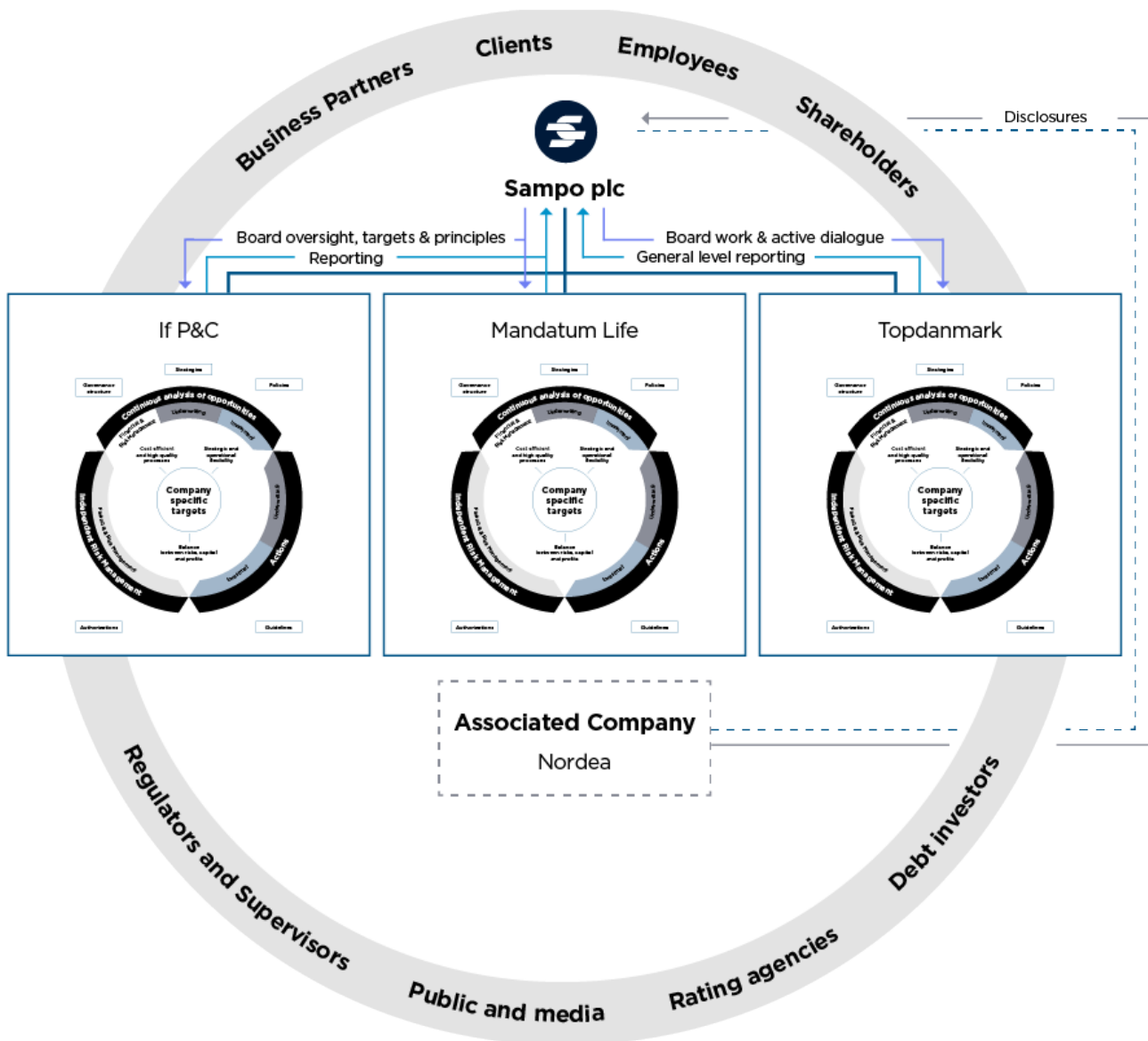


# Appendix 1: Sampo Group Steering Framework and Risk Management Process

When Sampo Group is organizing its business and risk management activities, clear responsibilities and simple and flat operational structures are the fundamental principles. The responsibilities and operational structures followed in Sampo plc and wholly-owned subsidiaries, as illustrated in the figure Sampo Group's Steering Framework are described in the following paragraphs. In regards to Topdanmark, its

Board and management share Sampo's view on how to prudently steer business activities and risk management process, although its current steering models and risk management processes do not have directly Sampo Group's practices as their basis. Hence, Topdanmark's current steering framework and risk management processes are not exactly the same as described next.

