

Compliance Charter and Framework

General Principle

Version	4
Date	June 2015
Department	Corporate Compliance

Policy Summary Sheet

Purpose of the policy document and key requirements

The purpose of this policy is to help businesses manage Compliance Risk. The first part of the document - the Charter - describes the organization, operation and governance of compliance for NN Group NV (“NN”). The Framework consists of structures, tools and processes that guide compliance activities. It enables senior management, business managers and employees to understand and effectively manage Compliance Risk.

Changes compared to the previous version

The main changes are in the Charter and reflect the strengthening of the operational independence of the Compliance Function and the positioning of the Chief Compliance Officer (“CCO”). The Charter is also more explicit on the demarcation of tasks and responsibilities, and elaborates on the cooperation with other (key) functions. In addition, minor changes have been made as a general update of the Charter, aligning it with current practices. Only minor textual changes and changes in lay-out were made to the Framework.

What is the impact and what is expected from the target group

This updated NN Group Charter and Framework impacts reporting of the Compliance Function and CCO to NN’s Management Board and NN’s Supervisory Board and requires involvement and commitment of the Chief Executive Officer of NN (“CEO”) and NN Boards. The changes have no significant impact on customers and other stakeholders.

Timeline

The changes to the Policy will become effective as of June 2015.

What can be expected from the policy owner to help the target group with implementation

Not applicable.

Information Sheet

Issued by:

NN Corporate Compliance

Replaces :

NN Group Compliance Risk Management Charter and Framework (November 2014)

Target audience:

Employees and Management of all majority owned NN businesses (or business units), businesses under NN 's Management control and NN corporate staff departments.

Approved by:

NN Management Board - June 2015

Effective date:

June 2015

Next review date:

June 2016

Contact person:

NN Corporate Compliance Department / +31 20 504 9640

Translation

In the event of any discrepancies between the English version of this document and a translated version, the English document prevails.

Contents

1.	Introduction.....	6
1.1	Objectives	6
1.2	Scope	6
1.3	Mandate	6
1.4	Key definitions	6
2.	Compliance Charter	8
2.1	Compliance Risk Strategy	8
2.1.1	Compliance Risk Mission	8
2.2	Compliance Risk in scope of the Compliance Function	8
2.2.1	In scope of the Compliance Function	8
2.2.2	Outside the scope of the Compliance Function	9
2.3	Compliance Function	9
2.3.1	Independence of the Compliance Function	9
2.3.2	Purpose of the Compliance Function	10
2.4	Roles & Responsibilities	10
2.4.1	Management	10
2.4.2	Chief Compliance Officer (CCO)	11
2.4.3	Local Compliance Officers ('LCO')	12
2.4.4	Employees	12
2.5	Authorities and capabilities of the CCO and the Compliance Function	13
2.5.1	Investigate and Challenge	13
2.5.2	Escalation	13
2.5.3	Access	13
2.5.4	Liaising and partnering	14
2.5.5	Capabilities, Development, Evaluation & Remuneration	14
2.5.6	Appointments and Terminations	16
2.6	Reporting	16
2.6.1	Reporting at Local Level	16
2.6.2	Reporting at Corporate Level	16
3.	Compliance Framework	18
3.1	NN Values – The Foundation for NN 's Framework	18

3.2	The Three Lines of Defence to Manage Compliance Risk	19
3.3	The Framework in Our Business	20
3.4	The Chart and the Five Key Activities	21
3.4.1	Identification of Compliance Obligations	22
3.4.2	Risk Assessment	23
3.4.3	Compliance Risk Mitigation	24
3.4.4	Compliance Risk Monitoring	26
3.4.5	Compliance Reporting	28
3.5	Compliance Advisory Role	30
3.6	Scorecard	31
4.	Administrative Matters.....	32
5.	Appendix	33
5.1	Delegated responsibilities Register	33
5.2	Roles & responsibilities of Corporate Compliance (Functional Oversight Team)	34
5.2.1	Compliance Chart	34
5.2.2	Risk Assessment (RA)	34
5.2.3	Training	35
5.2.4	Compliance Monitoring	35

1. Introduction

1.1 Objectives

It is NN's purpose to help customers secure their financial future. NN's strategy is to deliver an excellent customer experience based on great service and long term relationships. NN aims to achieve this objective by offering transparent products and services that serve customers' lifetime needs, by having multi-access distribution network available to customers wherever required and by maintaining effective operations that deliver excellent customer service.

Good Compliance helps us to live up to our purpose, our strategy and our values because it builds trust and protects our brand. It helps us to meet our compliance obligations and to protect NN from loss or reputational damage. It improves the way we do business for our stakeholders. It is vital for sustainable business and it is our licence to operate.

NN has adopted the NN Compliance Charter and Framework ('**Charter and Framework**') to help businesses manage their Compliance Risk. The first part of this document - the Charter - states the roles and responsibilities for managing Compliance Risk. The second part - the Framework - describes the tools NN businesses use to manage Compliance Risks.

1.2 Scope

The requirements included in this Charter and Framework are minimum requirements. Compliance with these requirements is mandatory at all times. In jurisdictions where (local) laws or regulations set stricter rules for managing Compliance Risk than those set out in this document the stricter rules prevail.

1.3 Mandate

The NN Management Board mandates the NN Corporate Compliance department with the development, coordination and maintenance of the Charter and Framework and Appendix and related minimum standards, guidelines, procedures and other statements.

Interpretation of the policy:

The CCO or, by delegation, the NN Corporate Compliance department, are solely authorised to provide interpretations in cases where needed.

1.4 Key definitions

Chief Compliance Officer (CCO)

The Chief Compliance Officer (CCO) is responsible for managing the compliance Charter and Framework for the entire NN organisation. Further details of CCO responsibilities are described in section 2.4.2.

Compliance Function

The department(s) or team(s) responsible for advising on and for managing the Compliance Charter and Framework within a business or organisation. These departments typically comprise of the LCO, Compliance Officers, Compliance Specialists and / or anyone fulfilling compliance responsibilities.

Compliance Risk

Compliance Risk is the risk of impairment of NN's integrity. It is a failure (or perceived failure) to comply with NN Values and the Compliance Risk-related laws, regulations and standards that are relevant to the specific financial services offered by a business or its ensuing activities, which could damage NN's reputation, lead to legal or regulatory sanctions and/or financial loss. A reference to

Compliance Risk in this Charter and Framework is a reference to the Compliance Risk in scope of the Compliance Function as set out under 2.2.1.

Local Compliance Officer (LCO)

The Head of the Compliance Function at business unit level.

CCO and NNIP LCO

The CCO is the next Higher Level Compliance Officer for the LCO. The CCO can delegate certain tasks and responsibilities within the Corporate Compliance department. For the local businesses of NN Investment Partners, the next Higher Level Compliance Officer is NNIP's LCO. This also applies to NN policies where reference is made to the next Higher Level Compliance Officer.

The LCO of NNIP's (non-Dutch) local businesses reports to the NNIP LCO, who functionally reports to the CCO. A reference to the CCO in clauses 2.5.2 (escalation), 2.5.5 (functional management) and 2.5.6 (appointment and termination), 2.6.1 and 2.6.2 (reporting) is a reference to the NNIP LCO, where it concerns NNIP's (non-Dutch) local businesses.

Employee

Anyone who is permanently or temporarily employed by NN or on secondment / as a trainee at NN , which includes, among others:

- all Management and other staff of NN;
- anyone who works at majority owned NN businesses; and
- anyone who works at businesses under NN 's control.

Management

The people, so appointed, who are individually or jointly responsible for the decision-making, general operation and administration of an NN entity (e.g. Corporate level, business line, business unit, branch).

First Point of Contact (FPOC)

Member of the NN Corporate Compliance team responsible for support and oversight in respect of one or more business units.

2. Compliance Charter

The NN Management Board approved the Charter on 8 June 2015. The Charter may be amended at any time with the approval of the NN Management Board. The Charter must be available to all NN employees.

With the Charter the NN Management Board emphasises the importance of managing Compliance Risk. The Charter defines the responsibility of the Compliance Function and provides a clear mandate to the Compliance Function to manage the Compliance Risk.

