access rights and should carefully monitor the correct implementation of and compliance with the "least privilege" and "need to know" principles.

This implies:

- that the institution should use authentication management solutions whereby the access rights of persons are assigned and managed based on the roles and specific tasks fulfilled by these persons, taking account of the necessary segregations of duties. The processes for a timely review of the access rights at the time of the recruitment, the departure or the internal transfer of an employee should receive special attention;
- that each application, each process and each user should only have privileges and access rights insofar as they are strictly necessary for the performance of their duties. Thus, for example, the use of e-mail and/or internet surfing with a privileged administrator profile must be avoided as much as possible;
- important and/or sensitive privileged administration accesses should be limited in time as much as possible and should be provided in a controlled manner ("Just In Time" or "Deny By Default Administration"), should be limited functionally ("Just Enough Administration") and should be subject to adequate logging and monitoring.

e. Logs, audit trails and monitoring

Logs and audit trails are essential in that, in combination with appropriate monitoring and research solutions, they make it possible to timely detect security incidents and to reconstruct and recover from malicious acts afterwards. Therefore the institution should have adequate security logs and audit trails of its IT systems and applications, which are created and maintained in a separate and sufficiently secure place in order to safeguard their reliability. The history of the logs that needs to be maintained needs to take into account the effectiveness of the institution in discovering malicious activities and/or attacks.

[31] I.e. authentication solutions which are based on the use of 2 or more of the following elements: 1) something only the user knows, 2) something only the user possesses and 3) something the user is (e.g. biometric characteristic). In addition, the various elements should be mutually independent and at least one of the elements should be non-reusable and should not be susceptible to being stolen surreptitiously. The location of the user ("where I am") may be important in this context.

In addition, the institution should have a monitoring policy, real time or near real time monitoring solutions and ex post research solutions which are appropriate to the nature and extent of the threats and are aimed at detecting major security incidents as quickly as possible, so that it can provide an efficient and effective incident response.

In this respect, the institution should have at least an adequate operational monitoring and analysis system for security alarms and/or incidents related to:

- attempts to break into its IT perimeter;
- suspicious activities connected to its most sensitive and/or critical systems, applications and data that are favoured targets for internal and external persons with malicious intentions (e.g. payment applications, sensitive payment card or client data, critical IT administration consoles and/or applications, etc.);
- suspicious outgoing network connections and/or information flows that may be generated by malicious software, insiders and/or external attackers with access to the internal IT systems;
- unauthorised creation or use of privileged access rights.

Depending on the nature of the security risks and threats involved, and the specificity of the monitoring activities, the institution should provide sufficient staff with appropriate training to monitor and examine such incidents on a permanent and ongoing basis. The security incidents identified should be handled in accordance with a pre-approved incident escalation and incident response process.

The institution should also periodically perform adequate announced and unannounced tests, where unauthorised activities and/or attack scenarios are simulated, to assess the effectiveness of the monitoring solutions and the accompanying incident escalation procedures.

f. Vulnerability monitoring and independent testing

The institution should have automated solutions in order to regularly (for example once a month) detect security vulnerabilities in its IT perimeter and in its internal IT systems and in order to implement the necessary corrective measures.

Periodically (for example every three years) the institution should also arrange for comprehensive security tests to be carried out with the involvement of independent expert specialists to verify the efficiency and quality of the security by means of ethically performed realistic attack scenarios involving various attack methods and techniques. Examples of such attack scenarios include attempts:

- to break into the internal IT systems from outside and carry out sensitive and/or critical transactions and/or gain access to sensitive and/or critical data;
- to penetrate into the internal IT systems from within, from a normal user workstation or an internal network gate, in order to carry out sensitive and/or critical operations and/or gain access to sensitive and/or critical data;

If and as long as the aforementioned comprehensive independent expert tests indicate substantial vulnerabilities in the perimeter and/or in internal IT security, the institution should ensure that these tests are repeated regularly (for example annually) in order to closely follow up the shortcomings identified and the effectiveness of the corrective measures taken, and to make adjustments where necessary.

4. Entry into force

The circular enters into force on 1 January 2016. The NBB expects systemically important institutions to assess their business continuity and security policies and solutions within 6 months after the entry into force of this circular, and adjust them where necessary in the light of the sound management practices referred to in this circular.

As regards the aspects which, for their technical specification and implementation, require important organisational changes and implementation deadlines, the institutions concerned should design a programme to ensure that the pre-established objectives are achieved within a reasonable period of time, which should be assessed in the light of the nature, scale and complexity of their business. If this programme provides for deadlines which exceed a period of two and a half years after the entry into force of this circular, this should be discussed with the NBB. The aforementioned multi-phased implementation does not preclude the prudential assessment by the NBB of the business continuity and security policy on the basis of these management practices.

Jan SMETS
Governor

Appendix: 1