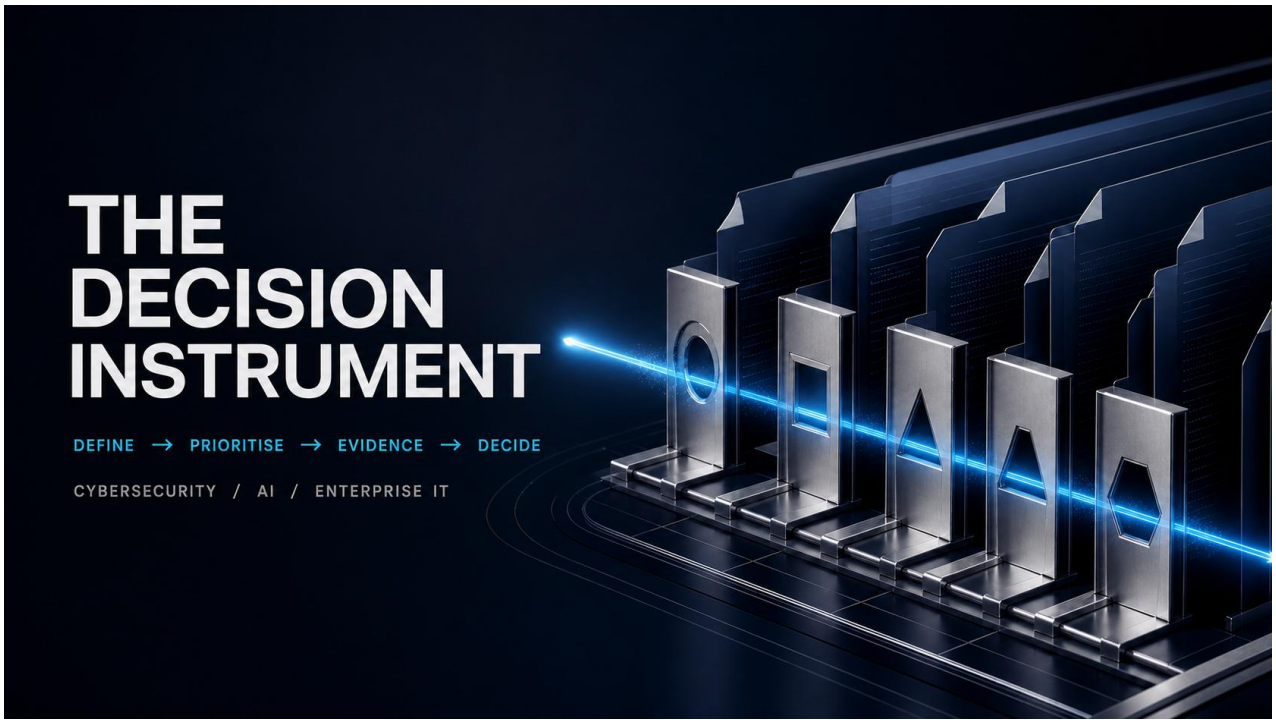
PRACTICAL PROCUREMENT FRAMEWORK

The Enterprise Technology RFP Template

A MoSCoW-structured framework for cybersecurity, AI and enterprise IT procurement



PURPOSE Use this working document to define scope, prioritise requirements, require comparable evidence, score responses and preserve a defensible decision record.

Independent evaluation | Zero fee to the client | Selected provider pays a capped fee

Your organisation contracts directly with the selected provider. CYBORIUM does not sell, deliver, operate or invoice technology.

How to use this template

This template is designed to be edited. Replace bracketed prompts, remove questions that are not material, and add requirements only when they help distinguish a suitable provider from an unsuitable one.

1. Define the business outcome, constraints and non-goals before writing detailed requirements.
2. Classify each requirement as Must, Should, Could or Won't for this procurement.
3. State the evidence expected for every scored requirement.
4. Issue one response format to all participating providers.
5. Score the evidence, not the presentation, and preserve the moderation rationale.
6. Keep commercials separate from solution merit until the technical evaluation is sufficiently mature.

DECISION RULE A requirement is only useful when it can change the decision. If it cannot affect eligibility, score, risk treatment, scope or contract terms, remove it.

