Internal Governance

BNG Bank Security Charter

Koninginnegracht 2
2514 AA Den Haag
T 070 3750 750
www.bngbank.nl

Datum
27 augustus 2018

Onze referentie
1874165

Contactpersoon
Lambrecht Nieuwenhuize/
Hans Noordam

1 Purpose of the Security Charter

Purpose
The purpose of the Security Charter is to define the objective of the 2nd line Security function and to explain the nature, stature, authority and roles & responsibilities of the Security function with BNG Bank.

Ownership and maintenance
The owner of this charter is the Corporate Information Security Officer (CISO). The charter is part of the internal governance framework of BNG Bank. As consistency and alignment with other internal governance elements is important, the maintenance of this charter will be initiated by Risk Management/Strategy & decision-making. Updates if and when required will be done jointly with the CISO.

Approval
The Security Charter is approved by the Management Board ('Directie Overleg DO') in its meeting of August 27th 2018.

2. Objective of the function

Mission and objective of the 2nd line Security function
The objective of the 2nd line Security function is to support the Management Board and business in safeguarding the reliability and continuity of the business processes of the organisation of BNG Bank and being in control relating to security risks. This includes ensuring that BNG Bank operates within its risk appetite.
The objective of the function is in line with the Governance framework for Information Management.
The Security function within BNG Bank is an element of the 'internal control function' as mentioned in the EBA guidelines on internal governance (EBA/GL/2017/11).
The 2nd line Security function of BNG Bank is performed by the PRC_Security department, headed by the CISO.

Key definitions
- *Corporate Information Security Officer (CISO)*: The independent officer, assigned by the Executive Board, to fulfill the 2nd line Security function, supporting and reporting to the Management Board of BNG Bank relating to security risks.
- *Security risk*: (source: Risk definitions BNG Bank, #2247199): The risk of unauthorised access to ICT systems and data from within or outside the institution (e.g. cyber-attacks).
- *Information security:* The security of internal and external access to systems and data, e.g. whether the ICT system provides information and access to the right people. *(source: EBA GL on common procedures and methodologies for SREP).*
- *Security incident:* Unauthorised internal and external access to systems or data.
- *Cyber security incident:* A security incident using the Internet interface.

3 Positioning of the Security function

Organisation

The Security function is hierarchically positioned in the Processing department, with a direct reporting line to the Management Board and the CRO.

Three lines of defense

The 3LoD (Three Lines of Defense) model is considered as the organisation model for managing risks within financial institutions and therefore is a very important part of governance. Figure 1 below shows the implementation of the 3LoD model within BNG Bank (we refer to # 2294280 for further explanation).

