Generali Life Assurance Philippines, Inc.

OPERATIONAL RISK MANAGEMENT POLICY

Chief Risk Officer Function

LOCAL POLICY
For internal purposes only

generali.com

Document summary

Title	Operational Risk Management Group Policy
GIRS Classification	Group Policy
Document code	GLAPI-2019-001-RM
Approved by	GLAPI Board of Directors
Effective date	08 June 2020
Local Accountable Function	Chief Risk Officer Function
Key contact	mjparistoteles@generali.com.ph

Versioning and Ownership

Version	Date of issuance	Document code	Reason for and Extent of Changes	Owner
3	2019-02-20	GLAPI-2019-001-RM	Update of the framework in order to include some improvements	Local Operational & IT Risks
2	2018-01-31	GP_2018_003	Update of the framework improving the formalization of processes to manage Operational Risk.	Local Operational & IT Risks
1	2014-05-14	-	-	Local Operational & IT Risks

Main related internal regulatory references

- GLAPI Risk Management Policy
- GLAPI Compliance Management System Policy

Any substituted/abrogated internal regulation

Reason for issuing

[X] **Regulatory**	[ ] **Group coordination**	- IC CL 2016-68, Amended Risk Based Capital (RBC2) Framework - IC CL 2005-31, Corporate Governance Principles and Leading Principles - IC CL 2018-45, Guidelines on the Minimum Capitalization and Net worth Requirements for Composite Insurance Companies under the Amended Insurance Code.

EXECUTIVE SUMMARY

The Operational Risk Management Policy (hereinafter the "Policy") outlines the strategies, principles and processes to manage present and forward-looking operational risks to which the Generali Life Assurance Philippines, Inc. is exposed to in the performance of its activity.

They are defined in line with internal rules and regulations adopted by the Board of Directors and formally set out in the Generali Group Directive on the System of Governance and in the Risk Management Group Policy.

The Policy covers the following areas:

Generali Group operational risk strategy and key principles for setting related **risk tolerance limits**, in order to provide direction on the way to manage main operational risk areas (**Paragraph 3**).

Activities and internal processes for managing operational risks (**Paragraph 4**):

- identification and measurement of the operational risks Legal Entities are or might be exposed to;
- definition of proper actions to activate in order to mitigate and/or reduce them;
- implementation of a reporting system ensuring that information gathered is circulated at the various level of the organization;
- developing proper IT systems to support the process defined.

Roles and responsibilities for an adequate management of operational risks, considering the company organizational model and the regulatory framework **(Paragraph 5).**

This policy is the local adoption of the Generali Operational Risk Management Group Policy.

INDEX

1. Glossary and definitions

Acronym/Term	Explanation/Definition
IC	Stands for Insurance Commission of the Philippines which act as the administrative, management or supervisory body. Where a two-tier board system comprising of a management body and a supervisory body is provided for under national law, means the management body or the supervisory body or both of those bodies as specified in the relevant national legislation or, where nobody is specified in the relevant national legislation, the management body
GLAPI	Generali Life Assurance Philippines, Inc.
GLAPI BOD / BOD	Board of Directors of Generali Life Assurance Philippines, Inc.
BU OPERATIONAL RISK FUNCTION	Geographical areas and global lines of business which the Generali Group is organized into
BU CRO	Business Unit Chief Risk Officer
CEO	Chief Executive Officer
CRO	Chief Risk Officer
GROUP	The Generali Group whose ultimate parent Company is Assicurazioni Generali S.p.A.
GROUP RM	Group Risk Management function
GHO	Group Head Office
LOCAL CEO	CEO of a Group Legal Entity
LOCAL CRO	Local Chief Risk Officer
LEGAL ENTITY	Entity belonging to Generali Group and falling within the scope of application of the Group Policy. Any reference to local level shall be intended as to Group Legal Entity level
LOCAL RM (LRM)	Local Risk Management function
RAF	Risk Appetite Framework
RISK OWNERS	Heads of operational areas (or operational departments)
SENIOR MANAGEMENT	The CEO, the General Manager (if any) and the Head of those functions that carry out management supervision duties including, at least, the first reporting line of the CEO and of the General Manager (first line of defence)

2. Introduction

2.1 OBJECTIVES

Generali Group believes that adequate operational risk management has the primary focus on pro-actively identifying and assessing operational risk events that may occur, with the goal to define initiatives to prevent or respond to such events.

