WOOLWORTHS GROUP

GROUP RISK MANAGEMENT POLICY

Purpose

Woolworths is committed to meeting high standards in the ways we manage our business. We seek to support Woolworths to achieve its business objectives by effectively managing its risks, which creates shareholder value and protects our people, customers and assets. Effective risk management is integral to supporting Woolworths Group's ("Woolworths") purpose, strategy, values and ways of working. The purpose of this policy is to articulate Woolworths overall approach and principles adopted in relation to risk management.

Risk management is everyone's responsibility. We aim to do the right thing by our customers, communities, suppliers and each other and are committed to delivering on our promises to our customers.

Scope

This Policy applies to all relevant Business Units, Business Areas, Contractors and Significant Third Parties who work for, or with the Woolworths Group, in all countries of operation. It should be read in conjunction with the Enterprise Risk Management (ERM) Framework.
This Policy seeks to align Woolworths' Risk Management approach with applicable frameworks including but not limited to:

- *Australian/New Zealand Standard (AUS/NZS ISO 31000:2009 Risk management – Principles and guidelines);*
- *ASX Corporate Governance Council's Corporate Governance Principles and Recommendation – Third Edition (2013); and*
- *Committee of Sponsoring Organisations of the Treadway Commission (COSO) Enterprise Risk Management Framework: Enterprise Risk Management- Integration with Strategy and Performance (2017).*

Principles

- ***Risk Ownership:*** Everybody in the organisation is responsible for risk management.
- ***Board Risk Oversight:*** The Board of Directors provides oversight of the strategy and carries out governance responsibilities to support management in achieving business strategy and objectives.
- ***Risk Culture:*** Woolworths defines desired behaviours that characterise desired risk culture. The Board and senior management lead by example and demonstrate a strong commitment to risk management.
- ***Operating Model:*** Governance and operating models are established in the pursuit of buisness strategy and objectives including the three lines of defence.
- ***Commitment to Core Values:*** Woolworths is committed to its purpose, values and ways of working.
- ***Resourcing Alignment:*** Woolworths demonstrates commitment to attract, develop and retain capable Team Members.
- ***Business Context:*** Woolworths considers potential effects of business context on risk profiles, including internal, external and emerging risk drivers. Risk management should be aligned to support strategy, objectives and initiatives.
- ***Defines Risk Appetite:*** Risk appetite assists in creating, preserving and realising value by influencing the Group's attitudes towards risk and risk taking behaviours
- ***Risk Identification:*** The business identifies key risks and their drivers (strategic, operational, financial or compliance) that could impact the performance of business strategy and objectives.
- ***Risk Assessment:*** Risk and control assessments are regularly conducted and reviewed.
- ***Risk Response:*** Risk responses are selected and action plans prioritised.
- ***Risk Management and Reporting:*** An enterprise portfolio view of risks is developed and evaluated.
- ***Continuous Improvement:*** A culture of continuous improvement is in place to review and enhance the suitability, adequacy and effectiveness of our framework and its elements.
- ***Technology Enabled:*** Leveraging information and technology systems supports ERM data governance and data integrity.
- ***Risk Reporting:*** Committed to enhancing risk reporting at multiple levels across Woolworths.
- ***Industry Standards:*** We seek to adhere to all relevant laws, regulations, legislation and Codes of Conduct as applicable, however for those parts of the Group that are impacted by foreign or local laws, regulatory requirements or contractual obligations that conflict with this policy, an exemption from the policy or specific obligations should be reasonably applied.

Risk Management

- Risk is defined as the chance of an event (an occurrence or set of occurrences) occurring which may have an impact on Woolworths strategy or objectives, either favourably or unfavourably and is often categorised by reference to consequences and the associated likelihood of occurrence.
- Risk management encompasses coordinated activities to direct and control Woolworths with regard to risk. Managing risk is part of how we do business. It is defined as the culture, capabilities and practices, integrated with strategy-setting and performance that Woolworths relies on to manage risk in creating, preserving and realising value. Failures in our ability to appropriately manage our risks can directly impact our Customer, Team Member experiences and may also be damaging to our brand, reputation and/or have financial or legal/regulatory consequences.
- This policy should be read in conjunction with the ERM Framework which outlines our approach and key elements of risk management. The ERM Framework has been developed to help all of us manage risks with confidence through our ways of working. The ERM Framework is designed to be simple and easy to follow, empowering each business to effectively identify, assess, respond, manage and report upon their risks, adopting a risk based approach.
- All material Business Units (as agreed by Group Risk) will provide risk reporting to the ARMCC on their Risk Profiles, supported by Risk and Control Self Assessments (RCSA) no less than annually.
- Integrating ERM practices seeks to prove risk-informed decision making in governance, strategy, objective-setting and day-to-day operations. It helps to enhance performance by more closely linking business strategy and objectives to risk. Risk management should support our strategy and is intended to be embedded within governance, operations, processes and systems with clear accountability and ownership and consistently applied across the Group.

