DIPRAC: A Framework for Managing Project Risk on Australia's Defence Estate

Version 0.2, For Review, 11 June 2025

WHITE PAPER

DECNet Pty Ltd
ACN: 670 900 259 / ABN: 35 670 900 259
Middle Cove, NSW 2068
darian.macey@decnet.com.au

11 June 2025

Request for Feedback – DIPRAC White Paper on Risk and Contingency Management

Dear colleagues,

I'm pleased to share with you a discussion draft of DECNet's new white paper, DIPRAC: A Framework for Managing Project Risk on Australia's Defence Estate. This paper proposes a standardised approach to risk and contingency management tailored specifically for the challenges of Defence infrastructure projects.

As many of you know, Defence projects often suffer from fragmented risk practices, excessive fee inflation due to poor contract conditions, and limited benchmarking across the Estate. The DIPRAC framework responds to these issues by providing a Defence-specific methodology that integrates calibrated risk assessments, historical benchmarking, and practical stakeholder engagement strategies.

The paper draws on real-world case studies, outlines practical implementation steps, and includes tools like a risk categorisation matrix, benchmarking data, and a calibrated question template.

We're now inviting comment from the Defence Estate community. Your feedback—particularly around implementation feasibility, integration with existing contract structures, and opportunities for policy alignment—will help refine this framework before formal release.

Please download the white paper and submit any comments or suggestions by Friday 30 June 2025. Feedback can be emailed to me directly at darian@decnet.com.au or through the DECNet website.

This is an opportunity to shape how risk is managed across the Defence Estate for years to come. Your input is valued and appreciated.

Kind regards,

Darian Macey
Founder

M: 0499 550 219
E: darian.macey@decnet.com.au

Contents

Executive Summary 3
1 Introduction 4
2 Current Challenges in Risk Management 5
2.1 Overview of Inherent Risks and Complexities 5
2.2 Limitations of Existing Risk Management Approaches 6
2.3 Consequences of Conventional Risk Allocation 7
2.4 Towards an Improved Approach 7
3 Proposed Framework 9
3.1 Overview 9
3.2 Principles and Objectives 9
3.3 Distinguishing Features and Improvements 9
3.4 Eight Categories of Project Risk 9
4 Implementation of the Framework 12
4.1 Benchmarking Process – Steps to Gauge Project Risk 12
4.2 Calibrated Questions – Quantifying Risk and Predicting Contingency 13
5 Case Studies 15
5.1 Case Study 1: Upgrading a Remote Communications Installation 15
5.2 Case Study 2: Construction of a New Training Facility 16
5.3 General Lessons from the Case Studies 16
6 Benefits of the Framework 18
7 Industry Implications and Recommendations 20
7.1 Widespread Adoption for Collective Benefit 20
7.2 Policy and Governance Integration 20
7.3 Recommendations for Policy Development: 20
7.4 Recommendations for Professional Training: 21
8 Call to Action 21
9 Conclusion 23
10 References 24
Appendices (Available upon request) 25

Executive Summary

This white paper presents a comprehensive proposal for a **standardised risk and contingency framework** specifically designed to address the unique challenges of Defence infrastructure projects. Recognising the critical nature of these projects to national security and the inherent complexities involved, the paper outlines a strategic approach to risk management that aims to significantly enhance project predictability, efficiency, and success.

Purpose and Key Findings: The primary purpose of this white paper is to introduce and advocate for the adoption of a standardised framework for managing risk and contingency planning within Defence infrastructure projects, titled the **Defence Infrastructure Project Risk and Contingency (DIPRAC) framework**. The findings highlight current shortcomings in existing risk management practices, notably the inadequate handling of project complexities and the problematic transfer of excessive risk onto design consultants. This often leads to inflated project costs and diminished efficiency, threatening the timely and budget-conscious delivery of essential Defence infrastructure.

Importance of the Framework: The DIPRAC framework has been developed with the specific needs and challenges of Defence infrastructure projects in mind. It offers a robust structure for identifying, categorising, and mitigating risks through a systematic, tailored approach. The framework emphasises the strategic allocation of contingencies, informed by detailed risk quantification and benchmarking against industry standards and historical data. Its implementation promises not only to streamline project delivery but also to foster more accurate budgeting and scheduling, ensuring that Defence infrastructure projects achieve their strategic objectives while optimising resource use.

Call to Action: We urge all stakeholders in the Defence infrastructure sector—ranging from policymakers and project managers to design consultants and contractors—to embrace and implement a standard risk and contingency framework. By doing so, the industry can collectively enhance the management of risk and contingency, leading to more predictable, efficient, and successful project outcomes. This call to action is not merely a recommendation for process improvement; it is a strategic imperative to uphold the integrity and effectiveness of national Defence infrastructure projects. Adopting this framework represents a significant step toward achieving excellence in project delivery, aligning with best practices and fostering a culture of continuous improvement and strategic foresight in Defence Estate development.

