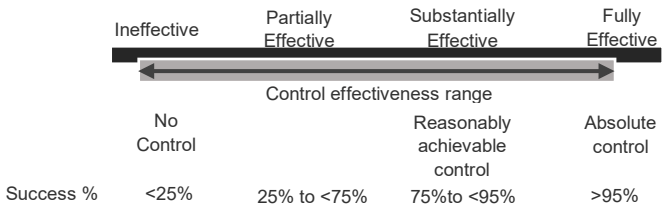
## Figure 1 - Control Effectiveness Rating

| INEFFECTIVE | PARTIALLY EFFECTIVE | SUBSTANTIALLY EFFECTIVE | FULLY EFFECTIVE |
|---|---|---|---|
| ▪ Significant control gaps.<br>▪ Either controls are not designed to treat root causes and/ or they do not operate at all effectively. | ▪ Some of the controls are designed correctly to treat root causes.<br>▪ More work to be done to improve design of controls and/ or operating discipline and reliability of controls. | ▪ Majority of controls are designed correctly to address the root causes.<br>▪ Some work to be done to improve operating discipline and reliability. | ▪ Controls are designed correctly to address the root causes. Management believes that controls are effective and reliable on almost all occasions.<br>▪ Management monitoring and review of controls is established |

## Figure 2 - Control Effectiveness Guidance




The Control Effectiveness Rating is a function of the level of control that is considered *reasonably achievable* for the specific risk event.
As illustrated in Figure 2, a reasonably achievable level of control is not necessarily equal to absolute control as the delivery of absolute control may not be considered reasonably practical or cost effective.

To support the Control Effectiveness Rating, challenge the current controls to test if they meet what is considered reasonably achievable by considering the questions below:

| | |
|---|---|
| CONTROL DESIGN | ❖ Are the controls meeting the applicable laws, regulations, and mandatory standards?<br>❖ Are the controls comparable with peers or accepted industry practice?<br>❖ If the environment has changed, are existing controls still fit for purpose?<br>❖ Are the controls designed to effectively manage/mitigate the risks? |
| CONTROL OPERATION | ❖ Can controls be demonstrated and evidenced through testing or other means?<br>❖ Are there any outstanding action items from audits, risk reviews, or investigations?<br>❖ In recent occurrences, did the controls work as intended, including throughout the life of the risk? Refer to recent incidents or issues. |

**DECIDE & ACT**

Decisions to address a risk involve comparing the Residual Risk against the University's Risk Appetite and considering the total 'cost' of the risk against the 'cost' of control. One exception is prescriptive legislation which may override any cost-benefit analysis and compels the business to adopt particular controls.

With the understanding of each risk event, the causes and effects of the existing controls:

- Explore the characteristics of the risk event, including the causes and consequences, and seek options that act against the causes and / or the consequences.
- Explore options to improve the design and operating effectiveness of existing controls or the design of new controls where a control gap has been identified.

Develop an understanding of the net business benefit of each option and engage with the Accountable Executive in Figure 3 to decide and act.

Where a decision to act is taken, document the control (its purpose and design intent), those accountable, allocate resources, agree deadlines, and how those responsible will demonstrate that the control is operating as intended when required.

**As the action is implemented, continue to monitor, and assess (update) the control effectiveness rating for the risk event.**

## Figure 3 - Priority and Accountable Executive Guidance

| LEVEL OF RISK | VERY LOW | LOW | MODERATE | HIGH | CRITICAL |
|---|---|---|---|---|---|
| Actions **endorsed** by | NA | NA | Business Unit Heads and/or Process Owners | Divisional Heads/Dean, makes recommendations to the Executive Committee | Divisional Heads/Dean, makes recommendations to the Executive Committee |
| Actions **approved** by | NA | Risk can be accepted by Business Unit Heads/Dean and/or Process Owners | Divisional Heads/Deans | Vice-Chancellor | Vice-Chancellor |
| Indicative time to implement risk mitigation actions. | NA | Nine months | Six months | Three months | As soon as practicable |

### MONITOR

It is important to regularly monitor and review the effectiveness of current controls to ensure they are fit for purpose and continue to mitigate the risks. Consider if current controls still treat root causes of the known risk events and if any new risks that have been introduced are currently not being treated. The risk owner is responsible for ensuring effective monitoring activities are in place.

