Project Risk Management
Applying the Three Lines of Defence Model to Project Risk Management
Table of Contents

Introduction  4
Enterprise Risk Management  6
Project Risk Management  8
Bridging the Gap – Applying Three Lines of Defence to Project Risk Management  9
Guiding Principles in Applying the Three Lines of Defence  13
A Closer Look at Project Risk Reviews  19
Introduction

It is no longer change, but disruption that is the norm

*Change = projects = risk*

A clear sign that the Australian economy is experiencing disruption is the rate that the gap is growing between businesses with increasing revenues and those with declining revenues. Businesses are facing more intense pressures to respond to changing customer demands and new market entrants. Policy makers are reshaping their agendas. The forces of disruption are not just driven by start-ups and felt by business leaders – they are driving significant change across all industries and organisations. Much of that change is implemented through programs and projects of work. The challenge for most organisations is that the track record for project success is patchy at best. Projects are synonymous with change, and change, by its very nature is risky. Often quoted reports from Standish over a 20 year period have consistently reported project failures at the rate of 20-40%, with a further 35-55% described as ‘challenged’. A recent report from Gartner highlights that 32% of Information, Communication and Technology (ICT) projects do not complete on budget and have an average budget variance of 19%. While the average figures are concerning, there are also the catastrophic failures, which cost exponentially more than was originally intended, not counting the reputational cost.

---

3. Gartner, 2014 ‘IT Key Metrics Data 2015: Key Applications Measures: Project Measures’
Financial exposure to project risk is typically unquantified and growing

The extent of exposure to financial risk from project failure receives surprisingly little attention, particularly for ICT projects. For a start, there is scant reporting or statistics on the cumulative spend for organisations in any one year on projects. In 2015 the Victorian Auditor-General was highly critical in a report on Government’s accountability for ICT projects expenditure, stating:

'It seems incongruous that there are financial reporting directions requiring agencies to report on their consultancy and government advertising spend and yet there is none for ICT, which costs government significantly more...I urge the Department of Premier and Cabinet, as the agency now responsible for the leadership of ICT use in the Victorian Government, to task agencies and entities across all sectors to better account for the significant expenditure of taxpayers funds for ICT projects.'

Typically, organisations spend anywhere between 10% and 40% of their annual budgets on ICT projects. This represents a significant financial exposure for any organisation, particularly when considering the high rate of failures and budget variances. Despite this, the application of project risk management measures is still inadequate both in quality and consistency as well as the linkage of project risk to the enterprise risk frameworks. In an environment where the mechanism to implement change is by way of complex projects, adequate management of these project risks is critical.

The current state of project risk management
There are various ways organisations manage project risks to keep their projects on track. In large organisations, this is typically managed through a combination of the following roles/groups:
• Project management teams
• Project Boards / Steering Committee
• Business-as-usual and end user stakeholders
• Project Management Office (PMO)
• Portfolio office
• Enterprise risk management specialists
• Compliance officers
• Quality inspectors
• Internal auditors.

Smaller organisations primarily manage project risk through the project management team with support from a project management or portfolio office. However, Gartner reports that only 28% of organisations they surveyed had risk assessment processes in place for their ICT development projects.

Purpose of this document
The purpose of this document is to outline a point of view and guiding principles on how to cohesively manage project risks. By applying risk, controls and assurance principles through the Three Lines of Defence model, we explore the roles of project management teams, risk functions and assurance functions in project risk management.
Enterprise Risk Management

Increasingly, effective enterprise risk management utilises a ‘three lines of defence’ model

The three lines of defence in effective risk management and control
The Three Lines of Defence model was created following the Global Financial Crisis to provide a cohesive and coordinated approach to risk and assurance by organising essential roles and duties into three levels or ‘lines of defence’. The model (Figure 1) has become a generally accepted industry framework for managing enterprise risk at the strategic, tactical and operational levels and sets out how risks can be managed effectively\(^6\). It is appropriate for any organisation regardless of size or complexity.