1 Introduction

In the planning of Defence infrastructure projects, the stakes are high and the complexities are vast. These projects—pivotal to national security and operational readiness—navigate a unique landscape of regulatory, environmental, and logistical challenges. Effective risk management within this context is not just beneficial; it is imperative. It ensures that projects not only meet their strategic objectives but do so within budget and on time, safeguarding both public resources and national interests.

However, the current landscape of risk management in the Defence infrastructure sector is fraught with challenges. Traditional approaches often fall short when confronted with the sector's inherent complexities, leading to cost overruns, delays, and, in some instances, compromised project outcomes. This situation is exacerbated by contractual conditions that disproportionately shift project risk onto design consultants, compelling them to inflate their fees to mitigate potential liabilities. The result is an escalation in the overall cost of the planning phase, impacting the efficiency and financial viability of crucial Defence infrastructure projects [1].

This white paper addresses these challenges by proposing a standard risk and contingency framework tailored for Defence infrastructure projects, titled the **Defence Infrastructure Project Risk and Contingency (DIPRAC) framework**. Building upon the Estate & Infrastructure Group's **Risk Management Framework (RMF)** published in 2016 [2], the objective is to enhance the predictability and efficiency of project delivery through a structured approach to risk management, thereby improving outcomes and safeguarding national interests.

2 Current Challenges in Risk Management

2.1 Overview of Inherent Risks and Complexities

Defence infrastructure projects are often caught in a web of multifaceted challenges, each adding a layer of difficulty to their successful delivery. These challenges are frequently interlinked and mutually reinforcing, collectively amplifying the overall risk profile of projects. Key areas of complexity include:

- **Geographic and Location Challenges:** The Defence Estate encompasses a wide range of sites across Australia, each with distinct location-specific risks. The remoteness of many sites poses significant access challenges, affecting logistics and the mobilisation of resources. Climate variability across regions introduces further unpredictability, impacting planning, construction timelines, and execution. Additionally, local industry capacity can vary widely, affecting the availability and cost of labour and materials. Executing similar projects across diverse geographies requires a nuanced understanding of regional differences.
- **Environmental Challenges:** Environmental considerations are paramount, ranging from the presence of unexploded ordnance and hazardous materials to the protection of natural, historical, and Indigenous heritage sites. These factors pose significant risks to safety and schedules, and they demand a careful balance between development and conservation. Projects often require extensive environmental impact assessments and mitigation strategies to manage these risks.
- **Coordination and Stakeholder Engagement:** Successful execution hinges on effective coordination and stakeholder engagement. Defence projects involve harmonising the diverse interests of stakeholders including federal and local government entities, Defence capability managers, and Indigenous communities. This requires sophisticated communication and negotiation to align objectives. Complexity is further enhanced by the need to integrate sustainability initiatives (such as adaptive reuse of assets) and operational considerations (like ensuring operational continuity during construction or aligning with capability upgrades).
- **Technical and Delivery Challenges:** Defence infrastructure initiatives often entail unique technical specifications, constrained budgets, ambitious schedules, and stringent quality standards. Meeting these demands requires advanced technical expertise and innovative project management strategies. Many projects involve integrating cutting-edge technologies or systems, which necessitates a skilled workforce capable of navigating high technical complexity.
- **Legal and Regulatory Compliance:** The legal and regulatory landscape for Defence projects is both dense and complex. Projects must comply with myriad laws, regulations,

and building codes, each introducing requirements that affect planning and execution. Compliance is not optional; it is a critical component of risk management. Failure to navigate legal requirements proactively can result in costly delays or penalties, making in-depth understanding and management of compliance risk essential.

2.2 Limitations of Existing Risk Management Approaches

The current risk management practices in the Defence infrastructure sector exhibit significant limitations that hinder effective handling of these complexities. Key shortcomings include:

- **One-Size-Fits-All Frameworks:** A prevalent reliance on generic risk management frameworks fails to account for the specific nuances of Defence infrastructure projects, leading to suboptimal risk assessment and contingency planning. For example, the Estate & Infrastructure Group's risk breakdown structure includes numerous risk categories irrelevant to Defence Estate projects[3], diluting focus on the most pertinent risks. Moreover, the RMF's guidance to rate financial consequences of risk events in absolute dollar values ignores the proportional impact on a project's budget, and its likelihood ratings (from "rare" to "almost certain") are impractical without thorough investigation, delaying early risk assessment efforts.
- **Focus on Known Risks Over Unknowns:** Traditional approaches, often cantered on exhaustive risk registers, tend to encourage a confirmation bias toward known risks. By emphasising risks that are already recognised, these methods can overlook emerging or unforeseen risks, leaving projects vulnerable to unexpected challenges.
- **Risk Avoidance vs. Contingency Planning:** Standard contract provisions in Defence projects have historically prioritised transferring risk to other parties rather than collaboratively managing it. Clauses driven by commercial interests – such as unlimited liability, unqualified fitness for purpose, and broad consequential loss – push excessive risk onto design consultants. In response, consultants defensively inflate their fees to cover these liabilities, which inflates upfront project costs. Effective risk management should instead be a partnership between clients and contractors, aimed at: (a) establishing a detailed project risk profile; (b) setting a justifiable contingency reserve based on this risk profile; and (c) allocating each risk to the party best equipped to manage it. Such a collaborative approach ensures contingency planning is robust, equitable, and defensible.
- **Lack of Adaptability:** Defence projects are dynamic, yet many existing frameworks are rigid and overly complex, making it difficult to adapt to new information or changing conditions. This rigidity is evident in the challenges faced when initial risk assumptions prove incorrect and contract variations must be negotiated. Without an iterative process to revisit and update risk assessments, projects struggle to accommodate change.

