Integrated Risk Management Framework

A balanced approach to risk

February 2023

Wayne Armour and David Barton

Contents

1 Purpose

This document sets out the Integrated Risk Management Framework (**the Framework**). The Framework covers the requirements, responsibilities, and processes for managing risk across BlueScope, including:

a) determining the Group's appetite for risk;
b) operating within risk tolerances; and
c) identifying, assessing, controlling and mitigating present and emerging risks.

2 Scope

The Framework applies to BlueScope Steel Limited, its controlled subsidiaries (**BlueScope** or the **Group**). The Framework applies to all directors and employees of BlueScope.

The Framework prescribes a set of components, principles and key processes that provide the foundation and arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the Group. Application of the Framework ensures consistency and a common language for risk management across the Group.

3 Context

This Framework has been designed to facilitate the management of risk at all levels across BlueScope, describe BlueScope's risk management policy statement (approved by the Board) and align with good practice guidance and regulatory requirements.

3.1 Effective management of risk at all levels across BlueScope (policy statement)

Risk is the effect of uncertainty on our objectives and is inherent in our business. Risk management is defined as coordinated activities to direct and control the business with regard to risk. Risk management is good business practice, it is a core and integral component of doing business at BlueScope. It is the responsibility of all business leaders and decision makers, not a separate function.

BlueScope is committed to an integrated approach to the management of all present and emerging business risks, both financial and non-financial. We aim to have a proactive risk culture, ensuring a balanced approach to managing uncertainty in the delivery of strategic objectives and commercial outcomes.

Determining in advance our **appetite** to take on financial and non-financial risk across a comprehensive range of business activities and endeavouring to operate within materially acceptable **tolerance** levels is a core component of risk management at BlueScope. It helps direct our efforts towards delivering sustainable long-term value that is aligned with Our Purpose, Our Bond and strategic objectives.

Effective risk management requires balance, enabling us to minimise the occurrence of material losses whilst being able to take advantage of opportunities. Decisions are made as close as possible to the source of risk. All BlueScope leaders and decision makers are empowered to own, assesses, monitor and manage risks directly within their area of responsibility and approved limits of delegated authority.

BlueScope maintains a **Risk Management Framework**, reviewed by the Risk & Sustainability Committee (RSC), and approved by the Board. The Framework is a model for risk management and control based on the 'three lines of defence' concept, and is aimed at ensuring clear accountabilities for risk management throughout the Group. The

Board has overall oversight of BlueScope's risk management and has established the RSC and other Committees (AC, ROC, HSEC) to assist fulfil its responsibilities in relation to specific areas of risk. Their respective roles and responsibilities, including in relation to risk oversight, are outlined in their Charters.

3.2 Australian Stock Exchange (ASX) Corporate Governance Principles and Recommendations

The ASX Corporate Governance Council's Corporate Governance Principles and Recommendations, 4th Edition 2019, sets out eight recommended corporate governance practices for entities listed on the ASX that are likely to achieve good governance outcomes and meet the reasonable expectations of investors. The board of a listed entity is ultimately responsible for deciding the nature and extent of the risks it is prepared to take to meet its objectives. To enable the board to do this, the entity must have an appropriate framework to identify and manage risk on an ongoing basis. It is the role of management to design and implement that framework and to ensure that the entity operates within the risk appetite set by the board.

Principle 7 of the ASX Recommendations provides that a listed entity should establish a sound risk management framework and periodically review the effectiveness of that framework.

> *[Recommendation 7.2] The board or a committee of the board should:*
>
> *(a) review the entity's risk management framework at least annually to satisfy itself that it continues to be sound and that the entity is operating with due regard to the risk appetite set by the board; and*
>
> *(b) disclose, in relation to each reporting period, whether such a review has taken place.*
>
> *[Recommendation 7.4] A listed entity should disclose whether it has any material exposure to environmental or social risks and, if it does, how it manages or intends to manage those risks.*

While not mandatory, BlueScope has adopted these principles and recommendations and confirms to the ASX that it complies with them each year or, if considered necessary, provides an "if not, why not" explanation.

3.3 Director's duties

The Australian *Corporations Act 2001* (Cth) sets out the general rule that a company officeholder must exercise their powers and discharge their duties with care and diligence and make business judgment that they rationally believe are in the best interests of the company (s180). This requires consideration of business risks by BlueScope directors and management.