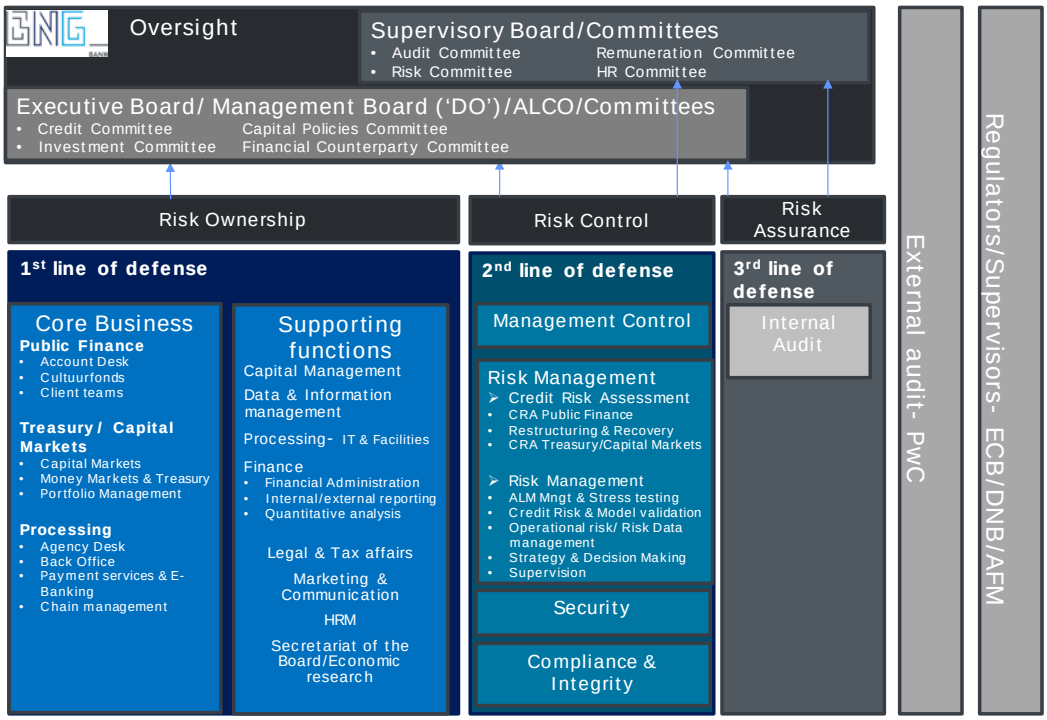

Figure 1: 3LoD model for BNG Bank based on activities

The principles of the 3 LoD model thus also apply to security risk management including the design of the 2nd line Security function. The 1st line is responsible for managing the security risks, supported by specifically educated and trained Security specialists, who combine their main function with product-specific expertise relating to security.

The 1st line responsibilities for managing security risks are further organised as follows:

- Data owners, product owners and system owners contribute to identifying and assessing security risks;
- Security specialists contribute to implementing mitigating measures to respond to identified security risks, based on laws & regulations and policies. They also periodically assess the design and effectiveness of the mitigating measures and manage security incidents;
- ICT Management: assessing, reviewing and monitoring the management of security risk by outsourcing parties (Centric FSS and cloud outsourcing parties related to ICT-systems).

Role in committees

The Management Board is the relevant governing body for non-financial risk. The CISO reports on a quarterly basis to the Management Board that includes the members of the Executive Board.
The security risk is 'represented' in the Management Board by the1st line Director Processing and Head of Data Information Management. The
Head of Risk Management represents the 2nd line risk function.
In these meetings, the CISO can be present to further explain and discuss the quarterly report.

Serious issues relating to security risk are also included in the quarterly risk report of Risk Management, which is addressed to the Executive Board and the Supervisory Board. (Risk Committee and entire Board).

Reporting line, access to Board and escalation

The CISO has the following reporting lines:

- Quarterly 'Security report" to the Management Board that includes the members of the Executive Board, including cyberthreats, status of mitigating measures, incident dashboard, attention points and status of follow-up of IAD recommendations;
- Monthly 'Management report' to CRO and Director Processing, including a dashboard with Key Security Indicators comparing the actual security risk profile with the risk appetite;
- Ad hoc: written reports with results from incident-investigations to the related director and, based on nature and impact, to other relevant persons.

In addition, the CISO can make use of the following escalation lines:

- Fraud-related issues: to the chair of the Executive Board or other relevant member of the Executive Board;
- Other topics; to the CRO.

4 General principles

The following general principles apply to all 2nd line functions:

General principles for 2nd line functions and explanation	
Assignment & with-drawal procedure	The appointment and withdrawal of the head of the 2nd line function is approved by the Executive Board.
Authority	The 2nd line function derives its authority from the Executive Board. The head of the 2nd line function is appointed to be responsible for the 2nd line function and is empowered to execute this role in an appropriate manner. This includes having full access to all necessary information required and having appropriate IT systems and support at its disposal.
Independency	The 2nd line function forms an expert judgement independent from the business (the 1st line of defense). This independence is safeguarded by the condition that the 2nd line function will have no operational involvement in day to day business operations and

	individual business decisions. Indirectly the 2nd line function can be involved by means of the advising and supporting role.
Objectivity	The 2nd line function will execute its activities in an objective manner, having an unbiased mental attitude and avoiding possible conflicts of interest.
Resources	The head of the 2nd line function ensures to have sufficient resources to perform the function. This includes requests for additional capacity if the number of qualified staff should become inadequate to fulfill the roles and responsibilities as set out in this charter.
Expertise & quality	The head of the 2nd line function ensures adequate expertise and quality of the resources including regular training (and on occasions hiring external expertise) to remain sufficiently qualified. This includes complying with relevant external standards/market practices up to the ambition level of BNG Bank.

5 Scope of the Security function

Main activities

The main activities of the Security function consist of two main areas as follows:

– Information Security; this relates to the areas of Information Security and Business Continuity;
– Fraud Investigations; this relates to judicial claims and interbank related information requests, fraud investigations and interbank collaboration initiatives, the latter with regard to cyber-crime in the financial sector.

Legal entities/organisation

The scope for the activities related to the Information Security and Fraud Investigations areas covers both BNG Bank and her 100% subsidiaries BNG Gebiedsontwikkeling BV and Hypotheekfonds voor Overheidspersoneel BV.

6 Roles & responsibilities and authority

6.1 Roles & responsibilities

General explanation for 2nd line functions

As explained in the 3 LoD document, the 2nd line functions help to ensure that risks are appropriately being identified and managed, thus enabling the organisation to be 'In Control'.

