Mining and Automotive Skills Alliance

# Enterprise Risk Management Framework

Version 1.0

## Contents

# 1 Purpose

The purpose of this Enterprise Risk Management Framework (ERMF) is to establish a structured, consistent and organisation-wide approach to managing risk across AUSMASA.

This framework supports informed decision-making and accountability by ensuring that risks are identified, assessed and managed in a transparent manner.

Risk management at AUSMASA is not a stand-alone activity. It is integral to strategic planning, project delivery, industry engagement, financial stewardship and compliance with funding and legislative obligations.

The framework is designed to:

- Protect public value, stakeholder confidence and organisational reputation;
- Support the achievement of strategic priorities;
- Enable informed innovation and responsible risk-taking; and
- Strengthen resilience in a complex and changing operating environment.

The Framework aligns with:

- AS ISO 31000:2018 Risk Management Guidelines; and
- The Commonwealth Risk Management Framework.

# 2 Scope

This framework applies to:

- The Board
- Chief Executive Officer (CEO)
- Executive Leadership Team (ELT)
- Advisory Groups and Committees
- Employees and contractors

# 3 Risk Management Principles

Our risk management approach is guided by ten principles. These are not aspirational - they are the standards by which we assess the quality of our risk management.

| Principle | What it means? |
|---|---|
| Strategic Alignment | Every risk decision must connect to our strategic priorities and the objectives. Risk appetite settings mirror the priorities in the AUSMASA Strategic Plan 2025-28. Risks that could prevent us from delivering on our strategy are treated with urgency. |
| Differentiated Appetite | We do not apply a single risk tolerance across the organisation. We accept higher risk in areas of innovation and workforce intelligence because the potential benefit justifies it. We maintain low tolerance for compliance, funding and integrity risks because failure in these areas is not recoverable. |

| | |
|---|---|
| Risk-Informed Decisions | All significant decisions, including new projects, partnerships and initiatives, must include an explicit risk assessment before approval. When a proposal sits outside defined appetite levels, it must be escalated for further review. |
| Clear Accountability | Every risk has a named Risk Owner at ELT/Executive Director (ED) level and a Risk Delegate. Accountability is not shared generically; it is assigned specifically. Owners report on their risks. Delegates manage them day-to-day. |
| Dynamic, Not Static | Our risk appetite and risk register are living documents. We review appetite settings annually and re-evaluate in response to major changes such as new Ministerial priorities, funding extensions, industry shifts or incidents. What we tolerate today may not be what we tolerate next year. |
| Integrated with Governance | Risk is embedded in our governance cycles. It appears as a standing agenda item at ELT, and Risk, Audit and Finance (RAF) committee meetings. Risk assessments are required for project approvals. |
| Supportive Culture | We actively cultivate a culture where people feel safe to speak up about risk. A team member who raises a concern is doing the right thing, not creating a problem. We address the systems that let risks materialise undetected. |
| Early Warning | Our KRIs are designed to give us early warning before a risk becomes a breach. KRIs provide a regular health check on our most important risk exposures and create the conditions for proactive management rather than reactive firefighting. |
| Stakeholder Trust | AUSMASA is a steward of public funding and a trusted partner to industry, government and unions. Our risk decisions must always reflect this responsibility. We protect our reputation, our relationships and our social licence to operate by managing risks with care and transparency. |
| Continuous Learning | Every risk incident, deep dive review and audit finding is an opportunity to improve. Lessons are captured, shared and acted upon. Our risk maturity grows with each cycle. |

# 4 Minimum Requirements (Policy)

AUSMASA must:

- Integrate risk appetite into all significant decisions, including new initiatives, partnerships and projects, by undertaking a documented risk appetite check prior to approval.
- Assess every identified risk against the relevant risk appetite level before a risk is accepted or closed.
- Ensure every strategic and operational risk always has a named Risk Owner at ED level and an assigned Risk Delegate.
- Apply standard likelihood, consequence and control effectiveness scales when assessing risks. Standard scoring tools must be used consistently across the organisation.
- Implement a documented risk treatment plan where residual risk exceeds appetite. Treatment plans must identify an owner, actions and timelines and be in place within 30 days.
- Escalate risk breaches promptly by reporting them to the Governance and Risk Team within 48 hours of identification.
- Report all material risks, including all high and extreme residual risks and all risk appetite breaches, through ELT and Board reporting.
- Ensure all staff complete all mandatory training within 30 days of commencing at AUSMASA.