The Framework is also designed to assist BlueScope and its directors meet regulatory requirements relating to Operating and Financial Review (OFR) disclosures in its annual report under s299 of the *Corporations Act 2001 (Cth)*, and further guidance provided by the Australian Securities and Investments Commission (ASIC) in its regulatory guide on the effective disclosure in an operating and financial review (RG247).

The OFR must set out information that shareholders would reasonably require to assess an entity's operations, financial position, and business strategies and prospects for future financial years. The OFR must include a disclosure of material business risks,

a) each risk should be described in its context (e.g. why the risk is important or significant, and its potential impact on the Company's financial prospects or operational performance);
b) include any relevant commentary (e.g. whether the risk is expected to increase or decrease in the foreseeable future); and
c) where the risk relates to factors within the control of management, specify how these factors will be controlled or managed by the Company.

Additional risk disclosures may also be required by law in other contexts, such as a prospectus or continuous disclosure announcement.

The Framework supports the assessment of material present and emerging risks. They will change over time (e.g. an increasing awareness of the likelihood and consequences of cybercrime, climate change and human rights risks) and a regular review process is required to facilitate the preparation of suitable disclosures.

3.4 Other compliance obligations in relation to managing specific risks

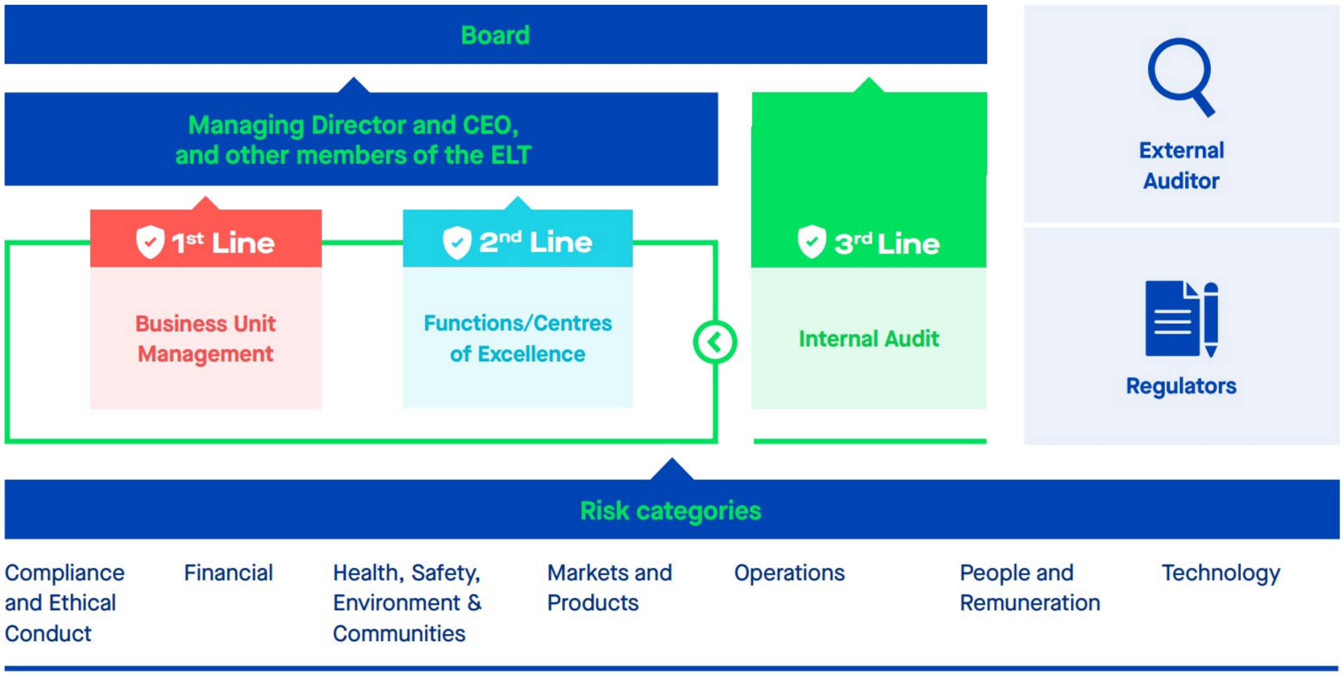
The Company operates in jurisdictions that impose a range of operating licence and regulatory compliance obligations addressing topics such as: Workplace Health and Safety, Environmental protection, Privacy, Anti-discrimination, Workers' compensation and Anti-money laundering.

