IRAP: Raising The Bar

Setting a new standard for operational sovereignty

AC3

Contents

Foreword

Public and regulated organisations face a growing challenge: how to modernise critical operations without surrendering control. The push to outsource infrastructure and security functions may offer efficiencies, but it often raises tough questions about governance, data ownership, and accountability.

This is especially true when those operations involve sensitive workloads, regulated information, or cross-border dependencies. Relying on generic assurances or broad claims of “security " is no longer enough. Decision-makers need a clear line of sight into how their services are governed and whether the controls in place stand up to scrutiny.

That’s where the value of an IRAP assessment becomes clear. The Information Security Registered Assessors Program (IRAP), governed by the Australian Signals Directorate (ASD), provides a formal mechanism to assess how well a service aligns with the requirements of the Information Security Manual (ISM), the national baseline for security and governance of government systems and data.

AC3 has extended this rigour across two critical service domains: our Security Operations Centre (SOC) and our managed Cloud environment. Both have been independently assessed by an ASD-endorsed IRAP assessor to PROTECTED level, giving our customers the flexibility to adopt either or both, depending on their needs.

This isn’t just about meeting compliance requirements. It’s about enabling organisations to operate with assurance, knowing that their systems are protected, monitored, and aligned to the expectations of Australia’s most security-conscious institutions.

Operational sovereignty is the goal. To retain control, gain transparency, and operate with confidence, even in the most sensitive or regulated environments. IRAP is one way to prove it, and AC3 is committed to helping customers achieve it.

WHY ORGANISATIONS ARE DEMANDING MORE THAN PROMISES WHEN IT COMES TO SECURITY AND CONTROL

1 The Confidence Gap

Trust in digital infrastructure has become more fragile than ever. Whether through increasing regulation, public scrutiny, or the complexity of hybrid environments, organisations are finding that vague reassurances are no longer enough.

What's missing isn't just technology, it's clarity. Who is responsible when something goes wrong? How are systems monitored, governed, and protected? What can be proven when it matters most?

This confidence gap shows up in a variety of ways. IT leaders unsure of whether their Cloud provider can meet IRAP requirements. Security teams trying to align response practices with internal policies. Procurement and legal teams struggling to assess whether third-party environments can meet their contractual or regulatory obligations.

And when providers handle sensitive data or deliver essential services, these uncertainties become unacceptable. Organisations need confidence in how those services are structured, operated, and verified.

That's where IRAP assessments become a differentiator. Unlike generic security claims, an IRAP assessment provides a structured, third-party audit aligned to the Australian Government's most rigorous standard: the Australian Signals Directorate (ASD) Information Security Manual (ISM).

AC3 has completed this assessment across two core offerings: our Security Operations Centre (SOC) and our independently designed and built managed Cloud platform.

Both have been assessed to PROTECTED level, giving our customers the ability to select services with a known level of assurance, based on their operational and compliance needs.

This dual offering supports a key strategic goal for our customers - operational sovereignty. It means retaining oversight and control, even when leveraging external expertise. It means being able to prove governance and assurance, not just claim it. And it means choosing infrastructure and security services that align with national expectations, not just market trends.

In short, it's about regaining clarity over risk, over responsibility, and over what "secure" really means in practice.

Top Emerging Security Pressures

(Gartner Top Trends in Cyber Security Survey, 2025)

- The continued emergence of GenAI use cases (and risks)
- Burnout as a result of the continued gap between security-talent supply and demand
- Relentless growth in cloud adoption, which is altering the composition of digital ecosystems
- Increasing regulatory obligations and government oversight of cyber security, privacy and data localisation
- Continued decentralisation of digital capabilities across enterprises
- Demand for business stability and security in a constantly evolving threat environment

UNDERSTANDING THE FRAMEWORK BEHIND ONE OF AUSTRALIA'S MOST TRUSTED BENCHMARKS

2

Behind the Acronym

What is IRAP and why does it matter?

The Information Security Registered Assessors Program (IRAP) is a framework governed by the ASD to assess the security posture of services handling sensitive data. It's not a certification, but a structured, independent review to determine how well a system or service aligns with the ISM.

For customers, an IRAP assessment provides credible insight into a provider's security maturity. It shows whether a service has the right controls in place to protect data, manage risks, and operate with a strong security baseline.

