Databricks, Inc.

System and Organization Controls (SOC) 2 Type 2

Report on Databricks, Inc.'s Description of Its Lakehouse Platform Services System on Amazon Web Services, Microsoft Azure, and Google Cloud Platform and on the Suitability of the Design and Operating Effectiveness of Controls Relevant to Security, Availability, Confidentiality, and the HIPAA Security and Breach Notification Requirements Provided Within 45 CFR Sections 164.308–316 and 164.400-414

Throughout the Period
October 1, 2022 to June 30, 2023

Contents

I. Independent Service Auditor's Report on a SOC 2 Examination

Tel: 415-397-7900
Fax: 415-397-2161
www.bdo.com

One Bush Street, Suite 1800
San Francisco, CA 94104

Independent Service Auditor's Report on a SOC 2 Examination

To the Management of
Databricks, Inc.
San Francisco, California

Scope

We have examined Databricks, Inc.'s (Databricks or service organization) accompanying description of its Lakehouse Platform Services system on Amazon Web Services (AWS), Microsoft Azure (Azure), and Google Platform (GCP) (the system) titled *Databricks, Inc.'s Description of Its Lakehouse Platform Services System on Amazon Web Services, Microsoft Azure, and Google Cloud Platform* throughout the period October 1, 2022 to June 30, 2023 (description), based on the criteria for a description of a service organization's system in DC Section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report*, in AICPA *Description Criteria* (description criteria), and the suitability of the design and operating effectiveness of controls stated in the description throughout the period October 1, 2022 to June 30, 2023, to provide reasonable assurance that Databricks' service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA *Trust Services Criteria*. We have also examined the suitability of the design and operating effectiveness of controls to meet the requirements set forth in the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH Act), provided within Title 45 Code of Federal Regulations Sections 164.308–316 and 164.400–414 (45 CFR Sections 164.308-316 and 164.400-414) (the HIPAA security and breach notification requirements). Our examination does not provide a legal determination on Databricks compliance with laws and regulations related to the HIPAA security and breach notification requirements throughout the period October 1, 2022 to June 30, 2023.

Databricks uses subservice organizations to perform certain activities. A list of these subservice organizations and the activities performed is provided in Section III. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Databricks, to achieve Databricks' service commitments and system requirements based on the applicable trust services criteria and of the HIPAA security and breach notification requirements. The description presents Databricks' controls, the applicable trust services criteria, the HIPAA security and breach notification requirements, and the types of complementary subservice organization controls assumed in the design of Databricks' controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

Databricks is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Databricks' service commitments and system requirements were achieved. Databricks has

provided the accompanying assertion, titled *Assertion of Databricks, Inc. Management* (assertion), about the description and the suitability of the design and operating effectiveness of controls stated therein. Databricks is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and the HIPAA security and breach notification requirements; and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of the design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria and the HIPAA security and breach notification requirements. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively.
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria and the HIPAA security and breach notification requirements.
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria and the HIPAA security and breach notification requirements.
- Evaluating the overall presentation of the description.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria and the HIPAA security and breach notification requirements. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risks that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls we tested and the nature, timing and results of those tests are listed in Section IV.

Opinion

In our opinion, in all material respects:

a. The description presents Databricks' Lakehouse Platform Services system on AWS, Azure, and GCP that was designed and implemented throughout the period October 1, 2022 to June 30, 2023, in accordance with the description criteria.

b. The controls stated in the description were suitably designed throughout the period October 1, 2022 to June 30, 2023 to provide reasonable assurance that Databricks' service commitments and system requirements would be achieved based on the applicable trust services criteria and the HIPAA security and breach notification requirements if its controls operated effectively throughout that period and if the subservice organizations applied the complementary controls assumed in the design of Databricks' controls throughout that period.

c. The controls stated in the description operated effectively throughout the period October 1, 2022 to June 30, 2023 to provide reasonable assurance that Databricks' service commitments and system requirements were achieved based on the applicable trust services criteria and the HIPAA security and breach notification requirements if complementary subservice organization controls assumed in the design of Databricks' controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of Databricks, user entities of Databricks' system during some or all of the period October 1, 2022 to June 30, 2023, business partners of Databricks subject to risks arising from interactions with the system, practitioners providing services to such

user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization.
- How the service organization's system interacts with user entities, business partners, subservice organizations and other parties.
- Internal control and its limitations.
- Complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
- The applicable trust services criteria and the HIPAA security and breach notification requirements.
- The risks that may threaten the achievement of the service organization's service commitments and system requirements, and how controls address those risks.

This report is not intended to be, and should not be, used by anyone other than these specified parties.

BDO USA, P.A.

August 7, 2023

II. Assertion of Databricks, Inc. Management

Assertion of Databricks, Inc. Management

We have prepared the accompanying description of Databricks, Inc.'s (Databricks or service organization) Lakehouse Platform Services system on Amazon Web Services (AWS), Microsoft Azure (Azure), and Google Cloud Platform (GCP), (the system) titled *Databricks, Inc.'s Description of Its Lakehouse Platform Services System on Amazon Web Services, Microsoft Azure, and Google Cloud Platform* throughout the period October 1, 2022 to June 30, 2023 (description) based on the criteria for a description of a service organization's system in DC Section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report,* in AICPA *Description Criteria* (description criteria). The description is intended to provide report users with information about the system that may be useful when assessing the risks arising from interactions with Databricks' system, particularly information about system controls that Databricks has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy,* in AICPA *Trust Services Criteria* and the requirements set forth in the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH Act), provided within Title 45 Code of Federal Regulations Sections 164.308–316 and 164.400–414 (45 CFR Sections 164.308-316 and 164.400-414) (the HIPAA security and breach notification requirements).

Databricks uses subservice organizations to perform certain activities. A list of these subservice organizations and the activities performed is provided in Section III. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Databricks, to achieve Databricks' service commitments and system requirements based on the applicable trust services criteria and the HIPAA security and breach notification requirements. The description presents Databricks' controls, the applicable trust services criteria and HIPAA security and breach notification requirements, and the types of complementary subservice organization controls assumed in the design of Databricks' controls. The description does not disclose the actual controls at the subservice organizations.

We confirm, to the best of our knowledge and belief, that:

a. The description presents Databricks' Lakehouse Platform Services system on AWS, Azure, and GCP that was designed and implemented throughout the period October 1, 2022 to June 30, 2023, in accordance with the description criteria.

b. The controls stated in the description were suitably designed throughout the period October 1, 2022 to June 30, 2023 to provide reasonable assurance that Databricks' service commitments and system requirements would be achieved based on the applicable trust services criteria and the HIPAA security and breach notification requirements if its controls operated effectively throughout that period, and if the subservice organizations applied the complementary controls assumed in the design of Databricks' controls throughout that period.

c. The controls stated in the description operated effectively throughout the period October 1, 2022 to June 30, 2023 to provide reasonable assurance that Databricks' service commitments and system requirements were achieved based on the applicable trust services criteria and the HIPAA security and breach notification requirements if complementary subservice organization controls assumed in the design of Databricks' controls operated effectively throughout that period.

Databricks, Inc.

August 7, 2023

III. Databricks, Inc.'s Description of Its Lakehouse Platform Services System on Amazon Web Services, Microsoft Azure, and Google Cloud Platform

Databricks, Inc.'s Description of Its Lakehouse Platform Services System on Amazon Web Services, Microsoft Azure, and Google Cloud Platform

Scope and Boundaries of the System

This is a System and Organization Controls (SOC) 2 Type 2 report and includes a description of Databricks, Inc.'s (Databricks, service organization, or Company) Lakehouse Platform Services system on Amazon Web Services (AWS), Microsoft Azure (Azure), and Google Cloud Platform (GCP) (the system), and the controls in place to provide reasonable assurance that Databricks' service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy,* in AICPA *Trust Services Criteria*, and requirements set forth in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH Act), provided within Title 45 Code of Federal Regulations Sections 164.308–316 and 164.400–414 (45 CFR Sections 164.308-316 and 164.400-414) (the HIPAA security and breach notification requirements) throughout the period October 1, 2022 to June 30, 2023 (the period), which may be relevant to the users of the system. It does not encompass all aspects of the services provided or procedures followed for other activities performed by Databricks.

Databricks uses subservice organizations to perform certain services. A list of these subservice organizations and the services performed is provided in the following table. The description does not disclose the actual controls at the subservice organizations.

Subservice Organization	Services Performed
Amazon Web Services, Inc. (Amazon)	Provides managed services over infrastructure, logging, and key management services.
Microsoft Corporation (Microsoft)	Provides managed services over infrastructure, logging, monitoring, vulnerability scan, and key management services.
Google LLC (Google)	Provides managed services over infrastructure, logging, and key management services.
Okta, Inc. (Okta)	Single sign-on (SSO) and authentication services.

Company Background

Databricks, Inc.'s (hereinafter referred to as Databricks) founders started the Spark research project at UC Berkeley, which later became Apache Spark™. Databricks was founded in 2013 by the original creators of popular open-source projects, including Apache Spark, Delta Lake, MLflow, and Koalas. As the world's first Lakehouse platform in the cloud, Databricks combines the best elements of data lakes and data warehouses to offer an open and unified platform for data, analytic, and AI.

Databricks is on a mission to simplify and democratize data and AI, helping data teams solve the world's toughest problems. As the leader in Unified Data Analytics, Databricks helps organizations make all their data ready for analytics, empower data science and data-driven decisions across the organization, and rapidly adopt machine learning to outpace the competition. It is simple, open, and supports multi-cloud. By providing data teams with the ability to process massive amounts of

data in the Cloud and power AI with that data, Databricks helps organizations innovate faster and tackle challenges like treating chronic disease through faster drug discovery, improving energy efficiency, and protecting financial markets. More than 9,000 organizations worldwide rely on Databricks to enable massive-scale data engineering, collaborative data science, full-lifecycle machine learning, and business analytics.

Databricks is venture-backed and headquartered in San Francisco, California with offices around the world and has over 1,200 global partners, including Microsoft, Amazon, Google, Tableau, Informatica, Qlik, Dataiku, Fivetran, Accenture, Capgemini, and Booz Allen Hamilton.

Services Provided

Databricks provides a Lakehouse Platform Service system for massive scale data engineering and collaborative data science. The Databricks solution consists of a Control Plane, Data Plane, and Customer Data Storage.

- *Control Plane* — The portion of the Lakehouse Platform Service system that is always hosted in the Databricks managed AWS, Azure, or GCP environments. It contains the core Databricks services such as web application, cluster management, access control to resources, and managing running or scheduled jobs. This report covers the Control Plane.
- *Data Plane* — This is where the extensive data processing occurs (server clusters of the compute layer). The type of data processed is chosen by the customer. As of the report date, there are two types of Data Planes.
    - *Serverless Compute Data Plane* — This resides in the customer's Databricks managed and owned AWS or Azure account rather than the customer owned AWS or Azure account. AWS and Azure Serverless Compute Data Plane is in-scope and covered by this report.
    - *Classic Compute Data Plane* — This resides in the customer owned AWS, Azure, or GCP account and is not covered by this report.
- *Customer Data Storage* — This is where customer data sets are stored at rest when they use Databricks services. As of the report date, for the AWS Serverless Compute model environment, customers may select from the below storage options:
    - Databricks-managed storage — AWS S3 bucket resides in the Databricks AWS account and is covered by this report.
    - Customer-managed storage — AWS S3 bucket resides in the customer-managed AWS account and is not covered by this report.

  For other environments, customers store the data in their managed cloud account (i.e., AWS S3 bucket, Azure Blob storage, Google GCS bucket) and are not covered by this report.

Databricks services enable customers to:

- Easily and quickly access data at scale.
- Process both structured data and unstructured data.
- Ingest from nontraditional data stores.
- Reduce the batch processing time.

- Deploy production-quality machine learning and streaming applications.
- Set up, tune, and scale Apache Spark clusters for the team.
- Keep clusters resilient and up-to-date with the latest versions.
- Schedule, run, and debug applications in production.
- Leverage more data science to aid in decision-making.
- Explore and visualize data interactively.
- Connect to Business Intelligence tools and build real-time dashboards.

Principal Service Commitments and System Requirements

In order to meet the security, availability, and confidentiality commitments of cloud services offered on the Lakehouse Platform, Databricks has designed and implemented several technologies, processes, and procedures across its environments. Databricks documents and communicates its service commitments to its customers in the form of customer agreements. Service Commitments include, but are not limited to:

Security

- The Lakehouse Platform is designed to permit system users to access the information they need based on their role, while restricting them from accessing information not required for their role.
- Encryption technologies are implemented to help protect customer data.
- Access and activity logging with appropriate audit controls are in place to support incident management. Security incident response planning and notification requirements procedures exist to monitor, react, notify, and investigate incidents.
- Vulnerability scans are performed on a regular basis, with external third-party penetration tests executed at least annually for each cloud. Remediation follows industry acceptable vulnerability management processes, defined exception processes, and defined service level agreements (SLAs).
- Industry recognized application development standards (e.g., OWASP Top 10) are followed.

Availability

- Support is provided according to contract and is available 24 hours a day, seven days a week, with committed response times based on severity of the issue.
- Availability monitoring and capacity monitoring are in place to identify and alert on spikes in activity above predefined critical availability and capacity thresholds. An investigation is conducted and remediation is performed as needed, based on the nature and severity of the incident.
- Business continuity and disaster recovery mechanisms are in place to minimize data loss and ensure return to operations in the case of a disaster using industry-standard mechanisms. Business continuity and disaster recovery plans are tested at least annually.

- For databases that reside in Databricks' managed AWS, Azure, and GCP accounts, backups are performed daily and retained.

Confidentiality

- Record retention policies are in place to retain information for periods defined by Databricks policies.
- Databricks identifies and maintains confidential information according to its objectives and applicable regulatory standards.
- Databricks deletes customer accounts per customer request in accordance with applicable laws and requirements outlined within customer contracts.

Databricks establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Databricks' system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organizationwide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the Lakehouse Platform. The HIPAA specific product offering of Databricks is subject to the security and privacy requirements of the Health Insurance Portability and Accountability Act, as amended, including relevant regulations, as well as state privacy security laws and regulations in the jurisdictions in which Databricks operates.

For more details on the security features of the Databricks product, please see the Security Features section of databricks.com/trust.

System Incidents

A system incident is an incident that leads to the loss of, or disruption to, operations, services, or functions and results in Databricks' failure to achieve its service commitments or system requirements. Such an occurrence may arise from a security event, security incident, failure to comply with applicable laws and regulations, error, or other means. In determining whether a system incident occurred resulting in Databricks' failure to achieve one or more of its service commitments or system requirements, considerations may include, but are not limited to, the following:

- Whether the occurrence resulted from one or more controls that were not suitably designed or operating effectively.
- Whether public disclosure of the occurrence was required (or is likely to be required) by cybersecurity laws or regulations.
- Whether the occurrence had a material effect on the service organization's financial position or results of operations and required disclosure in a financial statement filing.
- Whether the occurrence resulted in sanctions by any legal or regulatory agency.
- Whether the occurrence resulted in the service organization's withdrawal from material markets or cancellation of material contracts.

Incidents and events relevant to Databricks' service commitments and system requirements based on the applicable trust services criteria are important in monitoring, identifying, and evaluating if a system incident has occurred; however, incidents and events relevant to Databricks' service commitments and system requirements based on the applicable trust services criteria do not always rise to the level of a system incident. The evaluation of an incident or event relevant to Databricks' service commitments and system requirements based on the applicable trust services criteria will make that determination.

Databricks did not identify any system incidents that occurred during the period October 1, 2022 to June 30, 2023 resulting in Databricks' failure to achieve one or more of its service commitments or system requirements based on these considerations.

Components of the System Used to Provide the Services

Infrastructure

Databricks is headquartered in San Francisco, California. Databricks does not operate its own data centers; instead, it has contracted with subservice organizations, AWS, Azure, and GCP, in support of its Lakehouse Platform services to provide supporting infrastructure, logging, and key management services. Refer to section above titled, "Scope and Boundaries of the System" for additional information on the service provided by AWS, Azure, and GCP and the associated complementary subservice organization controls.

Primary infrastructure used to provide the Databricks hosted Lakehouse Platform Services system on AWS, Azure, and GCP includes but is not limited to the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Amazon Virtual Private Cloud (VPC)	Virtual Network	To provide network level isolation between major areas of the infrastructure.
Amazon Elastic Compute Cloud (EC2)	Virtual Machines	Virtualized servers for hosting the web application and its supporting services.
Amazon Relational Database Service (RDS)	Database	To store customer metadata (such as notebook data, login credentials, and job definitions).
Amazon Elastic Block Store (EBS)	Block Storage	To store the Operating Systems, Applications (as well as their configs), and any temporary Spark data (such as shuffle data).
Amazon Simple Storage Service (S3)	Object Storage	To provide general data storage that is primarily used for storing control plane artifacts for purposes of bootstrapping services.
AWS Key Management Service (KMS)	Cryptography	To provide cryptographic key management such as generation, distribution, and encryption for many components in the infrastructure.
AWS Identity and Access Management (IAM)	Identify and Access Management	To securely manage access to AWS services and resources.

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Azure Resource Manager	Management Layer	To manage resources (e.g., create, update, and delete) inside Azure deployment such as virtual machine, storage account, web app, database, and virtual network.
Azure Virtual Network (VNET)	Virtual Network	To provide network level isolation between major areas of the infrastructure.
Azure Virtual Machines (VMs)	Virtual Machines	Virtualized servers for hosting the web application and its supporting services.
Azure DB Database for MySQL	Database	To store customer metadata (such as notebook data, login credentials, and job definitions).
Azure Blob Storage	Object Storage	To provide a generic blob store that is primarily used for storing control plane artifacts for purposes of bootstrapping services.
Azure Key Vault (AKV)	Cryptography	To provide cryptographic key management such as generation, distribution, and encryption for many components in the infrastructure.
GCP Virtual Private Cloud (VPC)	Virtual Network	To provide network level isolation between major areas of the infrastructure.
GCP Compute Engine	Virtual Machines	Virtualized servers for hosting the web application and its supporting services.
GCP Database	Database	To store customer metadata (such as notebook data, login credentials, and job definitions).
GCP Persistent Disk	Block Storage	To store the Operating Systems, Applications (as well as their configs), and any temporary Spark data (such as shuffle data).
Google Cloud Storage (GCS)	Object Storage	To provide general data storage that is primarily used for storing control plane artifacts for purposes of bootstrapping services.
Google Cloud Key Management	Cryptography	To provide cryptographic key management such as generation, distribution, and encryption for many components in the infrastructure.
GCP Identity and Access Management (IAM)	Identify and Access Management	To securely manage access to GCP services and resources.

Software

Operating System and Database

Databricks uses Linux operating systems and SQL databases in AWS, Azure, and GCP environments.

Supporting Systems and Applications

Primary software tools and applications used to support Databricks' Lakehouse Platform Services system on AWS, Azure, and GCP and operations are outlined below:

Primary Software and Application	
Software/Application	**Purpose**
People Operations	
Workday	Workday is a human capital management software. Workday is the source of truth for managing Databricks employee and contractor accounts, payroll, and benefits. Workday is integrated with Okta.
Change Management	
GitHub	GitHub is a centralized source code control system. It is implemented internally for the management of code repositories.
Jenkins/Deployment Service	Jenkins/Deployment Service is a tool that helps to automate the software development process with continuous integration and facilitating technical aspects of continuous delivery.
Spinnaker	Spinnaker is a continuous delivery platform that orchestrates the continuous delivery pipelines that include many stages throughout the release cycle.
Atlassian Jira	Jira is a ticketing system to document and track changes including application changes, infrastructure changes, operational changes, etc.
FreshService	FreshService is a ticketing system used by the Corporate Engineering team and the People Operations team to provide and deliver employee support.
Customer Support	
Salesforce	Salesforce is the ticketing system used for customer support.
Identity and Access Management	
Okta	Okta is an SSO solution that manages and secures user authentication into modern applications. It provides a universal cloud-based platform to manage and secure identities.
Okta Verify/Yubikey	Okta Verify/Yubikey are multifactor authentication (MFA) tools that must be used by Databricks personnel.
GlobalProtect VPN	GlobalProtect VPN is the VPN solution provided by Palo Alto Networks. It is used to control remote access to the production systems via dedicated and on-demand encrypted tunnels.

Primary Software and Application	
Software/Application	**Purpose**
Zscaler	Zscaler is a VPN solution that is used to control remote access to the production systems via dedicated and on-demand encrypted tunnels.
Genie	Genie is an in-house application that Databricks uses for managing and logging temporary access to production infrastructure.
Security and Performance Logging and Monitoring	
PagerDuty	PagerDuty is a SaaS incident response platform that integrates with other applications and handles alert notifications and triaging.
M3	M3 is an open-source metrics engine that is Prometheus compatible. It provides monitoring solutions with an alerting toolkit to monitor network, machines, and applications.
AWS CloudTrail	AWS CloudTrail is an AWS service that enables governance, compliance, operational auditing, and risk auditing of Databricks AWS accounts.
AWS GuardDuty	AWS GuardDuty is a threat detection service used to monitor malicious activity and unauthorized behavior to protect Databricks AWS accounts.
Google Cloud Audit	Google Cloud Audit is a GCP service that enables governance, compliance, operational auditing, and risk auditing of Databricks GCP accounts. It provides Admin Activity, Data Access, System Event, and Policy Denied audit logs for each Cloud project, folder, and organization.
GCP Event Threat Detection	GCP Event Threat Detection is a threat detection service used to monitor malicious activity and unauthorized behavior to protect Databricks GCP accounts.
GCP Security Command Center	GCP Security Command Center is a security and risk management platform for Google Cloud. Google Cloud Audit and GCP Event Threat Detection services are integrated with the GCP Security Command Center and the findings are available to view there.
Secfood	Secfood is a Databricks application instance used by the Security Team as the Security Information and Event Management (SIEM) tool.
CrowdStrike	CrowdStrike provides next-generation anti-virus software for Databricks end-user endpoints that use a combination of artificial intelligence, behavioral detection, machine learning algorithms, and exploit mitigation.
AirWatch/Intune	AirWatch/Intune provides management software that enforces policies on Databricks end-user Microsoft Windows endpoints (i.e., host-based firewall, laptop disk encryption, etc.).
JAMF	JAMF provides management software that enforces policies on Databricks end-user MacOS endpoints (i.e., host-based firewall, laptop disk encryption, etc.).