This policy is the **local adoption** of the **Generali Operational Risk Management Group Policy**.

With this Policy, the company aims at implementing a robust operational risk management framework, defining the **key principles** that need to be considered and put in place to ensure:

- **Risk Owner awareness** about operational risks that may occur (through identification and measurement process);
- **effective Risk Owner decision making process**, in which the related operational risks are fully understood and proper actions are taken for reducing the risk, in coherence with the Risk Appetite Framework (through management process);
- **periodic risk monitoring** is performed by Risk Owners and Risk Management (through monitoring process);
- **proper reporting** is timely produced and circulated (through reporting process).

This policy defines minimum standards, BU and Local CROs are entitled to carry out a more detailed analysis, aligned with Group framework, if deemed appropriate.

2.2 APPROVAL AND REVIEW

The Policy has been approved by the Board of Directors (BoD) of Generali Life Assurance Philippines, Inc. upon proposal of the Head of the CRO function.

The Policy shall be promptly reviewed, and in any case at least once a year to include developments in legislation, market and/or best practices, company strategy and organisation.

2.3 EFFECTIVE DATE AND IMPLEMENTATION DEADLINE

The Effective Date of the Group Policy is 08 June 2020.

The Implementation Deadline of the Group Policy is 15 October 2020.

2.4 SCOPE OF APPLICATION

This Policy applies to:

- Controlled Regulated Group Legal Entities: concerning the Overall Risk Assessment, Loss Data Collection and Scenario Analysis activities, these Group Legal Entities should perform, at least:
    a. Internal Model Group Legal Entities:
        I. Overall Risk Assessment carrying out a Quantitative Risk Assessment (Light Scenario Analysis);
        II. Loss Data Collection;
        III. Scenario Analysis.
    b. Non-Internal Model Group Legal Entities:
        I. Overall Risk Assessment carrying out a Qualitative Risk Assessment;
        II. Loss Data Collection;
- Controlled Not Regulated Operative Group Legal Entities: concerning the Overall Risk Assessment, Loss Data Collection and Scenario Analysis activities, these entities should perform, at least:
        I. Overall Risk Assessment process carrying out a Simplified Risk Assessment.

This Policy does not apply to:

- Investment funds and vehicles, for which the application of this Policy is mandatory for the respective Group management company;
- Not controlled Legal Entities;
- Controlled Not Regulated Residual Group Legal Entities;

Moreover, for Joint Ventures the application of the Policy depends upon the specific provisions set forth within the shareholder agreement.

2.5 WAIVERS AND DISPENSATIONS

If a conflict exists between the Generali Operational Risk Management Group Policy with local laws, regulations or collective labor agreements arises or a proportionality[1] consideration applies, then the company CRO, in agreement with the Regional CRO, shall submit a waiver and/or dispensation request to the Regional CRO supporting and explaining the conflict.

The Regional CRO manages and tracks any waiver and/or dispensation request and provides the company CRO through the Regional CRO with the related feedback. The CRO shall report any significant waiver and/or dispensation to the GLAPI BOD

Company/Regional/Generali Group Compliance support a due evaluation of waivers, when they result from conflicts arising from laws and regulations falling into their mandate.

2.6 IMPLEMENTATION, MONITORING AND INFORMATION FLOWS

The Generali Group CRO Function is responsible for overseeing and supporting the implementation and monitoring of the Operational Risk Management Group Policy across the Group.

Company CRO[2] is responsible for guaranteeing a due information flow on the approval and implementation of the Generali Operational Risk Management Group Policy within the perimeter of responsibility.

Any relevant organizational unit within any entity in scope shall promptly inform its Actuarial, Internal Audit, Risk Management and Compliance function (where applicable) of any facts and/or circumstances connected with this Policy which may be relevant for the performance of their duties.

[1] Regarding the size, internal organization, nature, scope and complexity of the entity's activities.
[2] Or the relevant Local accountable function, in line with the local system of powers.

3. Risk strategy and tolerance limits

As stated in the Risk Management Policy, **operational risk is the risk of loss arising from inadequate or failed internal processes, personnel or systems, or from external events**.