Template map

Section	Decision purpose	Primary owner
1. RFP control sheet	Set governance, authority and process boundaries	Procurement lead
2. Context, outcome and scope	Make the problem and boundaries explicit	Executive sponsor
3. MoSCoW requirements	Separate non-negotiables from differentiators	Business and technical leads
4. Provider response and evidence	Create like-for-like answers	Evaluation lead
5. Evaluation and scoring	Convert evidence into a moderated result	Evaluation panel
6. Commercials and due diligence	Expose whole-of-life cost and provider risk	Finance, legal and risk
7. Process and decision record	Preserve probity and an auditable outcome	Procurement lead

Framework source: CYBORIUM's MoSCoW requirements method. Adapt this document to your organisation's procurement policy, delegations, legal requirements and recordkeeping obligations.

1. RFP control sheet

Complete this page before the RFP is issued. It establishes who controls the process, which approvals apply and how participants will receive consistent information.

Control field	Entry
RFP title and reference	[Complete before issue]
Issuing organisation	[Complete before issue]
Executive sponsor	[Complete before issue]
Procurement lead	[Complete before issue]
Evaluation chair	[Complete before issue]
Probity or legal adviser	[Complete before issue]
Issue date	[Complete before issue]
Clarification deadline	[Complete before issue]
Response deadline and time zone	[Complete before issue]
Expected decision date	[Complete before issue]
Contracting entity	[Complete before issue]
Approved contact channel	[Complete before issue]
Confidentiality classification	[Complete before issue]
Delegated approval authority	[Complete before issue]

Governance declarations

- [ ] All evaluation panel members have declared actual, potential or perceived conflicts of interest.
- [ ] Evaluation criteria and weights were approved before responses were opened.
- [ ] Material clarifications will be distributed consistently to participating providers.
- [ ] The decision record will retain scores, moderation notes, risk treatments and approval evidence.

2. Context, outcome and scope

2.1 Organisation context

[Describe the operating environment in terms that affect the solution: sector, scale, locations, critical services, regulatory context, data sensitivity, existing architecture and material dependencies. Avoid generic corporate history.]

2.2 Procurement outcome

Outcome field	Organisation entry
Problem to solve	[State the current condition and why it matters now.]
Target business outcome	[State the measurable change the procurement must enable.]
Measures of success	[List 3-6 outcome measures, their baselines and target dates.]
Executive risk if unresolved	[State operational, cyber, financial, legal or strategic exposure.]
Decision deadline	[State the deadline and the consequence of missing it.]

2.3 Scope boundaries

In scope	Out of scope	Dependencies / assumptions
[Service, capability, users, locations, data, integrations]	[Explicit exclusions and retained responsibilities]	[Program, platform, identity, network, data or resource dependencies]

2.4 Current-state evidence available to providers

- [ ] Architecture or data-flow diagrams
- [ ] Current service volumes and incidents
- [ ] Asset or application inventory
- [ ] Control maturity or audit findings
- [ ] Integration catalogue
- [ ] Relevant policies and standards

3. MoSCoW requirements schedule

MoSCoW prevents every stakeholder preference from becoming a false non-negotiable. The category belongs to the procurement decision, not to the feature in the abstract.

Tier	Meaning in this RFP	Evaluation treatment
MUST	Essential for the solution to be viable or the risk to be acceptable.	Pass/fail unless an approved exception and treatment exist.
SHOULD	Important and expected, but a credible workaround or staged delivery may be acceptable.	Scored and weighted; gaps require impact and treatment.
COULD	Useful additional value if justified by evidence, cost and complexity.	Low-weight differentiator; never allowed to mask a Must gap.
WON'T	Explicitly excluded from this procurement or phase.	Not scored; prevents scope drift and misleading assumptions.

Requirement-writing test

- Is the requirement connected to an outcome, control, constraint or material risk?
- Can a provider answer it without guessing what 'enterprise-grade', 'seamless' or 'best practice' means?
- Does it specify the evidence needed to support the answer?
- Can the evaluation panel distinguish partial, adequate and strong responses?
- Is the priority defensible if challenged by an executive, auditor or provider?