Primary Software and Application	
Software/Application	**Purpose**
Vulnerability Management	
Qualys	Qualys Cloud Platform is a third-party product used to perform infrastructure and web application vulnerability assessments.
HackerOne	HackerOne is a third-party platform used to facilitate penetration testing bug bounty programs to identify vulnerabilities on an ongoing basis.
Configuration Management	
AWS CloudFormation	AWS CloudFormation is an infrastructure as code service to deploy cloud resources in AWS.
Terraform	Terraform is an open-source, infrastructure as code, software tool to deploy cloud resources in Azure and GCP.

People

The Databricks staff provides support for the above services in each of the following functional areas:

Functional Areas	Responsibilities
Executive Management	• Develops and executes on company's strategy and oversees operations to achieve business objectives. • The executive team includes: Chief Executive Officer (CEO), Global Field Operations, Chief Financial Officer (CFO), Chief Security Officer (CSO), Senior Vice President of Engineering, Chief Operations Officer (COO), Chief Information Officer (CIO), Chief People Officer (CPO), Senior Vice President of Products, Senior Vice President & General Counsel.
Information Security	• Led by the CSO to meet security and compliance requirements. • Security policies and procedures documentation and review. • Overall security of the platform, maintaining compliance with ISO 27001, ISO 27018, ISO 27017, ISO 27701, HITRUST, SOC 1, SOC 2, HIPAA, PCI-DSS, and various industry standards. • Security monitoring and incident response. • Vulnerability scanning and penetration testing. • Organizational security awareness and training. • Security risk management. • Vendor security compliance.

Functional Areas	Responsibilities
Engineering	• Managing, monitoring, and supporting the cloud infrastructure required to run the product. • Responsible for day-to-day maintenance of AWS, Azure, and GCP cloud systems security, availability, and confidentiality as applicable. • Managing, monitoring, and supporting the cloud services required to support the product (i.e., Genie, Secret Management, etc.). • Managing base images. • Building services to ensure Databricks' infrastructure runs on a secure and performant base OS. • Overseeing the development of the product and release management. • Developing new features, fixing bugs, and vulnerabilities. • Monitoring and handling availability and capacity alerts.
Field Engineering	• Performing pre- and post-sales engineering. • Working with potential customers to try out Databricks' products and solutions.
Product Management	• Working closely with Engineering teams to ensure product improvements are tracked, implemented, and released in a timely manner. • Working closely with customers to get feedback and gather requirements for product improvements.
Customer Success	• Single point of contact for handling and directing customer issues. • Day-to-day customer support.
Sales Operations	• Customer sales onboarding, renewal, and account management. • Working with field engineering to provide training and professional services to customers.
Legal	• Managing contractual agreements with customers and third parties. • Addressing Databricks' legal concerns and handling legal related external matters.
People Operations	• Handling talent acquisition and employee benefits. • Reviewing and updating the Employee Handbook and Databricks Code of Conduct. • Handling employee termination and internal investigations. • Managing performance enablement reviews and focal programs.
IT	• Managing IT systems, applications, and office networks. • Managing employee onboarding and offboarding such as laptop setup, new hire account creation, laptop collection and disposal, applications assignment in Okta, and account removal from Okta.

Functional Areas	Responsibilities
Facilities	• Managing Databricks office locations and office physical security controls (for example, door access control, security camera, space management, building maintenance).
Professional Services	• Delivering customer projects from ideation to production. • Providing industry leading expertise on Spark, machine learning, cloud, streaming, data science, and engineering. • Empowering and enabling customers with the technical skills needed to deploy, maintain, and enhance their platforms.

Processes and Procedures

Databricks has put into place a set of policies and procedures designed to provide requirements and guidance for management and employees regarding security, availability, and confidentiality. Databricks reviews those policies annually and makes them available to all Databricks personnel. Teams are expected to implement procedures that define how services are delivered. Exceptions to Databricks policies are documented, tracked, and reviewed. Databricks personnel that fail to comply with Databricks' security policies are subject to a disciplinary process.

Databricks' security policies cover, but are not limited to, the following domains:

- Anti-Malware
- Application Development
- Asset Management
- Backup
- Business Continuity and Disaster Recovery
- Change Management
- Cryptography
- Data Classification and Handling
- Data Collection, Storage, and Use
- Data Retention and Destruction
- Incident Response Management
- Logging and Monitoring
- Network Security
- Personnel Management
- Remote Access and Teleworking
- Removable Media
- Risk Assessment
- Security Governance and Compliance
- Third Party Management
- Training and Awareness
- Vulnerability Management

Data

Databricks handles a variety of sensitive data, which, depending on contract, may include PII and PHI. Therefore, Databricks has implemented security controls throughout the data lifecycle.

Collection

The customer provides credentials to connect to the data sources. At runtime, the clusters access these data sources using temporary authorizations that were generated from customer-provided

credentials. Clusters access customer data during processing. Communications between the customer and Databricks services always use Hypertext Transfer Protocol Secure (HTTPS).

Handling and Storage

Databricks SQL or instructions within notebooks are stored in databases that reside in the Databricks managed Control Plane. Databases in the Databricks managed Control Plane are encrypted at rest with 256-bit keys. Encryption and retention of the data stored in customer-controlled data sources (e.g., AWS S3 bucket, Azure Blob Storage, Google GCS bucket, etc.) is the customer's responsibility.

Transmission

Data in transit between the Control Plane (Databricks managed AWS/Azure/GCP account) and the Data Plane is encrypted using the Transport Layer Security (TLS) 1.2 or 1.3 cipher suite. Notebook source data submitted from users of the Databricks web application to the Control Plane is encrypted in transit with TLS 1.2 or 1.3. Customers are responsible for using encrypted connections to their data sources. Note that for Azure Databricks, communication between the Control Plane and the customer Data Plane traverses the Azure network backbone, not across the public Internet.

Modification

Data is protected from modification through encryption and access controls.

Release/Disclosure

Databricks will not release or disclose customer data to a third-party unless required by applicable law.

Processing

With the Databricks Classic Compute platform, data is processed by clusters residing in the customer's AWS, Azure, or GCP account. With the Databricks Serverless Compute platform, data is processed by clusters residing in Databricks' cloud account.

Use

Databricks will use customers' data only to perform activities contractually agreed to. Datasets are stored and managed by the customer unless Databricks managed storage service is used. Databricks SQL or instructions within Databricks Notebooks are retained for a time specified according to the customer's contract. After that time, such data is deleted.

Description of the Controls Relevant to the Security, Availability, and Confidentiality Trust Services Categories

Control Environment

Integrity and Ethical Values

Databricks has developed a Global Code of Conduct that addresses acceptable business practices, conflicts of interest, and expected standards of ethical and moral behavior. These documents are provided to new employees. Employees are required to sign an acknowledgement form that they

received and agree to the Global Code of Conduct as part of onboarding. There is an established "tone at the top" including explicit guidance about what is right and wrong. This tone is communicated and practiced by executives and management throughout the organization. The importance of strong ethics and controls is discussed with newly hired employees throughout both the interview process and orientation.

Specific control activities implemented by Databricks in this area are described below:

- Formally documented organizational policy statements and codes of conduct communicate entity values and behavioral standards to personnel.
- New employees are required to sign an acknowledgment form indicating they understand their responsibility for adhering to the policies and procedures contained within the Global Code of Conduct.
- A Board of Directors meets at least quarterly and is consulted and involved in significant business decisions.
- Background checks are performed for employees and contractors (with an assigned corporate Databricks account) as a component of the hiring process.

Commitment to Competence

Databricks' management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements. Candidate resumes are evaluated against essential skills listed in the job description. If the minimum criteria are met, an interview is scheduled with the applicable manager. When the final candidate is selected, a written offer is provided.

Employees and contractors who require a corporate Databricks account are required to complete security awareness training upon hire and on an annual basis. The security awareness training covers information on relevant security best practices and includes the responsibility for employees to communicate security concerns. Various technical training and operating procedures are also recommended and made available to employees to help maintain employees' competency. Developers are required to take the secure software development training at least annually. Security Engineers, who are responsible for handling security incident responses, are required to take incident response training at least annually. Additionally, training is conducted on the job by the hiring manager. Team members are encouraged to broaden their skill sets by attending industry security conferences and other types of training.

Management's Philosophy and Operating Style

Databricks senior management takes a "hands on" approach to running the business. Senior management is heavily involved in all phases of the business operations. Databricks has at least one monthly staff meeting that enables the senior management team to remain in close communication with personnel and to emphasize appropriate behavior. Databricks' senior management team demonstrates attitudes and actions that consistently reflect a commitment to delivering quality services, superior customer support, and ethical values.

Specific control activities the service organization has implemented in this area are described below:

- Management is periodically briefed on regulatory and industry changes affecting the services provided.
- Executive management meetings are held to discuss major initiatives and issues that affect the business as a whole.

Organizational Structure and Assignment of Authority and Responsibility

Databricks has established appropriate lines of reporting, which facilitate the flow of information to appropriate people in a timely manner. Roles and responsibilities are segregated based on functional requirements. Databricks has an organization chart that sets forth Databricks' lines of reporting.

Management and employees are assigned appropriate levels of authority and responsibility to facilitate effective internal control.

Specific control activities the service organization has implemented in this area are described below:

- Organizational charts are in place to communicate key areas of authority and responsibility.
- Organizational charts are available to employees and updated as needed.

Human Resources Policies and Practices

Databricks maintains formal hiring policies and procedures. Databricks maintains current job descriptions and roles for key personnel. Also, Databricks has a process that is designed to ensure the correct personnel are responsible for key processes and technology.

Specific control activities the service organization has implemented in this area are described below:

- Employees and contractors (with an assigned corporate Databricks account) are required to sign acknowledgement forms, upon hire and annually thereafter, indicating they have read Databricks Security Policies.
- New employees and contractors (with an assigned corporate Databricks account) are required to sign a confidentiality agreement as part of their employment agreement.
- Performance evaluations for each employee are performed on at least an annual basis.
- Employee termination procedures are in place to guide the termination process and are documented.

Communication and Information

Internal Communication

Databricks has implemented various methods of communication designed to ensure that employees understand their individual roles and responsibilities. These methods include periodic training

programs for educating employees on internal developments, industry trends, and organizational development activities. Communication is the continual, iterative process of providing, sharing, and obtaining necessary information. Internal communication is the means by which information is disseminated throughout the organization, flowing up, down, and across the entity. It enables personnel to receive a clear message from senior management that control responsibilities must be taken seriously. Employees are encouraged to communicate to their direct supervisor.

Databricks obtains or generates and uses relevant, quality information to support the functioning of internal controls. Databricks maintains data flow diagrams, flowcharts, narratives, and procedural documentation to allow easy identification of data sources, responsible personnel, and other relevant information. Databricks has methods in place to help ensure information systems maintain and produce information that is timely, current, accurate, and complete.

External Communication

External communication is twofold: it enables inbound communication of relevant external information and provides information to external parties in response to requirements and expectations.

Specific information systems used to support Databricks' Lakehouse Platform Services system on AWS, Azure, and GCP are described in the Description of Services section above.

Risk Assessment

Databricks has a risk assessment process to identify and manage risks that could affect Databricks' ability to provide reliable services to its clients. This process requires management to identify significant risks in their areas of responsibility and to implement appropriate measures to address those risks. In designing its controls, Databricks has considered the risks that could prevent it from effectively addressing the criteria under the security, availability, and confidentiality trust services categories. The key risks that Databricks has identified and is focused on controlling include the following:

- Data security
- Compliance
- Competition
- Fraud
- Reputational risk if errors or fraud occur

Risk is defined as the possibility that an event will occur and adversely affect the achievement of objectives. Risk assessment involves a dynamic and iterative process for identifying and assessing risks to the achievement of objectives. Risks to the achievement of these objectives from across the entity are considered relative to established risk tolerances. Thus, risk assessment forms the basis for determining how risks will be managed. A precondition to risk assessment is the establishment of objectives linked at different levels of the entity. Management specifies objectives within categories relating to operations, reporting, and compliance with sufficient clarity to be able to identify and analyze risks to those objectives. Management also considers the suitability of the objectives for the entity. Risk assessment also requires management to consider the impact of

possible changes in the external environment and within its own business model that may render internal control ineffective.

Databricks identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed. Databricks' risk assessment process includes an analysis of possible threats and vulnerabilities relative to each of the objectives. The risk identification process includes consideration of both internal and external factors and their impact on the achievement of the objectives.

Appropriate levels of management are involved in the risk assessment process. Identified risks are analyzed through a process that includes estimating the potential significance of the risk. Databricks' risk assessment process includes considering how the risk should be managed and whether to accept, avoid, mitigate, or share the risk.

Databricks considers the potential for fraud in assessing risks to the achievement of objectives. The assessment of fraud risk considers fraudulent reporting, possible loss of assets or data, and corruption resulting from the various ways that fraud and misconduct can occur. It also considers opportunities for unauthorized acquisition, use or disposal of assets, altering of the entity's reporting records, or committing other inappropriate acts, and how management and other personnel might engage in or justify inappropriate actions.

Databricks identifies and assesses changes that could significantly impact the system of internal control. The risk identification process considers changes to the regulatory, economic, and physical environment in which Databricks operates.

Databricks considers the potential impacts of new business lines, dramatically altered compositions of existing business lines, acquired or divested business operations, rapid growth, and new technologies on the system of internal control.

As part of the risk assessment process, Databricks determines mitigation strategies for the risks that have been identified and designs, develops, and implements controls, including policies and procedures, to implement its risk mitigation strategy.

Health Information Security Risks

Health information security risks are assessed by the Security Assurance Team. Risk factors associated with the organization are evaluated considering compliance obligations, laws and regulations, policies and procedures, contracts, and best practices to which the organization has committed to. Information security assessments carried out by risk management personnel are rolled up to the CSO of the organization.

Vendor and Subprocessor Risks

New vendors undergo a risk management process prior to engaging their services. This includes the Security Assurance Team review of vendor service reports and questionnaires, where applicable. Cloud service vendors that are considered critical to the system requirements and commitments are monitored and reviewed annually to ensure that the terms and conditions of the agreements are being adhered to and that information security incidents and problems are managed properly. Subprocessors that are published on the Databricks website (https://databricks.com/databricks-subprocessors) are also reviewed annually.

Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of Databricks' Lakehouse Platform Services system on AWS, Azure, and GCP, as well as the nature of the components of the system, result in risks that the criteria will not be met. Databricks addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the criteria are met. Because each system and the environment in which it operates are unique, the combination of risks to meet the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the system, Databricks' management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

Monitoring Activities

Members of Databricks regularly participate in security or risk-based groups to monitor the impact of emerging technologies. Additionally, Databricks holds quarterly Security and Privacy Risk Committee meetings to discuss current projects and any potential security concerns.

Ongoing Monitoring

Ongoing evaluations, built into business processes at different levels of the entity, provide timely information. Separate evaluations, conducted periodically, vary in scope and frequency depending on assessment of risks, effectiveness of ongoing evaluations, and other management considerations. Findings are evaluated against criteria established by management and the Board of Directors, and deficiencies are communicated to management and the Board of Directors as appropriate. Databricks management and supervisory personnel monitor the quality of internal control performance as a routine part of their activities.

Reporting Deficiencies

Databricks evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the Board of Directors, as appropriate. Instructions for reporting deficiencies have been developed and are provided to employees and contractors who require a corporate Databricks account.

Remediation and Continuous Improvement

Areas of noncompliance in Databricks' internal control system may surface from many sources, including the Company's ongoing monitoring procedures, separate evaluations of the internal control system, and external parties. Management evaluates the specific facts and circumstances related to areas of noncompliance in internal control procedures and makes the decision for addressing any noncompliant items based on whether the incident was isolated or a change in the Company's policies, procedures, or personnel is required. Management has developed protocols to help ensure communication of findings of internal control noncompliance, if identified, are reported to control owners, process owners, and other personnel who are in the position to take corrective action.

Control Activities

Databricks has implemented specific policies and procedures to help carry out management's directives. These control activities, whether automated through use of technology (i.e., IT general

computer or application controls) or manual controls, have a range of objectives, and are applied at various organizational and functional levels to help Databricks achieve its service commitments and system requirements based on the trust services criteria relevant to security, availability, and confidentiality.

Although the applicable trust services criteria and the HIPAA security requirements and related controls are presented in Section IV, *Trust Services Criteria, the HIPAA Security Requirements and Breach Notification Requirements, Related Controls, Tests of Controls and Results of Tests,* they are an integral part of Databricks' system description.

Logical and Physical Access

Physical Access

Databricks hosts its application at AWS, Azure, and GCP managed data centers. As such, physical security is carved out from the scope of the description and report.

Logical Access

Databricks has documented security policies around logical access that include access management, data classification, acceptable use, and password management. Policy documents are available to Databricks employees through the Databricks intranet.

Access to the production environment follows the principle of least privilege and is based on business need. Access to systems is protected by authentication and authorization controls. Databricks utilizes an SSO solution with Yubikey MFA to manage access to key systems.

Databricks follows a formal process for managing user accounts and controlling access to resources designed to ensure that access is given based on their roles and the least privilege principle.

Upon notification of an employee termination, HR will initiate the termination process in Workday, which triggers an automated workflow to automatically deprovision the assigned system access of each terminated user in Okta and other systems.

On a quarterly basis, IT performs user access reviews for the in-scope production environments and systems. Appropriate action is taken for any issues identified in the review.

Databricks Access to Production Systems

By default, Databricks personnel do not have access to customer workspaces or to the production environments. Databricks staff may request temporary access to a customer workspace in order to investigate an outage or security event or to support deployment.

To grant secure access, Databricks uses an internal application called Genie. There are Genie instances for AWS, Azure, and GCP, respectively. Genie for AWS and GCP access requires MFA and requires users to be on the Databricks network or Databricks VPN. Genie for Azure requires MFA and requires users to be on the Databricks network, Databricks VPN, or the Microsoft internal support network. Databricks limits the set of users who can access Genie and which types of access may be granted to each user. See the following sections for the types of access.

Access to Web Application

Databricks customer support personnel (or individuals in direct support roles such as Solution Architects) can use Genie to request HTTPS access to the web application to provide support. For customers who deploy on Azure, support personnel also include authorized Azure support personnel.

Databricks support personnel must enter the Databricks web application ID of the customer and a valid Salesforce support ticket identification number. Microsoft support personnel must enter the customer ticket ID, subscription ID, requestor ID, and organization. Support personnel are required to gain and document customer consent before using Genie to access a customer workspace. If Databricks customer support personnel require additional troubleshooting, they create an internal Engineering Support Ticket for the Databricks Engineering Team.

The Databricks Engineering Team can log into Genie to request access to the customer's workspace in the web application for further troubleshooting or emergency support. The Databricks Engineering Team follows the same process as above except they enter the web application ID and an internal Engineering Support Ticket (not a Customer Support Ticket).

Both Databricks support personnel and engineers require a second person approval for customer workspace access. Genie grants web application access through a time-limited access token. After the session time expires, the request process must be repeated.

Access to Internal Core Production Infrastructure Systems

Only personnel in the Databricks Engineering organization who support internal infrastructure can log into Genie and access Databricks core production infrastructure systems. If Databricks personnel outside infrastructure support roles request access to such systems, additional approvals are required. Genie grants internal production system access through a time-limited TLS client certificate. After the session time expires, the request process must be repeated.

Genie Sessions

The default Genie session time for web application access is 60 minutes and infrastructure access is eight hours. However, time limits can also be set in advance to the expected duration of the support session. The maximum time for customer approved workspace login windows can last up to 48 hours.

Genie Access Logs

The Genie application logs all access requests, and the Genie logs are stored for at least a year. Additionally, the Databricks platform logs access in a way that allows auditing of Genie access events using Audit Logs. Customers can optionally receive the Audit Logs for their account in order to review the actions taken and to confirm the integrity and security of the system. For AWS customers, access to Audit Logs is part of the Premium tier and Enterprise tier. For Azure customers, access to Audit Logs requires the Premium tier. For GCP customers, access to Audit Logs is part of the Premium tier.

Customer Access to Web Application

Customers have the responsibility to manage their own Databricks application-level access and resource access using permissions that administrators may assign to individual users or groups. Databricks does not have access to user credentials.

AWS

Depending on how the customer creates their Databricks account, the customer may create and submit their Databricks account administrator credentials. In this case, credentials are encrypted in transit with HTTPS using TLS 1.2 or 1.3. If the sales team or other team initiates signup, the new customer gets a temporary credential via email and sets their password on first login.

For user login on Databricks hosted on AWS, this initial user account uses Databricks native authentication, which is the default non-SSO user authentication. Administrators can create other admin or non-admin accounts that use Databricks native authentication. The account owner and any new admin users can continue to use native authentication for those user accounts even if SSO support is added later. However, if SSO is added later, non-admin users must use SSO login for the web application. Credentials for Databricks native authentication are stored as passwords that are salted and hashed using PBKDF2 with the HMAC SHA1 function. It is stored in the central account workspace directory that manages user membership for workspaces and users across all geographies of the AWS system.

Enterprise security typically requires central authentication using SSO with an external directory. Customers can optionally configure SSO to authenticate users using their existing Identity Provider (IdP). For AWS customers, SSO users securely sign-in using IdPs that comply with the industry-standard SAML 2.0 protocol. Databricks supports the most popular SAML 2.0 IdPs including Okta, Google for Work, OneLogin, Ping Identity, and Microsoft Windows Active Directory. Customers can optionally configure their SAML IdP to use MFA. Databricks does not have access to the user's MFA credentials.