- **Absence of a Standardised System:** There is currently no mandated, standard risk management system across all Defence infrastructure projects. Contractors and consultants for Defence (Security & Estate Group) are allowed to use any risk framework of their choosing, as long as it aligns with their internal business processes. While this flexibility allows for tailored approaches, it severely limits the ability to compare risk data across projects or establish historical benchmarks. Inconsistent application of risk principles and difficulty in aggregating risk data mean lost opportunities for enterprise-level learning and improvement in contingency forecasting.

2.3 Consequences of Conventional Risk Allocation

Certain contractual practices in Defence projects have created significant financial and collaborative challenges:

- **"Unlimited Liability" Clauses:** When design consultants can be held responsible for all costs arising from their work (with no liability cap), they face potentially catastrophic financial exposure. Anticipating this, consultants increase their fees to insure against worst-case scenarios, driving up project costs.
- **"Unqualified Fitness for Purpose" Clauses:** These provisions require that delivered designs fully meet all operational requirements, often without acknowledging evolving or unclear specifications. This holds consultants to an exceptionally high standard under significant uncertainty, leading them to include buffers in time and cost to avoid failing to meet undefined expectations.
- **Broad "Consequential Loss" Clauses:** By exposing consultants to liability for indirect losses (e.g. lost productivity or delays impacting broader project outcomes), these clauses introduce high uncertainty. Consultants respond by inflating fees to cover the unpredictable scope of potential claims.

Implications: Together, these contractual conditions foster a risk-averse and adversarial environment. Design consultants, under threat of expansive liabilities, adopt defensive practices such as fee inflation and rigid adherence to scope, rather than engaging in innovative problem-solving or partnership. For Defence as the project owner, this results in higher upfront costs and a less collaborative project atmosphere. Ultimately, the traditional strategy of shifting risk outward has proven counterproductive, underscoring the need for a more balanced and proactive risk management approach.

2.4 Towards an Improved Approach

The challenges outlined above highlight a clear need to reform risk management in Defence infrastructure projects. One-size-fits-all frameworks, an overemphasis on known risks, rigid

contracts, and non-standardised practices not only hamper effective risk mitigation but also drive up costs and erode trust among stakeholders. To address these issues, the Defence infrastructure sector must shift toward a more nuanced, adaptive, and collaborative risk management paradigm. Embracing a new framework that accounts for Defence-specific complexities and encourages partnership in risk allocation is crucial for enhancing project predictability, efficiency, and success. The following section introduces the proposed DIPRAC framework, which is designed to meet these needs and set a new benchmark for risk management excellence in Defence projects.

3 Proposed Framework

3.1 Overview

The **Defence Infrastructure Project Risk and Contingency (DIPRAC) framework** is a structured yet flexible model developed to streamline risk management for Defence Estate projects. It is grounded in the recognition of the unique, recurring challenges these projects face and provides a systematic approach to identifying, assessing, and mitigating risks.

3.2 Principles and Objectives

The framework operates on core principles of thoroughness, adaptability, and stakeholder engagement. Its key objectives are to:

- Systematically identify and categorise risks at every stage of a project's lifecycle.
- Improve the quantification of risks to enhance the predictability of project outcomes.
- Enable more effective allocation of resources, particularly contingency funds, based on quantified risk insights.
- Strengthen collaborative decision-making by involving all relevant stakeholders in risk assessment and mitigation.

3.3 Distinguishing Features and Improvements

Unlike existing models, the DIPRAC framework introduces several improvements:

- It **tailors risk categories** specifically to Defence infrastructure intricacies, ensuring that risk assessment focuses on what truly matters for these projects.
- It incorporates **dynamic assessment techniques** that allow risk evaluations to be updated as projects evolve or as external conditions change.
- It promotes **continuous stakeholder involvement** in the risk management process, ensuring that diverse perspectives (from technical experts to end-users) inform risk identification and response strategies.

3.4 Eight Categories of Project Risk

At the heart of DIPRAC is a categorisation of project risks into eight domains common to Defence Estate projects:

1. **Coordination Risk:** Challenges in integrating various project components and stakeholder contributions. For example, coordinating multiple design disciplines for a facility upgrade can introduce delays or design conflicts if not managed properly.