**Sampo Group's Steering Framework**



## Parent Company's Guidance

Group's parent company steers the wholly-owned subsidiaries by setting targets for their capitalization and return on equity ("RoE") and by defining the main preconditions for the subsidiaries' operations in the form of the group-wide principles.

**Target Setting:** The Board of Directors of Sampo plc decides on the subsidiaries' return on equity targets which are currently 17.5 per cent for both If P&C and Mandatum Life. In addition, If P&C has a long-term target of maintaining the combined ratio below 95 per cent.

The parent company assesses the adequate level of capitalization and the suitability of the capital structure as described at the section "[Capitalization at the sub-group level](#)". Based on this analysis, the parent company estimates the amount of dividends distributed by the subsidiaries to the parent company. In Sampo Group, the excess capital from an operational point of view is held by the parent company which capitalizes the subsidiaries if needed.

The Board of Directors of Sampo plc decides on the main guidelines governing the subsidiaries' business activities and risk management. The most significant of these guidelines are the Code of Conduct, Risk Management Principles, Remuneration Principles and Compliance Principles. There are also further guidelines which are followed in order to prevent reputational and compliance risks, for example the Disclosure Policy.

Moreover, Sampo plc's Board of Directors' decisions and thereby also the guidance given to subsidiaries may be impacted by the external regulatory environment and expectations of different stakeholders on Sampo Group's operations. Further information on Sampo Group's relations with its stakeholders is available within the Code of Conduct at [www.sampo.com/steeringsystem](http://www.sampo.com/steeringsystem).

## Subsidiaries' Activities and Risk Management

Subsidiaries organize their activities independently, taking into account the specific characteristics of their business operations and the guidance from the parent company relating to targets, capitalization and group-wide principles. The stakeholders' expectations and external regulations also have a direct effect on the subsidiaries' activities.

Sampo Group's subsidiaries decide independently on the governance structure of their operations. The executive management of the subsidiaries have extensive experience in the insurance industry, as well as in financial and risk management. The members of different committees and governing bodies represent expertise related to business and other functions. The subsidiaries' operations are monitored by the different governing bodies and ultimately by the Boards of Directors whose members are mainly in senior management positions in Sampo or in Sampo Group companies.

Since only the main guidelines are prepared by the parent company, the subsidiaries' management have the power and responsibility to incorporate the specific characteristics of their own operations into the company specific policies, limits, authorizations and guidelines.

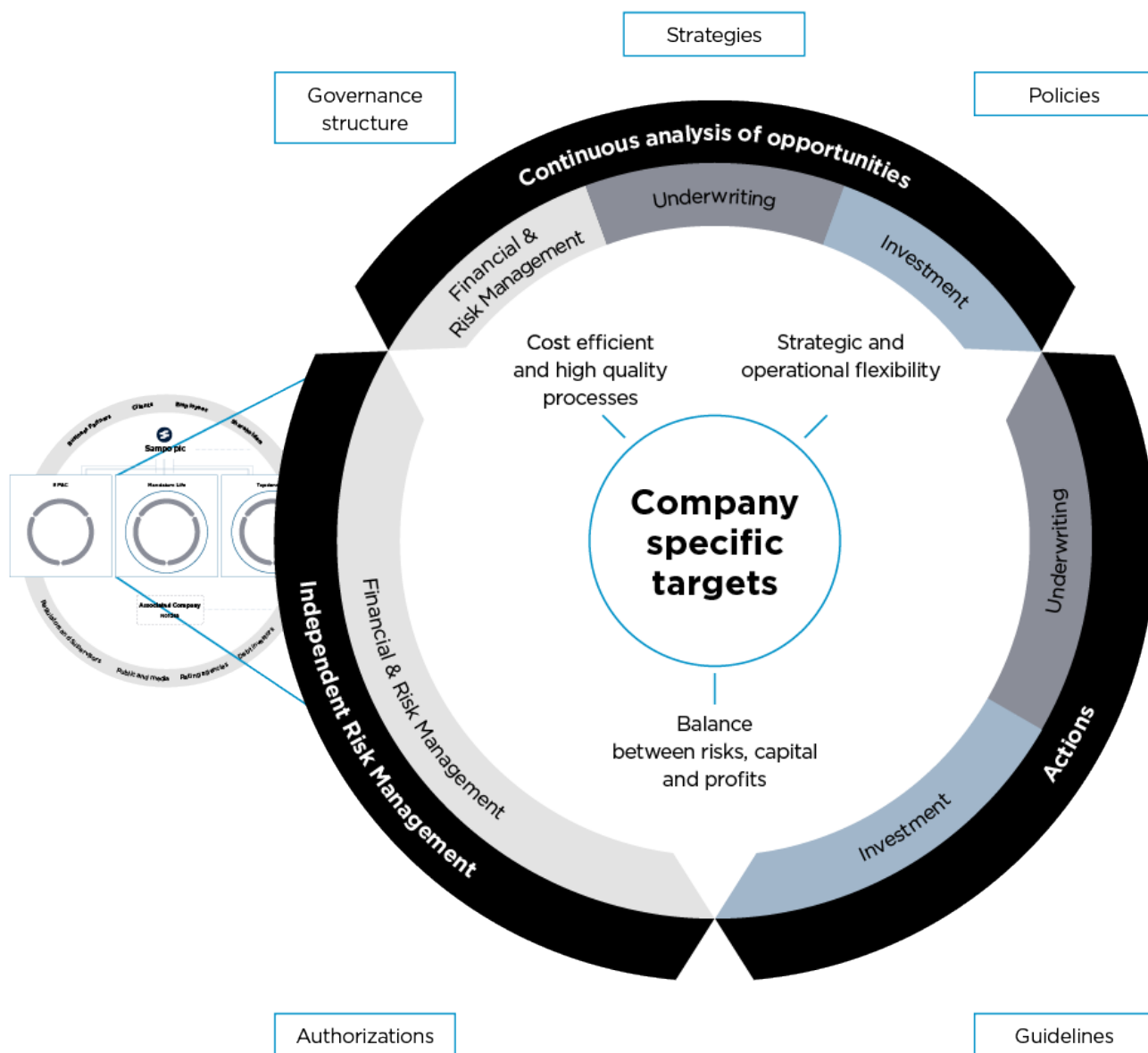
At the operative level, the subsidiaries focus on the effective execution of insurance operations and financial and risk management activities. Investments are managed according to the Investment Policies which are approved by the Boards of Directors of the respective subsidiaries. The parent company leads day-to-day management of investments; facilitates simultaneous effective execution of the subsidiaries' investment policies; and maintains group-wide oversight of the investment portfolios.

