IRAP: What it Means – Why it Matters

Veritas Alta SaaS Protection assessed at the PROTECTED information classification level.

June 2023
Veritas Alta SaaS Protection (ASP) recently completed IRAP (Information Security Registered Assessors Program), also interchangeably known as an ACSC Cyber Security Assessment, up to the PROTECTED information classification level.

This document serves as an overview of what IRAP is, what it means for ASP, and in turn, what it means to a Veritas client, be they federal or state government, a critical infrastructure entity as per the Security of Critical Infrastructure Act or other commercial entity.
Executive Summary

IRAP is a process by which providers to the federal government get assessed against a stringent set of criteria to determine their level of cyber security posture for use by the government.

Veritas Alta SaaS Protection has completed an IRAP Cloud Security Assessment evaluated against controls to support up to PROTECTED level security requirements, which means a government department or other party with similar security requirements, may review the IRAP Assessment Report for application against a PROTECTED SaaS requirement at either PROTECTED or UNCLASSIFIED levels.

The process to complete an IRAP assessment is governed by the Australian Cyber Security Centre (ACSC), which was born out of the Australian Signals Directorate (ASD), formerly part of the Department of Defence.

In the federal market, IRAP assessment is a critical determination as to whether security controls applied to cloud and SaaS platforms are considered effective for storing, processing, and communicating information for agencies. An IRAP assessment provides an agency or department a measure of security posture, and comfort that cloud and SaaS platforms may meet at least minimum standards, also identifying areas for improvement and further risk assessment or evaluation.

An IRAP assessment serves a purpose for agencies to review and conduct their own assessment of a cloud capability, its security preparedness, maturity, vulnerability, and mitigation strategies. Without an IRAP assessment, federal (and increasingly, state government agencies) are not adopting cloud and as-a-service market offerings.

IRAP assessment provides to:

- a federal agency or department:
  - knowledge that Veritas Alta SaaS Protection has been assessed against the requirements for PROTECTED and UNCLASSIFIED level of use in Microsoft Azure

- a state government department:
  - the same level of assurance – it is a platform that has been rigorously assessed against numerous federally mandated controls

- any entity that has been deemed by the federal government as critical infrastructure:
  - a similar level of comfort that Veritas Alta SaaS Protection has been reviewed to protect a Microsoft 365 environment to the same level of security as the federal government

- a private commercial entity
  - knowledge that the offering has been reviewed against PROTECTED security criteria in Australia and this review provides a level of assurance that Veritas Alta SaaS Protection is likely to satisfy their security requirements – also allowing all entities to evaluate and understand aspects of strength and aspects for further dialogue and evaluation based upon organisational requirements.
Veritas Alta SaaS Protection

Veritas Alta SaaS Protection (ASP) facilitates data protection for SaaS applications, most notably and significantly for the federal government, Microsoft 365. This protection is available to our commercial clients of course, but in addition, we can protect other commercial SaaS applications, such as Salesforce.

What this means is that in addition to the protections afforded to Microsoft 365 by native Microsoft capabilities, ASP augments this to generate and supply:

- an off-site backup of Microsoft 365 to a destination of choice, such as AWS or an on-premises location
- backups are no longer constrained by the parameters set inside Microsoft 365, for example, 30 days for the recycle bin now becomes indefinite – based upon retention design and appropriate data lifecycle management requirements
- the ability to ingest Teams, Zoom, Signal, WebEx, and other collaboration platforms into Microsoft 365, and back these up accordingly and make them available for discovery via Purview akin to email – or to a Veritas Archiving service offering defensible copy management, eDiscovery as per Electronic Discovery Reference Model (EDRM) standards
- Optimised backups to lower-cost tiered storage, lowering Azure costs accordingly, as opposed to Azure backups being on primary cloud storage
- the ability to backup other SaaS applications in the same platform, such as Salesforce.

What does PROTECTED mean?

Data in the federal government is classified against three levels:

- UNCLASSIFIED
  - generally, this is publicly available data
- PROTECTED
  - data that is not publicly available
- SECRET
  - data that is restricted to who can access it.

PROTECTED means that Veritas Alta SaaS Protection has been assessed against security requirements or controls at both UNCLASSIFIED and PROTECTED data. PROTECTED and UNCLASSIFIED data make up the bulk of federal government data.
What is IRAP?

IRAP - the Information Security Registered Assessors Program - provides a framework for assessing the implementation and effectiveness of an organisation’s security controls against the Australian government’s security requirements, as outlined in the Information Security Manual (ISM) and Protective Security Policy Framework (PSPF). IRAP was created by the Australian Cyber Security Center (ACSC) which is a part of the Australian Signals Directorate (ASD).

What is an IRAP assessment?

The assessment is an activity undertaken by an IRAP Assessor to review security controls for a system or service, along with its environment, to determine if it has been implemented or is to be considered effective for storing, processing, and communicating information up to a defined or agreed classification level.

Assessments are done in various stages. The first step is to commonly to plan and prepare for the assessment, which includes agreement with the Service Provider or Owner on resources, key people, milestones, timeframes, security clearances, etc.

