

1. Purpose

The purpose of this Risk Policy ('Policy') is to articulate BlueScope's approach and commitment to managing risk across the organisation. It establishes the principles and governance that support the effective identification, assessment and management of risk. This enables informed decision-making, operation within Board-approved risk appetite, and the achievement of strategic objectives. The Policy provides the foundation for the Risk Management Framework, through which risk management is embedded across BlueScope.

2. Scope

This Policy applies to BlueScope Steel Limited and its controlled subsidiaries (BlueScope or the Group) and to all directors, employees and third parties acting on behalf of BlueScope. It applies to all activities, decisions and processes that may impact the achievement of BlueScope's strategic objectives, and includes all categories of risk, including strategic, operational, project, and other enterprise risks.

3. Policy commitment

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 organisation with regard to risk. Risk management is a core business discipline and an integral part of how BlueScope operates. It is the responsibility of business leaders and decision makers, not a separate function.

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

The Board determines the level of risk the organisation is willing to accept through the Risk Appetite, supported by defined tolerance levels. Operating within this Risk Appetite is a core component of risk management and supports the delivery of sustainable long-term value aligned with *Our Purpose*, *Our Bond* and strategic objectives.

Effective risk management enables informed decision making by balancing potential losses with opportunities. Decisions are made as close as practical to the source of risk, within approved risk appetite and delegated authority. Leaders are accountable for managing risks within their areas of responsibility and for maintaining effective oversight and control.

BlueScope maintains a Risk Management Framework that establishes the principles, processes and accountabilities for managing risk across the organisation. The Framework is based on the Three Lines Model, which clarifies roles and responsibilities for risk management, oversight and independent assurance. The Board retains overall oversight of risk management and is supported by the Audit, Risk and Technology Committee and other Committees in fulfilling its responsibilities.

BlueScope is committed to protecting those who make a report when they know or suspect something is not right, including any conduct that is inconsistent with this document or the Code of Conduct.

You can make a confidential *Speak Up* report directly to the Head Office Investigations Team by email (Help_SpeakUp@bluescope.com) or online.