The risk management process consists of continuous activities that are partly the responsibility of the personnel involved in business activities and partly the responsibility of independent risk management specialists. Although the responsibilities of business lines and independent risk management are clearly segregated in Sampo Group, these functions are in continuous dialogue with each other. In Internal Control Policy Sampo Group has defined the roles and responsibilities of different internal stakeholders.

Parties independent of business activities are responsible for the risk management governance framework, risk policies, risk limits and authorizations which form the structure that sets the limits for business and investment units' risk taking as well as principles for risk monitoring. These structures are one prerequisite for the risk management process; they reflect capital adequacy targets and the risk appetite in general.

The figure Company Level Financial and Risk Management Process illustrates the (i) prerequisites, (ii) tasks together with the responsible functions and (iii) targets of company level risk management.

### Company Level Financial and Risk Management Process



The central prerequisites for facilitating successful risk management include the following:

- Risk management governance structure and authorizations (see [Risk Governance section](#)) and clear division of responsibilities between business lines and independent functions
- Companies’ own risk policies and more detailed instructions related to risk management
- Prudent valuation, risk measurement and reporting procedures.

The tasks included in the risk management process can be classified as follows:

### Independent Risk Management

Financial and risk management functions are explicitly responsible for preparing the above prerequisites of risk management. Operationally they are responsible for independent measurement and control, including the monitoring of operations in general as well as profitability, risk and capitalization calculations. The following items are examples of these responsibilities:

- Detailed reporting on risks to subsidiaries’ and Sampo’s Risk Committees and the Boards of Directors
- Internal reporting on Capital need and actual available Capital at least on a quarterly basis
- Internal reporting on regulatory and rating agency capital charges and capital positions on a quarterly basis

- Disclosure of internal and regulatory capitalization figures quarterly.

## Continuous Analysis of Opportunities and Risks

Both the business lines and the financial and risk management functions are active in supporting the business with continuous analysis and assessment of opportunities. This can be seen as a separate phase in the risk management process as the insurance and investment business units assess different business opportunities, especially their risk return ratios, on a daily basis. In the financial and risk management functions, on the other hand, a considerable amount of time is spent on risk assessment and capital planning.

This assessment of opportunities generates, for example, the following outputs:

- Identification of business opportunities (e.g. product and service development and investment opportunities) and analysis of respective earnings potential and capital consumption
- Intra-group and external dividend plans
- Hybrid and senior debt issuance initiatives.

