TBH

project delivery experts

INTEGRATED DEFENCE RISK MANAGEMENT

Transforming Risk from Abstraction to Action

November 2025

tbhconsultancy.com

Contents

This document has been prepared by TBH for general informational purposes only. It does not constitute professional advice, assurance or a commitment by TBH or any of its affiliates. While every effort has been made to ensure the accuracy and relevance of the information contained herein, TBH makes no representations or warranties, express or implied, about its completeness, reliability or suitability for any particular purpose.

References to Defence or Defence-related programs do not imply endorsement by the Department of Defence or any government entity. The views expressed are those of TBH. The information in this document is subject to change without notice. TBH accepts no liability for any loss or damage arising from reliance on the information contained herein.

Executive Summary

Defence acquisition and sustainment programs face unprecedented complexity. Multi-billion-dollar investments spanning decades must navigate technical uncertainty, evolving requirements, multiple stakeholders, supply chain challenges and increasingly compressed delivery timelines. In this environment, traditional approaches to risk management – characterised by qualitative assessments, red-amber-green indicators and siloed discussions – fall short of providing the clarity and foresight leaders need to make confident, data-driven decisions.

This white paper introduces TBH's Integrated Defence Risk Management service, a comprehensive framework that transforms how defence programs and the broader enterprise identify, quantify and manage risk. Rather than treating risk as an abstract concept discussed in isolation, this approach embeds risk directly into project delivery, governance and reporting. It quantifies impacts in terms of schedule delays and budget exposure in a pragmatic, efficient and scalable way that enables decision-makers to act with confidence.

Built on four founding principles and implemented through a structured transformation journey, the service moves organisations from qualitative discussions to data-driven decision-making while maintaining the pragmatism and flexibility essential to defence program realities.

This white paper explores the conceptual foundations, methodological approaches, implementation roadmap and distinctive value proposition of TBH's Integrated Defence Risk Management, demonstrating how defence organisations can achieve superior project outcomes with structured, quantitative risk management.

1. Introduction:

The Challenge of Risk in Defence Programs

Defence acquisition programs represent some of the most complex undertakings in government. A typical major defence capability project may span 10-20 years from initial concept to full operational capability. It can involve thousands of personnel across multiple organisations, integrate cutting-edge technologies with uncertain maturity and operate under intense public and parliamentary scrutiny; all while adapting to evolving strategic requirements.

In this environment, risk is not merely possible; it is inevitable. Technical challenges emerge. Supply chains experience disruptions. Requirements evolve as strategic circumstances change. Skilled personnel become scarce. Integration proves more complex than anticipated. External dependencies slip. The question is never whether risks will materialise, but which ones, when, and with what impact.

Traditional risk management approaches in defence programs typically involve:

- Establishing and maintaining, not necessarily consistently, risk registers that list potential issues with qualitative likelihood and consequence ratings
- Using red-amber-green (RAG) indicators to signal risk severity
- Conducting periodic risk reviews in dedicated risk committees separate from core program governance
- Escalating “high” risks to senior leadership for awareness, often only when they are close to materialising
- Developing mitigation strategies without ensuring the necessary resourcing or follow-through for effective implementation

While these practices provide some value, they share critical limitations:

Lack of Quantification: Describing a risk in a subjective and usually biased manner as “high likelihood, major consequence” tells decision-makers that something matters, but not how much. Is this risk worth spending $5 million to mitigate? Will it delay the program by two months or two years? Is that impact is localised or transferable? Without quantification, prioritisation becomes subjective.

Disconnection from Delivery: When risk management happens in separate forums using separate processes, it becomes an overlay on project delivery rather than an integrated part of it. Delivery teams may view risk management as compliance overhead rather than a tool that helps them succeed.

Static Assessment: Risk registers become documents to be maintained rather than dynamic tools for decision-making. Risks identified at program inception may persist unchanged for years, losing relevance as circumstances evolve.

Limited Integration: Individual project risks may be well-managed while program-level risks arising from interdependencies between projects remain invisible until they materialise.

Qualitative Escalation: Senior leaders often receive information that certain risks are “red”, usually without sufficient warning and without the quantitative data needed to make informed trade-offs between schedule, cost, and capability.

Ineffective mitigation: Strategies are often recorded but not adequately resourced, implemented or validated for effectiveness.

The consequence of these limitations is that risk management fails to fulfil its primary purpose: enabling better decisions. Program leaders cannot confidently answer fundamental questions: What is the realistic probability of delivering on the current schedule? How much contingency should be held for risks? Which mitigation investments offer the best return? Where should management attention focus?

Integrated Defence Risk Management addresses these limitations systematically by embedding quantitative risk analysis into every level of program governance and delivery, from individual work packages through to portfolio-level decision-making.

2. Founding Principles for Quantifiable Risk Management

Effective transformation of risk management practice must rest on clear conceptual foundations. TBH's Integrated Defence Risk Management service is built on four founding principles that distinguish it from traditional approaches and shape every aspect of implementation.

Principle 1:
Risk Is Not a Standalone, But Rather a Function of Time and Cost

The first and most fundamental principle recognises that risk, in a project delivery context, has meaning only insofar as it affects schedule or budget. A risk that materialises but has no impact on when capability is delivered or what it costs is, for project management purposes, not actually a risk – it may be an issue requiring attention, but it does not threaten project objectives.

This principle has profound implications for how risk is assessed and communicated. Instead of describing risks in abstract terms ("supplier may be unable to meet quality standards"), the focus shifts to quantified impacts ("supplier quality issues could delay integration by 6-12 weeks and require $1.2-2.4M in rework").

This quantification serves multiple purposes:

Enables Prioritisation: When all risks are expressed in common units (days of delay, dollars of cost impact), they can be objectively compared and prioritised based on actual threat to program objectives rather than subjective assessment.

Supports Decision-Making: Leaders can evaluate mitigation options against quantified risk exposure. Spending $500K to reduce a $3M risk exposure makes clear sense; spending the same amount on a $200K exposure does not.

Facilitates Aggregation: Quantified risks can be combined to understand cumulative program exposure, something impossible with qualitative ratings.

Improves Communication: Stakeholders across organisational levels and disciplines can understand and act on quantified information in ways that abstract risk descriptions do not enable.

Principle 2:
Change Is Led from the Top and Built from the Bottom

Transforming risk management practice requires genuine change management, not merely procedural updates. This principle recognises that successful change must be both sponsored by senior leadership and constructed through engagement with delivery teams.

Top-Down Leadership: Senior program leadership must visibly champion quantitative risk management, demonstrate its use in their own decision-making, hold their organisations accountable for quality risk information and allocate resources for implementation. Without this sponsorship, risk management transformation becomes an isolated initiative that withers when it encounters organisational resistance or resource constraints.

Bottom-Up Building: Simultaneously, frameworks, processes and tools must be developed from first principles, drawing on the most detailed and comprehensive information, and built in collaboration with delivery teams who understand ground-level realities. Risk quantification conducted in isolation from those doing the work often produces numbers disconnected from reality. Engaging delivery teams when identifying uncertainties, defining ranges and validating assumptions ensures that quantified risk information accurately reflects project conditions on the ground.

This principle shapes implementation by ensuring that while frameworks and standards are established centrally, their application is tailored to each stream or project's specific context, and delivery teams have genuine ownership of the risk information they produce.

Principle 3:
Accountability Rests at the Top; Responsibility Lies with Delivery Teams

Effective governance requires clarity about who is accountable for outcomes versus who is responsible for delivery. This principle establishes that program leadership holds ultimate accountability for managing risk to successful delivery, while delivery teams hold responsibility for identifying, assessing and managing risks within their domain.

Strategic Accountability: The Program Manager and senior leadership team are accountable for:

- Establishing risk management frameworks and standards
- Allocating contingency and making risk-based trade-offs
- Determining which risks to accept, avoid, transfer, or mitigate
- Ensuring adequate resources for risk management
- Making decisions when risks escalate beyond delivery team authority

Operational Responsibility: Delivery teams are responsible for:

- Identifying and assessing risks within their work scope
- Developing and implementing mitigation strategies
- Maintaining accurate, current risk information
- Escalating risks that exceed their authority or capability to manage
- Executing within the risk tolerances established by leadership

This distinction prevents the common failure mode where either risk management becomes entirely a delivery team exercise without strategic engagement, or conversely, where senior leaders attempt to manage individual risks better handled at lower levels.

Principle 4:
Phased Start Must Still Follow Structured Principles (Simple vs. Rudimentary)

The final principle recognises that while implementation must be pragmatic and phased, there is a critical difference between "simple" and "rudimentary." Even initial, simplified implementations must follow rigorous methodological principles.

Simple: A straightforward approach that matches the analysis depth to available data and project maturity, applies sound quantitative methods at appropriate scale, maintains methodological rigor and produces defensible results.

Rudimentary: An unsophisticated approach that applies superficial quantification without proper foundations, produces numbers disconnected from reality, lacks methodological defensibility and creates false confidence in unreliable data.

This principle ensures that early implementations – which may involve limited scope, streamlined processes, or simplified modelling – still produce trustworthy information that decision-makers can rely upon. It prevents the common failure where organisations implement "quick wins" that ultimately undermine confidence in quantitative approaches because they produce poor-quality results.

Together, these four principles create a foundation for sustainable transformation of risk management practice that balances rigor with pragmatism, engages all organisational levels appropriately, and maintains focus on risk management's fundamental purpose: enabling better decisions that lead to better outcomes.

3. The Transformation Journey:

From Qualitative to Quantitative

Moving from traditional qualitative risk management to integrated quantitative approaches requires a structured transformation journey. TBH's framework organises this journey around four interconnected pillars that build progressively toward mature risk capability.

Pillar 1: Enforce Quantifiable Metrics in Reporting

The first pillar focuses on changing what gets reported and how risk information flows through governance processes. This begins with risk-based planning and forecasting that moves beyond single-point estimates to probabilistic ranges.

Multiple Forecast Confidence Levels: Instead of reporting a single completion date, programs report multiple scenarios:

- P10 (optimistic): 10% probability of achieving or bettering this date (aggressive or very much risk-free target)
- P50 (most likely): 50% probability – the median outcome
- P80/ P90 (conservative): 80% probability – a high-confidence commitment (risk adjusted target)

This approach explicitly acknowledges uncertainty and enables decision-makers to understand the range of plausible outcomes rather than treating a single estimate as certain.

Program-Wide Risk Profile as a Single Number: Rather than maintaining lengthy lists of individual risks with subjective ratings, the program's overall risk exposure is expressed as a single quantified metric – for example, "current risk exposure is 127 days schedule delay and $43M cost impact at P80 confidence level." This provides an at-a-glance understanding of total program risk that can be tracked over time and will drive change and enforce responsibility.

