Internal Governance

BNG Bank Security charter

Approved by the ExCo on November 28th, 2023
Approved by the Supervisory Board on December 8th, 2023

Datum
5 oktober 2023

Onze referentie
3371340

Contactpersoon
Lambrecht Nieuwenhuize
T 070 3750 832
M 06 234 921 63
lambrecht.nieuwenhuize@
bngbank.nl

1. Purpose of the Security charter

Purpose
The purpose of the Security charter is to define the objective of the second line Security function and to explain the nature, stature, authority and roles & responsibilities of the Security function within BNG Bank.

Ownership and maintenance
The owner of this charter is the head of CRO-Security. The charter is part of the internal governance framework of BNG Bank. CRO-Security will perform maintenance of this charter and will seek consistency and alignment with other internal governance elements through Risk Management ORM.

Approval
The Security charter approved by the Executive Committee ('ExCo) in its meeting of November 28th, 2023 and approved by the Supervisory Board on December 8th, 2023.

2. Objective and scope of the function

Mission and objective of the 2nd line Security function
As business partner of the direct reports and Executive Committee, Security makes a significant contribution to fulfill the mission of BNG Bank.

Security advises, supports and challenges the direct reports and Executive Committee and monitors the efficiency and effectiveness of the (strategic, tactical and operational) security activities undertaken. Security ensures that the security related behavior and decisions of the management in the organization are consistent with the objectives and the strategy of the company.

The related objectives of the 2nd line Security function are translated in roles and responsibilities reflecting the 3LoD (Three Lines of Defense) model and summarized in figure 2 in section 5.
The Security function is an element of the so called 'internal control function' as mentioned in the EBA guidelines for Internal Governance (EBA/GL/2021/05).

Main activities
The main activities of the Security function relate to the main risk areas as defined in the banks 'Risk Definitions' and consist of Security risk. Figure 2 shows the specific explanation for the Security function.

Legal entities/ organization
The scope for the activities related to the security risk management areas covers BNG Bank and her 100% subsidiary BNG Gebiedsontwikkeling.

3. Positioning of the Security function

Organization
The Security function is hierarchically positioned in a separate department directly under the CRO. The 3LoD model is considered as the organization model for managing risks within financial institutions. See figure 1 the implementation of the 3LoD model within BNG Bank.

