# Risk Assessment Criteria

Document no: QD 5041

Version no: 7

Version date: 3/11/2022

Endeavour Foundation

# Contents

Purpose ..... 3
Scope ..... 3
Risk Assessment Criteria Scope ..... 4
Risk management process ..... 9
Figure 1 ISO 31000:2018 Risk Management Process ..... 9
Establishing the scope, context and criteria ..... 9
Risk assessment process ..... 11
Risk identification ..... 11
Table 1- Risk Categories ..... 12
Risk analysis ..... 13
Table 2 – Assessing Individual Control Effectiveness ..... 14
Table 3 – Overall Assessment of Control Effectiveness ..... 15
Table 4 – Assessing Control Effectiveness for Community Events ..... 16
Safety risk analysis ..... 17
Figure 2 – Hierarchy of Controls ..... 18
Assessing risk consequences ..... 19
Table 5 - Risk Category Consequences ..... 20
*Safety category ..... 20*
*Compliance category ..... 20*
*People, Brand and Reputation category ..... 21*
*Financial category ..... 22*
*Environment and Indigenous Heritage category ..... 22*
*Assets, Operations and Security category ..... 23*
Assessing risk likelihood ..... 24
Table 6 – Risk likelihood ..... 24
Table 7 – Community event likelihood ..... 24
Risk rating ..... 25
Table 8 - Risk Rating Matrix ..... 25
Risk evaluation and escalation ..... 25
Table 9 - Risk evaluation and escalation ..... 26
Communicate and consult ..... 27
Monitoring and reviewing ..... 27
Risk treatment ..... 27
Risk recording and reporting ..... 28
Risk assessments formally recorded in CORE ..... 28
Other risk assessment not formally recorded in Resolver CORE ..... 28
Related documents and references ..... 29

## Policies supported

QD 5027 Enterprise Risk Management Policy

QD 5028 Risk Appetite and Tolerance Policy

## Purpose

Endeavour Foundation Group's Risk Assessment Criteria has been developed to ensure that its risk assessment practice is applied consistently across the organisation.

This document complements other risk documents to support the implementation of Endeavour Foundation Group's Risk Management Plan and ***Risk Management Framework (QD 5006).***

## Scope

Endeavour Foundation Group's Risk Assessment Criteria applies to all Endeavour Foundation Group board members, executives, managers, senior leaders, leaders and employees at all locations.

In line with Endeavour Foundation Group's Risk Management Framework, this Risk Assessment Criteria applies to all types of risk assessments, in all areas of the organisation.

A summary table has been provided on the next pages to clearly identify the scope of where and when this Risk Assessment Criteria should be applied to risk assessments.

## Risk Assessment Criteria Scope

| Type of Risk | Risk Description | Who completes the risk assessment? | Which stakeholders participate? | Links to Goals or Objectives | How will I complete the risk assessment? Where are the risks recorded? |
|---|---|---|---|---|---|
| **Strategic** | **Strategic Risk Register**<br>risks related to the organisation's strategic direction, with risks having mostly external causes | • Head of Risk, Assurance & Quality<br>• Executive Leadership Team | • Board members<br>• Risk Team or other SME in NDVR review | **Business**<br>Linked to Endeavour Foundation Group's Strategic Plan | ✓ must apply ISO31000 best practice<br>✓ must use ***Risk Assessment Criteria (QD 5401)*** for the risk assessment<br>✓ formally record directly into the Integrated Risk Management System (CORE) Risk Module |
| **Corporate** | **Corporate Risk Report**<br>key operating and operational risks are aggregated to create a corporate risk report | • Risk Team | • Not applicable | Not applicable | ✓ aggregated and formally recorded in the CORE Risk Module |
| **Key Operating** | **Key Operating Risk Register**<br>risks related to the achievement of the organisational Operational Plan | • Senior Leaders<br>• Leaders | • Executive Team Member<br>• Risk Team<br>• other subject matter experts | **Business**<br>Linked to Endeavour Foundation Group's organisation Operational Plan | ✓ must apply ISO31000 best practice<br>✓ must use ***Risk Assessment Criteria (QD 5401)*** for the risk assessment<br>✓ approved Risk Assessment template ***Risk Assessment Tool A3 (QF 5041.01)*** (MS Word) or ***Risk Assessment Tool A4 (QF 5041.02)*** (MS Excel)<br>✓ formally recorded in the CORE Risk Module |

# Risk Assessment Criteria

| Type of Risk | Risk Description | Who completes the risk assessment? | Which stakeholders participate? | Links to Goals or Objectives | How will I complete the risk assessment? Where are the risks recorded? |
|---|---|---|---|---|---|
| **Operational** | **Operational Risk Register**<br>risks related to the achievement of the relevant business plan | • Senior Leaders<br>• Leaders<br>• Managers | • Executive Team Member<br>• Risk Team<br>• other subject matter experts<br>• other employees | **Business**<br>Linked to operational objectives in business planning documents at Division, Portfolio, Region or Site levels | ✓ must apply ISO31000 best practice<br>✓ must use ***Risk Assessment Criteria (QD 5401)*** for the risk assessment<br>✓ approved Risk Assessment template ***Risk Assessment Tool A3 (QF 5041.01)*** (MS Word) or ***Risk Assessment Tool A4 (QF 5041.02)*** (MS Excel)<br>✓ some site operational risk assessments may be informally recorded; saved in a local location; business solutions sites operational risk assessments are formally recorded in the CORE Risk Module<br>✓ regions, portfolios and division operational risk assessments are formally recorded in the CORE Risk Module |
| **Project** | **Project Risk Register**<br>risks related to the completion of the project | • Project Manager<br>• Project Team<br>• Third party contractors (if relevant) | • Executive Team Member<br>• Risk Team<br>• other subject matter experts<br>• other employees working on the project<br>• other stakeholders | **Business**<br>Linked to project plan objectives and outcomes<br>May be linked to business plan or operational plan | ✓ must apply ISO31000 best practice<br>✓ must use ***Risk Assessment Criteria (QD 5401)*** for the risk assessment<br>✓ approved Risk Assessment template ***Risk Assessment Tool A3 (QF 5041.01)*** (MS Word) or ***Risk Assessment Tool A4 (QF 5041.02)*** (MS Excel) informally recorded; saved in a local location |

# Risk Assessment Criteria

| Type of Risk | Risk Description | Who completes the risk assessment? | Which stakeholders participate? | Links to Goals or Objectives | How will I complete the risk assessment? Where are the risks recorded? |
|---|---|---|---|---|---|
| **Safety** | **Safety Hazard Identification and Risk Assessment**<br>identify hazards and exposures; complete a safety risk assessment (assess the risks, control the risks; review the controls and assess their effectiveness; evaluate whether the risks are acceptable at the managed risk level) | • Relevant Leader (e.g., Site Manager; Operations Manager)<br>• Site employees | • Internal safety team member<br>• other subject matter experts (internal or external)<br>• other stakeholders<br>• other employees | **Safety**<br>In line with legislative requirements<br>**Business**<br>Linked to operational objectives for the site – business plans | ✓ must apply ISO31000 best practice<br>✓ must use ***Risk Assessment Criteria (QD 5401)*** for the risk assessment<br>✓ approved template ***WHS Hazard Id Risk Assessment and Control Form (QF 4050.01)*** informally recorded; saved in a local location |
| **Activity** | **Activity Risk Assessment**<br>risks related to planning and delivering new activities at sites or as part of future business planning (this includes Safety risk) | • Employees planning to undertake new activities that have not previously been assessed | • Person we support<br>• Person's family/guardian/ other person who is a decisionmaker<br>• other subject matter experts<br>• team members who will facilitate the activity<br>• other contractors<br>• other subject matter experts | **Personal**<br>• may be linked to Individual Support Plan goals<br>**Business**<br>• Linked to operational objectives for the site, region, portfolio or division – business plans | ✓ must apply ISO31000 best practice<br>✓ must use - ***Risk Assessment Criteria (QD 5401)*** for the risk assessment<br>✓ approved Risk Assessment template ***Risk Assessment Tool A3 (QF 5041.01)*** (MS Word) or ***Risk Assessment Tool A4 (QF 5041.02)*** (MS Excel) informally recorded; saved in a local location |