2.1 Compliance Risk Strategy

Effectively managing Compliance Risk maximises NN's opportunities in the market and enhances our competitive position by building trust. Integrating a strong Compliance programme into daily business activities and strategic planning by NN's Management Boards helps NN to ensure that compliant conduct forms an integral part of everyday behaviour and decision making. This will help us protect our reputation, ensure transparency in product and service offerings and minimise the risk of regulatory action, including sanctions.

2.1.1 Compliance Risk Mission

Together with the business build sustainable competitive advantage by fully integrating Compliance in daily business activities and strategic planning.

2.2 Compliance Risk in scope of the Compliance Function

2.2.1 In scope of the Compliance Function

The Compliance Function operates within the context of NN's broader risk management framework. Within this framework the Compliance Function is responsible for four conduct related integrity risk areas:

- 1 **Client conduct related integrity risk; compliance-related risks** that can arise based on client characteristics, activities, location, etc.
- 2 **Personal Conduct related integrity risk;** compliance related risks that can arise based on NN Employee characteristics, conduct, location, etc.
- 3 **Financial services conduct related integrity risk;** compliance-related integrity risks that can arise based on the types of products, services and activities NN businesses engage in.
- 4 **Organisational conduct related integrity risk;** compliance related risks that can arise as a result of the organisational structure, governance, strategy and decisions.

See the table below for an overview of Compliance Risks per conduct related integrity risk area:

Client conduct related integrity risk	Personal conduct related integrity risk	Financial services conduct related integrity risk	Organisational conduct related integrity risk
Money laundering	Market abuse and personal trading	Marketing, sales and trading conduct	Organizational conflicts of interest, market abuse and insider trading
Terrorist financing	Breaches of the NN Values or local code of conduct	Conduct of advisory business	Anti-trust/Competition Law ¹
Politically exposed per-	Outside positions held	Transparency of prod-	New or modified prod-

¹ Shared responsibility with legal

son or person with an increased-risk reputation	by NN employees	uct offerings (e.g. costs, disclosures)	ucts and services (e.g. customer base, design) and governance changes
Client engagements or transactions with sanctioned countries	Gifts or entertainment given or received; bribery	Complaint handling	Agreed sector/industry standards
Tax evasion by U.S. taxpayers holding accounts with NN Group entities (Foreign Account Tax Compliance Act)	External incident reporting ²		Regulatory registration and reporting requirements (e.g. CREDO)
			Third party intermediaries as representatives of NN

2.2.2 Outside the scope of the Compliance Function³

Outside the scope of the Compliance Function is compliance with laws, regulations and standards that relate to the following NN support functions:

Risk type	Support function
Insurance	Risk
Employment	Human Resources
Accounting	Finance and Control
Tax	Tax
Operational (including Fraud, Processing, Information Technology, Security)	Risk Management
Legal	Legal
Credit + Market	Risk Management

However, NN has delegated to the Compliance Function responsibility to monitor some risks outside the scope of the Compliance Function. Reference is made to Appendix 5.1 for these delegated risks.

2.3 Compliance Function

To effectively manage Compliance Risk, NN has put in place a Compliance Function which is headed by a CCO with delegated responsibility for day-to-day management of the Compliance Function.

2.3.1 Independence of the Compliance Function

The Compliance Function is positioned independently from the business it supervises. This independent position is -amongst others- warranted by independent reporting, unrestricted access to senior management as well as structural, periodic meetings of the CCO with the CEO of the Management Board and the Chairman of the Risk Committee of the Supervisory Board.

² Risk that staff will report internal violations externally instead of through the internal Whistleblower procedure.
³ With approval of the CCO, businesses may agree to transfer responsibility for risks outside the scope of Compliance Risk to the Compliance Function

2.3.2 Purpose of the Compliance Function

Within NN's broader risk framework, the purpose of the Compliance Function is to:

- **understand and advocate the rules**, regulations and laws and the effective management of Compliance Risk; proactively work with and advise the business to manage Compliance Risk throughout our products' life cycle and our business' activities to meet stakeholder expectations;
- **develop and enhance tools** to strengthen the three lines of defence to detect, communicate, manage and to report on Compliance Risks;
- **support NN's strategy** by establishing clear roles and responsibilities to help embed good Compliance practices throughout the business by using a risk-based approach to align business outcomes with NN's risk appetite and
- **deepen the culture of compliance** by partnering with the business to increase the culture of trust, accountability, transparency and integrity in evaluating, managing and in reporting on Compliance Risk.

2.4 Roles & Responsibilities

2.4.1 Management

Management is the owner of Compliance Risk and is ultimately responsible for any business, corporate or strategic activities and decisions that entail such Risk. At all levels, Management must create an environment of awareness and accountability in which the importance of meeting compliance obligations, including our NN Values is well understood. Management must identify and communicate minimum compliance requirements that each employee must fulfil in day-to-day business activities (established at the departmental or organisational level) and to reward or sanction employees' performance against the requirements.

In summary, Management must set a good example by:

- considering stakeholders' expectations;
- knowing and applying the rules;
- encouraging a culture where people are trusted and accountable and
- managing Compliance Risks effectively.

To meet its compliance obligations, the NN Management Board appoints the NN General Counsel and Head of Compliance ("**General Counsel**") to establish and maintain an operationally independent Compliance Function at the corporate level led by the CCO. Whilst the General Counsel bears overall responsibility for the Compliance Function, the General Counsel has delegated day-to-day responsibility for managing the Compliance Function to the CCO. The General Counsel and the CEO appoint the CCO who reports hierarchically to the General Counsel. In addition, the CCO reports periodically to the CEO and the (Risk Committee of the) Supervisory Board of NN Group. The CCO is required to ensure accurate and timely reporting to the NN Management Board on Compliance Risk (see paragraph 2.4.2).

The CCO is supported by the Corporate Compliance department.

At the local level, Management must establish and maintain a Compliance Function and appoint a LCO. The LCO must hierarchically report to the CEO or to the Business Unit Head of Legal. If local level management has legitimate and specific reasons to deviate from this governance model and would like to change the hierarchical reporting line of the LCO to another member of the local management team or local board, prior approval must be obtained from the General Counsel.

The LCO's have a functional reporting line to the CCO⁴. If local level Management decides it can meet and manage its compliance obligations without a dedicated full-time or onsite LCO, Management must first obtain a waiver from the CCO⁵.

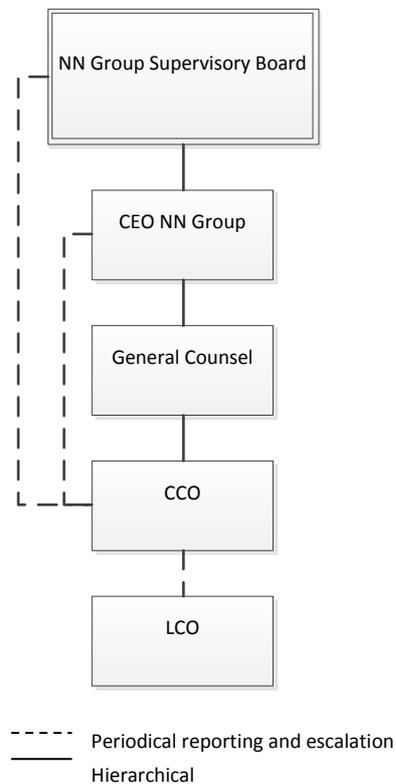


Figure 1: Overview of hierarchical reporting & periodic reporting and escalation lines (see 2.5.2)

Management is responsible to provide sufficient resources (training, budget, staffing, etc.) to its Compliance Function to ensure effective Compliance in the business. Issues concerning the adequacy of resources should be escalated to the CCO.

The specific responsibilities of Management are outlined in the Framework – Section 3 of this document.