Roles and Responsibilities

Roles and responsibilities relating to ERM encompass the following:

- The Board of Directors is responsible for providing risk oversight of ERM culture, capabilities and practices. It has primary responsibility for risk oversight including conducting reviews of ERM practices and may delegate governance oversight to a Board Committee and day to day oversight to Woolworths Group Executive Management.
- The CEO's is accountable to the Board and is responsible for overall ERM culture, capabilities, and practices required to achieve business strategy and objectives. Sets the tone at the top along with explicit and implicit values, behaviours and norms that define culture. The CEO's responsibilities includes:
    - Providing leadership and direction to senior management and shaping core values, standards, expectations of competence, organisation structure and accountability;
    - Evaluating strategy within risk appetite, maintaining oversight of risks facing Woolworths; and
    - Guiding the development and performance of the ERM process across Woolworths and appropriate delegation as well as communicating expectations and information requirements.
- Woolworths Group ExCo and Senior Management are accountable for the effective implementation and embedding risk management and elements of the ERMF across the Woolworths Group. Heads of Business Units and Business Areas are responsible for identifying, assessing, responding, managing and reporting upon risks within their Business Unit/Area and implementing appropriate risk treatment where risks exceed risk appetite. Heads of Business Units and Business Areas are responsible for making available appropriate and capable resources to effectively manage risks and implement the ERMF, recognising different responsibilities and accountabilities.
- General Manager – Group Risk and Assurance oversees the development of ERM as a part of their accountabilities in the second line of defence, assisting the Board and Senior Management in fulfilling their respective risk oversight responsibilities. The GM assists in establishing ongoing risk management practices, reviewing, communicating with management through relevant risk forums and escalating identified or emerging risk exposures to Senior Management/Committees and the Board as identified by the business.
- Business Risk Partners provide assistance to the Business Units/Areas in guiding the development of the RCSA to drive consistency where practical, support training, and partner with the business to enhance risk management practices and support the implementation of the ERMF.
- Team members must comply with all relevant policies, frameworks, standards and procedures addressing risk management.

Governance

Woolworths has adopted the 'Three Lines of Defence" model to clarify accountabilities for risk management across the Group, as highlighted in the diagram below:

- All relevant Team Members must be familiar with this Policy, and compliance with the Policy is mandatory.
- Any operation found to be in breach of this policy will be required to provide explanations for non-compliance, and provide an action plan for remediation and addressing deficiencies.

Entities covered by this Policy

This policy is relevant to Woolworth Group Limited and its controlled entities (Woolworths Group). It also applies to any entity over which Woolworths has significant influence and which is material to Woolworths.

Policy Changes	Changes to this policy shall be endorsed/approved by the ARMCC, other than administrative changes or changes to address unintended consequences, which can be approved by the GM – Group Risk & Assurance.	
Date approved:	**V1.0 November 2017**	
Accountable	General Manager - Group Risk & Assurance	
Related references, policies, frameworks and standards:	• AUS/NZS ISO31000:2009 Risk Management-Principles and Guidelines • ASX Corporate Governance Council's Corporate Governance Principles and Recommendations • Committee of Sponsoring Organisations of the Treadway Commission (COSO) Enterprise Risk Management Framework: Enterprise Risk Management- Integration with Strategy and Performance (2017).	• Enterprise Risk Management Framework • Business Resilience Framework • Business Continuity Management Policy and Framework • Group Crisis Management Plan • Emergency Management Business Rules • IT Disaster Recovery Policy • IT Disaster Recovery Management Plan • Technology Risk Framework • Procurement and Third Party Policy/Framework • Compliance Policy/ Framework • Safety and Health Framework