# Risk Assessment Criteria

| Type of Risk | Risk Description | Who completes the risk assessment? | Which stakeholders participate? | Links to Goals or Objectives | How will I complete the risk assessment? Where are the risks recorded? |
|---|---|---|---|---|---|
| **Personal** | **Personal Risk Assessment**<br>risks related to the achievement of a person's goals recorded in the Individual Support Plan (may also include an Advance Medication Risk Assessment or other relevant risk assessments) | • Leaders and Employees who support the person (e.g., Site Supervisor/ Manager, Support Workers, Employment Coaches) | • Person we support<br>• Person's family/guardian/ other person who is a decisionmaker<br>• other subject matter experts (internal or external)<br>• other stakeholders | **Personal**<br>Linked to the person's goals outlined in the Individual Support Plan or other planning documents | ✓ must apply ISO31000 best practice<br>✓ must use ***Risk Assessment Criteria (QD 5401)*** for the risk assessment<br>✓ approved ***Personal Risk Assessment (QF 1100.19)*** form informally recorded; saved in a local location<br>✓ approved Risk Assessment template ***Risk Assessment Tool A3 (QF 5041.01)*** (MS Word) or ***Risk Assessment Tool A4 (QF 5041.02)*** (MS Excel) informally recorded; saved in a local location<br>✓ ***Advanced Medication Risk Assessment Form (QF 5301.04)*** informally recorded; saved in a local location |
| **Security** | **Security Risk Assessment**<br>risks related to cyber and information security to identify vulnerabilities and weaknesses in controls that may lead to greater risks at the organisational level | • Employees reviewing security exposures | • Employees<br>• Third party contractors<br>• ICT Security Manager (or ICT security employee)<br>• other subject matter experts | **Business**<br>Linked to operational objectives for the site, region, portfolio or division – refer to business planning documents | ✓ must apply ISO31000 best practice<br>✓ must use ***Risk Assessment Criteria (QD 5401)*** for the risk assessment<br>✓ approved Risk Assessment template ***Risk Assessment Tool A3 (QF 5041.01)*** (MS Word) or ***Risk Assessment Tool A4 (QF 5041.02)*** (MS Excel) informally recorded; saved in a local location |

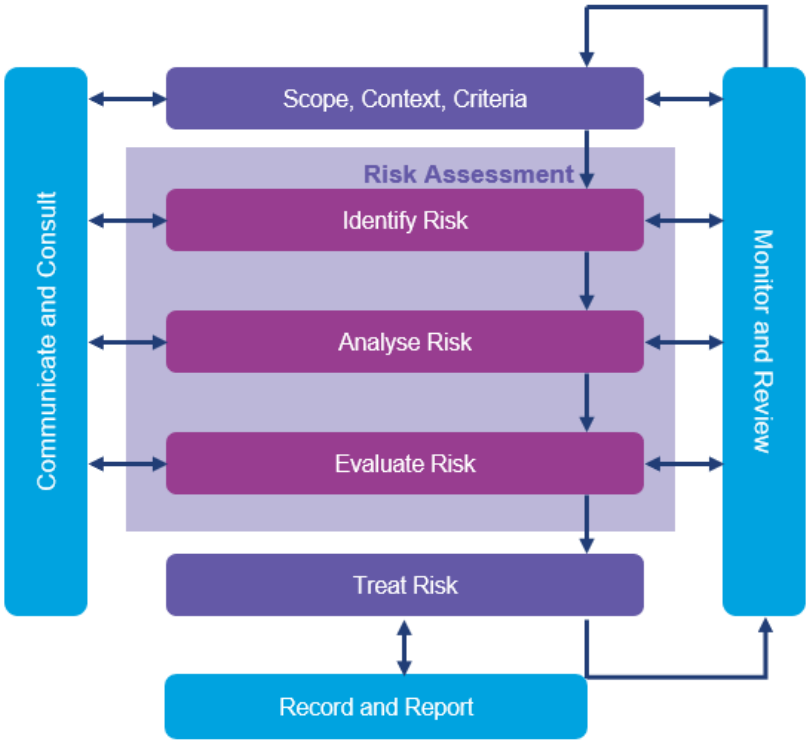
# Risk Assessment Criteria

| Type of Risk | Risk Description | Who completes the risk assessment? | Which stakeholders participate? | Links to Goals or Objectives | How will I complete the risk assessment? Where are the risks recorded? |
|---|---|---|---|---|---|
| **Community Event** | **Community Event Risk Assessment**<br>risks related to planning and delivering community events (e.g. Great Endeavour Rally or local community events) | • Employees planning community events (example – Great Endeavour Rally, open site day etc) | • Employees and contractors involved in the event<br>• Supporters<br>• Sponsors<br>• other subject matter experts | **Business**<br>• Linked to operational objectives in business planning or event planning/ management documents | ✓ must apply ISO31000 best practice<br>✓ must use ***Risk Assessment Criteria (QD 5401)*** for the risk assessment<br>✓ approved Risk Assessment template ***Risk Assessment Tool A3 (QF 5041.01)*** (MS Word) or ***Risk Assessment Tool A4 (QF 5041.02)*** (MS Excel) informally recorded; saved in a local location informally recorded in local location; > 2023 formally recorded in CORE |
| **Other** | **Other Risk Assessment**<br>a risk assessment completed for a particular purpose not covered by the above types of risk assessments | • Employees involved in the subject matter of the risk assessment | • Employees<br>• Third party contractors<br>• other subject matter experts | **Business**<br>Linked to operational objectives for the site, region, portfolio or division – refer to business planning documents | ✓ must apply ISO31000 best practice<br>✓ must use ***Risk Assessment Criteria (QD 5401)*** for the risk assessment<br>✓ approved Risk Assessment template ***Risk Assessment Tool A3 (QF 5041.01)*** (MS Word) or ***Risk Assessment Tool A4 (QF 5041.02)*** (MS Excel) informally recorded; saved in a local location |

## Risk management process

Endeavour Foundation Group adopts the International Best Practice Standard ISO31000 Risk Management Process (2018) which is outlined in Figure 1.

**Figure 1 ISO 31000:2018 Risk Management Process**




**Source**: ISO 31000:2018 Risk Management Guidelines

## Establishing the scope, context and criteria

### Scope

Before commencing a risk assessment, ensure that you have established the scope.

For example, identify who will be involved, what the subject matter includes (or highlight what it does not include), how will the assessment be undertaken, why is this assessment important and where the assessment applies.

You may also include any other information that you believe is relevant to the scope of the risk assessment.

# Risk Assessment Criteria

## Context

Establishing the context is very important in the risk assessment process. A well-researched and thought-out context provides clear boundaries and understanding of what was happening at a particular point in time.

Clearly defining "why" the risk assessment is being completed and ensuring all stakeholders are an active part of the process is essential. To be able to recognise a risk you must first know and understand what is at risk; therefore setting, establishing, or defining the scope and context is very important.

## Criteria

Endeavour Foundation Group's approved Risk Assessment Criteria enables all employees to apply the same tables and matrix to analyse and evaluate risk consistently across the organisation. This version of the Risk Assessment Criteria also supersedes the Events Risk Assessment Criteria which was previously used for large community events or fundraising activities.