Figure 1: Three lines of defence

<table>
<thead>
<tr>
<th>Enterprise Risk</th>
<th>Business Units</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Units</td>
<td>• Functions that own and manage risks directly. Responsible for corrective actions to address process and control deficiencies.</td>
</tr>
<tr>
<td>Risk and Compliance</td>
<td>• Functions that develop and maintain risk management policies and methodologies, identify and monitor new and emerging risks and enforce the enterprise risk management model</td>
</tr>
<tr>
<td>Internal Audit</td>
<td>• Limited independence</td>
</tr>
<tr>
<td></td>
<td>• Reports primarily to management.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>1st line of defence</th>
<th>Business Units</th>
</tr>
</thead>
<tbody>
<tr>
<td>Day to day risk management and control</td>
<td>• Functions that own and manage risks directly. Responsible for corrective actions to address process and control deficiencies.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2nd line of defence</th>
<th>Business Units</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functions that oversee risk</td>
<td>• Functions that develop and maintain risk management policies and methodologies, identify and monitor new and emerging risks and enforce the enterprise risk management model</td>
</tr>
<tr>
<td></td>
<td>• Limited independence</td>
</tr>
<tr>
<td></td>
<td>• Reports primarily to management.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>3rd line of defence</th>
<th>Business Units</th>
</tr>
</thead>
<tbody>
<tr>
<td>Independent assurance</td>
<td>• Functions that provide independent assurance that risk management is working effectively</td>
</tr>
<tr>
<td></td>
<td>• Greater independence</td>
</tr>
<tr>
<td></td>
<td>• Reports to governing body.</td>
</tr>
</tbody>
</table>

\(^6\)Internal Institute of Auditors, 2013. The three lines of defence in effective Risk Management and Control, IIA.
Roles and responsibilities of Executive Management, Board and Regulators

Across the three lines of defence, Executive Management and the Board of Directors play a key role in risk governance. From an enterprise risk perspective:

- The Board of Directors sets and monitors the organisation’s risk appetite, processes, risk model and reporting framework.
- Executive Management translates the organisation’s risk appetite and strategy, processes, risk model and reporting framework into operations.
- External auditors, regulators, and other external bodies reside outside the organisation’s structure, but they have an important role in the organisation’s overall governance and control structure. This is particularly the case in regulated industries, such as financial services or insurance.

Regulators sometimes set requirements intended to strengthen the controls in an organisation. On other occasions, they perform an independent and objective function to assess the whole or some part of the first, second, or third line of defence with regard to those requirements.

When coordinated effectively, external auditors, regulators, and other groups outside the organisation can be considered as additional lines of defence, providing assurance to the organisation’s shareholders, including the governing body and senior management. However, because the scopes and objectives of these reviews vary depending on the intention and audience, the risk information they gather is generally less extensive than what is addressed by an organisation’s internal three lines of defence.
Project Risk Management

There are a number of project methods and frameworks adopted by organisations, each of which considers project risk management. For the purposes of this document, we use one of the most prevalent methods, PRINCE2®

**PRINCE2®, risk management and project assurance**

PRINCE2®, a project and program methodology developed by the UK’s Office of Government Commerce, has become an international standard for project management. PRINCE2® recommends project risk management to be systematic and include the ‘proactive identification, assessment and control of risks that might affect the delivery of the project’s objectives’. It sees program and project assurance as integral to mitigating project risks. Program and project assurance is the responsibility of the Project Board, but can be delegated. PRINCE2® advocates three types of assurance: user, business and supplier. ‘Project assurance is not just an independent check. Personnel involved in project assurance are also responsible for supporting the Project Manager, by giving advice and guidance’.

[Figure 2: PRINCE2® Project Management Team Structure](#)
Bridging the Gap – Applying Three Lines of Defence to Project Risk Management

This section outlines the principles and considerations for applying the three lines of defence in project risk management.

An organisation can benefit when the Three Lines of Defence model is applied to project risk management by:

• Having a cohesive and proactive approach to identify, assess, mitigate, report, monitor and manage project risks
• Having a holistic and consistent approach to project risk management across the organisation
• Providing appropriate coverage and identifying ‘blind spots’ which may not be identified
• Clarifying roles in each line of defence, from project management, control functions (e.g. enterprise project management offices (ePMOs)), internal audit and external providers.
Applying the three lines of defence to project risk management

As the first line of defence, the project management team ensures that project risks are identified, analysed, owned and managed appropriately. Risk owners are accountable for ensuring that corrective actions are implemented to address project process and control deficiencies. Project management ensures that project risk management activities are consistent with the project’s goals and objectives.

There are some occasions where the first line of defence may be facilitated by a PMO (or Project Support Office). This PMO may include risk coordinators residing within the project. In this scenario, project management remains responsible for ensuring that projects’ risks are managed appropriately, with the PMO proactively facilitating the risk management process.