- If invited, fully participate in scheduled and ad hoc deep dive risk reviews, including providing timely information and cooperation across all departments.

# 5 Risk Taxonomy

A consistent taxonomy allows AUSMASA to compare, aggregate, and report risks across the enterprise. Every risk in our register is classified using one of the following seven categories. Risk appetite is set by category in the Risk Appetite Statement.

| Category | Description | AUSMASA Examples |
|---|---|---|
| **Strategic** | Risks threatening long-term priorities within our Strategic Plan. | Misalignment of initiatives with strategic priorities. |
| **Financial** | Risks to funding security or financial sustainability | Grant underspend or overspend. |
| **Operational** | Risks affecting delivery, processes, systems, or service quality. | CRM system failure or cyber-attack. |
| **People** | Risks arising from employee-base, culture, or resourcing. | Key person dependency or low staff engagement. |
| **Reputation and Stakeholder** | Risks to AUSMASA's standing, trust, or relationships with key partners. | Poor collaboration with the unions or RTOs. |
| **Compliance** | Risks of breaching legal, regulatory, or contractual obligations. | Missed grant reporting deadlines or ACNC non-compliance. |
| **Integrity** | Risks to ethical conduct, conflicts of interest, and public trust. | Undisclosed conflicts of interest, misuse of public funds or breach of the Code of Conduct. |

# 6 Risk Management Process

AUSMASA follows the ISO 31000:2018 risk management process, adapted to our operating context as a JSC. The seven steps below are not sequential checkboxes, they form a continuous cycle that evolves with our environment. Risk management happens every day, in every department, through every project and initiative.

| Process Step | What We Do | Tools and Outputs |
|---|---|---|
| **1. Establish Context** | Define the scope, environment, and objectives against which risks will be assessed. This includes understanding our operating context as a JSC, grant obligations, strategic priorities, and industry environment. | • AUSMASA Strategic Plan 2025-28<br>• Stage II Grant Agreement<br>• Ministerial Statement of Priorities<br>• Environmental scan (industry, regulatory, political) |
| **2. Identify Risks** | Systematically identify events or conditions that could affect our ability to achieve objectives. Inputs include staff workshops, stakeholder | • Enterprise Risk Register<br>• Project Risk Assessment Tool<br>• DEWR reporting and feedback |

| | | |
|---|---|---|
| | feedback, incidents, industry intelligence, and horizon scanning. | |
| **3. Analyse Risks** | Assess the likelihood and consequence of each risk to determine inherent risk rating. Evaluate the quality and coverage of existing controls. | • Control Effectiveness Assessment Tool<br>• Inherent risk scoring against risk matrix |
| **4. Evaluate Risks** | Calculate residual risk (after controls). Compare against risk appetite thresholds. Determine whether risk is acceptable, requires monitoring, or needs a treatment plan. | • Residual risk score compared to Board appetite<br>• Escalation triggers activated where needed<br>• KRI alignment checked |
| **5. Treat Risks** | Develop and implement treatment plans for risks outside appetite. Select from the four treatment options: avoid, reduce, share/transfer, or accept. Assign owners and timeframes. | • Treatment plans in Risk Register<br>• Corrective Action/ Treatment Plan<br>• Vendor due diligence, procurement, contracts<br>• Shared risk arrangements with DEWR, other JSCs or our insurance provider |
| **6. Monitor and Review** | Track residual risks against appetite on an ongoing basis. Review control effectiveness. Monitor KRIs for early warning signals. Deep-dive reviews for high/extreme risks. | • Regular risk register reviews<br>• Key Risk Indicators (KRI) dashboard<br>• Annual deep-dive review schedule<br>• Board and ELT risk reporting cycle |
| **7. Communicate and Consult** | Ensure risk information is shared with the right people at the right time. Foster open risk dialogue across all levels of AUSMASA. | • ELT monthly risk agenda item<br>• Staff induction and ongoing awareness<br>• DEWR reporting in the form of Annual Progress Report |

