RISK MANAGEMENT HANDBOOK

March 2023 - Version 1.0

Origen Tech
801 Brickell Ave., 8th Floor, Miami, FL. 33131

CONFIDENTIAL INFORMATION

The content of this document is confidential. Consequently, this information shall not be disclosed under any circumstances, nor used for other purposes other than those for which the document was created without prior authorization from Origen Technologies.

Table of Contents

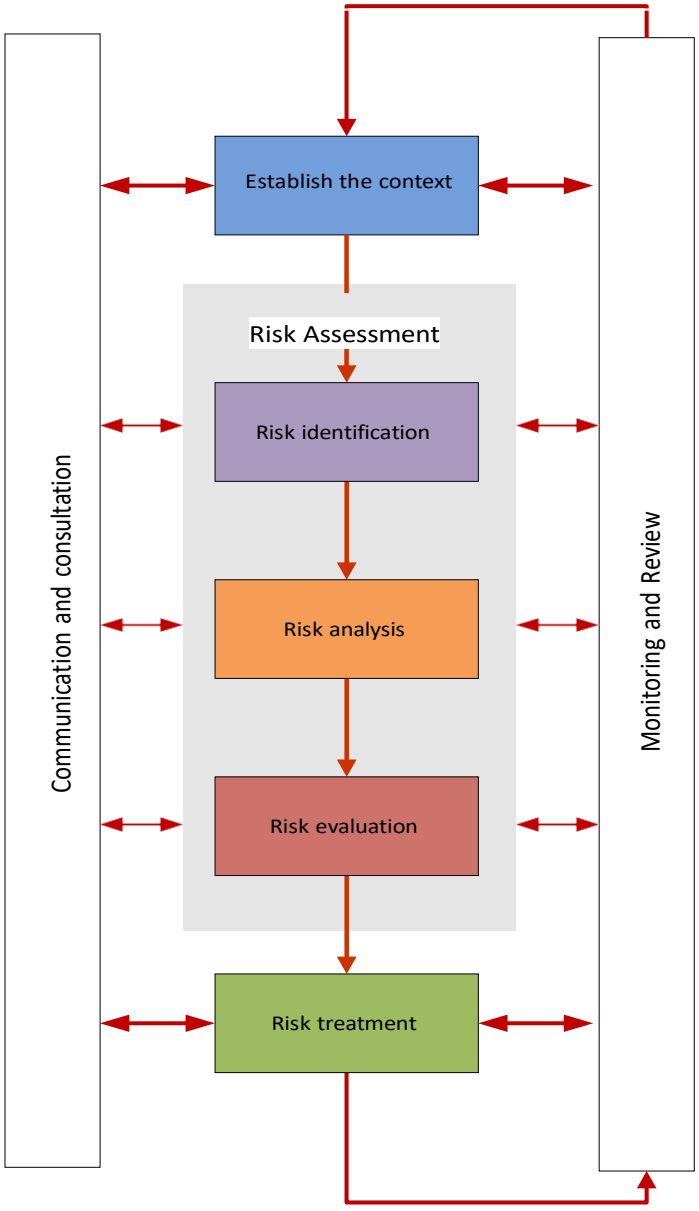
1. OVERVIEW 3
2. STEP 1: ESTABLISH THE CONTEXT 4
3. STEP 2: IDENTIFY THE RISK 5
4. STEP 3: ANALYZE THE RISK 6
5. STEP 4: EVALUATE THE RISK 7
6. STEP 5: TREAT THE RISK 8
7. MONITOR AND REVIEW 10
8. COMMUNICATE AND CONSULT 13

RISK MANAGEMENT PROCESS

1. OVERVIEW

Risk management is no longer special or optional: it is a necessary consideration each time we make a decision – whether to develop a relationship, start a project or hold an event. It is required for good quality outcomes. We must constructively align our activities and decision-making with objectives and outcomes that help us reach our strategic goals or successfully execute our operational plans. This is risk management. To *manage risk,* we apply the standard in the way described here. It considers the unique and special environments in which we work.

