Procuring Trusted Cyber Security Services

A practical guide for organisations in Australia and New Zealand

CREST

Table of Contents

Introduction

Organisations across Australia and New Zealand face increasing pressure to select trusted partners for cyber security services.

Whether engaging providers for penetration testing, red teaming, threat intelligence, incident response, or Security Operations Centre (SOC) services, the consequences of poor supplier selection can be significant ranging from unmanaged risk and operational disruption to reputational damage and regulatory exposure.

This guide outlines best practice procurement considerations for cyber security services and highlights how independent accreditation and certification frameworks such as those provided by CREST (International) can be used as objective assurance mechanisms.

It is designed to support organisations across government, critical infrastructure, enterprise, and not-for-profit sectors when procuring cyber security services.

Core Principles of Effective Cyber Security Procurement

When selecting cyber security providers, organisations should prioritise those that can demonstrate:

- ✓ Documented and repeatable methodologies
- ✓ Clear reporting, remediation, and retesting processes
- ✓ Delivery of actionable, intelligence-led outputs
- ✓ Tested incident response capabilities and readiness
- ✓ Well-defined monitoring, escalation, and communication frameworks
- ✓ Strong governance, data protection, and ethical practices

Independent validation of these capabilities provides confidence that services will be delivered consistently and effectively.

Why Independent Accreditation Matters

Cyber security services are complex and often difficult to evaluate based on marketing claims alone. Independent accreditation and professional certification provide a structured and objective way to assess:

- ✓ Technical capability
- ✓ Operational maturity
- ✓ Governance and oversight
- ✓ Quality and consistency of service delivery

By requiring independent, third-party validation, organisations can reduce procurement risk and ensure alignment with recognised industry standards.

Why Choose a CREST (International) Accredited Provider

CREST (International) is a globally recognised, not-for-profit accreditation and certification body for the cyber security industry. Engaging a CREST (International) Member company provides organisations with confidence that services are delivered to a high and independently validated standard.

Global Assurance Benchmark

CREST (International) is recognised by governments, regulators, and enterprises worldwide as a benchmark for cyber security assurance, supporting national initiatives in jurisdictions including Australia, Singapore, the United Kingdom, and the United Arab Emirates.

Independent Company Accreditation

Member companies undergo rigorous, independent assessment of business processes, governance, data security practices, and service delivery capability.

Validated Professional Competence

CREST (International) verifies that individuals delivering services have appropriate skills, experience, and certifications, with work reviewed and overseen by qualified professionals.

Ongoing Compliance and Assurance

Members are subject to continual reassessment, ensuring standards remain current and aligned with evolving threats.

Ethics and Accountability

All Member companies adhere to enforceable Codes of Conduct and are subject to formal complaints and resolution processes.

Engaging CREST (International) Members enables organisations to demonstrate due diligence and align procurement with internationally recognised best practice.

Important Clarification: CREST Australia New Zealand Ltd (“CREST ANZ”)

CREST ANZ operates as a separate organisation and does not deliver CREST (International) accreditation or certification frameworks. The formal relationship between CREST (International) and CREST ANZ ended in April 2019 and for the avoidance of doubt, CREST ANZ has no rights to the CREST International suite of company accreditations or individual certifications.

CREST ANZ has not adopted our Accreditation Standards and therefore CREST ANZ membership alone is not recognised by CREST International as being equivalent.

CREST (International) accreditation and certification are distinct and independently governed, with specific standards, assessment processes, and global recognition.

Recommendation for Buyers

When procuring cyber security services, organisations should explicitly require providers to be CREST (International) Member companies and ensure that services are delivered by CREST (International) certified professionals.

Procurement Guidance by Discipline

When selecting providers, organisations should prioritise those that demonstrate independently validated capability, structured methodologies, and accountable service delivery.

Penetration Testing and / or Red Teaming

- ✓ Providers should be CREST (International) accredited Member companies with penetration testing or red team accreditations
- ✓ Engagement teams should include CREST (International) certified professionals or equivalent
- ✓ Request evidence of methodologies, reporting standards, and retesting processes

Security Operations Centres (SOC)

- ✓ Providers should have CREST (International) accredited SOC capabilities
- ✓ Analysts should hold relevant SOC certifications
- ✓ Demand clarity on monitoring scope, escalation processes, and integration with internal teams

Threat Intelligence

- ✓ Providers should hold CREST (International) Threat Intelligence accreditation
- ✓ Analysts should hold relevant CREST (International) certifications or equivalent
- ✓ Ensure delivery of actionable intelligence, transparency of sources, and integration with security operations

Incident Response

- ✓ Providers should be CREST (International) accredited in Incident Response
- ✓ Teams should include CREST (International) certified incident responders or equivalent
- ✓ Require evidence of 24/7 capability, tested playbooks, and forensic readiness

Checklist for Procuring Cyber Security Providers

When evaluating potential providers, organisations should ask:

- ✓ Is the organisation a current CREST (International) Member for the relevant service(s)?
- ✓ Can they demonstrate that personnel hold current CREST (International) certifications or equivalent?
- ✓ How do they maintain skills, training, and alignment with evolving threats?
- ✓ What delivery methodologies are used, and how are they benchmarked against recognised standards?
- ✓ What governance controls ensure confidentiality, independence, and ethical conduct?

By prioritising independently accredited providers, organisations can reduce risk and demonstrate due diligence to stakeholders, regulators, and customers.

Finding a CREST (International) Provider

To support organisations in identifying suitable providers, CREST (International) has launched the CREST Marketplace. See here: **https://marketplace.crest.org/suppliers**

The Marketplace enables buyers to search for accredited Member companies by service, capability, and region, helping organisations quickly identify providers that meet CREST's internationally recognised standards.

Recommended Request for Tender (RFT) or Request for Proposal (RFP) Wording

To align procurement with best practice, the following wording is recommended:

"The supplier must be a current CREST (International) Member company for the relevant services (red team testing, penetration testing, threat intelligence, incident response, or security operations centre).

All personnel engaged in delivering the services should hold appropriate CREST professional certifications or equivalent.

Evidence of company accreditation and individual certifications must be provided with the tender submission.

Submissions that do not meet these requirements may be deemed noncompliant."

About CREST (International)

With more than 500 accredited Member companies globally, including a growing presence across Australia and New Zealand, CREST (International) plays a key role in strengthening cyber security capability and assurance.

CREST is an international not-for-profit membership body representing the global cyber security industry. Since 2006, we have been leading the cyber security community to collectively raise the standards of cyber service providers and professionals, quality assuring the sector and in turn providing confidence to the buying community, government and regulators.

Useful links for the CREST (International) Website

http://www.crest-approved.org/

CREST Accreditation Pathway:

https://www.crest-approved.org/membership/crest-accreditation-pathway/

CREST Accreditation Standards:

https://www.crest-approved.org/membership/accreditation-standards/

CREST Certifications and Exams:

https://www.crest-approved.org/skills-certifications-careers/about-crest-exams/

CREST Member Marketplace:

https://marketplace.crest.org/suppliers/

CREST Australasia Council:

https://www.crest-approved.org/membership/region-australasia/

www.crest-approved.org