## Acceptable risk – risk appetite and tolerance

The Board and the Executive Leadership Team have set their appetite and tolerance to support effective risk decision making. In determining whether a risk is acceptable at the managed level, ***Risk Appetite and Tolerance Policy (QD 5028)*** should be reviewed.

If the risk is considered to be managed and is acceptable, there would be no further action required. The Risk Owner would then monitor and review the risk in line with the timeframes outlined in the ***Enterprise Risk Management Framework (QD 5006)*** and in the Risk evaluation and Escalation table.

## Determining the Risk Owner

The Risk Owner is the person who is accountable with the delegation and authority to approve risk treatments, make decisions, communicate, monitor, review and reassess risk. Where risks are assessed as high or extreme, the Risk Owner must escalate the risk in line with **Table 9** (Risk evaluation and Escalation table).

All risk-based decision making should be documented. If the risk is not acceptable, the risk assessment process will continue to determine the appropriate treatment options to reduce the level of risk. In designing a risk treatment plan, the costs and efforts must be balanced with the benefits or opportunities. This will enable a risk to be reduced So Far As Is Reasonably Practicable (SFAIRP).

# Risk assessment process

The risk assessment process has three (3) parts:

1. **Risk identification**
   - risks are described to enable another person in the organisation to understand the risk
   - risk must be written to identify a future event that needs to be managed
   - risks are assigned a category or in some cases, a primary and a secondary category
2. **Risk analysis**
   - risk controls (currently in place) are identified and evaluated
   - risk is analysed and provided a consequence and likelihood rating
   - the risk category may require adjusting during analysis
3. **Risk evaluation**
   - the purpose of evaluating risk is to decide whether the level of risk is acceptable
   - if treatments are required, a detailed risk treatment plan should be designed

## Risk identification

Once a risk has been identified, reference should be made to Table 1 to identify the primary risk category. You may also consider whether other risk categories apply to affirm the consequence level later on in the process.

At Endeavour Foundation Group we write our risk descriptions in the following structure:

**There is a risk of** <INSERT RISK> **resulting in**

<INSERT MOST LIKELY CONSEQUENCE>

- What is a risk? A risk is a future event that we do not want to happen.
- The future event would impact our achievement of our objectives.
- It is recommended that you review your risk description to ensure *it is a risk* and not a ***cause or consequence*** of a future event.

# Risk Assessment Criteria

## Table 1- Risk Categories

This table identifies each of the 6 risk categories that are used to group risks for reporting.

| Safety | Compliance | Assets, Operations and Security |
|---|---|---|
| Protecting and ensuring safety of our people from harm, injury, neglect, exploitation or death<br><br>All operations, services, programs and activities promote the wellbeing, health and safety of all people<br><br>Harm to a person includes the entire person (physical, medical, psychological, social, emotional, financial, ethical, spiritual or cultural) | Managing our compliance obligations, requirements, registrations and verification activities<br><br>Examples:<br>• laws or regulations (e.g., Work Health and Safety, National Standards for Disability Services, National Standards for Mental Health Services)<br>• NDIS Framework, practice standards and requirements<br>• contractual obligations<br>• codes (legal and voluntary)<br>• standards, accreditations, and certifications<br>• quality assurance activities<br>• internal policies, frameworks procedures and requirements<br>• stakeholders, community and social expectations | **Assets** are owned or in the care, custody or control of Endeavour Foundation Group. Asset condition, reliability, accessibility and capability should be considered, along with operations, services, programs or activities that are dependent upon the asset<br><br>**Operations** includes services, programs, events or activities. People who we support or provide services or programs to are front of mind, along with delivery of orders for our commercial customers. We are prepared for disruption by ensuring currency and availability of our business continuity plans to ensure continuity of our internal processes, systems, operations, services, programs and activities. We invite members of the public and our stakeholders to participate in a range of planned activities. Events are carefully planned with contingency plans in place and safety and compliance are front of mind at all times. We focus on continuous improvement in all we do<br><br>**Security**: We protect our sensitive, personally identifiable information and corporate data. We protect and ensure availability of data within our critical systems or assets or third-party platforms. We insure, protect and secure our technology and other assets |

| Financial | People, Brand and Reputation | Environment and Indigenous Heritage |
|---|---|---|
| Financial position or exposure, for example, events impacting on net surplus, cash flow, credit and capital adequacy<br><br>Financial viability, **e**xposure, performance, liabilities<br><br>Fraud and corruption exposure, crime, intent, committing fraud to obtain something for themselves or others; dishonesty, falsifying data or documents, intentional misuse of funds, fraud investigations | **People**: Our people are our single most important asset, yet also our most vulnerable. People includes people we interact with, support, provide services, programs, events or activities to, and extends to people we partner with to achieve outcomes<br><br>We plan and deliver services, program, events and activities to people with their needs, interests and goals front of mind and we have capacity and capability to deliver efficient services, programs and activities. e act as a responsible, corporate citizen, we are committed to creating an environment where people are empowered to the full extent of their capabilities. Our employees are expected to conduct themselves with a high degree of integrity, to respectfully strive for excellence and delivery of outcomes. There is zero tolerance for bullying, harassment and discrimination<br><br>**Human Rights**: We respect and uphold the rights of all people based on principles of dignity, equality and mutual respect and shared across cultures, religions, abilities and philosophies are respected. We promote individual rights to choose and have freedom of expression and decision-making. In line with the **National Standards for Disability Services** and the **NDIS Quality & Safeguarding Framework**, we uphold the right to dignity and respect, to live free from abuse, neglect, violence and exploitation to participate inclusively in the community. We renounce modern slavery practices and continue to review our practice and the practices of those we affiliate with or establish commercial partnerships/arrangements<br><br>**Brand and Reputation**: We protect our brand and reputation and listen to our collective community or industry stakeholders. Negative perception or interest may be created through all forms of media, industry chatter or legal challenges that may impact our reputation | **Environment**: All processes, systems, and procedures we employ to ensure that our activities do not adversely impact the environment which includes flora, fauna, amenity and cultural significance<br><br>**Indigenous Heritage**: Native title recognises the rights of indigenous peoples to own their traditional land and waters recognised by common law. |

## Risk analysis

### Assessing control effectiveness

Control effectiveness is a subjective test that we use to identify whether a control is fully developed and implemented and assess whether the controls are effective in managing the risk. Control effectiveness represents an important measure that is applied to determine the current level of control compared with that which is reasonably achievable. If the control effectiveness is at the bottom end of the scale (i.e., none or largely ineffective), the control owner must take steps to further treat the risk by either improving the effectiveness and adequacy of existing controls or by providing further controls.

Controls may be preventative to reduce the likelihood of negative consequences. Control/s must be both adequate (valid) i.e., planned, designed correctly and address all causes and consequences; and be effective (i.e. operate as intended).

**Individual control effectiveness**

Table 2 should be used to assess the effectiveness of an individual control. It is recommended that the individual control table is used when assigning and specifically evaluating the effectiveness of one control.

**Overall assessment of control effectiveness**

Table 3 should be used to assess the overall effectiveness of a group of controls. For example, when reviewing the collective group of controls that are currently in place and operating to manage the risk.

**Assessing Control Effectiveness for Community Events**

Table 4 should be used when you are completing a risk assessment for a community event. Assess the effectiveness of a group of event controls.

