Risk Management Framework Operating Guideline - Enterprise

APPROVAL	
Approved By:	Kathryn Fric, SVP Enterprise & Operational Risk
Date approved by Policy Approval Committee:	May 25, 2021
Next scheduled review and Approval by Policy Approval Committee	May 2022
Effective Date of Latest Amendments	May 25, 2021
Sponsor:	Kathryn Fric, SVP Enterprise & Operational Risk
Responsible Person/Contact:	Janey Leung, VP Enterprise & Corporate Risk Management

Table of Contents

1.0 Purpose and Application

1.1. Purpose

The purpose of this Risk Management Framework - Enterprise Operating Guideline ("RM EOG") is to provide guidance for the implementation of the prescriptive requirements as codified in the Risk Management Framework (RMF).

1.2. Application

This Operating Guideline must be read with the RMF. The RMF and RM EOG apply uniformly to the Company, Business Groups (BG), Business Units (BU), and Subsidiaries. The applicability of the Risk Management Policies to the Corporate Functions and BGs will be defined within the respective policies.

The RMF and RM EOG are intended to apply directly to entities over which Sun Life has control. Joint Ventures under Sun Life management control are expected to adopt the RMF and the Risk Management Policies or have comparable policies and/or procedures in place, as applicable.

For the entities where Sun Life does not have management control, we seek to influence management through representation on the boards of directors and committees. Our risk appetite with respect to these entities is reflected in the Risk Appetite Policy.

We are guided by Sun Life's Data Privacy Principles where Client data is utilized in operationalizing the requirements set out in the RMF and RM EOG.

2.0 Risk Management Framework

2.1 Risk Governance and Accountabilities

Primary accountability for risk management is delegated by the Board of Directors to our CEO. The CEO further delegates responsibilities throughout the Company through management authorities and responsibilities.

Risk Management Governance Structure and Accountabilities

Board of Directors

The Board of Directors is responsible for ensuring the governance of all risks across the enterprise and has primary responsibility for taking action to ensure Risk Management Policies, programs and practices are in place. By approving our RMF and Risk Appetite Policy (including the Risk Management Policies listed in Appendix A) and providing risk governance, the Board of Directors monitors that key risks are appropriately identified and managed. The Board of Directors oversees business and strategic risk through review and approval of the Business and Strategic Plans and regularly discusses key themes, issues and risks arising in connection with the design or implementation of these plans. The Board of Directors also monitors risk management activities of our subsidiaries and risk posed to the Company through its joint venture arrangements.

Senior Management and Oversight Functions

The Three Lines of Defence (LOD) model has been adopted and is applied uniformly across all Risk Management Policies. Each policy individually outlines the roles and responsibilities for each line of defence as applicable. The principles used in the Three LOD framework as well as the high-level responsibilities associated with each line of defence are described in the RMF.

Each Business Group (BG) has a designated Business Group Chief Risk Officer (BG CRO) who along with other second LOD oversight functions, provides independent risk challenge and oversight for their BG. The BG CRO may place reliance on other second LOD oversight functions and is not expected to replicate such assessments. In Asia, this oversight may be at the BU level, with BG CRO still retaining accountability under the RMF.

At a BG level, there are BG Risk Committees (BGRC) where the first LOD is independently challenged by the second LOD risk oversight function, and that focus on matters particular to a BG. The standard BGRC mandate establishes the minimum requirements that need to be included in the respective BGRC mandate. The standard BGRC mandate is reviewed annually by the Enterprise Risk Management ("ERM) team. The standard BGRC mandate is circulated to the BG CROs who then align their respective committee mandates, as appropriate. The standard BGRC mandate can be found in Appendix D of the RMF.

At an Enterprise level, there are various Board Committees and Senior Management Committees, which are described in detail in the RMF.

2.2 Risk Universe

The Risk Universe provides a structured and consistent means for grouping and reporting on key risk across all BGs. Our risk universe comprises of six major categories – Business and Strategic, Credit, Market, Liquidity, Insurance and Operational.

It is important to not only identify the risks and their components, but also the potential interconnections that can exist between and among various risk categories. Refer to Appendix A of the RMF for the risk sub-categories and the alignment with the Risk Management Policies.

2.3 Risk Appetite

The Risk Appetite Policy is one of the key mechanisms used to operationalize our risk philosophy. The Risk Appetite Policy contains the Risk Capacity, Risk Appetite Statement and Risk Limits, as well as outlines the roles and responsibilities of those overseeing its implementation. Our Risk Appetite Statement defines the type and aggregate level of risk that we are willing to accept. Further details on Risk Appetite have been included in the Risk Appetite Policy as well as individual Risk Management Policies where applicable.

Risk Philosophy and Principles

The RMF describes the core principles that are included in our risk philosophy. These include strategic alignment, stakeholders' interests, capability alignment, portfolio perspective, risk adjusted returns and culture.

Our corporate strategy and business objectives are required to be established within the boundaries and prescriptions set out in the RMF and the Risk Appetite Policy. This requires us to consider whether a business activity intended to achieve the business and financial objectives will result in a residual risk profile that we are willing to accept and which we are prepared to manage. As part of the planning process, the key residual risks to the Business Plan (Plan) will be identified and discussed. The Plan is tested for alignment with the risk constraints codified in the Risk Appetite Policy. We review our strategy to confirm that it operates within the risk parameters through the:

- Enterprise Key Risk Process - Key Risks to the Plan focusing on residual risks
- Risk Appetite Policy - Testing to ensure that Plan operates within the Risk Appetite limits

Oversight of the inherent risks is provided through the risk management procedures and controls codified as part of the Risk Management Policies. The risk management process in the policies reflect the core processes we use to identify, measure, manage, monitor and report (IMMMR) risks. These risks are reported to the Board/Board Committees in various reports including the standard reports listed in Appendix C of the RMF.

Further detail on the linkage of the risks and planning process has been provided in various Risk Management Policies and operating guidelines including, but not limited to, the Risk Appetite Policy, the Capital Risk Policy and the Key and Emerging Risk Process Manual.

