Databricks

San Francisco, California 94105

USA

24 December 2025

Databricks – ACSC Cloud Security Assessment – Letter of Assessment

In May 2025, CyberCX was engaged by Databricks to conduct an ACSC Cloud Security Assessment of the Databricks Platform deployed within Australian regions. The objective of the assessment was to determine whether the security controls implemented for the cloud platform were effective for storing, processing, and communicating information up to the PROTECTED information classification level.

The assessment was conducted in line with the Australian Cyber Security Centre's (ACSC) Cloud Security Assessment and Authorisation Framework, Phase 1a. Databricks was assessed using the Australian Government Information Security Manual (ISM [March 2025 version]).

The following deployment types were in scope for the Phase 1a Assessment:

- Databricks Platform on Amazon Web Services (AWS)
- Databricks Platform on Microsoft Azure (Azure)
- Databricks Platform on Google Cloud Platform (GCP)

Cloud consumers including Australian Government Agencies, are responsible for granting cloud services an Authority to Operate within their environment. Cloud consumers should consider their own risk when using a cloud service provider and cloud services and understand their responsibilities when configuring and using the Databricks Platform. Additional information including findings and recommendations and alternate security controls can be found within the Databricks Platform IRAP Cloud Security Assessment Report and accompanying Cloud Controls Matrix.

To ensure ongoing awareness of information security risks and continued assurance of the security posture of the Databricks Platform, Databricks should:

- Address any assessment findings through a Plan of Action & Milestones (POA&M), within agreed timeframes.
- Continue to provide mechanisms to inform Cloud Consumers of applicable security events that may impact the security and risk of the Cloud Consumer's own systems and data.

- Continue to keep up to date with the latest ISM and inform Cloud Consumers of ISM changes that may impact the security of the Databricks Platform.
- Continue to identify and communicate significant changes that may impact the security of the Databricks Platform.
- Maintain the validity and accuracy of the CSP Security Fundamentals Assessment Report through the Addendum mechanism.

The Databricks Platform Cloud Security Assessment was conducted by Ravi Parmar, a registered assessor within the Australian Signals Directorate (ASD) Information Security Registered Assessors Program (IRAP).

Regards,

Ravi Parmar, Managing Consultant - Cloud Security Assessments, IRAP Assessor

CyberCX – Cloud Security and Solutions

From the assessment of the Databricks Platform, the effectiveness of applicable security controls was concluded as follows:

ISM Chapter	Effective	Not Effective
Guidelines for Cybersecurity Roles		
Board of directors and executive committee	✓	
Chief Information Security Officer	✓	
System owners	✓	
Guidelines for Cybersecurity Incidents		
Managing cybersecurity incidents	✓	
Responding to cybersecurity incidents	✓	
Guidelines for Procurement and Outsourcing		
Cyber supply chain risk management	✓	
Managed services and cloud services	✓	
Guidelines for Security Documentation		
Development and maintenance of security documentation	✓	
System-specific documentation	✓	
Guidelines for Personnel Security		
Cybersecurity awareness training	✓	
Access to systems and their resources	✓	
Guidelines for System Hardening		
Operating system hardening	✓	
Server application hardening	✓	

ISM Chapter	Effective	Not Effective
Authentication hardening	✓	
Guidelines for System Management		
System administration	✓	
System patching	✓	
Data backup and restoration	✓	
Guidelines for System Monitoring		
Event logging and monitoring	✓	
Guidelines for Software Development		
Software development fundamentals	✓	
Web application development	✓	
Guidelines for Database Systems		
Database servers	✓	
Databases	✓	
Guidelines for Networking		
Network design and configuration	✓	
Service continuity for online services	✓	
Guidelines for Cryptography		
Cryptographic fundamentals	✓	
ASD Approved Cryptographic Algorithms (AACA)	✓	
ASD Approved Cryptographic Protocols (AACP)	✓	

ISM Chapter	Effective	Not Effective
Transport Layer Security (TLS)	✓	
Secure Shell (SSH)	✓	