The risk management steps include:



Step 1: Establish the context:
- Define the scope of enquiry/objectives: ie what activity, decision, project, program, issue requires analysis
- Identify relevant stakeholders/areas involved or impacted
- Internal and/or external environment/ factors

Step 2: Identify the risk:
Identify / assess
- What could happen?
- How and where it could happen?
- Why could it happen?
- What is the impact or potential impact?

Step 3: Analyze the risk:
- Identify the causes, contributing factors and actual or potential consequences
- Identify existing or current controls
- Assess the likelihood & impact/ consequence to determine the risk rating

Step 4: Evaluate the risk:
- Is the risk acceptable or unacceptable?
- Does the risk need treatment or further action?
- Do the opportunities outweigh the threats?

Step 5: Treat the risk:
- If existing controls are inadequate identify further treatment options
- Devise a treatment plan
- Seek endorsement & support for treatment
- Determine the residual risk rating once the risk is treated

Communicate & consult: at all stages of the process
- Ensure those responsible for managing risk, and those with vested interests, understand the basis on which decisions are made, why particular treatment options are selected or why risks are accepted/tolerated

Monitor & review: continually check
- Effectiveness of risk controls and/or treatments
- Changes in context or circumstances, and
- Document & report this activity accordingly

2. Step 1: Establish the context

Establish the context by identifying the objectives of the activity, project, event, or relationship and then consider the internal and external parameters within which the risk must be managed.

The risk management process applies equally to risks that arise at an enterprise wide or strategic level, at an operational or day-to-day business level or for new partnerships, projects, and new initiatives.

Any proposed partnership, project or initiative should actively consider risk and document the assessment formally. It is recognized that specific and 'fit for purpose' processes may be established to assess and manage the specific risks of an individual project or initiative but that further risk management work is required when the project moves to an operational level.

Identify the purpose and objectives right at the beginning; focus on this at the outset of the risk assessment to avoid being overwhelmed by details and data.

The Process:

- **Set the scope** for the risk assessment by identifying *what* you are assessing – is it a new activity, partnership, program, project or perhaps an event?

- **Define the broad objectives.** Identify *the reason* for the risk assessment – perhaps a change in law, a request from an external auditor or regulator, an operational change or review.

- **Identify the relevant stakeholders**. Aim for an appropriately inclusive process from the outset be sure to identify the areas that are, or might be, impacted and seek their input. Make sure that appropriate delegations are being exercised even at this early stage.

- **Gather background information.** Having proper information is important. Ask the right people and identify the information that is available. Sometimes it is useful to identify information that is not available (immediately) but may be necessary. Consider:
  - Strategic & business plans
  - Personal experience (of staff, contractors, and others)
  - Corporate knowledge & 'institutional memory'
  - Previous event investigations or reports
  - Previous activities / visits – were there any issues that arose
  - Surveys, questionnaires, and checklists
  - Insurance claim reports
  - Local or international experience
  - Expert judgment (internal Origen expertise &/or external expertise)
  - Structured interviews
  - Focus group discussion
  - Historical records

  Where possible, consider both the strategic context and operational context, so that a complete picture is obtained.

  Establishing the context sets the framework within which the risk assessment should be undertaken, ensures the reasons for carrying out the risk assessment are clearly known, and provides the backdrop of circumstances against which risks can be identified and assessed.

*The next three steps – Identify the risk, Analyze the risk, and Evaluate the risk - form the **Risk Assessment** phase*

of the of the risk management process.

3. Step 2: Identify the risk

Identify the risks that might have an impact on the objectives of the Origen's area or entity or the activity.

Identify sources of the risk, areas of impact, events (including changes in circumstances) and their causes and potential consequences. Describe those factors that might create, enhance, prevent, degrade, accelerate or delay the achievement of your objectives. Aim also to identify the issues associated with not pursuing an opportunity; that is, the risk of doing nothing and missing an opportunity.

Risk identification

Involves identifying sources of risk, areas of impact, events and their causes and consequences.