2.4 Risk Management Policies

In order to support the effective communication, implementation and governance of the RMF, we have codified our processes and operational requirements in the Risk Management Policies and operating guidelines. These policies and guidelines promote the application of a consistent approach to managing risk exposures across our global business platform and may include regulatory requirements, as appropriate. Each policy and accompanying operating guidelines, where applicable, describes our risk exposures comprising our risk universe and outlines how the risk is managed. Risk Management Policies have been outlined in Appendix B of the RMF.

The Policy on Policy Governance (PPG) provides for the development, approval and management of frameworks, policies and operating guidelines. Its key objectives are to support governance and control of Frameworks, Policies and Operating Guidelines, with respect to consistency, ease of access, timely and orderly management of new and required amendment and periodic review and evaluation. Refer to the PPG for more details.

2.4.1 Compliance with Regulatory Requirements

When developing policies and operating guidelines, the alignment with legal and regulatory requirements needs to be considered as codified in the Compliance Risk Management Framework and associated guidelines. To the extent of any inconsistency between a policy or operating guideline and a law (including a regulatory requirement), the law shall prevail. As part of the review and approval of policies, Policy Sponsors/Contacts must attest that the policies have been updated to reflect the impact of regulations, as appropriate.

2.4.2 Review and Approval of Policies

The Board of Directors is ultimately responsible for ensuring the governance of all risks across the enterprise and has primary responsibility for taking action to ensure Risk Management Policies, programs and practices are in place.

Policy Sponsors must review the Risk Management Policies at least annually and update as necessary to reflect the impact of new and amended regulations, changes in the business environment, risk profile, or internal operations or enhanced governance. Policy Sponsors must socialize any changes to policies to their first LOD and second LOD stakeholders as codified in the respective policies and adhere to the Policy on Policy Governance requirements.

The Risk Committee of the Board of Directors will review Risk Management Policies at least once every three years or when there are significant changes to the Policy. In certain cases, the Board of Directors may require a review of the policies, as provided by the Charters of the Board of Directors. ERM supports this process under the mandate of the Policy Review Group (PRG) which is a sub-committee of the Policy Approval Committee (PAC).

More frequent review of the Risk Management Policies may be required by the PAC as described in the Policy on Policy Governance. All Risk Management Policies and significant amendments thereto are reviewed by the PAC prior to being presented to the Board/Risk Committees' Agenda for approval.

Please refer to **Appendix B – Risk Management Policies Approval Matrix.**

Operating Guidelines

Operating Guidelines support the ongoing communication, implementation and administration of Risk Management Policies. The Operating Guideline's content should include guidance to implement the requirements codified in the policy. Operating Guidelines and significant changes thereto are reviewed by the PAC.

Enterprise Operating Guidelines (EOG)

It is recommended that all Risk Management Policies have an EOG, which codifies enterprise-wide processes, measures, metrics and controls to implement the requirements. Clear accountability should be defined in the respective EOG following the principles of the Three LOD. The Policy Sponsor/Contact will maintain the EOG. It is expected that for all policies where there are significant revisions that the EOG will be formally updated to reflect these revisions and issued within three months following the policy's effective date. Any exceptions to the three-month timeline will be reported to the RMF Policy Sponsor.

Local/ Business Group Operating Guidelines (OG)

An Operating Guideline will be either an EOG or a Local/Business Group OG, as determined by the Sponsor after consultation with other Senior Management if needed. In rare instances, a Local/Business Group OG may be required in addition to an EOG where there are specific local operating and regulatory requirements, which need to be included in a Local/Business Group OG. Local/Business Group OG are intended to detail the Local/ Business Group specific procedures that support the implementation of Risk Management Policies. Local/Business Group OGs are not mandated for policies and the Policy Sponsor/ Contact should determine where they are necessary. Significant changes to the Local/ Business Group OG must be approved by the Policy Sponsor in addition to approval by the local PAC.

2.4.3 Risk Policy Compliance

Three Lines of Defence

The Three LOD model provides a consistent, transparent and clearly documented allocation of accountabilities and segregation of responsibilities with respect to compliance to the Risk Management Policies.

First Line of Defence

The first LOD is responsible for understanding its risks and requirements under the applicable policies. For all Risk Management Policies, the first LOD should report any non-compliances to the BGRO and respective Risk Policy Sponsors through the ERM reporting tool. Please refer to **Appendix C – Risk Policy Applicability by BG and Corporate Functional Areas (CFA)**.

Attestations of compliance to the Risk Management Policies is first LOD's confirmation of compliance to the Company's Risk Management policies and programs. On a quarterly basis, the BGs will present the policy compliance monitoring report at the BGRC meetings.

First LOD Attestation of Compliance (at year-end)

The first LOD attestation confirms that the BG Leader is aware of the:

- Policies (or sections of the policies) that apply to the BG;
- First LOD programs that support the BG to be in compliance;
- Results of the programs, including whether there have been material non-compliances; and
- Mitigating actions to address the non-compliances.

Second Line of Defence

BG CRO and BGRO Teams

The roles of the BG CRO's in policy oversight have been codified in the respective Risk Management Policies.

In general, the BG CROs and/or their BGRO teams:

- Provide oversight on first LOD risk policy requirements and review non-compliances reported by the first LOD, including suitability of action plans and target dates.
- Provide independent challenge and perform applicable second LOD roles and responsibilities as defined in the Risk Management Policies. Liaise with other second LOD functions, as appropriate, to obtain a view of policy non-compliances on a quarterly basis.

- Ensure materiality assessment of non-compliances along with the rationale for materiality are appropriate and documented and reported to the respective Risk Policy Sponsors through the ERM reporting tool.

BG CRO Certification of Review & Challenge (year-end)
The BG CROs will review the year-end attestation of compliance from the BG Heads. Based on input from the first LOD, the BG CRO will aggregate this information to ensure that the list of non-compliances is complete and may get inputs or updates from the Policy Sponsor/Contact, as appropriate. The accountability to retain evidence of all closed reported non-compliances is with the first LOD. The Policy Contact and/or BG CRO (or delegate) will review the closed reported non-compliances and challenge as appropriate.