2. **Environmental and Heritage Risk:** Risks arising from environmental regulations, site contamination, or heritage preservation requirements. For instance, encountering unexploded ordnance or protected species during construction can halt work and necessitate special mitigation measures.
3. **Location Risk:** Risks related to the project's geographical setting, such as remote site access difficulties, extreme climate conditions, security restrictions, operational importance, or regional regulatory differences. Projects in hard-to-access or harsh environments may incur higher logistics costs and scheduling uncertainties.
4. **Stakeholder Risk:** Risks stemming from the complexity of managing diverse stakeholder expectations and requirements. Conflicting needs or priorities among Defence branches or between Defence and local communities can lead to scope changes or delays.
5. **Information Risk:** Uncertainties due to gaps or inaccuracies in project data and documentation. Inadequate site surveys or incomplete project briefs can result in unforeseen problems emerging during design or construction.
6. **Technical Risk:** Challenges inherent in meeting the technical and engineering requirements of the project. High technical complexity or the need for specialised technologies and expertise can increase the risk of design revisions and cost escalations.
7. **Delivery Risk:** Challenges inherent in meeting the project's schedule, budget, and quality objectives, as well as integrating activities across concurrent projects. High time pressures, strict budget constraints, demanding quality expectations —such as requiring a high level of detail (LOD) in Building Information Modelling (BIM) deliverables—and the need to coordinate multiple related projects simultaneously can increase the risk of delays, cost overruns, and compromised outcomes.
8. **Contractual Risk:** Risks introduced by contract terms and conditions that unfairly allocate liability (such as the clauses described earlier). These can lead to increased costs and strained relationships if not addressed through balanced risk-sharing arrangements.

Key Considerations in Applying DIPRAC: Several factors influence how the framework is applied:

- **Timing of Application:** The planning phase of projects is critical for risk reduction. By applying DIPRAC at project initiation and revisiting it at each key planning milestone, risks can be progressively identified and mitigated before the execution phase. Early and iterative use of the framework ensures a smoother delivery later.
- **Economies of Scale:** Larger projects can leverage economies of scale in risk management. Many planning-phase risk assessment tasks have a fixed cost that does

not increase in proportion to project size (e.g. baseline studies or standard design tasks). Thus, on bigger projects, the relative cost (as a percentage of total budget) of thorough risk planning is lower, justifying bundling of smaller projects into larger ones.

- **Complexity Factors:** Beyond scale, project complexity can vary dramatically. A moderately sized project with significant complexity (for example, a build on a sensitive environmental site requiring extensive impact studies) may carry greater risk than a larger but straightforward project. DIPRAC uses calibrated questions to quantify complexity across the eight risk categories, allowing the project team to calculate a **complexity factor**. This factor adjusts the planning-phase budget by adding a risk premium (contingency) proportionate to the project's complexity and risk profile.

By accounting for timing, scale, and complexity, the framework facilitates a more accurate prediction of necessary contingencies. The result is that projects begin with appropriately scaled contingency reserves, leaving them better prepared to navigate the uncertainties inherent in Defence infrastructure development.

4 Implementation of the Framework

Implementing the DIPRAC framework requires a commitment to thorough analysis, accuracy in data, and active stakeholder participation. The process is both rigorous and adaptable, involving systematic benchmarking and the use of calibrated questions to quantify risks. The following outlines how project teams can put the framework into practice:

4.1 Benchmarking Process – Steps to Gauge Project Risk

Using DIPRAC begins with benchmarking the project against a notional "average" project to understand relative risk levels.

1. **Project Initiation and Data Collection:** Gather all relevant project information at the outset, including scope definition, site characteristics, intended operational requirements, and any preliminary designs. This comprehensive data collection forms the baseline for subsequent risk comparisons.
2. **Risk Identification and Categorisation:** Identify potential risks across the eight categories, tailoring the exercise to the project's specifics. Involve key stakeholders (engineers, end-users, contractors, etc.) in workshops or brainstorming sessions to ensure a comprehensive risk register that captures multiple perspectives.
3. **Benchmark Comparison:** Evaluate the project against historical data and comparable projects:
    - **Compare Project Characteristics:** Assess how the project's characteristics (size, complexity, location, technical requirements) stack up against similar past projects within the Defence Estate portfolio. This provides context on expected challenges.
    - **Analyse Historical Data:** Leverage data from past Defence projects to identify typical risk profiles and contingency usage. Look for patterns or deviations that indicate where the current project might face higher or lower risk exposure.
    - **Refer to Industry Standards:** Consult industry standards and best practices (e.g. PMI's *Project Management Body of Knowledge* Guide[4] and ISO 31000 risk management guidelines[5]) for managing risks in similar projects. These external benchmarks help validate the thoroughness of the risk identification and highlight any areas possibly overlooked.
4. **Quantitative and Qualitative Analysis:** For each identified risk, analyse both quantitative impact (e.g. potential cost increase, schedule delay in measurable terms) and qualitative impact (e.g. stakeholder satisfaction, reputation, operational readiness).