Quantified Impact Before and After Mitigation: Each significant risk is quantified both in terms of its gross exposure (if no mitigation occurs) and residual exposure (after planned mitigation). This enables evaluation of whether mitigation investments are worthwhile and whether residual risk remains acceptable.

Contingency in Concrete Terms: Contingency is expressed not as a percentage buffer but as specific amounts – "85 days schedule contingency" or "$12.4M cost contingency" – allocated based on quantified risk analysis rather than arbitrary percentages.

This pillar transforms reporting from descriptive to analytical, from subjective to objective, and from static to dynamic.

Pillar 2: Strengthen Foundations Through Bottom-Up Risk Inputs

The second pillar focuses on building the data foundations that enable reliable quantification. This requires systematic capture of risk information from delivery teams in structured, consistent formats.

Capture Uncertainty, Likelihood, and Impact Ranges: Rather than simply identifying that a risk exists, delivery teams quantify:

- The uncertainty in baseline estimates (best case, most likely, worst-case durations or costs)
- The likelihood that specific risk events will occur
- The range of possible impacts if risks materialise

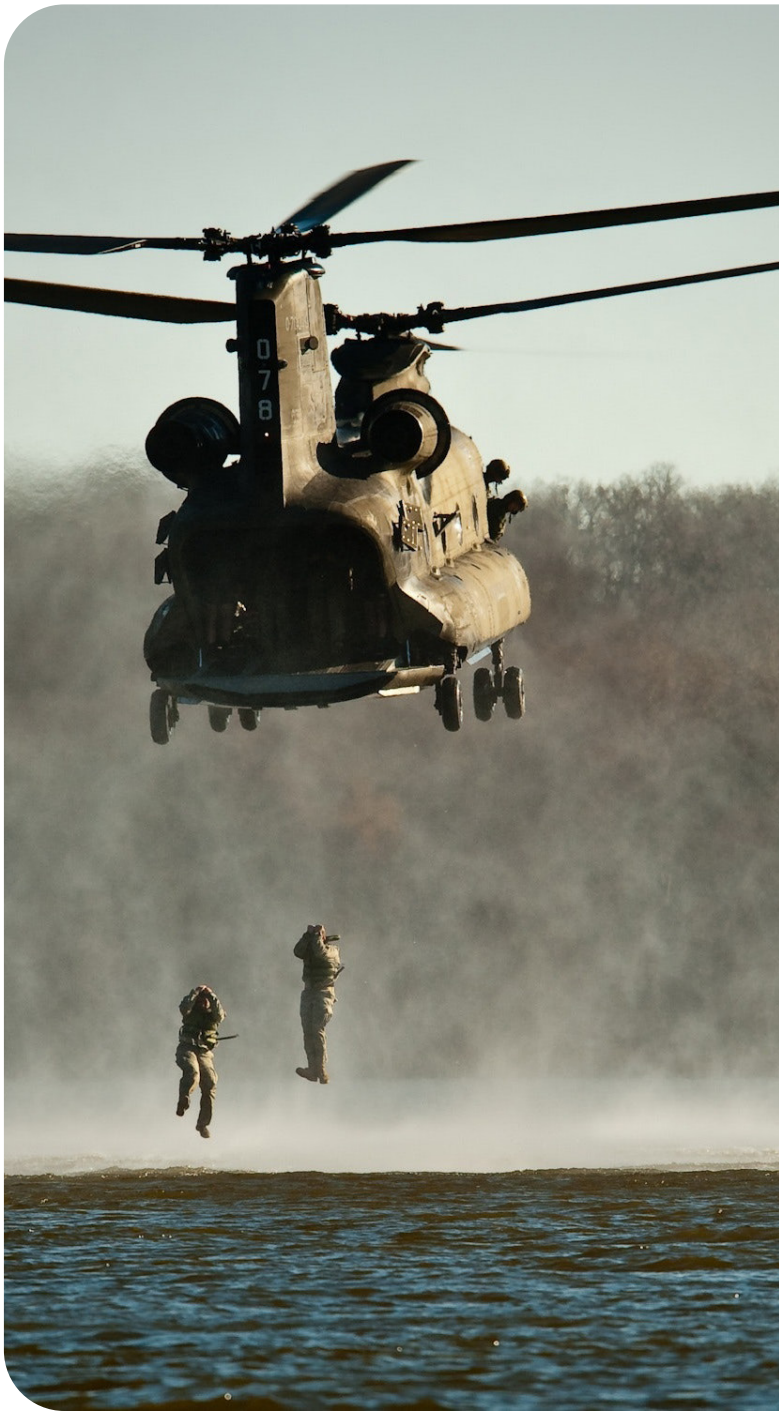
This information is captured in program management tools, particularly Primavera P6 for schedule risk, enabling integration with baseline plans.

Align Risks with Drivers: Each identified risk is explicitly linked to the scope elements, cost components, or schedule activities it could impact. This prevents “orphan risks” that float in registers without clear connection to what they actually threaten.

Consistent Templates: Standardised templates ensure that risk information is captured consistently across all projects and streams, enabling aggregation and comparison while still allowing flexibility for project-specific contexts.

Traceability: Clear audit trails connect individual risk assessments through to program-level reports, ensuring that senior leaders can drill down to understand the basis for any quantified risk figure.

This pillar ensures that quantitative analysis rests on solid foundations of validated, structured data rather than arbitrary assumptions.



Pillar 3: Apply Assurance Layers to Validate and Challenge Inputs

The third pillar recognises that quantitative risk analysis is only as good as the inputs it receives. Structured assurance processes validate that risk information is accurate, complete, unbiased, and properly reflected in analysis.

Multi-Level Review: Risk information is reviewed at multiple organisational levels:

- Project teams validate technical accuracy and completeness
- Program teams review for consistency across streams
- Portfolio oversight challenges assumptions and identifies gaps

Challenge Sessions: Structured workshops bring together diverse perspectives to challenge risk assessments, test assumptions, identify biases (particularly optimism bias), and ensure that groupthink hasn't led to systematic underestimation.

Pre-Escalation Validation: Before risk information escalates to senior decision-makers, assurance processes verify data quality, confirm that analysis methods were properly applied, check that conclusions are supported by evidence, and ensure consistency with other program information.

Cross-Stream Consistency: In multi-stream programs, assurance processes ensure that assumptions, methodologies and data quality are consistent across streams, enabling meaningful comparison and aggregation.

This pillar prevents the common failure mode where sophisticated quantitative methods are applied to poor-quality data, producing precise but inaccurate results.

Pillar 4: Integrate Expert Judgement for Context and Completeness

The final pillar ensures that quantitative analysis is enriched rather than replaced by expert judgement and qualitative context.

Data Frames Decisions: Quantitative risk analysis provides the primary framework for decision-making; the P80 completion date, the $43M cost exposure, the 85 days of contingency consumed. These numbers establish the foundation for discussions.

Expert Insights Add Context: Subject matter experts provide essential context that numbers alone cannot convey:

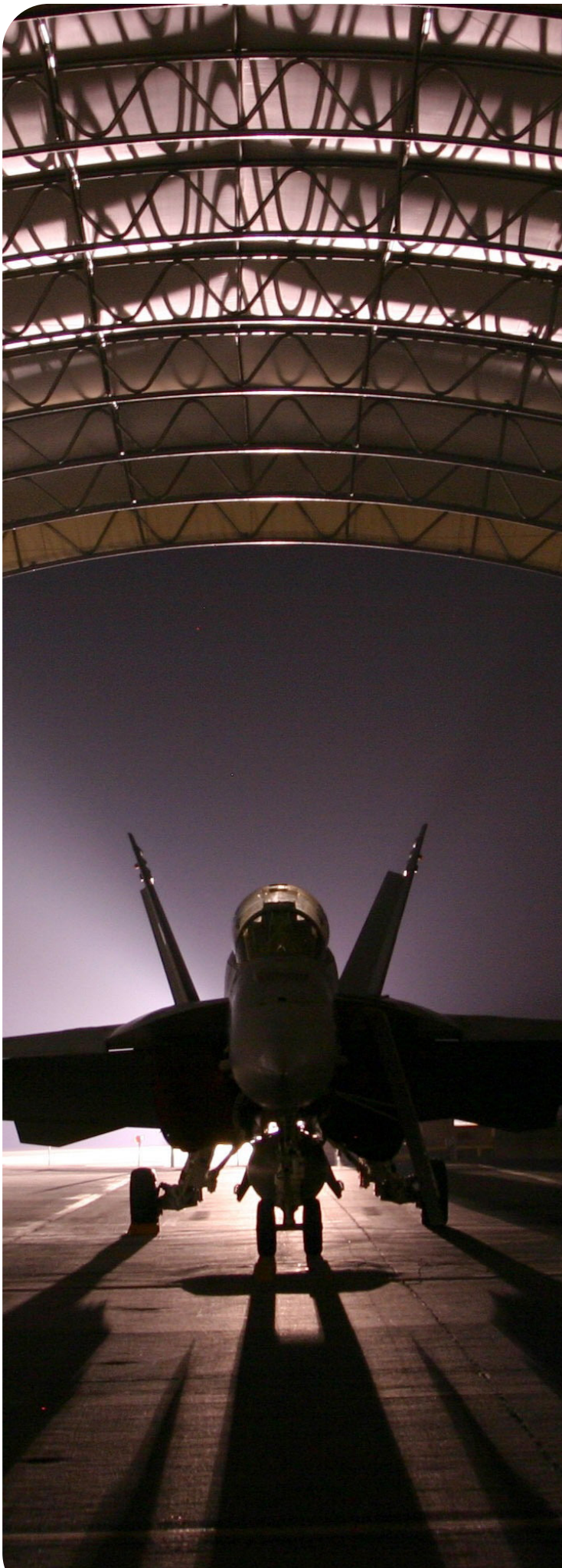
- Confidence levels in the underlying data
- Emerging trends not yet reflected in formal analysis
- Contextual factors that may affect likelihood or impact
- Alternative perspectives on mitigation approaches

Highlighting Unmodelled Risks: Experts identify risks that may be difficult to quantify but nonetheless warrant attention: strategic risks, political dimensions, capability gaps or emerging threats not yet captured in formal registers.

Balanced Decision-Making: Decision forums integrate both quantitative data and qualitative judgement, with clear protocols for how they interact. For example, qualitative considerations may override quantitative recommendations, but the rationale must be documented.

This pillar ensures that organisations gain the benefits of quantification without losing the insights that experienced professionals bring to risk management.

Together, these four pillars create a comprehensive transformation from traditional qualitative approaches to integrated quantitative risk management that is rigorous, practical, and sustainable.