## Table 2 – Assessing Individual Control Effectiveness

| Criteria | None (N) | Largely ineffective (LI) | Partially effective (PE) | Substantially effective (SE) | Effective (E) |
|---|---|---|---|---|---|
| Summary | No controls in place | Rating indicates treatments are required as controls do not reduce/maintain level of risk | Rating indicates a need for improvement in controls to reduce or maintain the level of risk | Rating indicates good risk management and a control framework that is nearing 'effective' | Rating indicates that the risk is controlled |
| Documenting controls | ☐ no control exists *or*<br>☐ designed controls may not yet be operating | ☐ no documentation is in place *or*<br>☐ documentation about the controls is limited | ☐ controls are partially documented (omits information and hinders understanding) | ☐ controls are documented and able to be understood | ☐ controls are well documented and easy to understand |
| Design of controls | | ☐ no controls have been designed | ☐ design of controls is incomplete | ☐ controls have been designed | ☐ controls are well designed |
| Implementing controls | | ☐ no controls can be implemented until they are designed *or*<br>☐ controls may be designed but not implemented *or*<br>☐ control implementation fails *or*<br>☐ control implementation is problematic *or*<br>☐ no clear communication | ☐ controls require redesign *or*<br>☐ controls are correctly designed but may not be operating effectively *or*<br>☐ controls are implemented inconsistently *or*<br>☐ controls are poorly communicated to stakeholders | ☐ controls are typically applied consistently<br>☐ strengthening of stakeholder communication may be required | ☐ controls are implemented and operating as designed<br>☐ controls are applied consistently<br>☐ effective stakeholder communication |
| Monitor, review and redesign of controls | | ☐ limited monitoring and review of controls<br>☐ controls need to be redesigned to operate as intended | ☐ periodic monitoring and review of controls<br>☐ controls need to be reviewed and improved | ☐ ongoing monitoring of control effectiveness or reliability of the control is required for continuous improvement | ☐ controls are regularly monitored and review for continuous improvement<br>☐ controls are effective and do not require any changes |
| Control ownership | | ☐ control owners may not have been identified or notified | ☐ control owners recognise their responsibility for controls within their delegation of authority | ☐ control owners accept responsibility for controls within their delegation of authority | ☐ control owners actively demonstrate responsibility for controls within their delegation of authority |

## Table 3 – Overall Assessment of Control Effectiveness

| Criteria | None (N) | Largely ineffective (LI) | Partially effective (PE) | Substantially effective (SE) | Effective (E) |
|---|---|---|---|---|---|
| Summary | No controls in place | Rating indicates treatments are required as controls do not reduce/maintain level of risk | Rating indicates a need for improvement in controls to reduce or maintain the level of risk | Rating indicates good risk management and a control framework that is nearing 'effective' | Rating indicates that the risk is controlled |
| Document controls | ☐ no control exists *or*<br>☐ designed controls may not yet be operating | ☐ no documentation is in place *or*<br>☐ documentation about the controls is limited, with little awareness which requires immediate remedy | ☐ controls are partially documented (omits information and hinders understanding) *or*<br>☐ controls are documented with some inadequacies | ☐ controls are documented and generally well understood | ☐ controls are well documented and understood |
| Design controls | | ☐ no controls have been designed *or*<br>☐ poor control design compromises the management of risk<br>☐ significant exposures have been noted that will likely result in loss | ☐ design of controls is incomplete. Several exposures that could result in loss have been noted<br>☐ during design, several weaknesses have been identified which could compromise management of risk, controls require redesign | ☐ controls have been designed, some risk exposures have been noted and, if not addressed, could result in loss<br>☐ during design, some weaknesses may be identified but when aggregated, do not compromise management of risk | ☐ controls are well designed |
| Implement controls | | ☐ no controls can be implemented until they are designed *or*<br>☐ implemented controls fail to effectively mitigate the risk stakeholders are not aware of the risk and/or controls | ☐ controls are correctly designed but may not be operating effectively *or*<br>☐ controls are implemented inconsistently *or*<br>☐ several weaknesses may have been identified<br>☐ controls are poorly communicated to stakeholders; greater awareness is required | ☐ controls are typically applied consistently and are effective<br>☐ during implementation, some weaknesses may be identified but when aggregated, do not compromise the management of risk<br>☐ stakeholder communication may require strengthening | ☐ key controls are in place and are operating effectively, controls appropriately and consistently mitigate risks |
| Monitor, review and redesign controls | | ☐ limited monitoring and review of controls<br>☐ controls need to be redesigned to operate as intended | ☐ periodic monitoring and review of controls *or*<br>☐ controls require review for improvement | ☐ ongoing monitoring of control effectiveness or reliability of the control is required for continuous improvement | ☐ ongoing monitoring of control effectiveness or reliability of the control is required for continuous improvement<br>☐ identified opportunities to improve, but little overall impact |
| Control owner/s | | ☐ control owners may not have been identified or notified | ☐ control owners recognise their responsibility for controls within their delegation of authority | ☐ control owners accept responsibility for controls within their delegation of authority | ☐ control owners actively demonstrate responsibility for controls within their delegation of authority |

## Table 4 – Assessing Control Effectiveness for Community Events

| Criteria | None (N) | Largely ineffective (LI) | Partially effective (PE) | Substantially effective (SE) | Effective (E) |
|---|---|---|---|---|---|
| Control framework in place | ☐ No controls in place | ☐ Control framework is not appropriate to adequately manage the risk, additional risk treatments are a priority | ☐ Control framework requires improvement to be effective, revision of a treatment plan is required | ☐ Good risk management and control framework operating as intended most of the time | ☐ Minimal uncontrolled risk |
| Controls are developed, implemented and operating as intended | ☐ No controls exist or have been implemented to manage the risk | ☐ Little to no controls in place or controls are not yet fully implemented | ☐ Controls may be correctly designed but may not be operating as intended or effectively | ☐ Controls may be well designed and documented, but may not be applied consistently to operate effective | ☐ Controls are fully developed, implemented and are operating as intended |

## Safety risk analysis

As part of the risk assessment process, risks that fall within the Safety category should also ensure that the most effective control measures (that are reasonably practicable in the circumstances) are identified and managed.

Figure 2 identifies the 3 levels of the hierarchy of control adopted by Endeavour Foundation Group.

**Managing risks with effective controls (hierarchy of control measures)**

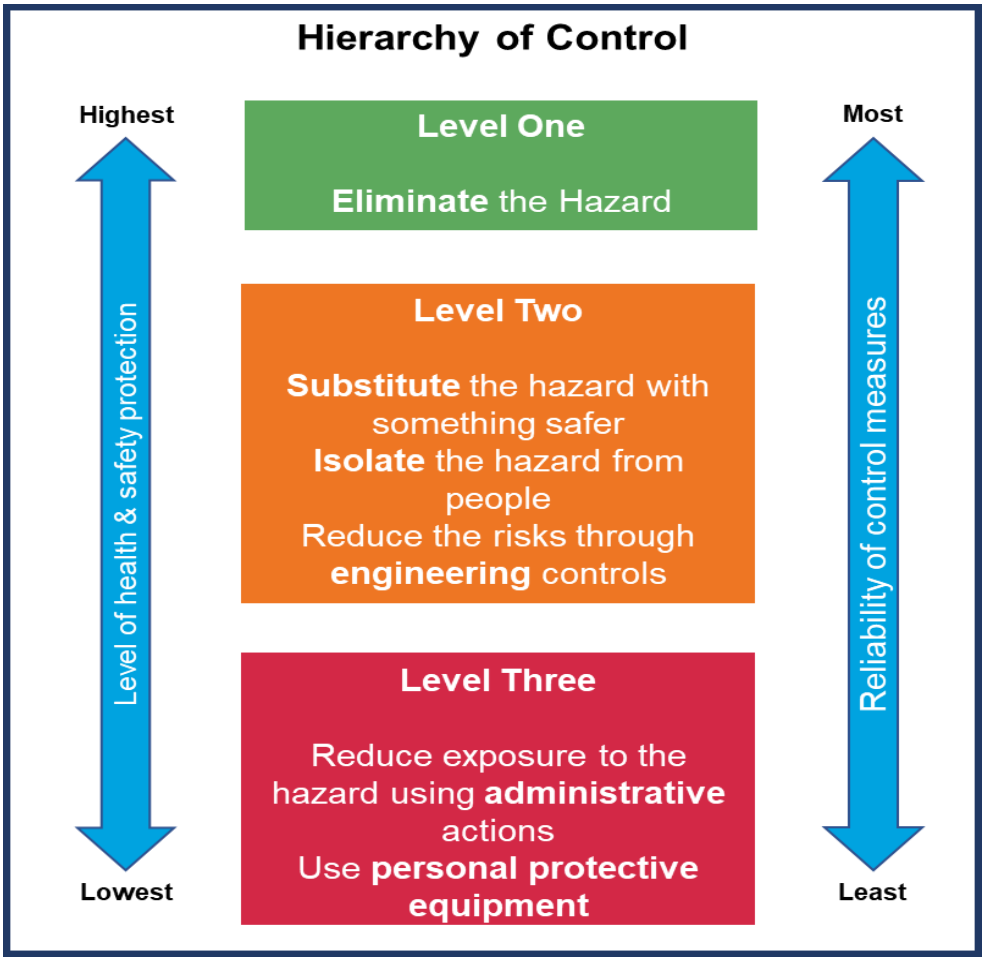
As part of the safety risk assessment process, we identify the hazards and the exposures to those hazards. We then can identify and assess the risks. A part of this process is identifying the controls that are currently in place to manage the risks and self-assessing the effectiveness of those controls to manage the risks.

