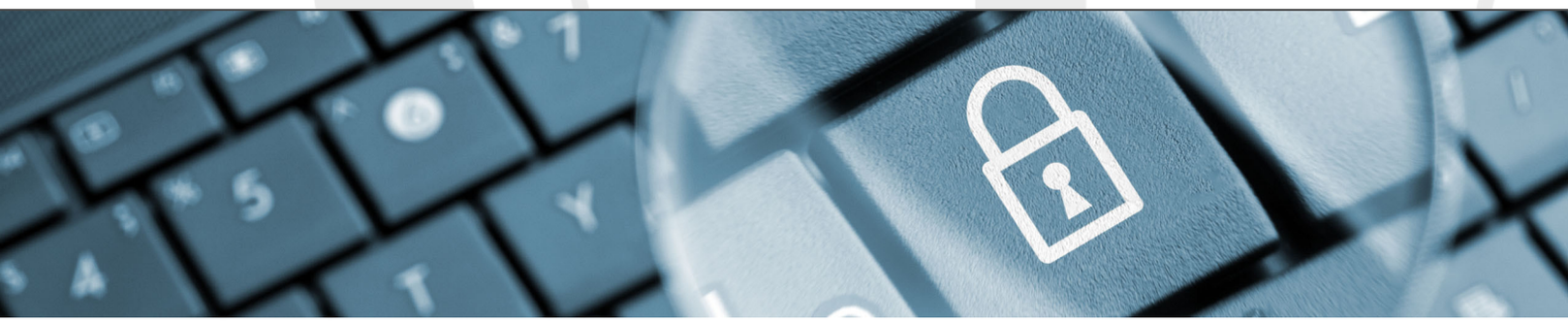
dotSec
dot com security

# Customer Case Study: Information Security Registered Assessors Program (IRAP) services and certification



## Background and Challenges

Our client, being a multinational service-provider for the Australian Government, must comply with the Australian Government's requirements for protective security and standardised information security practices.

Our client is an established government service provider and so already had an understanding of the value of the information that it managed, and of the importance of information security to the business' ongoing operations and reputation. Our client was not however familiar with the kind of formalised, system-oriented information security accreditation framework that is required in order to meet Australian Government standards.

DotSec's main challenge was to define and execute a collaborative program of work that would transform our client's systems, processes and governance arrangements into a state where they would be certified as compliant with the government's information security requirements.

### Executive Summary

#### Business challenge

Develop an IRAP-compliant information security management system for a multinational service-provider, on a tight schedule and fixed budget.

#### Solution

The business engaged DotSec as IRAP compliance specialists to prioritise, plan and guide the implementation of a complex set of information security controls.

#### Results

The project was successful and consequently, our client met their compliance requirements and gained an edge over their competitors. Our client continues to grow their business by successfully bidding for further Australian Government contracts that require IRAP compliance.

Additional challenges included the need for  our client to get clarification regarding the nature of the government requirements in some areas. The government-provided Statement of Applicability (SOA) is a subset of the full Information Security Manual (ISM) and Protective Security Policy Framework (PSPF). Some areas of inconsistency or confusion became apparent over the course of the project, and DotSec worked to get clarity on behalf of our client.

Finally, the transformational program of work presented significant coordination and management challenges, particularly the need to meet government deadlines and milestones, while also meeting our client's budget and resourcing constraints.

## The Solution

DotSec met these challenge in a number of steps.

First, DotSec defined and managed a gap analysis project to identify areas of non-compliance with the set of controls the department had specified in its Statement of Applicability (SOA). The gap analysis report was submitted to the federal government for review and acceptance.

DotSec presented the SOWs as part of an over-arching project proposal to the company board and executive, and provided detailed explanation in response to a range of technical and budgetary questions.

DotSec addressed challenges relating to the consistency and applicability of the SOA by liaising with the federal government department, seeking clarification, managing risk and assisting our client to understand when, how and why the various controls included in the department-provided SOA were to be implemented.