## Actions

Actions, i.e. transactions representing the actual insurance and investment operations are performed in accordance with the given authorizations, risk policies and other instructions. These actions are the responsibility of business and centralized functions such as the investment unit. Activities related to capitalization and liquidity positions are included in this part of the process. In Sampo Group, proactive actions to manage profitability, risks and capital are seen as the most important phase of the risk and capital management process. Hence, risk policies, limits and decision making authorizations, together with profitability targets, are set up in a way that they facilitate business and investment units to take carefully considered risks. Examples of the actions are as follows:

- Pricing of insurance policies and execution of investment asset transactions
- Dividend payments, share buy-backs, hybrid issuances and senior debt issuances
- Derivative and reinsurance transactions
- Business acquisitions and divestments.

High quality execution of the above tasks contributes to the achievement of the three central targets of the risk management process:

## Balance Between Risks, Capital and Earnings

- The risks affecting profitability as well as other material risks are identified, assessed and analyzed.
- Capitalization is adequate in terms of risks inherent in business activities and strategic risks, taking into account the expected profitability of the businesses.
- Risk bearing capacity is allocated to different business areas in accordance with the strategy.
- Underwriting risks are priced to reflect their inherent risk levels, expected returns from investment activities are in balance with their risks, and consequential risks are mitigated sufficiently.

## Cost Efficient and High Quality Processes

- Client service processes and internal operative processes are cost efficient and of high quality.
- Decision making is based on accurate, adequate and timely information.
- Continuity of operations is ensured and in the case of a discontinuity event, recovery is fast and comprehensive.

## Strategic and Operational Flexibility

- External risk drivers and potential strategic risks are identified and the company is in a good position, in terms of capital structure and management skills, to react to changes in the business environment.
- Corporate structure, knowledge and processes in the companies facilitate effective implementation of changes.

When the above targets are met, risk management contributes positively to return on equity and mitigates the yearly fluctuations in profitability. The risk management process is therefore considered to be one of the contributors in creating value for the shareholders of Sampo.

## Parent Company's Oversight and Activities

Sampo reviews Group as a business portfolio and is active especially in matters related to Group's capitalization and risks as well as related to the parent company's capital structure and liquidity.

Sampo reviews quarterly the performance of Sampo Group both on a company level and on a Group level based on the reporting provided by the subsidiaries and the associated company. The information on associated company is, however, based on publicly available material and is therefore less detailed. Reporting on the subsidiaries' performance to the Board of Directors and Audit Committee ("AC") of Sampo is based mainly on the reporting produced by the subsidiaries. The reporting concentrates on the balance

between risks, capitalization and profitability. The parent company is responsible for reporting on its own activities. Reporting from wholly-owned subsidiaries is more detailed than reporting from Topdanmark.

At group level, the central focus areas are potential concentrations arising from Group companies’ operations as well as Group’s capitalization and the parent company’s ability to generate liquidity. The parent company is also projecting and analyzing Group companies’ profitability, risks and capitalization with uniform scenarios to have company specific forecasts that are additive at group level.

Based on the above sub-group level work and Sampo Group level internal work Sampo Group prepares annually or more often if needed a Single Own Risk and Solvency Assessment document (“Single ORSA report”). The Single ORSA report has virtually the same structure and contents as quarterly Audit Committee reporting. The only substance difference is the addition of Group-wide solvency forecasts, which are not normally part of the quarterly reporting.

Based on both the company and group level information, the Board of Directors of Sampo decides on Group’s capitalization as well as sets the guidelines on the parent company’s capital structure and liquidity reserve. The underlying objective for Sampo is to maintain a prudent capital structure and adequate liquidity in order to be able to

arrange financing for strategic projects if needed. Strong liquidity and the ability to acquire financing are essential factors in maintaining Sampo Group’s strategic flexibility.