What does it mean to be IRAP assessed to PROTECTED level?

This means that an IRAP assessor has independently evaluated a service and confirmed that its people, processes, and technologies are appropriate for handling information classified up to PROTECTED level - a common requirement for government agencies and other regulated sectors.

Being IRAP-assessed at PROTECTED level gives commercial and public sector customers confidence that the provider aligns with a trusted national standard.

What does an IRAP assessment involve?

An IRAP assessment isn't a checkbox exercise. It involves a deep technical and procedural audit by an ASD-endorsed assessor, covering:

- Security architecture and infrastructure
- Operational processes, monitoring, and incident responses
- Physical and personnel security
- Data handling, access control, and encryption
- Logging, reporting, and governance structures

The assessor documents their findings in a comprehensive report, which includes consumer guidance, a summary of ISM controls and recommendations for improvement. The process is rigorous and aligned with real-world risk management.

> For customers, an IRAP assessment provides credible insight into a provider's security maturity. It shows whether a service has the right controls in place to protect data, manage risks, and operate with a strong security baseline.

How is IRAP different from other security assessments?

IRAP assessments are independently performed by ASD-endorsed individuals, based on a nationally recognised framework (the ASD ISM), and tailored to the assessed environment.

Unlike broad international certifications, IRAP:

- Is designed for Australian threat conditions
- Ties directly into government-grade security expectations
- Covers physical, personnel, and system-level controls
- Requires documented evidence and assessor verification

It's a more comprehensive and relevant benchmark for Australian organisations looking for superior cyber assurance.

WHY SOVEREIGNTY AND ASSURANCE ARE NOW BOARDROOM ISSUES

3 An Executive View

THE RISING DEMAND FOR PROOF

Across boardrooms and executive teams, one question is surfacing with increasing frequency: How do we know we're truly in control?

Leaders are being held accountable for the governance of critical systems, even when day-to-day management is outsourced. Inquiries from regulators, customers, and partners demand visibility and evidence that many organisations still struggle to produce.

This shift isn't confined to security incidents. It extends to the location of data, the integrity of Cloud platforms, and the governance of security operations.

Executives are expected to answer:

- Can you prove your provider's services meets a recognised benchmark?
- Do you know where your sensitive data is stored and processed?
- Is your incident response framework aligned with your own policies and obligations?
- How are you assured that changes to your systems are authorised, logged, and auditable?

WHY VERBAL ASSURANCE FALLS SHORT

When the answers to these questions rely on informal assurances, trust erodes quickly. Stakeholders want evidence - documented, independent, and defensible. Without it, even capable providers leave their customers exposed to doubt and scrutiny.

An IRAP assessment fills that gap. It's a formal, independent review of whether a service meets the requirements of the ISM. AC3's SOC and managed Cloud services have each been independently assessed to operate at PROTECTED level, giving customers verified proof of their provider's operational integrity.

Operational risk doesn't only arise from external threats. It can stem from unclear ownership of controls, poorly documented processes, or assumptions about how a provider operates. Independent IRAP assessment verifies that the right controls are in place, that responsibilities are clearly defined, and that the operational environment supports the level of assurance your organisation needs - before you find out the hard way that it doesn't.

EXECUTIVE PRIORITIES ADDRESSED

For executives, an independent IRAP assessment matters for a number of reasons:

Strengthening governance:
An IRAP-assessed SOC or Cloud service provides clear evidence of operational maturity, control frameworks, and adherence to a recognised benchmark.

Supporting accountability:
Regulatory and contractual obligations can be met with evidence, not just assurances, reducing both legal and reputational risk.

Enhancing transparency:
Independent assessment makes it clear where responsibilities lie - both within your organisation and with your provider - helping eliminate operational blind spots.

Reducing decision risk:
Knowing a service has been assessed to PROTECTED level gives boards and executives greater confidence in procurement and investment decisions.

Underpinning sovereignty:
Even in outsourced or hybrid models, you retain decision-making power and visibility over systems, data, and risk posture. The provider delivers capability, but you maintain control.

#1 Cyber security ranks as the number one concern for board executives.

71% of organisations don't conduct due diligence on their key suppliers' cyber security practices.

75% of organisations don't require mandatory reporting of cyber or data breaches affecting their suppliers.

