

MANAGING RISK AT SUNCORP

Managing risk is a key contributor to Suncorp's success.

The Board and management recognise that an effective system of risk management plays a critical role in the setting and achievement of Company objectives. Suncorp has systems, structures, policies, processes and people in place to identify, measure, evaluate, monitor, report and control or mitigate all internal and external sources of material risk.

Effective risk management at Suncorp is driven by:

- a risk management framework where the business takes accountability for risk management and owns its risk decisions
- an independent risk management function that advises and challenges the business in its risk taking
- monitoring of Suncorp's risk maturity and targeted actions to continually lift risk management capability
- inclusion of risk management outcomes in the assessment of performance
- a robust 'risk appetite' that sets out the nature and degree of risk the Board is willing to accept in pursuit of Suncorp's business objectives.

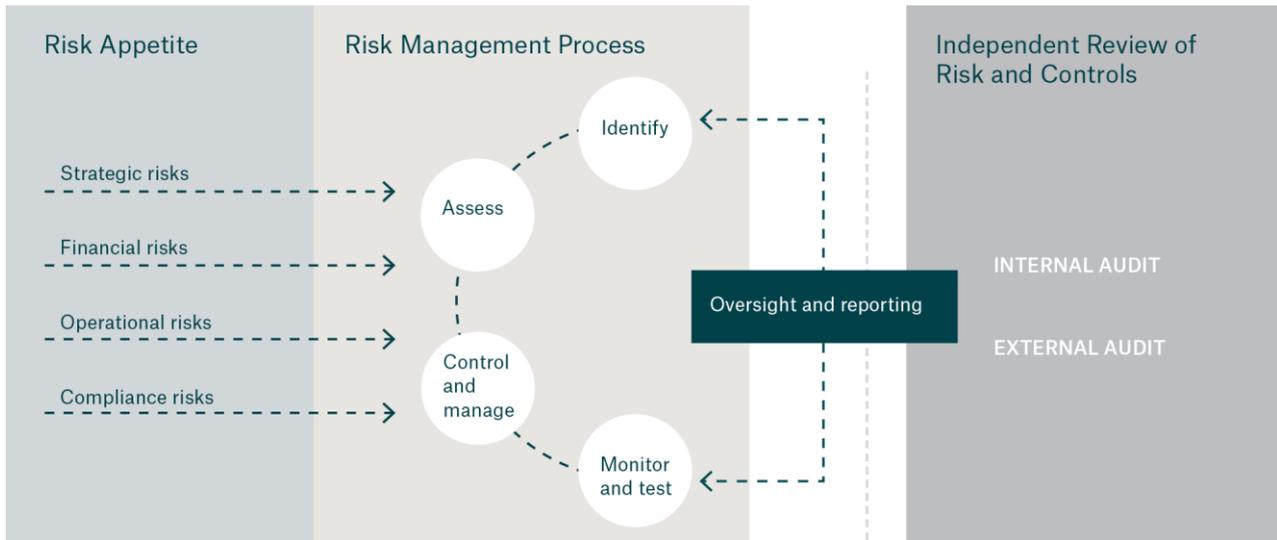
1. Suncorp enterprise risk management framework

Suncorp operates within an Enterprise Risk Management framework (**ERMF**) which lays the foundation for all risk management and demonstrates Suncorp's commitment to effective risk management as a key element of business success. The ERMF will continue to evolve in support of Suncorp's strategy and operating environment. The framework:

- links risk appetite to strategic business and capital plans
- supports a risk-aware culture
- sets out accountabilities and governance arrangements for the management of risk within the Three Lines of Defence model
- establishes processes to identify and manage risk on an ongoing basis
- enhances business risk-based decision-making.

The ERMF was reviewed in 2016-17 to satisfy the Board that it continues to be sound. Internal Audit independently tests and verifies the efficacy of risk standards and compliance, validates the overall risk framework, and provides assurance that it is functioning as designed. Internal Audit provides written reports to both the Audit and the Risk Committees. The Risk Committee conducts an annual review and endorses the framework for Board approval.