2.4.2

Chief Compliance Officer (CCO)

The CCO must:

- advise senior Management on Compliance policies and issues and support them with major regulatory Compliance Risk issues as they arise;
- establish and ensure a high quality Compliance network within NN ;
- establish a Compliance framework and ensure this framework and related corporate Compliance policies are implemented;
- ensure adequate monitoring and control through management information;
- develop, maintain, advise on, endorse and communicate new and changed NN Compliance policies and minimum standards;
- ensure timely and appropriate reviews of Compliance Risk issues;
- liaise with risk management functions and CAS to ensure an integrated approach to risk management;

⁴ LCO's of NNIP's (non-Dutch) local businesses have a functional reporting line to NNIP's LCO.

⁵ A waiver is not required if the business appoints the LCO to also carry out other second line of defence activities as long as any conflicts of interest are mitigated

- represent the Corporate Compliance department in NN projects;
- advise and support NN products, services, change and strategic projects;
- ensure accurate and timely reporting on compliance issues to the NN Management Board;
- ensure quarterly compliance reports to the NN Management Board;
- periodically meet with the CEO of the NN Management Board to discuss relevant Compliance topics and where appropriate available compliance reports;
- ensure semi-annual compliance reports to the Risk Committee of the Supervisory Board of NN Group;
- meet semi-annually with the Chairman of the Risk Committee of the Supervisory Board of NN Group;
- manage the day-to-day operations of the NN Corporate Compliance department;
- ensure, in conjunction with Management and in accordance with the matrix reporting structure for control functions, that all levels are adequately staffed with Compliance Function representatives who have sufficient knowledge and experience;
- provide hierarchical management to the NN Corporate Compliance department and functional management to the LCO's;
- provide input into the Corporate Compliance MTPs and BUs budget setting;
- develop and execute a Compliance year plan based on the Compliance Strategy and NN's Strategy;
- manage Compliance communications, training strategies and initiatives and ensure support to the business units as required;
- drive the ongoing evolution of the Charter and Framework to ensure relevance and strategic competitive advantage;
- keep abreast of regulatory and industry trends and advise relevant stakeholders and the Compliance Function;
- maintain an ongoing relationship with regulators relevant to NN;
- manage consolidated internal and external reporting on the status of Compliance Risks and Compliance frameworks across NN.

In consultation with the General Counsel, the CCO may delegate execution of his or her tasks and responsibilities as appropriate.

2.4.3 Local Compliance Officers ('LCO')

LCO's are responsible to manage the Compliance Function representatives at business unit level and to advise and assist local management to manage its Compliance Risk. To effectively support the business, LCO's must develop a clear understanding of the local level business practices and strategy. LCO's must act within the scope of the Charter and Framework and must review and continually improve the effectiveness of the local Compliance Charter and Framework.

The LCO may delegate execution of tasks and responsibilities as appropriate.

Further details of LCO responsibilities are outlined in the Framework – Section 3 of this document.

2.4.4 Employees

Managing Compliance Risks and complying with applicable laws, regulations and standards in both personal and business conduct is the responsibility of every employee.

Employees must be aware of which compliance obligations impact their day-to-day business activities and must make sure they understand and meet them.

2.5 Authorities and capabilities of the CCO and the Compliance Function

2.5.1 Investigate and Challenge

When Compliance Function representatives perceive a Compliance Risk or when a Management decision may give or has given rise to a significant financial or reputation risk for the business, NN or any of its affiliated entities, the LCO must investigate and challenge any actions or concerns without influence from the business. If the matter is not promptly resolved, the LCO and Management must follow the escalation process. Following notification to Management, the CCO has the authority to request Corporate Audit Services to perform an audit.

2.5.2 Escalation

If and when a matter is escalated by the LCO to the CCO, the LCO and the CCO⁶ must decide whether to advise local Management that the course of action would result in an unacceptable Compliance Risk, in which case Management cannot proceed.

Local Management must postpone execution of the initial decision until the issue has been resolved by the CCO and higher level Management.

Significant compliance issues must in any event be raised directly and without delay with the CCO who will promptly bring the issues to the General Counsel.

The CCO has the right to escalate significant compliance issues affecting NN to the CEO of NN Group and / or the Chairman of the NN Supervisory Board, where appropriate. This also applies to a situation where the CCO and General Counsel have a different opinion on a compliance issue or Compliance Risk or the compliance issue directly concerns the General Counsel.

The CEO is ultimately responsible for resolving Compliance Risk-related disputes. The General Counsel and the CCO provide advice to the CEO and have the right to escalate to the Chairman of the NN Supervisory Board if deemed appropriate.

2.5.3 Access

The CCO must at all times have access in accordance with local laws and regulations to all activities in his or her area of responsibility. This includes access to all documentation, systems (e.g. complaints register, whistleblower reports and files), employees (including, (senior) Management, executive and non-executive board members) and the NN Supervisory Board.

Likewise the LCO must, at all times, have access in accordance with local laws and regulations to all activities in its area of responsibility. This includes all documentation, systems (e.g. complaints register, whistleblower reports and files) and employees (including executive and non-executive board members) and the local supervisory board.

The LCO (or the compliance officer to whom this task is delegated) must attend product approval committee and non-financial risk committee meetings. Further, the LCO must have the opportunity to attend, or submit information to other relevant board and committee meetings to raise significant compliance matters.

⁶ In case of NNIP's (non-Dutch) local businesses have LCO will escalate to the NNIP LCO.

2.5.4

Liaising and partnering

Other key functions

Throughout the NN organisation, Compliance is in close contact with other key functions⁷:

- Corporate Audit Services (CAS)

CAS is designed to audit and evaluate the company's internal control environment as to its adequacy, efficiency and effectiveness, including the Compliance control environment.

To ensure an effective coordination of activities between the two functions, it is essential that they leverage a common language of risk and control. A common methodology for Compliance and CAS leads to agreement on the definition of risk types and the used risk thresholds (e.g. as used in the Non- Financial Risk dashboard (NFRD)). Hence, CAS is:

- 1 periodically auditing the Compliance function both on Corporate level as locally and
- 2 is challenging the Compliance periodic report NFRD.

- Risk function

The (Non-Financial-) Risk function and the Compliance function have a strong cooperation and relationship. It hereby deals with the following topics:

- 1 Reporting: for reporting (NFRD) Compliance and Risk –together with legal- are responsible for the content. All functions involved challenge each other's risk levels and input;
- 2 Incidents: coordination and reporting of (immediate and Non-Financial Risk) incidents takes place within the Risk function. Where material compliance incidents are reported, these must be handled through the Risk incident reporting process Also, Compliance incidents above the thresholds are reported to Risk.

- Actuarial Function

within the Product Approval and Review Process (PARP) both at Corporate and local level the Compliance Function works together with among others the Actuarial Function. Both functions are represented in the product risk committee. The product risk committee ensures proper implementation of the PARP Policy including practical governance aspects, monitors compliance to customer suitability rules when developing or updating products, and reviews trends and product risks.

Regulators and industry bodies

Where possible, Compliance Function representatives should liaise with regulators and industry bodies and participate in industry meetings to ensure knowledge exchange about regulations and to improve Compliance knowledge. Compliance Function representatives must partner with legal, risk management functions and employees (including Management, relevant boards and committees) to ensure integrated risk management efforts without duplication.

In addition, the LCO shall participate in knowledge exchange of issues, best practices and lessons learned with the CCO and with risk management functions as well as participate in the development of policies and business impact assessments issued by Corporate Compliance.

2.5.5

Capabilities, Development, Evaluation & Remuneration

CCO

The CCO must have the necessary qualifications, experience and professional and personal skills to enable him or her to carry out his or her responsibilities effectively. The CCO must have an overall understanding of NN and the commercial operation of NN. The CCO must understand the obligations, legislation and standards that impact NN. The General Counsel must coach and train the CCO to ensure the CCO meets these requirements.

⁷ Key functions as defined in Solvency II Directive; Risk Management, Internal audit, Actuarial and Compliance function

The CCO must have the opportunity to develop his or her skills. Together, the General Counsel and the CEO are responsible for career development and succession planning of the CCO.

The remuneration of the CCO takes place in accordance with the NN Group Remuneration framework. The General Counsel and the CEO set the performance and development objectives, including training and education targets and evaluate the CCO on these objectives. The General Counsel takes the lead in setting the objectives and obtains input from CEO on the draft objectives, performance and performance rating .

Performance appraisals shall be jointly signed by the General Counsel and the CEO and retained in the CCO's performance management file.