## Risk Governance

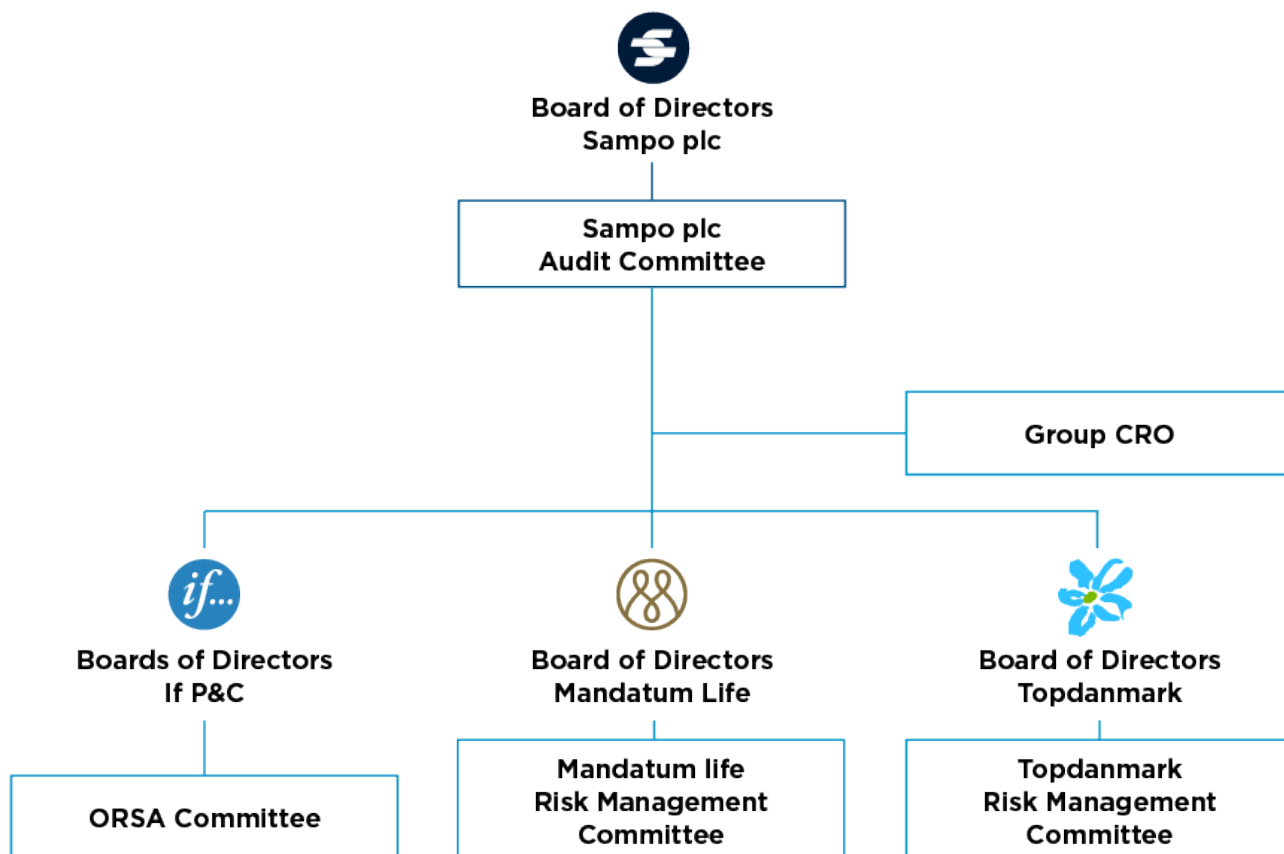
This section describes the governance framework of Sampo Group and its subsidiaries from a risk management perspective. A more detailed description of Sampo Group’s corporate governance and internal control system is included in the [Corporate Governance section](#).

### Risk Governance at Group Level

The Board of Directors of Sampo is responsible for ensuring that Group’s risks are properly managed and controlled. The Board of Directors of Sampo defines financial and capitalization targets for the subsidiaries and approves group level principles which steer the subsidiaries’ activities. The risk exposures and capitalization reports of the subsidiaries are consolidated at group level on a quarterly basis and reported to the Board and to the Audit Committee of Sampo.

The reporting lines of different governing bodies at group level are described in the figure Risk Governance in Sampo Group.

### Risk Governance in Sampo Group



The Audit Committee is responsible, on behalf of the Board of Directors, for the preparation of Sampo Group’s risk management principles and other related guidelines. The AC shall ensure that the operations are in compliance with these guidelines, control Sampo Group’s risks and risk concentrations as well as control the quality and scope of risk management in the Group companies. The committee shall also monitor the implementation of risk policies, capitalization and the development of risks and profit. At least three members of the AC must be elected from members of the Board who do not hold management positions in Sampo Group and are independent of the company. The AC meets on a quarterly basis.

The Group Chief Risk Officer (“CRO”) is responsible for the appropriateness of risk management at Group level. The CRO’s responsibility is to monitor Sampo Group’s aggregated risk exposure as a whole and coordinate and monitor company specific and group level risk management.