The ERMF is summarised in the following diagram.



Suncorp’s organisational design shapes how risk is managed and is based on three principles:

- Individuals are responsible for their actions and decisions.
- Structures and processes are simplified, to make it easier to manage risks.
- Each Function has functional accountability for all aspects of the business, including those risks managed by service providers.

1.1 Three Lines of Defence Model

Risk at Suncorp is assumed within a controlled framework that assigns clear lines of responsibility for risk. A Three Lines of Defence Model of risk management accountability is in place with the clear expectation that all business areas, as the first line of defence, are responsible for the management of their risks.



The Risk Function forms the Second Line of Defence and supports the business in its risk-taking through advice, monitoring and effective challenge. Internal and External Audit are the Third Line of Defence.

2. Risk management processes

Suncorp aims to conduct its business in compliance with all relevant laws, rules, regulations, industry standards and codes, internal policies and procedures, and having regard to accepted community and ethical standards. It also acts promptly to correct incidents of non-compliance no matter how identified, including determining whether a compliance failure is a breach that is reportable to a regulator.

As part of the ERMF, internal controls have been implemented across Suncorp to ensure appropriate risk identification, measurement, management, monitoring and reporting. These controls support the proactive management of risk, including the regular maintenance of risk profiles which provide the Board and management with clear oversight of risk.

Managers complete a periodic due diligence attestation to confirm the status of compliance within their area of responsibility. The compliance status, including actual and potential breaches, is captured in a Suncorp-wide incident and risk system to ensure necessary stakeholders are aware of material matters affecting business operations.

In accordance with APRA's Prudential Standards, regulated entities must submit a risk management declaration to APRA, signed by the Board annually, confirming the adequacy of the regulated entity's risk management systems. The risk management declarations are based on reports considered and reviews conducted by the Risk Committee during the year and on the representations management provides to the Board and CEO & Managing Director with regard to the adequacy of Suncorp's risk management systems.

Policies and procedures have been developed to ensure open communications with regulators occur in a timely manner including the referral of any material correspondence between Suncorp and regulators to the Board or relevant Board committee.

3. Risk appetite is defined at both Suncorp and entity levels

Risk appetite is the nature and level of risk that the Board is willing to accept in the pursuit of strategic objectives. There is a dynamic relationship between business planning, Risk Appetite Statements (**RAS**) and capital management in achieving Suncorp's strategic objectives. Risk appetite is articulated at both a Suncorp and entity level, and forms part of strategic business plans.

Risk appetite is strategic, forward-looking, and intended to be easy to communicate and understood by all stakeholders. Risk appetite informs policy, limits and delegation frameworks. Monitoring of Suncorp's position against the RAS is conducted regularly by the first line of defence with oversight by the second line of defence and reported by the Chief Risk Officer (**CRO**) to the Risk Committee every quarter. Escalation protocols are in place within the applicable policies and frameworks that detail the steps to be taken, should a risk target range or tolerance be exceeded.

4. Risk categorisation and policy-setting

The risks Suncorp manages include strategic, counterparty, credit, market, asset and liability, liquidity, insurance, operational, and compliance risks.

Board and management-approved policies, delegations, authorities and limits are influenced by Suncorp's risk appetite. Policies, procedures, limits and other controls are in place for the Suncorp-wide, legal entity or functional level to manage these risks and align to the Board's risk appetite, as depicted in the following table.