Policy Sponsors
The Board seeks assurances from Policy Sponsors (Senior Management) that the Risk Management Policies and controls are operating effectively across the enterprise and that Sun Life is in material compliance to these Risk Management Policies. ERM works in collaboration with the Policy Sponsors and Contacts to ensure that risk practices are aligned with the RMF and tools are provided for governance and oversight of risks.

To the extent that Policy Sponsors identify or are aware of a policy non-compliance (through their review and challenge), the Policy Sponsors/Contacts should inform the first LOD and/or BGRO as applicable.

Policy Sponsors or Contacts work with the BG CRO/ BGROs, where appropriate in performing review and challenge of non-compliances to the Risk Management Policies in line with the quarterly policy compliance monitoring and year-end attestation process. The Policy Contact and/or BG CRO (or delegate) will review the closed reported non-compliances and challenge as appropriate.

Second LOD Opinion of Compliance (year-end)
Policy Sponsors provide a statement of opinion on the compliance with and effectiveness of the Company's Risk Management Policies and programs, with supporting content for the opinion, e.g. non-compliances noted in the year and assessment of materiality of non-compliances.

Key Compliance Indicators
Key Compliance Indicators (KCIs) are used to set and align compliance expectations between first LOD and second LOD stakeholders. Policy Sponsors have defined KCIs that summarize the key requirements of the Risk Management Policies in their Technical Memo. The policies should ultimately be the basis of determining any non-compliances.

KCIs allow for a risk-based assessment of policy non-compliances based on residual risks, where the absence of controls prescribed in the policies could result to either material or non-material risk exposures.

Processes to monitor KCIs may differ between Risk Management Policies and may include critical inquiry, rejection of status quo, validation or verification. Policy Sponsors have established oversight structures that engage the first LOD throughout the year and allow each BG to fully demonstrate ownership and report on their state of compliance.

See Appendix A for the Key Compliance Indicators for the RMF.

Risk Management Policies - Technical Memo

The Risk Management Policy Technical Memo outlines the process that Policy Sponsors will use to support their opinion of compliance and effectiveness of the Company's Risk Management Policies and programs. Each year, the Policy Sponsors/Contacts will update the

Risk Management Policy Technical Memo, which prescribes the policy compliance oversight and controls in place.

The KCIs are the key elements of the Risk Management Policy Technical Memo. The Risk Management Policy Technical Memo provides more details on how materiality is assessed based on residual risks for each KCI.

Chief Risk Officer ("CRO)
Annually, the CRO provides a Report on Compliance with Consolidated Risk Management Policies to the Board of Directors and/or Risk Committee.

Quarterly, ERM aggregates all non-compliances and provides an enterprise-wide view of compliance to the Risk Management Policies to the Policy Approval Committee. Materiality of non-compliances is assessed based on aggregation and consultation with the Policy Sponsors.

3.0 Risk Management Process

3.1 Risk Identification

We use a consistent approach across BGs in our risk identification. We use a range of techniques and sources of information to identify current, emerging and potential risks, which includes historical data, external data and reports, forward-looking analysis and models and expert judgment. The techniques employed depend on the type of risk involved.

Each risk should be considered from the perspective of different types of uncertainties. Uncertainty can exist around expected financial results (mis-estimation risk), and from volatility, trend and extreme events of the key risks. In addition, risk correlation, interconnected risks, term of exposure and the risk horizon are important elements to consider while identifying risks.

We also have a process to identify and monitor emerging risks that may have a material impact on our finances, operations or reputation. We evaluate potential correlations between various risk events and categories, and monitor emerging risks, regulatory and rating agency requirements, and industry developments.

The risk identification process has been codified within the RMF, the Enterprise Key and Emerging Risk Process Manual and Risk Management Policies and Operating Guidelines. The Enterprise Key Risk Process reports on the key risks that Sun Life could be potentially exposed to across the Strategic and Business plan horizons.

Enterprise Key and Emerging Risk Process

The Enterprise Key Risk Process in conjunction with the RMF sets out how BGs identify, measure, manage, monitor and report on key and emerging risks impacting or likely to impact the achievement of the Business Plan over a one-year time horizon. The impact may be financial or nonfinancial, including impact on reputation. Given the wide spectrum of risks, the focus of the Enterprise Key Risk Process is on key risks and not all risks.

The Enterprise Key and Emerging Risk Process is an integral component of the RMF and has been embedded into all levels of the organization. The underlying principle of the Enterprise Key and Emerging Risk Process is that it is both "bottom-up" and "top-down" and emphasizes review and challenge by multiple stakeholders to ensure completeness of the key risks identified. In conjunction with the Risk Appetite Policy methodology, the Enterprise Key and Emerging Risk Process assesses and highlights the underlying residual risk profile and trends, which are then reported as part of the Planning process to the Board or the Risk Committee and updated quarterly.

The Enterprise Key and Emerging Risk Process is codified in a separate document – "Enterprise Key and Emerging Risk Process Manual".

3.2 Risk Measurement

Risk measurement involves determining and evaluating potential risk exposures and includes a number of techniques such as monitoring key risk indicators, probability and severity assessments, stress testing (including sensitivity and scenario analysis), reverse stress testing and stochastic modelling. Risk measures are expressed in quantitative and qualitative terms. The specific risk measurements techniques have been included, as applicable, in Risk Management Policies and EOGs

3.3 Risk Management, Monitoring and Reporting

As appropriate, and included in the respective Risk Management Policies, risk management decisions are formed by evaluating how well the outcomes of the risk measurements and risk assessments for a business activity conform to our risk appetite, including an assessment of risk adjusted return.

While many risks may be relevant to the organization, management prioritizes the key risks as a basis for selecting responses to risks. Risk management may take the form of one of the following risk responses: avoid, mitigate, transfer, and/or accept.