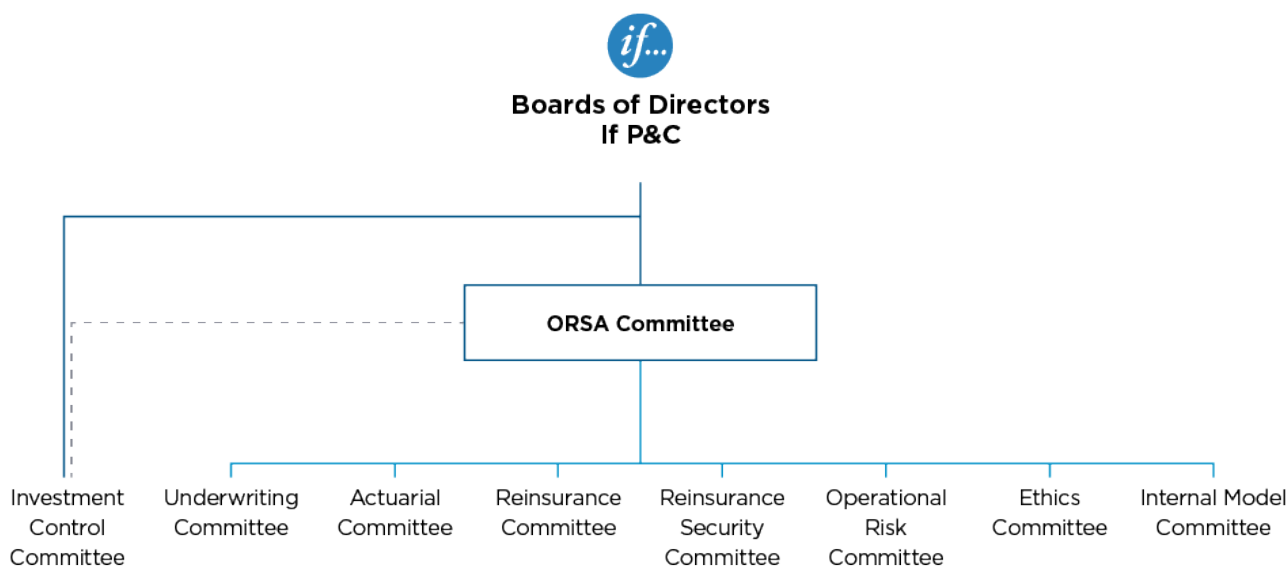
The Boards of Directors of If P&C and Mandatum Life are the ultimate decision making bodies of the respective companies

and have the overall responsibility for the risk management process in If P&C and Mandatum Life respectively. The Boards of Directors appoint the If P&C ORSA Committee and the Mandatum Life Risk Management Committee, and are responsible for identifying any need to change the policies, principles and instructions related to risk management.

### Risk Governance in If P&C

The main risk steering mechanism used by the Boards of Directors is the policy framework. As part of their responsibilities, the Boards of Directors approve the Risk Management Policy and the other risk steering documents; receive risk reports from the Chief Risk Officer and the Chief Executive Officers (“CEOs”); take an active part in the forward looking risk and solvency assessment process; and ensure that the management and follow-up of risks is satisfactory and effective. The reporting lines of different governing bodies in If P&C are described in the figure Risk Governance in If P&C.

### Risk Governance in If P&C



The Own Risk and Solvency Assessment Committee assists the Chief Executive Officers of If P&C in fulfilling their responsibilities to oversee the risk management process. The ORSAC reviews reporting from If P&C’s other committees within the Risk Management System as well as reporting from both corporate functions and the line organization. Furthermore, the ORSAC monitors If P&C’s short-term and long-term aggregated risk profile to ensure it is aligned with its risk strategy and capital adequacy requirements. The Risk Management function is responsible for coordinating the risk management activities on behalf of the Boards of Directors and the CEOs.

The responsibility to identify, evaluate, control and manage risks lies within the line organization. There are separate committees in place for key risk areas which have the responsibility of monitoring the management and control risks to ensure compliance with the instructions of the Boards of Directors. The risk committees in If P&C do not have a decision mandate.

There are policies in place for each risk area which specify restrictions and limits chosen to reflect and ensure that the risk level is constantly in compliance with the overall risk appetite and capital adequacy constraints of If P&C. The



committees also monitor the effectiveness of policies and give input to changes and updates if needed.

In addition to the risk specific committees, there are two other committees included in the Risk Governance structure. Their responsibilities are described as follows:

- The Ethics Committee (“EC”) discusses and coordinates ethical issues in If P&C. The committee gives recommendations on ethical issues and proposes changes to the Ethics Policy. The Chairman is responsible for the reporting of ethics risk and other issues dealt with by the committee.
- The Internal Model Committee’s tasks are to identify sources for potential model changes and to give its opinion to the Chairman on the assessment and classification of potential changes and on further validation activities or internal model development. In addition to the tasks above, the committee discusses and analyzes information related to the internal model from other committees as well as monitors the status of internal model use and development activities.

If P&C has also a Compliance Committee (CC), which is an advisory body for the Chief Compliance Officer regarding compliance issues. The task of the committee is to secure a

comprehensive view of compliance risk and activities in If P&C.