Description	Key Policies, Controls And Limits
<p>STRATEGIC RISKS</p> <p>Strategic risk is the most fundamental of business risks. At its most basic, it is the risk associated with Suncorp's operating model and how it wants to position itself strategically. Strategic risk threatens the viability of the operating model and our strategic position and emerges from external changes and the execution of Suncorp's strategy.</p>	<ul style="list-style-type: none"> – Strategic and Business Planning – Internal Capital Adequacy Assessment Processes (ICAAPs) – Risk Appetite Statements (RAS) – Enterprise Risk Management (ERM) – Mergers and Acquisitions (M&A)
<p>FINANCIAL RISKS</p> <p>Counterparty risk – the risk to each party to a contract that the counterparty will not meet its financial obligations in accordance with agreed terms.</p> <p>Market risk – the risk of unfavourable changes in foreign exchange rates, interest rates, equity prices, credit spreads, commodity prices, and market volatilities.</p> <p>Asset and Liability risk – the risk to earnings and capital from mismatches between assets and liabilities with varying maturity and repricing profiles and from mismatches in term.</p> <p>Liquidity risk – the risk that Suncorp will be unable to service its cash flow obligations today or in the future.</p> <p>Insurance risk – the risk of financial loss and the inability to meet liabilities due to inadequate or inappropriate insurance product design, pricing, underwriting, concentration risk, reserving, claims management or reinsurance management.</p>	<p>Policies</p> <ul style="list-style-type: none"> – Bank Credit Risk Management – Credit and Counterparty Risk Management – Intra-Group Transactions and Exposures – Investment Governance – Foreign Exchange Risk Management – Bank Traded Market Risk – Interest Rate Risk in the Banking Book (IRRBB) – Bank Securitisation and Covered Bonds – Liquidity Management – Life Product Pricing and Reinsurance Advice – Bank Funds Transfer Pricing – Derivatives Management – Unit Pricing
<p>OPERATIONAL RISKS</p> <p>The risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This includes legal risk, but excludes strategic and reputational risks.</p>	<ul style="list-style-type: none"> – Business Continuity – Delegations of Authority – Financial Crimes – Group Security – IT Acceptable Use – Procurement – Product Approval – Human Resources – Model Integrity – Code of Conduct
<p>COMPLIANCE RISKS</p> <p>The risk of legal or regulatory sanctions, financial loss, or loss to reputation which Suncorp may suffer as a result of its failure to comply with all applicable regulations, codes of conduct and good practice standards.</p>	<ul style="list-style-type: none"> – Code of Conduct – Compliance Management and Regulator Engagement – Conflicts of Interest – Disclosure – Fit and Proper – Privacy Management – Anti-Money Laundering, Counter-Terrorism Financing (AML CTF) and Sanctions – Securities Trading – Whistleblower

5. Strategic risk management

Management of strategic risks is the most fundamental business risk and is integral in the development of strategy and the decision-making process for all business initiatives. Strategic risk threatens the viability of the operating model and Suncorp's strategic position, and emerges from changes in the external environment such as the political landscape, regulation, technology and the actions of competitors that could impact a Function or Suncorp's performance.

Key threats to achievement of strategy are assessed by Functions and overseen by the CEO & Managing Director, Chief Financial Officer and CRO through performance management processes, including formalised quarterly review meetings.

The Board oversees:

- strategic and emerging risks through regular reporting to the Risk Committee
- monthly rotational 'function in focus' reports
- regular 'deep dive' reports overseen by the Risk Committee.

As part of their three-year business plans, the Functions have in place target risk maturity levels. These targets help identify improvement areas and inform the remuneration framework, driving the link between risk capability and business planning and importantly, further embedding risk awareness and optimal risk management practices.

6. Internal Capital Adequacy Assessment Process

Suncorp has implemented an Internal Capital Adequacy Assessment Process (**ICAAP**) to determine the amount of capital that should be held to protect the interests of stakeholders. In addition to establishing processes to ensure the amount of capital that is held to support the risks of the relevant business (and its strategy) is adequate, the ICAAP ensures that:

- accountabilities for managing capital are clearly defined, both in normal operating conditions and in times of distress
- there is a clear articulation of the linkage between Suncorp's business strategy and its risk appetite, and there are adequate capital resources to support the strategy
- appropriate capital targets and triggers are established to support the degree of risk associated with Suncorp's business plans and enable Suncorp to absorb unexpected losses that are in accordance with its risk appetite
- capital positions are effectively monitored and reported
- key management decisions are based on a robust assessment of the relevant risk and capital implications
- contingency arrangements and capital restoration processes are in place, and reliably can be drawn upon in times of distress.