The Framework is intended to ensure an integrated approach that aligns the management of specific compliance and regulatory risk across all aspects of BlueScope's business and jurisdictions.

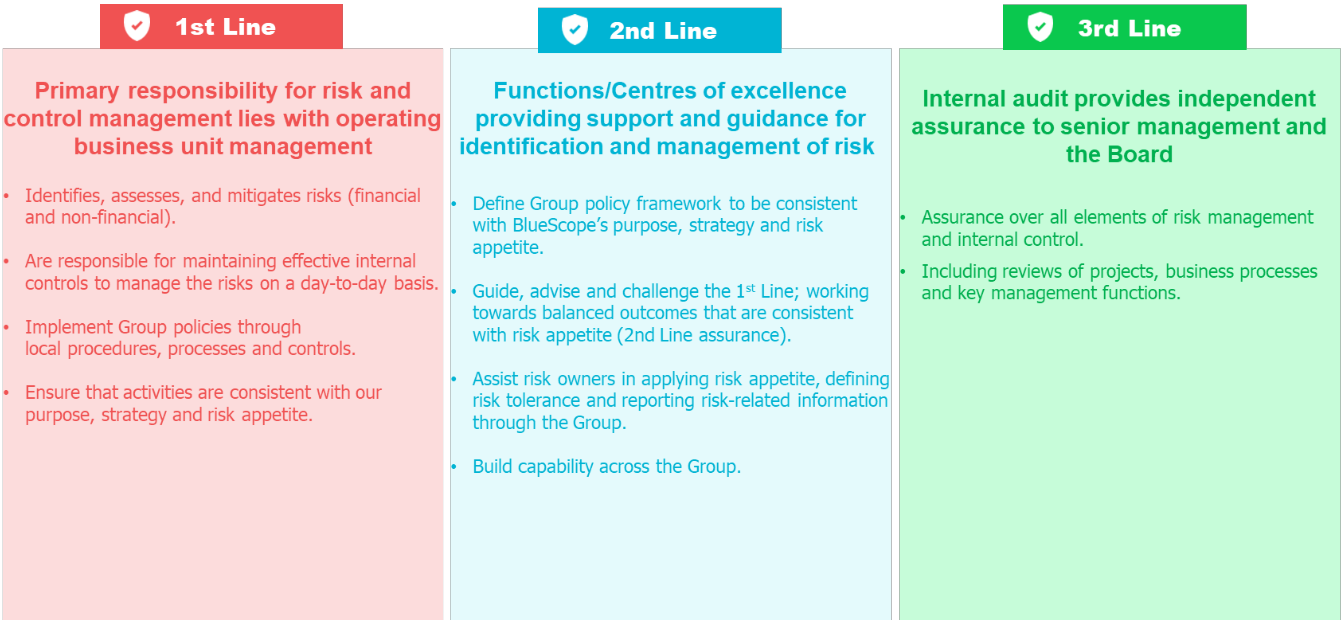
4 Accountability

4.1 Three lines of accountability

BlueScope uses the following model for risk management and control based on the "three lines of defence" concept, aimed at ensuring clear accountabilities throughout the Group.



The general accountabilities for each Line of Accountability are summarised below.



1st Line

Primary responsibility for risk and control management lies with operating business unit management

- Identifies, assesses, and mitigates risks (financial and non-financial).
- Are responsible for maintaining effective internal controls to manage the risks on a day-to-day basis.
- Implement Group policies through local procedures, processes and controls.
- Ensure that activities are consistent with our purpose, strategy and risk appetite.

2nd Line

Functions/Centres of excellence providing support and guidance for identification and management of risk

- Define Group policy framework to be consistent with BlueScope's purpose, strategy and risk appetite.
- Guide, advise and challenge the 1st Line; working towards balanced outcomes that are consistent with risk appetite (2nd Line assurance).
- Assist risk owners in applying risk appetite, defining risk tolerance and reporting risk-related information through the Group.
- Build capability across the Group.

3rd Line

Internal audit provides independent assurance to senior management and the Board

- Assurance over all elements of risk management and internal control.
- Including reviews of projects, business processes and key management functions.