Source: 2024 McGrathNicol 'Risk & Security Report' survey of over 300 C-Suite and board-level directors.

REDUCING REGULATORY EXPOSURE

For boards and executives, IRAP assessment is an operational milestone, not a technical one. It demonstrates that sovereignty, governance, and accountability are actively maintained, not assumed. It provides assurance that the assessed environment has been built and is being run in a way that supports your obligations, aligns with national standards, and can withstand external scrutiny.

This distinction is critical. Technology investments may change, platforms may evolve, and contracts may be renewed or replaced, but the requirement for demonstrable control over your systems and data remains constant. An IRAP-assessed SOC or Cloud service becomes part of your organisation's capability to meet that requirement, rather than a one-off compliance exercise.

It also changes the nature of conversations in the boardroom. Instead of debating whether a provider can be trusted, the discussion shifts to how best to leverage the capabilities of a service that has already been independently validated. That frees leadership teams to focus on strategic priorities - knowing that the foundation is solid, tested, and aligned with the highest expectations in the country.

In a climate where operational resilience is under greater scrutiny than ever, the organisations that can evidence their control over critical systems are already ahead of the curve. Whether through AC3's IRAP-assessed SOC, IRAP-assessed managed Cloud, or both, the result is the same: a service environment that meets the highest national standard, and proof that you are operating with authority over your most critical assets.

HOW IRAP ASSESSMENT SIGNALS OPERATIONAL MATURITY AND BUILDS CONFIDENCE BEYOND COMPLIANCE

4 Raising the Standard

An IRAP assessment doesn't just raise the bar technically, it creates a new standard of accountability.
A standard that's visible, defensible, and capable of building trust in ways traditional outsourcing simply can't.

For years, the standard approach to selecting and evaluating providers was to review their security documentation, confirm they adhered to common frameworks, and take them at their word. That's no longer enough. The bar for trust has moved, and independent validation has become the expectation, not the exception.

An IRAP assessment represents a step-change in how assurance is demonstrated. It's not an internal audit or a vendor self-attestation. It's an independent, ASD-governed process that evaluates a provider's environment against the controls in the ASD ISM. The outcome is a clear, evidence-backed report of whether the service can operate at a specific classification level.

AC3 has taken this process further by applying it to two distinct service areas. Our SOC has been IRAP-assessed to PROTECTED level, validating the maturity of our monitoring, incident response, operational controls, and personnel.

Separately, our purpose-built managed Cloud environment has also been assessed to PROTECTED level, confirming that the platform meets the highest expectations for governance, data handling, and operational security.

This matters because not all providers can demonstrate the same depth of assurance across these individual domains, and fewer still can do so independently for both services. By having both SOC and Cloud services IRAP-assessed as stand-alone environments, AC3 gives customers the freedom to choose what they need, without compromising on the level of assurance they expect.

For customers in government and highly regulated industries, this means procurement decisions can be backed by verifiable evidence rather than subjective risk assessments. For other organisations, it signals a level of discipline that strengthens trust with partners, customers, and stakeholders.

In practice, an IRAP assessment to PROTECTED level sets a new benchmark. It shows that a provider is not only capable of delivering secure services but is also willing to open their operations to independent scrutiny and meet the highest standards. This is the foundation of operational sovereignty: knowing that the systems you rely on are controlled, governed, and proven to meet the most rigorous national requirements.