This dual analysis ensures understanding of not just how much a risk could cost in dollars or days, but also how it might affect less tangible project success factors.

5. **Contingency Determination:** Based on the benchmarking insights and risk analyses, determine an appropriate contingency reserve for the project. This involves assigning contingency amounts aligned with both industry benchmarks and the specific risk profile of the project. The goal is to neither over-allocate (tying up funds unnecessarily) nor under-allocate (leaving the project exposed).

4.2 Calibrated Questions – Quantifying Risk and Predicting Contingency

A core feature of DIPRAC is the use of calibrated questions to systematically measure risk factors.

1. **Develop Tailored Questions:** Create a set of pointed questions targeting each of the eight risk categories and the identified complexities of the project. These should include broad questions (e.g. "On a scale of 1 to 5, how challenging is the project's technical complexity relative to typical projects?") and specific ones (e.g. "How many different engineering disciplines must coordinate on this project's design?"). The aim is to convert qualitative judgments into quantifiable scores.

2. **Score the Responses:** Assign numeric scores or ratings to each question's answers. This might involve direct values (such as an estimated number of months of potential delay) or a scale (where, for instance, a score of 5 indicates extremely high risk). Use defined scoring rubrics to maintain consistency and objectivity in how responses are translated into risk levels.

3. **Aggregate into a Risk Profile:** Compile the scores from all questions to build an overall risk profile for the project. This profile gives a quantified view of the project's risk landscape, essentially summing up how "risky" the project is across all dimensions relative to an average project.

4. **Translate into Contingency Needs:** Use statistical methods or risk modelling tools to convert the risk profile into a contingency estimate. This could involve simulations (like Monte Carlo analysis) or simpler aggregation models, and should consider best-case, worst-case, and most likely scenarios to capture uncertainty ranges. The outcome is a recommended contingency reserve tailored to the project's risk profile.

5. **Stakeholder Review and Refinement:** Present the preliminary risk profile and contingency recommendations to key stakeholders (e.g. project sponsors, senior engineers, end-user representatives) for validation. Their feedback can reveal additional insights or considerations. Refine the risk assessments and contingency allocations based on this input to ensure no major concerns are overlooked and that there is broad buy-in on the risk management plan.

6. **Documentation and Monitoring:** Document the entire risk assessment process, including the questions used, scoring methodology, risk profile, and how contingency was determined. This documentation will be valuable for transparency, future audits, or lessons learned. Additionally, establish a plan to continuously monitor risks and the adequacy of the contingency as the project progresses. If new risks emerge or existing ones evolve, update the risk profile and adjust the contingency reserve accordingly, keeping stakeholders informed throughout.

By systematically benchmarking projects and employing calibrated questions for risk quantification, project managers can set more reliable contingency reserves and enhance overall project predictability and success.

5 Case Studies

The DIPRAC framework has been piloted on several Defence infrastructure projects, providing valuable insights into its effectiveness and adaptability. The following two case studies illustrate how the framework was applied and the outcomes achieved:

5.1 Case Study 1: Upgrading a Remote Communications Installation

Project Overview: This project involved upgrading telecommunications infrastructure at a remote Defence site in Northern Australia. The site's remoteness, environmental sensitivity, and technical complexity presented significant challenges to traditional project delivery.

Application of the Framework:

- **Benchmarking:** In comparison to similar past telecom upgrades, this project showed above-average logistical and environmental risk due to its isolation and the presence of protected wildlife habitat in the area.
- **Calibrated Questions:** The project team focused questions on logistics (e.g. difficulty of transporting equipment to site), environmental impact (e.g. likelihood of work stoppages due to wildlife protections), and technical integration (e.g. compatibility of new systems with legacy infrastructure). These questions quantified how much harder this project would be relative to a baseline scenario.
- **Risk Quantification & Contingency:** The responses revealed substantial logistic and environmental risks. Accordingly, a higher contingency was allocated specifically for transportation delays and environmental mitigation. Technical risk was assessed as moderate given the team's prior experience with similar systems.

Outcomes: With the framework's insights, the project was executed with a clear understanding of its unique risks. The contingency set aside for logistics was tapped to handle unexpected transport issues (e.g. weather-related access delays), but overall the project remained within budget and on schedule. No significant budget overruns occurred, validating the accuracy of the risk-based contingency.

Insights: This case underscored the importance of thorough logistical planning and environmental risk assessment during project planning. By quantifying these risks upfront, the project team was able to allocate sufficient resources to manage them without derailing the project.

5.2 Case Study 2: Construction of a New Training Facility

Project Overview: The project entailed constructing a new training facility on an active Defence base. This required careful coordination with ongoing military operations and integration with existing base infrastructure and security protocols.