4.2 Key roles and responsibilities

The Board has overall oversight of BlueScope's risk management and has established the Risk & Sustainability Committee (RSC) and other Committees (AC, ROC, HSEC etc.) to assist fulfil its responsibilities in relation to specific areas of risk. Their respective roles and responsibilities, including in relation to risk oversight, are outlined in their Charters.

The Chief Financial Officer (CFO) supported by the Corporate Risk team has overall 2nd line responsibility for risk management processes and systems, with other functional groups (e.g. Finance, Safety, Ethics & Compliance, Environment, Technology, Legal, People) responsible for processes and systems pursuant to their function that are aligned to the risk management framework, relevant legislative requirements and industry standards e.g. HSE functions have procedures specifically aimed at identifying, managing and reporting health, safety and environmental risks. These are described in specific functional risk procedures.

Consistent with the Three Lines of Accountability outlined above, 1st line accountability for risk management is the responsibility of the Chief Executive of each business; responsibility for specific risks may be delegated.

The roles and responsibilities outlined below are intended to provide high level guidance on the primary focus of these groups with respect to the management of risk. Further details regarding responsibilities are in other documentation such as Board, Board Committees and Executive Leadership Team (ELT) charters, role descriptions, work performance systems and other procedures relating to activities conducted by these roles.

Key risk management roles and responsibilities:

Role	Responsibility	Authority
Board and Committees	• Oversee the management of risk, including review of the risk management policy statement. • Review the appetite for risk at least annually. • Review the risk profile including risks that are material to the achievement of the Company's objectives and management's assessment of mitigating controls and actions relating to those risks, with a mid-year high level update. • Oversee the specific risks allocated to the Board or delegated to Committees as set out in each Committee's Charter;	• Approve Risk Management Policy Statement (Board). • Approve the Company's risk appetite (Board). • Approve disclosures in relation to material risks (Board). • Approve the Group's insurance programs (D&O to Board, credit to AC, all others RSC). • Approve the Company's Risk Management Framework and report to the Board on the soundness in accordance with ASX Principle 7 (RSC).

Role	Responsibility	Authority
Executive Leadership Team	• Promote the Company's risk management policies, processes and culture across the Group. • Review material risks and drive effective implementation of risk treatment activities. • Report to Board and Committees on significant and emerging risks, in accordance with the requirements outlined in the Committees Charters. • Report business unit risks and status of mitigation actions as part of their Quarterly Business Reviews by the CEO and CFO and business unit reports to the Board. • Report to Board and Committees on the effectiveness of risk management processes, including providing the Board with an annual representation that the risk management framework is operating effectively.	• Decisions, actions, resources for delivering the management of material risks.
All Personnel	• Reporting of risks. • Participation in consultation regarding the control of risks to which they or others may be exposed. • Implementing the risk controls provided to manage risks to which they or others may be exposed.	• Challenge any activity where they feel the risk is not being adequately managed.
Management (1st Line)	• Implement the risk management framework to their areas of control and manage risks that are material to their business activities. • Verify compliance to the risk management framework and its effectiveness. • Report on risks and their management for due diligence and governance reporting purposes.	• Decisions, actions, resources within their delegation of authority regarding the management of risks material to their business activities.
Group Risk Management (2nd Line)	• Review and report annually to the RSC on the Company risk management framework to which all BlueScope risk management activities will align. • Develop and maintain an insurance program consistent with the Group risk appetite and strategic objectives. • Consolidate material business risks for ELT and Board reporting	• Propose changes to the risk management policy and process for review and approval by the Board/Committee. • Propose changes to the insurance program for review and approval by the Board/Committees • Prepare and report on risk governance to Board and RSC.
Functional Groups/ Centre's of excellence e.g. Finance, Safety, Environment, Technology, Legal, People (2nd Line)	• Develop and maintain risk management tools and processes pursuant to their function that are aligned to the risk management policy, relevant legislative requirements and industry standards. • Provide stewardship and technical expertise to the ELT and management groups implementing their risk management processes and the control of risks. • Develop and maintain a network of risk management facilitators across BlueScope. • Assist risk owners in defining the target risk exposure and reporting risk-related information through the Group. • Through research, data analysis and other technical work advise management, ELT and Board of any significant risks including changes to existing material risks or new emerging material risks relevant to their function.	• Prepare reports and recommendations to appropriate Board, ELT members or Management groups regarding material risks and risk management processes and controls associated with their function.
Internal Audit (3rd Line)	• Conduct reviews on the effectiveness of controls and make recommendations for corrective actions and business improvement opportunities. • Provide assurance on the risk management process. • Advise new and emerging risks identified from the audit programs.	• Prepare audit reports and make recommendations to the Board and associated committees regarding BlueScope's financial position and selected business processes. • Execute approved audit plans

5 Risk Appetite

Risk appetite is the level of risk that an organisation it is willing to accept to achieve its objectives.