The definition includes the compliance risk and financial reporting risk[3] and excludes the Strategic and Reputational Risks.

The operational risk could be generated by:

- **internal processes**: failure in the design and execution of core (re)insurance and support processes such as sales and marketing, underwriting, policy issuance, customer billing and premium collection, reinsurance placement, claims payments, actuarial reserving and outsourcing processes;
- **people**: human errors, fraud, unmanaged staff turnover, overreliance on key personnel, unmatched skills to job requirements, inadequate management oversight;
- **systems**: inadequate data and security protections, weak access controls, unstable and overly complex systems, lack of adequate testing prior to production, deficient systems/tools;
- **external events**: natural disasters (floods, fires, earthquakes, etc.) as well as man-made disasters (terrorism, political and social unrest) that may impact the ability to operate on an ongoing basis; changes in the regulatory environment including new regulations.

Operational risk is present in all activities conducted within the company and typically cannot be avoided. The operational risk management framework aims to reduce operational losses and other indirect consequences**,** including reputational damage and missed business revenues, resulting from the occurrence of operational risk events.

In consistency with the Risk Appetite Framework, considering the nature of operational Risk described above, the **operational risk strategy** is to have in place **an effective framework to continuously assess and mitigate operational risk**, while ensuring compliance with the applicable legislations, administrative provisions and internal regulations.

3.1 KEY PRINCIPLES

In order to be effective in the implementation of the operational risk strategy, the following key principles should be respected:

- pursue a strong **risk culture** ensuring a relevant level of competency within the organizational structure to guarantee a clear understanding of the risks faced within processes and systems (also through training initiatives, Code of Conduct, etc.);
- develop, implement and maintain the company **operational risk framework** that is **fully integrated** into the overall risk management processes;
- develop a clear, effective and robust **governance** structure with well-defined transparent and consistent lines of responsibility (considering that all employees are responsible of managing the operational risk), that allows the managing of operational risk in all processes and systems, consistently with the risk appetite and tolerance;
- define, effectively implement and maintain throughout the organization **policies**, **guidelines, technical measures** and **procedures** for managing operational risk in processes and systems consistent with the risk appetite and tolerance. In this regards, the Risk Owners define and promote internal regulations in order to support also a proactive management of operational risk;
- ensure the **identification** of the operational risk is embedded in company processes and systems, to make sure the risks are well understood. In particular, developing a forward looking mechanism to steer risk by **integrating operational risk** management processes, wherever possible, directly **within business processes**;
- Operational risks should be managed on a proactive rather than reactive basis, taking into account internal or external changes with potential to alter the operational risk profile of the company and responding to such changes in advance of the occurrence of operational risk events;
- implement a process to regularly **monitor** operational risk profiles and material exposures to losses;
- define and implement appropriate strategies to **mitigate and/or reduce** the operational risks.

3.2 RISK TOLERANCE

The company accepts that some level of operational risk needs to be tolerated in order to conduct business. In particular:

- For Compliance Risk, the company aims at acting in full compliance with the applicable legislations, administrative provisions and internal regulations. When the need to mitigate the compliance risk arises, a risk-based approach can be applied. The risk-based approach to compliance management does not mean that for low compliance risk situations, noncompliance is accepted. It assists the organization in focusing primary attention and resources on higher risks as a priority, and ultimately will cover all compliance risks.
- For Financial Reporting Risks the company aims at minimizing the exposure.
- For all other Operational Risks, the exposures are assessed and mitigated based on a cost-benefit perspective, whereby the expected incremental value of loss reduction exceeds the associated costs of strengthening the controls. Moreover, cost-benefit exceptions related to protecting the company reputation and other strategic objectives may also exist.

The company define and review risk tolerance limits both from a forward-looking perspective and for a backwards perspective, setting up effective escalation mechanism in case of limits violations, according to Operational Risk Methodological Guidelines and related Operating Procedures.