TURNING INDEPENDENT ASSESSMENT INTO OPERATIONAL ADVANTAGE

5

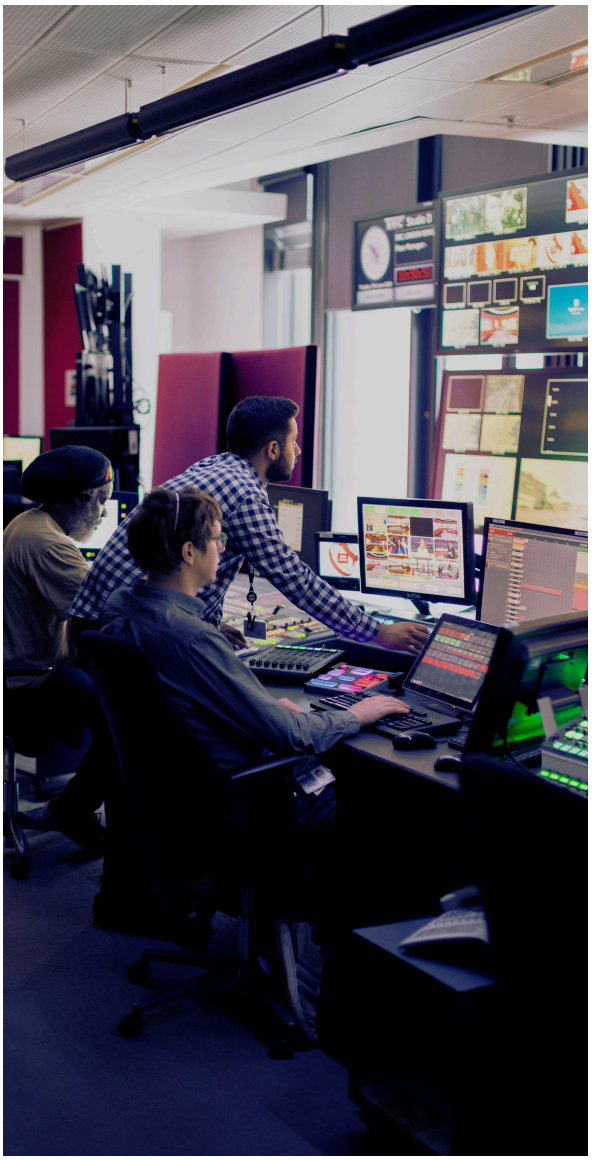
How AC3 Delivers

An IRAP assessment is a milestone. But it's what happens after the assessment that defines its real value. At AC3, the focus is on embedding the same discipline, governance, and transparency demonstrated in our IRAP-assessed SOC and Cloud services into the everyday experience of our customers.

Two independently assessed services, built for assurance
AC3's Security Operations Centre (SOC) operates 24/7, providing continuous monitoring, incident detection, and response aligned with the controls required for PROTECTED-level environments. Separately, our secure Cloud platform delivers the same standard of governance and protection for workloads that require the highest degree of control and data security. Each has been independently IRAP-assessed, allowing customers to adopt the service that fits their needs, or combine them for a fully assured technology stack.

Operational sovereignty at the core
Every design choice, process, and service integration is shaped to give customers visibility and control over their environment. This means clarity of where data is stored, how it is accessed, and how operational changes are approved and documented. It also means that customers retain ownership over decision-making, while AC3 handles the complexity of maintaining secure, compliant operations.

Integration without compromise
Whether your organisation is migrating sensitive workloads to the Cloud or engaging a managed SOC to strengthen cyber security resilience, integration is handled without diluting the assurance provided by the IRAP assessment. Controls are maintained consistently across platforms, and reporting is structured to meet both regulatory requirements and internal governance needs.



A partnership built on evidence
Because both the SOC and Cloud services have been assessed to PROTECTED level, every engagement begins with a baseline of proven capability. This foundation allows AC3 to work with customers on higher-value objectives, optimising workflows, improving incident response times, or enabling secure innovation, without having to first address gaps in governance or operational maturity.

More than compliance - a lasting capability
The true benefit of working with AC3 is not just passing an audit or meeting a contractual requirement. It's building a lasting capability that supports both compliance and agility. By aligning with the highest standards and maintaining that alignment over time, AC3 enables customers to operate with confidence, knowing their services have been tested, validated, and are continually upheld to the same benchmark.

Raising the bar means choosing services that have been assessed, not assumed.

Leaders need to know their organisation is prepared.
Not hypothetically, not aspirationally, but demonstrably.

That means being able to stand behind your operations when they're tested. To show where data is stored, how systems are governed, the actions taken, and to know that those decisions and controls meet a recognised national benchmark.

Trust is built on evidence. Confidence comes from discipline. And resilience depends on services that hold firm when it matters most.

These are the signals that separate assurance from assumption, and they're becoming the standard by which all critical operations will be judged.

The question is no longer whether to raise the bar. It's how high, how soon, and who you can trust to help you get there.

AC3

Get in touch today:

1300 223 999 I www.ac3.com.au

0800 258 773 | www.ac3.co.nz