ANTI-PATTERN Do not make every requirement a Must. An oversized Must list narrows the market, encourages unsupported compliance claims and removes the information needed to compare credible options.

3.1 Requirements register

Copy rows as required. Give each requirement one owner, one priority and one evidence request. Split compound requirements.

ID	Requirement	MoSCoW	Evidence required	Owner	Treatment
SEC-01	The service must support phishing-resistant MFA for privileged access.	Must	Configuration evidence and implementation approach	IAM lead	Pass/fail
AI-04	The solution should provide traceable source references for generated answers.	Should	Demonstration using client-supplied test cases	AI product owner	Weighted score
IT-08	The platform could automate low-risk fulfilment workflows without custom code.	Could	Live demonstration and two comparable references	Service owner	Differentiator
SCP-01	Autonomous production changes are out of scope for this phase.	Won't	Provider acknowledgement	Change manager	Not scored
[ID]	[Atomic requirement]	[Tier]	[Document, demo, test, reference or contract commitment]	[Role]	[Method]
[ID]					
[ID]					
[ID]					
[ID]					
[ID]					
[ID]					

Recommended coding: domain abbreviation + sequence (for example, SEC-01, AI-04, COM-03). Keep a separate change log if requirements are amended after issue.

4. Provider response and evidence schedule

Require every provider to answer in the same structure. Marketing collateral may be supplied as supporting material, but it must not replace the response schedule.

Response field	Provider instruction
Compliance	Select Comply / Partially comply / Does not comply / Not applicable.
Response	Explain how the proposed solution meets the requirement in the offered scope.
Evidence	Identify the attached document, contract commitment, demonstration, test result or reference.
Dependency	State client actions, third parties, licences, data, access or assumptions required.
Delivery timing	State whether available at contract start, during implementation or on a committed roadmap.
Commercial impact	Identify included cost, optional cost or pricing dependency.
Exception	Describe any qualification, workaround, limitation or contractual exclusion.

Evidence strength scale

Level	Evidence	Evaluation meaning
0	No answer or unsupported assertion	No usable evidence
1	Roadmap, intention or general collateral	Material uncertainty
2	Documented capability with limited applicability evidence	Some support; material gaps remain
3	Relevant documentation plus a credible demonstration or artefact	Adequate evidence
4	Client-specific test, contract commitment or closely comparable reference	Strong evidence
5	Independently verifiable evidence across the offered service and operating model	Exceptional confidence

RULE Score what is evidenced in the offered scope. Do not score a capability that exists only in another edition, future roadmap or unpriced service tier.

5. Evaluation criteria and scoring

Approve weights and disqualification rules before responses are opened. Keep the scale behavioural so panel members can explain why a score was assigned.

Score	Descriptor	Behavioural anchor
0	No response	No usable answer or evidence.
1	Materially deficient	Fails most of the criterion or introduces unacceptable risk.
2	Partially meets	Some capability, but meaningful gaps or weak evidence remain.
3	Meets	Satisfies the criterion with adequate evidence and manageable risk.
4	Exceeds	Provides relevant additional value with strong evidence.
5	Exceptional	Materially strengthens the outcome with highly credible evidence.

WEIGHTED FORMULA Weighted result = (moderated score / 5) x criterion weight. Keep pass/fail Must requirements outside the weighted total unless policy requires otherwise.

Illustrative weighting

Criterion	Weight	Provider A	Provider B	Moderation note
Outcome and functional fit	25%			
Security, privacy and risk	20%			
Implementation and operating model	15%			
Evidence and referenceability	10%			
Commercial and whole-of-life value	20%			
Provider viability and strategic fit	10%			
TOTAL	100%			

5.1 Moderation and decision controls

Individual scoring

- Each evaluator scores only the criteria assigned to their expertise.
- Scores are recorded before the moderation meeting.
- Every score includes a short evidence-based rationale and a source reference.
- Material uncertainty is recorded as a question, assumption or risk - not silently resolved in the provider's favour.

Moderation

- Discuss the evidence and scoring anchor, not the arithmetic average.
- Record why a moderated score differs from an evaluator's original score.
- Do not change weights after seeing which provider benefits.
- Record Must exceptions separately, with an owner, risk acceptance and contractual treatment.