For REST API authentication, Databricks provides built-in revocable personal access tokens that are created through the web application user interface. Individual tokens have their own lifespan, including revocation and optional expiration dates. Additionally, users who authenticate with Databricks native authentication (non-SSO authentication) have the option to authenticate to REST APIs using a username and password. However, it is recommended to use revocable user security tokens instead of a username and password because of the value of token revocation and optional expiration dates.

Databricks also supports the System for Cross-domain Identity Management (SCIM) protocol, which is typically used in conjunction with SSO. SCIM is a standard for automating the exchange for user identity information between identity domains or IT systems for automatic provisioning and deprovisioning of users. The Databricks SCIM REST APIs also allow external systems to create groups and assign group membership. Alternatively, customers can also invoke the Databricks SCIM REST API directly to manage provisioning.

Azure

Azure Databricks always uses SSO authentication using Azure Active Directory using OpenID Connect. An important security benefit of SSO is that Azure Databricks does not have access to user passwords or other secure credentials used by MFA. By default, customers can add (provision) individual users

in Azure Databricks in the Admin page using their email address, but new users must be part of the Azure Active Directory account to log in.

Azure Databricks can also use REST API authentication. Azure Databricks provides built-in revocable user security tokens that are created through the web application or API. These are called personal access tokens (PATs). Tokens have their own lifespan, including revocation and optional expiration dates. Without token management, when token-based authentication is enabled, workspace users can choose to generate and use tokens that authenticate to the Databricks REST API.

Azure Databricks also supports the SCIM protocol, allowing customers to synchronize Azure Active Directory with the directory in Azure Databricks. This benefits customer security in three primary ways: (1) when they remove a user, the user is automatically removed from Azure Databricks; (2) users can be disabled temporarily via SCIM, often used for soft lockouts or for investigations; and (3) groups and roles are automatically synchronized.

GCP

Databricks workspace users authenticate with their Google Cloud Identity account (or GSuite account) using Google's OAuth 2.0 implementation, which conforms to the OpenID Connect spec and is OpenID certified. Databricks provides the OpenID profile scope values in the authentication request to Google. Optionally, customers can configure their Google Cloud Identity account (or GSuite account) to federate with an external SAML 2.0 IdP to verify user credentials. Google Cloud Identity can federate with Azure Active Directory, Okta, Ping, and other IdPs. However, Databricks only directly interacts with the Google Identity Platform APIs. There are two pathways for a workspace user to log in to a workspace:

- All users can use the workspace URL directly.
    - Both non-admin users and admin users (account owners) can use the workspace URL directly. The user authenticates to the Databricks control plane through its integration with Google Cloud Identity OAuth 2.0 implementation.
- Admin users (account owners) can additionally use the Google Cloud console to access the workspace.
    - Admin users (account owners) authenticate with Google Identity OAuth 2.0 in the Account Console. The Account Console offers a list of available workspaces to choose from. The user is redirected to the workspace login page with an authentication token. If the token is accepted, the user is not prompted to log in again. On the first login, the user will be challenged to consent to OAuth scopes.

Customers can optionally use the REST APIs for SCIM, which is typically used in conjunction with SSO. SCIM is a standard for automating the exchange of user identity information between identity domains or IT systems for automatic provisioning and deprovisioning of users. The Databricks SCIM REST APIs also allow external systems to create groups and assign group membership. If the customer configures Google Cloud Identity to federate with an external IdP, that IdP may have built-in SCIM integrations. Customers can also directly invoke the Databricks SCIM REST API directly to manage user and group provisioning.

More information can be found in Databricks product documentation.

System Operations

Backups

Databricks leverages the database backup and recovery services of the cloud service provider for data that resides in the Databricks-managed accounts. The database backups are scheduled and performed automatically daily. The backups are stored in AWS, Azure, or GCP with access restricted to authorized employees. Backup and restoration procedures are tested at least annually.

For Customer-managed storage, the customer is responsible for backing up, securing access to, and encrypting customer data in the AWS S3 bucket, Azure Blob storage, or Google GCS bucket for their account. Databricks is not responsible for backups of these data or any other customer data for customer-managed storage. Databricks provides customers with the ability to back up and restore their notebook data within the Databricks Control Plane so that they can selectively restore data.

Automated backup systems are in place to perform scheduled replication of production data and systems at predefined intervals.

Disaster Recovery and Continuity

Databricks has developed business continuity and disaster recovery plans that are reviewed and communicated to relevant team members on an annual basis. These plans are also tested on an annual basis.

Databricks performs a Business Impact Assessment (BIA) that covers critical services, supporting infrastructure, process, and critical business functions to assess the impact of a disaster.

Incident Management

Databricks has implemented incident response procedures that are designed to efficiently and effectively manage unexpected incidents impacting the business including breach notification requirements as mandated by HITECH. Databricks utilizes an incident response platform and a ticketing system to assign tasks and track incidents to resolution. When an event related to security, availability, or confidentiality is reported or detected, operations personnel examine the issue, create a security incident ticket when needed, and investigate the issue. If the outcome of the investigation is not a false positive, operations personnel will assign the event a severity score and may involve necessary individuals from other teams to resolve the issue. All Sev0 incidents require a mandatory and extended postmortem. The postmortem focuses on the correctness of the root cause(s) assessment, systemic problems that led to the root cause(s), process improvement for incident handling, and post-incident review.

Security incident management policies are communicated to employees and incident response capabilities are tested on at least an annual basis.

Performance Monitoring

Databricks monitors the health of Databricks managed production systems and the capacity utilization of computing infrastructure to ensure that service delivery matches SLAs. Databricks evaluates the need for additional infrastructure capacity in response to growth of existing customers and/or the addition of new customers. In the event that monitored systems exceed a predefined

threshold, an alert will be generated automatically and notify the corresponding engineering teams for further investigation and remediation, if needed.

Change Management

Methodology

Engineering at Databricks follows an Agile development methodology using a continuous integration and continuous deployment process. Changes to customer impacting services are tracked, reviewed, tested, and approved.

Release Management

There are two types of releases: Databricks Control Plane release (changes made to the Control Plane) and Databricks Runtime release (changes made to the Data Plane). Databricks releases for the multitenant environments are deployed through independent release pipelines that are managed by Service Teams. For example, webapp service team, apiproxy service team, job service team, etc. Service Teams are responsible for their own releases and release processes. Release cadence could be every two weeks or more frequent depending on each service team's needs. Deployment to the single-tenant Control Plane follows a bi-weekly train release schedule. Changes are typically pushed into production in a phased deployment to limit the blast radius of any outages starting with the lowest impact sites.

Code versioning software, GitHub, is used to track and provide control over changes to source code. The software allows development personnel to check out code and modify it locally on their computer to ensure the production code will not be affected during the development process. Each piece of code that is checked back in is assigned a different version number which allows users to rollback to previous versions if changes impair system operations. The ability to modify source code within the versioning software is restricted to authorized personnel. Development and testing environments are logically separated from production and customer data is not used for testing purposes unless authorized by the customer. The ability to promote changes in the production environment is restricted to each service team.

Pull requests have supporting engineering tickets or design documents, based on the size of the change. Once a pull request is ready, peer review is performed, and review comments are addressed, the pull request must be approved by a functional owner for that area. Approval is documented in GitHub and automatically validated.

A continuous delivery platform, Spinnaker, is used to orchestrate the continuous delivery pipelines. Jenkins/Deployment Service is used to execute jobs that would conduct the deployment.

Customer-facing feature changes are published as release notes on Databricks websites and available to all customers.

Risk Mitigation

Network Security

Databricks uses AWS security groups, Azure network security groups, and GCP VPC firewall rules to filter unauthorized inbound network traffic from the internet and deny network connections that are not explicitly authorized (deny all, allow by exception). Administrative access to AWS, Azure,

and GCP is restricted to authorized employees. Changes to the AWS, Azure security groups, and GCP firewall rules follow the Databricks change management process and are tracked in a ticketing system.

AWS GuardDuty is deployed as an Intrusion Detection System (IDS) to monitor and analyze production systems for possible or attempted security breaches. Alerts are automatically triaged through PagerDuty. For identified incidents, tickets are opened to track actions taken. Intrusion detection on the Azure side is monitored and managed by Microsoft. GCP Event Threat Detection is a Google Cloud built-in service as an IDS to continuously monitor and analyze production systems to identify threats in near-real time. Alerts are reviewed by the Security Detection and Response Team. For identified incidents, tickets are opened to track actions taken.

Vulnerability Management

Databricks installs Qualys agents on Control Plane and Serverless hosts and as part of the deployment process to perform vulnerability scanning on at least a weekly basis or as needed. Web application vulnerability scans are performed twice a month. Databricks also engages an independent third party to conduct a bug bounty program to discover bugs and vulnerabilities on a continual basis. Additionally, third-party penetration testing is performed on at least an annual basis for each cloud. The penetration testing scope is determined based on Databricks areas of risk and compliance requirements.

Findings from the vulnerability scans and penetration tests are reviewed, validated, and addressed if needed. Vulnerabilities are remediated according to Databricks defined SLAs; 14 days for critical, 30 days for high, 60 days for medium, and as needed for low. Vulnerabilities that cannot be addressed and remediated within the SLA are required to go through an exception process to obtain approval.

Databricks has implemented a patch management process during which patches are evaluated and applied in accordance with the Databricks change management process.

Description of the Additional Controls Relevant to the Availability Trust Services Category

Refer to the *System Operations* and *Risk Mitigation* sections above.

Description of the Additional Controls Relevant to the Confidentiality Trust Services Category

Refer to the *Data* section above, specifically its subsections *Collection*, *Handling and Storage*, *Release/Disclosure*, and *Modification*.

Description of the Additional Controls Relevant to the HIPAA Security and Breach Notification Requirements

Databricks has developed a health information security management program to meet the information security and compliance requirements related to Lakehouse Platform services and its customer base. The program incorporates the elements of HIPAA and HITECH. The description below is a summary of safeguards that Databricks has implemented to adhere to the applicable components of HIPAA security requirements and the breach notification requirements of HITECH.

Administrative Safeguards

Policies and procedures designed to show how Databricks complies with the act:

- Management has adopted a written set of health information security policies and designated the information security officer to be responsible for developing and implementing the required policies and procedures.
- Procedures address access authorization, establishment, modification, and termination.
- Documented incident response policies for reporting security incidents are in place to guide employees in the identifying and reporting of security incidents.
- Business continuity plans are documented to enable continuation of critical business processes in the event of an emergency.
- Privileged administrative access to systems is restricted to authorized individuals.
- Automated backup systems are in place to perform scheduled replication of production data and systems at predefined intervals.
- Next-generation antivirus software is utilized to protect against all types of attacks from commodity malware to sophisticated attacks on endpoint devices.

Physical Safeguards

Controlling physical access to protected data:

- Documented physical security policies and procedures are in place to guide personnel in physical security administration.
- Physical access procedures are in place to restrict access, log visitors, and terminate access to the office facility.
- Inventory listings are utilized to track and monitor media devices.
- Data destruction procedures are in place to guide the secure disposal of data.

Technical Safeguards

Controlling access to computer systems and enabling covered entities to protect communications containing PHI transmitted electronically over open networks from being intercepted by anyone other than the intended recipient:

- Access to in-scope systems is restricted to authorized personnel based on a valid user account and password.
- Systems are configured to enforce predetermined thresholds to lock user sessions due to invalid login attempts.
- Security monitoring applications and manual reviews are utilized to monitor and analyze the in-scope systems for possible or actual security breaches.
- Encryption technology is in place to help protect customer data.

Organizational Safeguards

Adherence to policies and procedures regarding to PHI documentation availability, as well as documentation retention:

- Documented policies address the confidentiality threshold of PHI documents and the length of time they should be retained before being destroyed.
- Contractual responsibilities by subparts of an organization are written and maintained in contracts.
- Separation of duties is existent in order to protect confidentiality, availability, and integrity of PHI.
- Ensure that only appropriate parties gain access to PHI internally and external to the organization.

Breach Notification

A business associate shall, following the discovery of a breach of unsecured protected health information, notify the covered entity of such breach:

- Documented policies and procedures are in place to guide personnel in notifying the covered entity upon discovery of a breach.
- Documented policies and procedures are in place to guide personnel in responding to discovery of a breach.
- Documented policies and procedures require disclosure of the unsecured protected health information and include, to the extent possible, the identification of each individual and a description of the event.
- Documented policies and procedures are in place to guide personnel in the exception processes of delaying and documenting notifications.
- Documented policies and procedures are in place to guide personnel in documentation of administrative requirements for demonstrating that all notifications were made as required.

Complementary Subservice Organization Controls

In some instances, a service organization's controls cannot provide reasonable assurance that its service commitments and system requirements were achieved without the subservice organizations performing certain activities in a defined manner. Such activities are referred to as complementary subservice organization controls (CSOCs). The following CSOCs are those controls that Databricks' management assumed, in the design of the system, would be implemented by a subservice organization and are necessary, in combination with controls at Databricks, to provide reasonable assurance that the service organization's service commitments and system requirements are achieved.

Number	CSOC	Applicable Trust Services Criteria and HIPAA Security and Breach Notification Requirements
Amazon Web Services, Microsoft Corporation, Google LLC, and Okta, Inc.		
1.	Physical access to facilities housing the production servers and other system components is restricted to authorized personnel only.	CC6.4, §164.310(a)(1), §164.310(a)(2)(ii), §164.310(a)(2)(iii), §164.310(a)(2)(iv)
2.	Physical access to data centers is approved by an authorized individual.	
3.	Physical access is revoked in a timely manner of the employee or vendor record being deactivated.	
4.	Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.	
5.	Logs and maintenance records for physical access to data centers are retained for a defined period.	
6.	Physical access points to server locations are recorded by closed circuit television cameras. Images are retained for a defined period, unless limited by legal or contractual obligations.	
7.	Physical access points to server locations are managed by electronic access control devices.	
8.	The entity implements logical access policies, security software, infrastructure, and architectures over protected information assets to protect them from unauthorized access and security events.	CC6.1, CC6.6, §164.312(a)(1), §164.312(a)(2)(i) §164.312(a)(2)(iii), §164.312(a)(2)(iv), §164.312(b), §164.312(c)(2), §164.312(d), §164.312(e)(1), §164.312(e)(2)(ii)
9.	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	CC6.2, §164.308(a)(3)(ii)(C), §164.308(a)(4)(ii)(B) §164.308(a)(5)(ii)(D), §164.312(a)(1), §164.312(a)(2)(i), §164.312(a)(2)(iii)
10.	Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.	§164.308(a)(3)(ii)(A)
11.	Industry standard encryption algorithms are used to manage production infrastructure.	CC6.1, CC6.7, §164.312(a)(2)(iv), §164.312(e)(2)(ii)

Number	CSOC	Applicable Trust Services Criteria and HIPAA Security and Breach Notification Requirements
12.	External and internal security vulnerability assessment and penetration testing is performed on an annual basis.	CC7.2, §164.308(a)(1)(ii)(A), §164.308(a)(1)(ii)(B)
13.	Procedures for evaluating security events and managing security incidents are implemented. Security incidents are communicated as appropriate.	CC7.3, CC7.4, CC7.5, §164.308(a)(1)(ii)(D), §164.308(a)(6), §164.308(a)(6)(ii)
14.	Changes (including emergency/nonroutine) to production infrastructure and applications are recorded, authorized, tested, and approved prior to migration.	CC8.1, §164.312(e)(2)(i)
15.	Environmental protections of systems at the data center are designed, developed, implemented, operated, maintained, and monitored to meet availability commitments and requirements.	A1.2, A1.3, §164.308(a)(7), §164.308(a)(7)(ii)(A), §164.308(a)(7)(ii)(B), §164.308(a)(7)(ii)(C), §164.308(a)(7)(ii)(D)
16.	Data centers are protected by fire detection and suppression systems.	
17.	Data centers are air conditioned to maintain appropriate atmospheric conditions. Personnel and systems monitor and control air temperature and humidity at appropriate levels.	
18.	Data centers electrical power systems are designed to be fully redundant and maintainable without impact to operations and Uninterruptible Power Supply units provide back-up power in the event of an electrical failure for critical and essential loads in the facility.	
19.	Data centers have generators to provide backup power in case of electrical failure.	
20.	Preventative maintenance is performed on environmental protections on at least an annual basis.	
21.	Data centers contingency plan (e.g., disaster recovery plan, business continuity plan, etc.) is in place. The contingency plan is reviewed and tested on at least an annual basis.	
22.	Access to encryption keys and recovery key materials is appropriately restricted.	CC6.1, CC6.7, §164.312(a)(1), §164.308(a)(3)(ii)(A), §164.312(a)(2)(iv), §164.312(e)(2)(ii)

Number	CSOC	Applicable Trust Services Criteria and HIPAA Security and Breach Notification Requirements
Microsoft Corporation and Google LLC		
23.	Databases are encrypted, securely backed up, and stored in separate data center facilities.	CC6.1, CC6.6, CC7.5, A1.2, C1.1, §164.308(a)(7)(ii)(A) §164.310(a)(2)(i) §164.310(d)(2)(iv) §164.312(a)(2)(iv), §164.312(c)(1), §164.312(e)(2)(ii)

Databricks management, along with the subservice organizations, define the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as SLAs. In addition, Databricks performs monitoring of the subservice organization controls, including the following procedures:

- Holding periodic discussions with vendors and subservice organizations.
- Reviewing attestation reports over services provided by critical cloud service vendors and subservice organizations annually.
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organizations.

User Entity Responsibilities

User entities must perform specific activities in order to benefit from Databricks' services. These activities may affect the user entity's ability to effectively use Databricks' services but do not affect the ability of Databricks to achieve its service commitments and system requirements. These activities may be specified in agreements between user entities and Databricks, user manuals, and/or other communications. These activities are referred to as user entity responsibilities (UERs).

UERs are listed in the following table. They are the responsibility of the user entities of the system and are expected to be in operation at user entities to complement Databricks' controls. The list of UERs does not represent a comprehensive set of all the controls that should be employed by user entities. Other controls may be required at user entities.

Number	UER
1.	Customers are responsible for setting up separate development and production Lakehouse Platform workspaces to isolate the production work from development, where applicable.
2.	Customers are responsible for implementing an SSO solution and MFA, where applicable, for controlling user access to the Lakehouse Platform.

Number	UER
3.	If available in their subscription tier, customers are responsible for enabling Lakehouse Platform audit log delivery features and implementing appropriate monitoring and incident response processes.
4.	Customers are responsible for reviewing Lakehouse Platform audit logs of actions performed by the customer support personnel, if applicable.
5.	Customers are responsible for making any changes to data stored within the Lakehouse Platform, where applicable.
6.	Customers are responsible for (1) backing up data that is stored in customer-controlled storage locations (e.g., AWS S3 bucket/Azure Blob Storage/Google GCS bucket); and (2) backing up notebooks with tools provided by Databricks within the product. For the data that is backed up by customers, customers are responsible for retaining the data for a specified retention period to protect from erasure or destruction.
7.	Customers are responsible for developing their disaster recovery and business continuity plans that address the inability to access or use Databricks services.
8.	Customers are responsible to determine based on their needs, including on the relative sensitivity of the data they are processing, which product tier (and features) are appropriate for their intended uses.
9.	Customers are responsible for managing their organization's instance(s) of the Lakehouse Platform through any customized security solutions or automated processes using setup features, application development tools, and API integration tools.
10.	Customers are responsible for ensuring that authorized users are appointed as organizational administrators and the authorized users should follow a defined logical access management process to manage and protect the admin account user credentials to administer the Lakehouse Platform, where applicable. Customers are responsible for appropriately managing user access to the Lakehouse Platform and customer managed AWS, Azure, or GCP account(s).
11.	Customers are responsible for data classification and the implementation of encryption features available where deemed necessary by customer-defined requirements. Additionally, customers are responsible for their choices of libraries to prevent the inadvertent transmission of sensitive data (including PHI) over the wire in an unencrypted fashion.
12.	Customers are responsible for securing and protecting account credentials and security tokens for REST API access.
13.	Customers are responsible for securing and protecting the encryption keys that are stored in the customer managed environment, where applicable.

Number	UER
14.	Customers are responsible for encrypting their sensitive data at rest (e.g., S3 bucket encryption, Azure Blob storage encryption, GCS bucket encryption) that is used and processed by the Databricks services. Customers are responsible for proper use of encryption tools including but not limited to up to date Web browsers and REST API client tools when accessing Lakehouse Platform services (e.g., use of tools that properly implement TLS 1.2 encryption). Where applicable, customers are responsible for encrypting data in transit to Databricks personnel or Microsoft personnel (for Azure Databricks customers) over the network for interactions outside of the Lakehouse Platform services (e.g., using TLS 1.2 encryption).
15.	Where applicable, customers are responsible for authorizing temporary access to customer support personnel from Databricks or Microsoft Azure (e.g., for technical support and troubleshooting).
16.	Customers are responsible for notifying Databricks of any unauthorized use of any password or account or any other known or suspected breach of security related to the use of the Lakehouse Platform.
17.	Customers are responsible for communicating issues and incidents related to security, availability, and confidentiality to the support personnel (Databricks and Microsoft Azure, as appropriate) through identified channels.

IV. Trust Services Criteria, HIPAA Security and Breach Notification Requirements, Related Controls, Tests of Controls, and Results of Tests

Trust Services Criteria, HIPAA Security and Breach Notification Requirements, Related Controls, Tests of Controls, and Results of Tests

This report is intended to provide information to the management of Databricks, user entities of Databricks' Lakehouse Platform Services system on AWS, Azure, and GCP, and prospective user entities, independent auditors, and practitioners providing services to those entities, who have a sufficient understanding to consider it, along with other information, including information about the controls implemented by the user entities. This report is intended to provide information about the suitability of the design and operating effectiveness of controls implemented to achieve the service commitments and system requirements based on the criteria relevant to security, availability and confidentiality (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA *Trust Services Criteria*, and the HIPAA security and breach notification requirements throughout the period October 1, 2022 to June 30, 2023.