When we seek to manage risks, we rely on the design and implementation of the controls. We rank these controls from the highest level of protection and reliability to the lowest level of protection and unreliability (further treatments are needed). This ranking is known as the hierarchy of control measures.

The hierarchy of control measures can be applied in relation to any safety related risk. While we aim to eliminate the risk, this is not always reasonably practicable, and you must minimise the likelihood and consequences of the risk by working through the other alternatives in the hierarchy. Administrative controls and Personal Protective Equipment (PPE) are the least effective at minimising risk because they do not control the hazard at the source and rely on human behaviour and supervision.

**Figure 2** (over the page) outlines the Hierarchy of Controls.

**Figure 2 – Hierarchy of Controls**




**What is reasonably practicable?**

Deciding what is reasonably practicable to protect people from harm requires those involved in the risk assessment taking into account and considering all the relevant information related to the hazard and risk, including:

- the likelihood of the hazard or risk occurring;
- the degree of harm that might result from the hazard or risk;
- knowledge about the hazard or risk, and ways of minimising or eliminating the risk;
- the availability and suitability of ways to eliminate or minimise the risk; and
- after assessing the extent of the risk and the available ways of eliminating or minimising the risk, the cost associated with available ways of eliminating or minimising the risk, including whether the cost is grossly disproportionate to the risk.

## Assessing risk consequences

Identify the risk category/categories that are relevant and review the descriptions in Table 5 to determine which rating descriptor best describes the risk consequences.

### Primary risk category

1. Identify the primary category of risk. Select the category with the greatest consequences.
2. Review the descriptions for the risk category in Table 5 to determine which descriptor best describes the consequences of the risk. This is your consequence rating.

   *For example, the primary risk category is Safety. After reading the descriptions for each level of consequences, Major (4) is selected as the consequence rating for the risk.*

### Secondary risk categories

1. If you have secondary risk categories, apply the same process as above.
2. Make a decision to record your primary risk category level or average the consequence ratings for the categories; or
3. Where there is a secondary category with a consequence level significantly higher than a primary risk category, you may wish to reassign that category as the primary category and record this consequence rating.

   *For example, the secondary risk category is Compliance. After reading the descriptions for each level of consequences, Severe (5) is selected as the consequence rating for the risk. A decision is made to record the higher consequence rating and to make Compliance the primary risk category.*

## Table 5 - Risk Category Consequences

**Safety category** any injury, illness or death caused by harm, neglect, exploitation, serious abuse, error or omission or failure

| Minimal (1) | Minor (2) | Moderate (3) | Major (4) | Severe (5) |
|---|---|---|---|---|
| ☐ near miss; no injury; no illness | ☐ first aid required for injury or illness | ☐ medical advice and/or treatment required for injury or illness | ☐ emergency services and/or ongoing medical advice/treatment for injury or illness<br>☐ restricted from routine activities; lost time injury | ☐ emergency services and hospital admission for injury or illness<br>☐ permanent disability or fatality<br>☐ termination of routine activities; multiple lost time injuries |
| **Community Events:**<br>☐ first aid, little to no disruption | **Community Events:**<br>☐ first aid and/or professional medical advice; (1-10 people); minor event change or delay | **Community Events:**<br>☐ first aid and/or professional medical advice (> 10 people); disrupts or delays part of the event | **Community Events:**<br>☐ emergency services and medical support or treatment (10-20 people); < 10 hospital admission; event paused/delayed | **Community Events:**<br>☐ emergency services; medical support or treatment (> 20 people); > 10 hospital admissions; event termination |

**Compliance category** includes any breach of law, regulation, licence, accreditation, registration, or contractual obligation. Noncompliance with relevant legislation, standards and frameworks including the National Standards for Disability Services, Mental Health Services or other national standards with which we must comply

| Minimal (1) | Minor (2) | Moderate (3) | Major (4) | Severe (5) |
|---|---|---|---|---|
| ☐ notification of non-conformance and/or non-compliance or provisional improvement notice<br>☐ third-party claims/ contract dispute payments $5K to < $50K below deductible limits | ☐ non-conformance is easily remedied; non-compliance is easily resolved<br>☐ corporate fine; or prosecution; or monetary loss to < 50K; third-party claims/contract dispute payments $25K to < 100K below deductible limits | ☐ additional resources to remedy non-conformance/non-compliance; temporary restriction of licence, registration, certification, accreditation, or contract - possible disruption to 1 or more critical business activity<br>☐ corporate fine; or prosecution; or monetary loss $50K to < $500K; third-party claims/contract dispute payments $50K to < $500K below deductible limits | ☐ non-conformance or non-compliance is not easily remedied or rectified and requires significant redeployment of resources; stop work notice, prohibition or accreditation, licence, registration, certification is revoked; threat of contract termination; major disruption of multiple critical business activities (1+ sites)<br>☐ corporate fine; or prosecution; or monetary loss $250K to < $1MIL; multiple third-party claims; or contract dispute payments of $250K to < $1MIL below deductible limits | ☐ limited or no opportunity to remedy, rectify or reinstate multiple accreditations, licences, certifications, registrations within reasonable timeframes; multiple contracts are rescinded, terminated or withdrawn; extreme disruption to multiple critical activities (multiple sites)<br>☐ corporate fine, prosecution or monetary loss, executive/employee charges/jailed $500,000 to < $5MIL loss; multiple third-party claims or contract dispute payments of $500K to < $5MIL above insurable limit of liability |
| **Community Events:**<br>☐ non-compliance is easily prevented during planning; event continues as scheduled | **Community Events:**<br>☐ a minor part of the event is deemed non-compliant; non-conformance is easily remedied; event continues as scheduled | **Community Events:**<br>☐ a major component of the event is deemed non-compliant, additional resources required to remedy; event postponed | **Community Events:**<br>☐ multiple components of the event are deemed non-compliant; redeployment of resources is required to remedy, event is postponed/cancelled: consequences include fines; loss; prosecution; or legal action | **Community Events:**<br>☐ event is deemed non-compliant, with insufficient resources available to remedy within required timeframes, event is postponed/ cancelled; consequences: fines; loss; prosecution; or legal action |