With limited time and resources available, monitoring activities should be prioritised to focus on the most critical controls (i.e., controls that are most effective in treating causes and reducing the highest risk exposure).

Some examples of monitoring activities include observing personnel or procedures, analytical review, inquiries or interviews with relevant personnel, review of periodic reporting, testing of controls and conducting audits.

Information produced from monitoring activities can help provide learnings and feedback on whether control effectiveness ratings require any adjustment, if there is a need to implement additional controls to reduce the level of risk and opportunities to improve controls to enhance operational discipline and reliability.

### RECORD & REPORT

All risk assessments must be recorded and maintained in the approved Risk Management System (WesternERM).

If utilising this system is not practical, risk information is to be captured as specified in the approved management system.

Risks rated High & above that impact University operations and require a coordinated treatment must be communicated to the Office of Audit & Risk Assessment for reporting to the Executive Committee and the Audit & Risk Committee.

## Figure 4 - Impact / Consequence Rating

| Impact Score | Generic Impact Description | Impact – Description of Consequence | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | Education & Research | Health and Safety | Operations / Service Delivery | Brand & Reputation | Financial | Legal | Compliance |
| (5) Catastrophic | Event or circumstance with potentially disastrous impact on business or significant material adverse impact on a key area. | Unsustainable reduction in student enrolment/retention.<br><br>Critical impact on meeting teaching/research goals over a long period.<br><br>Loss of critical partnerships / collaborations. | Death or permanent disability.<br><br>Widespread/sustained industrial action, sustained student protest/violence. | Cessation of critical business operations, systems or Education/Research programs for a long period and at a crucial time in the University calendar.<br><br>Nearly all service delivery targets are not met. | Irreparable damage to or loss of brand / image / reputation.<br><br>Serious / long-term damage to University status / international rankings.<br><br>Widespread / persistent / sustained negative media attention. | Financial loss greater than $25m.<br><br>Significant budget impact (revenue shortfall or expense over-run) with no capacity to adjust within the existing budget resources. | Serious breach of contract / duty of care that results in significant prosecution, potential litigation and significant damages and / or costs awarded.<br><br>Criminal or civil proceedings initiated or Board liability. | Serious non-compliances of statutory obligations, that results in significant prosecution, fines, loss of future funding / registrations / licenses.<br><br>Criminal or civil proceedings initiated or Board liability.<br><br>Regulator publishing failure to comply with notices / Regulator sanctions / Immediate corrective action required. |
| (4) Major | Critical event or circumstance that can be endured with proper management. | Major reduction in student enrolment/retention.<br><br>Major impact on meeting teaching/research goals over a long period.<br><br>Long-term impact to partnerships / collaborations. | Serious injury/harm, including sexual assault/rape.<br><br>Dangerous near miss, student protests, or threats of industrial action. | Major impact on critical business systems or Education / Research programs for an unacceptable period or at a critical time in the University calendar.<br><br>Major service delivery targets cannot be met. | Major damage to brand / image / reputation nationally / internationally.<br><br>Long term national or local negative media coverage. | Financial loss greater than $10m.<br><br>Requires significant adjustment or cancellation to approved/funded projects/programs. | Major breach of contract / duty of care that results in investigations, major fines, senior executive liability, potential for high value litigation. | Major non-compliances of statutory obligations, that attract regulatory action, infringement notices, reporting, regulatory audits and investigations.<br><br>Allegations of criminal / unlawful conduct.<br><br>Senior Executive liability.<br><br>Potential for litigation, major fines or loss of future funding / registrations / licenses. |
| (3) Moderate | Significant event or circumstance that can be managed under normal circumstances. | Moderate reduction in student enrolment/retention.<br><br>Moderate impact on meeting teaching/research goals over a short period.<br><br>Short-term impact to partnerships / collaborations. | Moderate impact on person's health/wellbeing.<br><br>Loss time or penalty notice due to unsafe act/plant/equipment.<br><br>Severe staff morale / increase in workforce absentee rate / student dissatisfaction. | Loss / interruption / compromise of some business systems or Education / Research programs for a short period.<br><br>Few service delivery targets cannot be met. | Moderate or short-term damage to brand / image / reputation.<br><br>Moderate issues or concerns relating to student / stakeholder or community.<br><br>Prominent local negative media coverage. | Financial loss greater than $5m.<br><br>The impact may be reduced by reallocating resources. | Breach of contract or duty of care that leads to allegations of criminal / unlawful conduct, individual liability, legal proceedings of relatively high value. | Non-compliances of statutory obligations that result in regulatory attention, potential allegations of criminal/unlawful conduct, individual liability.<br><br>Moderate level fines. |
| (2) Minor | Event with consequences that can be readily absorbed but requires management effort to minimise the impact. | Short-term reduction in student enrolment/retention.<br><br>Minor impact on meeting teaching/research goals.<br><br>Limited impact to partnerships / collaborations. | Minor impact on person's health/wellbeing.<br><br>Inappropriate behaviour, workplace safety compromised, dialogue required with industrial groups or student body. | Loss / interruption / compromise of critical business systems or Education / Research program for a tolerable period but at an inconvenient time.<br><br>Minor impact on | Low negative media coverage.<br><br>Minor issues or concern raised by students / stakeholders. | Financial loss greater than $2m.<br><br>Requires monitoring & possible corrective action within existing resources. | Minor breach of contract / duty of care that doesn't result in litigation or adverse legal actions against the University. | Minor non-compliances of statutory obligations that result in minor regulatory scrutiny via improvement letters.<br><br>Minor fines. |