The second line of defence provides subject matter expertise through a facilitation or support role to assist the first line in project risk management. The specific functions will vary by organisation, industry, size and risk of the project, but typical functions in this second line of defence are outlined in Table 1.

<table>
<thead>
<tr>
<th>Function</th>
<th>Responsibilities</th>
</tr>
</thead>
</table>
| Risk Management Function or Committee | • Facilitates and monitors the implementation of effective risk management practices by project management  
• Assists risk owners in defining the target risk exposure and reporting adequate risk-related information throughout the organisation for all projects, or a select number of projects which are high risk or critical to an organisation’s success. |
| Compliance Function | • Monitors various specific risks such as non-compliance with applicable strategies, policies and regulations. In this capacity, the separate function (e.g. an ICT architecture committee, business reference groups) reports directly to the project governance forum (e.g. Steering Committee, Project Board). |
| Enterprise PMO | • Monitors risks and reporting issues  
• Supports the Project Director or Project Manager to ensure the first line of defence is properly designed, in place and operating as intended. |

Table 1: Second line of defence functions (examples only)
It is possible that specific second line expertise may be outsourced or co-sourced by an external provider.

These functions have some degree of independence from the first line of defence, but are management functions by nature. As management functions, they may intervene directly in modifying and developing the risk management and internal control systems. Therefore, the second line of defence serves a vital purpose, but cannot offer truly independent risk assessments to governing bodies. The responsibilities of these functions vary on their specific nature, but can include proactively:

- Developing, enforcing and maintaining project risk management frameworks
- Identifying known and emerging risks and issues to Executive Management, Board of Directors, Project Sponsor, project governance forums and project management in the project’s ability to deliver successfully
- Supporting project risk management policies and processes, defining roles and responsibilities, and setting goals for implementation. This may be part of the overall risk management policy or framework, or part of the organisation’s project management methodology
- Assisting management in developing processes and controls to manage project risks and issues
- Providing guidance and training on project risk management policies and processes
- Providing guidance, advice or subject matter expertise to the project in managing its risks, however not playing a role in project delivery
- Aggregating project risks across the portfolio and reporting these to Executive Management and Board of Directors
- Identifying shifts in the organisation’s implicit risk appetite and determining how this will impact on project risk management processes and methodologies
- Facilitating and monitoring implementation of effective project risk management practices by project teams to ensure consistency across projects
- Monitoring the adequacy and effectiveness of project controls, accuracy and completeness of project reporting, project’s compliance/alignment with policy and strategy, and timely remediation of deficiencies.

When managing project risk, this arms-length, proactive advisory role can make a significant difference to a project’s likelihood for success.

The third line of defence provides the organisation’s executive management, Board of Directors, Audit and Risk Committee and/or Project Board with independent assurance on the effectiveness of governance, risk management, and internal controls within a project. This includes the manner in which the first and second lines of defence achieve risk management and control objectives. From a project risk management perspective, the third line of defence function can provide these groups with insight on the organisation’s effectiveness in managing project risks, especially for projects having a major financial, compliance or regulatory impact to the organisation. The scope of this assurance usually covers:

- Efficiency and effectiveness of project management practices
- Reliability and integrity of reporting processes
- Compliance with laws, regulations, policies, procedures and contracts
- That the risk of the project has been assessed, an appropriate assurance plan is in place, and the plan is being delivered.

It should also ensure that the business functions used within the project are consistent with the organisational standards and policies – including contract, procurement, communication, safety, HR management, financial management and asset management.

This level of assurance is typically provided by an external project assurance provider or through an organisation’s internal audit function.
Summarising the three lines of defence for project risk

In a project environment, the Project Board (or Project Steering Committee) is ultimately accountable for the governance of the project and ensures that risks are managed appropriately. It plays a critical role in ensuring that the three lines of defence are cohesively working together and managing risks to enable the project to succeed. Executive Management and the Board of Directors provide oversight over the high risk projects and the organisation’s cumulative risk profile.

Figure 3: Three lines of defence
Guiding Principles in Applying the Three Lines of Defence

Applying the Three Lines of Defence model to project management is not a ‘one size fits all’ approach.

The roles and responsibilities for each line of defence and who is assigned to perform each line is dependent on the organisation’s capabilities, industry, resources and the project’s risk profile, size, complexity and environment.

