Risk Management Policy

Spirit Technology Solutions Ltd

ACN 089 224 402

Table of Contents

Document History

Version	Summary of Amendments	Approved by	Approval date
2020.1	Document creation	Board	19 May 2020
2025.1	Document revocation and subsequent adopt new.	Board	25 August 2025

Applicable External Frameworks

Authority	Law, Resolution, or Regulation
Standards Australia	AS/NZS ISO 31000:2018 – Risk Management
ASX	ASX Corporate Governance Council's Corporate Governance Principles and Recommendations, 4th Edition

Other Policy Details

Key Information	Details
Policy Custodian	Company Secretary
Responsibility for Implementation	Group CFO and CISO
Oversight and Reporting Body	Board, Audit and Risk Committee, supported by the internal Risk Governance Forum
Key Stakeholders	Spirit Staff (All of the Group's staff, workers, Board members, volunteers, contractors, student placements, and visitors.)
Next Review Date	August 2027

Associated Documents

This document should be read in conjunction with related policies, procedures, and guidelines, including (without limitation):

a) This Risk Management Policy ("**Policy**");

b) Risk Appetite Statement ("**Statement**");

c) Risk Management Framework ("**Framework**");

d) Risk Register; and

e) Delegations of Authority Policy.

1. INTRODUCTION

1.1 This Risk Management Policy ("**Policy**") sets out Spirit Technology Solutions Ltd's ("**Company**") and its subsidiaries (collectively, the "**Group**") commitment to a structured and integrated approach to the oversight and management of material risks that may impact strategic, operational, financial, compliance, reputational, or sustainability objectives.

1.2 Spirit recognises that risk-taking is intrinsic to value creation and innovation. This Policy seeks to balance risk and reward in a manner that supports our purpose: delivering secure, sustainable and scalable solutions across cyber, managed IT, and collaboration.

2. PURPOSE

The purpose of this Policy is to:

- Encourage appropriate levels of risk-taking within the parameters of the Statement.
- Set out guiding principles for identifying, assessing, managing, monitoring, and reporting risks.
- Establish governance, delegations, and responsibilities for risk management.
- Ensure risk oversight adapts to changes in the operating environment, business model, or strategy.

3. DEFINING A RISK

A "risk" is classified differently to an "issue". The differences are as follows:

Risk	Issue
A *potential* event or condition that *might* occur in the future and could impact objectives.	An *actual* event or problem that *has already happened* or is currently happening.
Managed *proactively* – assessed, scored, and (if necessary) added to the risk register.	Managed *reactively* – resolved operationally through corrective action, potentially without being recorded as a risk.
May never occur.	Has already occurred.

E.g. "If our cloud service is misconfigured, sensitive data might be exposed."	E.g. "We experienced a data exposure due to a misconfigured cloud setting."

4. RISK APPETITE STATEMENT

4.1 The Statement articulates the aggregate level and types of risk the Company is willing to tolerate in pursuit of its strategic goals.

4.2 The Statement is structured around six core risk categories:

- People and Culture
- Cyber Security, Information Technology (IT) and Intellectual Property (IP)
- Customer and Market Delivery
- Sustainability
- Financial (incl. tax)
- Governance

4.3 The Company's risk appetite ranges from High Appetite (e.g. innovative product development or technology-enabled transformation) to Very Low / No Appetite (e.g. illegal conduct, regulatory non-compliance, privacy breach, unsafe work practice). Where the Company's appetite for a given risk is low or there is no appetite for that risk, it is expected that appropriate controls exist, are actively monitored and that the controls and monitoring are substantially effective. Where the Company's appetite for a given risk is high, controls may exist or appropriate controls may be developed in parallel with the risk-taking initiative.

4.4 The Board reviews and endorses the Statement on a regular basis and in the event of any material change, consistent with the Audit and Risk Committee ("**ARC**") Charter.

4.5 The ARC oversees the Statement's implementation and management reporting.

4.6 The key determinants of the Company's risk appetite include (without limitation):

- shareholder and investor preferences;
- expected business performance (return on capital);
- the capital needed to support risk taking;
- the culture of the organisation;
- management experience along with risk and control management skills; and

- longer-term strategic priorities.

5. RISK MANAGEMENT FRAMEWORK

5.1 The Company believes that risk should be managed and monitored on a continuous basis. To this end, the Company has implemented a dynamic Framework designed to manage risks effectively and efficiently, enabling both short-term operational priorities and longer-term strategic objectives to be achieved.

5.2 The Framework sets out how the Company manages risks across the enterprise and business segments.

5.3 The Framework includes:

- Identification of risks (strategic, operational, financial, compliance, people, technology, etc.);
- Risk assessment using qualitative and, where relevant, quantitative measures (likelihood and impact);
- Treatment strategies (avoid, accept, mitigate, transfer, or insure);
- Monitoring, review, and escalation procedures, including the preparation and consideration of operational reports with relevant data and metrics to inform decision-making at governance forums;
- A structured approach to categorising risks in alignment with the approved Statement.