### 6.1 Risk Identification in Practice

Risk identification is everyone's job. At AUSMASA we identify risks through:

- Regular risk workshops with each department (minimum annually).
- Project risk assessments completed before any activity project or initiative commences.
- Incident and near-miss reporting through our standard incident process on Employment Hero.
- Stakeholder feedback and complaints, which often surface risks before they appear in internal processes.
- Industry intelligence gathered through our SWAPs, Technical Committees (TC), and JSC CEO Network and Working Group meetings.
- Horizon scanning, which includes monitoring policy, regulatory, technology, and sector developments that could change our risk profile.
- Grant agreement milestones and the review of missed milestones or emerging delivery pressures are risk signals.

New risks must be logged in the Enterprise Risk Register within 5 business days of identification.

### 6.2 Monitoring and Review in Practice

Risk registers are not static documents. Every entry in our register must be reviewed at least quarterly. Review means:

- Checking whether the risk score has changed (and why).
- Confirming whether controls are still operating effectively.
- Updating the treatment plan status: is it progressing, stalled, or completed?
- Checking whether the risk remains within appetite or whether escalation is needed.
- Reviewing KRI readings for early warning signals.

For high and extreme residual risks, the Governance and Risk Team conducts a deep-dive review with the relevant Risk Owner at least twice per year, or when triggered by a KRI breach or significant change in operating conditions.

### 6.3 Shared and Emerging Risks

Some of AUSMASA's most significant risks are not entirely within our control. These include:

- Shared risks with DEWR, for example, risks related to grant agreement interpretation, policy changes, or reporting requirements
- Shared risks with other JSCs, for example, risks related to cross-sectoral training product development or shared stakeholder relationships
- Emerging risks are those not yet fully visible but which our horizon scanning suggests may become material

Shared risks must be documented in the risk register with clear notes about joint ownership and the mechanisms for coordination. Emerging risks must be documented even if their likelihood and consequence cannot yet be fully assessed.

## 7 Roles and Responsibilities

Good risk management requires clear accountability at every level. The table below defines who is responsible for what across AUSMASA.

| Role | Responsibility | Key Actions | Frequency / Trigger |
|---|---|---|---|
| **Board** | Ultimate accountability for risk culture and appetite | • Approve the ERMF and RAS annually<br>• Receive material risk and KRI reports<br>• Challenge adequacy of risk management<br>• Ensure alignment with grant obligations | Bi-monthly Board reports on risk |
| **RAF Committee** | Oversight of risk reporting, controls and assurance | • Review enterprise risk register (high/extreme risks)<br>• Oversee control effectiveness<br>• Commission deep-dive reviews<br>• Monitor KRI trends | At each committee meeting or at least quarterly |