**People, Brand and Reputation category** includes people we support, clients, participants, commercial customers; trainees, apprentices or other stakeholders any event or series of events which creates a negative perception of our capability and capacity to deliver safe and efficient services, or act as a responsible corporate citizen. We respect all people and upholding human rights, right to privacy, commitment to eradication of modern slavery. We uphold individual rights to freedom of expression, self-determination and decision-making; encourage meaningful participation and inclusion, we plan for individualised outcomes to achieve personal goals; we seek feedback; we manage access, commencement and leaving a service transparently, equitably, fairly and in a responsive way. We have effective accountable management and leadership.

| Minimal (1) | Minor (2) | Moderate (3) | Major (4) | Severe (5) |
|---|---|---|---|---|
| ☐ *an individual* expresses dissatisfaction with operations, services, programs; activities; or professional relationship; issue is quickly remedied with minimal consequences | ☐ *multiple people* express dissatisfaction with operations, services, programs; activities; or professional relationship; minor consequences | ☐ *multiple people continue to be dissatisfied;* manageable change is required; review of continuity plans may be required | ☐ *multiple people continue to be dissatisfied* and *terminate participation or professional relationship*; possible disruption to critical business activities | ☐ *multiple people terminate participation or professional relationships;* operational impacts require significant resource redeployment to ensure continuity of critical business activities |
| ☐ little or no interest from external groups – individual impacts; minimal loss of confidence and limited negative media | ☐ interest to local community members; loss of community confidence is easily restored; occasional once off negative media attention | ☐ increasing interest and community discussion; loss of community confidence may require a plan to rebuild and restore relationships; increasing negative media or community discussions; negative media attention (> 3 days); local or regional media coverage | ☐ high interest to local community; possible concern broadened to state or national level; significant loss of community confidence requires targeted plan to restore brand and reputation; ongoing negative media attention (> 1 week); increase in negative social media (x 3 average); strategy is required to manage and resolve; state/national media coverage likely | ☐ high interest to all stakeholders at all levels due to major public concerns raised; large-scale class action; confirmed breaches with administrative, judicial or other remedies; legal action is unable to be resolved/settled out of court (significant cost and reputation damage) |
| ☐ informal questioning of commitment to human rights, privacy, reconciliation and ending modern slavery practices | ☐ local resolution of complaints or concerns re action/inaction that contravenes human rights; breach of privacy; breach of code of conduct or commitment to eradicating modern slavery are resolved locally, supported by internal teams | ☐ formalised allegations in relation to action/inaction that contravenes human rights; code of conduct; commitment to reconciliation; and/or eradicating modern slavery; complaints are investigated internally, taking time to resolve; allegations or threats of legal action resolved/settled out of court; breaches may require administrative, judicial or other remedies | ☐ multiple formalised allegations require internal investigation, in conjunction with an investigation by an external stakeholder/body; process takes significant time to investigate and provide an outcome; breach results in administrative; judicial; or other remedies; threats of legal action required resources to be redeployed and are resolved/settled out of court | ☐ ongoing community concerns (> 3 weeks) continue, complaints are formalised at all levels; a prescribed timeframe is outlined to investigate and provide an outcome |
| | | | | ☐ significant loss of community/stakeholder confidence, irreparable reputation damage; weeks of adverse regional, state or national media attention and/or reporting to government bodies; increasing negative social media requires targeted strategy to manage and resolve |

**Financial category** any expected or confirmed loss caused by error; fraud; overrun; failure to deliver projects; asset write downs; devaluations

| Minimal (1) | Minor (2) | Moderate (3) | Major (4) | Severe (5) |
|---|---|---|---|---|
| ☐ < $100k loss<br>☐ budget variance: <5% or up to <$10k *whichever is greater*<br>☐ impacts critical path: < 5 days;<br>☐ fraud < $5k<br>☐ *events*: minimal costs outside budget | ☐ $100k - $5 million loss<br>☐ budget variance: 5% < 10% or $10k to < $50k *whichever is greater*<br>☐ impacts critical path: > 5 days to 10 days;<br>☐ fraud > 5k and < $20k<br>☐ *events*: additional costs associated with cancellation or postponing part of event | ☐ $5m - $10 million loss<br>☐ budget variance: 10% < 20% or $50k to < $100k *whichever is greater*<br>☐ impacts critical path: >10 days to 1 month<br>☐ fraud > $20k and < $70k<br>☐ *events*: additional costs due to cancellation, postponement or forced event closure | ☐ $10m - $15 million loss<br>☐ budget variance: 20% < 30% or $100k - $150k *whichever is greater*<br>☐ impacts critical path > 1 month to 3 months<br>☐ fraud > $70k and < $100k<br>☐ *events*: costs related to the cancellation, postponement or forced closure of the event well exceed the planned budget and escalation is required | ☐ $15 million loss<br>☐ budget variance: 30% or > 30% of > $150k *whichever is greater*<br>☐ impact to critical path > 3 months or all objectives are not achievable<br>☐ fraud > $100k<br>☐ *events*: escalation is required with a detailed cost analysis and plan to recover costs due to cancellation, postponement or forced closure of the event |

**Environment and Indigenous Heritage category** any event or series of events which damage/have the capability to damage the environment, indigenous heritage or cultural amenity

| Minimal (1) | Minor (2) | Moderate (3) | Major (4) | Severe (5) |
|---|---|---|---|---|
| ☐ a complaint from a community member through accessible complaints processes<br>☐ minimal environmental impact; short term, transient disturbance; able to easily remedy<br>☐ minimal disturbance to heritage or cultural significance of site | ☐ multiple complaints communicating their perception or position on an issue at a site/region<br>☐ minor environmental harm with notice to remedy - resources redeployed to restore or remediate<br>☐ minor disturbance to a site with heritage or cultural significance; damage to artefacts requires restoration and/or remediation | ☐ multiple complaints with clear communication of position on an issue at a site or region; local protests and media attention<br>☐ moderate environmental harm with notice to remedy; penalties impending<br>☐ moderate disturbance to a site with heritage or cultural significance; damage to artefacts requires restoration and/or remediation along with aadministrative; judicial; penalties or other remedies | ☐ multiple complaints continue to be received on an issue at a site, region or state level; well-organised campaigns or protests and broadening interest/exposure<br>☐ major environmental harm requires long term recovery; notice to remedy and penalties impending; significant resources required to remediate; operations may be required to cease impacting business continuity<br>☐ major disturbance to a heritage or cultural site requires immediate restoration; extensive damage or loss of artefacts; resources are required to prioritise the restoration or remediation; strategy to rebuild community relationships; requires multiple administrative; judicial; or other remedies | ☐ ongoing multiple complaints; stakeholder class action or coordinated protests initiated; broadening media attention<br>☐ irreversible environmental harm; significant resources reinvested to address notice to remedy and penalties; strategic plans in place to reduce the future likelihood of harm/restoration/remediation and ensure continuity; administrative, judicial or other remedies<br>☐ severe disturbance or destruction of heritage, cultural site or valued artefacts; significant restoration, reparation and rebuilding of community relationships requires dedicated budget to facilitate |

## Assets, Operations and Security category

any event or series of events which results an inability to meet stakeholder expectations, requirements, or standards; compromises the security of our systems and information of a personal or corporate nature; or compromises the success of a community event.