Primary responsibility of monitoring and reporting risks lies with the BGs and BUs. Monitoring of compliance to the Risk Management Policies is codified within the individual policies and may include formal BG attestation, independent deep dives, and regular dashboard and reports at the Business Group Risk Committee meetings and PAC meetings.

Monitoring processes include governance by the Board of Directors, which is exercised through Committees of the Board of Directors and supported by Senior Management Committees. At least on a quarterly basis, the Senior Management Committees, Committees of the Board of Directors and the Board of Directors review reports that summarize the firm's risk profile against the Board approved risk appetite, including the exposures across our principal risks, any changes in risk trends, forward-looking view of risks and emerging risks. These committees also review the effectiveness of the mitigation strategies presented in the reports.

The specific risk monitoring and reporting requirements have been included in the respective Risk Management Policies.

Types of Reporting

Each Risk Management policy codifies specific reporting processes applicable to that particular risk. In addition, regular reporting is enhanced through utilization of a number of standard key enterprise reports. This ensures that risks are monitored on a regular, ongoing basis by the appropriate committees and individuals. Refer to Appendix C of the RMF, which outlines examples of Standard Risk Reports.

Each report owner is responsible to ensure that the distribution lists for reports stay up to date and that reports are being distributed to all appropriate stakeholders. Key principles for risk reporting are codified in the Risk Data Aggregation & Risk Reporting Operating Guideline.

- Sun Life's risk data aggregation and risk reporting capabilities meet our requirements given the nature of risks we face, the speed at which risk can change and the nature of decisions made based upon risk data. Capabilities should consider reporting requirements both during normal operations and during a period of financial duress or crisis.
- Sun Life's controls over risk data aggregation and risk reporting are designed and operating in a manner to provide reasonable assurance regarding the reliability, completeness and accuracy of key risk reports.

The specific set of key risk reports where the Risk Data Aggregation & Risk Reporting Operating Guideline applies is determined on an annual basis by the Risk Category Owner.

We complement our standard management reports with periodic "Deep Dive" reports or special briefings to the Board of Directors, Committees of the Board of Directors and Senior Management Committees to ensure key risk issues are well communicated.

4.0 Three Lines of Defence and Effective Challenge

The Three LOD model principles, responsibilities and risk activities are outlined in the RMF. This Operating Guideline supports the implementation of effective challenge.

The second LOD has the responsibility to provide independent challenge to the first LOD to efficiently and appropriately oversee the respective risks. Effective Challenge is achieved through the processes and activities undertaken by the second LOD teams to assess the reasonableness and effectiveness of the first LOD's management of risks. Effective Challenge supports the integrity of risk data and facilitates ongoing monitoring of key control activities and changes in the risk profile. The characteristics and concepts around effective challenge outlined below should be read in conjunction with the Three LOD principles codified in the RMF.

Characteristics of effective challenge may include some or all of the following:

- **Critical Inquiry** – Analyzing and questioning decisions, actions/in-actions, to arrive at effective and value-added outcomes
- **Rejecting the Status Quo** – applying a different perspective; testing the 'unproven', exploring opportunities for advancement/improvement; and challenging the norm to avoid complacency
- **Validation –** applying specific technical expertise and professional skill(s), to challenge underlying assumptions, methodologies, processes and conclusions to ensure they are effective, appropriate, and performing as intended
- **Verification –** testing and confirming that internal controls, processes, and systems are performing effectively and as intended

4.1 Second Line of Defence Attributes

The following attributes are used to operationalize second LOD challenge:

1) The first LOD may conduct first LOD quality assurance and provide the results to the BG or BU (Business Unit) Head and to support their recommendations.

2) Reviews carried out by the first LOD are not independent and cannot alone be used to satisfy the second LOD independent challenge required by the Board of Directors and other stakeholders.

3) Challenges by the second LOD should be appropriate for the risk, objective, critical and professional.

4) Challenges by the second LOD will not necessarily be directed towards the elimination of residual risk but rather seek to ensure business decisions and related risks are within risk appetite.

5) The second LOD provides the interpretation of Risk Management Policies as part of its supporting role to the Board of Directors/Risk Committee, while the first LOD demonstrates compliance to the Risk Management Policies.

6) The second LOD can provide advice to the first LOD in the manufacture or design of a risk position, however, the second LOD can never assume responsibilities of the first LOD as the primary agent in the manufacture, or creation and management of a risk.

7) The second LOD has full and complete right of access to information that is required to oversee the risk

8) The second LOD has the right and a duty to review, challenge and escalate risks if they are of the view that the risk considerations of a particular business recommendation or action are not

appropriately captured or conveyed to Senior Management and the Board of Directors/Risk Committee by the first LOD.

9) Challenge should be documented and demonstrable.

10) The severity and likelihood of risks should drive the extent of challenge and evidence captured.

11) One second LOD risk function can place reliance on the work done within another second LOD function and not replicate the same challenge.

4.2 Approach for Implementing Effective Challenge

The following approach is recommended for implementing effective challenge

A. Prepare:

- Gather required knowledge of the relevant business operations through both internal and external research and develop a thorough understanding of the risks by exploring the facts, assumptions and biases

- Review the risks and related assessments conducted by the business in advance of the working sessions and explore potential issues

B. Challenge

- Seek explanations and rationalizations provided on strategic business and risk decisions, and question the assumptions and exceptions

- Produce facts to challenge business and risk decisions - a fact-based challenge assists with the socialization and finalization of assessments in a professional manner

C. Evidence

- Document the challenge provided during the working session and the outcome of the challenge using the evidence mechanisms outlined in the next section.

- Establish a process to maintain the evidence of Effective Challenge. This evidence should be available on request.