| Impact Score | Generic Impact Description | Impact – Description of Consequence | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | Education & Research | Health and Safety | Operations / Service Delivery | Brand & Reputation | Financial | Legal | Compliance |
| | | | | operations / service delivery. | | | | |
| (1) Insignificant | Some loss but not material; existing controls and procedures should cope with the event or circumstance. | Minor downturn in student enrolment / retention.<br>Negligible impact on meeting teaching/research goals.<br>Negligible impact to partnerships / collaborations. | Minimal or no adverse impact on person's health/wellbeing. | Negligible impact on the business operations, systems and/or delivery of service. | Minor / localised damage to brand / image / reputation. | Financial loss less than $2m.<br>Unlikely to impact on budget or funded activities.<br>Daily business running costs can absorb impact. | Immaterial breach of terms and conditions of contract / duty of care that doesn't result in litigation or adverse legal actions against the University. | Isolated non-compliances of statutory obligations that do not result in adverse regulatory response or action.<br>Immaterial level of fines. |

## Figure 5 - Likelihood Rating

| Likelihood Score | Definition of Likelihood |
|---|---|
| (5) Almost Certain | Highly likely to happen, possibly frequently or already happened |
| (4) Likely | Will probably happen, but not a persistent issue |
| (3) Possible | May happen occasionally |
| (2) Unlikely | Not expected to happen, but it is a possibility |
| (1) Rare | Very unlikely this will ever happen |

## Figure 6 - Level of Residual Risk / Overall Risk Level (Impact x Likelihood)

| Impact | Likelihood | | | | |
|---|---|---|---|---|---|
| | Rare (1) (remote) | Unlikely (2) (uncommon) | Possible (3) (occasional) | Likely (4) (probable) | Almost Certain (5) (frequent) |
| **Catastrophic (5)** | Moderate | Moderate | High | Critical | Critical |
| **Major (4)** | Low | Moderate | High | High | Critical |
| **Moderate (3)** | Low | Low | Moderate | Moderate | High |
| **Minor (2)** | Very Low | Low | Moderate | Moderate | Moderate |
| **Insignificant (1)** | Very Low | Very Low | Low | Low | Low |