| Minimal (1) | Minor (2) | Moderate (3) | Major (4) | Severe (5) |
|---|---|---|---|---|
| ☐ site/s are unavailable for a manageable duration; little to no operational impact | ☐ site/s are unavailable for a duration which is manageable; with some operational changes and impacts | ☐ site/s are unavailable for a duration that exceeds stakeholder tolerance; significant changes and impact to operations | ☐ multiple sites unavailable for a duration that exceeds stakeholder tolerance; operations are adversely impacted with significant changes | ☐ several sites are unavailable for a duration that exceeds stakeholder tolerance |
| ☐ assets are in good condition; serviced/ repaired/replaced in acceptable timeframes; | ☐ assets are maintained, repaired or replaced within acceptable timeframes | ☐ assets are in average condition; some are unable to be maintained/ repaired/replaced in acceptable timeframes | ☐ poor to average asset condition; some assets continue to not be maintained/repaired/replaced in acceptable timeframes | ☐ assets are in very poor unserviceable condition, or may be experiencing repetitive failures; renewal of critical assets may not be possible within reasonable timeframes and escalation occurs as required |
| ☐ minimal system outages/disruption to processes; within tolerance changes to delivery of safe and efficient operations, services, programs or activities; disruption is easily and quickly resolved as BAU | ☐ intermittent systems/processes may begin to impact continuity of some operations, services, programs or activities; changes to delivery of safe and efficient operations, services, programs or activities require review of workaround strategies in business continuity plans | ☐ intermittent systems or processes impacts continuity; continued changes to delivery of safe and efficient operations, services, programs or activities exceeds stakeholder expectations and activation of business continuity plans is required | ☐ sustained disruption of systems or processes | ☐ sustained disruption of systems or processes |
| ☐ quick resolution by third parties | ☐ third parties remedy outages within reasonable, agreed timeframes | ☐ third party suppliers remedy outages/ provide workarounds within reasonable timeframes | ☐ third party suppliers fail to ensure continuity, provide workarounds or remedy outages within reasonable timeframes | ☐ multiple operations, services, programs or activities cease due to loss of systems or processes; |
| | | ☐ inability to provide continuity of 1 or more operations, services, programs or activities > business continuity plan work-around procedures are enacted | ☐ stakeholder expected levels of service are not met; workarounds are prioritised to ensure capabilities to return to an acceptable level of service: redeployment of resources; additional resources; outsourcing or referrals; inability to provide continuity for multiple critical business activities | ☐ multiple third-party suppliers fail to ensure continuity, provide workarounds or remedy outages within reasonable timeframes |
| | | | ☐ business continuity plan work-around procedures continue and are escalated as required | ☐ inability to provide continuity for critical business activities with cascading consequences; some sites may be unlikely to reopen within reasonable timeframes; business continuity plan workarounds for critical business activities are prioritised and implemented |
| | | | ☐ workarounds prioritised and implemented, redeployment of staff, support, outsourcing or referrals to ensure minimum levels of service are provided to people we support and participants | ☐ organisational strategic response plan is enacted alongside division, region and site business continuity plans |
| **Security:** ☐ breach of security policies or requirements with little or no consequences | **Security:** ☐ a small volume of non-personal; corporate information; or non-critical systems/assets are lost, compromised or unavailable - within-tolerance; breaches of security policies or requirements by an individual; security incidents with minor consequences | **Security:** ☐ a large volume of non-sensitive, corporate information or non-critical systems or assets are lost, compromised or unavailable; repeated security incidents by an individual resulting from breaches of security policies or requirements | **Security:** ☐ sensitive, corporate, or personally identifiable information in critical systems/assets is lost, compromised or unavailable for an extended period; legal costs and/or financial penalties; repeated security incidents by one or more individuals; ongoing breaches of security policies or requirements | **Security:** ☐ a high volume of sensitive, corporate, and personally identifiable information in critical systems or assets is lost, compromised or unavailable for an extended period; extensive legal costs and/or financial penalties; escalating security incidents by one or more individuals; escalating breaches of security policies or requirements |
| **Community Events:** ☐ minimal delay to an activity (typically < 2 weeks) ☐ cancellation/event closure <1hr | **Community Events:** ☐ minor delay to 1 or more of the activities (typically 2 weeks to < 1 month) ☐ cancellation/event closure 1hr-6hrs | **Community Events:** ☐ delay to 1 or more activities (typically 1 to < 3 months) ☐ cancellation/event closure 6hrs-12hrs | **Community Events:** ☐ significant delay to 1 or more activities (typically 3 to < 6 months) ☐ cancellation/event closure 12hrs - 3 days | **Community Events:** ☐ extreme delay to 1 or more of the activities (typically > 6 months) ☐ total cancellation/event closure > 3 days |

## Assessing risk likelihood

When considering the likelihood of an event occurring, consider whether this event will occur in the next three (3) years.

We should ask: *"What is the likelihood of this event occurring in the next three (3) years?"*

If you have previous experience or available incident data/reports, take these into consideration.

The **frequency** column is based on evidence, number of incidents or other available data where a risk eventuated.

The **qualitative** column is used when no data is available to inform our assessment.

The **quantitative probability** column is used for projects or other activities where numerical probability is important.

**Likelihood rating** is a rating that indicates the probability that a risk may eventuate.

Make sure you also consider the **current controls** in place to manage the risk and whether the control effectiveness increases the likelihood of a risk occurring.

Use **Table 6** to identify the likelihood rating for each risk.

Use **Table 7** to identify the likelihood rating for community event risks.

### Table 6 – Risk likelihood

| Rating | Frequency | Qualitative | Probability |
|---|---|---|---|
| Certain (5) | 10 times a year or greater | **Always** occurs within Endeavour Foundation Group and/or the Not-for-Profit industry. | > 95% |
| Likely (4) | 2 to 10 times a year | **Periodically** occurs within Endeavour Foundation Group and/or the Not-for-Profit industry. | > 75% to 95% |
| Possible (3) | Once a year | **Occasionally** occurs within Endeavour Foundation Group and/or the Not-for-Profit industry. | > 30% to 75% |
| Unlikely (2) | Once every 2 to 9 years | **Infrequently** occurs within Endeavour Foundation Group and/or the Not-for-Profit industry. | 5% to 30% |
| Rare (1) | Greater than every 10 years | **Has never occurred** in Endeavour Foundation Group and/or the Not-for-Profit industry. | < 5% |

### Table 7 – Community event likelihood

| Rating | Likelihood | Chance |
|---|---|---|
| Certain (5) | Impact can be confidently expected to occur | > 80% |
| Likely (4) | Impact may reasonably be expected to occur | 60% to 80% |
| Possible (3) | Impact should occur at some time | 40% to 60% |
| Unlikely (2) | Impact could but is not expected to occur | 20% to 40% |
| Rare (1) | Impact may only occur in exceptional circumstances | < 20% |

## Risk rating

Table 8 provides a graphical representation of Endeavour Foundation Group's risk profile when the ratings of consequence and likelihood are applied.

Transfer your likelihood rating and consequence rating onto the matrix to identify the risk rating (where the two ratings meet). This will then identify your risk rating.

**For example:**

The consequence is Moderate (3) and the likelihood is Possible (3)

The Risk Rating is Medium. We multiple the two scores to provide a total (9).

The Risk Rating is Medium (9).

### Table 8 - Risk Rating Matrix

| Endeavour Foundation Risk Matrix | | Likelihood | | | | |
|---|---|---|---|---|---|---|
| | | Rare (1) | Unlikely (2) | Possible (3) | Likely (4) | Certain (5) |
| Consequence | Severe (5) | HIGH | HIGH | HIGH | EXTREME | EXTREME |
| | Major (4) | MEDIUM | MEDIUM | HIGH | HIGH | EXTREME |
| | Moderate (3) | LOW | MEDIUM | MEDIUM | HIGH | HIGH |
| | Minor (2) | LOW | LOW | MEDIUM | MEDIUM | MEDIUM |
| | Minimal (1) | LOW | LOW | LOW | MEDIUM | MEDIUM |

## Risk evaluation and escalation

### Determining the Risk Owner

The Risk Owner is the person who is accountable with the delegation of authority to approve risk treatments, make decisions, communicate, monitor, review and reassess risk. Where risks are assessed as high or extreme, the Risk Owner must escalate the risk in line with **Table 9**.