Clarification log

Ref	Provider	Question	Response	Decision impact	Closed by/date
CL-01					
CL-02					
CL-03					
CL-04					

Risk and exception log

Ref	Gap / risk	Likelihood	Impact	Treatment	Owner	Residual rating
R-01						
R-02						
R-03						

6. Commercial response schedule

Require one whole-of-life pricing basis. Do not accept a single headline figure if material implementation, consumption, integration, support, data, exit or indexation costs sit outside it.

Cost category	Year 1	Year 2	Year 3	One-off	Assumption / unit
Subscription / licence					
Implementation and migration					
Integration and configuration					
Data ingestion, storage or egress					
Managed service / support					
Training and change					
Required third-party products					
Exit, extraction and transition					
TOTAL excluding GST					

Commercial declarations

- [Provider to state] Pricing currency, GST treatment and validity period
- [Provider to state] Minimum commitments, volume bands and overage rates
- [Provider to state] Indexation basis, timing and cap
- [Provider to state] Included and excluded environments, users, data and service hours
- [Provider to state] Payment milestones and acceptance dependencies
- [Provider to state] Renewal, termination, data return and transition charges
- [Provider to state] Third-party pass-through costs and foreign-exchange exposure
- [Provider to state] Assumptions that would trigger a change request or repricing

6.1 Vendor due diligence question bank

Select the questions that are proportionate to the risk. Require an answer, evidence reference, exception and owner for any remediation commitment.

Corporate, financial and supply-chain

- Identify the contracting entity, ownership structure, material subcontractors and service locations.
- Provide evidence of financial capacity proportionate to the contract term and implementation dependency.
- Disclose material litigation, regulatory action, insolvency events or control changes relevant to delivery.
- Describe subcontractor selection, assurance, concentration risk and notification controls.
- Provide certificates of currency for required insurance and state material exclusions.

Security, privacy and resilience

- Describe the security governance model, independent assurance and remediation of findings.
- State data locations, cross-border disclosures, subprocessors and change-notification process.
- Explain identity, privileged access, encryption, logging, vulnerability and secure-development controls.
- State incident notification commitments, cooperation model and access to evidence.
- Provide recovery objectives, resilience test evidence and service-continuity dependencies.
- Describe data extraction, deletion verification and transition support at exit.

Delivery and service management

- Identify named delivery roles, location, capacity assumptions and use of subcontractors.
- Provide the implementation plan, critical path, client dependencies and acceptance gates.
- Define service levels, exclusions, service credits, escalation and chronic-failure treatment.
- Provide two references with comparable scale, complexity and regulated operating context.

6.2 AI-specific due diligence

Use this module when the proposed capability trains, fine-tunes, retrieves, classifies, recommends or generates outputs using AI.

- Identify all models used, their providers, hosting locations, update mechanisms and material dependencies.
- State whether client inputs, outputs, feedback or metadata are used to train or improve any model, and how this is controlled contractually.
- Describe provenance, licensing and permitted use of training, fine-tuning and retrieval data where relevant.
- Explain testing for accuracy, harmful outputs, bias, security abuse, privacy leakage and task-specific failure modes.
- Provide evaluation results for the proposed use case, not only generic model benchmarks.
- Describe human review, override, escalation and contestability for consequential outputs.
- State how model, prompt, guardrail and data changes are versioned, tested, communicated and reversible.
- Describe monitoring for drift, degraded performance, cost volatility, misuse and material incidents.
- Explain recordkeeping sufficient to reconstruct a material output and its supporting sources where required.
- Provide exit options if a foundation model, hosting region or third-party service becomes unavailable or unacceptable.

AUSTRALIAN CONTEXT Map questions and contract treatment to your organisation's privacy obligations, risk appetite and sector requirements. For AI governance, align the operating model to Australia's Guidance for AI Adoption and any applicable regulatory obligations.