4. Embedding Quantitative Risk Analysis at Portfolio and Program Levels

Quantitative Cost and Schedule Risk Analysis (QCSRA) forms the technical core of integrated risk management. Rather than being a one-off analytical exercise performed occasionally for major reviews, QCSRA becomes an embedded planning, assurance and governance tool used continuously throughout program delivery.

PROGRAM-LEVEL APPLICATION

At the program level – typically covering multiple streams or major projects that must be integrated – QCSRA serves several functions:

Planning and Forecasting: During planning, QCSRA helps to establish realistic schedules and budgets by:

- Testing whether proposed timelines are achievable given identified uncertainties
- Determining appropriate contingency levels based on quantified risk
- Identifying critical paths and high-risk activities requiring management focus
- Evaluating trade-offs between different delivery approaches

Assurance and Challenge: As programs progress, QCSRA provides assurance that:

- Baseline plans remain realistic as circumstances evolve
- Contingency consumption aligns with risk reduction
- Schedule compression or budget reductions are achievable
- Claims of “on track” status are supported by probabilistic analysis

Governance and Decision-Making:
In governance forums, QCSRA informs decisions about:

- Whether to authorise progression to the next phase
- How to allocate limited contingency across competing needs
- Which mitigation investments offer the best return
- When to escalate issues to higher authority

LEVERAGING THE INTEGRATED MASTER SCHEDULE

All QCSRA must anchor to a consolidated Integrated Master Schedule (IMS) that reflects interdependencies across streams. The IMS serves as the single source of truth for:

- Activity sequencing and logic
- Duration estimates
- Resource assignments

- Milestone commitments
- Progress tracking

Risk analysis that operates independently of the IMS produces results disconnected from how the program is actually managed. Integration ensures that schedule risk drivers identified through QCSRA directly relate to activities in the working schedule, enabling targeted mitigation and clear accountability.

INTERDEPENDENCIES AND ASSUMPTIONS BASELINE

A critical component of program-level QCSRA is the comprehensive documentation of assumptions relating to:

- High-cost items and how they were estimated
- Trade packages and their interdependencies
- Bundled activities and their internal logic
- External dependencies and their reliability
- Resource availability and productivity rates

This assumptions baseline serves several key purposes:

- Provides transparency around the foundations of uncertainty estimates
- Enables challenge and validation of analytical inputs
- Creates an audit trail to support gate reviews and external scrutiny
- Facilitates lessons learned by documenting which assumptions proved accurate or inaccurate

PROJECT-LEVEL APPLICATION

At individual project level, QCSRA maintains a more granular focus on stream-specific risks while feeding up to program-level aggregation.

Localised Risk Quantification: Each project maintains its own risk register with quantified impacts specific to that project's scope, schedule and budget. These should reflect concrete uncertainties rather than generic portfolio-wide risks that are actually owned at higher levels.

Stream-Specific Analysis: Projects apply QCSRA methods appropriate to their maturity and complexity: bottom-up for well-defined projects, hybrid for mixed maturity or top-down for early-stage initiatives. The key is consistency in how results are expressed and reported to enable program-level aggregation.

Integration Points: Project-level QCSRA explicitly identifies and quantifies risks associated with integration points—where a project's deliverables interface with other projects' outputs. These integration risks often represent the highest program-level exposure.

The power of embedded QCSRA comes from its continuous use throughout the program lifecycle rather than episodic application only at major gates.

5. Methodology Selection:

Matching Analysis to Project Maturity

A critical insight in practical QCSRA implementation is that methodology selection should match project definition maturity, not organisational process maturity or project size. TBH's approach offers three calibrated methodologies, each appropriate for different contexts.

BOTTOM-UP (FIRST PRINCIPLES) METHODOLOGY

The bottom-up approach develops risk and uncertainty estimates from first principles through to direct engagement with delivery teams, detailed analysis of work breakdown structures, and granular examination of specific project contexts.

When to Use:

- Large, complex projects with high organisational criticality
- Mid-to-late stage projects with detailed designs and well-defined scope
- Projects with high data availability and mature planning
- Situations requiring robust, defensible assessments for external scrutiny

Characteristics:

- Develops uncertainty estimates at work package or activity level
- Identifies risks through workshops with subject matter experts
- Quantifies impacts based on specific project conditions and constraints
- Does not rely on generic benchmark factors or historical analogies
- Provides highest accuracy but requires significant effort

Focus:
Directly derived risk and uncertainty, built from the ground up based on what is actually happening on this specific project in this specific context.

HYBRID METHODOLOGY

The hybrid approach combines bottom-up analysis where project definition is mature with top-down factors where detail is lacking or unnecessary.

When to Use:

- Medium-to-large projects in transitional or mid-stage phases
- Projects with mixed maturity – some elements well-defined, others conceptual
- Situations requiring balance between analytical rigor and pragmatic timelines
- Programs with limited resources for full bottom-up analysis across all elements

Characteristics:

- Applies detailed bottom-up methods to high-risk or critical path elements
- Uses strategic factors or benchmarks for less critical or immature elements
- Combines schedule-level uncertainty with stream-level discrete risks
- Balances the rigor of first principles with efficiency of parametric approaches

Focus:
Best of both – detailed analysis where it matters most, indicative estimates where practical and sufficient.

TOP-DOWN (FACTORS) METHODOLOGY

The top-down approach applies generic risk factors, uncertainty allowances, and strategic assumptions based on benchmarks, historical data or expert judgement.

When to Use:

- Small projects or early-stage initiatives with limited detail
- Situations with low data availability or immature scope definition
- Strategic or directional analysis where precision is less critical than speed
- Portfolio-level screening to identify projects warranting deeper analysis

Characteristics:

- Assumes variability as percentages or factors applied to high-level estimates
- Uses benchmarks from similar projects or industry standards
- Requires minimal detailed data collection or workshop time
- Provides quick, indicative insights without extensive analysis effort
- Less defensible in detailed scrutiny but appropriate for its purpose

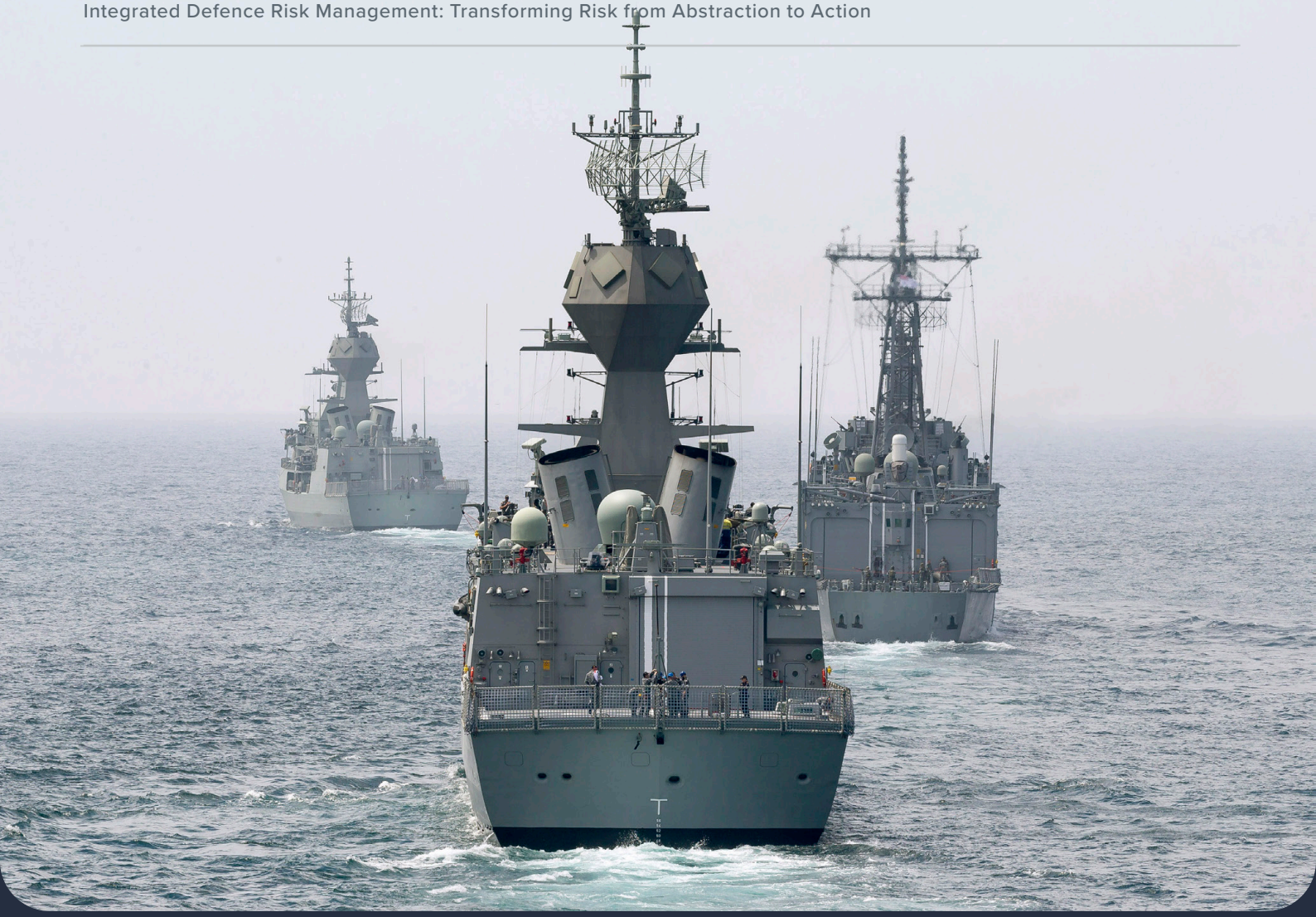
Focus:
High-level risk factors and allowances applied without project-specific analysis of root causes, used when this level of detail is sufficient for decisions at hand.

THE CRITICAL DISTINCTION: APPROPRIATE VS. IMMATURE

The most important principle in methodology selection is recognising that the choice is about appropriateness, not sophistication. An early-stage project using top-down factors is not applying an “immature” or “low-quality” method, but rather exactly the right method for its circumstances.

Conversely, attempting to apply bottom-up methods to a project that lacks sufficient definition does not produce better analysis. It produces false precision: numbers that appear rigorous but rest on speculative assumptions because the necessary detail does not yet exist.

Organisations often make the mistake of equating more detailed analysis with better analysis. In reality, the best analysis is that which matches method to available information and decision needs.



DECISION FRAMEWORK FOR METHODOLOGY SELECTION

FACTOR	BOTTOM-UP	HYBRID	TOP-DOWN
Project Size	Large, complex	Medium to large	Small, strategic
Stage of Project	Mid to late	Transitional/mid	Early concept
Data Availability	High	Medium	Low
Purpose	Detailed, robust	Balanced, fit-for-purpose	Directional, indicative
Time & Effort Required	High	Medium	Low
Accuracy	High	High	High (for purpose)

The key insight is that all three methodologies, when properly applied, produce high accuracy **relative to their purpose and the information available.** The issue is not whether top-down is “worse” than bottom-up, but whether the chosen method matches the context.