The overall roles and responsibilities of 2nd line functions generally consist of three fundamental roles: 1) Advise, 2) Facilitate & Support and 3) Challenge & Monitor. Within these fundamental roles, a (large) number of accompanying responsibilities and activities can be identified. The rationale and general considerations for each fundamental role are explained extensively in the3LoD document.

Specific explanation for the Security function

Based on the three fundamental roles, and aligned to the summary of the roles and

responsibilities of the Security function that is included in the Three lines of defense document , the following figure provides an extensive overview of the roles and responsibilities:

Topics	Advise	Facilitate & Support	Challenge & Monitor
Risk strategy	► Advise MB and 1st line on security related matters, including risk appetite on Security/ BCM and actual potential threats ► Advise on implementation of actual Security/ BCM sound practices and standards	► Support 1st line and outsourcing partner (CFFS) regarding generic security-approach/choices	► Monitor actual security risk profile against risk appetite and compliance with security related laws & regulations ► Monitor potential impact of internet threats
Risk governance & framework	► Advise MB and 1st line on security governance design and security framework design (including methodologies and policies) ► Advise on design of Crisis Management Organisation	► Develop and maintain security framework (Information Security policy, BCM policy and generic security guidelines) ► Support 1st line with design of specific security guidelines ► Initiate and promote bank-wide security activities ► Support Crisis Management Team with expertise (incl. development calamities scenarios) ► Process supervision of Crisis Management Team during a crisis ► Support projects with expertise	► Challenge quality of security management activities in daily operations (information risk analysis, business impactanalysis, and design of specific security solutions) ► Monitor business continuity tests ► Coordinate and investigate serious security related (fraud) incidents ► Monitor quality and consistent use of security framework ► Monitor and report on security risk profile and on serious security related incidents to MB
Risk culture	► Advise MB and 1st line on sound security culture and adequate awareness ► Advise MB and 1st line on bankwide employee security level requirements and education program	► Create and promote awareness ► Develop and maintain awareness and trainingprogram ► Train Crisis Management Team	► Challenge effectiveness of management/employee-performance processes (through embedding security elements in risk management approach) ► Monitor actual embedding
Relation with regulator	► Advise on compliance with regulatory requirements on security and on follow-up on recommendations supervisor	► Support MB with pro-active and effective coordination and communication with regulators relating to security-topics	► Monitor compliance with security-related laws & regulations ► Ensure that relevant security risk related incidents are reported by RM/CRO to the external regulator

Figure 2: Overview of roles & responsibilities Security function

A number of topics can be further explained as follows:

– In order to optimally fulfill the advisory function, it is important for the CISO to cooperate with colleague- CISO's within the financial sector to obtain the necessary external perspectives on actual/potential threats;
– Obtaining an external perspective is also necessary for judging and monitoring threat intelligence information and the potential impact for BNG Bank with regard to internet threats;
– The CISO supports MB and the 1st line by being the contact person and having periodic content-related update meetings with the 2nd line security function of the outsourcing partners;
– In developing and maintaining the security framework including the Information Security Policy, the CISO seeks alignment with the general risk management framework as developed and maintained by the 2nd line function Risk Management (see Risk Governance Framework #2151925). The cooperation is embedded by monthly meetings with Risk Management-Head of ORM and CISO;
– To better facilitate and support the 1st line, the CISO participates in the 'Architectuur Advies Groep (AAG)' and the monthly Demand meetings;
– To facilitate and support the 1st line, the CISO can participate in projects.

6.2 Authority

General competencies for 2nd line functions

In order to safeguard adequate 'stature' of the 2nd line functions, a number of general competencies are at their disposal. They underpin the authority of the function.

- Access to all data, information, people; necessary to adequately fulfill the function. This can include hard copy documents, digital data, e-mail, physical and logical access- registration, camera recordings, recorded phone calls;
- Hire external experts; autonomously decide to make use of external expertise if necessary;
- Obtain support from other functions/departments/people for responding to requests from supervisors; this includes delivery of needed input on a timely basis;
- Have adequate data quality, data definitions and sufficient ICT-systems for support.

Specific competencies, related to the 2nd line Security function

- The CISO can initiate, if necessary, investigations to potentially relevant incidents without prior consent;
- The CISO can give mandatory instructions to BNG-personnel relating to resolving incidents;
- The CISO informs the head of IAD about all fraud-related investigations, thus enabling the head of IAD to form an opinion on the proportionate and subsidiar use of the authority by the CISO.