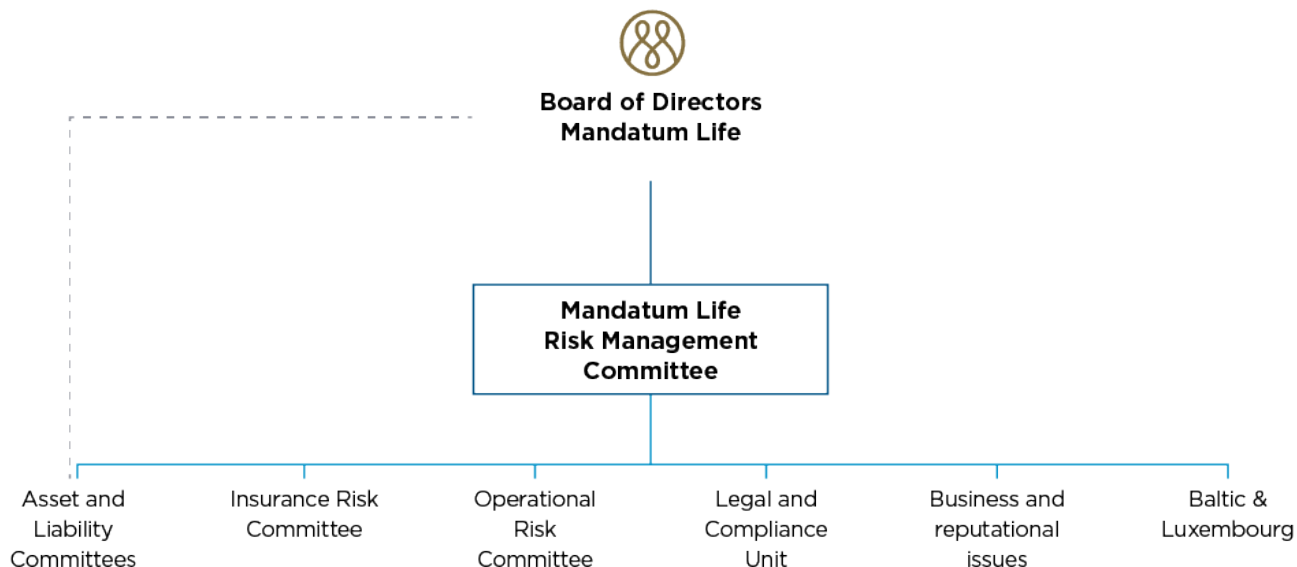
### Risk Governance in Mandatum Life

In Mandatum Life the Board of Directors is responsible for risk management and the adequacy of internal control. The Board of Directors annually approves the Risk Management Plan, Investment Policy and other risk management and internal control instructions.

The Managing Director of Mandatum Life has the overall responsibility for risk management according to the Board of Directors’ instructions. The Managing Director is the Chairman of the Risk Management Committee which coordinates and monitors all risks in Mandatum Life. The risks are divided into groups, the main groups being insurance, market, operational, legal and compliance risks as well as business and reputation risks. Each risk area has its own specialized committee or unit and a responsible person in the RMC.

The reporting lines of the main governing bodies in Mandatum Life are described in the figure Risk Governance in Mandatum Life.

### Risk Governance in Mandatum Life



In addition to the risk specific committees, the duties related to compliance and risk management of the Baltic branches have been organized as follows:

- The Legal and Compliance Unit takes care of compliance matters with the Head of the Unit being a member of the Risk Management Committee.

- The Baltic branches has its own risk management procedures. All major incidents are also reported to Mandatum Life’s Risk Management Committee.
- Internal Audit, through its audit recommendations, has a role to ensure that adequate internal controls are in place and provides Internal Audit’s annual review to the Board of Directors.

## Risk Governance in Topdanmark

Topdanmark's policy is to hedge against risks arising from the Company's activities or to limit such risks to a level that allows the Company to maintain normal operations and implement its planned measures even in the case of highly unfavourable events in the outside world. As a consequence of this policy, for a number of years, the Company has identified and reduced or eliminated the risks which could potentially cause losses exceeding what Topdanmark considers to be acceptable. The Board of Directors determines the overall risk policies and limits. The internal auditors report to the Board of Directors and report on, among other things, the observance of these risk policies and limits.