6. Integration with Defence Acquisition Gates

Defence acquisition follows a structured series of gates and reviews that govern progression from initial concept through to operational capability and eventual disposal. Integrated Defence Risk Management aligns with this lifecycle, with QCSRA playing different roles at different gates.

PROJECT INITIATION REVIEW (PIR)

QCSRA Focus: Assess feasibility of proposed options within desired timeframe

At PIR, projects are at the earliest conceptual stage. QCSRA helps determine whether proposed capability options can realistically be delivered within strategic timelines and budgets, or whether fundamental re-scoping is required.

Recommended Methodology: Top-down factors based on strategic assumptions and analogous programs

GATE 0 REVIEW

QCSRA Focus: Analyse design, environmental, and planning risks; refine timeline scenarios

Gate 0 involves selection of a preferred option for further development. QCSRA helps compare option risk profiles, identify high-risk elements requiring early attention, and develop realistic development timelines that account for uncertainty.

Recommended Methodology: Top-down or hybrid depending on option maturity.

GATE 1 REVIEW (FIRST PASS APPROVAL)

QCSRA Focus: Validate schedule readiness and tendering risks

At Gate 1, the project seeks approval to proceed to detailed design and tender. QCSRA validates that the development schedule is achievable and quantifies risks associated with different procurement approaches.

Recommended Methodology: Hybrid; blending detailed analysis of critical elements with strategic factors for less-defined aspects

GATE 2 REVIEW (SECOND PASS APPROVAL)

QCSRA Focus: Test scope, procurement, risk allocation, value engineering and strategic robustness

Gate 2 represents the major investment decision. QCSRA provides comprehensive analysis of:

- Whether the project can deliver within approved schedule and budget
- How risks are allocated between Commonwealth and contractors
- Whether proposed contingency levels are adequate
- What value engineering options exist and their risk implications

Recommended Methodology: Bottom-up or hybrid, providing robust, defensible analysis for this critical decision point

CONTRACT READINESS REVIEW (CRR)

QCSRA Focus: Confirm commercial and delivery readiness; test risk allocation

Prior to contract signature, QCSRA validates that commercial arrangements adequately address identified risks, that contractor plans are realistic, and that interfaces between Commonwealth and contractor responsibilities are well-defined.

Recommended Methodology: Bottom-up or hybrid with detailed focus on contract-specific risks

INTEGRATED BASELINE REVIEW (IBR)

QCSRA Focus: Establish and validate baseline schedule; assess realism, logic, float integrity, and risk exposure

The IBR establishes the formal baseline against which progress will be measured. QCSRA plays a central role in validating that this baseline is realistic, properly structured and supported by adequate contingency.

Recommended Methodology: Bottom-up, providing detailed validation of the baseline schedule

IMPLEMENTATION REVIEW

QCSRA Focus: Confirm mobilisation readiness; assess claims and acceleration risks; evaluate mobilisation plans

During implementation, QCSRA helps assess whether the project is genuinely on track, whether schedule compression is achievable if required and what risks exist around contractor claims for delays or variations.

Recommended Methodology: Bottom-up with continuous updating as actual performance data becomes available

OPERATIONAL READINESS REVIEW (ORR)

QCSRA Focus: Assess commissioning and operational risks

As the project transitions to operations, QCSRA focuses on commissioning risks, initial operational capability milestones and risks during the transition from project delivery to sustained operations.

Recommended Methodology: Bottom-up for commissioning risks, hybrid for longer-term operational risks

PROJECT CLOSURE REVIEW

QCSRA Focus: Evaluate benefits realisation; capture lessons learned

At closure, QCSRA contributes to lessons learned by comparing actual outcomes to probabilistic forecasts, analysing which risks materialised and which did not, and documenting factors that influenced accuracy of risk predictions.

Recommended Methodology: Bottom-up comparison of forecast to actual

This gate-aligned approach ensures that QCSRA remains relevant and valuable throughout the entire program lifecycle, adapting its focus and methodology as project maturity evolves.

7. Building Program-Level Risk Capability

For large, complex programs comprising multiple delivery streams – such as major defence infrastructure programs, fleet replacement programs, or enterprise system implementations – effective risk management requires capability uplift across the entire program, not just within individual projects.

RISK INTEGRATION INTO PROGRAM GOVERNANCE

The first requirement is embedding risk into core program governance rather than treating it as a separate, parallel process.

Link to Central PPRM Systems: Stream-level risk information must flow into central Project, Program & Portfolio Management (PPRM) systems where it can be consolidated, analysed and reported alongside schedule, cost and scope information. This integration prevents risk becoming an isolated data set disconnected from other program metrics.

Core Governance Forum Integration: Risk discussions must occur in core program governance forums – Project Steering Groups, Program Boards, Executive Review Committees – not relegated to separate Risk Working Groups that operate in parallel. This ensures that risk informs actual decisions, rather than being discussed separately and then ignored when decisions are made.

Standing Agenda Item: Risk should be a standing agenda item in governance forums, with structured reporting on:

- Current program risk profile and trends
- Critical risks and cross-stream dependencies
- Contingency status and burn rate
- Mitigation progress and effectiveness
- Emerging risks requiring attention

Replacing Isolated Risk Committees: Rather than maintaining separate Risk Working Groups that operate independently, embed risk discussions into stage gates and decision points where they naturally inform choices about progression, resource allocation and mitigation investments.

CAPTURING TWO TYPES OF PROGRAM-LEVEL RISK

Effective program-level risk management must distinguish between two fundamentally different types of risk:

Governance-Level Risks: These are strategic risks arising at portfolio oversight level:

- Strategic alignment with evolving defence priorities
- Resource prioritisation across competing programs
- Delivery direction and scope changes

- Stakeholder management and political considerations
- Funding profile and budget constraints

These risks are typically owned by senior program leadership or portfolio executives and may not be directly controllable by delivery teams.

Cross-Stream Risks: These are operational risks where the performance, delays or challenges of one stream impact another:

- Access dependencies (the work of one stream blocking another's access)
- Sequencing constraints (work that must occur in specific order across streams)
- Approval bottlenecks (single approval processes affecting multiple streams)
- Shared resources (skilled personnel, equipment, facilities needed by multiple streams)
- Shared trades or suppliers (capacity constraints affecting multiple streams)

These risks require joint visibility, coordinated response and clear accountability for managing the interdependency even when individual stream risks are well-controlled.

EMBEDDED RISK MANAGEMENT PER STREAM

While program-level integration is essential, each stream must maintain robust local risk management:

Stream-Specific Risk Registers: Each stream maintains its own risk register focused on risks within its scope and control. Registers should reflect genuine local uncertainties, not generic portfolio-wide risks that are actually owned at higher levels.

Consistent Principles, Tailored Application: All streams apply the same risk analysis principles (quantification, validation, assurance) but tailor their application to stream-specific contexts: complexity, maturity, criticality and available resources.

Clear Escalation Protocols: Well-defined protocols govern when risks escalate from stream to program level based on:

- Impact magnitude (exceeding stream authority or contingency)
- Cross-stream implications (affecting other streams' delivery)
- Strategic significance (affecting program objectives or stakeholder commitments)
- Mitigation requirements (requiring program-level resources or decisions)

LEVERAGING CONSISTENT METHODOLOGIES

To enable program-level aggregation and comparison, all streams must apply consistent methodologies:

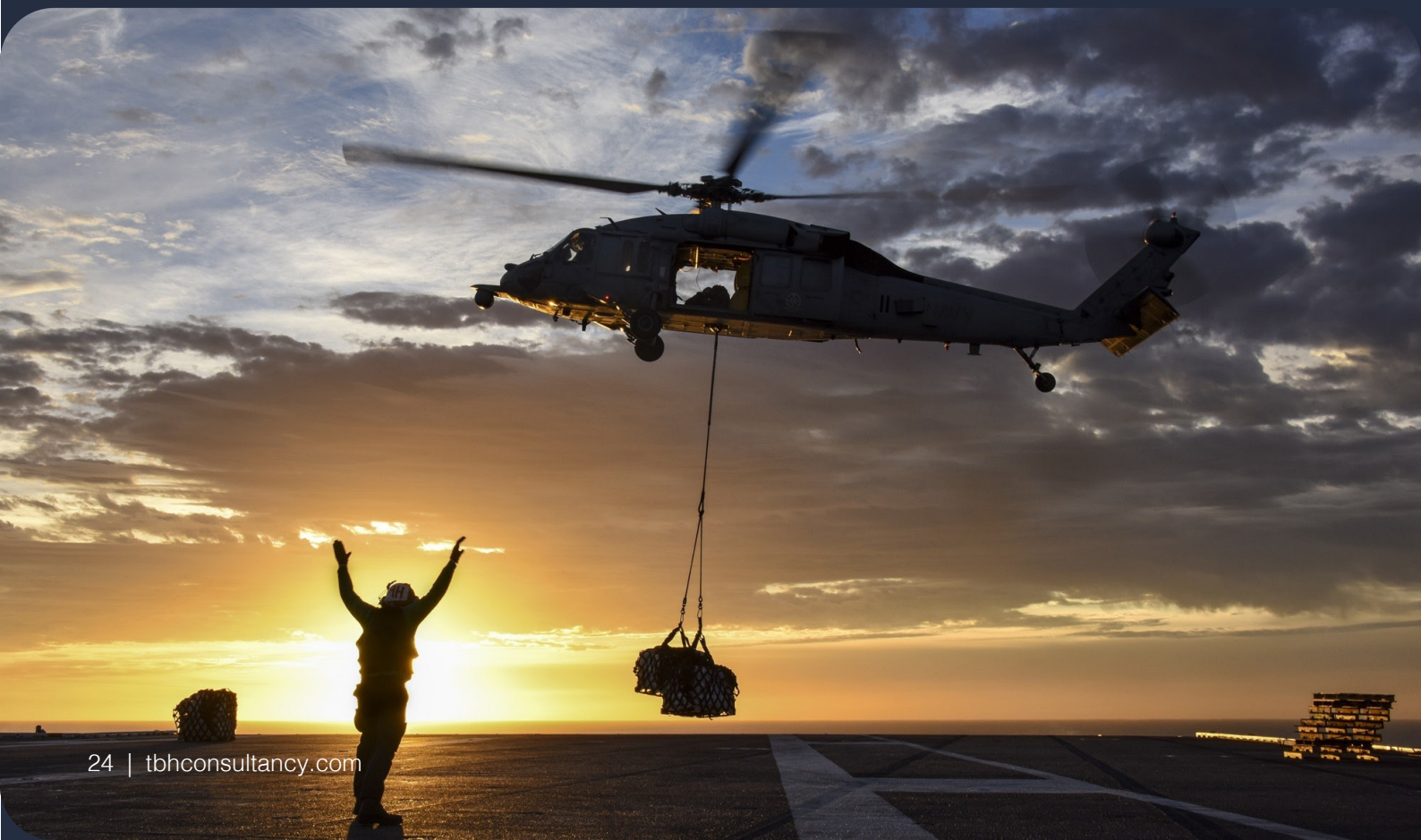
Common Methodology Framework:
The program establishes whether streams will use bottom-up, hybrid or top-down approaches, ensuring that results are expressed in comparable formats even if detailed methods vary.