4.3 Capturing and Demonstrating Evidence of Challenge

The primary objectives of Effective Challenge should be kept in mind when conducting the challenge – few high-quality challenges that significantly improve risk decisions are better than a large number of ineffective challenges. Challenge can be demonstrated based on transactional evidence or non-transactional evidence:

- **Transactional evidence** includes Committee memo / Reports, minutes of the meeting and emails

- **Non-transactional evidence** includes changes in outcome (demonstrable changes in outcomes and results, as a result of Effective Challenge), ongoing engagement (demonstrable involvement in projects, meetings and committees) and Risk Culture (demonstration of risk integration within business, change in culture and/or use of risk techniques in business artifacts).

Verbal challenge is the most common form of challenge. It continues to be necessary and is encouraged in day-to-day activities. Verbal challenge can be evidenced where it is captured in writing such as emails, minutes or formal reports.

One of the ways we capture “challenge” by the second LOD is through risk reports presented at the appropriate committee, which create a formal interface between the first and second LOD using a systematic and structured approach.

One of the attributes of "challenge" required to operationalize the challenge in the three LOD is the requirement that it is documented and demonstrable. Some of the effective ways to capture evidence of challenge are described in the table below.

Source of evidence of Transactional Challenge	Comments
Committee Memo / Reports	Challenge documented in the reports/memos submitted to a Committee is considered the best practice. This documentation may include recommendations as well as alternatives or choices, as appropriate, which may be for the Committee's review or approval. It should also include the identification of issues raised by various functions operating in the second LOD and responses to those issues. In some cases, the challenge may be documented in the form of a memo from second LOD with their independent opinion and summary of review that is tabled along with the first LOD proposal
Minutes of the Meeting	Minutes are the official record of a meeting. They are one of the most common and important tools to demonstrate review and challenge that took place at the meeting. Challenge taking place at a meeting should generally be recorded and maintained.
Email	Email is a commonly used form of challenge. It usually manifests itself through a set of questions from second LOD to the first LOD. Historical e-mails are often difficult to find, particularly after changes in roles or departures from the company, however where the emails can be retrieved and evidenced, they are accepted as a formal evidence of challenge.

5.0 Risk Culture

Our risk culture is supported by a strong tone from the top, which emanates from the Board of Directors and cascades through the Committees of the Board of Directors, our CEO (Chief Executive Officer) and executive officers, management and staff. A key premise of our risk management culture is that all employees have an important role to play in managing the Company's risks.

There are six elements that support our Risk Culture: tone from the top, transparency (what risk is being taken, for what objective and benefit, how the risk will be managed, and who is accountable), effective challenge, incentives, effective communication and accountability.

Risk management is embedded in the enterprise's culture, which encourages ownership and responsibility for risk management at all levels, aligned with business goals and compensation. We continuously reinforce and embed the culture through:

- Communication and training on the risk culture elements at various forums and across various levels.
- All directors and employees are required to complete training on the Code of Conduct annually and to complete the Annual Code of Conduct Declaration confirming compliance over the last year.
- Clearly defining roles, responsibilities and expectations in the Risk Management Policies.
- Reinforcing accountability through performance reviews and compensation.
- Continually assessing and monitoring processes.

One of the ways our risk culture is embedded in the organization is through alignment of compensation and risk management.

Compensation Alignment
Our compensation programs are aligned to the organization's risk management practices through our governance structure for the approval of incentive compensation plans. In establishing annual performance objectives, we consider risk management goals to ensure that business decisions are consistent with the desired risk and return profile of the Company. A Risk and Control measure is included in the Annual Incentive Plan (AIP) that provides management with a direct lever to recommend adjustments within the AIP to the Management Resources Committee (MRC) on any issues identified. The MRC /Board have the discretion to lower or eliminate the AIP awards if they conclude results were achieved by taking risks outside of Board approved risk appetite levels.

A group of senior executives from Finance, Actuarial, Risk Management, Legal/Compliance, Human Resources and Internal Audit comprise our Incentive Plan Review Group (IPRG) and participate in the compensation decision-making process. Annually, at a minimum, the Chief Risk Officer (CRO) will present a report to the MRC of the Board of Directors on whether enterprise risks are being managed appropriately and recommend whether, in their opinion, amendments to compensation may be required. The various parameters used to support the assessment include, but are not limited to:

- Enterprise Risk Appetite Policy and risk reporting results, including any changes in trends,
- Enterprise and Business Group key and emerging risk process and related management actions
- Assessment of Compliance with Consolidated Risk Management Policies
- The Strategic and Business Plan Risk Profile
- Other Enterprise key risk reports

These parameters are codified in various Board and Board Committee reports including the Risk Appetite Report and the Enterprise Key Risk Report. The CRO will also form their opinion based on the discussions undertaken at the Business Group Risk Committee meetings and in consultation with other oversight functions.

6.0 Annual Review and Compliance Reports

Annual Review
The RMF and RMF EOG must be reviewed annually by the Sponsor to determine whether revisions are required to respond to legal (including regulatory) developments, reflect changes in the business environment, internal operations or enhanced governance practices. ERM will also evaluate how the RMF aligns with industry standards or best practices.

On an annual basis, the Sponsor of the RMF will seek approval from the PAC and the ERC that the RMF be submitted to the Risk Committee for review and recommendation to the Board for approval.

Compliance Reports
The Sponsor must report annually to the PAC, ERC and to the Risk Committee on the status of compliance with the effectiveness of the RMF.

7.0 Glossary

Board of Directors means the Board of Directors of each of Sun Life Financial Inc. and Sun Life Assurance Company of Canada.

Business Group means a business segment by which the Corporation manages its operations and reports its financial results, namely, Canada, U.S., Asia, Asset Management and Corporate. Corporate includes the Corporate Functional Areas, U.K. and Digital, Business and Technology Solutions.

Business Unit means a BU within a BG. For example, Group Benefits is a Business Unit within the Canadian Business Group or MFS and Sun Life Capital Management are Business Units within the Asset Management Business Group. "Business Unit" may include a Subsidiary and shall not include a corporation that is not a Subsidiary.

Board Committees means the Audit Committee, the Governance, Investment and Conduct Review Committee, the Management Resources Committee, or the Risk Committee of the Board of Directors.