Issues in relation to capabilities, development, evaluation and remuneration shall follow the escalation procedure outlined in this Charter and Framework under 2.5.2.

LCO

The LCO must have the necessary qualifications, experience and professional and personal skills to enable him or her to carry out his or her responsibilities effectively. The LCO must have an overall understanding of NN and the commercial operation of NN. The LCO must understand the obligations, legislation and standards that impact the business unit at local level. The hierarchical manager of the LCO together with the CCO must coach and train the LCO to ensure the LCO meets these requirements.

The LCO must have the opportunity to develop his or her skills. Together, the CCO and the hierarchical manager of the LCO are responsible for career development and succession planning of the LCO.

The CCO and Management, together, decide on the LCO's remuneration (fixed and variable) and appraisals. They set performance and development objectives, including training and education targets, and evaluate the LCO on these. The CCO takes the lead for these tasks and obtains input from the hierarchical manager on performance and outcomes.

Issues in relation to capabilities, development, evaluation and remuneration shall follow the escalation procedure outlined in this Charter and Framework under 2.5.2.

Compliance Function Representatives

Compliance Function representatives (not being the LCO) must have the necessary qualifications, experience and professional and personal skills to enable them to carry out their responsibilities effectively. They must have an overall understanding of NN and the commercial operation of their business. They must understand the obligations, legislation and standards that impact their business. The LCO must coach and train new Compliance Function representatives to ensure they meet these requirements.

Compliance Function representatives must have the opportunity to develop their skills. The LCO is responsible for career development and succession planning for the Compliance Function representatives.

Performance appraisals of Compliance Function representatives shall be signed by the LCO and retained in the Compliance Function representatives performance management file. The LCO is responsible for the performance and development objectives and evaluation of their Compliance

Function representatives. However, the CCO has the right to provide input on the objectives, appraisal and remuneration and to challenge the appraisal of Compliance Function representatives.

Issues in relation to capabilities, development, evaluation and remuneration shall follow the escalation procedure outlined in this Charter and Framework under 2.5.2.

2.5.6 Appointments and Terminations

CCO

After having consulted the NN Management Board, the General Counsel and the CEO decide on hiring. With respect to firing, the General Counsel and the CEO must agree after having consulted the chairman of the NN Group Supervisory Board.

LCO

The CCO together with local Management decide on the appointment or termination of employment of an LCO.

Local Management takes the lead for appointments and must seek advice from the CCO to ensure that the candidate meets the education, skill and experience requirements set out in the job description. Local Management also takes the lead for terminations of employment.

However, the CCO has the right to propose and veto candidates for appointment and has the right to terminate employment, or veto a proposed termination of employment, a person serving as the LCO.

In the event an agreement cannot be reached between the CCO and local Management, the escalation process described under 2.5.2 should be followed.

The LCO is responsible for the appointment and termination of employment of his or her Compliance Function representatives. However, the CCO shall be consulted on the appointment and termination of employment of Compliance Function representatives.

2.6 Reporting

2.6.1 Reporting at Local Level

LCO's must report at least quarterly to Management, relevant boards and committees on the effectiveness of implementation and embedding of the Charter and Framework and related policies in addition to other relevant Compliance topics that may be required by NN or by local regulations. The LCO must ensure reports are accurate, up-to-date, and on-time. Reports must also be sent to the CCO.

In addition, the LCO must report incidents and issues to regulators, local level Management and the CCO, as necessary or required. Management is responsible to appoint a Reporting Officer for the Whistleblower Policy. The Reporting Officer is responsible for reporting on new and updated whistleblower cases at least quarterly.

2.6.2 Reporting at Corporate Level

The CCO -in conjunction with other non-financial risk functions- reports at least quarterly to the NN Management Board on relevant Compliance topics. In order to do so, the CCO will challenge the content of the local reports to independently form an opinion on relevant Compliance Risks. Based on this challenge and opinion, the CCO will consolidate local reports for reporting at the Corporate Level. In addition, the CCO will report to the NN Management Board on a quarterly basis on the

effectiveness of implementation and embedding of the Charter and Framework and Compliance Risk-related policies across NN.

In addition to formal reporting, the CCO has periodic meetings with the CEO in which issues as well as ongoing business related issues will be discussed. Where appropriate available compliance reports will be (pre-) discussed.

The CCO reports at least semi-annually to the Risk Committee of the NN Supervisory Board on relevant Compliance topics.

In addition to formal reporting, the CCO will have bi-annual meetings with the Chairman of the Risk Committee of the Supervisory Board in which issues as well as ongoing business related issues will be discussed.

The General Counsel is responsible to appoint the CCO as the Reporting Officer for the Whistleblower Policy for the entire NN organisation. The Reporting Officer is responsible to report on new and updated whistleblower cases at least quarterly.

The CCO, as part of his or her assurance activities, reviews the LCO's supporting evidence and inquires whether the reports are accurate and current.

3. Compliance Framework

The NN Compliance Framework ('Framework') comprises the principles, processes and tools that NN Management and the Compliance Function use to manage Compliance Risk.

The Framework is the key tool for NN Management and Employees to understand – and apply – our approach to managing Compliance Risk. It also creates transparency for our external stakeholders.

The key considerations for managing Compliance Risk are:

- 1 Our NN Values – the Foundation for NN's Framework (subsection 3.1)
- 2 The Three Lines of Defence to Manage Compliance Risk (subsection 3.2)
- 3 The Framework in Our Business (subsection 3.3)
- 4 The Key Components of the Framework (subsections 3.4, 3.5 and 3.6)

The Framework complements, and should be read with, the Charter. Modifications to the Framework must be aligned with the scope of the Charter.

3.1 NN Values – The Foundation for NN's Framework

NN VALUES

The NN Values express what we hold dear, what we believe in and what we aim for. Individually, each principle is equally important, and taken as a whole, they form our collective conscience. As such, they are the foundation of our strategy, culture, day-to-day work and of this Framework.

The NN Values:

Care

This means we

Empower people to be their best

That is why at NN, we

- See our customers as the starting point of everything we do
- Work hard to meet and exceed our customers' expectations
- Provide our customers with the knowledge and confidence they need to make sound financial decisions
- Give our employees the opportunity to develop themselves, and provide them with an inspiring and healthy work environment
- Stand by our customers, and our colleagues, in their moments of truth

Respect each other and the world we live in

That is why at NN, we

- Treat others the way we want to be treated
- Appreciate our colleagues, who are the ones that make it happen
- Believe that working together leads to better results
- Respect human rights, advocate equal opportunities and encourage diversity of thinking
- Avoid or responsibly manage any negative impact our business activities may have on people or the environment, and seek positive change in society

Clear

This means we

Communicate proactively and honestly

That is why at NN, we

- Say what we mean and mean what we say

- Offer our customers trustworthy advice
- Use understandable language that addresses the heart of the matter
- Carefully explain the conditions, risks, returns and costs of our products and services
- Report timely and accurately on our financial and non-financial performance

Are accessible and open

That is why at NN, we

- Are there where our customers want us to be
- Are easy to approach, attentive and responsive
- Listen with genuine interest and empathy
- Engage in a candid dialogue and welcome feedback
- Strive to minimise complexity

Commit

This means we

Act with integrity

That is why at NN, we

- Take responsibility for our actions and deliver on our promises
- Comply with all applicable laws, regulations and internal policies and guidelines
- Use our knowledge responsibly and keep confidential what is entrusted to us
- Prevent or responsibly manage possible conflicts of interest
- Only do business with responsible, reputable and lawful parties

3.2

The Three Lines of Defence to Manage Compliance Risk

Both internal and external regulation shapes the risk environment in which NN operates. Our three lines of defence risk management model helps us to mitigate these risks – it applies to all businesses across NN. This model is essential for the effective operation of the Framework.



NN manages its Compliance Risks using three lines of defence: Business Management, the Compliance Function and Corporate Audit Services. The three lines of defence model distinguishes among functions that own and manage risks, functions that oversee risks and functions that provide independent assurance.