In particular, it should be considered that:

- **The Annual Overall Risk Assessment** exercise provides clarity on those risks that may affect, also in a forward-looking perspective, the business planning and strategies, to support risk-informed decisions at the Senior Management (executive committee) level and to enable proper risk oversight by the GLAPI BOD. This exercise allows the Risk Owners to define proper actions to bring the risks within the defined risk tolerance.
- **The Loss Data Collection** process triggers different escalation process for losses occurred above pre-defined thresholds (backwards perspective), in order to manage the root cause, identify and implement managing actions. In particular:
    - For losses with an impact at least above €1,000 – Php 60,000[4], Risk Owners provide, quarterly, a set of information related to the event (e.g.: description, date of occurrence) to the Risk Management. Quarterly data are then submitted for information to the Regional Risk Management.
    - For losses with a potential impact above €40,000 – Php 240,000, Risk Owners inform timely Risk Management about the event, the potential consequences and the related actions identified. Risk Management informs Regional Risk Management.

[4] According to the proportionality principle, lower thresholds can be applied by Legal Entity. Threshold definition is regulated by Operational Risk Operating Procedures.

4. Processes

The Generali Group operational risk management framework is composed by the following processes:

- **Identification and evaluation:** it establishes principles, tools and methodologies for adequate identification and classification of operational risks;
- **Measurement**: it establishes principles, tools and methodologies to assess operational risks;
- **Management**: it establishes principles for the decision process to reduce, mitigate or retain the risk;
- **Monitoring**: it monitors the evolution of the risk profile and the consistency with the principles stated by this Policy;
- **Reporting**: it aims at ensuring adequate information flows on operational risks towards the internal bodies and the GHO as well as towards supervisory authorities and other external stakeholders.

These processes are defined in accordance with the Group risk management framework ensuring a disciplined and consistent approach, auditable and traceable. Group Legal Entities, in accordance with the scope of application defined, should at least apply the following minimum standards:

		Identification and evaluation (Overall Risk Assessment)			Measurement			Management Monitoring Reporting
		Quantitative Risk Assessment	Qualitative Risk Assessment	Simplified Risk Assessment	Loss Data Collection	Scenario Analysis	Risk Capital Calculation	
Controlled Regulated	Internal Model	✔			✔	✔	✔	✔
	Non-Internal Model		✔		✔		✔	✔
Controlled Not Regulated Operative				✔				✔

Table 1 – Scope of activities

The BUCRO, in agreement with the relevant Business Unit Compliance Officer, may decide to perform the qualitative risk assessment also for Controlled Not Regulated Operative Legal Entities in relation to the magnitude of their exposure to the operational risks.

4.1 IDENTIFICATION AND EVALUATION

The **risk identification** process is under the responsibility of the Risk Owners during the continuous accomplishment of their activities, with the support of the Local Risk Management and Local Compliance, performed by means of the following tools:

- Group operational risk map
- Identification and classification catalogues
- Risk evaluation: through the Annual Overall Risk Assessment (ORA) performed by risk owners in order to ensure a comprehensive evaluation and identification of the operational risks.

Operational risk map: the operational risks to which the company is exposed to are identified and classified declining the Risk Map defined in the Risk Management Policy as follows:

- *Internal fraud*: events arising from intentional acts that are illegally performed by one or more employees and agents directly or by way of third parties, in order to obtain a profit for themselves or for others.
- *External fraud*: events arising from acts of fraud, robbery or misappropriation, which involve only external parties with the intention to violate/circumvent the law, internal policies and regulations, to obtain a personal profit.
- *Employment practices*: events arising from acts/omissions, intentional or unintentional, inconsistent with applicable laws on employment, health and safety and from claims pertaining to personal injuries or to diversity/discrimination acts which the company is responsible for.

- *Clients and Products*: events arising from unintentional or negligent failures (where there is an advantage for the company) to meet a professional obligation to specific clients or to the market in general.
- *Damage to physical assets*: events arising from natural disasters, terrorism, criminal damage or from violation of public security norms for which the Company is not responsible.
- *Business disruption and system failure*: events arising from disruption of business or system failures including the failure of utilities. Disruption and/or failures caused by hacking attacks or natural disasters are excluded.
- *Execution and process management*: events arising from inadequate design, management or conclusion of processes or operational practices or from relations with trade counterparties and suppliers.

Compliance risk and financial reporting risk are crosswise with respect to the aforementioned risks.