7. Process, timeline and decision record

7.1 Indicative procurement timeline

Stage	Owner	Target date	Output / gate
Requirements approval			Approved scope, MoSCoW register and criteria
RFP issue			Controlled release and acknowledgement
Clarification window			Shared clarification log
Response deadline			Complete responses locked
Conformance review			Must gaps and exclusions identified
Individual evaluation			Scores and rationales recorded
Demonstrations / tests			Scripted evidence captured
Moderation			Moderated scores and risk log
Commercial / contract			Comparable offer and agreed departures
Approval and notification			Signed decision record and communications

7.2 Demonstration and proof-of-value controls

- Issue the same scenario, data assumptions and time limit to each provider.
- Use client-relevant tasks and exception conditions, not a provider-led product tour.
- Record which features are standard, configured, custom, simulated or roadmap.
- Score evidence against pre-approved criteria; do not add novelty points during the session.
- Capture dependencies, limitations, unanswered questions and commercial implications.

Worked example A: cybersecurity procurement

Scenario: an organisation is evaluating a managed detection and response service across a hybrid Microsoft, cloud and operational environment.

Tier	Example requirement	Evidence request	Evaluation treatment
Must	Provide 24x7 triage and escalation for agreed severity-one events within the contracted service boundary.	Redacted incident timeline, SLA wording and staffing model	Pass/fail plus risk review
Must	Support phishing-resistant MFA for all provider privileged access into client systems.	Configuration evidence and access-control procedure	Pass/fail
Should	Enrich detections with threat intelligence relevant to the organisation's Australian operating context.	Three examples showing source, action and analyst value	Weighted score
Could	Provide co-managed threat hunting workspaces for the internal security team.	Live demonstration and licence impact	Differentiator
Won't	Full security operations centre replacement is not in scope.	Acknowledgement and scope boundary	Not scored

Questions that expose delivery risk

- Which telemetry sources are included in the base fee, and which require additional engineering or ingestion charges?
- What actions can analysts take without client approval, and how is authority controlled?
- Show the escalation path when the assigned team cannot determine severity within the target time.
- Which parts of the service depend on subcontractors or offshore delivery locations?
- How will detection content, cases, evidence and configurations be returned at exit?

Worked example B: enterprise AI procurement

Scenario: an organisation is selecting a generative AI assistant for staff to retrieve and draft from internal knowledge sources.

Tier	Example requirement	Evidence request	Evaluation treatment
Must	Client content, prompts and outputs must not be used to train a shared model without explicit written approval.	Contract clause, architecture and configuration evidence	Pass/fail
Must	Access to retrieved content must inherit the source system's user permissions.	Client-scripted test using users with different entitlements	Pass/fail
Should	Generated answers should show traceable source references at passage level.	Demonstration using supplied ambiguous and conflicting sources	Weighted score
Could	Teams could configure approved task-specific assistants without code.	Governance workflow demonstration and cost impact	Differentiator
Won't	Autonomous external communications are excluded from this phase.	Acknowledgement and control boundary	Not scored

Questions that expose AI risk

- Which model and model version will serve the proposed workload, and what changes can occur without client approval?
- Show measured performance on the organisation's representative tasks, including failure cases.
- How can an administrator investigate a harmful, inaccurate or unauthorised output?
- What is the cost impact of retrieval volume, token consumption, model changes and retention?
- How does the client export prompts, evaluation sets, configurations and audit evidence at exit?