- 1 **Business Management**, the first line of defence, develops and implements mitigation activities, including monitoring and reporting, for managing Compliance Risks in business activities. Managers manage risk day-to-day; they bear the consequences of losses.
The first line of defence designs, implements and embeds business procedures, tracks internal mitigation activities, plans and executes training and executes other Framework activities.
- 2 **The Compliance Function**, the second line of defence, partners with legal to identify relevant Compliance Risk-related laws, regulations and standards. They translate the laws into compliance obligations and assist Management to identify their Compliance Risks. They help Management to identify activities to mitigate the risk based on the Management Board NN Group 's risk appetite, monitor local level Management's control of Compliance Risks and advise Management on Compliance matters. They work with other second line of defence functions to provide objective challenge and support, escalating matters when necessary to help optimise the trade-off between risk and reward. The second line of defence serves in an advisory role as the business designs, implements and embeds business procedures, tracks internal mitigation activities, plans and executes training and executes other Framework activities.
- 3 **NN 's Corporate Audit Services**, the third line of defence, provide Management with independent objective assurance on the overall effectiveness of the design and operation of internal controls (mitigation activities and tracking and monitoring activities performed by the first and second lines of defence).

3.3

The Framework in Our Business

NN operate in a complex, international regulatory environment with local and international compliance obligations. NN aim to comply with the letter and spirit of our obligations in our conduct and in our systems and processes. Therefore NN utilise a framework to manage its Compliance Risk.

Compliance Framework

The Framework consists of three key components: the Compliance Chart, Advisory Services and Scorecard. The Compliance Chart reflects the key activities performed by a business unit to understand and manage its Compliance Risks. Advisory Services, which impacts all components and activities of the Framework, is the mechanism that ensures that the business receives specialised support and advice to help manage its Compliance Risks more effectively. The Scorecard is a tool that allows a business unit to measure its progress towards effective Compliance.

The key Framework documents must be translated from the local language into English. The next subsections explain each of the components in detail.



3.4 The Chart and the Five Key Activities

For local levels, the Compliance Chart ('Chart') is a vital part of the Framework. The Chart provides an overview of the relevant local and international laws, regulations and standards as they relate to a business' operations. It also outlines how Compliance Risk mitigation activities are embedded in business processes. In other words, how compliance with the laws, regulations and standards is embedded and ensured. It helps a business to meet its compliance obligations to customers, regulators, shareholders and Employees because it centralises important information.

The Chart is an output of five key activities carried out in accordance with the requirements of the Framework:

ACTIVITIES

- a Identification of Compliance Obligations
- b Risk Assessment
- c Compliance Risk Mitigation (includes Training and Education)
- d Compliance Risk Monitoring (includes Action Tracking)
- e Compliance Risk Reporting (includes Incident Management)

The Chart must contain the following:

- 1 Reference to the key⁸ compliance-related laws, regulations, industry standards and NN compliance-related policies and standards;
- 2 Concise statements that capture the relevant internal and external compliance obligations and the risks arising from those obligations;
- 3 Inherent and managed risk level (critical, high, medium, low) of the identified obligations;
- 4 The business processes or people to which the compliance obligations are linked or on which they have an impact;
- 5 Specific Compliance Risk mitigation activities and Compliance Risk tracking and monitoring for managing the compliance obligations;

⁸ The key compliance-related laws, regulations, industry standards and NN compliance-related policies and standards will be determined by the local business on a risk-based approach. The evaluation must always be evidenced.

- 6 To whom and how frequently compliance-related results and findings are reported;
- 7 Clear ownership of the processes, activities and obligations outlined in the Chart.

The Chart must be as practical and concise as possible, and it must link specifically to existing and newly identified business activities.

MANAGEMENT MUST	LOCAL COMPLIANCE OFFICERS MUST
1 Help the LCO develop and update the Chart by clearly identifying the principle business activities and relevant processes affected by the obligation(s);	1 Develop and maintain a Chart for the business with assistance from Management;
2 Identify the individuals having accountability for executing the activities outlined in the Chart including those individuals with managerial responsibility;	2 Ensure that all components of and material changes to the Chart have been discussed with and formally approved by Management;
3 Formally approve the Chart;	3 Report material changes to the Chart to Management and the CCO.
4 Notify the LCO of any changes to products, activities, strategy or governance structures.	

3.4.1

Identification of Compliance Obligations

The Chart must be kept up-to-date. The Chart must reflect the compliance obligations and associated risks that arise. Such obligations may be based on policies issued by NN and / or international and local laws, regulations and standards that apply to a business' activities.

Obligations communicate to the business what it should or should not do. Inclusion of obligations should be risk-based.

Where there is a policy issued by NN , research must be conducted to identify whether additional or different local or international obligations exist. If a conflict between policies issued by NN , local law and/or international law arises, the conflict must be resolved and the appropriate obligation must be identified. Where the obligations of local laws or regulations impose greater or more stringent requirements than those included in a policy issued by NN (or if the opposite situation exists), the more stringent obligations must prevail.

Legal function must	Management must	Local compliance officers must
1 Proactively identify new and changed relevant local laws, regulations and standards in addition to those laws, regulations and standards identified by NN 's legal functional line, and advise the LCO of these in writing;	1 Identify, with the LCO risks that arise from the compliance obligations;	1 Translate Compliance Risk-related rules, laws and regulations into compliance obligations and enter those obligations into the Compliance Chart;
	2 Communicate compliance obligations to Employees.	2 Identify, with Management, the risks that arise from the compliance obligations;

- | | |
|--|--|
| <p>2 Review compliance-related policies issued by NN and determine whether additional or different obligations arising from local or international regulations or standards apply and communicate those additional requirements to the LCO in writing;</p> <hr/> <p>3 Work together with the LCO when there is a conflict between policies issued by NN, local law and/or international law to identify the relevant obligations; approve, in writing, identified compliance obligation(s) and the agreed upon resolution;</p> <hr/> <p>4 Confirm by signature, at least annually and more frequently, if required, that the key relevant laws and regulations are accurately translated and reflected in the Chart.</p> | <p>3 Work with legal when there is a conflict between policies issued by NN, local law and/or international law to identify the correct compliance obligation(s) and ensure the agreed obligation(s) and resolution(s) appear in the Compliance Chart.</p> <hr/> |
|--|--|

3.4.2

Risk Assessment

Management has ultimate accountability for the effective control of risks affecting their business and must take ownership and responsibility for execution of risk assessments. The Compliance Function oversees and objectively challenges execution, management, control and reporting of risks.

The Risk Assessment process, based on the Risk Assessment Minimum Standards, an on-going process, follows identification of compliance obligations. The first step includes identifying the obligations to be included in the Chart. The next step is to identify the inherent risk of each obligation as critical, high, medium or low⁹. The outcome determines the type of risk mitigation, first line tracking and second line monitoring needed to effectively manage the risk. Thereafter the business assesses its managed risk levels for the identified compliance obligations.

Risk assessments should be performed as the business' profile changes. Such changes may result because of new laws or regulations, new interpretations of existing laws or regulations, new theories of liability, a new activity of the business or changing social standards.

There are two types of risk assessments that can be performed: high-level risk assessment and detailed risk assessments.

High Level Risk Assessment

The risk identification and assessment and the detailed risk assessment results are required inputs for the annual integrated high level risk assessment facilitated by representatives of Risk Management. The current and anticipated critical and high Compliance Risks must be included in the high

⁹ In order to assess the inherent risk level, all relevant risk factors must be taken into account.

level risk assessment process. The outcome of the risk assessment is the high level risk assessment report.

Reports from the detailed and high level risk assessments must include key Compliance Risks, with existing and approved risk mitigation activities. Reports must be discussed and signed off in accordance with the risk management procedure on IRAP, which can be found on the NN intranet.

Risk assessment techniques can be a combination of desk assessments, interviews and/or workshops; however they should be aligned with risk management standards.