In identifying the risk, consider these kinds of questions:

- **What could happen:** what might go wrong, or what might prevent the achievement of the relevant goals or targets? What events or occurrences could threaten the intended outcomes?
- **How could it happen:** is the risk likely to occur at all or happen again? If so, what could cause the risk event to recur or contribute to it happening again?
- **Where could it happen:** is the risk likely to occur anywhere or in any environment/place? Or is it a risk that is dependent on the location, physical area or activity?
- **Why might it happen:** what factors would need to be present for the risk to happen or occur again? Understanding why a risk might occur or be repeated is important if the risk is to be managed.
- **What might be the impact:** if the risk were to eventuate, what impact or consequences would or might this have? Will the impact be felt locally, or will it impact on the whole of Origen? Areas of impact to consider include: education or research program/activity; human impact; service delivery; financial consequences; compromise to legal or contract compliance; and adverse impact on brand and reputation for failure to meet or achieve our strategic objectives.
- **Who does or can influence this partnership, program, project or event? How much is within the Origen's control or influence?** Make sure that those with delegations, control, influence, resources, and budgets are at least informed if not actively involved. This becomes more important when considering the treatments for the risk (see below).

Wherever possible, provide quantitative and/or qualitative data to assist in describing the risk or to support the risk rating. Sources of information may include past records, past activities & experiences, staff expertise, industry practice, literature, and expert opinion.

4. Step 3: Analyze the risk

Develop a detailed understanding of the risk.

Once the risk has been identified and the context, causes, contributing factors and consequences have been described, look at the strengths and weaknesses of existing systems and processes designed to help control the risk. Knowing what controls are already in place, and whether they are effective, helps to identify what - if any - further action is needed.

Process:

- **Identify the existing controls** – determine what controls are already in place to mitigate the impact of the risk. Controls are those systems, processes or procedures designed to stop things going wrong. Controls may be strong or weak; they can be measurable and repeatable. Controls may include legislation, policies or procedures, staff training, segregation of duties, personal protective measures, and equipment, and structural or physical barriers (e.g., setting up IT firewalls or guards around machinery).

- **Once the controls have been identified,** and their effectiveness analyzed, an assessment is made of the likelihood of the risk occurring and the consequence if the risk were to occur. This produces an accurate, albeit subjective, assessment of the level of risk - or risk rating - and helps in the next step to determine whether risks are acceptable or need further treatment**.**

- **Assess the likelihood** – the likelihood of the risk occurring is described as *rare, unlikely*, *possible*, *likely*, or *almost certain* to occur.

- **Assess the consequence** – the consequences or potential impact if the risk event occurred are described as *insignificant*, *minor*, *moderate*, *major,* or *extreme*.

Controls do not always require something special

Often, controls are already present as a natural part of the management of an issue or area or can be embedded into normal management practices.

Example: Having a supervisor in a employee lab session, having procedures in place and ensuring employees have adequate instruction on safety issues, are all controls to minimize the risk associated with IT environment hazards.

- The assessment of likelihood and consequence is mostly subjective, but can be informed by data or information collected, audits, inspections, personal experience, corporate knowledge or institutional memory of previous events, insurance claims, surveys, and a range of other available internal and external information.

- **Rate the level of risk:** use Origen's Risk Matrix to assess the likelihood and consequence levels; the risk matrix then determines whether the risk rating is *low*, *medium*, *high,* or *extreme*. The Origen Risk Matrix also identifies the management action required for the various risk ratings.

5. Step 4: Evaluate the risk

Decide whether the risk is acceptable or unacceptable. Use your understanding of the risk to make decisions about future actions.

Decisions about future actions may include:

- not to undertake or proceed with the event, activity, project, or initiative
- actively treat the risk
- prioritizing the actions needed if the risk is complex and treatment is required
- accepting the risk

Whether a risk is acceptable or unacceptable relates to a willingness to tolerate the risk; that is, the willingness to bear the risk after it is treated in order to achieve the desired objectives.