DotSec was able to assist in these situations, relying on our practical information security expertise, understanding of the ISM and PSPF, and ability to present and discuss issues with both the government department and the client.

Finally, DotSec addressed budget and resource challenges by managing and executing the project, providing expert information security consultancy and project management services over a period of 18 months.  The project successfully addressed the identified gaps and the client was able to implement the required security controls within time and budget constraints.

A subsequent audit confirmed the client's security-control compliance, and resulted in the government's acceptance of the final IRAP assessment report.

## The Outcomes

Detailed planning and careful task execution ensured that the project was successful across a range of business units, within the allocated time and cost, and within the constraints of the demanding day-to-day operational pace of the organisation.

Our client successfully complied  with over 400 controls from the Australian Government Protective Security Policy Framework (PSPF) and Information Security Manual (ISM). Such a far-reaching program required significant changes to all aspects of the organisation, from business-executive roles and responsibilities, through to changes in business practices, modifications to the organisation's IT and information security architecture, and implementation of technical and procedural controls.  DotSec guided the project to a successful outcome whereby these organisational changes were accepted and implemented.

DotSec designed an effective 18-month program of work that included gap-analysis, business-process analysis, information-architecture analysis, Statement Of Work definition, project management, risk management, specialist technical guidance, education and mentoring.  DotSec was able to assist the client with meeting the SOA requirements while also meeting aggressive and demanding new-business and business-as-usual goals.  The entire project was completed on time and on budget.

## Project Legacy

Our client has secured a number of significant outcomes from the project, and these outcomes will continue to benefit the client's business for years to come:

- DotSec's emphasis on developing a formal security risk-management framework and capability ensured that the client invested in ICT security initiatives and controls that actually reduced business risk.

- By implementing the controls that were defined in the SOA, our client was able to materially and significantly improve its organisational information security governance arrangements. The result has been an improvement in a range of business operations through standardised, integrated, effective processes.

- By clearly defining roles and responsibilities, our client improved accountability for safeguarding critical assets. In place of unstructured incident response procedures, the organisation has developed the capability to quickly detect, recover and learn from incidents and mistakes.

- With the help of DotSec's mentoring and guidance, the client has developed the internal capability of its infosec team, and is now better able to operate, maintain and improve its information security management system.

- Our client successfully addressed the IRAP compliance requirements in its Australian Government contract and has subsequently secured further contracts with similar requirements, confident that it had the necessary policies, processes and technologies already in place.

## The Next Steps

DotSec can provide you with experienced specialists who can guide your organisation through the challenging ISM and PSPF maze, and help your organisation to achieve its IRAP-compliance goals. Our expert infosec architects understand the challenges of the IRAP-compliance process.

We are experienced not just in the theory of compliance and assessment, but in the implementation of secure information systems (both in-house and hosted/cloud) for private and government organisations alike. Our experience, gained over 18 years, ensures that we are able to identify and implement security controls effectively and efficiently.


Australian Government

Get in contact with us now to discuss how improved information security governance can not only achieve your compliance goals, but can also increase customer trust, reduce operational uncertainty and add value to your business.

### IRAP

The Information Security Registered Assessors Program (IRAP) is an Australian Signals Directorate (ASD) initiative to provide high-quality information and communications technology (ICT) services to government in support of Australia's security. IRAP provides the framework to endorse individuals from the private and public sectors to provide security assessment services.

### ISM

The Information Security Manual or ISM is a standard that is produced by the Australian Government, and that governs the security of government (and government service-provider) ICT systems.

### PSPF

The Protective Security Policy Framework or PSPF is a structured collection of policies, protocols, standards and guidelines that identify personnel, physical and information-security requirements and outcomes.

## DO MORE BUSINESS, MORE SECURELY

https://www.dotsec.com/
+61 7 3221 2442
enquiries@dotsec.com

Level 2, 303 Adelaide St.
Brisbane. QLD. 4000