Standardised Reporting:
All streams report risk using common formats, time units, cost units and confidence levels, enabling aggregation into program-level metrics.

Shared Assumptions:
Cross-stream assumptions (productivity rates, trade availability, approval durations) are documented and shared to ensure consistency and identify where streams have conflicting assumptions requiring resolution.

Integrated Schedules:
Stream schedules integrate into the program-level Integrated Master Schedule, ensuring that cross-stream dependencies are visible and that schedule risk analysis captures interdependencies.

This program-level capability ensures that risk management serves its ultimate purpose: enabling the program as a whole to make better decisions that ultimately lead to better delivery outcomes.



8. Governance and Assurance Architecture

Effective risk governance requires clear structures defining roles, responsibilities and information flows across organisational levels. TBH's framework implements a four-layer assurance model that balances autonomy with oversight.

LAYER 1: DELIVERY TEAMS (FUNCTION/UNIT LEVEL)

Role: Operational risk identification and management

Responsibilities:

- Identify and assess risks within assigned work scope
- Develop and implement mitigation strategies
- Maintain current, accurate risk information in registers
- Execute work within established risk tolerances
- Escalate risks exceeding authority or capability

Activities:

- Weekly or bi-weekly risk reviews within delivery teams
- Continuous risk identification as work progresses
- Real-time updating of risk status and mitigation progress
- Immediate escalation of emerging high-impact risks

LAYER 2: STREAM-LEVEL OVERSIGHT

Role: Validation and consistency within delivery streams

Responsibilities:

- Validate quality and completeness of risk information
- Ensure consistency of methods and assumptions within the stream
- Challenge delivery team assessments to counter bias
- Aggregate stream-level risk profile
- Manage cross-functional risks within the stream

Activities:

- Fortnightly stream risk reviews
- Monthly deep-dive on critical or high-value risks
- Quarterly assurance reviews of risk processes
- Preparation of stream risk reporting to program level

LAYER 3: PROGRAM-LEVEL DECISION MAKING

Role: Integrated risk management and decision-making

Responsibilities:

- Consolidate risk information across all streams
- Manage cross-stream risks and interdependencies
- Allocate contingency and mitigation resources
- Make risk-based trade-offs between schedule, cost and scope
- Escalate strategic risks to portfolio level

Activities:

- Monthly Program Board with risk as standing agenda item
- Quarterly Program Risk Reviews with deep analysis
- Continuous monitoring of program risk profile trends
- Gate review preparation and risk input to decision papers

Key Forum: Project Steering Group meets monthly with structured risk reporting covering:

- Program risk profile (quantified exposure and trends)
- Critical risks (top 10 by impact or urgency)
- Cross-stream dependencies and their status
- Contingency status (allocated, consumed, remaining)
- Mitigation decisions required from the Board

LAYER 4: PORTFOLIO OVERSIGHT AND STRATEGIC DIRECTION

Role: Strategic alignment and resource prioritisation

Responsibilities:

- Ensure risk management aligns with organisational strategy
- Prioritise resources across competing programs
- Set risk appetite and tolerance levels
- Provide strategic direction when risks threaten objectives
- Maintain oversight of governance-level risks

Activities:

- Quarterly portfolio reviews
- Annual risk capability assessments
- Gate reviews and approval decisions
- Strategic risk scenario planning

INFORMATION FLOW: VERTICAL AND HORIZONTAL

The governance architecture ensures information flows both vertically (through organisational levels) and horizontally (across delivery streams):

Vertical Flow: Risk information moves upward through layers with progressive aggregation and filtering:

- Delivery teams report all identified risks to stream level
- Stream level aggregates and filters, escalating significant risks to program level
- Program level consolidates across streams, escalating strategic risks to portfolio level
- Each layer adds context, validation, and analysis to support decision-making at the next level

Horizontal Flow: Risk information moves across streams to identify and manage interdependencies:

- Cross-stream risk registers capture dependencies
- Regular cross-stream coordination meetings identify emerging interdependencies
- Program-level forums provide visibility of all streams' critical risks
- Integrated schedules make interdependencies explicit and trackable

ASSURANCE MECHANISMS

Beyond structural governance, specific assurance mechanisms validate risk information quality:

Challenge Sessions: Structured workshops bring together diverse perspectives to:

- Test assumptions underlying risk assessments
- Challenge estimates that may reflect optimism bias
- Identify risks that may have been overlooked
- Validate that mitigation strategies are realistic and adequately resourced

Independent Review: Periodic independent reviews by internal assurance functions or external experts provide:

- Objective assessment of risk management maturity
- Validation of methodology application
- Benchmarking against industry practice
- Recommendations for continuous improvement

Data Quality Checks: Automated and manual checks ensure:

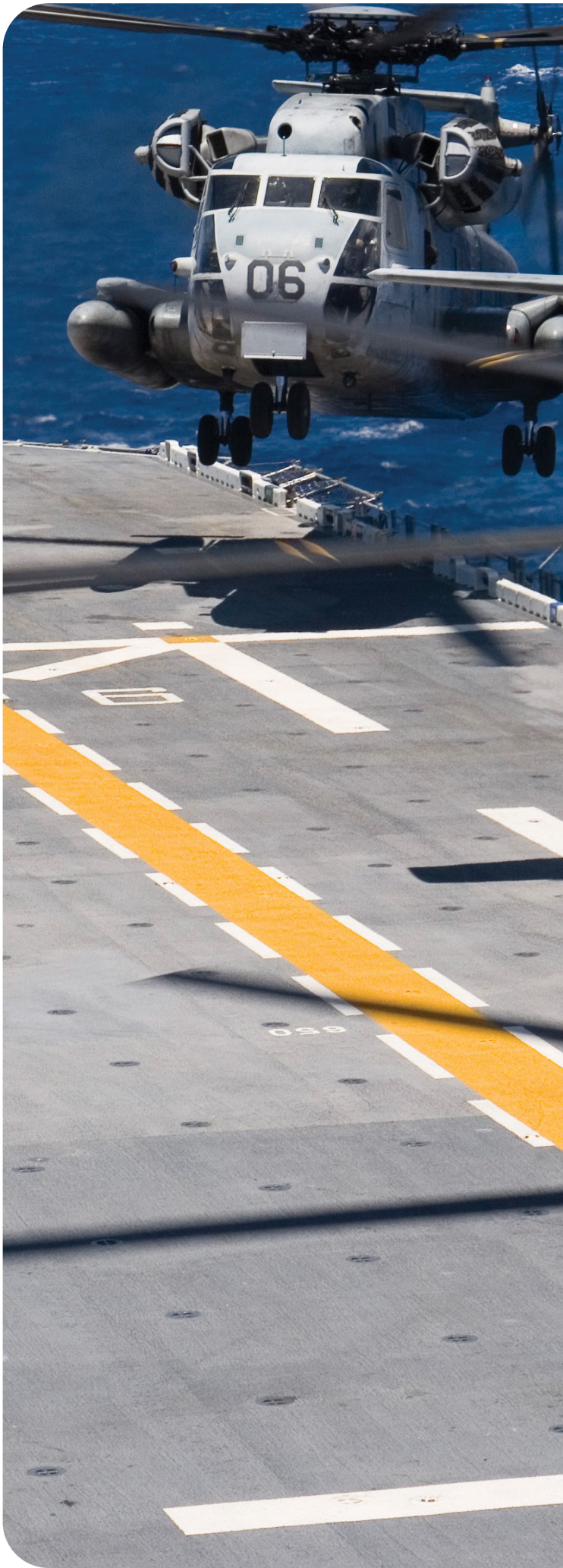
- Completeness (all required fields populated, no orphan risks)
- Consistency (assumptions align across related risks)
- Currency (risks regularly reviewed and updated)

- Accuracy (quantified impacts properly calculated and validated)

Pre-Escalation Validation: Before risk information escalates to senior forums, validation processes confirm:

- Analysis methods were properly applied
- Conclusions are supported by evidence
- Information is consistent with other program data
- Presentation is clear and decision-focused

This multi-layered governance architecture ensures that risk management operates effectively at all organisational levels while maintaining integration and consistency across the program.



2. The Implementation Roadmap

Transforming risk management practice requires structured change management implemented over time. TBH's implementation roadmap spans approximately 12 months, organised into four phases that build progressively toward mature capability.

Phase 1: Current State and Foundation (Weeks 1-2)

OBJECTIVES:

- Establish baseline understanding of current risk management maturity
- Develop roadmap for capability uplift
- Gain organisational commitment to transformation
- Define governance structures and roles

ACTIVITIES:

Maturity Baseline Assessment: Structured assessment of current state across multiple dimensions:

- Governance: How risk integrates with program governance
- Process: Quality and consistency of risk processes
- Capability: Skills, tools, and organisational capacity
- Culture: How risk is perceived and valued

The assessment identifies strengths to build upon, gaps requiring attention, and quick wins that can demonstrate value early.

Maturity Uplift Roadmap: Based on the baseline assessment, development of a detailed roadmap defining:

- Target maturity levels for each capability dimension
- Sequenced initiatives to close gaps
- Resource requirements and dependencies

- Success metrics and milestones

Conceptual Framework Presentation: Introduction of the integrated risk management framework to key stakeholders, covering:

- Founding principles and their rationale
- The transformation journey and four pillars
- Methodology options and selection criteria
- Expected benefits and change impacts

Governance Structure Design: Definition of the four-layer governance architecture including:

- Roles and responsibilities at each level
- Meeting cadences and agenda structures
- Information flows and escalation protocols
- Decision rights and authorities

Tools Requirements Definition: Assessment of technology needs and gaps:

- Risk Management Information System (RMIS) requirements
- Integration with existing project management tools (P6, etc.)
- Reporting and analytics capabilities
- Data migration and interfaces

DELIVERABLES:

- Maturity assessment report
- Implementation roadmap
- Governance structure documentation
- Tools requirements specification
- Stakeholder engagement plan

Phase 2: System Established (Weeks 3-8)

OBJECTIVES:

- Implement foundational frameworks and processes
- Launch pilot projects to test approaches
- Begin capability building through training
- Deploy initial technology solutions

ACTIVITIES:

Framework Implementation: Rollout of standardised risk management framework including:

- Risk register templates and standards
- Risk assessment methodologies and guidance
- Escalation protocols and thresholds
- Reporting templates and requirements

Pilot Project Selection and Launch: Identification of 2-3 pilot projects representing different:

- Sizes and complexities
- Maturity levels
- Delivery approaches
- Organisational contexts

Pilots enable testing and refinement of frameworks before broader rollout while generating early examples of value delivered.