The following principles provide guidance on how the three lines can be used in project risk management along with a number of considerations to reflect upon.
Principle 1
Align with the organisation’s capabilities, industry and resources

The assignment of roles and responsibilities for each line of defence to a function or individual are dependent on the organisation’s capability, industry and available resources.

The first line of defence is typically provided by the project or program management team. It may also be provided by a PMO or Project Support Office specifically established for the project. The role of business units in a project environment should not be discounted, as their involvement will support the project in managing risks outside of the project’s control, aligning with expected customer outcomes and balancing the focus between customer needs and delivering in the expected time, cost and quality.

While PMOs may institute a form of governance, the results of their project risk management activities do not necessarily get escalated to the Board or an independent person in the organisation. PMOs have also had little organisational authority to intervene if a project is under-performing, or to ensure assurance recommendations are actioned.

The second line of defence is where the most variation comes in. It is not only dependent on the organisation’s capabilities and resources, but also on the project’s risk profile, size, complexity and environment (see Principle 2). Enterprise PMOs typically operate in the second line to have oversight of project delivery and facilitate the project risk management process. In larger organisations, it is frequently observed that the ePMO will have second and third lines responsibilities. Specifically, an assurance function within an ePMO will operate in the third line of defence to provide project assurance expertise on higher risk projects.

The third line of defence must be independent of the project and is typically provided by an internal audit function or external project assurance provider. In smaller organisations, the internal audit function or an ePMO with a project assurance function may sometimes play a role in performing second line activities. Where both second line and third line functions exist, reliance can often be placed on project assurance activities performed by the internal audit function or project assurance function within the ePMO to provide independent assurance to Executive Management, the Project Board or an Audit and Risk Committee.

Role of Internal Audit: Internal Audit has typically focused on adherence to project management methodologies rather than reviewing the effectiveness of controls to increase the likelihood of project success. At a minimum, Internal Audit should be ensuring that Executive Management and the Board of Directors are getting visibility of high risk projects and the organisation’s cumulative risk profile. A proactive assurance framework should be in place and have been provided by resources with the appropriate expertise and capability. Increasingly, Internal Audit is bolstering its capability in providing project assurance by sourcing external experts, and providing consistent and coordinated reporting the relevant governance forums.

---

Principle 2
Consider the project’s risk profile, size, complexity and environment

The level of involvement of each line of defence depends on the project’s risk profile, size, complexity and environment. For example, a large, complex project may require:

- A more proactive, frequent and efficient risk management and escalation process for the first line
- The second line function/s to perform targeted reviews for specific risk areas (e.g. security, fraud) which are sourced from an external party with specific expertise. The scope of this role is broader, covering the project context (including governance), the project itself, and the solution being delivered. Increasingly, this external capability is being sourced through ePMOs to ensure a consistent service and appropriate skill sets are engaged.

Principle 3
Application is based on the key stakeholders who need to be informed and involved in managing project risk

From a first, second and third line perspective, the project sponsor and project board are informed to provide oversight over how project risks are managed.

From a third line perspective, in addition to the project sponsor and project board, activities could also be reported to executive management, other agencies (e.g. Treasury in Government) and the Board or Audit and Risk Committee, depending on the risk of the project.

The Project Board is ultimately accountable for project governance, which will include understanding the impacts of the risks reported or escalated to them, and providing strategic direction on how these risks can be mitigated.

\footnotesize{Huibers, S. 2015, ‘The Evolution of Project Auditing, 2015 Global Benchmark Study Results’}
Principle 4

Document and approve the framework or plan to undertake project risk activities

The second line function defines, enforces and maintains a risk management framework and/or project management methodology to guide the first line function on how to manage project risks.

A project assurance plan which derives all relevant project risk reviews for a specific project is documented with an agreed purpose, scope and approach. This ensures that each item in the plan has a distinct purpose and collectively addresses enterprise and project risks.

The responsibility for deriving an assurance plan is dependent on the project’s risk profile, size, complexity and organisation’s resources and capabilities. For a large and complex project, this will typically involve the third line function coordinated with the first and second line functions.