6. RISK RATING AND EVALUATION

6.1 Risk rating is conducted by assessing each identified risk against two core criteria: likelihood (probability of occurrence) and impact (severity of consequences). Using the Company's approved Risk Likelihood and Risk Impact tables, these factors are combined in the Risk Matrix to produce an overall risk rating (Low, Low-Medium, Medium, Medium-High, or High). This process ensures consistent classification of risks across the enterprise.

6.2 A High rating indicates an unacceptable risk that requires escalation to the ARC and consideration for immediate mitigation or elimination.

6.3 Medium-High and Medium ratings require proportionate treatment within agreed timeframes.

6.4 Low-Medium and Low risks may be managed through routine procedures and monitoring.

6.5 Risk ratings are reviewed regularly, and whenever there are significant changes in the risk context, incidents, or emerging threats. Where treatment plans are implemented, ratings are re-evaluated to confirm residual risk remains within the appetite articulated in the Statement.

6.6 The process for determining, recording, and monitoring risk ratings is detailed in the Framework.

7. RISK OVERSIGHT AND GOVERNANCE

7.1 (**Purpose**) The Company's risk oversight and governance structure establishes clear accountability for identifying, assessing, treating, and monitoring risks in line with the approved Framework and Statement.

7.2 (**Roles and responsibilities**) The following roles and responsibilities ensure risk management is embedded across all levels of the organisation, from Board oversight to day-to-day operational execution:

Role	Responsibility
Board	Holds ultimate accountability for the Company's risk management performance and outcomes. • Set and approve the Statement, Framework, and Policy. • Oversee and review the systems of risk management and internal compliance and control to ensure the Company is operating within its risk appetite. • Monitor material risks and the effectiveness of related controls. • Ensure that risk management is integrated into strategic planning, budgeting, and performance monitoring. • Receive regular, fit-for-purpose Board reports that enable informed decision-making and transparent escalation of material risks.
ARC	Supports the Board in fulfilling its risk governance obligations in accordance with its ARC Charter. • Review the effectiveness of the Framework and associated policies. • Monitor the Company's exposure to key risks, including financial, operational, compliance, and strategic risks. • Oversee the integrity of the Company's financial reporting and the adequacy of internal controls. • Review internal and external audit findings, ensuring timely and effective remediation. • Monitor compliance with laws, regulations, and other external requirements.

CFO / CISO	Provide executive custodianship of the risk management system, ensuring registers, controls, treatments, and governance remain robust and aligned to the Statement and strategic objectives. • Maintain and oversee the completeness, accuracy, and currency of enterprise and business unit risk registers. • Oversee the development, implementation, and monitoring of treatment plans, ensuring they address root causes and are delivered within agreed timeframes. • Escalate material risk issues, emerging threats, and breaches of the Statement to the ARC and Board in a timely manner. • Lead the periodic review and update of the Statement and Framework, incorporating lessons learned from incidents, assurance activities, and changes in the operating environment. • Facilitate cross-functional risk capability development and provide guidance to business units on best-practice risk management. • Oversee the effectiveness of the Company's financial and cybersecurity controls environment, ensuring design, implementation, and monitoring of controls are robust, operating effectively, and aligned to the Statement and strategic objectives.
Governance Forum (internal)	Serve as the operational hub for enterprise risk coordination, challenge, and escalation across the business. • Coordinate risk identification, assessment, treatment, and monitoring activities. • Review new and emerging risks and changes to risk ratings. • Challenge treatment plans and ensure alignment with the Statement. • Consider incident reports, audit findings, and compliance breaches. • Escalate risks to the CFO/CISO for ARC reporting.
Management	Implement the Framework and embed risk management into day-to-day business processes. • Identify, assess, and manage risks within delegated authorities. • Ensure that adequate resources, systems, and processes are in place to manage risks effectively. • Report on emerging risks, control effectiveness, and treatment progress to the ARC and Board. • Foster a culture where risk awareness and accountability are core to decision-making at all levels.

All Staff	Act as the 'first line of defence' by identifying, managing, and escalating risks within their areas, fostering a proactive risk-aware culture. • Identify, assess, and manage risks in day-to-day activities. • Comply with the Framework, Statement, and relevant policies. • Escalate emerging risks through appropriate channels. • Contribute to a culture of transparency, accountability, and continuous improvement.

7.3 (**Risk Culture and Behaviour**) The Board and Management are committed to fostering a strong risk culture that:

- Encourages open, timely, and accurate risk reporting;
- Supports constructive challenge and diversity of thought in decision-making;
- Recognises and rewards behaviours that align with the Company's risk appetite and values; and
- Embeds accountability for risk at all levels of the organisation.

7.4 (**Continuous Improvement**) The Company is committed to the ongoing enhancement of its risk management capability. Lessons learned from incidents, audits, reviews, and industry developments are incorporated into the Framework to ensure it remains effective, relevant, and aligned with the Company's evolving strategy and operating environment.

8. REVIEW AND ASSURANCE

8.1 The Policy will be reviewed every two years or earlier if there is a material change in strategy, risk profile, or regulatory expectations.

8.2 Independent internal or external reviews may be commissioned by the ARC to test the effectiveness of the Framework.

8.3 Management provides assurance that controls and procedures are operating effectively via quarterly reports.

8.4 This Policy will be reviewed at least every **two years** and when required, to ensure that it remains effective and meets the requirements of the applicable external frameworks.