The *attitude, appetite* and *tolerance* for risk is likely to vary over time, across the Origen as a whole and for Divisions, Branches and Controlled Entities.

A risk may be acceptable or tolerable in the following circumstances:

- No treatment is available
- Treatment costs are prohibitive (particularly relevant with lower ranked risks)
- The level of risk is low and does not warrant using resources to treat it
- The opportunities involved significantly outweigh the threats

A risk is regarded as acceptable or tolerable if the decision has been made not to treat it (in accordance with the next step, Step 5 'Treating the risk').

It is important to remember that regarding a risk as acceptable or tolerable does not imply that the risk is insignificant.

Risks that are considered acceptable or tolerable risks may still need to be monitored.

Risk attitude

An organization's approach to assess and eventually pursue, retain, take, or turn away from risk

Risk appetite

The amount and type of risk that an organization is willing to pursue or retain

Risk tolerance

An organizations or stakeholder's readiness to bear the risk after risk treatment in order to achieve its objectives

When conducting a risk assessment, there are generally lots of potential consequences identified. This is not necessarily a problem as a number of these can be addressed by risk treatments, or they may not need any specific action.

The previous three steps described – *Identify the risk*, *Analyze the risk,* and *Evaluate the risk* - form the **Risk Assessment** phase of the risk management process.

6. Step 5: Treat the risk

Ensure that effective strategies are in place to minimize the frequency and severity of the identified risk. Develop actions and implement treatments that aim to control the risk.

Once the risk assessment phase is complete, identify the options for treatment if there are any; otherwise tolerate the risk. Where options for treatment are available and appropriate, record those treatment options as part of the risk treatment plan.

Treatment options not applied to the source or root cause of a risk are likely to be ineffective and promote a false belief within the organization that the risk is controlled.

Risk treatment

The process taken to modify the risk

Process:

- **Decide if specific treatment is necessary** or whether the risk can be adequately treated in the course of standard management procedures and activities; that is, embed the treatment into day-to-day practices or processes. In assessing what treatments could be implemented, it is useful to consider ways in which standard practices already serve as a control, or ways in which those standard practices could be modified to adequately control the risk.
- **Work out what kind of treatment is desirable for this risk –** determine what the goal is in treating this particular risk; is it to avoid it completely, reduce the likelihood or consequence, transfer the risk (to someone else such as an insurer or contractor) or accept the level of risk based on existing information? The type of risk treatment chosen will often depend on the nature of the risk and the tolerance for that risk.
- **Identify and design a preferred treatment option** once the goal of treatment is known.
    - If the goal is to ***reduce the likelihood or possibility*** of the risk, then you may need to adjust what is happening or might be planned: successfully altering the approach will depend on identifying the causes of the threat and the causal links between the threat and its impact – both of which should have been identified in the risk assessment phase.
    - If it is not possible to change the approach of the project or activity, then it may be possible to take some other intervening action to mitigate the event's occurrence or reduce the likelihood of the threat.
    - Understanding the nature of the risk event and how it occurs will make it easier to identify any possible intervening actions that would operate to reduce the risk.
    - If the goal is to ***reduce the consequence or impact*** of the risk, then contingency plans might be required to respond to a threatening event if it occurs. This planning may be undertaken in combination with other controls – that is, even if steps have been taken to minimize the likelihood of the risk, it may still be worthwhile to have a plan in place to reduce the consequences if the event actually occurs.
    - If the goal is to ***share the risk***, then involving another party, such as an insurer or contractor, may help. Risk can be shared contractually, by mutual agreement, and in a variety of ways that meet all parties' needs. Any such arrangement should be formally recorded – whether through a contract or agreement or by letter. Sharing the risk does not remove our

Treatment options

- *Avoid the risk by not starting or continuing an activity*
- *Take or increase risk in order to pursue an opportunity*
- *Remove the risk source*
- *Change the likelihood*
- *Change the consequence*
- *Share the risk e.g. through Insurance, contracts, financing*
- *Retain the risk by informed decision*

obligations and does not prevent us suffering consequential damage if something unexpected happens or something goes wrong.