5.1 Normal operations

BlueScope has established qualitative risk appetite statements across a broad range of business activities, both financial and non-financial. These are reviewed and approved by the Board at least annually.

Risk appetite statements set the fundamental principles that govern the way we will execute our strategy and the acceptable level of risk the Group is willing to take. Understanding risk, and our appetite for particular types of risk, is a key consideration in our decision making.

Seven broad categories set the framework by which business risks are to be identified and managed;

- Compliance & Ethical Conduct;
- Health, Safety, Environment & Communities;
- Markets & Products;
- Operations;
- Financial;
- Technology; and
- People and remuneration.

In support of the risk appetite statements approved by the Board, management are encouraged to consider how they apply at the more granular level within their area of delegated authority (e.g. credit risk, construction risk, operational security risk) specific to a function or business unit.

5.2 Strategic projects

In addition to these broad categories of business risk noted above, BlueScope may also identify specific risks and uncertainties associated with the execution of strategic projects, such as;

- market development and business restructuring programs;
- major capital development projects;
- carbon reduction programs; and
- M&A activities.

Business decisions for these strategic projects are supported by a detailed consideration of the risks and uncertainties for the design and execution of each project. This may include scenario analysis, use of third parties to provide external perspectives and on-going reviews through the life of the project.

Strategic projects may be infrequent and each will have a unique set of risks, however, the concepts outlined in this framework still apply. That is, management are responsible for identifying and ensuring a balanced approach to the design and execution of each project, including consideration of the impact the project has on BlueScope's suite of risk appetite statements, and the level of risk the Group is willing to take in relation to the project.

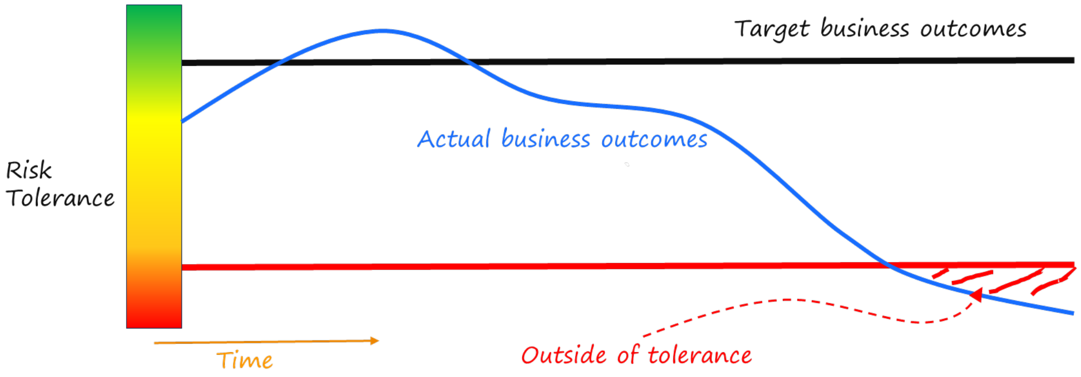
6 Risk Tolerance

Built upon the qualitative risk appetite statements, risk tolerance represents quantitative metrics that define the boundaries that BlueScope targets to operate within.

To be effective tolerance metrics should be specific, measurable and directly linked to the appetite statements. In most cases these metrics already exist and are used by 1st line teams for the day-to-day management of performance, sometimes referred to as Key Performance Indicators (KPIs).

A graphical way to represent risk tolerance is shown below. The blackline indicates the targeted business outcomes, the redline shows the limit of what we can tolerate for this risk. The blueline depicts actual business outcomes which vary over time, in the example below initially improving then dropping off to the point where performance is outside of tolerance (the redline).

The intent of setting tolerance levels which reflects our risk appetite, and then monitor performance is to prompt an early discussion on risk trends and take action to remain within acceptable levels (if within the amber zone) or to reposition back within acceptable tolerance levels (if consistently in the red zone).



Tolerance levels will vary over time, jurisdictions, and types of risk. The target business outcomes, tolerance levels and business outcomes need to be monitored and reassessed over time.