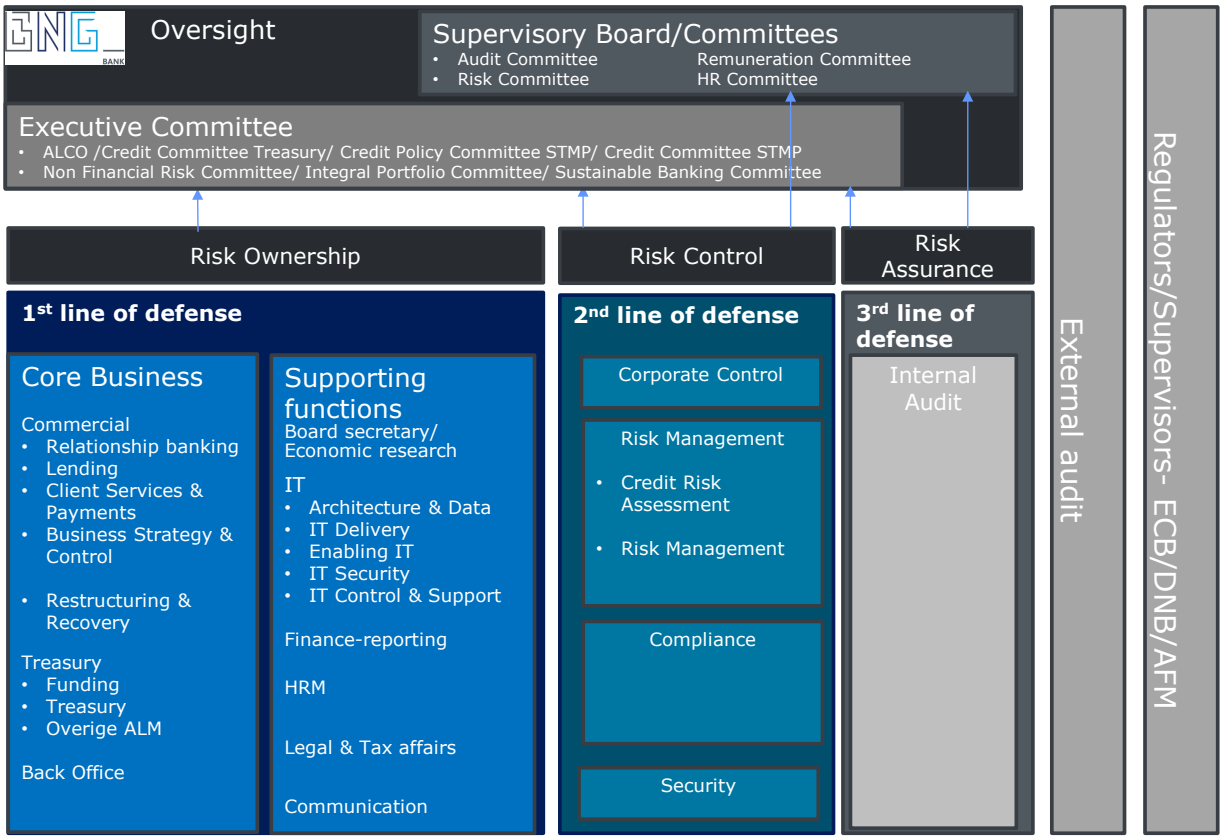

Figure 1: 3 Lines of defense within BNG Bank

The principles of the 3LoD model thus also apply to security including the design of the 2nd line Security function. The 1st line is risk owner and responsible for:

- Identification & assessment of the security risks and determination of the risk response (accept, mitigate, avoid, pursue or transfer the risks);
- Implementation, execution, monitoring and reporting on security controls including compliance with laws and regulations;

Day-to-day management of security risks generated by its activities implying ownership of security risks and responsibility for effective security controls.

<u>Role in committees</u>

a) Security advises on security and Business Continuity Management (BCM) related matters in the Executive Committee and Risk Committee (part of the supervisory board);
b) The Head of Security participates in the Non-Financial Risk Committee (NFRC);
c) Security is participant in the Taskforce IT-Risk and the Taskforce monitoring/key controls.

<u>Reporting line, access to Board and escalation</u>

The Head of Security has a direct reporting line to the Executive Committee and Supervisory Board (SB). The following report is prepared:

- Quarterly high level security risk report as part of the integrated risk report relating to monitoring the actual security risk profile against the risk appetite and analyzing actual developments.

The Head of Security has at all times the possibility to escalate to the CRO. If necessary the Head of Security has the right to escalate matters to other members of the Executive Committee and SB.

4. General principles

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

General principles for 2nd line functions and explanation	
Assignment & withdrawal 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. Roles & responsibilities

<u>General explanation for 2nd line functions</u>
As explained in the 3LoD document, the 2nd line functions help to ensure that risks are appropriately being identified and managed, thus enabling the organization 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.

<u>Specific explanation for the Security function</u>
Based on the three fundamental roles and aligned to the summary of the roles and responsibilities of the Security function in the 3LoD document, figure 2 provides an overview (see next page).

The scope of the monitoring role is limited to ensure that all identified risks are effectively monitored by the 1st line. This implies that Security will monitor if 1st line management takes responsibility of their risk ownership, by verifying if (key) controls are executed. In doing so, Security may rely on information received from 1st line, without performing systematic, in depth checks and testing procedures to determine the reliability of the information received.

Topics	Advise	Facilitate & Support	Challenge & Monitor
Security strategy	▶ Advise ExCo and 1st line on security and BCM related matters, including risk appetite, changes and new products. ▶ Advise on implementation of actual Security/ BCM sound practices and standards	▶ Formulate the security and BCM policy ▶ Establish the actual threat landscape	▶ Monitor actual security risk profile against risk appetite and compliance with security related laws & regulations and report to NFRC, ExCo and SB
Security gover-nance & framework	▶ Advise ExCo and 1st line on security/BCM governance design and security/BCM framework design (including methodologies and standards) ▶ Advise on design of Crisis Management Organisation.	▶ Develop and maintain the management system for Security and BCM ▶ Develop process and methodology for security risk identification and assessment (S-RCSA)	▶ Monitor and challenge the quality of security /BCM activities in daily operations (information risk analysis, business impact analysis, and design of specific security solutions) ▶ Monitor compliance with security governance requirements and security policies including security risk limits and detect and report (potential) violations. ▶ Monitor effectiveness of security controls ▶ Coordinate and investigate serious fraud related incidents ▶ Report on serious security related incidents to ExCo and SB
Security culture	▶ Advise ExCo and 1st line on sound security culture and awareness	▶ Create and promote security awareness ▶ Develop and maintain security awareness program, including the training of the crisis management organisation	▶ Challenge and monitor effectiveness of management/employee-secure behavior
Relation with regulator	▶ Advise on compliance with regulatory requirements on security and on follow-up on supervisory recommendations	▶ Support ExCo and process owners with regulators relating to security-topics	▶ Ensure that relevant security risk related incidents are reported by RM/CRO to the external regulator Monitor compliance with security-related laws & regulations

Figure 2: Overview of roles & responsibilities Security function