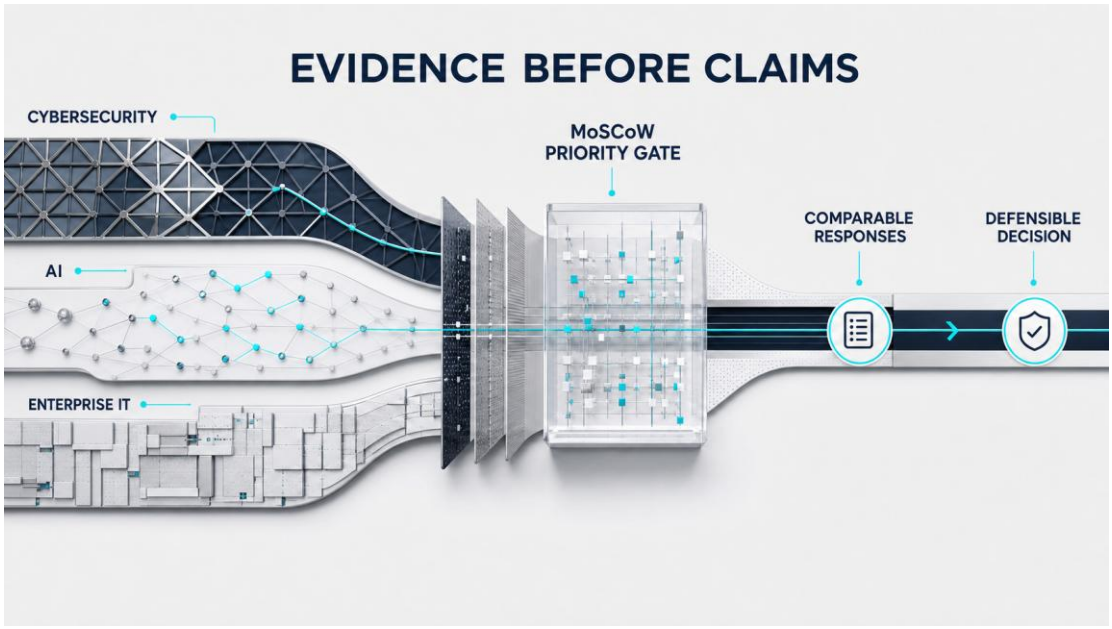
Worked example C: enterprise IT procurement

Scenario: an organisation is selecting an IT service management platform to replace a heavily customised legacy environment.

Tier	Example requirement	Evidence request	Evaluation treatment
Must	Support SSO, automated user lifecycle and role-based administration through the organisation's identity platform.	Configuration demonstration and implementation design	Pass/fail
Must	Migrate agreed active and historical records with reconciled counts and an auditable exception report.	Migration method, sample reconciliation and acceptance plan	Pass/fail
Should	Support low-code workflow design with governed promotion between environments.	Build a supplied workflow and show change controls	Weighted score
Could	Provide native service-cost modelling for selected business services.	Demonstration and licence impact	Differentiator
Won't	Re-creation of every legacy customisation is excluded.	Acknowledgement and rationalisation approach	Not scored

Questions that expose implementation risk

- Which outcomes rely on configuration, custom code, marketplace products or professional services?
- Show how a governed workflow moves from design to test and production, including rollback.
- What data will not migrate cleanly, and how will exceptions be priced and accepted?
- Which integrations are included, and who owns changes when upstream APIs change?
- What capabilities or data become inaccessible when the subscription ends?



Decision record

Decision field	Approved record
Selected provider	
Approved scope and term	
Total evaluated cost	
Highest-ranked alternative	
Material Must exceptions	
Accepted residual risks	
Key negotiated protections	
Conditions before signature	
Decision rationale	

Approvals

Role	Name	Decision	Date
Executive sponsor		Approve / decline	
Procurement		Approve / decline	
Security / risk		Approve / conditions	
Legal / privacy		Approve / conditions	
Financial delegate		Approve / decline	

Run the process with CYBORIUM

The template gives your team a disciplined starting point. CYBORIUM can help define the requirement, map the market, run the evaluation, test evidence, benchmark commercials and support negotiation through to a clear, defensible decision.

ZERO FEE TO THE CLIENT If a provider is selected, that provider pays CYBORIUM a capped fee. Your organisation contracts directly with the provider and retains control of the decision. CYBORIUM remains independent and vendor-neutral.

CYBORIUM does not sell, deliver, operate or invoice technology.

Request a consultation: https://cyborium.com.au/contact-us/

Related frameworks

MoSCoW Requirements: A Practical Framework for Enterprise Technology Procurement
https://cyborium.com.au/moscow-requirements-a-practical-framework-for-enterprise-technology-procurement/

Cybersecurity Vendor Evaluation Framework
https://cyborium.com.au/cybersecurity-vendor-evaluation-framework-a-practical-guide-for-enterprise-buyers/

Enterprise AI Vendor Selection Criteria
https://cyborium.com.au/enterprise-ai-vendor-selection-criteria-a-practical-framework-for-australian-buyers/