Application of the Framework:

- **Benchmarking:** Against other construction projects on active bases, this project was identified to have elevated stakeholder and coordination risks, given the need to work around active training schedules and high-security requirements.
- **Calibrated Questions:** Questions were devised to gauge stakeholder involvement (e.g. extent of consultation needed with base command), integration complexity (e.g. difficulty of connecting new utilities to existing systems), and security constraints (e.g. impact of base access restrictions on contractors).
- **Risk Quantification & Contingency:** The analysis highlighted high stakeholder management and coordination risks. Consequently, a significant portion of the contingency budget was earmarked for potential schedule delays or scope changes resulting from stakeholder feedback or operational interruptions.

Outcomes: The proactive stakeholder engagement strategy guided by the framework allowed the project team to adjust plans quickly in response to evolving military needs. While there were some schedule adjustments to accommodate training operations, these were anticipated and managed within the allocated contingency and revised timelines. The facility was ultimately delivered to the satisfaction of both the end-users and base management.

Insights: This case highlighted the critical need for flexibility and continuous stakeholder engagement when working in a live Defence environment. By planning for stakeholder-related risks and involving stakeholders throughout, the project maintained alignment with operational priorities and avoided conflict or rework.

5.3 General Lessons from the Case Studies

Across these case studies, several key benefits of the DIPRAC framework became evident:

- **Flexibility and Adaptability:** The framework's flexible structure allowed it to be tailored to each project's context. It proved applicable to a range of project types, from remote infrastructure upgrades to complex base constructions.
- **Enhanced Stakeholder Engagement:** By formally integrating stakeholder considerations into the risk process (through calibrated questions and ongoing reviews),

project teams achieved better stakeholder buy-in and identified issues that might have otherwise surfaced later as surprises.

- **Accurate Contingency Allocation:** The detailed risk quantification led to more accurate and justified contingency reserves. In both cases, the contingencies set were sufficient for their purposes, reducing the likelihood of budget overruns while also not unnecessarily inflating project budgets.
- **Proactive Risk Mitigation:** Perhaps most importantly, the framework encouraged a proactive mindset. Project teams were identifying and planning for risks early, rather than reacting to issues as they arose. This forward-looking approach contributed to smoother execution and more predictable outcomes.

These case studies demonstrate the practical benefits of implementing a structured, Defence-specific risk management framework. Not only did the DIPRAC framework improve risk identification and management, but it also contributed to more predictable and successful project results.

6 Benefits of the Framework

The implementation of the DIPRAC framework brings about significant improvements in managing Defence infrastructure projects. Key benefits include:

- **Improved Risk Identification and Assessment:** By providing a comprehensive structure (with its eight risk categories and guided questions), the framework ensures a thorough examination of potential risks. Project teams are less likely to overlook critical risk factors, resulting in a more nuanced understanding of the project's risk landscape and well-targeted mitigation strategies.
- **Enhanced Predictability in Planning:** With systematic benchmarking against historical data and industry standards, DIPRAC improves the predictability of project outcomes. Project managers can develop more realistic schedules and budgets by learning from analogous projects and understanding likely risk impacts upfront. This greater foresight reduces the incidence of unforeseen issues that derail plans.
- **Strategic Contingency Allocation:** Quantifying risks allows for contingency funds to be allocated in proportion to actual risk exposure. This means budgets include adequate buffers where needed (and avoid excessive padding where not necessary). Such precision in contingency setting protects projects from unexpected costs while optimising the use of funds, potentially freeing resources for other needs or enabling more competitive project pricing.
- **Better Stakeholder Communication and Buy-In:** The framework's emphasis on stakeholder engagement throughout the risk management process leads to more transparent and collaborative project environments. Stakeholders, from Defence clients to consultants and contractors, gain confidence that risks are understood and managed. This shared understanding fosters trust and a sense of partnership, which in turn supports smoother project execution and faster resolution of issues that do arise.
- **Increased Project Delivery Efficiency:** By anticipating challenges and allocating resources to deal with them, projects experience fewer disruptive surprises. This proactive management means less downtime, fewer expensive last-minute changes, and more consistent progress. Additionally, the framework's adaptability allows project teams to quickly adjust to new information or changing conditions, maintaining momentum and efficiency even when circumstances shift.
- **Cost Savings:** Over the lifecycle of a project (and across a portfolio of projects), the efficiencies gained through DIPRAC can translate into substantial cost savings. Avoiding major cost overruns or delays is the most direct saving, but there are indirect savings as well: improved planning reduces waste, better risk allocation lowers the "risk premiums" contractors add to their bids, and enhanced coordination reduces duplication of efforts

and conflict. Collectively, these factors help deliver more value for each dollar invested in Defence infrastructure.

In summary, the DIPRAC framework represents a significant advancement in risk management for Defence infrastructure projects. Its structured yet flexible approach allows for iterative risk analysis, strategic planning, and effective stakeholder engagement. By enhancing predictability, optimising contingency allocation, and improving overall project delivery efficiency, the framework not only mitigates the inherent risks of complex projects but also unlocks potential cost savings and performance gains.