Corporation/ Company/ Organization means each of Sun Life Financial Inc. and Sun Life Assurance Company of Canada. Reference to the terms "Sun Life", "we", "our", and "us" within this document refers to each of Sun Life Financial Inc. and Sun Life Assurance Company of Canada.

Enterprise means the Corporation, BGs, BUs, and Subsidiaries,

Enterprise Operating Guideline means an Operating Guideline that is uniformly applicable across the Enterprise

Enterprise Policy means a Policy that is uniformly applicable across the Enterprise.

Executive Risk Committee means the Executive Risk Committee for Sun Life. See RMF Appendix D for the ERC Mandate.

Framework means an enterprise-wide framework that is subject to review and approval by the Board of Directors or a Committee of the Board of Directors. Framework is further defined in section 2.1.1 of the Policy on Policy Governance.

Joint Venture means a corporation or other entity in which the company has a substantial interest. A joint venture is considered to be under management control where Sun Life has supervision over and authority to direct the day-to-day business and operations of the joint venture in the ordinary course of business. The following joint ventures are under management control as of the date of this policy approval: Sun Life Malaysia Assurance Berhad, Sun Life Malaysia Takaful Berhad and Sun Life Grepa Financial Inc.

Operating Guideline will contain detail needed at the operating level to implement the principles, standards and requirements established in a Policy. Operating Guideline – is further defined in section 2.1.3 of the Policy on Policy Governance.

Operational Risk and Compliance Committee (ORCC) means the Operational Risk and Compliance Committee for Sun Life. See RMF Appendix D for the ORCC Mandate.

Oversight Functions are functions led by the Chief Risk Officer, Chief Compliance Officer, Chief Legal Officer Actuary and Chief Auditor. The function led by the Chief Financial Officer also includes some control and oversight responsibilities.

Policy establishes principles, standards and requirements with respect to the subject matter addressed in the Policy. It only contains provisions requiring mandatory compliance. Policy is further defined in section

2.1.2 of the Policy on Policy Governance. It also includes a Standing Investment Authorization approved by the Board of Directors.

Policy Contact means the individual who aids the Policy Sponsor in executing the requirements within the Policy

Policy Sponsor means the owner of the Policy on behalf of the Corporation.

Policy Approval Committee (PAC) means, regarding the Corporation, the Operational Risk and Compliance Committee acting in its policy approval committee role. This role has been delegated to the Operational Risk and Compliance Committee by the Executive Risk Committee.

Policy Review Group (PRG) means a sub-committee of the Policy Approval Committee.

Senior Management means the relevant Senior Management of the Corporation, Business Group, Business Unit, or Subsidiary. It includes the Sponsor. It may or may not include a member of the Policy Approval Committee or Local Policy Approval Committee.

Subsidiary means a corporation whereby more than 50 per cent of each of the total voting power and total value of the shares (other than non-voting preferred shares) are owned, directly or indirectly, by the Corporation and/or a Subsidiary or Subsidiaries. Thus, where a Joint Venture does not meet the said "more than 50%" test, it is not a Subsidiary. For the purposes of the RMF and this operating guideline, "Subsidiary" excludes Sun Life Assurance Company of Canada.

8.0 References

8.1 Policies

- Policy on Policy Governance
- Risk Management Framework
- Risk Appetite Policy

8.2 Operating Guidelines

- Risk Appetite Operating Guideline - Enterprise
- Stress Testing Guideline - Enterprise

8.3 Other

- Key Risk Process Manual
- Risk Data Aggregation and Risk Reporting (RDARR) Operating Guideline

Items listed above are for guidance only and are not necessarily exhaustive.

9.0 Appendices

Appendix A: Key Compliance Indicators
Appendix B: Risk Management Policies Approval Matrix
Appendix C: Risk Policy Applicability by BG and CFA
Appendix D: Modification History

APPENDIX A – KEY COMPLIANCE INDICATORS

This section summarizes the Key Compliance Indicators for the RMF. Examples of material non-compliances are provided and are not exhaustive. Policy Sponsor approves the materiality assessment associated with a policy non-compliance.

KCI Descriptions	Evidence of Compliance	Materiality Guidance
Risk Management Policies		
KCI-1 PRG maintains a Risk Policy and Enterprise Operating Guideline (EOG) review schedule to ensure risk policies and EOGs are reviewed on a timely basis. Risk Management Policies align to the Risk Management Framework. • Risk Universe align with the RMF • Risk IMMMR is embedded within the Risk Management Policies • Three Lines of Defence is included • Annual Review & Compliance is included	PRG Meeting Materials: • Forward Agenda • Minutes • Policy Review and Approval Summary	Material if Risk Management Policies are not updated and submitted to the Risk Committee of the Board/Board in the timeframe required (per Risk Committee/ Board schedule) Material if there is no IMMMR process established for the Risk Management Policies
Policy Non-Compliance monitoring and reporting		
KCI-2a Policy non-compliances are logged in the ERM policy non-compliance reporting tool on a quarterly basis. Policy non-compliances including action plans, assessments of materiality and target dates for closure are reviewed by the BG Risk Office and Corporate Policy contact. Policy non-compliances are aggregated, analyzed for trends, and reported quarterly by RMF policy contact and/or delegate to PAC (ORCC)	ERM reporting tool evidences BGRO and Policy contact reviews. Quarterly Risk Policy Non-Compliance Monitoring Report to PAC (ORCC)	Material if Policy Sponsor does not have a process to identify, assess, monitor and report policy non-compliances
KCI-2b First LOD BG Heads and Corporate Functional Area (CFA) Heads will provide at year-end the First LOD Attestation of Compliance to Risk Management Policies.	Year-end Attestation Process for Risk Management Policies. Attestations reviewed by respective Policy Sponsors/contacts.	Material if attestations on the status of compliance to applicable Risk Management Policies is not received, reviewed, and reported annually to the Risk Committee'
KCI-2c BG CROs will provide at year-end a BG CRO Certification of Review and Challenge after a review of the year-end attestation of compliance to Risk Management Policies from the BG Heads. For Corporate Functions, the BG CRO will review the attestations from the CFA Heads.	Year-end Attestation Process for Risk Management Policies. Attestations reviewed by respective Policy Sponsors/contacts	
KCI-2d Policy Sponsors will provide at year-end the Second LOD Opinion of Compliance. The Policy Sponsors will use the Technical Memo, including Key Compliance Indicators (KCI) to support their opinion of policy compliance and attestation	Year-end Attestation Process for Risk Management Policies. Attestations reviewed by RMF policy contact and/or delegate to support CRO attestation.	