Management must	Local compliance officers must
1 Participate in all high level risk assessments and, on request, detailed risk assessments;	1 Ensure, on behalf of Management, Compliance Risks are included in the risk assessment process;
2 Work with the LCO and the legal function to identify the ongoing and anticipated critical and high Compliance Risks for inclusion in the assessments;	2 Participate in all high level risk assessments;
3 Work with the LCO to identify mitigation activities for inclusion in the assessments;	3 Identify, rate and rank, in cooperation with the legal function and Management, the ongoing and anticipated critical and high Compliance Risks and mitigation activities for inclusion in the assessments;
4 Work with the LCO to prioritise the ongoing and anticipated Compliance Risks for discussion in the high level risk assessment;	4 Approve the proposed risk assessment technique(s) to be used;
5 Approve the proposed risk assessment technique(s) to be used;	5 Participate in, as requested, or conduct detailed risk assessments when further input is required or when needed;
6 Approve the outcome of risk assessments;	6 Ensure reports from risk assessments include required Compliance Risk-related information;
7 Inform the LCO of any changes that may impact Compliance Risks in the business.	7 At least annually, review, update or confirm the Compliance Risks accepted in previously executed high level risk assessments and determine if further detailed risk assessments should be undertaken.

Detailed Risk Assessment

To ensure that risk is properly assessed and mitigated, a detailed risk assessment may be appropriate, particularly when further input is needed from support functions and/or to manage certain current and anticipated critical and high risk areas. To avoid duplication, this process should be aligned with assessments initiated by other risk functions.

3.4.3

Compliance Risk Mitigation

Compliance risk mitigation is the process of developing and implementing controls such as standards, policies, procedures and guidelines to prevent or minimise risks arising from compliance obligations.

From time to time, Corporate Compliance may issue a policy that must be implemented at the local level. If a Corporate policy does not encompass local obligations, a local policy to facilitate the effective management of the identified Compliance Risk must be developed.

Framework components, policies and procedures must be developed and communicated so Employees understand their obligations (e.g. how to make a Whistleblower report, complaints handling process, gifts, entertainment and anti-bribery procedures, etc.).

All documentation must be easily accessible to Employees. Maintenance of the material can be in the form of a manual, handbook or other physical or electronic means.

Management must	Local compliance officers must
1 Establish and implement specific, appropriate activities, within the time agreed with the LCO, to mitigate Compliance Risk in business processes;	1 Advise Management about compliance obligations;
2 Ensure that Framework components, policies, procedures and processes are drafted and presented in a way that Employees at all levels can access and understand;	2 Assist Management to identify risk mitigation activities;
3 Ensure that the business meets its obligations and embeds activities to mitigate risk in business activities;	3 Assess any corporate compliance policy, particularly its applicability, to determine whether the policy encompasses local obligations and if it does not, develop a policy that includes those local obligations;
4 Take the measures necessary to ensure that Employee behaviour conforms to the Framework (Compliance Risk-related policies and procedures, including NN Values) and	4 Raise issues to Management that may have an impact on the suitability of existing mitigation activities;
5 Include in all job descriptions and conditions of employment that the Employee is responsible and will be held accountable for meeting their compliance obligations.	5 Monitor that Framework components, policies and procedures are developed and communicated so that Employees understand their obligations and
	6 Establish and maintain compliance department information and procedures that the LCO uses, such as a compliance department organisation chart and LCO responsibilities; such information may be integrated into the Compliance Chart, incorporated in the form of a manual or maintained in any other physical or electronic means.

Training and Education

A strong Compliance training and education programme reinforces NN 's compliance culture. It builds awareness and understanding of Compliance standards, procedures, guidelines and issues. Specifically, it should build awareness and understanding of:

- NN 's Framework, including the four conduct-related integrity risk areas;
- Roles and responsibilities outlined in the Charter and Framework;
- Critical and high compliance obligations identified in the Chart;
- The process for addressing compliance issues and reporting concerns and
- Consequences of failing to meet compliance obligations.

An annual plan for Compliance Risk-related training and education must be developed and updated, as necessary, and should indicate the target audience and training delivery method.

Compliance Risk-related training programmes should, to the extent possible, be integrated into existing training programmes and plans.

Plans for compliance training and education programmes must include:

- 1 Concise statements that capture the relevant internal and external compliance obligations and the risks arising from those obligations;
- 2 The business processes to which the compliance obligations are linked or on which they have an impact;
- 3 Brief description of the training or education activity;
- 4 Target audience (refresher for existing Employees, induction for new Employees, or ad-hoc when required);
- 5 Frequency of training or education activity;
- 6 Whether an assessment (test) is required and
- 7 Person to Act (PTA).

Updates to the training programme or materials must include Lessons Learned and best practices.

Management must	Local compliance officers must
1 Develop, or integrate into, training programmes and annual plan Compliance Risk-related training and education topics;	1 Assist the training department and / or other department identified by Management in developing, maintaining and executing the annual plan for Compliance training and education;
2 Identify, with the LCO, the target audience and method for delivery of the training and education programmes;	2 Identify, with Management, the target audience and method for delivery of training;
3 Ensure delivery of Compliance Risk-related training for new hires , and regularly refresh knowledge, including new subjects, so all Employees receive the training and education they need to fulfil their roles and	3 Serve as a content expert for Compliance Risk-related training material
4 Ensure the execution of Compliance Risk-related training and education, and maintain attendance and assessment records.	4 Monitor the quality and frequency of the training and education.

3.4.4

Compliance Risk Monitoring¹⁰

Compliance Risk monitoring makes it possible for the business to test if its risk mitigation activities are working properly and to identify new or changed risks.

The plan for monitoring must be documented and reviewed and, if necessary, updated annually and more frequently based on other Framework activities and monitoring results. The plan must include:

- Critical and high Compliance Risks, focusing on inherent and managed risk levels;
- Key Compliance Risk mitigation activities;
- Routine business transactions to which compliance obligations or risks are associated;
- The implementation / embedding of the Framework and all policies issued by the corporate compliance department;

¹⁰ More information about monitoring can be found in the Monitoring guideline located on the Policy House – Social Collaboration Platform – SAM)

- Compliance with the laws, regulations and standards included in the Chart, including the NN Values and
- The obligations that have been delegated to the Compliance Function (e.g. Complaints Handling, Privacy- related obligations).

The plan for monitoring must include:

- 1 Concise statements that capture the relevant internal and external compliance obligations and the risks arising from those obligations;
- 2 The business processes to which the compliance obligations are linked or on which they have an impact;
- 3 Specific Compliance Risk mitigation activities for managing the compliance obligations;
- 4 The first line tracking (ongoing tracking as part of the normal course of business activities), second line monitoring (health check performed by the Compliance Function) and third line assurance (independent review performed by internal audit) for efficiency and / or effectiveness of first and second line activities);
- 5 Brief description of how tracking and monitoring activities are performed;
- 6 Frequency of tracking and monitoring activities;
- 7 Recipient(s) of the tracking and monitoring reports; and
- 8 Persons to Act (PTA).

The plan may be integrated into the Chart or may be a stand-alone document.

Management must	Local compliance officers must
1 Work with the LCO to identify the first line tracking activities and the persons accountable for executing the tracking activities for inclusion in the monitoring plan;	1 Work with the business to document an annual plan for monitoring (updated as required and based on other Framework activities and monitoring results);
2 Establish and execute first line of defence (business) tracking and report deficiencies to the LCO;	2 Establish second line of defence monitoring activities;
3 Work with the LCO to ensure appropriate evaluation of the first line tracking activities;	3 Submit the plan for monitoring to Management and the CCO for approval;
4 Address, within the time agreed with the LCO, issues that arise out of first line of defence (business) tracking and second line of defence (compliance) monitoring and	4 Execute second line of defence monitoring and report deficiencies to Management and the CCO.
5 Ensure adequate resources for executing an appropriate monitoring plan for all lines of defence.	

Action Tracking

Action tracking is a process used to ensure the visibility and resolution of Compliance Risk-related findings and issues. Compliance Risk-related findings and issues include:

- a Actions identified by Management in its day-to-day operations and from first line of defence (business) tracking;
- b Actions coming from second line of defence monitoring and other Framework activities and
- c Internal / external audit or regulatory findings and related actions.

Tracking of actions and issues assigned to mitigate identified risks (mitigation measures) must be done in accordance with the risk management Minimum Standard Issue and Action Tracking¹¹ requirements.