The examination was performed in accordance with attestation standards established by the AICPA, specifically, AT-C Sections 105 and 205 and the guidance contained in the AICPA Guide, *SOC 2 Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy*. It is each user entity's responsibility to evaluate this information in relation to its own system of internal control in order to assess its system of internal control. If an effective system of internal control is not in place at user entities, Databricks' controls may not compensate for such weaknesses.

This description is intended to focus on Databricks' controls surrounding the system throughout the period October 1, 2022 to June 30, 2023; it does not encompass all aspects of the services provided or controls performed by Databricks. Unique processes or control situations not described in the report are outside the scope of this report.

Tests of Controls

Our examination of the description of the service organization's system and the suitability of the design and operating effectiveness of controls to achieve the related service commitments and system requirements, based on the applicable trust services criteria and the HIPAA security and breach notification requirements stated in the description, involved performing procedures to obtain evidence about the presentation of the description of the system in accordance with the description criteria and the suitability of the design and operating effectiveness of those controls to achieve the related service commitments and system requirements, based on the applicable trust services criteria and the HIPAA security and breach notification requirements stated in the description. Our procedures included assessing the risks that the description is not presented in accordance with the description criteria and that the controls were not suitably designed or operating effectively to achieve the related service commitments and system requirements based on the applicable trust services criteria and the HIPAA security and breach notification requirements stated in the description.

Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the related service commitments and system requirements based on the applicable trust services criteria and the HIPAA security and breach

notification requirements stated in the description were achieved throughout the period October 1, 2022 to June 30, 2023.

Our tests of controls were designed to cover a representative number of activities throughout the period October 1, 2022 to June 30, 2023, for each of the controls listed in Section IV, which are designed to achieve the related service commitments and system requirements based on the applicable trust services criteria and the HIPAA security and breach notification requirements. In selecting particular tests of controls, we considered: (a) the nature of the controls being tested, (b) the types and competence of available evidential matter, (c) the criteria to be achieved, (d) the assessed level of control risk, and (e) the expected efficiency and effectiveness of the test.

BDO USA, P.A.'s testing of controls was restricted to the controls specified by Databricks in Section IV, and was not extended to controls in effect at user entities or other controls that were not documented as tested under each control criteria listed in Section IV. The description of BDO USA, P.A.'s tests of controls and the results of those tests are presented in this section of the report. The description of the tests of controls and the results of those tests are the responsibility of BDO USA, P.A. and should be considered information provided by BDO USA, P.A.

The basis for all tests of operating effectiveness includes inquiry of the individual(s) responsible for the control. As part of our testing of each control, we inquired of the individual(s) to determine the fairness of the description of the control and to evaluate the design and implementation of the control. As part of our inquiries, we also gained an understanding of the knowledge and experience of the personnel managing the control(s) and corroborated evidence obtained as part of other testing procedures. While inquiries were performed for every control, our inquiries were not listed individually for every control activity tested and shown in Section IV.

Additional testing of the control activities may have been performed using the following methods:

Method	Description
Inquiry	Inquired of appropriate personnel and corroborated responses with management.
Observation	Observed the application, performance, or existence of the specific control(s), as represented by management.
Inspection	Inspected documents and records indicating performance of the control.
Reperformance	Reperformed the control or processing application to ensure the accuracy of its operation.

When using information produced by the service organization, we evaluated whether the information was sufficiently reliable for our purposes by obtaining evidence about the accuracy and completeness of such information and evaluating whether the information was sufficiently precise and detailed for our purposes.

Presentation of Controls

Controls presented in the following tables may appear more than once if a control supports the achievement of multiple criteria.

Databricks Control Domains

The controls included in the tables below depict Databricks' controls which are related to the applicable Security, Availability, and Confidentiality criteria and the HIPAA Security and Breach Notification Requirements. Each control is assigned a unique control number indicated as the Control Number in the tables that follow. Certain control activities support multiple criteria or requirements. In instances where a control supports multiple criteria, the control number does not change, and the unique control number is referenced.

Control domains are identified as follows:

- Asset Management (AST)
- Business Continuity & Disaster Recovery (BCD)
- Capacity & Performance Planning (CAP)
- Change Management (CHG)
- Compliance (CPL)
- Configuration Management (CFG)
- Continuous Monitoring (MON)
- Cryptographic Protections (CRY)
- Data Classification & Handling (DCH)
- Endpoint Security (END)
- Human Resources Security (HRS)
- Identification & Authentication (IAC)
- Incident Response (IRO)
- Mobile Device Management (MDM)
- Network Security (NET)
- Physical & Environmental Security (PES)
- Project & Resource Management (PRM)
- Risk Management (RSK)
- Secure Engineering & Architecture (SEA)
- Security & Privacy Governance (GOV)
- Security Awareness & Training (SAT)
- Technology Development & Acquisition (TDA)
- Third-Party Management (TPM)
- Vulnerability & Patch Management (VPM)