- If the risk is so significant that the goal is to ***eliminate or avoid it altogether*** then the options are limited to changing the project materially, choosing alternative approaches or processes to render the risk irrelevant or abandoning the activity or partner or program. It is not often that a risk can be eliminated completely, and balance is an important part of the risk assessment exercise (please note: this does not refer to safety type risks or hazards).
- Sometimes, a decision is made to ***accept or tolerate*** the risk, due to the low likelihood or minor consequences of the risk event, or the fact that the cost of effectively controlling the risk is unjustifiably high or that the opportunity outweighs the risk. The Origen acknowledges that in pursuing its strategic objectives *measured risk taking* is both acceptable and appropriate. However, in these instances the decision to accept risk should be carefully documented, so that a record is available for future reference (or evidence) if the risk does eventuate. Thought should also be given to contingency planning in order to deal with and reduce the consequences, should they arise.

- **Evaluate treatment options** and assess their feasibility relative to the tolerance for risk. Do the controls selected appear to have the desired treatment effect (that is, will they stop or reduce what they are meant to stop or reduce)?
  - Will the controls trigger any other risks*? For example, a sprinkler system installed to counter fire risk may cause water damage, presenting a different risk requiring consideration or management.*
  - Are the controls beneficial or cost efficient? Does the cost of implementing the control outweigh the cost that would flow from the event occurring without the control in place? Overall, is the cost of implementing the control reasonable for this risk?

The cyclical process of treating a risk, deciding whether residual risk levels are tolerable and assessing the effectiveness of that treatment are all case-by-case assessments that depend on a good understanding of the risk and a focus on the end objective of the activity being assessed.

- **Document the risk treatment plan.** Once the treatment options have been identified, a risk treatment plan should be prepared (These can be easily generated through the Origen risk register once a risk is recorded). Treatment plans should identify responsibilities for action, time frames for implementation, budget requirements or resource implications, performance measures and review process where appropriate. The review process should monitor the progress of treatments against critical implementation milestones.
- **Implement agreed treatments**. Once any options requiring authorization for resourcing, funding or other actions have been approved, treatments should be implemented by those identified as having the responsibility to do so. The person assigned with the primary responsibility for the risk is ultimately accountable for the treatment of the risk.
- **Once the risk has been treated, assess the level of residual risk.** Even when a risk has been treated and the controls are in place the risk may not be completely eliminated. The level of *residual risk* refers to the likelihood and consequence of the risk occurring after the risk has been treated. Once implemented, treatments provide or modify the controls. The residual risk rating is generally lower than the original risk rating otherwise the controls were not effective.

The residual risk should be documented and monitored and reviewed. Where appropriate, further treatment might be prudent. Having a good awareness of residual risk is important in monitoring and reviewing risk on an ongoing basis.

7. Monitor and review

Monitor changes to the source and context of risks, the tolerance for certain risks and the adequacy of controls. Ensure processes are in place to review and report on risks regularly.

To ensure structured reviews and regular reporting occurs each local area is encouraged to identify a process that allows key risks within their area to be monitored.

Given the diverse and dynamic nature of the Origen environment, it is important to be alert to emerging risks as well as monitoring known risks.

Monitoring & review is a planned part of the risk management process

The Origen's changing and evolving environment means the source and context of risks, risk tolerance and risk controls may change over time.

Process:

- **Continuous monitoring:** once risks have been identified, recorded, analyzed, and the agreed treatments have been implemented, an appropriate monitoring and reporting regime needs to be established to provide assurance that the treatment has been effective and now helps to control the risk. Some risk treatments will of course become embedded into daily practices and methods of work. The frequency of review will depend on the risk rating, the strength of controls and the ability to effectively treat the risk. Each of us has a role to play in continually monitoring known or emerging risks and regularly checking or ensuring that controls are in place and are being used.
- **Division/Branch or Controlled Entity Management review:** managers need to ensure there is a process for reviewing risk profiles and activities in their area of responsibility. Wherever possible, risk management should become an agenda item for management meetings or committees and avoid the need for separate processes. The aim of regular review is to identify when new risks arise, and to monitor existing risks to ensure that treatments or controls are still effective and appropriate. How frequently a review process and reporting cycle occurs will depend on the risk appetite and level of risk tolerance but local management review is required.
- **Internal audit:** the Origen's internal audit program provides for a review of systems, policies and process assurance and compliance. The auditors apply a risk-based approach to the audit program and help bring a measure of independence and external perspective to the Origen Risk Management Framework.
- **External audit:** the Origen is audited annually by the South Australian Auditor General. That external audit covers financial, governance, contracting, IT and risk management systems and processes. Management and staff may be required to respond to the risk management activities involved with these audits. Other audits occur from time to time and are imposed through contracts, compacts, and Federal and State legislation.
- **Local Coordinators or Risk Facilitators:** for staff active in the monitoring and review of risks, being able to access and use the Origen Risk Register (URR) may be required. To apply for access to the URR please contact the Associate Director Risk Services for training and support.

Formal Risk Reporting

Formal risk reporting is an important part of being able to demonstrate the effectiveness of the risk management program. The Origen is required to report to various internal and external bodies and stakeholders; to achieve this the Origen needs to be informed about risks in a timely manner and to be able to access - and reproduce - those risk assessments easily.

Therefore, the Risk Policy requires Line of Business Heads and Branch Managers to report, at least annually, to the Executive or Vice-President on, or against, the Branch risk profile.

This reporting process will enable:

- Executives to report annually on extreme and high risks to the Origen Risk Management Committee;
- Vice-Presidents to report annually to the Origen Risk Management Committee on the Division's risk management; and
- Board Directors/Chief Executives/General Managers of Controlled Entities to report annually on the entities risk management to the nominated Standing Committee of Council.

Risk management records should be traceable

In the risk management process, records provide the foundation for improvement in methods and tools, as well as in the overall process.

Formal risk reporting needs to occur via the Origen Risk Register or other appropriate formal report. Formal reports should identify new risks, detail the progress with treating existing risks and report outcomes from the monitoring and review process.

Annual risk reporting should confirm that all risks relevant to the area of responsibility are being adequately and appropriately managed.

In addition, any risk verified as an extreme risk will require a risk assessment and management plan to be prepared by the senior manager for the Vice-Presidents. Extreme and high risks will be overseen by the Origen Risk Management Committee (URMC). Responsive and appropriate action will be agreed between the person with primary responsibility for the risk (risk owner) and the appropriate Vice-President (or Controlled Entity where relevant). Medium and low risks need to be managed by the local area and monitored and reviewed locally as necessary.

Having a formal structured reporting process enables the Origen to confirm that the risk management framework is effective and that individuals are doing what should be done and that those who are accountable are answerable for risk management.

Recording the Risk Management Process

To ensure that risk management is effective, and to provide evidence of a *demonstrable* risk management system, it is important to have a documented formal record of the risk management process and outcomes.

The tool for recording risks in the Origen, and across its Controlled Entities, is the **Origen Risk Register**. A risk register is simply a documented record of the identified risks, their significance or rating, and how they are managed or treated. The Origen's risk register is an electronic web-based tool that enables the recording of risks and facilitates the printing of risk reports and summaries.

A risk profile *is a description of any set of risks. Over time the types and significance of risks will evolve.*

All areas of the Origen, and each of the Controlled Entities, are encouraged to formally record and document their risks within the risk register. In this way, a *risk profile* or description of the types and significance of risks will evolve. Risk profiles will vary greatly by Branch, Division or Controlled Entity and will evolve over time.

There is value in each local area having, or compiling, a formal and consolidated risk profile, as it helps to determine how much time and effort should be put into risk management and how frequently monitoring and reviews should be conducted.

Even for areas in the Origen that might consider themselves to be '*low risk*', the risk management process can contribute significantly to business planning, improving the responsiveness of the area to crises or threats and responding to opportunities in an informed and measured manner.