| | | | |
|---|---|---|---|
| **CEO** | Organisational risk leadership and accountability | • Embed risk-aware culture<br>• Escalate material breaches to Board<br>• Ensure implementation of ERMF across all departments | Immediate escalation for material breaches |
| **ELT (Risk Owners)** | Departmental risk ownership and cross-functional coordination | • Own strategic and operational risks in their domain<br>• Ensure risk registers are current<br>• Support EDs as risk delegates<br>• Review and endorse treatment plans | Monthly ELT risk discussions and quarterly formal review |
| **Risk Delegates** | Day-to-day risk management and control implementation | • Maintain operational risk entries<br>• Identify and escalate emerging risks<br>• Ensure project risk assessments are completed<br>• Test and report on control effectiveness | Risk register updates at least quarterly |
| **Governance and Risk Team** | Framework custodianship, reporting and capability | • Maintain the ERMF, risk register, RAS and tools<br>• Coordinate deep dives and KRI monitoring<br>• Provide training and guidance<br>• Prepare board and ELT risk reports | Reports on standard cycle |
| **All Staff** | Risk identification and early warning | • Identify and report risks in daily work<br>• Participate in risk training<br>• Apply risk-aware thinking in decisions<br>• Complete risk assessments for their activities | Report risks promptly when identified |

# 8 Three Lines of Defence and Assurance

AUSMASA applies the three lines of defence model to ensure that risk management is embedded, independent, and assured at every level.

| Line | Who | Role in Risk Management | AUSMASA Examples |
|---|---|---|---|
| **First Line** | All staff, program managers, project coordinators | • Identify, own and manage risks day to day<br>• Implement controls<br>• Escalate when thresholds are approached | • EDs managing operational risk in their department<br>• Project managers using the Risk Assessment Tool |

| | | | |
|---|---|---|---|
| | | • Complete risk assessments for projects and activities | • Staff reporting incidents or near-misses in a timely way |
| **Second Line** | Governance and Risk Team, ELT - Risk Owners (EDs) | • Design and maintain the risk framework<br>• Monitor aggregate risk exposure<br>• Challenge risk assessments<br>• Report to Board and CEO<br>• Coordinate deep-dive reviews<br>• Monitor KRIs | • Governance and Risk team maintaining the enterprise risk register<br>• ELT reviewing risk trends each quarter<br>• CEO reporting material risks to the Board |
| **Third Line** | External Audit | • Independent assurance over risk management effectiveness<br>• Challenge adequacy of controls | • External audit review of internal controls |

# 9 Reporting and Escalation

AUSMASA operates a clear and structured reporting cycle. The table below sets out what is reported, to whom, and when. Our escalation framework uses four levels of breach response. Ask yourself: does this risk breach reach the Anywhere (strategic), Budget (financial), or Control (governance) test?

| Report / Activity | Audience | Frequency | Content |
|---|---|---|---|
| **Risk Register Review** | Risk Owners / ELT | Monthly | Update risk scores, control status, treatment progress and emerging risks |
| **KRI Dashboard** | ELT / CEO | Monthly | Traffic light status for all KRIs, trend analysis and escalation flags |
| **ELT Risk Discussion** | ELT | Monthly | Emerging risks, KRI alerts, treatment plan progress and cross-departmental issues |
| **RAF committee Update** | RAF committee | At least quarterly | High and extreme residual risks, KRI summary, appetite breaches and control effectiveness findings |
| **Board Risk Update** | Board | Bimonthly | Strategic risk profile, material risk summary, KRI heat map and appetite breach report |
| **Deep-Dive Review** | ELT / RAF committee | Bi-annually (or triggered) | Detailed review of one or two risk categories, control effectiveness, gap analysis and improvement actions |
| **DEWR Annual Progress Report** | DEWR | Annual | Risk and compliance status as required under the Stage II Grant Agreement |

The escalation table below defines how we respond when risks exceed appetite:

| Breach Category | Trigger | Escalate To | Required Action |
|---|---|---|---|
| **Minor** | Risk moves above appetite; single instance; no external consequence | Risk Delegate & Risk Owner (ED) | Document within 24 hours; implement corrective action; and monitor for recurrence. |
| **Moderate** | Residual risk remains above appetite after initial response; pattern of recurrence; stakeholder impact | Governance and Risk Team + ELT | Assess within 48 hours; develop corrective actions; include in ELT agenda; and weekly monitoring until resolved. |
| **Major** | Impact on strategic objective, funding, or compliance; reputational or legal consequence; financial impact >$50k | CEO and Board | Immediate notification to CEO and Report to the Board Chair within 5 business days. |
| **Critical** | Actual funding breach; regulatory non-compliance; data breach under Privacy Act; severe governance failure | Board Chair + DEWR | Same-day notification to Board Chair; DEWR notification as required; CEO-led response plan; and involvement of Law Enforcement if required. |