Principle 5

Minimum impact and cost for project risk reviews

Specifically from a second and third line perspective:

- Project risk management activities, especially risk reviews done on a project, are designed to support the project by minimising the impact on the project, working with the project team and supporting them in achieving project success. However, the organisation should consider how often their involvement will be with the project. For example, it is recommended that project reviews should start early in the project’s planning stages, and then at a minimum, timed to coincide with key decision points and at regular points in the project lifecycle for longer term projects (i.e. reviews held no more than 6 months apart)

- The costs associated with the level of involvement for project risk reviews are appropriate, justified and aligned with the project’s risk profile

- There are currently no clear guidelines on costing efforts relating to project risk review activities done in the second and third line. However, there is an emerging trend that this cost can be 2% of a project’s budget and is allocated to second and third lines for a medium – risk project

- From a funding perspective, there are two main options for consideration: whether funding for project assurance is sourced from the project’s budget or managed through a central funding source. There are pros and cons for each option, but increasingly organisations are mandating that it is funded by the project and costed into the project’s business case.

Oakes, G. 2008, ‘Project Reviews, Assurance and Governance’
Principle 6
Align with project management standards

The approach for project risk management is aligned with current industry standards in project management, such as PRINCE2®.

Principle 7
Consistent with risk and assurance frameworks and standards

The approach for project risk management is consistent with risk and assurance frameworks for the organisation and the industry it is in.

From a third line perspective, the approach and plan are consistent with Internal Audit standards and frameworks, such as the International Professional Practices Framework (IPPF) and Institute of Internal Auditors (IIA) standards.

Principle 8
Integrated, risk-based and action oriented

The three lines of defence work best when they are operating in a cohesive and integrated manner. The approaches for the first line (owning and managing risks), second line (defining methods and tools and supporting the first line) and third line (project assurance) should be risk-based and action oriented. Specifically for the second and third lines, project assurance plans, which derive all relevant project risk reviews for a specific project, should be integrated with other project assurance plans (especially if the project is part of a program) and the broader assurance plan for the organisation. They should also be risk-based and lead to action.

From a governance perspective, the application of the three lines of defence will need to be integrated or overlayed with the organisation’s governance framework and structure.

Consider if there is a need to integrate project risk registers with risk registers belonging to dependent projects, programs (if the project is part of an overall program), operations and the whole enterprise. The link between project, operational and enterprise risk registers will be important if a specific risk will materially impact business-as-usual operations or the entire organisation.
Figure 4 shows an illustrative example of a governance structure for a medium sized, high risk project in a large organisation. In this scenario, the ePMO plays across the second and third lines, to support the first line with methodologies and tools (second line role) and working with an external project assurance provider and internal audit together to define and deliver a project assurance plan (second and third line role).

Figure 4: Governance Structure Example
A Closer Look at Project Risk Reviews

Increasingly, effective enterprise risk management utilises a ‘three lines of defence’ model

The three lines of defence in effective risk management and control
From a second and third line perspective, a project assurance plan defines all reviews to be undertaken during the life of the project to help manage project risk and improve delivery confidence. This plan should align with the original business case, which will drive the budget and scope for this activity irrespective of whether it is provided internal or external to the organisation. Ideally, reviews should be linked to the organisation’s risk appetite, however most organisations are only just starting to consider risk appetites in their assurance design.

Many large organisations have a panel of external providers or a preferred partner. Often, the project is given the choice of determining who from the panel should provide these services. In determining a provider, the key factors to consider should be experience, capability and relevance. Our recommendation is that:

• The mandate for project risk reviews is embedded in investment decision committees
• Assurance plans are developed for all major programs (especially those that support the delivery of an organisation’s strategy)
• An external assurance partner is chosen through a competitive process that includes someone independent to the project. The selected partner takes accountability for proactive project risk management throughout the project’s lifecycle, and is committed to the project’s success.
**The three dimensions**

In all projects, there are three dimensions to a project that can be the subject of project risk reviews, depending on the risk:

- **Project Environment**: the context that the project is operating in
- **Project Delivery**: how the project is being managed
- **Solution**: the ability of the solution to meet business requirements.

In each of these dimensions, there are areas of risk that can be an area of focus:

<table>
<thead>
<tr>
<th>Table 2: Project Risk Review Dimensions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Project Environment</strong></td>
</tr>
<tr>
<td>• Governance</td>
</tr>
<tr>
<td>• Strategic alignment</td>
</tr>
<tr>
<td>• Process alignment</td>
</tr>
<tr>
<td>• Positioning with other projects and</td>
</tr>
<tr>
<td>change initiatives</td>
</tr>
<tr>
<td>• Business environment risk</td>
</tr>
<tr>
<td>• Stakeholder management</td>
</tr>
<tr>
<td>• Corporate culture</td>
</tr>
<tr>
<td>• PMO Support</td>
</tr>
<tr>
<td><strong>Project Delivery</strong></td>
</tr>
<tr>
<td>• Business case</td>
</tr>
<tr>
<td>• Benefits</td>
</tr>
<tr>
<td>• Scope</td>
</tr>
<tr>
<td>• Schedule</td>
</tr>
<tr>
<td>• Cost</td>
</tr>
<tr>
<td>• Project integration</td>
</tr>
<tr>
<td>• Quality and Testing</td>
</tr>
<tr>
<td>• Organisational change</td>
</tr>
<tr>
<td>• Human resourcing</td>
</tr>
<tr>
<td>• Communications</td>
</tr>
<tr>
<td>• Procurement</td>
</tr>
<tr>
<td>• Risks and Issues</td>
</tr>
<tr>
<td>• Planning</td>
</tr>
<tr>
<td>• Contract and Vendor Management</td>
</tr>
<tr>
<td>• Deployment strategy</td>
</tr>
<tr>
<td>• Integration and Interfacing</td>
</tr>
<tr>
<td><strong>Solution</strong></td>
</tr>
<tr>
<td>• Lifecycle related specialist products</td>
</tr>
<tr>
<td>• Technical environment adequacy</td>
</tr>
<tr>
<td>(including privacy/security)</td>
</tr>
<tr>
<td>• Solution sustainability</td>
</tr>
<tr>
<td>• Business case alignment</td>
</tr>
<tr>
<td>• Integration with existing systems/</td>
</tr>
<tr>
<td>processes</td>
</tr>
<tr>
<td>• Business process controls</td>
</tr>
<tr>
<td>• Business Continuity</td>
</tr>
<tr>
<td>• Target Operating Model</td>
</tr>
<tr>
<td>• Data Migration and Management</td>
</tr>
<tr>
<td>• Business readiness</td>
</tr>
</tbody>
</table>

The assurance plan would typically contain one of the four types of reviews:

<table>
<thead>
<tr>
<th>Deep Dives or Targeted Reviews</th>
<th>Specific areas of risk to the project context, delivery or solution are assessed in detail to identify any areas to improve delivery or reduce specific areas of risk (e.g. data migration, security).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health Checks</td>
<td>Higher level, broad assessment of project context and delivery which is used to identify areas of program risk and opportunities to improve successful delivery.</td>
</tr>
<tr>
<td>Continuous Assurance</td>
<td>Checkpoint review (at least monthly intervals aligned with project governance meetings) and continuous review which include a point in time project assessment, attending key governance meetings and assess risks and activities particular to the stage of the project.</td>
</tr>
<tr>
<td>Gateway Reviews</td>
<td>Point in time assessment to support a decision-making milestone.</td>
</tr>
</tbody>
</table>

20
To determine the level of involvement for a project, an assurance plan should be developed in the early stages of a project. Ideally a risk workshop is conducted, involving the key project stakeholders and experts in the particular type of project to identify the major risks. These risks form the basis for the assurance plan, taking into consideration these risks, the organisational capability to deliver, govern and assure the project, governance and funding requirements both internal and external to the organisation, the program structure and the project duration.

Sample Assurance Plan

To provide a holistic assurance activity across the second and third lines of defence, the following outlines a sample assurance plan with deep dive topics determined by the outcomes of a risk workshop.

Figure 5: Sample Assurance Plan

<table>
<thead>
<tr>
<th>Stage 1</th>
<th>Stage 2</th>
<th>Stage 3</th>
<th>Stage 4</th>
<th>Stage 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project Initiation</td>
<td>Project Definition</td>
<td>Project Execution</td>
<td>Project Transition</td>
<td>Benefits Realisation</td>
</tr>
</tbody>
</table>

2nd line of defence

3rd line of defence

Continuous Assurance

Legend

- Deep dives/ Targeted review
- Health check
- Gateway Review
Contact Us

**Sid Maharaj**  
National Project Risk Lead Partner  
Tel: +61 (0) 406 568 171  
sidmaharaj@deloitte.com.au

**Phil Goulstone**  
Project Risk, Sydney  
Tel: +61 (0) 406 705 611  
phgoulstone@deloitte.com.au

**Alastair Banks**  
Project Risk, Melbourne  
Tel: +61 (0) 414 252 138  
abanks@deloitte.com.au

**Natalie Smith**  
Project Risk, Brisbane  
Tel: +61 (0) 405 106 221  
natasmith@deloitte.com.au