KCI-2e RMF policy contact reports Compliance with the Consolidated Risk Management Policies to the PAC (ORCC) on a quarterly basis	Risk Policy Non-Compliance Monitoring Report (Quarterly) and Annual Report on Compliance with Consolidated Risk Management Policies	
KCI-2f The Chief Risk Officer/delegate reports the status of compliance to applicable Sun Life Risk Management Policies to the Executive Risk Committee and Risk Committee.	Report on Compliance with Consolidated Risk Management Policies	
Risk Management Process		
KCI-3 Business Group Risk Committee (BG RC): There is oversight of the risk profile, risk appetite, risk management strategies and implementation of those strategies.	BG RC Mandate and minutes of meetings	Material if there is no oversight (by both first and second line) of the BG's risk profile, risk appetite, risk management strategies and implementation of those strategies.
KCI-4 Key Risk Identification: Key Risk heat maps from Business Groups are consolidated and reviewed by ERM. An Enterprise key risk heat map is reported to the ERC and Risk Committee on a quarterly basis	BG key risk heat map and emerging risks Enterprise key risk heat map in Quarterly Emerging and Top Risk report.	Material if key risks are not reported to the Board/Board Committees at least quarterly
KCI-5 Stress Testing: Financial Risk Management maintains the Stress Testing Enterprise Operating Guideline which outlines Sun Life's stress testing framework, processes including various stress testing activities and controls.	Risk Policy attestations and following reports as presented to ERC: • Quarterly Risk Appetite Limits Monitoring Report • Quarterly Stress Testing Analysis • Quarterly Asset Liability Management Risk Report • Annual FCT Report	
KCI-6 Risk Data Aggregation and Risk Reporting (RDARR): Enterprise & Corporate Risk Management maintains the RDARR EOG and performs annual compliance validation and testing. On an annual basis, the independent test program to be completed by Enterprise & Corporate Risk Management is presented to the ORCC	Risk Policy attestation (for applicable Risk Management Policies) and RDARR report to ORCC.	Material if annual (RDARR) compliance validation and testing is not completed.

APPENDIX B – RISK MANAGEMENT POLICIES APPROVAL MATRIX

Enterprise Risk Management Policies	PRG/PAC/RC[1]		ERC[2]		Full Board[3]
1. Risk Management Framework	√		√		√
2. Risk Appetite Policy	√		√		√
3. Capital & Liquidity Management Framework	√		√		√
4. Capital Risk Policy	√		√		√
5. Asset Liability Management Policy*	√				
6. Business Continuity Management Policy	√				
7. Information Management Risk Policy	√				
8. Information Technology Risk Policy	√				
9. Insurance Risk Policy*	√				
10. Investment & Credit Risk Management Policy*	√				
11. Mergers and Acquisitions Policy	√		√		
12. Model and End User Computing Management Policy	√				
13. Operational Risk Management Framework	√				
14. Product Design & Pricing Policy*	√				
15. Security Risk Policy	√				
16. Third Party Risk Management Policy	√				

Note:

All Risk Management Policies are reviewed by PRG, PAC and the Risk Committee.

- PRG is a sub-committee of the PAC established to provide adequate time for detailed policy-related discussions that normally would have taken place during PAC meetings. PRG is responsible for in-depth review of the policy and escalation/endorsement to PAC. PRG review does not replace the review and approval provided by the applicable Senior Management Committee.
- PAC reviews and endorses the Policy Sponsor's recommendations for Board/Board Committee review and approval of p Policies.
- ERC has delegated its PAC role to ORCC but maintains a review of select policies as per the ERC Mandate.
- The Risk Committee is the Committee of the Board responsible for reviewing and approving all Risk Management Policies (except those listed to be approved by the Board of Directors)
- The Board of Directors oversees and approves select policies as specified in the Charters of the Board of Directors.

*These policies go to a Senior Management Committee for approval before they go to PAC.