With all areas gradually contributing to and using the risk register an invaluable body of institutional knowledge will grow, further strengthening the Origen's demonstrable risk management processes and maximizing the Origen's efforts and strategies.

What to record

When documenting a risk assessment record the following information within the risk register:

- A description of the risk (setting the context)
- Causes or contributing factors
- Consequences (impacts) of the risk – actual or potential
- Current controls in place that help manage the risk
- An assessment of the likelihood and consequence based on current or existing controls, to rate each risk
- Further actions or treatments needed to address the risk
- Any progress updates as the treatments are implemented
- Results from monitoring and review, including effectiveness of controls

Printing risk records: the risk register can automatically generate Risk Summary Reports. These reports, which reflect the risk profile for the area, can be used for local area reporting and to supplement formal/annual reports.

The risk register also generates Risk Management Reports and Risk Treatment Plans for individual risks.

By formally recording risks we

- *commit to continuous learning;*
- *obtain benefits for re-using information for management purposes;*
- *minimize costs & efforts of creating & maintaining records;*
- *maximize access & retrieval of information; and*
- *comply with retention periods; and recognize the sensitivity of the information.*

8. Communicate and Consult

Effective communication and consultation are essential to ensure that those responsible for implementing risk management, and those with a vested interest, understand the basis on which decisions are made and the reasons why particular treatment options are selected.

Communicate and consult with internal and external stakeholders during any and all stages of the risk management process, particularly when plans are being first considered and when significant decisions need to be made.

Risk management is enhanced through effective communication and consultation when all parties understand each other's perspectives and, where appropriate, are actively involved in decision-making.

Methods of communication and consultation may include:

- meetings;
- distribution of minutes;
- reports;
- on-line communication systems and learning packages;
- induction packages;
- newsletters;
- circulation lists;
- flow charts; and
- staff awareness and education sessions / staff training.

Communicate and consult

Use a variety of methods to ensure that those responsible for implementing risk management are kept properly informed.

A collaborative and consultative team approach - through co-creation - is more likely to:

- Help establish the context appropriately;
- Ensure the interests of all stakeholders are understood and considered;
- Ensure that risks are adequately identified;
- Bring together different areas of expertise when assessing or analyzing risks;
- Ensure that different, and sometimes opposing, views are appropriately considered when defining risk criteria and in evaluating risks;
- Help secure endorsement and support for a treatment plan; and
- Enhance any change management processes associated with the risk.

9. ORIGEN RISK MATRIX (LIKELIHOOD & CONSEQUENCE)

Score	Description of likelihood
A Almost Certain	Highly likely to happen, possibly frequently
B Likely	Will probably happen, but not a persistent issue
C Possible	May happen occasionally
D Unlikely	Not expected to happen, but is a possibility
E Rare	Very unlikely this will ever happen

RISK RATING - MANAGEMENT ACTION REQUIRED
• **Extreme risk** = immediate attention & response needed; requires a risk assessment & management plan prepared by relevant senior managers for Vice-President; risk oversight by Council or nominated Standing Committee or Management Committee
• **High risk** = risk to be given appropriate attention & demonstrably managed; reported to Vice-President or other senior Executives / Management Committees as necessary
• **Medium risk** = assess the risk; determine whether current controls are adequate or if further action or treatment is needed; monitor & review locally, e.g., through regular business practices or local area meetings
• **Low risk** = manage by routine procedures; report to local managers; monitor & review locally as necessary

RISK MATRIX

CONSEQUENCE / LIKELIHOOD	1 Insignificant	2 Minor	3 Moderate	4 Major	5 Extreme
A - Almost certain (frequent)	**M**	**M**	**H**	**E**	**E**
B - Likely (probable)	**L**	**M**	**H**	**H**	**E**
C - Possible (occasional)	**L**	**M**	**M**	**H**	**H**
D - Unlikely (uncommon)	**L**	**L**	**M**	**M**	**H**
E - Rare (remote)	**L**	**L**	**L**	**L**	**M**