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
Common Criteria Related to Control Environment					
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	HRS-06	Employees and contractors are required to sign appropriate agreements, that include confidentiality requirements, prior to being granted access to Databricks systems.	Inspected signed agreements for a selection of new hires and contractors to determine whether they signed appropriate agreements including confidentiality requirements before being granted access to systems.	No exceptions noted.
		HRS-07	A policy exists that establishes sanctions for personnel misconduct.	Inspected the Sanctions Policy to determine whether sanctions for personnel misconduct are established.	No exceptions noted.
		HRS-504	Databricks' Code of Conduct is in place and made available to all employees on the intranet.	Inspected the Code of Conduct and the Databricks' intranet to determine whether the Code of Conduct was documented and accessible.	No exceptions noted.
		HRS-505	All contractors with Databricks accounts and employees are required to review and acknowledge the security policy upon hire and at least once per year.	Inspected the security and privacy training course material and certifications for a selection of new hires and contractors to determine whether the security policy was acknowledged within the training upon hire.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
Common Criteria Related to Control Environment					
				Inspected the security and privacy training course material and certifications for a selection of employees and contractors to determine whether the security policy was acknowledged at least once per year.	No exceptions noted.
		SAT-02	All contractors with Databricks accounts and employees are required to take security and privacy training upon hire and at least once per year.	Inspected the security and privacy training certifications for a selection of new hires and contractors to determine whether the employees and contractors completed the training upon hire.	No exceptions noted.
				Inspected the security and privacy training certificates for a selection of contractors and employees to determine whether the training was completed on an annual basis.	No exceptions noted.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	GOV-501	The Board of Directors and executive management maintain independence from those that operate the key controls within the environment.	Inspected the Board of Directors and executive management member biographies to determine whether they were independent from those that operate the key controls within the environment.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
Common Criteria Related to Control Environment					
		GOV-504	Executive management meets quarterly with the Board of Directors to discuss the operations of Databricks, including relevant information on internal controls and external assessments.	Inspected the Board of Directors meeting agendas for a selection of quarters to determine whether executive management met with the Board of Directors and discussed the operations of Databricks, including internal controls and external assessments.	No exceptions noted.
CC1.3	Management establishes, with board oversight, structures, reporting lines and appropriate authorities and responsibilities in the pursuit of objectives.	GOV-04	An individual is assigned as CSO with the mission and resources to centrally manage, coordinate, develop, implement, and maintain an enterprisewide security program.	Inspected the organizational chart and the security policy to determine whether the CSO is responsible for the enterprisewide security program.	No exceptions noted.
		GOV-503	A companywide organizational structure is defined to meet Company commitments and system requirements relevant to security, availability, and confidentiality.	Inspected Databricks organizational charts to determine whether it is structured to meet Company commitments and system requirements relevant to security, availability, and confidentiality.	No exceptions noted.
		HRS-03	Security roles and responsibilities are defined in Databricks security policies.	Inspected various information security policies including the Information Security Management System Policy and the Security Program Policy to determine whether security roles and responsibilities have been established and documented.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
Common Criteria Related to Control Environment					
		PRM-03	Resources required for the implementation and management of the security program have been identified and allocated.	Inspected the Information Security Management System Policy and organizational chart to determine whether the implementation and management of the security program have been identified and allocated.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	HRS-03.2	The competency and experience of candidates is evaluated prior to hiring to verify that candidates are qualified and have the necessary skill set.	Inspected the evaluation forms for a selection of new employees to determine whether they were evaluated prior to employment.	No exceptions noted.
		HRS-04	Background checks are completed on new employees, and those new contractors who are issued logical access to systems, as part of the onboarding process.	Inspected the background check results for a selection of new employees and contractors to determine whether a background check was conducted as part of the onboarding process.	No exceptions noted.
		HRS-501	Performance reviews of full-time employees are conducted at least once per year to ensure employee competency and qualification.	Inspected the performance reviews for a selection of current employees to determine whether performance reviews were conducted annually.	No exceptions noted.
		IRO-05	Incident response resources are trained at least annually.	Inspected the incident response training attendee list to determine whether incident response resources were trained at least annually.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
Common Criteria Related to Control Environment					
		SAT-01	A security training and awareness program has been implemented.	Inspected the security training procedure to determine a security training and awareness program has been formally documented and implemented.	No exceptions noted.
		SAT-02	All contractors with Databricks accounts and employees are required to take security and privacy training upon hire and at least once per year.	Inspected the security and privacy training certifications for a selection of new hires and contractors to determine whether the employees and contractors completed the training upon hire.	No exceptions noted.
				Inspected the security and privacy training certificates for a selection of contractors and employees to determine whether the training was completed on an annual basis.	No exceptions noted.
		SAT-03	Developers are required to take security training annually that relates to secure coding techniques.	Inspected the secure coding techniques training certificates for a selection of developers to determine whether developers completed the training on an annual basis.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
Common Criteria Related to Control Environment					
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	HRS-06	Employees and contractors are required to sign appropriate agreements, that include confidentiality requirements, prior to being granted access to Databricks systems.	Inspected signed agreements for a selection of new hires and contractors to determine whether they signed appropriate agreements including confidentiality requirements before being granted access to systems.	No exceptions noted.
		HRS-07	A policy exists that establishes sanctions for personnel misconduct.	Inspected the Sanctions Policy to determine whether sanctions for personnel misconduct are established.	No exceptions noted.
		HRS-501	Performance reviews of full-time employees are conducted at least once per year to ensure employee competency and qualification.	Inspected the performance reviews for a selection of current employees to determine whether performance reviews were conducted annually.	No exceptions noted.
		HRS-505	All contractors with Databricks accounts and employees are required to review and acknowledge the security policy upon hire and at least once per year.	Inspected the security and privacy training course material and certifications for a selection of new hires and contractors to determine whether the security policy was acknowledged within the training upon hire.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
Common Criteria Related to Control Environment					
				Inspected the security and privacy training course material and certifications for a selection of employees and contractors to determine whether the security policy was acknowledged at least once per year.	No exceptions noted.
		SAT-02	All contractors with Databricks accounts and employees are required to take security and privacy training upon hire and at least once per year.	Inspected the security and privacy training certifications for a selection of new hires and contractors to determine whether the employees and contractors completed the training upon hire.	No exceptions noted.
				Inspected the security and privacy training certificates for a selection of contractors and employees to determine whether the training was completed on an annual basis.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
Common Criteria Related to Communication and Information					
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	AST-02	An inventory of assets is maintained.	Inspected the asset inventory listing to determine whether Databricks tracked inventory of production assets hosted in AWS, Azure, and GCP using an asset management tool.	No exceptions noted.
		CPL-03.1	Independent assessors are used to assess the Databricks information security program, including key controls, at least once per year.	Inspected the most recent independent assessors' reports to determine whether Databricks was independently assessed on an at least annual basis.	No exceptions noted.
		MON-03.3	Production servers are configured to log security events, including the actions of privileged users.	Inspected the AWS, Azure, and GCP server build configurations and security event logs for selected servers to determine whether they were configured to enable logging, including the actions of privileged users.	No exceptions noted.
		MON-501	Databricks usage of cloud service data center provider administration platforms is configured to log audit events, including the actions of privileged users.	Inspected the logging configuration and events log for AWS, Azure, and GCP to determine whether they are configured to log audit events, including the actions of privileged users.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
Common Criteria Related to Communication and Information					
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	CPL-02	A Security and Privacy Risk Committee meets at least once per quarter to provide a security oversight function.	Inspected the Security and Privacy Risk Committee meeting minutes for a selection of quarters to determine whether the committee met at least once per quarter to provide a security oversight function.	No exceptions noted.
		CPL-502	Audit reports and certifications are communicated to internal stakeholders and are available to external stakeholders upon request.	Inspected the Security and Privacy Risk Committee meeting minutes for a selection of quarters to determine whether audit reports and certifications were communicated to internal stakeholders.	No exceptions noted.
				Inspected the Databricks internal site to determine whether the audit reports were made available to Databricks Solution Architects for distribution to customers upon request.	No exceptions noted.
		GOV-02	Security policies and procedures are documented, communicated, made available on the internal Databricks network to appropriate personnel, and versions are maintained.	Inspected the internal Databricks network and the security policies and procedures to determine whether they are formally documented, maintained, and made available to Databricks personnel.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
Common Criteria Related to Communication and Information					
				Inspected the annual security policy certification to determine whether the security policy has been communicated as part of the annual security training.	No exceptions noted.
		GOV-05	Measures of performance for the security program are developed and reported.	Inspected the Information Security Management System Effectiveness Measurements Framework and Procedures to determine whether measures of performance for the security program are developed.	No exceptions noted.
				Inspected the Security and Privacy Risk committee meeting minutes for a selection of quarters to determine whether measures of performance were reported.	No exceptions noted.
		HRS-03	Security roles and responsibilities are defined in Databricks security policies.	Inspected various information security policies including the Information Security Management System Policy and the Security Program Policy to determine whether security roles and responsibilities have been established and documented.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
Common Criteria Related to Communication and Information					
		HRS-502	A complaint process and a whistleblower hotline exist for employees to report unethical and misconduct behaviors in a confidential manner.	Inspected the Employee Handbook to determine whether a complaint process and whistleblower hotline exist to report unethical and misconduct behaviors in a confidential manner.	No exceptions noted.
		IRO-02	Information on how to report possible security incidents is made available to Databricks personnel.	Inspected the Databricks intranet and Incident Response documents to determine whether information on how to report possible security incidents is made available.	No exceptions noted.
		IRO-10	Applicable security and privacy incidents are reported to internal stakeholders, affected clients, third parties, and regulatory authorities.	Inspected the Databricks Security Incident Management Procedure to determine whether Databricks has a procedure for reporting applicable security and privacy incidents to internal stakeholders, affected clients, third parties, and regulatory authorities.	No exceptions noted.
				Inspected tickets for a selection of security and privacy incidents to determine whether appropriate stakeholders were notified.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
Common Criteria Related to Communication and Information					
		PRM-01	Security objectives are documented and communicated.	Inspected the Information Security Management System objectives and the Security and Privacy Risk Committee meeting slide deck for a selection of quarters to determine whether security objectives were documented and communicated.	No exceptions noted.
		SAT-02	All contractors with Databricks accounts and employees are required to take security and privacy training upon hire and at least once per year.	Inspected the security and privacy training certifications for a selection of new hires and contractors to determine whether the employees and contractors completed the training upon hire.	No exceptions noted.
				Inspected the security and privacy training certificates for a selection of contractors and employees to determine whether the training was completed on an annual basis.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	CHG-501	Customers are notified of new features and major changes that may affect their usage of the application through release notes.	Inspected the release notes for a selection of months to determine whether customers were notified of new features and major changes.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
Common Criteria Related to Communication and Information					
		CPL-501	Customers using the Databricks managed AWS and GCP environment must agree to a service agreement that includes both their responsibilities as well as Databricks' responsibilities. Customers using the Databricks managed Azure environment must sign an agreement with Microsoft as they are customers of Microsoft, not Databricks. Databricks has an agreement in place with Microsoft.	Inspected the contracts for a selection of new customers on the AWS and GCP platforms to determine whether the service agreements were established which included both the customer and Databricks responsibilities.	No exceptions noted.
				Inspected the agreement in place between Databricks and Microsoft to determine whether contractual provisions are established regarding security, availability, and confidentiality.	No exceptions noted.
		CPL-502	Audit reports and certifications are communicated to internal stakeholders and are available to external stakeholders upon request.	Inspected the Security and Privacy Risk Committee meeting minutes for a selection of quarters to determine whether audit reports and certifications were communicated to internal stakeholders.	No exceptions noted.
				Inspected the Databricks internal site to determine whether the audit reports were made available to Databricks Solution Architects for distribution to customers upon request.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
Common Criteria Related to Communication and Information					
		CPL-503	Changes to commitments and requirements to customers are communicated.	Inspected Databricks public facing website to determine whether changes to security, availability, and confidentiality commitments and requirements were communicated.	No exceptions noted.
		CPL-504	An externally facing customer support system allows customers to report information on failures, issues, incidents, and other concerns.	Inspected the public Databricks website to determine whether an externally facing customer support system is established to allow customers to report information on failures, issues, incidents, and other concerns.	No exceptions noted.
		IRO-10	Applicable security and privacy incidents are reported to internal stakeholders, affected clients, third parties, and regulatory authorities.	Inspected the Databricks Security Incident Management Procedure to determine whether Databricks has a procedure for reporting applicable security and privacy incidents to internal stakeholders, affected clients, third parties, and regulatory authorities.	No exceptions noted.
				Inspected tickets for a selection of security and privacy incidents to determine whether appropriate stakeholders were notified.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
Common Criteria Related to Risk Assessment					
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	CPL-02	A Security and Privacy Risk Committee meets at least once per quarter to provide a security oversight function.	Inspected the Security and Privacy Risk Committee meeting minutes for a selection of quarters to determine whether the committee met at least once per quarter to provide a security oversight function.	No exceptions noted.
		PRM-01	Security objectives are documented and communicated.	Inspected the Information Security Management System objectives and the Security and Privacy Risk Committee meeting slide deck for a selection of quarters to determine whether security objectives were documented and communicated.	No exceptions noted.
		RSK-04.1	A risk register is maintained that facilitates monitoring and reporting of risks.	Inspected the risk register to determine whether it is maintained for monitoring and reporting of risks.	No exceptions noted.
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	RSK-04	A risk assessment is conducted and documented at least annually that includes internal and external threats, likelihood, impact, controls, and level of risk, as well as fraudulent activities and key fraud factors. Risks are ranked and high risks are managed and tracked.	Inspected the annual risk assessment results to determine whether a risk assessment was performed and included threats (e.g., internal, external, and fraud) were identified and assessed for likelihood, impact, controls, and level of risk.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
Common Criteria Related to Risk Assessment					
				Inspected the risk register and associated residual risk rating, and inquired of management, and determined there were no high risks identified.	The circumstances that warrant the operation of this control did not occur during the examination period and, as a result, this test procedure could not be tested.
		RSK-04.1	A risk register is maintained that facilitates monitoring and reporting of risks.	Inspected the risk register to determine whether it is maintained for monitoring and reporting of risks.	No exceptions noted.
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	RSK-04	A risk assessment is conducted and documented at least annually that includes internal and external threats, likelihood, impact, controls, and level of risk, as well as fraudulent activities and key fraud factors. Risks are ranked and high risks are managed and tracked.	Inspected the annual risk assessment results to determine whether a risk assessment was performed and included threats (e.g., internal, external, and fraud) were identified and assessed for likelihood, impact, controls, and level of risk.	No exceptions noted.
				Inspected the risk register and associated residual risk rating, and inquired of management, and determined there were no high risks identified.	The circumstances that warrant the operation of this control did not occur during the examination period and, as a result, this test procedure could not be tested.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
Common Criteria Related to Risk Assessment					
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	RSK-04	A risk assessment is conducted and documented at least annually that includes internal and external threats, likelihood, impact, controls, and level of risk, as well as fraudulent activities and key fraud factors. Risks are ranked and high risks are managed and tracked.	Inspected the annual risk assessment results to determine whether a risk assessment was performed and included threats (e.g., internal, external, and fraud) were identified and assessed for likelihood, impact, controls, and level of risk.	No exceptions noted.
				Inspected the risk register and associated residual risk rating, and inquired of management, and determined there were no high risks identified.	The circumstances that warrant the operation of this control did not occur during the examination period and, as a result, this test procedure could not be tested.
		TPM-08	Independent security audit reports of cloud service data center providers, subprocessors, subcontractors, and critical vendors are reviewed at least once a year. If control deficiencies are disclosed, the impact to Databricks is evaluated.	Inspected the most recent independent security audit report reviews of the cloud service data center providers and a selection of subprocessors, subcontractors, and critical vendors to determine whether they were reviewed and identified deficiencies were evaluated for impact to Databricks, as appropriate.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
Common Criteria Related to Monitoring Activities					
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	CPL-03.1	Independent assessors are used to assess the Databricks information security program, including key controls, at least once per year.	Inspected the most recent independent assessors' reports to determine whether Databricks was independently assessed on an at least annual basis.	No exceptions noted.
		TPM-08	Independent security audit reports of cloud service data center providers, subprocessors, subcontractors, and critical vendors are reviewed at least once a year. If control deficiencies are disclosed, the impact to Databricks is evaluated.	Inspected the most recent independent security audit report reviews of the cloud service data center providers and a selection of subprocessors, subcontractors, and critical vendors to determine whether they were reviewed and identified deficiencies were evaluated for impact to Databricks, as appropriate.	No exceptions noted.
		VPM-07	Third-party penetration testing is conducted on at least an annual basis. Identified vulnerabilities are tracked and remediated according to Company policy.	Inspected the annual penetration test results for the Lakehouse Platform Services system hosted on AWS, Azure, and GCP, and associated remediation tickets to determine whether penetration tests were performed and vulnerabilities were tracked and remediated according to Company policy.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
Common Criteria Related to Monitoring Activities					
		VPM-501	A bug bounty program is established to continually identify vulnerabilities. Identified vulnerabilities are tracked and remediated according to Company policy.	Inspected the bug bounty dashboard to determine whether vulnerabilities were continually identified.	No exceptions noted.
				Inspected the remediation tickets for a selection of vulnerabilities identified from the bug bounty program to determine whether vulnerabilities were tracked and remediated according to Company policy.	No exceptions noted.
CC4.2	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	CPL-502	Audit reports and certifications are communicated to internal stakeholders and are available to external stakeholders upon request.	Inspected the Security and Privacy Risk Committee meeting minutes for a selection of quarters to determine whether audit reports and certifications were communicated to internal stakeholders.	No exceptions noted.
				Inspected the Databricks internal site to determine whether the audit reports were made available to Databricks Solution Architects for distribution to customers upon request.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
Common Criteria Related to Monitoring Activities					
		GOV-504	Executive management meets quarterly with the Board of Directors to discuss the operations of Databricks, including relevant information on internal controls and external assessments.	Inspected the Board of Directors meeting agendas for a selection of quarters to determine whether executive management met with the Board of Directors and discussed the operations of Databricks, including internal controls and external assessments.	No exceptions noted.
		IRO-10	Applicable security and privacy incidents are reported to internal stakeholders, affected clients, third parties, and regulatory authorities.	Inspected the Databricks Security Incident Management Procedure to determine whether Databricks has a procedure for reporting applicable security and privacy incidents to internal stakeholders, affected clients, third parties, and regulatory authorities.	No exceptions noted.
				Inspected tickets for a selection of security and privacy incidents to determine whether appropriate stakeholders were notified.	No exceptions noted.
		RSK-503	Audit nonconformities and the remediation to correct nonconformities, noted during the audits or assessments of security controls, are managed and tracked.	Inspected the corrective action ticket for the only audit nonconformity noted during audits or assessments of security controls to determine whether nonconformities were managed and tracked.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
Common Criteria Related to Monitoring Activities					
		VPM-06	Host images are scanned for vulnerabilities weekly as part of the deployment process. Identified vulnerabilities are risk ranked, tracked, and remediated according to Company policy.	Inspected vulnerability scan configurations to determine whether host images are configured to be scanned at least weekly.	No exceptions noted.
				Observed the subsequent week's vulnerability scan results for a selection of vulnerabilities to determine whether the identified vulnerabilities were remediated according to Company policy and did not appear in the subsequent weeks scan.	No exceptions noted.
		VPM-502	The Databricks web application is scanned for vulnerabilities at least monthly. Identified vulnerabilities are risk ranked, tracked, and remediated according to Company policy.	Inspected the Databricks web application vulnerability scan configuration and the vulnerability scans for a selection of months and the associated tickets to determine whether a vulnerability scan was performed and vulnerabilities were risk ranked, researched, and resolved according to Company policy.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
Common Criteria Related to Control Activities					
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	GOV-502	A suite of controls is maintained to comply with external laws, regulations, industry requirements, and internal information security policies.	Inspected the Databricks suite of controls to determine whether it is maintained to comply with external laws, regulations, industry requirements, and internal information security policies.	No exceptions noted.
		RSK-01	A policy exists that establishes the risk management program and requirements.	Inspected the Information Security Management System Policy to determine whether requirements for the risk management program have been established.	No exceptions noted.
		RSK-04	A risk assessment is conducted and documented at least annually that includes internal and external threats, likelihood, impact, controls, and level of risk, as well as fraudulent activities and key fraud factors. Risks are ranked and high risks are managed and tracked.	Inspected the annual risk assessment results to determine whether a risk assessment was performed and included threats (e.g., internal, external, and fraud) were identified and assessed for likelihood, impact, controls, and level of risk.	No exceptions noted.
				Inspected the risk register and associated residual risk rating, and inquired of management, and determined there were no high risks identified.	The circumstances that warrant the operation of this control did not occur during the examination period and, as a result, this test procedure could not be tested.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
Common Criteria Related to Control Activities					
		RSK-04.1	A risk register is maintained that facilitates monitoring and reporting of risks.	Inspected the risk register to determine whether it is maintained for monitoring and reporting of risks.	No exceptions noted.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	GOV-04	An individual is assigned as CSO with the mission and resources to centrally manage, coordinate, develop, implement, and maintain an enterprisewide security program.	Inspected the organizational chart and the security policy to determine whether the CSO is responsible for the enterprisewide security program.	No exceptions noted.
		GOV-502	A suite of controls is maintained to comply with external laws, regulations, industry requirements, and internal information security policies.	Inspected the Databricks suite of controls to determine whether it is maintained to comply with external laws, regulations, industry requirements, and internal information security policies.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	DCH-01	A policy exists that establishes data classification and data handling requirements.	Inspected the Data Classification and Handling Policy to determine whether requirements have been established and documented.	No exceptions noted.
		DCH-12	A policy exists that prohibits personnel from using removable media to store confidential data.	Inspected the Removable Media Policy to determine whether requirements regarding use of removable media have been established and documented.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
Common Criteria Related to Control Activities					
		END-03	Policies and procedures exist that govern the installation of software on all laptop and desktop computers.	Inspected the Acceptable Use Policy to determine whether policies and procedures that govern the installation of software on all laptop and desktop computers exists.	No exceptions noted.
		GOV-02	Security policies and procedures are documented, communicated, made available on the internal Databricks network to appropriate personnel, and versions are maintained.	Inspected the internal Databricks network and the security policies and procedures to determine whether they are formally documented, maintained, and made available to Databricks personnel.	No exceptions noted.
				Inspected the annual security policy certification to determine whether the security policy has been communicated as part of the annual security training.	No exceptions noted.
		GOV-03	Security policies and procedures are reviewed and approved at least annually or if significant changes occur.	Inspected the DocuSign approval by the CSO to determine whether security policies and procedures have been reviewed and approved within the last year.	No exceptions noted.
		GOV-04	An individual is assigned as CSO with the mission and resources to centrally manage, coordinate, develop, implement, and maintain an enterprisewide security program.	Inspected the organizational chart and the security policy to determine whether the CSO is responsible for the enterprisewide security program.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
Common Criteria Related to Control Activities					
		GOV-506	A policy exists that establishes the requirements for the security program.	Inspected the Security Program Policy to determine whether the policy established requirements for the security program.	No exceptions noted.
		GOV-511	A policy exists that establishes the requirements for the Information Security Management System.	Inspected the Information Security Management System policy to determine whether it addresses Databricks' commitment to ISO 27001.	No exceptions noted.
		HRS-03	Security roles and responsibilities are defined in Databricks security policies.	Inspected various information security policies including the Information Security Management System Policy and the Security Program Policy to determine whether security roles and responsibilities have been established and documented.	No exceptions noted.
		IAC-01	A policy exists that establishes access management and authentication requirements.	Inspected the Access Control and Authentication Policy to determine whether a policy exists that establishes access management and authentication requirements.	No exceptions noted.
		IAC-07	A formal user registration, provisioning, and deprovisioning process is documented.	Inspected the Access Control and Authentication Policy to determine whether a formal user registration, provisioning, and deprovisioning process is documented.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
Common Criteria Related to Control Activities					
		IAC-10.8	Vendor-supplied default passwords are required to be changed as part of the installation process.	Inspected the Databricks Password Policy to determine whether requirements to change vendor-supplied default passwords as part of the installation process is defined.	No exceptions noted.
		MDM-01	A policy exists that establishes the security requirements for user workstations and mobile devices.	Inspected the Workstation and Mobile Device Policy to determine whether it establishes the security requirements for user workstations and mobile devices.	No exceptions noted.
		NET-01	A policy exists that establishes network security requirements.	Inspected the Network Security Policy to determine whether it establishes network security requirements.	No exceptions noted.
		NET-14.5	A policy exists that establishes remote access and teleworking requirements.	Inspected the Remote Access and Teleworking Policy to determine whether it establishes remote access and teleworking requirements.	No exceptions noted.
		TDA-01	A policy exists that establishes security requirements for application development.	Inspected the Application Development Policy to determine whether it establishes the security requirements for application development.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
Common Criteria Related to Control Activities					
		VPM-01	A policy exists that establishes security vulnerability identification, tracking, and remediation requirements.	Inspected the Vulnerability and Patch Management Policy to determine whether the policy establishes security vulnerability identification, tracking, and remediation requirements.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
Common Criteria Related to Logical and Physical Access					
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	AST-02	An inventory of assets is maintained.	Inspected the asset inventory listing to determine whether Databricks tracked inventory of production assets hosted in AWS, Azure, and GCP using an asset management tool.	No exceptions noted.
		AST-06	All laptop and desktop computers are configured to implement a password protected screensaver lockout after ten minutes of inactivity.	Inspected the mobile device management lockout configuration to determine whether laptops and desktops are configured to lockout after ten minutes of inactivity.	No exceptions noted.
		CRY-03	TLS 1.2 is used to protect the confidentiality and integrity of data being transmitted over the internet.	Inspected the TLS certificates for the AWS, Azure, and GCP environments to determine whether TLS 1.2 or greater was implemented to protect the confidentiality and integrity of data being transmitted over the internet.	No exceptions noted.
		CRY-05	Databricks database systems are configured to store information encrypted.	Inspected the AWS database baseline template configuration and the AWS encryption configuration for a selected database to determine whether databases were encrypted, and inspected Azure and GCP vendor backup documentation to determine whether databases were encrypted by default.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
Common Criteria Related to Logical and Physical Access					
		CRY-09	Key management systems are in place to protect the confidentiality, integrity, and availability of keys.	Inspected the key management systems and vaults to determine whether a system is in place to protect the confidentiality, integrity, and availability of keys.	No exceptions noted.
				Inspected the system generated list of administrators who have access to create, delete, or modify keys within the key management systems, the administrators' associated job titles, and inquired of management to determine whether administrative access is restricted to authorized personnel.	No exceptions noted.
		CRY-501	Full disk encryption is enabled on all laptop and desktop computers.	Inspected the MDM encryption settings and the encryption configuration for a selection of computers to determine whether full disk encryption was enabled.	No exceptions noted.
		IAC-02	Users, and processes acting on behalf of users, are uniquely identified.	Inspected a system generated list of all users including service and system accounts to determine whether all accounts were uniquely identified.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
Common Criteria Related to Logical and Physical Access					
				Re-performed an attempt to create a username that already exists in the system to determine whether the username was rejected.	No exceptions noted.
		IAC-08	Access to production servers is limited to authorized users.	Inspected the system generated list of users with access to the production servers, the users' associated job titles, and inquired of management to determine whether their access is appropriate.	No exceptions noted.
		IAC-501	Authentication infrastructure enforces passwords for workstations and SSO applications that comply with Databricks policy for password expiration, length, complexity, and history.	Inspected the workstation and SSO password configuration settings to determine whether they are configured according to the password requirements established in the security policy.	No exceptions noted.
		IAC-503	Access to administer office network infrastructure is limited to authorized users.	Inspected the system generated list of administrators for the office network infrastructure, Palo Alto Networks, the administrators' associated job titles, and inquired of management to determine whether access is limited to authorized users.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
Common Criteria Related to Logical and Physical Access					
		IAC-505	Databricks access to cloud service data center provider administration platforms is limited to authorized users.	Inspected the system generated list of administrators to the cloud service data center provider administration platforms, administrators' associated job titles, and inquired of management to determine whether access is limited to authorized users.	No exceptions noted.
		IAC-506	Access to authentication infrastructure is limited to authorized users.	Inspected the system generated list of users who have access to the authentication infrastructure, inspected the users' job titles, and inquired of management to determine whether access is limited to authorized users.	No exceptions noted.
		MON-03.3	Production servers are configured to log security events, including the actions of privileged users.	Inspected the AWS, Azure, and GCP server build configurations and security event logs for selected servers to determine whether they were configured to enable logging, including the actions of privileged users.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
Common Criteria Related to Logical and Physical Access					
		MON-08	Security event logs are protected from unauthorized access, modification, and deletion.	Inspected the system generated list of users that can access the security logs, their associated job titles, and inquired of management to determine whether security event logs are protected from unauthorized access, modification, and deletion.	No exceptions noted.
		NET-07	VPN sessions require reauthentication after a period of inactivity.	Inspected the VPN configuration for Databricks to determine whether a user is required to reauthenticate after a period of inactivity.	No exceptions noted.
		NET-14	Access to Databricks' networks and production systems require MFA.	Inspected the MFA configuration to determine whether access to Databricks' networks and production systems require MFA.	No exceptions noted.
				Observed a user authenticate to the network and production environments to determine whether MFA is required to gain access.	No exceptions noted.
		SEA-20	Critical system clocks are synchronized to time servers.	Inspected the Network Time Protocol configurations to determine whether critical system clocks are synchronized to time servers.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
Common Criteria Related to Logical and Physical Access					
		TDA-20	Administrative access to software libraries is limited to authorized users.	Inspected the system generated list of users who have administrative access to software libraries, the users' associated job titles, and inquired of management to determine whether access is limited to authorized users.	No exceptions noted.
		TDA-501	The application code, system design, and the platform architecture isolate processing of different tenant requests in their own context and prevent users from accessing data of other customers.	Inspected the configuration for multitenant databases to determine whether the system is designed to prevent users from accessing data of other customers.	No exceptions noted.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	IAC-07.2	User access is revoked within 24 hours after termination of employment or contract.	Inspected access termination documentation for a selection of separated employees and contractors to determine whether access was removed within 24 hours.	No exceptions noted.
		IAC-17	User access reviews are performed at least quarterly and appropriate action is taken.	Inspected Databricks user access review for a selection of quarters and associated access removal tickets to determine whether the access review was conducted and inappropriate access was corrected.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
Common Criteria Related to Logical and Physical Access					
		IAC-502	User access to production systems is authorized by role or approver before temporary credentials with predefined expiration period are granted to access the Databricks web application and production servers in order to provide customer support.	Inspected the Genie confluence page to determine whether temporary credentials with predefined expiration period is granted to authorized users for accessing the Databricks web application and production servers in order to provide customer support.	No exceptions noted.
				Observed an authorized user request access to the Databricks web application and production server using the Genie application to determine whether the request is routed for approval prior to access being granted.	No exceptions noted.
		IAC-507	New hire access is granted through a formal provisioning process.	Inspected the birthright access group rules and new employees access permissions for a selection of new employees to determine whether access is granted based on role and team.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
Common Criteria Related to Logical and Physical Access					
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	IAC-07.2	User access is revoked within 24 hours after termination of employment or contract.	Inspected access termination documentation for a selection of separated employees and contractors to determine whether access was removed within 24 hours.	No exceptions noted.
		IAC-17	User access reviews are performed at least quarterly and appropriate action is taken.	Inspected Databricks user access review for a selection of quarters and associated access removal tickets to determine whether the access review was conducted and inappropriate access was corrected.	No exceptions noted.
		IAC-502	User access to production systems is authorized by role or approver before temporary credentials with predefined expiration period are granted to access the Databricks web application and production servers in order to provide customer support.	Inspected the Genie confluence page to determine whether temporary credentials with predefined expiration period is granted to authorized users for accessing the Databricks web application and production servers in order to provide customer support.	No exceptions noted.
				Observed an authorized user request access to the Databricks web application and production server using the Genie application to determine whether the request is routed for approval prior to access being granted.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
Common Criteria Related to Logical and Physical Access					
		IAC-507	New hire access is granted through a formal provisioning process.	Inspected the birthright access group rules and new employees access permissions for a selection of new employees to determine whether access is granted based on role and team.	No exceptions noted.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	TPM-08	Independent security audit reports of cloud service data center providers, subprocessors, subcontractors, and critical vendors are reviewed at least once a year. If control deficiencies are disclosed, the impact to Databricks is evaluated.	Inspected the most recent independent security audit report reviews of the cloud service data center providers and a selection of subprocessors, subcontractors, and critical vendors to determine whether they were reviewed and identified deficiencies were evaluated for impact to Databricks, as appropriate.	No exceptions noted.
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	AST-09	Media is securely destroyed when it is no longer needed for business or legal reasons.	Inspected the Data Destruction Policy to determine whether destruction policies and procedures are formally documented.	No exceptions noted.
				Inspected media decommissioning tickets and/or third-party destruction certificate for a selection of decommissioned media to determine whether the media was securely destroyed when it was no longer needed for business or legal reasons.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
Common Criteria Related to Logical and Physical Access					
		TPM-08	Independent security audit reports of cloud service data center providers, subprocessors, subcontractors, and critical vendors are reviewed at least once a year. If control deficiencies are disclosed, the impact to Databricks is evaluated.	Inspected the most recent independent security audit report reviews of the cloud service data center providers and a selection of subprocessors, subcontractors, and critical vendors to determine whether they were reviewed and identified deficiencies were evaluated for impact to Databricks, as appropriate.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	CRY-03	TLS 1.2 is used to protect the confidentiality and integrity of data being transmitted over the internet.	Inspected the TLS certificates for the AWS, Azure, and GCP environments to determine whether TLS 1.2 or greater was implemented to protect the confidentiality and integrity of data being transmitted over the internet.	No exceptions noted.
		CRY-05	Databricks database systems are configured to store information encrypted.	Inspected the AWS database baseline template configuration and the AWS encryption configuration for a selected database to determine whether databases were encrypted, and inspected Azure and GCP vendor backup documentation to determine whether databases were encrypted by default.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
Common Criteria Related to Logical and Physical Access					
		CRY-07	Wireless access to the Databricks corporate network is encrypted.	Inspected the wireless access configuration to determine whether access to the Databricks corporate network is encrypted.	No exceptions noted.
		END-05	A host-based firewall is enabled on all laptop and desktop computers.	Inspected the firewall configuration for a selection of computers to determine whether a host-based firewall was enabled.	No exceptions noted.
		NET-02.2	A secure wireless guest network is implemented, separate from the corporate network.	Inspected the configuration for Databricks wireless guest network to determine whether a secure wireless guest network is implemented that is separate from the corporate network.	No exceptions noted.
		NET-03.3	Network Address Translation (NAT) is performed on outbound communications to protect devices' internal IP addresses from exposure.	Inspected the NAT configurations to determine whether NAT is performed on outbound communications to protect devices' internal IP addresses from exposure.	No exceptions noted.
		NET-04	Inbound network traffic from the internet and outbound network traffic to the internet are configured to be restricted through firewalls.	Inspected the firewall configurations to determine whether inbound and outbound traffic are configured to be restricted through firewalls.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
Common Criteria Related to Logical and Physical Access					
		NET-08	A Network Intrusion Detection System (IDS) is used to monitor, detect, and alert on intrusions into the network.	Inspected the IDS configuration to determine whether it is configured to monitor, detect, and alert on intrusions into the network.	No exceptions noted.
		NET-08.1	A Demilitarized Zone (DMZ) separates untrusted networks from trusted networks.	Inspected the DMZ security group configurations to determine whether it is configured to separate untrusted networks from trusted networks.	No exceptions noted.
		NET-12	Remote access to Databricks networks is restricted through an IT managed, encrypted VPN solution.	Inspected the VPN configuration and observed a user remotely VPN to determine whether remote access to the Databricks network and production environments are restricted through an encrypted VPN solution.	No exceptions noted.
				Observed a user attempt to access the Databricks network and production environments without VPN to determine whether the user was denied access.	No exceptions noted.
		NET-14	Access to Databricks' networks and production systems require MFA.	Inspected the MFA configuration to determine whether access to Databricks' networks and production systems require MFA.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
Common Criteria Related to Logical and Physical Access					
				Observed a user authenticate to the network and production environments to determine whether MFA is required to gain access.	No exceptions noted.
		NET-501	Network Access Control is implemented on the Databricks corporate network.	Inspected the Network Access Control Dashboard to determine whether it is implemented on the Databricks corporate network.	No exceptions noted.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	BCD-11.4	Database backups are encrypted.	Inspected the AWS base image configuration and the backup configuration for a selected AWS database to determine whether backups were encrypted, and inspected Azure and GCP vendor backup documentation to determine whether backups are configured to be encrypted by default.	No exceptions noted.
		CRY-03	TLS 1.2 is used to protect the confidentiality and integrity of data being transmitted over the internet.	Inspected the TLS certificates for the AWS, Azure, and GCP environments to determine whether TLS 1.2 or greater was implemented to protect the confidentiality and integrity of data being transmitted over the internet.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
Common Criteria Related to Logical and Physical Access					
		CRY-07	Wireless access to the Databricks corporate network is encrypted.	Inspected the wireless access configuration to determine whether access to the Databricks corporate network is encrypted.	No exceptions noted.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	END-04	Anti-malware software is installed on all laptop and desktop computers and cannot be disabled or altered by unauthorized users.	Inspected the anti-malware software clients for a selection of computers to determine whether anti-malware software was installed and cannot be disabled or altered by unauthorized users.	No exceptions noted.
		END-04.1	Anti-malware software is configured to automatically update on all laptop and desktop computers.	Inspected the anti-malware configuration to determine whether anti-malware software is configured to update automatically on all laptop and desktop computers.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
Common Criteria Related to System Operations					
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	CFG-02	Secure baseline hardening configurations are developed and implemented that are consistent with industry-accepted system hardening standards.	Inspected the secure baseline hardening configurations to determine whether Databricks has developed system hardening configuration guidelines.	No exceptions noted.
		CFG-02.1	Secure baseline hardening configurations are reviewed and updated, if necessary, at least annually.	Inspected the baseline hardening configurations to determine whether they were reviewed and updated at least annually.	No exceptions noted.
		MON-02	The Databricks Secfood application is used as a Security Incident Event Management (SIEM) tool, to support the centralized collection of security related event logs and near real-time analysis and escalation of events.	Inspected the SIEM tool to determine whether it is configured to support the centralized collection of security related event logs.	No exceptions noted.
				Inspected event tickets for a selection of security related events to determine whether events were escalated and resolved.	No exceptions noted.
		MON-03.3	Production servers are configured to log security events, including the actions of privileged users.	Inspected the AWS, Azure, and GCP server build configurations and security event logs for selected servers to determine whether they were configured to enable logging, including the actions of privileged users.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
Common Criteria Related to System Operations					
		MON-08	Security event logs are protected from unauthorized access, modification, and deletion.	Inspected the system generated list of users that can access the security logs, their associated job titles, and inquired of management to determine whether security event logs are protected from unauthorized access, modification, and deletion.	No exceptions noted.
		MON-501	Databricks usage of cloud service data center provider administration platforms is configured to log audit events, including the actions of privileged users.	Inspected the logging configuration and events log for AWS, Azure, and GCP to determine whether they are configured to log audit events, including the actions of privileged users.	No exceptions noted.
		VPM-06	Host images are scanned for vulnerabilities weekly as part of the deployment process. Identified vulnerabilities are risk ranked, tracked, and remediated according to Company policy.	Inspected vulnerability scan configurations to determine whether host images are configured to be scanned at least weekly.	No exceptions noted.
				Observed the subsequent week's vulnerability scan results for a selection of vulnerabilities to determine whether the identified vulnerabilities were remediated according to Company policy and did not appear in the subsequent weeks scan.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
Common Criteria Related to System Operations					
		VPM-502	The Databricks web application is scanned for vulnerabilities at least monthly. Identified vulnerabilities are risk ranked, tracked, and remediated according to Company policy.	Inspected the Databricks web application vulnerability scan configuration and the vulnerability scans for a selection of months and the associated tickets to determine whether a vulnerability scan was performed and vulnerabilities were risk ranked, researched, and resolved according to Company policy.	No exceptions noted.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	IRO-01	A policy and procedure exist that establishes security incident response requirements.	Inspected the Security Incident Management Policy and Procedure to determine whether security incident response requirements are established.	No exceptions noted.
		IRO-501	Security and privacy incidents are documented, tracked, and a root cause analysis is performed.	Inspected the tickets for a selection of security and privacy incidents to determine whether incidents were documented, tracked, and a root cause analysis was performed.	No exceptions noted.
		MON-01	A policy exists that establishes logging and monitoring requirements.	Inspected the Logging and Monitoring Policy to determine whether requirements have been established and are documented.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
Common Criteria Related to System Operations					
		MON-01.5	A process is in place to detect rogue wireless networks if an unauthorized access point is connected to the Databricks corporate network.	Inspected the alert configuration to determine whether there is a process in place to detect rogue wireless networks if an unauthorized access point is connected to the Databricks corporate network.	No exceptions noted.
		MON-02	The Databricks Secfood application is used as a Security Incident Event Management (SIEM) tool, to support the centralized collection of security related event logs and near real-time analysis and escalation of events.	Inspected the SIEM tool to determine whether it is configured to support the centralized collection of security related event logs.	No exceptions noted.
				Inspected event tickets for a selection of security related events to determine whether events were escalated and resolved.	No exceptions noted.
		MON-03.3	Production servers are configured to log security events, including the actions of privileged users.	Inspected the AWS, Azure, and GCP server build configurations and security event logs for selected servers to determine whether they were configured to enable logging, including the actions of privileged users.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
Common Criteria Related to System Operations					
		MON-501	Databricks usage of cloud service data center provider administration platforms is configured to log audit events, including the actions of privileged users.	Inspected the logging configuration and events log for AWS, Azure, and GCP to determine whether they are configured to log audit events, including the actions of privileged users.	No exceptions noted.
		NET-08	A Network Intrusion Detection System (IDS) is used to monitor, detect, and alert on intrusions into the network.	Inspected the IDS configuration to determine whether it is configured to monitor, detect, and alert on intrusions into the network.	No exceptions noted.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	IRO-01	A policy and procedure exist that establishes security incident response requirements.	Inspected the Security Incident Management Policy and Procedure to determine whether security incident response requirements are established.	No exceptions noted.
		IRO-10	Applicable security and privacy incidents are reported to internal stakeholders, affected clients, third parties, and regulatory authorities.	Inspected the Databricks Security Incident Management Procedure to determine whether Databricks has a procedure for reporting applicable security and privacy incidents to internal stakeholders, affected clients, third parties, and regulatory authorities.	No exceptions noted.
				Inspected tickets for a selection of security and privacy incidents to determine whether appropriate stakeholders were notified.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
Common Criteria Related to System Operations					
		IRO-501	Security and privacy incidents are documented, tracked, and a root cause analysis is performed.	Inspected the tickets for a selection of security and privacy incidents to determine whether incidents were documented, tracked, and a root cause analysis was performed.	No exceptions noted.
		MON-02	The Databricks Secfood application is used as a Security Incident Event Management (SIEM) tool, to support the centralized collection of security related event logs and near real-time analysis and escalation of events.	Inspected the SIEM tool to determine whether it is configured to support the centralized collection of security related event logs.	No exceptions noted.
				Inspected event tickets for a selection of security related events to determine whether events were escalated and resolved.	No exceptions noted.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	IRO-06	Incident response capabilities are tested at least annually.	Inspected the incident response plan and test results to determine whether capabilities are tested at least annually.	No exceptions noted.
		IRO-07	Resources are assigned for addressing and coordinating security incident response operations.	Inspected the security incident management procedure to determine whether resources are assigned for addressing and coordinating security incident response operations.	No exceptions noted.
				Inspected tickets for a selection of incidents to determine whether resources were assigned.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
Common Criteria Related to System Operations					
		IRO-10	Applicable security and privacy incidents are reported to internal stakeholders, affected clients, third parties, and regulatory authorities.	Inspected the Databricks Security Incident Management Procedure to determine whether Databricks has a procedure for reporting applicable security and privacy incidents to internal stakeholders, affected clients, third parties, and regulatory authorities.	No exceptions noted.
				Inspected tickets for a selection of security and privacy incidents to determine whether appropriate stakeholders were notified.	No exceptions noted.
		IRO-14	Contacts with applicable regulatory and law enforcement agencies are identified and documented.	Inspected the security incident management procedure and the Contact with Authorities SOP to determine whether contacts with applicable regulatory and law enforcement agencies are identified and documented.	No exceptions noted.
		IRO-501	Security and privacy incidents are documented, tracked, and a root cause analysis is performed.	Inspected the tickets for a selection of security and privacy incidents to determine whether incidents were documented, tracked, and a root cause analysis was performed.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
Common Criteria Related to System Operations					
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	BCD-01	A policy exists that establishes contingency planning and recovery requirements.	Inspected the Business Continuity and Disaster Recovery Policy to determine whether it is formally documented with established requirements.	No exceptions noted.
		BCD-02.2	Business Continuity and Disaster Recovery plans are documented and updated at least annually to ensure the continuation of essential business functions.	Inspected the Business Continuity and Disaster Recovery Plans to determine whether they are reviewed and updated on an annual basis.	No exceptions noted.
		BCD-04	Business Continuity and Disaster Recovery plans are tested at least annually.	Inspected the completed business continuity and the AWS, Azure, and GCP disaster recovery tests to determine whether it was tested and documented on an annual basis.	No exceptions noted.
		BCD-11	Databricks enables recurring backups to ensure the availability of systems.	Inspected the AWS base image configuration and the backup configuration for a selected AWS database, Azure and GCP vendor backup documentation to determine whether backups are enabled to ensure availability of the systems.	No exceptions noted.
		IRO-01	A policy and procedure exist that establishes security incident response requirements.	Inspected the Security Incident Management Policy and Procedure to determine whether security incident response requirements are established.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
Common Criteria Related to System Operations					
		IRO-06	Incident response capabilities are tested at least annually.	Inspected the incident response plan and test results to determine whether capabilities are tested at least annually.	No exceptions noted.
		IRO-501	Security and privacy incidents are documented, tracked, and a root cause analysis is performed.	Inspected the tickets for a selection of security and privacy incidents to determine whether incidents were documented, tracked, and a root cause analysis was performed.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
Common Criteria Related to Change Management					
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	CHG-01	A policy exists that establishes change management requirements.	Inspected the Change Management Policy to determine whether the policy establishes change management requirements.	No exceptions noted.
		CHG-02	Changes to production systems are documented, tracked, tested (e.g., regression, functional, etc.), and authorized prior to implementation.	Inspected the pull request logs for a selection of changes to production systems to determine whether changes were documented, tracked, tested (e.g., regression, functional, etc.), and authorized prior to implementation.	No exceptions noted.
		IAC-509	The ability to promote code to the production environment is limited to authorized individuals based on job roles and responsibilities.	Inspected the code merge approval configuration, system generated list of users who have the ability to promote code to the production environment, the users' associated job titles, and inquired of management to determine whether access was limited to authorized users and requires an independent approval prior to code promotion.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
Common Criteria Related to Change Management					
		TDA-08	Development and test environments are separated from production environments to reduce: • The risks of unauthorized access. • Changes to the operational environment. • Impact to production systems.	Inspected AWS, Azure, and GCP environments to determine whether development and test environments are separated from the production environments.	No exceptions noted.
		TDA-09	Security testing is performed during development, before features are moved to production.	Inspected the scan configurations and testing results for a selected release to determine whether security testing was performed during development, before features are moved to production.	No exceptions noted.
		TDA-10	Test data, not production customer data, is created and used in development and test environments.	Observed the development and test environments and inquired of management to determine whether synthetic test data is generated for use.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
Common Criteria Related to Risk Mitigation					
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	RSK-04	A risk assessment is conducted and documented at least annually that includes internal and external threats, likelihood, impact, controls, and level of risk, as well as fraudulent activities and key fraud factors. Risks are ranked and high risks are managed and tracked.	Inspected the annual risk assessment results to determine whether a risk assessment was performed and included threats (e.g., internal, external, and fraud) were identified and assessed for likelihood, impact, controls, and level of risk.	No exceptions noted.
				Inspected the risk register and associated residual risk rating, and inquired of management, and determined there were no high risks identified.	The circumstances that warrant the operation of this control did not occur during the examination period and, as a result, this test procedure could not be tested.
		RSK-501	Databricks maintains cybersecurity insurance to offset the financial impact of loss events.	Inspected the insurance policy to determine whether Databricks maintains insurance to offset the financial impact of loss events.	No exceptions noted.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	TPM-01	A policy exists that establishes security requirements for using third-party vendors.	Inspected the Third Party Security Policy to determine whether requirements for third-party vendors is established and documented.	No exceptions noted.
		TPM-04.1	A program is in place to manage third party risks. A security assessment is conducted prior to the acquisition or outsourcing of technology-related services.	Inspected the vendor risk management procedures to determine whether a program is in place to manage third party risks.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
Common Criteria Related to Risk Mitigation					
				Inspected the security assessments for a selection of new third-party vendors to determine whether each vendor had completed a security assessment prior to the acquisition or outsourcing of technology-related services.	No exceptions noted.
		TPM-05	Third-party confidentiality, Nondisclosure Agreements, and other contracts that reflect the organization's needs to protect systems and data, are implemented, and updated as necessary.	Inspected the Data Processing Agreement and Master Supplier Agreement templates to determine whether contracts are implemented and updated as necessary.	No exceptions noted.
				Inspected signed contracts for a selection of new third parties to determine whether the confidentiality and Nondisclosure Agreements or other applicable contracts were signed, as necessary.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
Common Criteria Related to Risk Mitigation					
		TPM-08	Independent security audit reports of cloud service data center providers, subprocessors, subcontractors, and critical vendors are reviewed at least once a year. If control deficiencies are disclosed, the impact to Databricks is evaluated.	Inspected the most recent independent security audit report reviews of the cloud service data center providers and a selection of subprocessors, subcontractors, and critical vendors to determine whether they were reviewed and identified deficiencies were evaluated for impact to Databricks, as appropriate.	No exceptions noted.