# 10 Risk Culture

Risk culture is the shared values, norms, and behaviours that shape how risk is understood and managed in practice. At AUSMASA, we aspire to a risk culture characterised by:

| Attribute | What It Looks Like at AUSMASA |
|---|---|
| **Psychological safety** | People raise risk concerns without fear of blame. Bad news travels up quickly without a fear of repercussion. |
| **Risk ownership** | Managers actively own their risks rather than treating the risk register as a compliance exercise. |
| **Proportionality** | Risk processes are proportionate to the decision at hand. Not every activity requires a full formal review. |
| **Growth mindset** | Incidents and near misses are treated as learning opportunities, not performance failures. |
| **Transparency** | Risk information flows openly across the organisation and to the Board. No one is surprised. |
| **Integration** | Risk thinking is embedded in planning cycles, project approvals, and everyday decisions. |

# 11 Key Terms and their Definitions

| Term | Definition |
|---|---|
| **Risk** | The effect of uncertainty on objectives. Risk can have positive or negative consequences and is assessed in terms of likelihood and consequence. |
| **Risk Appetite** | The amount and type of risk AUSMASA is willing to pursue or accept in the pursuit of its strategic objectives. |
| **Risk Tolerance** | The acceptable variation around a risk appetite level - the boundary within which we can operate before escalation is required. |
| **Inherent Risk** | The level of risk before any controls or mitigations are applied. Represents the worst-case scenario. |
| **Residual Risk** | The level of risk remaining after controls have been applied. This is the score compared against risk appetite. |
| **Control Effectiveness** | A rating of how well a control is designed and operating to reduce risk exposure: Strong, Moderate, Weak, or Absent. |
| **Risk Owner** | The ED responsible for managing a specific risk, including monitoring, treating, and reporting. |
| **Risk Delegate** | The individual (typically a manager or project coordinator) who manages a specific risk on behalf of the Risk Owner on a day-to-day basis. |
| **Material Risk** | A risk that, if realised, could significantly impact AUSMASA's objectives, reputation, operations, or compliance obligations. |
| **Breach** | A situation where a risk exceeds the stated appetite or tolerance, or where a control fails. |
| **Corrective Action** | A structured response to a risk breach or control failure. |
| **Deep-Dive Review** | A structured, detailed review of a specific risk category or high-rated risk, conducted bi-annually or when triggered. |
| **KRI** | Key Risk Indicator is a quantitative or qualitative measure that signals whether a risk is moving toward or beyond its appetite threshold. |
| **Three Lines of Defence** | A model for structuring accountability: first line (operational), second line (oversight), third line (independent assurance). |

# 12 Related Internal Policies, Procedures and Documents

This policy should be read alongside:

- AUSMASA Compliance Policy
- AUSMASA Delegation of Authority Policy and Procedure
- AUSMASA Work, Health and Safety Policy

# 13 Appendix A: Risk Assessment and Scoring

We use a standardised 5×5 risk matrix. All risks, strategic, operational, and project-based, are assessed using the same methodology. This ensures consistency across departments and over time.

## 13.1 The Three Scores

- Inherent Risk: The level of risk before any controls are applied (worst case). Score = Likelihood × Consequence.
- Control Effectiveness: An assessment of how well controls are designed and operating. Rated: Strong / Moderate / Weak / Absent.
- Residual Risk: The risk that remains after controls are applied. This is the score compared against risk appetite.