7 Industry Implications and Recommendations

The introduction of the DIPRAC framework marks a pivotal opportunity to elevate risk management practices across the Defence infrastructure sector. While the framework provides the methodology and tools for better project outcomes, realising its full benefit requires industry-wide understanding and adoption.

7.1 Widespread Adoption for Collective Benefit

Defence infrastructure projects carry high stakes and strategic importance. To consistently deliver these projects on budget and on schedule, a robust and sophisticated risk management approach is required. The DIPRAC framework offers such an approach, but it will be most effective only if embraced broadly. Consistent use of a standard framework across Defence projects would enable accumulation of valuable data, allow benchmarking across projects, and drive continuous improvement sector-wide. In short, the more organisations and projects that adopt DIPRAC (or align with its principles), the more the entire industry stands to benefit through shared learning and greater predictability.

7.2 Policy and Governance Integration

Policymakers and Defence governing bodies have a role to play in fostering adoption of the framework. Integrating DIPRAC principles into Defence infrastructure planning guidelines and procurement requirements can set expectations for risk management rigor. For example, official Defence project management policies could recommend or mandate the use of a standardised risk framework (like DIPRAC) for all major (CFI) and medium (estate works) projects, ensuring a baseline of practice.

7.3 Recommendations for Policy Development:

1. **Incorporate Framework in Guidelines:** Update Defence and government infrastructure delivery guidelines to reference the DIPRAC framework (or its key components) as a best-practice model for risk management on projects.
2. **Develop Industry Standards:** Through collaboration between Defence, industry associations, and bodies like Consult Australia, establish formal industry standards or codes of practice that align with the framework's approach. This creates a clear benchmark for companies to strive towards.
3. **Incentivise Compliance:** Introduce incentives for contractors and consultants to apply the framework. For instance, tender evaluation criteria could reward detailed risk

management plans that follow DIPRAC principles, or pilot projects that use the framework could receive support or recognition.

7.4 Recommendations for Professional Training:

1. **Training Programs:** Develop targeted training programs and workshops on the DIPRAC framework for project managers, risk officers, and consultants in the Defence sector. These programs should cover the methodology (risk categorisation, calibrated questions, benchmarking, etc.) and use real project scenarios for practice.
2. **Certification:** Establish a certification in Defence infrastructure project risk and contingency management. Professionals who demonstrate proficiency in applying the framework could be certified, signalling their expertise. This not only builds individual capability but also encourages uptake as organisations seek certified staff.
3. **Continuous Development:** Promote ongoing professional development by integrating DIPRAC topics into Defence infrastructure conferences, seminars, and publications. Regular knowledge-sharing sessions (for example, an annual forum on risk management best practices in Defence infrastructure projects) will help keep the community updated and engaged with the framework's evolution and lessons learned from its application.

By embedding DIPRAC into policies and skill development initiatives, the Defence infrastructure community can create an environment where structured risk management becomes the norm. This alignment between policy, practice, and people will greatly enhance the likelihood of the framework's success and longevity.

8 Call to Action

The Defence infrastructure sector now stands at a crossroads with an opportunity to fundamentally improve how project risks are managed. The DIPRAC framework provides a clear path forward, but its success depends on collective action by all stakeholders in the ecosystem. Therefore, we call on:

- **Defence Agencies and Clients:** Embrace the framework and integrate its processes into your project management and governance structures. Advocate for its use in all new project initiatives and require robust risk management plans from contractors.
- **Industry Firms and Consultants:** Adopt the framework within your organisations as a standard practice for Defence projects. Train your teams to apply it and share feedback to continue refining the approach. Demonstrating strong risk management capability will not only improve project outcomes but also be a competitive advantage in securing Defence contracts.

- **Professional and Industry Bodies:** Support the rollout of the framework through awareness campaigns, training, and resources. Facilitate forums for exchange of experiences, and work with Defence to incorporate the framework into industry guidelines and contracts.

By taking these steps, the sector can achieve a new standard of excellence in project delivery. Projects will be executed more efficiently and effectively, with fewer surprises and greater confidence in outcomes. Most importantly, improving risk management in Defence infrastructure ensures that vital projects—those that underpin national security and Defence capability—are delivered with the highest degree of integrity, reliability, and fiscal responsibility.

9 Conclusion

The Defence Infrastructure Project Risk and Contingency (DIPRAC) framework represents a significant advancement in the management of Defence infrastructure projects. It offers a comprehensive and tailored approach to address the unique risks and complexities inherent in these endeavours. This white paper has detailed the framework's structure and components, including its innovative categorisation of risks, strategies for implementation, and the use of calibrated questions for precise risk quantification. Through real-world case studies, we have demonstrated the framework's adaptability and effectiveness, underscoring its potential to greatly enhance project predictability, efficiency, and success.