Additional Criteria Related to the Availability Category

Criteria	Trust Services Criteria	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
Additional Criteria Related to Availability					
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	CAP-01	System capacity and performance are monitored 24/7/365 by Engineering teams. Incidents are documented and tracked to resolution.	Inspected the monitoring software, monitoring alert configurations, and system monitoring procedures to determine whether the system is configured to monitor system capacity and performance 24/7/365.	No exceptions noted.
				Inspected resolution tickets for a selection of system capacity and performance events to determine whether they were documented and tracked to resolution.	No exceptions noted.
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes and recovery infrastructure to meet its objectives.	BCD-02	A BIA is documented and updated at least annually.	Inspected the BIA to determine whether the BIA was documented and updated at least annually.	No exceptions noted.
		BCD-02.2	Business Continuity and Disaster Recovery plans are documented and updated at least annually to ensure the continuation of essential business functions.	Inspected the Business Continuity and Disaster Recovery Plans to determine whether they are reviewed and updated on an annual basis.	No exceptions noted.
		BCD-04	Business Continuity and Disaster Recovery plans are tested at least annually.	Inspected the completed business continuity and the AWS, Azure, and GCP disaster recovery tests to determine whether it was tested and documented on an annual basis.	No exceptions noted.

Additional Criteria Related to the Availability Category

Criteria	Trust Services Criteria	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
Additional Criteria Related to Availability					
		BCD-11	Databricks enables recurring backups to ensure the availability of systems.	Inspected the AWS base image configuration and the backup configuration for a selected AWS database, Azure and GCP vendor backup documentation to determine whether backups are enabled to ensure availability of the systems.	No exceptions noted.
		BCD-11.1	Database restoration testing is performed at least annually.	Inspected the AWS, Azure, and GCP database backup restoration test results to determine whether database restoration testing was performed annually.	No exceptions noted.
		BCD-11.2	Databricks enables backups to separate facilities in cloud service data center provider environments.	Inspected the base image configuration and the backup configuration for a selected AWS Multitenant, Azure, and GCP database to determine whether Databricks enabled backups to separate facilities.	No exceptions noted.
		BCD-11.4	Database backups are encrypted.	Inspected the AWS base image configuration and the backup configuration for a selected AWS database to determine whether backups were encrypted, and inspected Azure and GCP vendor backup documentation to determine whether backups are configured to be encrypted by default.	No exceptions noted.

Additional Criteria Related to the Availability Category

Criteria	Trust Services Criteria	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
Additional Criteria Related to Availability					
		BCD-501	A policy exists that establishes backup requirements.	Inspected the Backup Policy to determine whether backup requirements have been established and documented.	No exceptions noted.
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	BCD-02.2	Business Continuity and Disaster Recovery plans are documented and updated at least annually to ensure the continuation of essential business functions.	Inspected the Business Continuity and Disaster Recovery Plans to determine whether they are reviewed and updated on an annual basis.	No exceptions noted.
		BCD-04	Business Continuity and Disaster Recovery plans are tested at least annually.	Inspected the completed business continuity and the AWS, Azure, and GCP disaster recovery tests to determine whether it was tested and documented on an annual basis.	No exceptions noted.
		BCD-11.1	Database restoration testing is performed at least annually.	Inspected the AWS, Azure, and GCP database backup restoration test results to determine whether database restoration testing was performed annually.	No exceptions noted.

Additional Criteria Related to the Confidentiality Category

Criteria	Trust Services Criteria	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
Additional Criteria Related to Confidentiality					
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	BCD-11	Databricks enables recurring backups to ensure the availability of systems.	Inspected the AWS base image configuration and the backup configuration for a selected AWS database, Azure and GCP vendor backup documentation to determine whether backups are enabled to ensure availability of the systems.	No exceptions noted.
		CRY-01	A policy exists that establishes cryptographic requirements.	Inspected the Cryptographic Policy to determine whether it is formally documented with established cryptographic requirements.	No exceptions noted.
		DCH-01	A policy exists that establishes data classification and data handling requirements.	Inspected the Data Classification and Handling Policy to determine whether requirements have been established and documented.	No exceptions noted.
		IAC-01	A policy exists that establishes access management and authentication requirements.	Inspected the Access Control and Authentication Policy to determine whether a policy exists that establishes access management and authentication requirements.	No exceptions noted.
		IAC-02	Users, and processes acting on behalf of users, are uniquely identified.	Inspected a system generated list of all users including service and system accounts to determine whether all accounts were uniquely identified.	No exceptions noted.

Additional Criteria Related to the Confidentiality Category

Criteria	Trust Services Criteria	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
Additional Criteria Related to Confidentiality					
				Re-performed an attempt to create a username that already exists in the system to determine whether the username was rejected.	No exceptions noted.
		IAC-07	A formal user registration, provisioning, and deprovisioning process is documented.	Inspected the Access Control and Authentication Policy to determine whether a formal user registration, provisioning, and deprovisioning process is documented.	No exceptions noted.
		IAC-07.2	User access is revoked within 24 hours after termination of employment or contract.	Inspected access termination documentation for a selection of separated employees and contractors to determine whether access was removed within 24 hours.	No exceptions noted.
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	AST-09	Media is securely destroyed when it is no longer needed for business or legal reasons.	Inspected the Data Destruction Policy to determine whether destruction policies and procedures are formally documented.	No exceptions noted.

Additional Criteria Related to the Confidentiality Category

Criteria	Trust Services Criteria	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
Additional Criteria Related to Confidentiality					
				Inspected media decommissioning tickets and/or third-party destruction certificate for a selection of decommissioned media to determine whether the media was securely destroyed when it was no longer needed for business or legal reasons.	No exceptions noted.
		DCH-18	A records retention policy exists that establishes retention requirements in accordance with applicable statutory, regulatory, and contractual obligations.	Inspected the Data Retention Policy to determine whether requirements surrounding data retention had been established and documented.	No exceptions noted.
		DCH-21	Customer workspaces are deleted per customer request.	Inspected the customer data deletion request page, the daily data deletion source code, and a recent data deletion action to determine whether workspaces are configured to delete cancelled workspaces daily per customer request.	No exceptions noted.

Additional Considerations Related to the HIPAA Security and Breach Notification Requirements Provided Within 45 CFR Sections 164.308-316 and 164.400-414

Criteria	HIPAA Security and Breach Notification Requirements	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
H1	§164.308(a)(1)(i) Security Management Process: Implement policies and procedures to prevent, detect, contain, and correct security violations.	GOV-02	Security policies and procedures are documented, communicated, made available on the internal Databricks network to appropriate personnel, and versions are maintained.	Inspected the internal Databricks network and the security policies and procedures to determine whether they are formally documented, maintained, and made available to Databricks personnel.	No exceptions noted.
				Inspected the annual security policy certification to determine whether the security policy has been communicated as part of the annual security training.	No exceptions noted.
		GOV-506	A policy exists that establishes the requirements for the security program.	Inspected the Security Program Policy to determine whether the policy established requirements for the security program.	No exceptions noted.
		IRO-01	A policy and procedure exist that establishes security incident response requirements.	Inspected the Security Incident Management Policy and Procedure to determine whether security incident response requirements are established.	No exceptions noted.

Additional Considerations Related to the HIPAA Security and Breach Notification Requirements Provided Within 45 CFR Sections 164.308-316 and 164.400-414

Criteria	HIPAA Security and Breach Notification Requirements	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
H2	§164.308(a)(1)(ii)(A) Risk Analysis: Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.	RSK-04	A risk assessment is conducted and documented at least annually that includes internal and external threats, likelihood, impact, controls, and level of risk, as well as fraudulent activities and key fraud factors. Risks are ranked and high risks are managed and tracked.	Inspected the annual risk assessment results to determine whether a risk assessment was performed and included threats (e.g., internal, external, and fraud) were identified and assessed for likelihood, impact, controls, and level of risk.	No exceptions noted.
				Inspected the risk register and associated residual risk rating, and inquired of management, and determined there were no high risks identified.	The circumstances that warrant the operation of this control did not occur during the examination period and, as a result, this test procedure could not be tested.
		RSK-04.1	A risk register is maintained that facilitates monitoring and reporting of risks.	Inspected the risk register to determine whether it is maintained for monitoring and reporting of risks.	No exceptions noted.
		VPM-06	Host images are scanned for vulnerabilities weekly as part of the deployment process. Identified vulnerabilities are risk ranked, tracked, and remediated according to Company policy.	Inspected vulnerability scan configurations to determine whether host images are configured to be scanned at least weekly.	No exceptions noted.

Additional Considerations Related to the HIPAA Security and Breach Notification Requirements Provided Within 45 CFR Sections 164.308-316 and 164.400-414

Criteria	HIPAA Security and Breach Notification Requirements	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
				Observed the subsequent week's vulnerability scan results for a selection of vulnerabilities to determine whether the identified vulnerabilities were remediated according to Company policy and did not appear in the subsequent weeks scan.	No exceptions noted.
		VPM-07	Third-party penetration testing is conducted on at least an annual basis. Identified vulnerabilities are tracked and remediated according to Company policy.	Inspected the annual penetration test results for the Lakehouse Platform Services system hosted on AWS, Azure, and GCP, and associated remediation tickets to determine whether penetration tests were performed and vulnerabilities were tracked and remediated according to Company policy.	No exceptions noted.
		VPM-502	The Databricks web application is scanned for vulnerabilities at least monthly. Identified vulnerabilities are risk ranked, tracked, and remediated according to Company policy.	Inspected the Databricks web application vulnerability scan configuration and the vulnerability scans for a selection of months and the associated tickets to determine whether a vulnerability scan was performed and vulnerabilities were risk ranked, researched, and resolved according to Company policy.	No exceptions noted.

