Assessment summary

Databricks, as a provider of services to the Australian government, has undertaken a Cloud Security Assessment of the Databricks on AWS service.

The primary focus of this IRAP Assessment was the Databricks on AWS Platform. This service, hosted on Amazon Web Services (AWS), provides a unified data lakehouse solution. The fundamental design of Databricks on AWS supports data analytics, data engineering, data science and machine learning activities, to enable collaboration between data teams.

The objective of the assessment was to provide Databricks and Australian Government Cloud consumers visibility of the implementation state and effectiveness of security controls relevant to the operation and authorisation of the systems at the PROTECTED classification.

The IRAP Assessment procedure involves applying the security guidelines outlined in the Attorney-General's Department's Protective Security Policy Framework (PSPF), the Australian Government Information Security Manual (ISM), and the Digital Transformation Agency's Secure Cloud Strategy and Hosting Certification Framework. These resources serve as the basis for the security controls that Trustwave utilised to conduct a thorough evaluation of the system under assessment.

Security control implementation within Databricks on AWS and its supporting infrastructure underwent an evaluation by Trustwave against the March 2023 ISM to the PROTECTED level. The assessment was completed between May and October 2023 by Aditya Sinha, Harpreet Cheema, and Edward Dexter, certified Information Security Registered Assessor Program (IRAP) assessors, on behalf of the cybersecurity consultancy Trustwave.

Information supporting this assessment was gathered from review of documentation, interviews, and inspection of technical systems, process, and system outputs, to evidence the effectiveness of implemented security controls. Due to the global nature of the Databricks business, all work was performed remotely making use of teleconferencing, collaboration, and sharing services.

Assessment Findings

Databricks has demonstrated a commitment to operating and maintaining the environment in line with ISM control objectives and requirements.

The assessment of the Databricks on AWS product found a high level of security maturity across all relevant ISM domains and no significant weaknesses were identified. In total,

95.5% of applicable controls (474 of 496) have been assessed as effective or have suitable alternate controls.

The main consideration for consumers of the service will be in selection of architecture, deployment models, and configurations options to suit their risk profile and business needs.

Trustwave has provided Databricks with a cloud security assessment report for the consumption of the Authorising Officer, internal stakeholders, Australian Government agencies, and other Databricks customers, where required. The assessment report details control state and consumer responsibilities on a control-by-control basis. An overview of operational responsibilities is provided as Appendix A – Shared Security Model, and the assessment report can be made available upon request from Databricks.

As Databricks service a global market, applications and services can be configured to meet a wide range of compliance requirements. A key consideration for consumers of the service at the PROTECTED level will be in selection of architecture, deployment models, and configurations to suit their risk profile and business needs.

Edward Dexter

Director and IRAP assessor

Trustwave

This report has been produced by an ASD endorsed IRAP Assessor

Appendix A – Shared Security Model

The below section provides and overview of AWS, Databricks, and Cloud Consumer operational responsibilities.

Layer	Responsibility		
	Amazon Web Services (AWS)	Databricks	Cloud Consumer
Governance			
Incident Response	Yes	Yes	Yes
Backups	Yes	Yes	Yes
Technical			
Data	No	No	Yes
Identity & Access Management	Yes	Yes	Yes
Application	No	Yes	No
Platform	No	Yes	No
Virtualisation	Yes	No	No
Physical Hosts	Yes	No	No
Physical Networking	Yes	No	No
Physical Datacentre	Yes	No	No