Identification and classification catalogues: the information on the identification and classification of operational risks is gathered and managed based on standard classifications of elements upon which the operational risk management process is based:

- *operational event:* any occurrence that could directly cause one or more operational losses to the company;
- *cause of the operational event:* reason for which the event occurred or could occur;
- *effect of the operational event:* economic or management impact arising from an operational event taking place, which jeopardizes or could jeopardize the fulfilment of the company objectives;
- *value Chain:* representation of all the processes of an insurance company;
- *management tools:* set of elements of organizational nature that the company shall establish to manage, monitor and reduce the risk.

Risk Evaluation through Annual Overall Risk Assessment (ORA): performed by the Risk Owners according to the Scope of application:

1. Quantitative Risk Assessment (Light Scenario Analysis). The Risk Assessment is a structured process, steered by Local CRO and Local Compliance Officer functions, through which the Risk Owners and Risk Owner Representatives are in charge of providing a forward-looking assessment over all operational risks. In this activity, they are supported by Subject Matter Experts, who possess a proper level of technical knowledge, seniority and experience, enabling them to contribute towards the assessment of the risks in their area of responsibility. The assessment is performed considering:
    a. **Control system adequacy** of Operational Risks**,** evaluated considering internal/external regulation and a set of key indicators (e.g.: past controls and assessments, audit findings & inspection, complaints & litigations);
    b. **Residual Risk Assessment**: measured through a **Scenario Analysis** approach, a structured process in which plausible future material events are estimated in terms of Typical Case impact, Worst Case impact and the Frequency. The estimation and the combination of these parameters determine the Value at Risk (VaR) related to the risk under analysis, taking into consideration any measure in place to reduce the risk.

    As specified in paragraph 3, this estimation does not consider the Reputational and Strategic impacts. However, in order to reduce indirect consequences related to these impacts, during the Risk Assessment process further qualitative considerations are made, taking into account also reputational impacts and potential loss of business triggered by Operational Risks. These impacts are related to losses that do not materialize in Profit&Loss (P&L), but in lower future incomes or worsening of strategic assets, that could increase the final residual risk.

2. Qualitative Risk Assessment. The risk assessment is performed annually and jointly steered by Local CRO and Local Compliance Officer functions. Risk Owners are in charge of providing a detailed forward-looking assessment over the operational risks, obtained via the evaluation of two dimensions:
    a. **potential risk exposure**, obtained combining potential losses and likelihood defined via expert judgement and a list of key indicators (e.g.: sanction, past internal losses and operational risk data and information from the industry);
    b. **control system adequacy** evaluated considering internal/external regulation and a set of key indicators (e.g.: past controls and assessments, audit findings & inspection, complaints & litigations and training).
3. Simplified Risk Assessment. The risk assessment is performed annually and addressed to Local CEOs, who are in charge of providing a simplified forward-looking assessment over the operational risks.

The outcome of the above risk assessment is a heat map that represents the residual risks into four main buckets, that triggers different actions for each bucket:

- Very High / High priority risks, which require immediate / prompt actions, such as definition of projects or initiatives to enhance the control system adequacy, traditional insurance mitigation actions to transfer the risk to third parties or, ultimately, to refuse the risk by limiting the activities and therefore the underlying risk cause.
- Medium priority risks, which require actions and interventions compatible with potential other priorities.
- Low and very Low priority risks, where cost/benefit analysis could potentially lead to postponed or no interventions.

The results of the risk assessment have to be discussed within the Group Legal Entity Risk committees or other equivalent Senior Management committee and the risk assessment outcomes have to be a significant driver for the definition of the annual activity plan.

4.2 MEASUREMENT

In order to ensure operational risks are measured and evaluated in an integrated and homogeneous manner, the following steps are in place:

- **Loss Data Collection**: for identification and collection of operational events that arise operational losses;
- **Risk capital calculation**.

The aim of identifying operational events materialized is pursued via the **Loss Data Collection** Process: this is the process for gathering information on experienced losses by the company, where Risk Owners collect information with the support of Risk Management function. The process is integrated by a structured analysis of external losses occurred to other institutions different from the Generali Group. The main objectives of this activity are:

- strengthen the awareness around operational risk into the business lines;
- improve reliability of the forward-looking self-assessments on operational risks provided by the Risk Owners;
- support identification and planning of actions to mitigate risks and to monitor their effectiveness.