Additional Considerations Related to the HIPAA Security and Breach Notification Requirements Provided Within 45 CFR Sections 164.308-316 and 164.400-414

Criteria	HIPAA Security and Breach Notification Requirements	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
H3	§164.308(a)(1)(ii)(B) Risk Management: Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306(a).	RSK-01	A policy exists that establishes the risk management program and requirements.	Inspected the Information Security Management System Policy to determine whether requirements for the risk management program have been established.	No exceptions noted.
		RSK-04	A risk assessment is conducted and documented at least annually that includes internal and external threats, likelihood, impact, controls, and level of risk, as well as fraudulent activities and key fraud factors. Risks are ranked and high risks are managed and tracked.	Inspected the annual risk assessment results to determine whether a risk assessment was performed and included threats (e.g., internal, external, and fraud) were identified and assessed for likelihood, impact, controls, and level of risk.	No exceptions noted.
				Inspected the risk register and associated residual risk rating, and inquired of management, and determined there were no high risks identified.	The circumstances that warrant the operation of this control did not occur during the examination period and, as a result, this test procedure could not be tested.
		VPM-06	Host images are scanned for vulnerabilities weekly as part of the deployment process. Identified vulnerabilities are risk ranked, tracked, and remediated according to Company policy.	Inspected vulnerability scan configurations to determine whether host images are configured to be scanned at least weekly.	No exceptions noted.

Additional Considerations Related to the HIPAA Security and Breach Notification Requirements Provided Within 45 CFR Sections 164.308-316 and 164.400-414

Criteria	HIPAA Security and Breach Notification Requirements	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
				Observed the subsequent week's vulnerability scan results for a selection of vulnerabilities to determine whether the identified vulnerabilities were remediated according to Company policy and did not appear in the subsequent weeks scan.	No exceptions noted.
		VPM-07	Third-party penetration testing is conducted on at least an annual basis. Identified vulnerabilities are tracked and remediated according to Company policy.	Inspected the annual penetration test results for the Lakehouse Platform Services system hosted on AWS, Azure, and GCP, and associated remediation tickets to determine whether penetration tests were performed and vulnerabilities were tracked and remediated according to Company policy.	No exceptions noted.
		VPM-502	The Databricks web application is scanned for vulnerabilities at least monthly. Identified vulnerabilities are risk ranked, tracked, and remediated according to Company policy.	Inspected the Databricks web application vulnerability scan configuration and the vulnerability scans for a selection of months and the associated tickets to determine whether a vulnerability scan was performed and vulnerabilities were risk ranked, researched, and resolved according to Company policy.	No exceptions noted.

Additional Considerations Related to the HIPAA Security and Breach Notification Requirements Provided Within 45 CFR Sections 164.308-316 and 164.400-414

Criteria	HIPAA Security and Breach Notification Requirements	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
H4	§164.308(a)(1)(ii)(C) Sanction Policy: Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.	HRS-07	A policy exists that establishes sanctions for personnel misconduct.	Inspected the Sanctions Policy to determine whether sanctions for personnel misconduct are established.	No exceptions noted.
H5	§164.308(a)(1)(ii)(D) Information System Activity Review: Implement procedures to regularly review records of information system activity, such as audit logs, access reports and security incident tracking reports.	IRO-501	Security and privacy incidents are documented, tracked, and a root cause analysis is performed.	Inspected the tickets for a selection of security and privacy incidents to determine whether incidents were documented, tracked, and a root cause analysis was performed.	No exceptions noted.
		MON-01	A policy exists that establishes logging and monitoring requirements.	Inspected the Logging and Monitoring Policy to determine whether requirements have been established and are documented.	No exceptions noted.
		MON-02	The Databricks Secfood application is used as a Security Incident Event Management (SIEM) tool, to support the centralized collection of security related event logs and near real-time analysis and escalation of events.	Inspected the SIEM tool to determine whether it is configured to support the centralized collection of security related event logs.	No exceptions noted.
				Inspected event tickets for a selection of security related events to determine whether events were escalated and resolved.	No exceptions noted.

Additional Considerations Related to the HIPAA Security and Breach Notification Requirements Provided Within 45 CFR Sections 164.308-316 and 164.400-414

Criteria	HIPAA Security and Breach Notification Requirements	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
		NET-08	A Network Intrusion Detection System (IDS) is used to monitor, detect, and alert on intrusions into the network.	Inspected the IDS configuration to determine whether it is configured to monitor, detect, and alert on intrusions into the network.	No exceptions noted.
H6	§164.308(a)(2) Assigned Security Responsibility: Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.	GOV-04	An individual is assigned as CSO with the mission and resources to centrally manage, coordinate, develop, implement, and maintain an enterprisewide security program.	Inspected the organizational chart and the security policy to determine whether the CSO is responsible for the enterprisewide security program.	No exceptions noted.
		HRS-03	Security roles and responsibilities are defined in Databricks security policies.	Inspected various information security policies including the Information Security Management System Policy and the Security Program Policy to determine whether security roles and responsibilities have been established and documented.	No exceptions noted.

Additional Considerations Related to the HIPAA Security and Breach Notification Requirements Provided Within 45 CFR Sections 164.308-316 and 164.400-414

Criteria	HIPAA Security and Breach Notification Requirements	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
H7	§164.308(a)(3)(i) Workplace Security: Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) from obtaining access to electronic protected health information.	IAC-01	A policy exists that establishes access management and authentication requirements.	Inspected the Access Control and Authentication Policy to determine whether a policy exists that establishes access management and authentication requirements.	No exceptions noted.
		IAC-07	A formal user registration, provisioning, and deprovisioning process is documented.	Inspected the Access Control and Authentication Policy to determine whether a formal user registration, provisioning, and deprovisioning process is documented.	No exceptions noted.
		IAC-17	User access reviews are performed at least quarterly and appropriate action is taken.	Inspected Databricks user access review for a selection of quarters and associated access removal tickets to determine whether the access review was conducted and inappropriate access was corrected.	No exceptions noted.
		IAC-502	User access to production systems is authorized by role or approver before temporary credentials with predefined expiration period are granted to access the Databricks web application and production servers in order to provide customer support.	Inspected the Genie confluence page to determine whether temporary credentials with predefined expiration period is granted to authorized users for accessing the Databricks web application and production servers in order to provide customer support.	No exceptions noted.

Additional Considerations Related to the HIPAA Security and Breach Notification Requirements Provided Within 45 CFR Sections 164.308-316 and 164.400-414

Criteria	HIPAA Security and Breach Notification Requirements	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
				Observed an authorized user request access to the Databricks web application and production server using the Genie application to determine whether the request is routed for approval prior to access being granted.	No exceptions noted.
H8	§164.308(a)(3)(ii)(A) Authorization and/or Supervision: Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.	IAC-07	A formal user registration, provisioning, and deprovisioning process is documented.	Inspected the Access Control and Authentication Policy to determine whether a formal user registration, provisioning, and deprovisioning process is documented.	No exceptions noted.
		IAC-08	Access to production servers is limited to authorized users.	Inspected the system generated list of users with access to the production servers, the users' associated job titles, and inquired of management to determine whether their access is appropriate.	No exceptions noted.
		IAC-17	User access reviews are performed at least quarterly and appropriate action is taken.	Inspected Databricks user access review for a selection of quarters and associated access removal tickets to determine whether the access review was conducted and inappropriate access was corrected.	No exceptions noted.

Additional Considerations Related to the HIPAA Security and Breach Notification Requirements Provided Within 45 CFR Sections 164.308-316 and 164.400-414

Criteria	HIPAA Security and Breach Notification Requirements	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
		IAC-502	User access to production systems is authorized by role or approver before temporary credentials with predefined expiration period are granted to access the Databricks web application and production servers in order to provide customer support.	Inspected the Genie confluence page to determine whether temporary credentials with predefined expiration period is granted to authorized users for accessing the Databricks web application and production servers in order to provide customer support.	No exceptions noted.
				Observed an authorized user request access to the Databricks web application and production server using the Genie application to determine whether the request is routed for approval prior to access being granted.	No exceptions noted.
H9	§164.308(a)(3)(ii)(B) Workforce Clearance Procedure: Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.	IAC-08	Access to production servers is limited to authorized users.	Inspected the system generated list of users with access to the production servers, the users' associated job titles, and inquired of management to determine whether their access is appropriate.	No exceptions noted.
		IAC-17	User access reviews are performed at least quarterly and appropriate action is taken.	Inspected Databricks user access review for a selection of quarters and associated access removal tickets to determine whether the access review was conducted and inappropriate access was corrected.	No exceptions noted.

Additional Considerations Related to the HIPAA Security and Breach Notification Requirements Provided Within 45 CFR Sections 164.308-316 and 164.400-414

Criteria	HIPAA Security and Breach Notification Requirements	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
		IAC-502	User access to production systems is authorized by role or approver before temporary credentials with predefined expiration period are granted to access the Databricks web application and production servers in order to provide customer support.	Inspected the Genie confluence page to determine whether temporary credentials with predefined expiration period is granted to authorized users for accessing the Databricks web application and production servers in order to provide customer support.	No exceptions noted.
				Observed an authorized user request access to the Databricks web application and production server using the Genie application to determine whether the request is routed for approval prior to access being granted.	No exceptions noted.
		IAC-506	Access to authentication infrastructure is limited to authorized users.	Inspected the system generated list of users who have access to the authentication infrastructure, inspected the users' job titles, and inquired of management to determine whether access is limited to authorized users.	No exceptions noted.
		IAC-507	New hire access is granted through a formal provisioning process.	Inspected the birthright access group rules and new employees access permissions for a selection of new employees to determine whether access is granted based on role and team.	No exceptions noted.

Additional Considerations Related to the HIPAA Security and Breach Notification Requirements Provided Within 45 CFR Sections 164.308-316 and 164.400-414

Criteria	HIPAA Security and Breach Notification Requirements	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
		TDA-20	Administrative access to software libraries is limited to authorized users.	Inspected the system generated list of users who have administrative access to software libraries, the users' associated job titles, and inquired of management to determine whether access is limited to authorized users.	No exceptions noted.
H10	§164.308(a)(3)(ii)(C) Termination Process: Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.	IAC-07.2	User access is revoked within 24 hours after termination of employment or contract.	Inspected access termination documentation for a selection of separated employees and contractors to determine whether access was removed within 24 hours.	No exceptions noted.
		IAC-17	User access reviews are performed at least quarterly and appropriate action is taken.	Inspected Databricks user access review for a selection of quarters and associated access removal tickets to determine whether the access review was conducted and inappropriate access was corrected.	No exceptions noted.
H11	§164.308(a)(4)(i) Information Access Management- Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.	IAC-01	A policy exists that establishes access management and authentication requirements.	Inspected the Access Control and Authentication Policy to determine whether a policy exists that establishes access management and authentication requirements.	No exceptions noted.

Additional Considerations Related to the HIPAA Security and Breach Notification Requirements Provided Within 45 CFR Sections 164.308-316 and 164.400-414

Criteria	HIPAA Security and Breach Notification Requirements	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
		IAC-07	A formal user registration, provisioning, and deprovisioning process is documented.	Inspected the Access Control and Authentication Policy to determine whether a formal user registration, provisioning, and deprovisioning process is documented.	No exceptions noted.
H12	§164.308(a)(4)(ii)(A) Isolating Health Care Clearinghouse Functions: If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.	Not Applicable — Databricks is not a healthcare clearinghouse.			
H13	§164.308(a)(4)(ii)(B) Access Authorization: Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.	IAC-07	A formal user registration, provisioning, and deprovisioning process is documented.	Inspected the Access Control and Authentication Policy to determine whether a formal user registration, provisioning, and deprovisioning process is documented.	No exceptions noted.

Additional Considerations Related to the HIPAA Security and Breach Notification Requirements Provided Within 45 CFR Sections 164.308-316 and 164.400-414

Criteria	HIPAA Security and Breach Notification Requirements	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
		IAC-08	Access to production servers is limited to authorized users.	Inspected the system generated list of users with access to the production servers, the users' associated job titles, and inquired of management to determine whether their access is appropriate.	No exceptions noted.
		IAC-502	User access to production systems is authorized by role or approver before temporary credentials with predefined expiration period are granted to access the Databricks web application and production servers in order to provide customer support.	Inspected the Genie confluence page to determine whether temporary credentials with predefined expiration period is granted to authorized users for accessing the Databricks web application and production servers in order to provide customer support.	No exceptions noted.
				Observed an authorized user request access to the Databricks web application and production server using the Genie application to determine whether the request is routed for approval prior to access being granted.	No exceptions noted.

Additional Considerations Related to the HIPAA Security and Breach Notification Requirements Provided Within 45 CFR Sections 164.308-316 and 164.400-414

Criteria	HIPAA Security and Breach Notification Requirements	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
H14	§164.308(a)(4)(ii)(C) Access Establishment and Modification: Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.	IAC-07.2	User access is revoked within 24 hours after termination of employment or contract.	Inspected access termination documentation for a selection of separated employees and contractors to determine whether access was removed within 24 hours.	No exceptions noted.
		IAC-17	User access reviews are performed at least quarterly and appropriate action is taken.	Inspected Databricks user access review for a selection of quarters and associated access removal tickets to determine whether the access review was conducted and inappropriate access was corrected.	No exceptions noted.
H15	§164.308(a)(5)(i) Security Awareness Training: Implement a security awareness and training program for all members of its workforce (including management).	SAT-01	A security training and awareness program has been implemented.	Inspected the security training procedure to determine a security training and awareness program has been formally documented and implemented.	No exceptions noted.
		SAT-02	All contractors with Databricks accounts and employees are required to take security and privacy training upon hire and at least once per year.	Inspected the security and privacy training certifications for a selection of new hires and contractors to determine whether the employees and contractors completed the training upon hire.	No exceptions noted.

Additional Considerations Related to the HIPAA Security and Breach Notification Requirements Provided Within 45 CFR Sections 164.308-316 and 164.400-414

Criteria	HIPAA Security and Breach Notification Requirements	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
				Inspected the security and privacy training certificates for a selection of contractors and employees to determine whether the training was completed on an annual basis.	No exceptions noted.
H16	§164.308(a)(5)(ii)(A) Security Reminders: Periodic security updates.	SAT-01	A security training and awareness program has been implemented.	Inspected the security training procedure to determine a security training and awareness program has been formally documented and implemented.	No exceptions noted.
		SAT-02	All contractors with Databricks accounts and employees are required to take security and privacy training upon hire and at least once per year.	Inspected the security and privacy training certifications for a selection of new hires and contractors to determine whether the employees and contractors completed the training upon hire.	No exceptions noted.
				Inspected the security and privacy training certificates for a selection of contractors and employees to determine whether the training was completed on an annual basis.	No exceptions noted.
H17	§164.308(a)(5)(ii)(B) Security Reminders: Procedures for guarding against, detecting, and reporting malicious software.	END-04	Anti-malware software is installed on all laptop and desktop computers and cannot be disabled or altered by unauthorized users.	Inspected the anti-malware software clients for a selection of computers to determine whether anti-malware software was installed and cannot be disabled or altered by unauthorized users.	No exceptions noted.

Additional Considerations Related to the HIPAA Security and Breach Notification Requirements Provided Within 45 CFR Sections 164.308-316 and 164.400-414

Criteria	HIPAA Security and Breach Notification Requirements	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
		END-04.1	Anti-malware software is configured to automatically update on all laptop and desktop computers.	Inspected the anti-malware configuration to determine whether anti-malware software is configured to update automatically on all laptop and desktop computers.	No exceptions noted.
H18	§164.308(a)(5)(ii)(C) Log-in Monitoring: Procedures for monitoring log-in attempts and reporting discrepancies.	MON-02	The Databricks Secfood application is used as a Security Incident Event Management (SIEM) tool, to support the centralized collection of security related event logs and near real-time analysis and escalation of events.	Inspected the SIEM tool to determine whether it is configured to support the centralized collection of security related event logs.	No exceptions noted.
				Inspected event tickets for a selection of security related events to determine whether events were escalated and resolved.	No exceptions noted.
		MON-03.3	Production servers are configured to log security events, including the actions of privileged users.	Inspected the AWS, Azure, and GCP server build configurations and security event logs for selected servers to determine whether they were configured to enable logging, including the actions of privileged users.	No exceptions noted.

Additional Considerations Related to the HIPAA Security and Breach Notification Requirements Provided Within 45 CFR Sections 164.308-316 and 164.400-414

Criteria	HIPAA Security and Breach Notification Requirements	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
		MON-501	Databricks usage of cloud service data center provider administration platforms is configured to log audit events, including the actions of privileged users.	Inspected the logging configuration and events log for AWS, Azure, and GCP to determine whether they are configured to log audit events, including the actions of privileged users.	No exceptions noted.
H19	§164.308(a)(5)(ii)(D) Password Management: Procedures for creating, changing, and safeguarding passwords.	IAC-501	Authentication infrastructure enforces passwords for workstations and SSO applications that comply with Databricks policy for password expiration, length, complexity, and history.	Inspected the workstation and SSO password configuration settings to determine whether they are configured according to the password requirements established in the security policy.	No exceptions noted.
H20	§164.308(a)(6)(i) Security Incident Procedures: Implement policies and procedures to address security incidents.	IRO-01	A policy and procedure exist that establishes security incident response requirements.	Inspected the Security Incident Management Policy and Procedure to determine whether security incident response requirements are established.	No exceptions noted.
H21	§164.308(a)(6)(ii) Response and Reporting: Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.	IRO-10	Applicable security and privacy incidents are reported to internal stakeholders, affected clients, third parties, and regulatory authorities.	Inspected the Databricks Security Incident Management Procedure to determine whether Databricks has a procedure for reporting applicable security and privacy incidents to internal stakeholders, affected clients, third parties, and regulatory authorities.	No exceptions noted.

Additional Considerations Related to the HIPAA Security and Breach Notification Requirements Provided Within 45 CFR Sections 164.308-316 and 164.400-414

Criteria	HIPAA Security and Breach Notification Requirements	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
				Inspected tickets for a selection of security and privacy incidents to determine whether appropriate stakeholders were notified.	No exceptions noted.
		IRO-501	Security and privacy incidents are documented, tracked, and a root cause analysis is performed.	Inspected the tickets for a selection of security and privacy incidents to determine whether incidents were documented, tracked, and a root cause analysis was performed.	No exceptions noted.
H22	§164.308(a)(7)(i) Contingency Plan: Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.	BCD-01	A policy exists that establishes contingency planning and recovery requirements.	Inspected the Business Continuity and Disaster Recovery Policy to determine whether it is formally documented with established requirements.	No exceptions noted.
		BCD-02.2	Business Continuity and Disaster Recovery plans are documented and updated at least annually to ensure the continuation of essential business functions.	Inspected the Business Continuity and Disaster Recovery Plans to determine whether they are reviewed and updated on an annual basis.	No exceptions noted.
H23	§164.308(a)(7)(ii)(A) Data Backup Plan: Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.	BCD-11	Databricks enables recurring backups to ensure the availability of systems.	Inspected the AWS base image configuration and the backup configuration for a selected AWS database, Azure and GCP vendor backup documentation to determine whether backups are enabled to ensure availability of the systems.	No exceptions noted.

Additional Considerations Related to the HIPAA Security and Breach Notification Requirements Provided Within 45 CFR Sections 164.308-316 and 164.400-414

Criteria	HIPAA Security and Breach Notification Requirements	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
		BCD-11.1	Database restoration testing is performed at least annually.	Inspected the AWS, Azure, and GCP database backup restoration test results to determine whether database restoration testing was performed annually.	No exceptions noted.
		BCD-11.2	Databricks enables backups to separate facilities in cloud service data center provider environments.	Inspected the base image configuration and the backup configuration for a selected AWS Multitenant, Azure, and GCP database to determine whether Databricks enabled backups to separate facilities.	No exceptions noted.
H24	§164.308(a)(7)(ii)(B) Disaster Recovery Plan: Establish (and implement as needed) procedures to restore any loss of data.	BCD-01	A policy exists that establishes contingency planning and recovery requirements.	Inspected the Business Continuity and Disaster Recovery Policy to determine whether it is formally documented with established requirements.	No exceptions noted.
		BCD-02.2	Business Continuity and Disaster Recovery plans are documented and updated at least annually to ensure the continuation of essential business functions.	Inspected the Business Continuity and Disaster Recovery Plans to determine whether they are reviewed and updated on an annual basis.	No exceptions noted.

Additional Considerations Related to the HIPAA Security and Breach Notification Requirements Provided Within 45 CFR Sections 164.308-316 and 164.400-414

Criteria	HIPAA Security and Breach Notification Requirements	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
H25	§164.308(a)(7)(ii)(C) Emergency Mode Operation Plan: Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.	BCD-02.2	Business Continuity and Disaster Recovery plans are documented and updated at least annually to ensure the continuation of essential business functions.	Inspected the Business Continuity and Disaster Recovery Plans to determine whether they are reviewed and updated on an annual basis.	No exceptions noted.
H26	§164.308(a)(7)(ii)(D) Testing and Revision Procedures: Implement procedures for periodic testing and revision of contingency plans.	BCD-02.2	Business Continuity and Disaster Recovery plans are documented and updated at least annually to ensure the continuation of essential business functions.	Inspected the Business Continuity and Disaster Recovery Plans to determine whether they are reviewed and updated on an annual basis.	No exceptions noted.
		BCD-04	Business Continuity and Disaster Recovery plans are tested at least annually.	Inspected the completed business continuity and the AWS, Azure, and GCP disaster recovery tests to determine whether it was tested and documented on an annual basis.	No exceptions noted.
		BCD-11.1	Database restoration testing is performed at least annually.	Inspected the AWS, Azure, and GCP database backup restoration test results to determine whether database restoration testing was performed annually.	No exceptions noted.

Additional Considerations Related to the HIPAA Security and Breach Notification Requirements Provided Within 45 CFR Sections 164.308-316 and 164.400-414

Criteria	HIPAA Security and Breach Notification Requirements	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
H27	§164.308(a)(7)(ii)(E) Applications and Data Criticality Analysis: Assess the relative criticality of specific applications and data in support of other contingency plan components.	BCD-02	A BIA is documented and updated at least annually.	Inspected the BIA to determine whether the BIA was documented and updated at least annually.	No exceptions noted.
H28	§164.308(a)(8) Evaluation: Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operations changes affecting the security of electronic protected health information, that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart.	CPL-03.1	Independent assessors are used to assess the Databricks information security program, including key controls, at least once per year.	Inspected the most recent independent assessors' reports to determine whether Databricks was independently assessed on an at least annual basis.	No exceptions noted.
		VPM-06	Host images are scanned for vulnerabilities weekly as part of the deployment process. Identified vulnerabilities are risk ranked, tracked, and remediated according to Company policy.	Inspected vulnerability scan configurations to determine whether host images are configured to be scanned at least weekly.	No exceptions noted.
				Observed the subsequent week's vulnerability scan results for a selection of vulnerabilities to determine whether the identified vulnerabilities were remediated according to Company policy and did not appear in the subsequent weeks scan.	No exceptions noted.