Training Commencement: Structured capability building targeting different organisational levels:

- Executive briefings on risk-informed decision-making
- Project manager training on quantitative risk analysis
- Scheduler training on risk-aware scheduling
- Risk practitioner training on detailed methodologies

Training combines classroom instruction with hands-on application in pilot projects, ensuring learning translates to practice.

RMIS Deployment: Implementation of Risk Management Information System:

- System configuration and customization
- Data migration from existing systems
- User access provisioning and training
- Integration with project management tools
- Reporting dashboard configuration

Initial Program Reporting: Development and issuance of first integrated program risk reports demonstrating:

- Quantified program risk profile
- Cross-stream dependencies and their status
- Critical risks requiring management attention
- Contingency status and trends

DELIVERABLES:

- Implemented framework documentation
- Pilot project risk analyses
- Training materials and records
- Operational RMIS
- First program risk report

Phase 3: Stabilisation and Short-Term Maturity (Weeks 8-24)

OBJECTIVES:

- Expand proven approaches beyond pilots to full program
- Embed risk information into decision-making processes
- Achieve consistent application across all functions
- Demonstrate measurable value from risk management

ACTIVITIES:

Program-Wide Rollout: Extension of frameworks and processes to all delivery streams:

- Tailored implementation plans for each stream
- Stream-specific training and support
- Gradual transition from old to new approaches
- Continuous support and troubleshooting

Risk Data Informing Decisions: Progressive integration of risk information into actual business decisions:

- Risk profiles inform resource allocation choices
- Contingency drawdown based on quantified risk reduction
- Schedule commitments reflect probabilistic analysis
- Trade-off decisions explicitly consider risk impacts

Consistent Application: Achievement of consistency across the program:

- All streams using standardised templates and methods
- Risk reporting on common cadence and format
- Cross-stream coordination functioning effectively
- Governance forums operating as designed

Evidence of Value: Documentation of tangible benefits:

- Decisions that were improved by risk information
- Issues identified early through risk analysis
- Resources allocated more effectively based on risk
- Stakeholder confidence increased through transparency

Continuous Improvement: Systematic refinement based on experience:

- Regular retrospectives on what's working and what isn't
- Framework adjustments based on user feedback
- Process streamlining to reduce administrative burden
- Enhanced integration with other program processes

DELIVERABLES:

- Comprehensive program risk database
- Consistent monthly program risk reports
- Evidence of value case studies
- Refined framework documentation
- Lessons learned and improvements implemented

Phase 4: Full Risk Maturity (Weeks 24-54)

OBJECTIVES:

- Embed risk management into organisational culture
- Achieve self-sustaining capability
- Continuously improve and evolve practices
- Position risk as strategic enabler

ACTIVITIES:

Cultural Embedding: Risk management becomes "how we work" rather than an additional process:

- Delivery teams proactively identify and manage risks
- Risk considerations are natural part of planning
- Open discussion of uncertainty without blame
- Learning from both risks that materialize and those that don't

Self-Sustaining Capability: Organisation maintains and evolves risk management independently:

- Internal experts can train new team members
- Frameworks adapted to changing program needs
- Technology systems maintained and enhanced internally
- Continuous improvement driven from within

Advanced Capabilities: Organisation develops sophisticated practices:

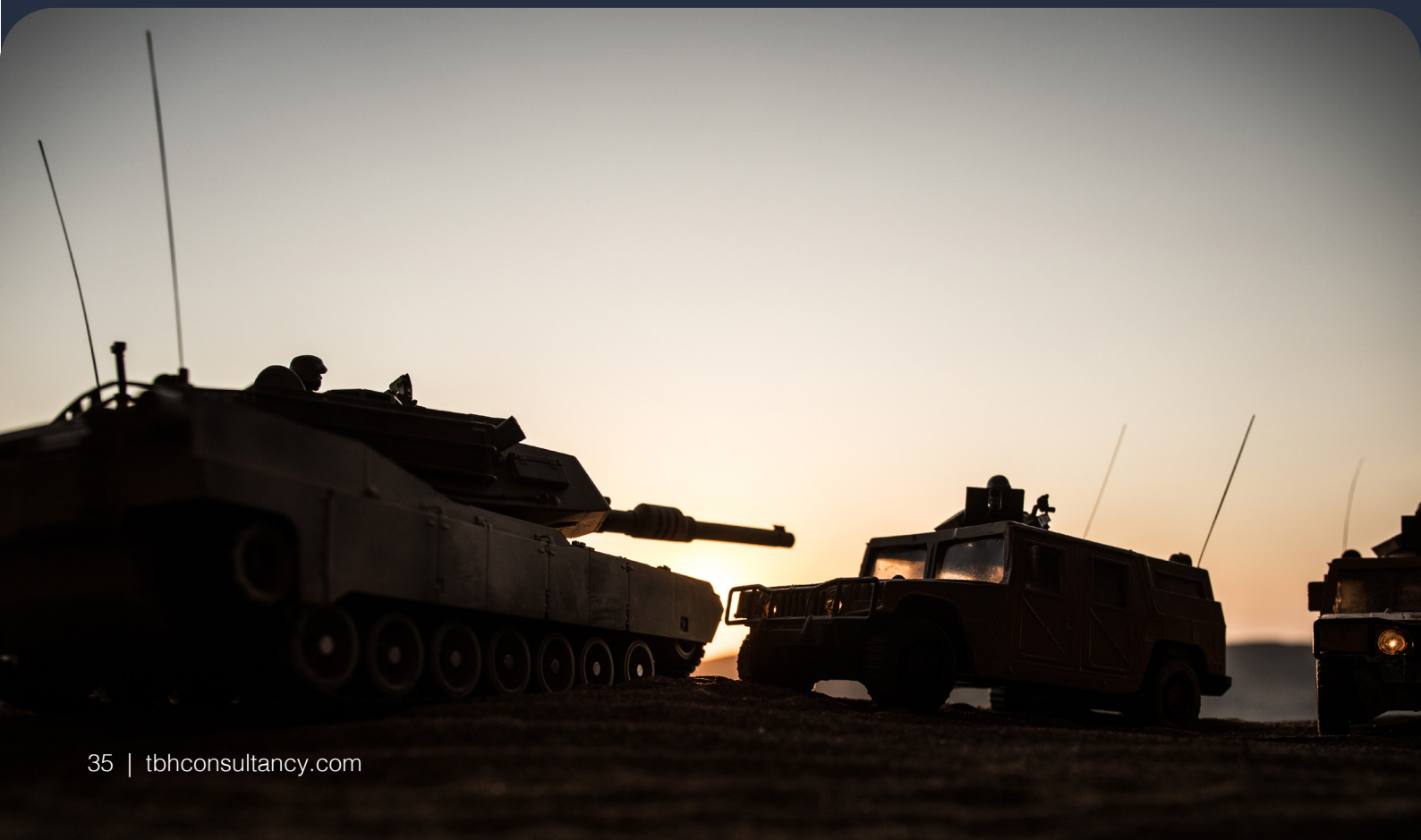
- Predictive analytics identifying emerging risk patterns
- Portfolio optimization based on risk-return trade-offs
- Scenario planning for strategic uncertainties
- Risk culture assessment and enhancement

Strategic Positioning: Risk management recognised as strategic capability:

- Risk information central to strategic planning
- Competitive advantage in bidding on complex programs
- Organisational reputation for delivery excellence
- Benchmark for other programs

DELIVERABLES:

- Mature, embedded risk management capability
- Track record of improved delivery outcomes
- Internal capability to sustain and evolve practices
- Documentation of journey for lessons sharing



IMPLEMENTATION SUCCESS FACTORS

Several factors prove critical to successful implementation:

Executive Sponsorship: Visible, active championship by senior program leadership, demonstrating use of risk information in their own decisions and holding the organisation accountable for quality risk management.

Adequate Resourcing: Sufficient resources (people, tools, time) allocated to implementation. Under-resourced transformation efforts inevitably fail.

Pragmatic Approach: Balance between methodological rigor and practical application, avoiding perfectionism that delays value delivery.

Change Management: Explicit attention to the human dimensions (communication, training, support, recognition) that determine whether frameworks are adopted or ignored.

Quick Wins: Early demonstration of value that builds momentum and stakeholder confidence, enabling sustained investment in longer-term transformation.

Persistence: Recognition that cultural change takes time, with sustained effort over months and years rather than quick fixes.

This phased roadmap provides structure while remaining flexible enough to adapt to specific organisational contexts and challenges encountered during implementation.

10. Tools, Technology, and Capability Development

Effective integrated risk management requires the right combination of tools, technology, and human capability. TBH's approach addresses all three dimensions in a coordinated manner.

TECHNOLOGY ARCHITECTURE

Risk Management Information System (RMIS): The core technology platform provides:

Risk Register Management:

- Structured capture of risk information with mandatory fields
- Workflow for risk identification, assessment, and approval
- Version control and audit trail of changes
- Attachment storage for supporting documentation
- Filtering and searching across large risk databases

Quantitative Analysis Integration:

- Integration with scheduling tools (Primavera P6) for schedule risk analysis
- Integration with cost estimating tools for cost risk analysis
- Monte Carlo simulation capabilities for probabilistic modelling
- Sensitivity analysis to identify key risk drivers
- What-if scenario modelling

Reporting and Dashboards:

- Pre-configured reports for different organisational levels
- Interactive dashboards with drill-down capabilities
- Trend analysis and visualisation
- Export capabilities for presentations and documents
- Automated report distribution

Collaboration Features:

- Risk review and comment workflows
- Cross-stream visibility and coordination
- Notification and alerting for changes
- Mobile access for field teams
- Integration with collaboration platforms (Teams, SharePoint)

INTEGRATION WITH PROJECT MANAGEMENT TOOLS

The RMIS must integrate seamlessly with existing project management ecosystem:

Primavera P6 Integration: Bi-directional integration enables:

- Import of schedule activities for risk assignment
- Export of risk-adjusted durations back to schedules

- Synchronisation of progress and status information
- Consistent milestone and critical path visibility

Cost Management Integration: Connection to cost management systems provides:

- Import of cost breakdown structures
- Export of risk-adjusted cost estimates
- Tracking of contingency allocation and consumption
- Variance analysis comparing risk forecasts to actuals

Document Management Integration: Links to document repositories enable:

- Association of risks with relevant documents
- Access to assumptions and basis of estimate documentation
- Audit trail connecting risk analysis to source information

CAPABILITY DEVELOPMENT FRAMEWORK

Technology alone does not create capability. Structured development of human skills and organisational competency is equally critical.