Operational loss data are collected and analyzed, at least quarterly, in an accurate approach to guarantee complete traceability also in the accounting systems.
To built-up the **loss distribution** in one-year period, the first step is to select the main risks to use in the following simulation of quantification. The selection is done according to priorities identified via the Qualitative Risk Assessment.
While Generali Group conducts Operational risk Scenario Analysis for quantification, a waiver has been granted and scenario analysis not applicable to the company. Quantification will be done through the qualitative assessments
The overall process is steered by Risk Management, which involve the Risk Owner and appropriate experts for support and challenge.

The operational risk **capital requirement** is calculated by GLAPI according to the applicable regulation and Generali Risk Management Policy. In particular:

- Philippine Insurance Commission Circular Letter 2016-68.
- Philippine Insurance Commission Circular Letter 2018-45.

4.3 MANAGEMENT

This process refers to the actions to put in place to manage operational risk in line with the defined risk strategy. In particular, the choice consists of:

- *reducing* the risks and consequently decreasing the exposure to risk by the implementation of dedicated initiatives (e.g. additional controls, ad-hoc project, etc.);
- *mitigating* the risks, that it may include the use of traditional insurance mitigation actions in order to transfer the risk to another entity;
- *retaining* the risks, considering a conscious acceptance of risk exposure linked to the activities of the business.
- *avoiding* the risks, preventing from executing the activity carrying the risk.

The Senior Management is responsible to take appropriate decisions, duly documented, leveraging on the results of the activities carried out within the operational risk framework. In particular, Senior Management is responsible to:

- assess the actions identified to manage the risks;
- act consistently with the risk strategy, in particular according to a cost benefit analysis.

At least on a yearly basis the results of the operational risk processes are summarized, submitted for discussion to the Risk Committee (or equivalent Senior management committees) and approved by the CEO as ultimate Risk Owner.

4.4 MONITORING

The monitoring is based on the analysis of the results of the identification and measurement phases performed through the Loss Data Collection and the Risk Assessment processes, to verify the operational risk profile based on the processes evidences.

The monitoring of operational risks shall be implemented through an on-going process which involves, on the basis of the respective levels of responsibility, the Risk Owners, the Senior Management, Risk Management function, Compliance function and, as a third line of defence, Internal Audit function.

The monitoring of the evolution of the operational risk profile within the Legal Entities and the compliance with principles stated by this Policy and Operational Risk Methodological Guidelines is ensured by the Risk Management function.

Any major operational risk failure needs to be immediately managed and reported to Regional Risk Management via CRO.

4.5 REPORTING

The Legal Entities adopt a reporting system which ensures that information gathered at the different phases of the process is circulated at the various levels of the organizational structure, including Risk Committees (or other equivalent Senior Management Committees).

The presentation and classification of operational risk processes outcomes is performed in a structured manner and includes all relevant evidences emerged in the Operational Risk Processes.
In particular, the reporting includes:

- key operational risks the company is exposed to.
- main operational losses that occurred in the company.
- relevant management actions in order to reduce the risk;
- any other information significant for understanding the Company's Operational Risk Profile.

The whole documentation concerning the Operational Risk processes is adequately formalized and promptly archived.
In order to achieve an effective documentation storage, the database of operational risk management process is supported by specific IT tools. The outcomes of operational risk processes are systematically stored in dedicated IT applications that:

- ensure traceability over time;
- allow detailed analysis of operational risk components such as events, root causes, scenarios;
- guarantee the principle of ownership and visibility of the data;
- allow prompt visibility for audit purposes.

With the aim to enhance and strengthen the reporting system and to facilitate prompt reaction and remediation, the functions involved in the operational risk management process (including Local Compliance function, Local Financial Reporting Risk function, etc.), on the basis of the respective levels of responsibility, mutually exchange significant information on the main outcomes of their respective activities.

5. System of Governance

In addition to the tasks already indicated in the Generali Group Directives on the System of Governance, in the Risk Management system, in the Risk Management Policy as well as in the Compliance Management System Policy, the following roles and responsibilities are attributed in connection to the management of the operational risks.