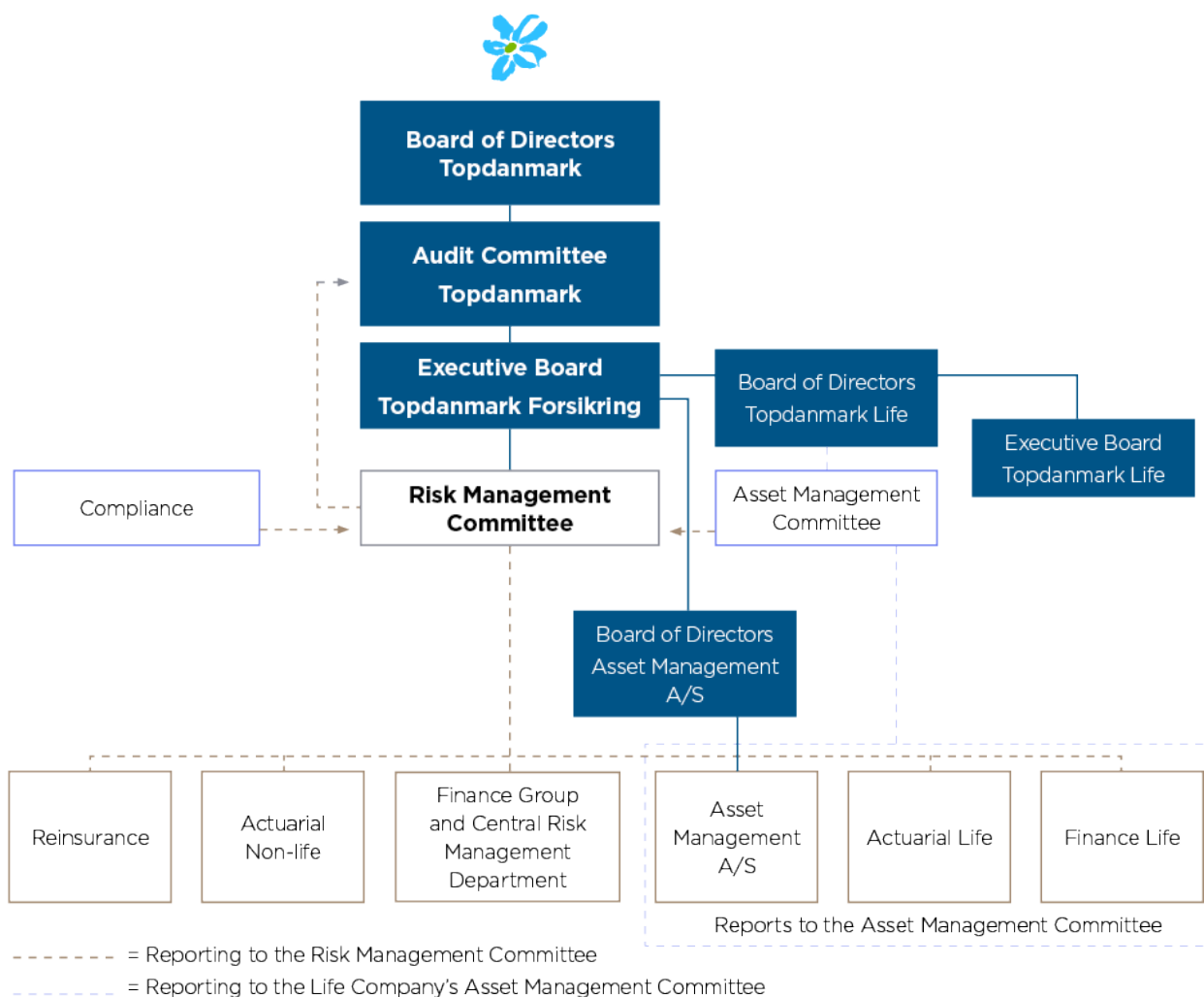
Topdanmark's risk management function identifies, assesses and quantifies risks. It reports to the Risk Committee, which is responsible for risk policies, risk limits, solvency calculation, capital plans, Topdanmark's own risk and solvency assessment (ORSA), and Topdanmark's partial,

internal model for non-life insurance risks. The members of the Risk Committee are the CFO of the Group, the head of the Compliance Function and the heads of the primary risk areas, which are: Asset Management, Statistical Services, Reinsurance, Finance, Life Actuarial Services and Life Finance. The Risk Committee reports and recommends to the Board of Directors via the Executive Board.

The Risk committee has set up the Model Committee, which is responsible for developing and operating Topdanmark's internal model for calculation of results probabilities and risks of the non-life insurance portfolio based on random simulation. The model is used for, among other things, optimising the reinsurance programme, calculation of cost of capital, forecast balancing and calculating capital requirements.

The reporting lines of the main governing bodies in Topdanmark are described in the figure Risk Governance in Topdanmark.

### Risk Governance in Topdanmark





The risk management function implements an annual ORSA process identifying risks in the business, quantifying these risks and collecting them in a risk register. Additionally, the principles of solvency calculation are reviewed, and the risk

management process is updated. An ORSA report has been prepared, which, together with the risk register and risk management process, was considered at a Board seminar in the autumn of 2017.