Score	Generic impact description	Area of impact - description of consequence					
		Education & Research	Human	Service delivery	Brand & reputation	Finance	Compliance
5 Extreme	Event or circumstance with potentially disastrous impact on business or significant material adverse impact on a key area	• Huge loss / reduction in employee enrolments / retention • Loss of a Branch • Serious reduction in research activity / output • Serious problems reaching a number of employees, training, or research targets • Irreparable impact on relationship with partners / collaborators	• Serious injury or death • Loss of significant number of key staff impacting on skills, knowledge & expertise • Staff industrial action • Employee unrest / protest / violence	• Cessation of major critical business systems or Education / Research programs for an intolerable period and / or at a critical time in the Origen calendar	• Long term damage to reputation or G08 status • Sustained negative media attention; • Brand / image affected nationally and / or internationally	• Huge financial loss • Significant budget over-run with no capacity to adjust within existing budget / resources • May attract adverse findings from external regulators or auditors	• Serious breach of contract or legislation • Significant prosecution & fines likely • Potential for litigation including class actions • Future funding / approvals / registration / licensing in jeopardy
4 Major	Critical event or circumstance that can be endured with proper management	• Significant loss / reduction in employee enrolment / retention • Loss of a employee key • Major impact on research activity over a sustained period • Major problems meeting training or research targets • Serious long-term damage to partnership / collaboration	• Serious injury • Dangerous near miss • Loss of some key staff resulting in skills, knowledge & expertise deficits • Threat of industrial action • Threat of employee protest / activity	• Cessation of major critical business systems or Education / Research programs for an unacceptable period and / or at a critical time in the Origen calendar	• Sustained damage to brand / image or reputation nationally or locally • Adverse national or local media coverage	• Major financial loss • Requires significant adjustment to approved / funded projects / programs	• Major breach of contract, Act, regulations or consent conditions • Expected to attract regulatory attention • Investigation, prosecution and / or major fine possible
3 Moderate	Significant event or circumstance that can be managed under normal circumstances	• Significant loss / reduction of number of employees in a course • Loss of a key academic course • Significant impact on research activity over a sustained period • Significant problem meeting or research targets • Significant but short-term damage to partnership	• Staff injury, lost time or penalty notice due to unsafe act, plant, or equipment • Short term loss of skills, knowledge, expertise • Severe staff morale or increase in workforce absentee rate • Employee dissatisfaction	• Major service delivery targets cannot be met • Loss / interruption / compromise of critical business systems or Education / Research program for a protracted period of time	• Significant but short-term damage to reputation • Employee/ stakeholder and / or community concern • Sustained / prominent local media coverage	• Significant financial loss • Impact may be reduced by reallocating resources	• Significant breach of contract, Act, regulation or consent conditions • Potential for regulatory action
2 Minor	Event with consequences that can be readily absorbed but requires management effort to minimize the impact	• Moderate reduction in employee enrolments / retention • Minor impact on research activity • Temporary problems meeting some training / research targets	• Health & safety requirements compromised • Lost time or potential for public liability claim • Some loss of staff members with tolerable loss / deficit in skills • Dialogue required with industrial groups or employee body	• Local service or Education / Research program delivery problems • Loss / interruption / compromise of critical business systems or Education / Research program for tolerable period but at an inconvenient time	• Some short-term negative media coverage • Concern raised by employees / stakeholders	• Some financial loss • Requires monitoring & possible corrective action within existing resources	• Minor non compliances or breaches of contract, Act, regulations, consent conditions • May result in infringement notice

1 Insignificant	Some loss but not material; existing controls and procedures should cope with event or circumstance	• Minor reduction in employee enrolments / retention • Negligible impact on research activity or achievement of training / research targets	• Incident with or without minor injury • Negligible skills or knowledge loss • Dialogue with industrial groups / employees may be required	• Negligible impact on delivery of service	• Minor damage to brand, image, or reputation	• Unlikely to impact on budget or funded activities	• Unlikely to result in adverse regulatory response or action