## 13.2 Likelihood Scale

| Score | Descriptor | Guidance |
|---|---|---|
| **1** | Rare | Highly unlikely; may occur only in exceptional circumstances; no precedent at AUSMASA |
| **2** | Unlikely | Possible but not expected; could occur in unusual circumstances; has occurred in similar organisations |
| **3** | Possible | Might occur at some point during the operating period; has occurred at AUSMASA previously |
| **4** | Likely | Expected to occur in most operating periods; recurs with some regularity; current conditions are conducive |
| **5** | Almost Certain | Expected to occur; may already be occurring; strong indicators present |

## 13.3 Consequence Scale

| Score | Descriptor | Examples of Impact on AUSMASA |
|---|---|---|
| **1** | Insignificant | Minimal operational impact; easily managed; no external effect; cost <$5k |
| **2** | Minor | Small delays; minor cost overrun; minor stakeholder concern; no reputational impact; cost $5k-$20k |
| **3** | Moderate | Moderate project delay; stakeholder dissatisfaction; some media interest; cost $20k-$50k; requires ELT attention |
| **4** | Major | Significant disruption to programs; reputational damage; adverse media; DEWR concern; cost $50k-$100k |
| **5** | Catastrophic | Critical failure; loss of funding; regulatory breach; severe reputational harm; cost >$100k; potential loss of JSC status |

## 13.4 Risk Rating Matrix

The matrix below shows how likelihood and consequence combine to produce a risk rating. Residual risk ratings are compared against risk appetite thresholds.

| | Rare (1) | Unlikely (2) | Possible (3) | Likely (4) | Almost Certain (5) |
|---|---|---|---|---|---|
| Catastrophic (5) | Medium | High | Extreme | Extreme | Extreme |
| Major (4) | Medium | Medium | High | High | Extreme |
| Moderate (3) | Low | Medium | Medium | High | High |
| Minor (2) | Low | Low | Medium | Medium | High |
| Insignificant (1) | Low | Low | Low | Low | Medium |

| Rating | Meaning | Required Response |
|---|---|---|
| Low | Within appetite; risk is manageable | Monitor periodically; no treatment plan required unless trend worsening |
| Medium | Generally within appetite; controls must be maintained | Review controls regularly; ensure owner is monitoring; consider treatment if trending up |
| High | Approaching or exceeding appetite; attention required | Treatment plan required within 30 days; executive oversight; quarterly tracking |
| Extreme | Outside appetite; immediate action required | Immediate escalation to CEO and Board; treatment plan within 5 days; fortnightly monitoring |

## 13.5 Control Effectiveness

| Rating | Meaning | Residual Risk Impact |
|---|---|---|
| Strong | Controls well-designed, consistently applied, regularly tested. Evidence documented. | Residual risk typically 3 levels below inherent |
| Moderate | Controls generally effective but may have gaps in design or consistency. | Residual risk typically 2 level below inherent |

| | | |
|---|---|---|
| Weak | Controls exist but are poorly designed, under-resourced, or inconsistently applied. | Residual risk close to inherent; limited reduction, typically 1 |
| Absent | No meaningful controls in place. | Residual risk equals inherent risk, which is 0 |

# 14 Document History and Contact Details

Version

| | |
|---|---|
| **Number** | 1 |
| **Version** | 1.0 |
| **Implementation date** | 04 2026 |
| **Review date(s)** | 04 2028 |
| **Next review date** | 04 2028 |
| **Review frequency** | ☐ Every year<br>☒ Every two years<br>☐ Every three years |

Revision History

| Revision date | Summary of amendments | Prepared by | Version |
|---|---|---|---|
| | | | |

Contact Details

| | |
|---|---|
| Owner | ☒ Board<br>☐ Chief Executive Officer<br>☐ Executive Director, Operations and Corporate Services |
| Contact officer | ☐ Head of People and Culture<br>☒ Manager, Governance and Risk<br>☐ Finance Business Partner |