



# Group Risk Policy



## Extracted from the Risk Management Policy and Framework

### 1. Risk Management Policy

#### 1.1 Purpose

Coles Group Limited and its subsidiaries (**Coles**) is committed to the effective and robust management of risk with the purpose of:

- becoming the most trusted retailer in Australia and growing long-term shareholder value;
- strengthening confidence across our team members, business partners, shareholders and communities in which we operate;
- operating ethically and responsibly, including the safeguarding of human rights; and
- meeting our business objectives and legal and regulatory obligations.

The purpose is achieved through the delivery of our risk management objectives, which focus on the proactive management of risks to:

- support the pursuit of our strategy and operational objectives whilst managing associated risks within a pre-defined level of appetite;
- facilitate informed decision making based on a comprehensive understanding of the threats and opportunities;
- establish appropriate risk management responses so that we reduce surprises and associated costs and losses; and
- provide the Board and Executive with clear and transparent information to enable appropriate oversight of Coles' risk management program including current risks and mitigation.

#### 1.2 Policy application

The Group Risk Policy (**Policy**) applies to all Coles functions and Business Units; and to all Coles team members, contractors and partners. The Coles Risk Management Framework must be applied to all levels of the Coles and to all processes, practices and activities which involve the achievement of set of business objectives. At a minimum this must include the following:

- Coles' Corporate Planning process;
- when setting strategy, business plans and budgets for each function;
- the lifecycle and delivery of all approved projects, including Capital Approval Committee (**CAC**) and Cost Leadership Committee (**CLC**);
- when managing third parties including sourcing, contracting and off-boarding; and
- when planning or implementing significant changes to existing organisational structures, IT systems, or business processes, and business partners.

#### 1.3 Definitions

Coles defines risk as "the effect of uncertainty on objectives" in accordance with the AS/NZ ISO 31000 Risk Management Guidelines and Principles. Refer to [Appendix A – Glossary Of Terms](#) for the definitions used by Coles which are aligned to the ISO Guide 73: Risk Management - Vocabulary.

## 1.4 Policy requirements

- (a) Understanding and managing our risks is part of how we work at Coles. It helps us meet our business objectives and obligations, make better decisions, and act ethically in the best interests of Coles and our shareholders.
- (b) Risk management is everyone's responsibility. All team members must understand relevant risks and their impacts when making business decisions. Accountability for risk management must be assigned, including who will design and implement the Risk Management Policy and Framework, and roles responsible for managing specific risks.
- (c) We have a 'no surprises' approach to risk management. Risks should be quickly raised and communicated and consulted about in an open, timely and transparent manner when they become known. If team members identify a risk and are unsure who to raise it with, talk to your manager or to a member of the Risk and Compliance team.
- (d) Risk appetite, organisational thresholds and limits must be evaluated when making decisions about how risks are to be treated. These limits may be in the form of appetite statements, policies and procedures, delegations of authority and other organisational measures.
- (e) Appropriate action plans must be put in place if a decision is made to mitigate a risk, or if a risk is outside of risk appetite, organisational thresholds and limits.
- (f) Risks within risk appetite and organisational thresholds and limits can be accepted, as long as all decision makers (in accordance with the Coles Delegation of Authority and Document Execution Authority) understand the consequences of accepting the risks and agree to the risk acceptance.
- (g) Description of the risk, action plans and risk decisions must be documented for Coles material risks. This will help us to better understand our risks and communicate them to others.
- (h) Risks change over time. Team members must continue to monitor and review risks so that plans and actions to manage them, including risk acceptance decisions, remain relevant.
- (i) A positive risk culture of accountability must be maintained and fostered at all levels of the business. This will encourage positive risk management behaviours, whilst exercising strong stewardship and good corporate governance.
- (j) Executives must ensure their areas of accountability are appropriately resourced to perform their risk management duties, and an appropriate level of capability is maintained to implement the Risk Management Policy and Framework.

## 1.5 Breach of Policy

Failure to comply with this Policy may result in disciplinary action, up to and including dismissal.

Adopted by the Board 24 March 2020.