7. Stress-testing

Improvements in risk management and planning are dependent on properly understanding the consequences of changes in the internal and external operating environment. To this end, 'stress testing' and scenario analysis is undertaken across different risk categories to better support the Board and management assess risk, improve decision-making, and support responsiveness and resilience.

The Enterprise Stress Testing and Scenario Analysis Framework provides structure for Suncorp to conduct meaningful stress tests with a focus on achieving its risk management objectives. Such objectives include:

- improving operational risk limits and delegations
- establishing appropriate capital buffers
- testing recovery actions over different timeframes.

8. Risk-based capital

Risk-based capital (**RBC**) modelling continues to contribute to the ICAAP, and provides for a link between risk, capital management and business planning. In particular, the RBC models:

- are a key input into reviews of internal capital targets
- contribute to the articulation of risk appetite, particularly in relation to capital and earnings volatility
- assist in informing business decisions such as strategic asset allocation, the setting of optimal reinsurance programs and product pricing decisions.

9. Risk committee – comprises independent board members

The Risk Committee provides the Board with oversight across Suncorp for all categories of risk, through the identification, assessment and management of risk and monitoring adherence to internal risk management policies and procedures. The Risk Committee receives written reports from management on the status of risk appetite, Suncorp's current and emerging risk profile, and the effectiveness of the risk framework in operation.

The Risk Committee (which met five times during 2016-17):

- consists of five independent non-executive directors including the Board Chairman, Dr Zygmunt Switkowski AO, as an ex officio member
- is chaired by Mr Ewoud Kulk, an independent non-executive director with extensive experience in insurance and risk management
- has Ms Christine McLoughlin, Mr William Bartlett, and Ms Audette Exel AO among its members, all of whom have an extensive understanding of risk management.

The Risk Committee undertook a review of the ERMF during 2016-17 and takes primary responsibility for ensuring the Board-approved ERMF constitutes an appropriate and effective framework for risk management.

The Committee annually reviews and endorses the ERMF for Board approval, and oversees supporting policies, internal controls and processes. The Committee also endorses or approves significant changes to the ERMF, risk appetite, and risk management policies.

A summary of the key responsibilities of the Risk Committee is set out in the Risk Committee Charter, available at suncorpgroup.com.au/about-us/governance.

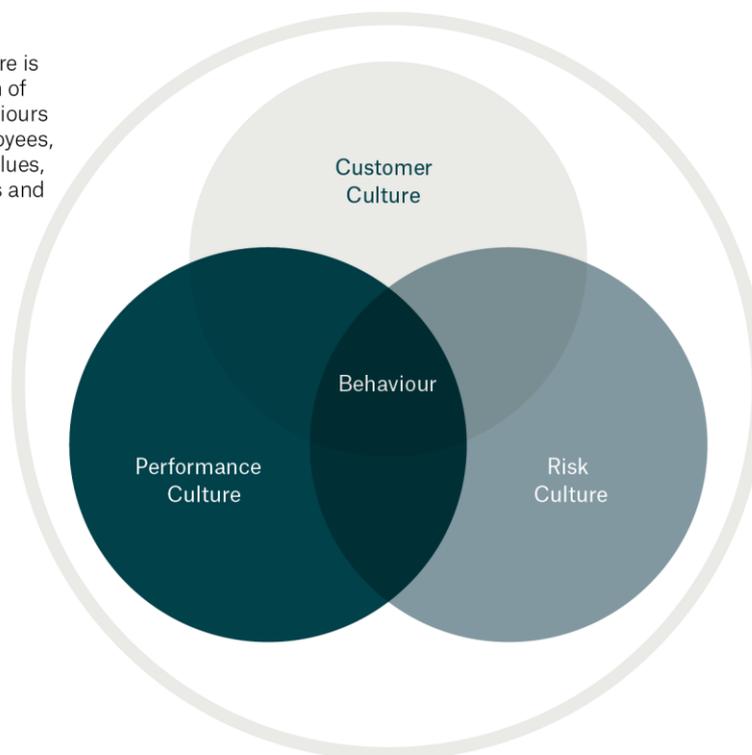
10. Risk culture

Suncorp's risk culture is recognised as a core component of Suncorp's overall culture. It is defined as the aggregation of observed behaviours across all employees in the organisation arising from our shared values and beliefs and shaped by symbols, systems and structures adopted by Suncorp.