Management must	Local compliance officers must
1 Ensure compliance-related items are recorded in iRisk;	1 Monitor all Compliance Risk-related findings and issues until they are resolved;
2 Resolve identified issues in a sustainable manner within agreed deadlines;	2 Verify that findings and issues delegated to risk management for tracking in iRisk have been appropriately resolved;
3 Provide the LCO with status updates on open Compliance Risk-related items until the issues are resolved and	3 Incorporate, with Management, lessons learned into the components and activities, as appropriate, of the Framework (e.g. risk mitigation, Compliance Chart, etc.) and
4 Incorporate, with the LCO, lessons learned into the components and activities of the Framework (e.g. risk mitigation, Chart, etc.) and the business' policies, procedures, processes, etc.	4 Ensure resolution of, or escalate to Management and the CCO, unaddressed or overdue items.

3.4.5

Compliance Reporting

Compliance reporting allows Management and the Compliance Function to assess whether Compliance Risks exceed the risk appetite of NN or the local level. Reporting also allows for communication and discussion of potential Compliance Risks.

Management and the LCO are responsible for gathering information, and then analysing and communicating the results so that informed, timely decisions can be made. At least quarterly, reports should be discussed at the Non-Financial Risk Committee meeting (or equivalent Management team meeting).

There are two primary types of reporting: Cyclical Reporting and Incident Reporting. Management or regulators may request other reporting.

Cyclical Reporting

At least quarterly, the LCO works with Management and other risk functions to provide non-financial risk reporting. Management may require more frequent or other types of Compliance-Risk related reporting.

Incident Reporting and Management

Where material compliance incidents are reported, they must be handled through the risk management incident reporting process¹². Material compliance incidents are defined as events that have impaired NN's integrity, leading to material damage to NN's reputation, legal or regulatory sanctions, or financial loss, as a result of a failure (or perceived failure) to comply with applicable compliance-related laws, regulations and standards.

Some incidents are so critical they must be reported immediately; some can be reported periodically. They must, however, be reported. All relevant risk management functions and Management must work cooperatively to ensure that:

- reporting is encouraged;

¹¹ The Action Tracking Minimum Standard can be found on the Policy House – Social Collaboration Platform – (SAM)

¹² Incident Management and Reporting requirements and procedures can be found on the Policy House - Social Collaboration Platform (SAM)

- an integrated procedure is communicated to all Employees;
- incidents are clearly communicated;
- the issues raised are addressed and
- the business can develop and implement remedial actions and lessons learned.

There are two types of incident reporting: Immediate Reporting and Periodic Reporting.

Immediate Reporting

As per the Immediate Reporting Minimum Standards, the following findings and issues must be immediately reported to Management, risk management, the CCO and the NN Corporate Compliance department:

- Exceeds Euro 1 million actual loss;
- Can lead / could have led to a (potential) loss of Euro 5 million (including near-misses);
- Involves any senior Management;
- Can lead / could have led to material adverse reputation damage;
- Reports through the Whistleblower procedure that require the attention of Management after preliminary investigation; or
- Reports to external authorities including those (potentially) leading to investigation by external authorities.

Periodic Reporting

Periodic reporting is a type of reporting that occurs at a set period. At least quarterly, material compliance incidents must be reported to Management, risk management and the CCO and included as part of the non-financial risk (cyclical) reporting process. Management and the CCO may also require more frequent reporting.

Material compliance incidents include:

- Breach of NN Values;
- Breach of applicable laws, regulations and standards;
- Findings and issues that can lead to reputation damage;
- Regulatory sanctions (all events to be reported regardless of amount);
- Falls within the risk management (not immediate) incident amount thresholds ;
- Any other Whistleblower reports received not in the immediate reporting category and
- Near-miss not in the immediate reporting category.

Cross Border Compliance Related Incidents

When a Compliance Risk-related incident involves more than one local level business and / or jurisdiction, the relevant LCO's must notify the CCO. The CCO must coordinate remediation of the incident with the LCO's.

The remediation must be sufficient for all affected businesses or jurisdictions

Management must	Local compliance officers must
1 Develop and maintain an environment in which Employees are encouraged to report compliance incidents;	1 Work with Management, other risk functions and legal to provide business-relevant reporting on Compliance Risks and related matters to Management and the CCO;
2 Ensure that the risk management incident reporting process is available to all Employees;	
3 Ensure that any suspected compliance incident is reported to the LCO and/or Incident Reporting Officer (as outlined in the risk management incident reporting process);	2 Report information that Management needs to know, including information on key Compliance Risk issues, monitoring results, emerging trends, status of policy embedding and lessons learned;
4 Ensure accurate, complete and timely infor-	3 Ensure reports are accurate, up-to-date and on

	mation in compliance-related reports and address any issues that arise from reporting;		time;
		4	Incorporate the compliance-related requirements for incident reporting into the risk management incident reporting procedure;
5	Partner with the LCO to develop Lessons Learned (including risk mitigation activities) to help the business avoid future incidents and	5	Partner with Management to develop Lessons Learned (including risk mitigation activities) to help the business avoid future incidents;
6	Implement remediation strategies, including mitigation activities, within the time agreed with the LCO.	6	Ensure that the Non Financial Risk Committee discusses Compliance Risk-related incidents, remedial actions and lessons learned;
		7	Keep accurate records of reported material compliance incidents in the action tracking tool and
		8	Escalate to the CCO when Management is not resolving an incident (appropriately).

3.5

Compliance Advisory Role

The Compliance Function play a proactive advisory role: they advise Management, local boards and committees, the CCO and Employees. They provide advice on Compliance Risk, responsibilities, obligations, concerns and other compliance issues that are suitable for the business' practices and operational constraints.

Management must		Local compliance officers must	
1	Create and maintain an environment that supports the LCO in the role of advisor;	1	Respond to requests from Employees and Management for guidance on Compliance Risks and reports of Compliance Risks;
2	Seek advice from the LCO when developing new products and services, modifying existing products and services and changing local level governance (for example business models, corporate structures or strategy) and	2	Assess whether particular conduct or activities (including governance changes, (new) product review processes, mergers and acquisitions, outsourcing, etc.) comply with Compliance Risk-related laws, regulations and standards;
3	Work closely with the LCO to find compliant solutions that are suitable to the business' practices and operational constraints.	3	Advise officers or committees responsible for approval of conduct or activities (for example, Management committees, investment committees, product, service or transaction or new business approval committees);
		4	Take appropriate action where Compliance Risks are evident;
		5	Seek advice from the CCO when it is unclear what actions will result in a compliant outcome;
		6	Document and maintain records of advice given and
		7	Advise Management of responsibilities in regulatory implementation programmes.

In the event that a significant Compliance Risk is identified and Management's planned course of action may put NN at risk, the LCO must immediately escalate the matter to the CCO for an opinion. Together, a decision will be made whether to advise Management in writing that the course of action would result in an unacceptable Compliance Risk.

If Management is advised not to proceed, but nonetheless wishes to proceed, Management must follow the escalation process outlined in this Charter and Framework under 2.5.3.

3.6**Scorecard**

The Compliance Scorecard ('Scorecard') is a tool that Management use to evaluate the maturity of the Compliance Risk and framework (i.e. how well the framework are embedded in the business). As it measures a local level's progress towards effective risk management, the Scorecard is a vital part of managing risk.

Progress on Compliance risk management, measured by the Scorecard, is evaluated annually. From time to time, an interim evaluation is executed.

LCO's assist Management in evaluating the Compliance Risk-related elements of the Scorecard.

Management must	Local compliance officers must
1 Participate in the annual Scorecard process;	1 Assist Management in evaluating the compliance-related risks.
2 Identify remedial actions needed for deficiencies or gaps.	2 Gather and provide evidence for the compliance-related risks.

4. Administrative Matters

Waiver

If, for all circumstances, Management wishes to:

- exclude or
- implement a less strict requirement or
- use a different method to meet a requirement

of the Charter and Framework or policies issued by NN Corporate Compliance, Management must obtain written approval ('Waiver') from both the member of the Management Board NN who is responsible for the relevant business and from the CCO.

Please refer to the Minimum Standard Waivers for additional information over this process.