7 Risk identification, assessment and mitigation

In addition to considering risk appetite and risk tolerance, periodic risk assessments provide an overview of present and emerging businesses risks, their causes, consequences and the likelihood of the risk materialising. This process provides input to decision-making about:

- whether certain business activities should be undertaken;
- controls required to manage risks and whether additional actions and resource allocations are required;
- choosing between options with different risk profiles; and
- prioritising risk treatment (mitigation) options.

These periodic reviews assist 1st Line management assess their business risk prolife and provide supporting documentation for the consolidated Group Risk Profile which proves a view of material business risks across the group (high and emerging) for the ELT and Board.

The Corporate risk function maintains a number of reference documents and templates to be used by business units and functions to manage risk. These include:

Document	Purpose and use
Risk Management Standard	Provides further guidance on identifying and evaluating risks.
Consequence & Likelihood Tables	Tables that describe the consequence of an event structured against the seven categories in our risk appetite, and a table that describes the likelihood of an event occurring.

Document	Purpose and use
Templates	Risk Profile – high and emerging risks, including bow tie analysis for high rated risks.
	Risk Tolerance reporting for inclusion in QBR packs.
	Risk Evaluation template for strategic or other projects.
Workshop Guidance	To assist businesses, facilitate and document annual risk workshops.

These materials are updated from time to time and are available on the intranet. Training is also provided where there are significant updates or new users join the business.

8 Risk management processes

A fundamental principle of BlueScope's risk management approach is that a balanced approach to risk should be a consideration in all decision making. Processes, involving the consideration of risk and whether performance is consistent with the Group's appetite, including:

Process	Timing and intent	Output
Strategy review	Once a year, a formal update of three-year business plans.	Assessment of emerging trends and conditions in each market.
Risk discussions	Anytime, to evaluate if a business decision is consistent with our risk appetite.	A business decision, action.
Risk workshop (BU)	Once a year, a formal deep dive with business leader to evaluate current risks, identify emerging risks and trends.	The Risk Profile for the BU, including descriptions of the high rated risks and mitigating controls. Listing of lower rated and emerging risks.
QBR Risk Tolerance reporting (QBR)	Each quarter, business unit to present risk metrics to measure performance against the risk appetite principles. Also include a 2 page summary of the BU risk profile; high & emerging risks.	QBR pack.
Group Risk Profile (a) appetite and tolerance levels (Board)	Annual review of Risk Appetite and tolerance levels to ensure they are fit for purpose (updated infrequently).	Annual report to Board on the risk profile of the Group, mid-year update.
Group Risk Profile (b) current and emerging risks (Board)	Consolidated view of business risks across the group (high and emerging).	
Quarterly Risk Tolerance report (RSC)	Corporate consolidated risk metrics to measure performance against the risk appetite principles.	Report to RSC.
Strategic projects (Board)	Anytime, evaluate the risks and proactively taking actions to manage exaction risk.	Reporting at approval and during project execution.

9 Other Reference Materials

Additional mechanisms supporting the Risk Management Framework include:

a) Delegation of Authority policy and guidelines including Pathfinder;
b) Our Bond and Code of Conduct – How We Work (along with associated requirements such as Speak up policy);
c) Approval processes, including sign off requirements, executive briefings and inclusion of key projects, contracts and regulatory matters in pipelines which are updated regularly (e.g. CLO /CFO);
d) HSEC Policy, Safety Beliefs, Environmental Principles, HSE Standards and Management Systems;
e) Financial governance framework, including accounting policies, account reconciliations, reporting accounting matters for consideration and balance sheet stewardship reviews;
f) Treasury governance framework, including liquidity, funding, hedging, currency, credit, guarantees and banking relationships;
g) Tax governance framework;
h) Capital and investment framework;
i) Internal and external audit;
j) Litigation reporting; and
k) Property, general liability, D&O and other insurances.

10 Ownership and Review of the Framework

The owner of this Framework is the Head of Risk Management.

This Framework will be reviewed each year and approved by the Board. The document will be reviewed more frequently where there is an event such as a significant change of law or approach to risk management that could affect the operational effectiveness of the Framework.

At BlueScope we value inclusion and encourage our People to share their ideas and feedback. We are committed to rostering a culture of speaking up when something isn't right.

Our Purpose
Our Bond

SpeakUp