The **Risk Owner** is the head of operational departments and has direct responsibility to take charge for operational risks, manage them and implement appropriate control measures. In particular, he/she has the following responsibilities:

- acts as first line of defence for the identification and assessment and management of the operational risk and for the implementation of the necessary management actions;
- involves relevant support functions (such as Organization, HR, Legal, etc.) for identification, measurements and management of the operational risk;
- cooperates with RM to provide adequate communication and training.

The **CRO** is responsible to ensure completeness, functionality and efficacy of the operational risk tools, systems and practices and supervises the implementation of the Operational Risk Policy at local level. Furthermore, he/she ensures guidance, coordination and alignment within the company.

In order to achieve his/her objectives, the CRO steers and supervises the following activities of the Risk Management:

- implements and monitors all phases of the operational risk management process at company level;
- ensures the process deployment at local level according to Generali Group standards (methodologies and guidelines);
- contributes to the overall Generali Group operational risk system providing feedback for management reporting at Generali Group level;
- supports the local first line of defence to properly identify, measure and manage operational risks.

For Operative Group Legal Entities, for which no Local CRO is appointed, it is responsibility of the BU CRO to coordinate the execution of the requirements defined in the Policy itself as well as their verification.

The Compliance function is kept informed across the entire operational risk management process. In line with its mission, it is responsible for the compliance risk assessment process and cooperates with Risk Management in assessing operational and compliance risks.

6. Roles and Responsibilities

Role	Responsibility
Group CRO	• sets up and runs an appropriate operational risk management system and the accurate implementation of the directions given by the BoD and the provisions of the Operational Risk Management Group Policy • steers and supervises all the activities performed by the Group CRO function
Group CRO Function	• designs and implements the operational risk governance model • defines principles, tools, methodologies and related guidelines for operational risk management • ensures completeness, functionality and efficacy of the tools, systems and practices undertaken to identify, measure and manage operational risks • supervises the definition and implementation of Operational Risk Management Group Policy, Guideline and related Technical Measures • ensures adequate monitoring and reporting of operational risks and specifically reporting to BoD, assisted by the Risk and Control Committee (and Senior Management) on the risk profile and main operational risks being identified • supports the Group Legal Entities in performing operational risk activities to identify, measure and mitigate operational risks • steers the Scenario Analysis process together with Local CRO function
Group Compliance Officer Function	• is kept informed across the entire operational risk management process • it is responsible for the compliance risk assessment process and can advise in the definition of the operational risk methodology
BU CRO	• Coordinate the execution of the requirements defined in the Policy itself as well as their verification, for operative entities, for which no Local CRO is appointed
Local CRO	• ensures completeness, functionality and efficacy of the operational risk tools, systems and practices • supervises the implementation of the Operational Risk Management Group Policy at local level • ensures guidance, coordination and alignment within the Business Unit at Group Legal Entity level • steers and supervises all the activities performed by the Local CRO function
Local CRO Function	• implements and monitors all phases of the operational risk management process at local level • ensures the process deployment at local level according to Group standards (methodologies and guidelines) • contributes to the overall group operational risk system providing feedback for management reporting at Group level • supports the local first line of defence to properly identify, measure and manage operational risks • informs Group CRO function on Loss Data collected in line with thresholds defined • supports Risk Owners in identify and assess operational risks • steers operational risks evaluation together with Local Compliance Officer function
Local Compliance Officer Function	• is kept informed across the entire operational risk management process • it is responsible for the local compliance risk assessment process and cooperates with Local CRO function in assessing operational and compliance risks • supports Risk Owners in identify and assess operational (compliance) risks • steers operational (compliance) risks evaluation together with Local CRO function
Risk Owner	• as head of operational areas, is the ultimate responsible for the Operational Risk evaluation performed within Overall Risk Assessment and Scenario Analysis, if applicable • leads the identification and reporting of the operational risk loss events.
Risk Owner Representative	• delegate of the Risk Owner for conducting the operational risk evaluation, with the support of Subject Matter Experts if needed and performing LDC related activities (e.g. collection of information, input data into database, etc.)
Subject Matter Expert	• Support Risk Owner and Risk Representative in the final evaluation, as professional with a strong business knowledge providing its own expertise in supporting the expert judgment