Exception

If, for a one-time situational occasion, Management wishes to:

- implement a less strict requirement or
- use a different method to meet a requirement

of the Charter and Framework or policies or minimum standards issued by NN Corporate Compliance, they must obtain written support from the CCO. The LCO must prepare and make a recommendation to the CCO, who must issue a final advice. Senior Management of the business making the request approves the exception.

5. Appendix

5.1 Delegated responsibilities Register

The NN Corporate Compliance department maintains the Delegated Responsibilities Register ('Register'). The Register provides an overview of responsibilities that have been delegated to the Compliance Function. Even though the corresponding policies (or procedures) are "owned" or managed by another Corporate (or other) department, there are particular compliance-related risks associated with or included in the policies (or procedures). Therefore, the Compliance Function is responsible to ensure that these particular responsibilities are executed.

Policy	Owner	Compliance task(s)
Anti-Trust / Competition	Corporate Legal / Corporate Compliance	Monitor the business' operations and activities to ensure compliance with competition law requirements
Complaints Handling	NN business unit's departments that interact with external clients	Monitor that complaints are: <ul style="list-style-type: none"> Handled timely Tracked Responses are appropriate
NN Statement of Living our Values	Corporate Communications and Affairs	Monitor that behaviors conform to the NN Values All senior management/Top 50 will sign off that they understand and will comply with the NN Values on specifically occasions and all employees when signing the Labor Contract.
Outsourcing	Corporate Risk Management	When activities are (performed as) an inherent part of NN 's business activities and directly affect or relate to NN 's integrity and if the Compliance Function would pay attention to the activities if they were performed by NN itself, the Compliance Officer must monitor that: <ul style="list-style-type: none"> third parties abide by and comply with (the relevant provisions of) NN 's Compliance policies third party files are periodically checked to ensure continuing adherence to compliance requirements

5.2 Roles & responsibilities of Corporate Compliance (Functional Oversight Team)¹³

5.2.1 Compliance Chart

The LCO must send the Compliance Chart for review to the First Point of Contact (FPOC) from the Functional Oversight Team. If necessary, depending on the complexity of the changes, the Compliance Chart should be accompanied by a version control document or attachment containing all changes included in the update, and history of updates.

Frequency for update

The Compliance Chart must be up-dated at least annually, by the end of the first quarter of a calendar year, to prioritize the activities to be performed during that year.

The Compliance Chart must also be updated on an ongoing basis based on, for example:

- when Legal has identified material changes in laws, regulations or regulator instructions;
- in case NN Group issues new or up-dated policies; or
- when the result(s) of risk identification and assessment exercises or from monitoring activities (of all lines of defence) warrant it.

Role of FPOC:

All material changes to the Compliance Charts must also reported to the FPOC of the respective BU. The FPOC will, in writing:

- review and give feedback on the document;
- provide support and advice whenever needed;
- compare the status of the most recent version of the Compliance Chart which reflects the embedding level of the Compliance (function); this should be aligned with the latest NFRD risk level. Any variations should be challenged.

Both the FPOC and the LCO must archive the FPOC's feedback for audit trail purposes.

5.2.2 Risk Assessment (RA)

The Risk Assessment process follows identification of compliance obligations:

1 a high level compliance risk assessment is **mandatory** to be performed at least once a year

The scope of the annual process is to:

- review, identify and prioritize potential areas of compliance risk, and advise on appropriate standards, procedures and solutions;
- review and/ or identify violations by clients (or related third parties) of laws, regulations or standards applicable to such third parties, or otherwise employing or selling or distributing, products or services we offer;
- review and/ or identify conduct related risks related, for example, to business practices, competition law, miss-selling, etc., as well as other conduct inconsistent with NN internal standards and guidelines.

2 it is **advised** to perform a Risk Assessment:

- Whenever there are compliance-related new or changed laws, regulations or standards, new theories of liability, new or changed activities of the business;
- As a result of performing a monitoring activity that indicates deficient controls or a possible change in risk profile;

¹³ For specific areas, like FEC, PAD and CREDO, the Functional Oversight team aligns with the specialists of those areas. Regarding these areas there is also direct alignment possible between BU's and relevant specialists from Corporate Compliance, but they both have to keep the FPOC informed of material developments.

- As a result of findings identified through (internal/ external) audits;
- As a result of media releases (newspaper, internet articles, etc.);
- In case of internal or external changes: for example, new NN strategy, changes at other insurance companies;
- Upon management request.

Role of FPOC:

Whenever planning the regular annual High level Risk Assessment and any topic-oriented Detailed Risk Assessment (for example: GEAB Risk Assessment), the LCO should involve their FPOC in order to discuss the topics on the agenda for the Risk Assessment and approach.

- FPOC should challenge the approach and document the Risk Assessment discussions with the LCO;
- Once the Risk Assessment is complete and approved by the local NFRC, the LCO should also inform the FPOC on how critical, high and medium risks are closed and if any issues are encountered;
- Following a risk-based approach (critical, high and medium inherent risks), the mitigation of the risks identified in the RA will be monitored through the regular NFRD report and can be discussed with the BU during NFRD calls;

5.2.3

Training

An annual training plan for Compliance Risk-related training and education must be developed and updated by the LCO. This should be done by the end of the first quarter of every year, in order to have a clear approach for the following months. Once the plan is created/ updated, the LCO must also send the plan for review to the FPOC. After incorporating the input received from FPOC, the training plan must be approved in the local NFRC.

Compliance Risk-related training programs should, to the extent possible, be integrated into other training programs and plans, in collaboration with other departments (incl. Corporate Compliance).

Role of FPOC:

- FPOC will advise on content and timing of the training plan using a risk-based approach (e.g. high and medium compliance risk areas are included at least in an annual training; audience should be chosen based on exposure, etc.);
- FPOC will monitor timely execution of training plan in the BU and efficiency (percent of attendance out of the proposed audience). FPOC will support the LCO in improving the training plan and execution;
- In case the training material is provided by Corporate Compliance, the LCO will support enrolment of all targeted staff and will report attendance and any issues to their FPOC;
- All communication with the Local Compliance Officer regarding training must be archived by FPOC.

5.2.4

Compliance Monitoring

Monitoring plan

A monitoring plan for compliance risk related monitoring activities must be developed and updated by the LCO. This should be done by the end of the first quarter of every year, in order to have a clear approach for the following months. Once the plan is created/ updated, the LCO must also send the plan for review to the FPOC. After incorporating the input received from FPOC, the training plan must be approved in the local NFRC.

On a regular timescale the adequacy and accuracy of the monitoring plan should be evaluated. New legislation and Risk Assessments output will influence priorities and regular changes need to be

adjusted in the plan. All changes made to the monitoring plan must be discussed with the FPOC and afterwards approved in the local NFRC.

Role of FPOC:

- Review annual monitoring plans for BUs and advise on topics and approach;
- Provide advice and support during the execution of monitoring by the LCO, if requested;
- Review and give feedback on monitoring reports, using a risk based approach: only reports with critical, high and medium identified or sensitive areas (Need Based Sales, Client Suitability, FEC and CDD, GEAB, Complaints, etc.) or if LCO requests support/feedback;
- Offer support or advice for tracking and closing critical and high risk findings;
- All communication with the LCO regarding monitoring plan and monitoring reports must be archived by FPOC.

Activity	Responsible	Timing	Input	Approval
Operational plan HO (to be sent to BUs)	Corporate Compliance team	Once a year Q4 previous year		CCO
Operational plan LCO	LCO	Yearly Q1	policies, feedback from FPOC	NFRC + FPOC
Chart	LCO	At least 1 x per year Q1	Laws and legislation, Corporate policies	Legal + NFRC + FPOC
Risk assessment	LCO	At least 1 x per year	Previous monitoring activities, CAS audits, legal changes, etc.	NFRC + FPOC
Training plan	LCO	At least 1 x per year Q1	Corporate policies, legal changes, feedback from FPOC, etc.	NFRC + FPOC
Monitoring plan	LCO	At least 1 x per year Q1	Risk assessment results, CAS audits, new developments, Corporate policies, feedback from FPOC, etc.	NFRC + FPOC