Competency Levels: The framework defines progressive competency levels:

Level 1 - Awareness: All program personnel understand:

- Why risk management matters to program success
- Basic risk concepts and terminology
- Their role in risk identification and escalation
- How to access risk information relevant to their work

Level 2 - Application: Project managers and risk coordinators can:

- Maintain risk registers with quality information
- Facilitate risk identification workshops
- Apply appropriate assessment methodologies
- Develop and track mitigation plans
- Prepare risk reports for governance forums

Level 3 - Analysis: Risk specialists and analysts can:

- Conduct quantitative cost and schedule risk analysis
- Select and apply appropriate methodologies
- Validate and challenge risk assessments
- Interpret and communicate analytical results
- Support decision-making with risk insights

Level 4 - Design: Senior risk practitioners can:

- Design risk management frameworks
- Customise methodologies for specific contexts
- Lead organisational capability building
- Provide expert advice to senior leadership
- Drive continuous improvement initiatives

Training Programs: Structured training addresses each competency level:

Executive Briefings (Half-day):

- Risk-informed decision-making
- Interpreting probabilistic forecasts
- Evaluating risk vs. return trade-offs
- Case studies of risk management value

Risk Fundamentals (2 days):

- Risk management principles and frameworks
- Risk identification and assessment techniques
- Risk register management
- Mitigation planning and tracking
- Roles and responsibilities

Quantitative Risk Analysis (3 days):

- Statistical foundations (probability, distributions)
- Methodology selection and application
- Monte Carlo simulation techniques
- Results interpretation and communication
- Software tools (hands-on)

Advanced Topics (Variable):

- Specific methodologies (bottom-up, hybrid, top-down)
- Industry-specific contexts (defence acquisition)
- Integration with earned value management
- Risk modelling in complex programs

Ongoing Support: Beyond formal training, sustained capability building requires:

Communities of Practice: Regular forums where practitioners:

- Share experiences and lessons learned
- Discuss challenging risk scenarios
- Develop consistent interpretations of frameworks
- Maintain peer support networks

Coaching and Mentoring: One-on-one support for practitioners applying methods to real projects, providing guidance through complex analyses and helping develop judgement alongside technical skills.

Knowledge Management:
Documented library of:

- Standard methodologies and templates
- Case studies and examples
- Lessons learned from past projects
- FAQs and troubleshooting guides

Certification Programs: Optional professional certification providing:

- Formal recognition of capability
- Career development pathways
- Quality assurance for key roles
- Alignment with industry standards

TECHNOLOGY AND CAPABILITY MATURITY PATH

Organisations typically progress through maturity stages:

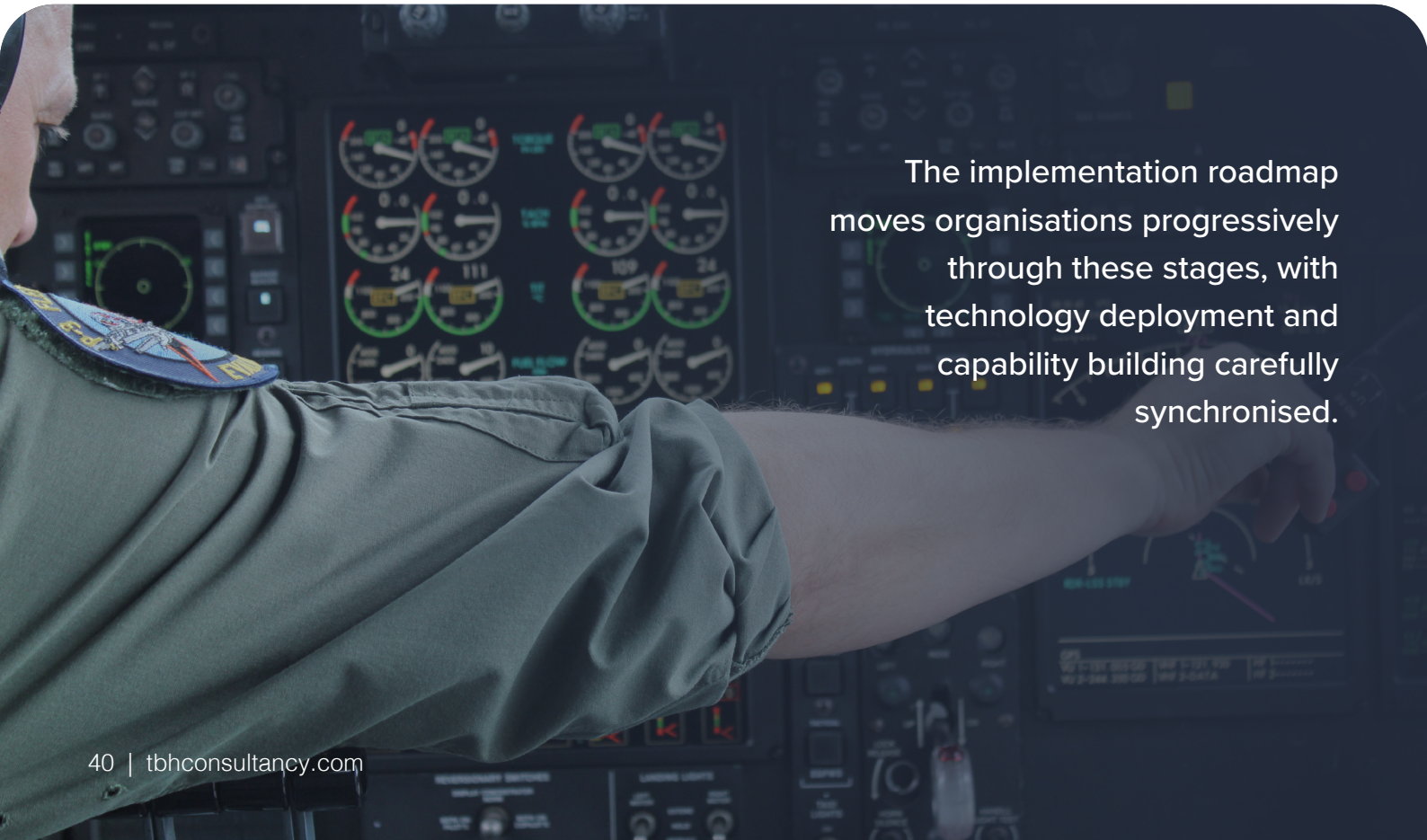
Stage 1 Manual:
Basic spreadsheets and documents, heavy manual effort, inconsistent approaches.

Stage 2 - Systematic:
Standardised templates and processes, basic RMIS for register management, growing consistency.

Stage 3 - Integrated:
Full RMIS deployment with analytics, integration with PM tools, consistent quantitative analysis.

Stage 4 - Optimised:
Advanced analytics and automation, predictive capabilities, continuous improvement culture.

Stage 5 - Innovative
Risk management as competitive advantage, industry-leading practices, strategic risk optimisation.



The implementation roadmap moves organisations progressively through these stages, with technology deployment and capability building carefully synchronised.

11. Reporting Framework:

Making Risk Visible and Actionable

Risk information has value only when it reaches decision-makers in forms they can understand and act upon. The reporting framework must serve multiple audiences with different needs while maintaining consistency and traceability.

HIERARCHICAL REPORTING STRUCTURE

Executive Summary (Portfolio Level):
Single-page view for senior executives covering:

- Portfolio-wide risk exposure (single number at P80)
- Top 5 risks across entire portfolio
- Critical cross-program dependencies
- Strategic risks requiring executive attention
- Trend indicators (improving/stable/deteriorating)

Program Dashboard (Program Leadership):
Comprehensive view for Program Boards including:

- Program risk profile with confidence levels (P20/P50/P80)
- Quantified schedule and cost impacts
- Risk breakdown by category or stream
- Top 10-15 critical risks with status
- Cross-stream dependencies and integration risks
- Contingency status (allocated/consumed/remaining)
- Mitigation status for critical risks
- Trends over past 3-6 months

Stream Reports (Delivery Managers):
Detailed view for stream management:

- Complete stream risk register
- All risks with quantified impacts
- Detailed mitigation plans and progress
- Emerging risks requiring attention
- Integration points with other streams
- Resource requirements for risk response
- Detailed assumptions and basis of estimates

Specialised Reports: Targeted reports for specific purposes:

- Gate review packages for approval decisions
- Deep-dive analyses of specific high-impact risks
- Scenario analysis for strategic options
- Benchmarking against similar programs
- Lessons learned and retrospectives

REPORT CONTENT STANDARDS

All risk reports adhere to consistent content standards:

Quantified Impacts:

All significant risks express impacts in concrete terms:

- Schedule impacts in days or weeks
- Cost impacts in dollars
- Both gross (pre-mitigation) and residual (post-mitigation) exposures
- Probability of occurrence
- Expected value (probability × impact)

Temporal Information:

- When the risk might materialise (risk period)
- How long impacts would persist
- Lead time required for mitigation
- Dependencies on schedule milestones

Ownership and Accountability:

- Clear risk owner (individual, not committee)
- Mitigation action owners
- Escalation path if mitigation fails
- Resources committed to response

Status and Trends:

- Current status (open/closed/mitigated)
- Trend direction (increasing/stable/decreasing)
- Changes since last reporting period
- Trigger events or indicators to watch

Context and Narrative:

- Clear description of the risk
- Why it matters to program objectives
- What has been done to address it
- What decisions are needed
- Links to related risks or issues

REPORTING CADENCE

Different reporting frequencies serve different purposes:

Weekly:
Internal delivery team risk reviews, minimal formal reporting, focus on emerging issues.

Fortnightly:
Stream-level consolidated updates, tracking of high-priority risks, coordination across functions.

Monthly:
Program Board reporting, full program risk profile, critical risk deep-dives, cross-stream coordination.

Quarterly:
Portfolio reviews, trend analysis, maturity assessments, strategic risk scenarios.

Event-Driven:
Gate reviews, major decision points, significant risk materialisation, crisis situations.

VISUALISATION AND COMMUNICATION

Effective risk communication uses appropriate visualisation:

Risk Matrices: Visual plot of risks by likelihood and consequence, helping identify priorities and concentrations.

Tornado Diagrams: Bar charts showing relative contribution of individual risks to total program exposure, highlighting where mitigation effort should focus.

Trend Charts: Time-series showing how program risk profile evolves, demonstrating whether risk management is effective.