The IRAP Assessor will define the scope together with the Service Provider or Owner using existing documentation such as System Security Plans, network and data flow diagrams, architecture and configuration detail, technical specifics, shared responsibility matrices, demarcation points et al.

In the next step, the assessor will conduct the security control assessment including documentation reviews, technical interviews, evidence collection and attestation to verify effectiveness against a set of applicable ISM controls. For example, a cloud data capture and retention service would not be assessed against controls for the likes of printers or technology endpoints.

The assessor will document the occurrence of non-implemented or ineffective security controls and in some cases outline the risk or perceived risk and or suggest areas for further focus or mitigation.

The final stage is to produce the IRAP Assessment report which commonly addresses:

- the scope of the security assessment
- a view of the platform or service strengths and weaknesses
- security risks associated with people, process, technology, maturity and or operations
- the effectiveness of security controls against ISM expectations.

The above enables the reviewer of the report to make an informed risk-based decision about the system’s suitability for their security needs and risk appetite.

The IRAP assessment for Veritas Alta SaaS Protection took 5 months to complete.
Why IRAP is relevant to your organisation?

It is important to note that IRAP assessors do not accredit, certify, endorse or register systems, services and cloud-based platforms on behalf of ASD or ACSC.

IRAP provides a report against a common set of standards that have been set by the ACSC/ASD to allow for a risk-based assessment – by the reviewer – to validate that Veritas Alta SaaS Protection is suitable for use. IRAP provides an assurance that Veritas Alta SaaS Protection has been assessed against the specific version of the Australian Government Information Security Manual, at a specific point in time.

In most cases, the security risks associated with Veritas Alta SaaS Protection’s adoption for a federal government department or agency may be acceptable, and Veritas will be granted Authorisation to Operate. As is the case with SaaS-based services for large entities, an Authorising Officer within an agency, may request for further work or customisation in order to proceed.

The Authorisation to Operate assessed capability is left with the Authorising Officer, who could be the IT Security Advisor (ITSA) or Chief Information Security Officer (CISO) within the relevant federal government agency or department.

Ultimately, the Authorising Officer will review the assessment report and other supporting documents and make an informed risk-based decision as to whether the security risks associated with the operation of the system are acceptable or not.

How serious is the Australian Government about cyber security?

The current government was the first to introduce a Minister of Cyber Security. This position is held by the Hon Clare O’Neil MP, Minister for Home Affairs and Minister for Cyber Security.

The ACSC falls under the Hon Richard Marles MP, Deputy Prime Minister and Minister for Defence.

Between these two ministers, they strive to make the Australian Government, and Australia, safer for all Australian businesses and individuals.
What does this mean with regards to Microsoft 365?

Microsoft announced at Microsoft Inspire 2023 that backing up Microsoft 365 is a requirement if an organisation wants to improve their ability to combat the threat of ransomware.

“The rise in ransomware encryption attacks and security breaches means organizations are making cybersecurity a priority to safeguard themselves from losing data and sensitive information. Organisations need to have a system to help them meet regulatory requirements.”

*Microsoft Inspire 2023 announcement*

The message to the Microsoft 365 community is clear; relying on the recycle bin, or the standard 91-day retention policies of Microsoft 365, may not be sufficient.

Veritas is a development partner with Microsoft to complement what Microsoft 365 Backup will do in its release in early 2024.

The areas where we complement Microsoft 365 Backup are;

- we back up outside Microsoft 365, providing an air-gapped copy of the backup in a separate security boundary to that of Microsoft 365
- we also back up Microsoft Teams, which the initial release of Microsoft 365 backup will not do
- we can ingest collaboration feeds such as Zoom, WebEx, Signal, WhatsApp and so on, and then have this backed up
- we support user-defined backup and granular recovery of Microsoft 365 data
- we optimise the storage tier of Microsoft 365 to take advantage of BLOB storage both for the active files and for the backup
- we offer retention windows beyond one year.
Further Information

Should you require further information about the **IRAP Cloud Security Assessment for Veritas Alta SaaS Protection**, including a copy of the **official assessment letter, assessment report** and **detail**, please contact:

Pete Murray  
Managing Director, Veritas Australia & New Zealand  
pete.murray@veritas.com  
+61 (0) 44 88 66 765

Howard Noble  
Client Manager – Federal Government, Veritas Australia & New Zealand  
howard.noble@veritas.com  
+61 (0) 417681681

Geoffrey Coley  
Regional CTO, Veritas Technologies  
geoffrey.coley@veritas.com  
+61 (0) 412 985 272

About Veritas

Veritas Technologies is a leader in multi-cloud data management. Over 80,000 customers—including 95 percent of the Fortune 100—rely on Veritas to help ensure the protection, recoverability, and compliance of their data. Veritas has a reputation for reliability at scale, which delivers the resilience its customers need against the disruptions threatened by cyberattacks, like ransomware. No other vendor is able to match the ability of Veritas to execute, with support for 800+ data sources, 100+ operating systems, 1,400+ storage targets, and 60+ clouds through a single, unified approach. Powered by **Cloud Scale Technology**, Veritas is delivering today on its strategy for Autonomous Data Management that reduces operational overhead while delivering greater value. Learn more at [veritas.com](http://veritas.com). Follow us on Twitter at @veritastechllc.