Key takeaways include:

- The framework introduces a detailed categorisation of risk factors specific to Defence infrastructure projects, enabling a more nuanced understanding and management of project complexities than generic models.
- A systematic benchmarking approach (using historical data and industry standards) informs more accurate planning and contingency allocation, reducing the likelihood of budget and schedule overruns.
- Active stakeholder engagement and the use of calibrated questioning lead to a comprehensive risk profile for each project, ensuring that both obvious and latent risks are accounted for.
- Pilot applications of the framework have shown tangible benefits, including better risk preparedness, more appropriate contingencies, and improved stakeholder satisfaction.

The call to action for industry stakeholders is clear: to realise the full benefits of the DIPRAC framework, a concerted effort across the Defence infrastructure sector is required. This means integrating the framework into standard practice, developing supportive policies and training programs, and maintaining a commitment to collaboration and continuous improvement in risk management.

Industry leaders, government policymakers, and practitioners are urged to champion the adoption and implementation of this framework. By doing so, they will foster a culture of risk management excellence within the Defence infrastructure community. Embracing DIPRAC is not just about improving outcomes on individual projects—it is about elevating the performance of the entire sector. With robust risk practices in place, the Defence infrastructure sector can more reliably meet its objectives and deliver critical projects with unparalleled confidence, ultimately strengthening national security infrastructure with efficiency and integrity.

10 References

1. Proximity Advisory Services Pty Ltd. (2020). *Smart buyers and industry partnering in Defence procurement*. (Insight article by D. Pidgeon, published Oct 29, 2020).
2. Estate and Infrastructure Group. (2016). *Risk Management Framework* (Joint Directive 30/2015 on the Management of Risk in Defence).
3. Estate and Infrastructure Group. (2016). *Defence SAP E&IG Risk Category Definitions* (Standardised approach for risk identification and assessment in Defence Estate projects).
4. Project Management Institute. (2021). *A Guide to the Project Management Body of Knowledge (PMBOK® Guide)* (7th Edition). PMI Publications.
5. Standards Australia/Standards New Zealand. (2018). *AS/NZS ISO 31000:2018 – Risk Management – Guidelines*.
6. Standards Australia/Standards New Zealand. (2015). *AS/NZS IEC 62198:2015 – Managing risk in projects – Application guidelines*.
7. Department of Finance (Australia). (2023). *Commonwealth Risk Management Policy*. (Mandates principles and requirements for risk management in government activities).
8. Defence Science and Technology Organisation. (2005). *Australian Defence Risk Management Framework: A Comparative Study*. (Analysis of Defence's enterprise risk management approach in the early 2000s).
9. Consult Australia (2023) – *Unravelling Risk* Report. (Industry guidance document for consultancy firms in infrastructure projects).

Appendices (Available upon request)

Appendix A: Risk Categorisation Matrix – A detailed matrix defining the various types of risk associated with Defence infrastructure projects. This matrix provides definitions, examples, and potential mitigation strategies for each risk category, serving as a comprehensive guide for project teams. (Based on the Defence SAP E&IG Risk Category Definitions, 2016.)

Appendix B: Calibrated Questions Template – A template listing sample calibrated questions used to assess project complexity and risk levels. It outlines the methodology for scoring responses and converting them into quantitative risk metrics, which inform contingency planning.

Appendix C: Benchmarking Data and Analysis – A summary of benchmarking analyses drawn from historical Defence infrastructure projects. This appendix presents data on project performance versus initial risk assessments and contingencies, demonstrating how the framework's predictions compare to actual outcomes.

Appendix D: Contingency Allocation Models – An explanation of the mathematical models recommended for determining contingency amounts based on a project's risk profile. Worked examples show how adjustments to contingency are made in response to changes in project scope, complexity, or external risk factors.

Appendix E: Stakeholder Engagement Plan – Guidelines for effective stakeholder engagement throughout the project risk management process. This plan includes strategies for securing stakeholder buy-in, collaboratively identifying risks, and incorporating stakeholder feedback into risk mitigation decisions.

Appendix F: Framework Implementation Checklist – A step-by-step checklist for implementing the DIPRAC framework on a project. This tool ensures that all aspects of the framework are systematically applied, from initial risk identification and question calibration through to contingency review and project close-out evaluation.

Appendix G: Case Studies – Detailed Analysis – An extended analysis of the case studies presented in the white paper. This section includes additional data, project documentation, and post-project review findings, providing deeper insights into the challenges faced and strategies employed, as well as lessons learned from the framework's application.

Appendix H: Glossary of Terms – Definitions of key terms and concepts used in the white paper and appendices. The glossary clarifies terminology and acronyms (e.g. DIPRAC, RMF, contingency, etc.) to ensure all stakeholders have a common understanding of the language of risk management in the Defence context.

Appendix I: Professional Development Resources – A curated list of resources for further professional development in risk management and Defence project management. This includes recommended training programs, certification courses, and seminal publications or articles that underpin best practices in this field.