## Table 9 - Risk evaluation and escalation

Reference should be made to Endeavour Foundation Group's ***Risk Appetite and Tolerance Policy (QD 5028)***

### Risk evaluation

#### Low risk

- managed by routine procedures
- long exposure (up to 12 months)
- review every 12 months*

**Division/Portfolio/Site Level**

**Who is responsible and accountable for risks and approves risk treatment plans?**

- Risk Owner

#### Medium risk

- managed by routine procedures
- medium exposure (1 and 6 months)
- review every 6 months*

**Division/Portfolio/Site Level**

**Who is responsible and accountable for risks and approves risk treatment plans?**

- Risk Owner

**NOTES:**

* unless a review is requested or required earlier than the timeframe set in the Risk Management Framework

#### High risk (You must escalate high risks)


- risk level is not acceptable
- escalation is required
- short exposure ( > 1 month
- review monthly*

**Division/Portfolio Level**

**Who is responsible and accountable and approves risk treatment plans?**

- relevant ELT member

**Communication**

- Leader and Senior Leader
- Senior Leader and ELT member

**Escalate**

- Senior Leader to ELT member

**Reporting**

- Monthly to ELT member
- Quarterly to Audit & Risk Committee

**Site Level**

**Who is responsible, accountable and approves risk treatment plans for high risks?**

- Operations Manager

**Communication**

- Site Manager and Operations Manager
- Operations Manager and Senior Leader

**Escalate**

- Site Manager to Operations Manager

**Reporting**

- Monthly to Operations Manager

#### Extreme risk (You must escalate extreme risks)


- risk level is not acceptable
- escalation is required
- no tolerance for exposure, cease activity
- review every week*

**Division/Portfolio Level**

**Who is responsible and accountable and approves risk treatment plans?**

- Chief Executive Officer

**Communication**

- Senior Leader and ELT member
- ELT member and CEO

**Escalate**

- ELT member to CEO

**Reporting**

- Weekly to ELT
- Monthly to Board
- Quarterly to Audit & Risk Committee

**Site Level**

**Who is responsible, accountable and approves risk treatment plans for extreme risks?**

- Senior Leader

**Communication**

- Site Manager and Operations Manager
- Operations Manager and Senior Leader

**Escalate**

- Operations Manager to Senior Leader

**Reporting**

- Weekly to Senior Leader
- Monthly to ELT member

## Communicate and consult

The communicate and consult steps continue throughout the process. Engaging with stakeholders (both internal and external) ensures an accurate assessment. Regular feedback with internal and external stakeholders must take place through all stages of the risk management process.

A completed risk assessment is a living document that relies on effective communication. Risks must be communicated – so it's important to maintain open lines of communication and ensure engagement with people that need to be consulted and informed. It is best practice to communicate the final draft risk assessment for review by peers with risk management expertise and knowledge prior to finalisation.

## Monitoring and reviewing

Monitoring and reviewing are a vital component that occurs throughout the process. Periodic monitoring and reviewing of risks must be set during the risk assessment phase. Risks can cease to exist, new risks may arise, likelihood or impact or risk may change. The efficiency and effectiveness of controls that are in place may change. New treatments may have been developed over time. Risk owners can learn from successes, failures and near-misses – identifying and recording these lessons are important and add value moving forward as they may indicate changes to the control environment. Monitoring and review can also be undertaken on an adhoc basis, as requested by a Senior Leader, ELT member or the CEO.

## Risk treatment

There are 5 risk treatment options:

- avoid the risk;
- terminate the risk;
- transfer the risk;
- treat the risk; or
- retain the risk (take the opportunity).

Treating the risk enables the activity or action to continue, but action will be required to reduce the risk to an acceptable level. In developing new or modified risk treatments there is a need to consider the causes and consequences of each risk and then consider:

- ways the risk can be removed or changed so that it can no longer occur (elimination);
- ways to change the likelihood of the risk occurring (likelihood treatments);
- ways to change the consequences of the risk (consequence treatments); and
- ways the risk can be transferred to another party (transfer).

Once a treatment has been implemented it should be added to the existing controls of the risk, this will ensure it is monitored on an ongoing basis.

# Risk recording and reporting

## Risk assessments formally recorded in CORE

Endeavour Foundation Group's Integrated Risk Management System (CORE) will be used to record all strategic, key operating, operational risk assessments. The CORE system promotes active review and monitoring of all recorded risks in alignment with the ***Risk Management Framework (QD 5006).***

Refer to the **Risk Assessment Criteria Scope** section of this plan if you are unsure where to record your risk assessment. If you have further questions, please contact Endeavour Foundation Group's Risk Team.

## Other risk assessment not formally recorded in Resolver CORE

There are other types of risk assessments that are not required to be formally recorded in the Integrated Risk Management System (CORE) at the time of publishing this document. These may include:

- Personal risk assessments;
- Safety risk assessments;
- Security risk assessments;
- Site Activity risk assessments; and
- other site related risk assessments (recorded informally).

Where a risk assessment is required to be completed but not formally recorded in CORE, the following tools/templates should be used to record the risk assessment:

- ***Risk Assessment Tool (A3 MS Word version) (QF 5041.01)***; or
- ***Risk Assessment Tool (A4 MS Excel version) (QF 5041.02)***.

In compliance with ***Enterprise Risk Management Policy (QD 5027)***; and ***Enterprise Risk Management Framework (QD 5006)***, you must use this approved Risk Assessment Criteria to assess your risks. Speak to your leader about where the risk assessment document should be saved.

## Related documents and references

| Policy | |
|---|---|
| QD 5027 | Enterprise Risk Management Policy |
| QD 5028 | Risk Appetite and Tolerance Policy |

| Framework | |
|---|---|
| QD 5006 | Risk Management Framework |

| Procedure | |
|---|---|
| QP 5027 | Risk Management Procedure |

| Supporting documents | |
|---|---|
| QF 5041.01 | Risk Assessment Tool A3 |
| QF 5041.02 | Risk Assessment Tool A4 |

| Legislations/Standards/Acts | |
|---|---|
| **ISP 31000: 2018** | This international best practice standard provides guidelines on managing risk faced by organisations. The application of these guidelines can be customised to any organisation and its context. It provides a common approach to managing any type of risk and is not industry or sector specific and it can be used throughout the life of the organisation and can be applied to any activity, including decision-making at all levels. |

## Document information

| | |
|---|---|
| **Division** | Office of the CEO |
| **Portfolio** | Legal and Governance |
| **Document Executive Team Member** | Legal and Governance Executive General Manager |
| **Document owner** | Ian Bowyer, Head of Risk Assurance and Quality |
| **Review period (in months)** | 12 months |
| **Purpose (for new documents)** | Corporate standard to assess risks across the organisation |
| **Rationale for change/s (legislative, review due etc)** | Improvement for employee use |
| **Action/s required** | Replace any previous versions of the document |
| **Classification** | In-confidence |

# Risk Assessment Criteria

| Version | Date | Section(s) amended | Summary of amendment |
|---|---|---|---|
| 07 | 03/11/22 | Whole document | Revision of whole document for currency – minor amendments and update of inclusive language |
| | | Revision of each table to best meet the scope and diversity of Endeavour Foundation Group scope | Merging of Risk Assessment Criteria and Events Risk Assessment Criteria to ensure alignment with the Integrated Risk Management System (CORE). |