It is recognised that Suncorp's overall culture is underpinned by three core elements: Customer Culture, Risk Culture and Performance Culture (refer to the following diagram).

Culture

Suncorp's culture is the aggregation of observed behaviours across all employees, driven by the values, beliefs, symbols and systems.



Customer centric culture is the set of symbols, systems and processes that empower all our people to put their customers at the heart of every decision. Our customer culture is critical at all stages of the customer life cycle, including claims management.

Risk culture is the set of acceptable norms and behaviours that determine the collective ability to identify, understand, openly discuss and manage the Group's current and future risks within our risk appetite.

Performance culture is the set of symbols, practices and policies that help people understand what behaviours and outcomes are valued and rewarded at Suncorp.

The relationship between these cultural dimensions is at the heart of Suncorp's cultural health and collectively these three dimensions shape the behaviour of our workforce and have a direct impact on all of our stakeholders. Aligning these cultural forces results in lowering of conduct risk and maximising the outcomes for our customers, shareholders and our workforce.

The Board and management recognise the importance of a positive culture (and risk culture), as well as the aspects that are critical in shaping and maintaining a positive culture, including the following:

- Culture starts from the top – senior leaders are critical in deciding on the systems and symbols, such as reward systems and policies that drive appropriate behaviours and employee actions.
- Culture is made manifest by the decisions and behaviour of all employees – Individual decisions and actions taken by employees on a daily basis have an impact on the overall culture of Suncorp.
- Culture is about doing the right thing in all situations and employees should always consider “What is the right thing to do?” in any situation.
- The Company's purpose must motivate employees and drive a positive culture.
- Culture must appropriately balance all key stakeholders – Suncorp's customer-led strategy is a key focus, but this must also be balanced with the importance of delivering shareholder value.

- Suncorp’s actual culture is best understood by identifying and understanding the alignment between the three core dimensions of the culture and by monitoring how Suncorp responds to and rectifies issues when those dimensions are found to be misaligned (owning and fixing mistakes).
- It is an ongoing process to understand and influence an organisational culture – It is not a ‘set and forget’ exercise.

11. Specific accountabilities for risk management

Management has a mandate and an obligation to manage risk in accordance with the Board-approved RAS and, more broadly, in accordance with Suncorp’s risk policies.

The Board has delegated to the CEO & Managing Director its authority to manage and supervise the day-to-day operations and activities, including authorities and limits for key risks facing Suncorp and the authority to commit and make operational and capital expenditures.

The Board has authorised the CEO & Managing Director to further delegate authorities to individuals in accountable positions. The CEO & Managing Director has discretion to delegate these authorities and limits to management. Specifically:

- The Senior Leadership Team (**SLT**) members are executives who report to the CEO & Managing Director and provide executive oversight and direction-setting across Suncorp, taking risk considerations into account.
- Each SLT member has end-to-end accountability for risks arising from their functional area.
- The CRO, who is a member of the SLT, is responsible for promoting and supporting risk considerations and is charged with the accountability for the ERMF and overall risk adequacy. The CRO reports to the CEO & Managing Director and has unfettered access to the Board.
- All functional CROs have formal lines of accountability to the CRO, and are part of the Functions’ management teams to provide guidance, support and challenge to the respective Function’s Chief Officer/SLT member and executive team, and promote a culture within the Function that reinforces risk management as core to business operations.
- At management level, governance committees form an important part of the risk accountabilities model with a number of committees comprising executives from both Suncorp and the Functions. These committees perform a valuable role in bringing together key subject matter experts to monitor and oversee elements of the ERMF.