APPENDIX C – RISK POLICY APPLICABILITY BY BG AND CFA

1st Line Head	BG CRO/ BGRO	*Risk Policy & Policy Sponsor, Contact/ Business Group, Corporate Functions and other entities in scope*	Asset Liability Risk Management Policy	Business Continuity Management Policy	Capital & Liquidity Management Framework	Capital Risk Policy	Information Management Risk Policy	Information Technology Risk Policy	Insurance Risk Policy	Investment and Credit Risk Management Policy	Mergers and Acquisitions Policy	Model and End User Computing Management Policy	Operational Risk Management Framework	Product Design and Pricing Policy	Risk Appetite Policy	Risk Management Framework	Security Risk Policy	Third Party Risk Management Policy
			Kathryn Fric	Kathryn Fric	Leigh Chalmers	Leigh Chalmers	Kathryn Fric	Kathryn Fric	Kathleen Alfano	Patrick Romain	Linda Dougherty	Paul Fryer	Kathryn Fric	Kevin Morrissey	Kathryn Fric	Kathryn Fric	Mark Saunders/ Kathryn Fric	Kathryn Fric
			Cory Wiebe	Dimitri Alexander	Anne Hancock	Anne Hancock	Abbas Syed	Abbas Syed	*Underwriting:* Lianne Heppenstrijdt *Medical:* Dr. Aurora Hollo *Claims :* Antonio Ferrante *Reinsurance :* Romy Silva	Ali Mozaffari	Raymond Duong	Dave Wylie	Nathalie Maillet	Valerio Valenti	Paul Fryer	Janey Leung	Abhay Raman/ Abbas Syed	Nathalie Maillet
Leo Grepin	Lucy CL Chou/ David Iee	**Sun Life Asia**		✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
Jacques Goulet	Mike Schofield/ John Delangen	**Sun Life Canada**		✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
Katherine Garner	Nicholas Shanahan	**Sun Life UK**		✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
Dan Fishbein	Julie O'Neill	**Sun Life US**		✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
Steve Peacher	Patrick Romain/ Ali Mozaffari	**SLC Management**		✓	✓	✓	✓	✓		✓	✓	✓	✓		✓	✓	✓	✓
Laura Money	Maureen Shewchuk/ Nathalie Maillet	**Digital, Business & Technology Solutions (DBTS)**		✓			✓	✓				✓	✓			✓	✓	✓
		MFS		✓	✓	✓	✓	✓			✓	✓	✓		✓	✓	✓	✓
		JV - SLGFI (Philippines)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
		JV - SL Malaysia	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Kathryn Fric	Janey Leung/ Merly Agellon	**Corporate Risk Management**	✓	✓			✓	✓	✓	✓		✓	✓		✓	✓	✓	✓
Brennan Kennedy		**Global ALM (Cdn, US, UK & Asia)**	✓	✓			✓	✓				✓	✓			✓	✓	✓
tbd		**Run Off Reinsurance (US)**		✓			✓	✓	✓			✓	✓			✓	✓	✓
Leigh Chalmers		**Corporate Capital and Treasury & Investor Relations**		✓			✓	✓				✓	✓			✓	✓	✓
Kevin Morrissey		**Corporate Actuarial**		✓			✓	✓				✓	✓	✓		✓	✓	✓
Linda Dougherty		**Corporate Strategy & Global Marketing**		✓			✓	✓			✓	✓	✓			✓	✓	✓
Kevin Morrissey		**Malta and Other Foreign Governances**		✓			✓	✓				✓	✓			✓	✓	✓
Rebecca Vass/ Natalie Brady		**Corporate Finance**		✓			✓	✓				✓	✓			✓	✓	✓
Samiha Sachedina		**Corporate Audit**		✓			✓	✓				✓	✓			✓	✓	✓
Helena Pagano		**Corporate Communications**		✓			✓	✓				✓	✓			✓	✓	✓
Helena Pagano		**Corporate Human Resources**		✓			✓	✓				✓	✓			✓	✓	✓
Kent Savage		**Corporate Compliance**		✓			✓	✓				✓	✓			✓	✓	✓
tbd		**Corporate Legal**		✓			✓	✓				✓	✓			✓	✓	✓
Troy Krushel		**Corporate Secretary**		✓			✓	✓				✓	✓			✓	✓	✓
Remi Benoit		**Corporate Taxation**		✓			✓	✓				✓	✓			✓	✓	✓

APPENDIX D: MODIFICATION HISTORY

Amended May 2021

- Updated Glossary to be consistent with the approved RMF
- Key Compliance Indicators added in the Appendix
- Best Practices for Review of Policies removed from Appendix and added to ERM – PRG SharePoint
- Notes added under Risk Management Policies Approval Matrix to clarify the roles of the various groups/committees

Amended November 2020

- Added Sun Life's Data Privacy Principles in the Application section
- Expanded Section 2.1 on Risk Governance to include accountabilities for Sun Life's Board of Directors and Senior Management and Oversight Functions.
- Updated Section 2.2. Risk Universe to align with the RMF and added the interconnections of risks
- Expanded Section 2.4.3 Risk Policy Compliance to include expectations on policy non-compliance reporting for Risk Management Policies
- Updated Section 3.0 Risk Management Process to align with the RMF
- Updated Section 5.0 Risk Culture to align with the RMF
- Updated Section 6.0 Annual Review and Compliance for consistency with the RMF language.
- Added the definition of Framework in the Glossary, consistent with the change to the Policy on Policy Governance.
- Updated PRG Mandate (posted separately from EOG)
- Updated Appendix – Risk Management Policies Approval Matrix to include the ERC approval on RMF, Risk Appetite Policy, Capital & Liquidity Management Framework, Capital Risk Policy and Mergers & Acquisitions Policy; also indicated policies that go to respective Senior Management Committee for approval.
- Updated Appendix – Best Practices for Review of Policies to include a step on Board/Board Committee Review after the Annual Review.
- Updated Appendix - Risk Policy Applicability:
    - First LOD: added JVs and MFS and split Enterprise Services into Information Technology and Enterprise Services
    - Second LOD: RMF and Capital Risk Policy are applicable to all BGs, JVs and MFS.

Amended November 2019

- Expanded the Risk Policy Compliance section to describe the Attestation Process and the application of the Three Lines of Defence model. This will eliminate the separate documentation issued yearly on Risk Policy Compliance Guidance.
- Added sections on Key Compliance Indicators (KCIs) & Technical Memo to reflect current practices
- Added Appendices for: Policy Review Group (PRG) Mandate, Risk Policies Approval Matrix, Best Practices for Review of Policies and Risk Policy Applicability Matrix.
- Aligned the structure of the EOG to the approved 2019 RMF. The EOG is meant to be read together with the RMF.
- Added language on EOG and BGOG to clarify intent of both documents.

Amended: June 2017

- Provide clarification on inherent and residual risk assessment.
- Provide clarification on review of risk policies and Board/Management committee review process
- Additional details provided on effective challenge including training material
- Updated the risk definitions of the taxonomy.

Amended: May 2016

- Moving key elements from the RMF to create a new EOG, which includes the following items:
    - Operationalizing Policy review and Policy Compliance processes to make roles and responsibilities clearer
    - Sections on strategic alignment, compensation and risk alignment have been further elaborated to clarify the current process around these practices.
    - Guidance on effective challenge have been provided on how to conduct and document challenge and the role of the three lines of defence.
    - Policy review and approval requirements and underlying process which was codified in the RMF has been brought forward as part of the RMF EOG.