Probability Distributions: S-curves or histograms showing the range of possible outcomes and their probabilities, supporting probabilistic decision-making.

Heat Maps: Color-coded matrices showing risk status across multiple dimensions (streams, categories, time periods), providing at-a-glance status.

Network Diagrams: Visual representation of risk interdependencies, showing how risks relate and potentially cascade.

MAKING REPORTS ACTIONABLE

The ultimate test of reporting effectiveness is whether it drives action. Actionable reports:

Focus on Decisions: Each report clearly identifies what decisions are needed, by whom, and by when, rather than simply presenting information.

Provide Options: Where mitigation or response choices exist, reports present options with evaluated trade-offs rather than single recommendations.

Highlight Changes: Emphasis on what has changed since last reporting, avoiding repeated presentation of static information.

Escalate Appropriately: Information escalates only when it requires attention or decision at that level, avoiding drowning senior leaders in operational detail.

Enable Drill-Down: Summary reports link to detailed supporting information, allowing readers to pursue deeper understanding where needed without cluttering primary reports.

This reporting framework ensures that risk information flows effectively through the organisation, reaching the right people at the right time in forms that enable confident decision-making.

12. Case for Change:

Why Traditional Approaches Fall Short

Understanding why integrated quantitative risk management represents such a significant improvement requires examining the specific failures of traditional qualitative approaches.

THE ILLUSION OF CONTROL

Traditional risk matrices plotting likelihood against consequence create an illusion of precision and control. A risk rated “likely” with “major” impact appears to be well-understood and managed. In reality, these qualitative ratings mask fundamental uncertainties:

What does “likely” mean?:
Different individuals interpret “likely” as probabilities ranging from 30% to 70%, producing inconsistent assessments.

What constitutes “major”?:
Without quantified thresholds, “major” means different things to different assessors and in different contexts.

How do we compare risks?:
Is a “possible/catastrophic” risk more or less concerning than a “likely/moderate” risk? Qualitative matrices provide no objective way to answer.

How much mitigation is enough?:
If mitigation reduces a risk from “likely/major” to “possible/moderate,” is that sufficient? Have we actually reduced exposure meaningfully or just changed labels?

THE AGGREGATION PROBLEM

Individual projects may maintain high-quality qualitative risk registers while program-level understanding remains poor because qualitative assessments cannot be meaningfully aggregated.

If Stream A reports three "high" risks and Stream B reports five "high" risks, the program doesn't have eight "high" risks; some may overlap, some may be interdependent, and their cumulative impact cannot be determined from qualitative ratings alone.

This aggregation problem means program leaders lack visibility into total risk exposure and cannot make informed decisions about portfolio-level contingency, resource allocation or strategic priorities.

THE DISCONNECTION FROM PLANNING

Traditional risk management often operates independently from schedule and cost planning. Planners develop schedules and budgets using single-point estimates with perhaps a percentage contingency, while risk managers separately maintain registers identifying what might go wrong.

This disconnection produces several failures:

Incompatible Baselines: The schedule baseline assumes everything goes according to plan, while the risk register documents all the things that won't. These contradictory views create confusion about what is realistic.

Invisible Dependencies: Risk impacts on critical path and schedule dependencies remain invisible until risks materialise, at which point it's too late for proactive management.

Arbitrary Contingency: Without quantified risk analysis, contingency levels are set based on precedent, policy, or negotiation rather than actual exposure, leading to either inadequate contingency (program failure) or excessive contingency (inefficient resource use).

THE OPTIMISM BIAS TRAP

Psychological research consistently demonstrates that individuals and organisations systematically underestimate how long tasks will take and how much they will cost – the "planning fallacy" or optimism bias.

Qualitative risk management fails to counter this bias effectively. When asked to identify risks, teams typically identify discrete events ("supplier fails to deliver") while failing to capture the inherent uncertainty in their baseline estimates ("this task will actually take longer than our estimate").

The result is systematically optimistic plans that fail predictably, eroding stakeholder confidence and damaging organisational credibility.

THE STATIC REGISTER PROBLEM

Traditional risk registers become static documents that grow ever longer but provide diminishing value. Risks identified at program inception persist unchanged for years. New risks are added but old ones rarely removed. Reviews become ritual recitations of familiar risks rather than dynamic management tools.

Decision-makers stop engaging with risk reports because they contain no new information and don't demonstrably help with decisions. Risk management becomes compliance activity – maintaining the register because governance requires it – rather than strategic capability.

THE MISSING LINK TO ACTION

Perhaps most critically, traditional approaches fail to create clear links between risk information and management action. When a risk is identified and rated "high," what should leadership do? Allocate more resources? Accept the risk? Change the approach? The qualitative information provides no basis for these choices.

Without quantified impact and probability, cost-benefit analysis of mitigation options is impossible. Without integration into schedules and budgets, tracking whether mitigation is working is difficult. Without clear accountability and resources, mitigation remains aspirational.

THE EVIDENCE FOR CHANGE

Multiple studies and reviews of major programs document these failures:

Defence acquisition programs consistently experience schedule delays averaging 30-40% and cost overruns of 20-30%, largely due to inadequate risk management.

Independent reviews repeatedly cite failure to quantify risk, inadequate contingency and optimism bias as contributing factors to program failures.

Industry research demonstrates that programs using quantitative risk analysis achieve significantly better outcomes on schedule and cost performance.

Organisational maturity models consistently show that progression from qualitative to quantitative risk management represents a critical capability uplift.

The case for change is compelling: traditional qualitative approaches, while better than ignoring risk entirely, systematically fail to provide the information decision-makers need to manage complex programs effectively. Quantitative, integrated approaches address these failures directly, providing the foundation for superior program outcomes.

13. Conclusion

A New Paradigm for Defence Risk Management

Defence programs operate in an environment of irreducible uncertainty. Technical challenges, schedule dependencies, resource constraints, supply chain disruptions, regulatory approvals and stakeholder expectations all introduce variability that cannot be eliminated through better planning alone. The question is not whether programs will face risks, but whether they will manage those risks effectively.

Traditional qualitative approaches to risk management, while representing improvement over ignoring risk entirely, prove inadequate for the complexity, scale, and stakes of major defence acquisition programs. These approaches produce information that is subjective, inconsistent, difficult to aggregate and insufficiently actionable for the decisions program leaders must make.

Integrated Defence Risk Management represents a fundamentally different paradigm. In quantifying risk impacts in terms of schedule and cost, embedding risk analysis into planning and governance processes, applying rigorous methodologies matched to project maturity and maintaining structured assurance of information quality, this approach transforms risk from abstract discussion topic to actionable intelligence.

The benefits of this transformation are substantial and measurable:

Better Decisions: Leaders make choices based on probabilistic forecasts and quantified trade-offs rather than subjective judgement, leading to decisions better calibrated to actual risk.

More Realistic Plans: Schedules and budgets developed through risk-informed planning reflect the uncertainty inherent in complex programs, setting achievable commitments rather than aspirational targets.

Appropriate Contingency: Contingency levels determined through quantitative analysis match actual risk exposure, avoiding both inadequate contingency (leading to overruns) and excessive contingency (leading to inefficiency).

Earlier Issue Identification: Continuous quantitative analysis identifies emerging problems while time remains for effective response, rather than recognising issues only when they become crises.

Improved Stakeholder Confidence: Transparent, quantified risk information builds confidence among stakeholders who see that risks are acknowledged, understood, and actively managed.

Superior Delivery Outcomes: Ultimately, programs using integrated quantitative risk management demonstrate better performance on schedule adherence, cost control, and capability delivery.

IMPLEMENTATION IMPERATIVES

Organisations seeking to achieve these benefits must recognise several imperatives:

Leadership Commitment: Transformation requires sustained executive sponsorship, not merely endorsement. Leaders must demonstrate use of risk information in their decisions and hold the organisation accountable for quality risk management.

Adequate Resources: Implementation requires investment in technology, training, and dedicated capability. Under-resourced efforts inevitably fail to deliver value, undermining confidence in the approach.

Patience and Persistence: Cultural change takes time. Organisations must maintain commitment through the inevitable challenges and setbacks of transformation, recognising that capability building is a journey measured in years, not months.

Pragmatic Rigor: The approach must balance methodological soundness with practical application, avoiding both the trap of oversimplification (producing unreliable results) and the trap of perfectionism (never delivering value).

Continuous Improvement: Risk management capability must evolve based on experience, lessons learned and changing program contexts. The framework provides structure but must remain flexible enough to improve.

THE PATH FORWARD

For defence organisations and programs ready to embark on this transformation, TBH's Integrated Defence Risk Management service provides comprehensive support throughout the journey:

- Assessment of current maturity and development of tailored roadmaps
- Design and implementation of governance structures and frameworks
- Selection and application of appropriate quantitative methodologies
- Technology deployment and integration with existing systems
- Capability building through training, coaching, and mentoring
- Ongoing support for continuous improvement and maturity progression

The service is designed to work alongside program teams, building capability through doing rather than simply delivering frameworks and departing. The goal is not merely to implement risk management processes, but to fundamentally change how programs think about and manage uncertainty.

A STRATEGIC IMPERATIVE

In an era of increasingly complex defence capabilities, compressed timelines, budget constraints and intense scrutiny of program performance, effective risk management is not optional – it is a strategic imperative. Programs that manage risk well deliver capabilities on time, on budget, and to specification. Programs that manage risk poorly face delays, overruns, capability compromises and stakeholder loss of confidence. The choice is clear: persist with traditional qualitative approaches that have repeatedly proven inadequate, or embrace integrated quantitative methods that provide the information modern defence programs require for success.

Integrated Defence Risk Management represents more than a new set of tools and processes. It represents a new paradigm for how defence organisations approach the fundamental challenge of delivering complex capabilities amid uncertainty. Organisations that embrace this paradigm position themselves for superior delivery performance, enhanced stakeholder confidence and sustained competitive advantage in an increasingly demanding environment.

The journey is substantial but the destination is worth pursuing: defence programs that acknowledge uncertainty rather than ignore it, quantify risk rather than describe it abstractly, and make better decisions that lead to better outcomes. This is the promise – and the proven reality – of Integrated Defence Risk Management.

About TBH

TBH is a leading project delivery expert specialising in complex programs across defence, infrastructure, and major capital projects. With deep expertise in quantitative risk analysis, schedule assurance, and program governance, TBH helps organisations deliver better outcomes through structured, data-driven approaches to project management.

The Integrated Defence Risk Management service represents TBH's commitment to transforming how defence programs manage uncertainty, combining rigorous quantitative methods with pragmatic implementation approaches that build sustainable organisational capability.

For more information about Integrated Defence Risk Management or to discuss how TBH can support your program's risk management transformation, **visit tbhconsultancy.com** or contact our team directly.

tbhconsultancy.com