Additional Considerations Related to the HIPAA Security and Breach Notification Requirements Provided Within 45 CFR Sections 164.308-316 and 164.400-414

Criteria	HIPAA Security and Breach Notification Requirements	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
		VPM-07	Third-party penetration testing is conducted on at least an annual basis. Identified vulnerabilities are tracked and remediated according to Company policy.	Inspected the annual penetration test results for the Lakehouse Platform Services system hosted on AWS, Azure, and GCP, and associated remediation tickets to determine whether penetration tests were performed and vulnerabilities were tracked and remediated according to Company policy.	No exceptions noted.
		VPM-502	The Databricks web application is scanned for vulnerabilities at least monthly. Identified vulnerabilities are risk ranked, tracked, and remediated according to Company policy.	Inspected the Databricks web application vulnerability scan configuration and the vulnerability scans for a selection of months and the associated tickets to determine whether a vulnerability scan was performed and vulnerabilities were risk ranked, researched, and resolved according to Company policy.	No exceptions noted.

Additional Considerations Related to the HIPAA Security and Breach Notification Requirements Provided Within 45 CFR Sections 164.308-316 and 164.400-414

Criteria	HIPAA Security and Breach Notification Requirements	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
H29	§164.308(b)(1) Business Associate Contracts and Other Arrangements: A covered entity, in accordance with §164.306, may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with §164.314(a) that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.	Not Applicable — Databricks is not a covered entity.			

Additional Considerations Related to the HIPAA Security and Breach Notification Requirements Provided Within 45 CFR Sections 164.308-316 and 164.400-414

Criteria	HIPAA Security and Breach Notification Requirements	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
H30	§164.308(b)(2) Business Associate Contracts and Other Arrangements: A business associate may permit a business that is a subcontractor to create, receive, maintain, or transmit ePHI on its behalf only if the business associate obtains satisfactory assurances, in accordance with §164.314(a), that the subcontractor will appropriately safeguard the information.	TPM-502	Subcontractors or subprocessors that create, receive, maintain, or transmit ePHI on behalf of Databricks, have appropriate contractual agreements in place to protect ePHI.	Inspected the contractual agreements for a selection of subcontractors to determine whether they have agreements in place to protect ePHI.	No exceptions noted.
H31	§164.308(b)(3) Written Contract or Other Arrangements: Document the satisfactory assurances required by paragraph (b)(1) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of §164.314(a).	TPM-502	Subcontractors or subprocessors that create, receive, maintain, or transmit ePHI on behalf of Databricks, have appropriate contractual agreements in place to protect ePHI.	Inspected the contractual agreements for a selection of subcontractors to determine whether they have agreements in place to protect ePHI.	No exceptions noted.

Additional Considerations Related to the HIPAA Security and Breach Notification Requirements Provided Within 45 CFR Sections 164.308-316 and 164.400-414

Criteria	HIPAA Security and Breach Notification Requirements	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
H32	§164.310(a)(1) Facility Access Controls: Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.	PES-01	A policy exists that establishes physical and environmental protection requirements for Databricks offices.	Inspected the Physical Security Policy to determine whether it establishes physical and environmental requirements for Databricks offices.	No exceptions noted.
		Not Applicable — This requirement is the responsibility of the subservice organizations. Refer to the subservice organizations section above for controls managed by the subservice organizations.			
H33	§164.310(a)(2)(i) Contingency Operations: Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.	BCD-02	A BIA is documented and updated at least annually.	Inspected the BIA to determine whether the BIA was documented and updated at least annually.	No exceptions noted.
		BCD-02.2	Business Continuity and Disaster Recovery plans are documented and updated at least annually to ensure the continuation of essential business functions.	Inspected the Business Continuity and Disaster Recovery Plans to determine whether they are reviewed and updated on an annual basis.	No exceptions noted.
		BCD-04	Business Continuity and Disaster Recovery plans are tested at least annually.	Inspected the completed business continuity and the AWS, Azure, and GCP disaster recovery tests to determine whether it was tested and documented on an annual basis.	No exceptions noted.

Additional Considerations Related to the HIPAA Security and Breach Notification Requirements Provided Within 45 CFR Sections 164.308-316 and 164.400-414

Criteria	HIPAA Security and Breach Notification Requirements	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
		BCD-11	Databricks enables recurring backups to ensure the availability of systems.	Inspected the AWS base image configuration and the backup configuration for a selected AWS database, Azure and GCP vendor backup documentation to determine whether backups are enabled to ensure availability of the systems.	No exceptions noted.
		BCD-11.1	Database restoration testing is performed at least annually.	Inspected the AWS, Azure, and GCP database backup restoration test results to determine whether database restoration testing was performed annually.	No exceptions noted.
		BCD-11.2	Databricks enables backups to separate facilities in cloud service data center provider environments.	Inspected the base image configuration and the backup configuration for a selected AWS Multitenant, Azure, and GCP database to determine whether Databricks enabled backups to separate facilities.	No exceptions noted.
H34	§164.310(a)(2)(ii) Facility Security Plan: Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.	PES-01	A policy exists that establishes physical and environmental protection requirements for Databricks offices.	Inspected the Physical Security Policy to determine whether it establishes physical and environmental requirements for Databricks offices.	No exceptions noted.
		Part of this requirement is the responsibility of the subservice organizations. Refer to the subservice organizations section above for controls managed by the subservice organizations.			

Additional Considerations Related to the HIPAA Security and Breach Notification Requirements Provided Within 45 CFR Sections 164.308-316 and 164.400-414

Criteria	HIPAA Security and Breach Notification Requirements	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
H35	§164.310(a)(2)(iii) Access Control and Validation Procedures: Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.	Not Applicable — This requirement is the responsibility of the subservice organizations. Refer to the subservice organizations section above for controls managed by the subservice organizations.			
H36	§164.310(a)(2)(iv) Maintenance Records: Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).	Not Applicable — This requirement is the responsibility of the subservice organizations. Refer to the subservice organizations section above for controls managed by the subservice organizations.			

Additional Considerations Related to the HIPAA Security and Breach Notification Requirements Provided Within 45 CFR Sections 164.308-316 and 164.400-414

Criteria	HIPAA Security and Breach Notification Requirements	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
H37	§164.310(b) Workstation Use: Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.	Not Applicable — This requirement is the responsibility of the subservice organizations. Refer to the subservice organizations section above for controls managed by the subservice organizations.			
H38	§164.310(c) Workstation Security: Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.	Not Applicable — Databricks does not store customer data (i.e., ePHI) in a separate physical environment.			
H39	§164.310(d)(1) Device and Media Controls: Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information, into and out of a facility, and the movement of these items within the facility.	Not Applicable — The ePHI data for the environment is hosted on AWS, Azure, and GCP cloud environments. The controls over removal of electronic protected health information from electronic media are performed by the cloud service providers.			

Additional Considerations Related to the HIPAA Security and Breach Notification Requirements Provided Within 45 CFR Sections 164.308-316 and 164.400-414

Criteria	HIPAA Security and Breach Notification Requirements	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
H40	§164.310(d)(2)(i) Disposal: Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.	Not Applicable – The ePHI data for the environment is hosted on AWS, Azure, and GCP cloud environments. The controls over removal of electronic protected health information from electronic media are performed by the cloud service providers.			
H41	§164.310(d)(2)(ii) Media Re-use: Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.	Not Applicable – The ePHI data for the environment is hosted on AWS, Azure, and GCP cloud environments. The controls over removal of electronic protected health information from electronic media are performed by the cloud service providers.			
H42	§164.310(d)(2)(iii) Accountability: Maintain a record of the movements of hardware and electronic media and any person responsible therefore.	Not Applicable – The ePHI data for the environment is hosted on AWS, Azure, and GCP cloud environments. The controls over removal of electronic protected health information from electronic media are performed by the cloud service providers.			
H43	§164.310(d)(2)(iv) Data Backup and Storage: Create retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.	BCD-11	Databricks enables recurring backups to ensure the availability of systems.	Inspected the AWS base image configuration and the backup configuration for a selected AWS database, Azure and GCP vendor backup documentation to determine whether backups are enabled to ensure availability of the systems.	No exceptions noted.

Additional Considerations Related to the HIPAA Security and Breach Notification Requirements Provided Within 45 CFR Sections 164.308-316 and 164.400-414

Criteria	HIPAA Security and Breach Notification Requirements	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
		Not Applicable — The ePHI data for the environment is hosted on AWS, Azure, and GCP cloud environments. The controls over removal of electronic protected health information from electronic media are performed by the cloud service providers.			
H44	§164.312(a)(1) Access Control: Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).	IAC-01	A policy exists that establishes access management and authentication requirements.	Inspected the Access Control and Authentication Policy to determine whether a policy exists that establishes access management and authentication requirements.	No exceptions noted.
		IAC-07	A formal user registration, provisioning, and deprovisioning process is documented.	Inspected the Access Control and Authentication Policy to determine whether a formal user registration, provisioning, and deprovisioning process is documented.	No exceptions noted.
		IAC-07.2	User access is revoked within 24 hours after termination of employment or contract.	Inspected access termination documentation for a selection of separated employees and contractors to determine whether access was removed within 24 hours.	No exceptions noted.
		IAC-08	Access to production servers is limited to authorized users.	Inspected the system generated list of users with access to the production servers, the users' associated job titles, and inquired of management to determine whether their access is appropriate.	No exceptions noted.

Additional Considerations Related to the HIPAA Security and Breach Notification Requirements Provided Within 45 CFR Sections 164.308-316 and 164.400-414

Criteria	HIPAA Security and Breach Notification Requirements	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
		IAC-17	User access reviews are performed at least quarterly and appropriate action is taken.	Inspected Databricks user access review for a selection of quarters and associated access removal tickets to determine whether the access review was conducted and inappropriate access was corrected.	No exceptions noted.
		IAC-501	Authentication infrastructure enforces passwords for workstations and SSO applications that comply with Databricks policy for password expiration, length, complexity, and history.	Inspected the workstation and SSO password configuration settings to determine whether they are configured according to the password requirements established in the security policy.	No exceptions noted.
		IAC-502	User access to production systems is authorized by role or approver before temporary credentials with predefined expiration period are granted to access the Databricks web application and production servers in order to provide customer support.	Inspected the Genie confluence page to determine whether temporary credentials with predefined expiration period is granted to authorized users for accessing the Databricks web application and production servers in order to provide customer support.	No exceptions noted.
				Observed an authorized user request access to the Databricks web application and production server using the Genie application to determine whether the request is routed for approval prior to access being granted.	No exceptions noted.

Additional Considerations Related to the HIPAA Security and Breach Notification Requirements Provided Within 45 CFR Sections 164.308-316 and 164.400-414

Criteria	HIPAA Security and Breach Notification Requirements	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
		IAC-506	Access to authentication infrastructure is limited to authorized users.	Inspected the system generated list of users who have access to the authentication infrastructure, inspected the users' job titles, and inquired of management to determine whether access is limited to authorized users.	No exceptions noted.
		IAC-507	New hire access is granted through a formal provisioning process.	Inspected the birthright access group rules and new employees access permissions for a selection of new employees to determine whether access is granted based on role and team.	No exceptions noted.
		NET-14	Access to Databricks' networks and production systems require MFA.	Inspected the MFA configuration to determine whether access to Databricks' networks and production systems require MFA.	No exceptions noted.
				Observed a user authenticate to the network and production environments to determine whether MFA is required to gain access.	No exceptions noted.
H45	§164.312(a)(2)(i) Unique User Identification: Assign a unique name and/or number for identifying and tracking user identity.	IAC-02	Users, and processes acting on behalf of users, are uniquely identified.	Inspected a system generated list of all users including service and system accounts to determine whether all accounts were uniquely identified.	No exceptions noted.

Additional Considerations Related to the HIPAA Security and Breach Notification Requirements Provided Within 45 CFR Sections 164.308-316 and 164.400-414

Criteria	HIPAA Security and Breach Notification Requirements	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
				Re-performed an attempt to create a username that already exists in the system to determine whether the username was rejected.	No exceptions noted.
H46	§164.312(a)(2)(ii) Emergency Access Procedure: Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.	BCD-02.2	Business Continuity and Disaster Recovery plans are documented and updated at least annually to ensure the continuation of essential business functions.	Inspected the Business Continuity and Disaster Recovery Plans to determine whether they are reviewed and updated on an annual basis.	No exceptions noted.
		BCD-04	Business Continuity and Disaster Recovery plans are tested at least annually.	Inspected the completed business continuity and the AWS, Azure, and GCP disaster recovery tests to determine whether it was tested and documented on an annual basis.	No exceptions noted.
		IAC-01	A policy exists that establishes access management and authentication requirements.	Inspected the Access Control and Authentication Policy to determine whether a policy exists that establishes access management and authentication requirements.	No exceptions noted.
H47	§164.312(a)(2)(iii) Automatic Logoff: Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	AST-06	All laptop and desktop computers are configured to implement a password protected screensaver lockout after ten minutes of inactivity.	Inspected the mobile device management lockout configuration to determine whether laptops and desktops are configured to lockout after ten minutes of inactivity.	No exceptions noted.

Additional Considerations Related to the HIPAA Security and Breach Notification Requirements Provided Within 45 CFR Sections 164.308-316 and 164.400-414

Criteria	HIPAA Security and Breach Notification Requirements	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
H48	§164.312(a)(2)(iv) Encryption and Decryption: Implement a mechanism to encrypt and decrypt electronic protected health information.	CRY-03	TLS 1.2 is used to protect the confidentiality and integrity of data being transmitted over the internet.	Inspected the TLS certificates for the AWS, Azure, and GCP environments to determine whether TLS 1.2 or greater was implemented to protect the confidentiality and integrity of data being transmitted over the internet.	No exceptions noted.
		CRY-05	Databricks database systems are configured to store information encrypted.	Inspected the AWS database baseline template configuration and the AWS encryption configuration for a selected database to determine whether databases were encrypted, and inspected Azure and GCP vendor backup documentation to determine whether databases were encrypted by default.	No exceptions noted.
		CRY-09	Key management systems are in place to protect the confidentiality, integrity, and availability of keys.	Inspected the key management systems and vaults to determine whether a system is in place to protect the confidentiality, integrity, and availability of keys.	No exceptions noted.

Additional Considerations Related to the HIPAA Security and Breach Notification Requirements Provided Within 45 CFR Sections 164.308-316 and 164.400-414

Criteria	HIPAA Security and Breach Notification Requirements	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
				Inspected the system generated list of administrators who have access to create, delete, or modify keys within the key management systems, the administrators' associated job titles, and inquired of management to determine whether administrative access is restricted to authorized personnel.	No exceptions noted.
		NET-12	Remote access to Databricks networks is restricted through an IT managed, encrypted VPN solution.	Inspected the VPN configuration and observed a user remotely VPN to determine whether remote access to the Databricks network and production environments are restricted through an encrypted VPN solution.	No exceptions noted.
				Observed a user attempt to access the Databricks network and production environments without VPN to determine whether the user was denied access.	No exceptions noted.

Additional Considerations Related to the HIPAA Security and Breach Notification Requirements Provided Within 45 CFR Sections 164.308-316 and 164.400-414

Criteria	HIPAA Security and Breach Notification Requirements	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
H49	§164.312(b) Audit Controls: Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	MON-02	The Databricks Secfood application is used as a Security Incident Event Management (SIEM) tool, to support the centralized collection of security related event logs and near real-time analysis and escalation of events.	Inspected the SIEM tool to determine whether it is configured to support the centralized collection of security related event logs.	No exceptions noted.
				Inspected event tickets for a selection of security related events to determine whether events were escalated and resolved.	No exceptions noted.
		MON-03.3	Production servers are configured to log security events, including the actions of privileged users.	Inspected the AWS, Azure, and GCP server build configurations and security event logs for selected servers to determine whether they were configured to enable logging, including the actions of privileged users.	No exceptions noted.
		MON-501	Databricks usage of cloud service data center provider administration platforms is configured to log audit events, including the actions of privileged users.	Inspected the logging configuration and events log for AWS, Azure, and GCP to determine whether they are configured to log audit events, including the actions of privileged users.	No exceptions noted.

Additional Considerations Related to the HIPAA Security and Breach Notification Requirements Provided Within 45 CFR Sections 164.308-316 and 164.400-414

Criteria	HIPAA Security and Breach Notification Requirements	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
H50	§164.312(c)(1) Integrity: Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.	CRY-01	A policy exists that establishes cryptographic requirements.	Inspected the Cryptographic Policy to determine whether it is formally documented with established cryptographic requirements.	No exceptions noted.
		CRY-03	TLS 1.2 is used to protect the confidentiality and integrity of data being transmitted over the internet.	Inspected the TLS certificates for the AWS, Azure, and GCP environments to determine whether TLS 1.2 or greater was implemented to protect the confidentiality and integrity of data being transmitted over the internet.	No exceptions noted.
		CRY-05	Databricks database systems are configured to store information encrypted.	Inspected the AWS database baseline template configuration and the AWS encryption configuration for a selected database to determine whether databases were encrypted, and inspected Azure and GCP vendor backup documentation to determine whether databases were encrypted by default.	No exceptions noted.
		CRY-09	Key management systems are in place to protect the confidentiality, integrity, and availability of keys.	Inspected the key management systems and vaults to determine whether a system is in place to protect the confidentiality, integrity, and availability of keys.	No exceptions noted.

Additional Considerations Related to the HIPAA Security and Breach Notification Requirements Provided Within 45 CFR Sections 164.308-316 and 164.400-414

Criteria	HIPAA Security and Breach Notification Requirements	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
				Inspected the system generated list of administrators who have access to create, delete, or modify keys within the key management systems, the administrators' associated job titles, and inquired of management to determine whether administrative access is restricted to authorized personnel.	No exceptions noted.
		NET-12	Remote access to Databricks networks is restricted through an IT managed, encrypted VPN solution.	Inspected the VPN configuration and observed a user remotely VPN to determine whether remote access to the Databricks network and production environments are restricted through an encrypted VPN solution.	No exceptions noted.
				Observed a user attempt to access the Databricks network and production environments without VPN to determine whether the user was denied access.	No exceptions noted.

Additional Considerations Related to the HIPAA Security and Breach Notification Requirements Provided Within 45 CFR Sections 164.308-316 and 164.400-414

Criteria	HIPAA Security and Breach Notification Requirements	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
H51	§164.312(c)(2) Mechanism to Authenticate Electronic Protected Health Information: Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.	MON-02	The Databricks Secfood application is used as a Security Incident Event Management (SIEM) tool, to support the centralized collection of security related event logs and near real-time analysis and escalation of events.	Inspected the SIEM tool to determine whether it is configured to support the centralized collection of security related event logs.	No exceptions noted.
				Inspected event tickets for a selection of security related events to determine whether events were escalated and resolved.	No exceptions noted.
		MON-03.3	Production servers are configured to log security events, including the actions of privileged users.	Inspected the AWS, Azure, and GCP server build configurations and security event logs for selected servers to determine whether they were configured to enable logging, including the actions of privileged users.	No exceptions noted.
		MON-501	Databricks usage of cloud service data center provider administration platforms is configured to log audit events, including the actions of privileged users.	Inspected the logging configuration and events log for AWS, Azure, and GCP to determine whether they are configured to log audit events, including the actions of privileged users.	No exceptions noted.

Additional Considerations Related to the HIPAA Security and Breach Notification Requirements Provided Within 45 CFR Sections 164.308-316 and 164.400-414

Criteria	HIPAA Security and Breach Notification Requirements	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
H52	§164.312(d) Person or Entity Authentication: Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	IAC-07	A formal user registration, provisioning, and deprovisioning process is documented.	Inspected the Access Control and Authentication Policy to determine whether a formal user registration, provisioning, and deprovisioning process is documented.	No exceptions noted.
		IAC-501	Authentication infrastructure enforces passwords for workstations and SSO applications that comply with Databricks policy for password expiration, length, complexity, and history.	Inspected the workstation and SSO password configuration settings to determine whether they are configured according to the password requirements established in the security policy.	No exceptions noted.
		NET-14	Access to Databricks' networks and production systems require MFA.	Inspected the MFA configuration to determine whether access to Databricks' networks and production systems require MFA.	No exceptions noted.
				Observed a user authenticate to the network and production environments to determine whether MFA is required to gain access.	No exceptions noted.

Additional Considerations Related to the HIPAA Security and Breach Notification Requirements Provided Within 45 CFR Sections 164.308-316 and 164.400-414

Criteria	HIPAA Security and Breach Notification Requirements	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
H53	§164.312(e)(1) Transmission Security: Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.	CRY-03	TLS 1.2 is used to protect the confidentiality and integrity of data being transmitted over the internet.	Inspected the TLS certificates for the AWS, Azure, and GCP environments to determine whether TLS 1.2 or greater was implemented to protect the confidentiality and integrity of data being transmitted over the internet.	No exceptions noted.
		NET-12	Remote access to Databricks networks is restricted through an IT managed, encrypted VPN solution.	Inspected the VPN configuration and observed a user remotely VPN to determine whether remote access to the Databricks network and production environments are restricted through an encrypted VPN solution.	No exceptions noted.
				Observed a user attempt to access the Databricks network and production environments without VPN to determine whether the user was denied access.	No exceptions noted.
H54	§164.312(e)(2)(i) Integrity Controls: Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.	CRY-03	TLS 1.2 is used to protect the confidentiality and integrity of data being transmitted over the internet.	Inspected the TLS certificates for the AWS, Azure, and GCP environments to determine whether TLS 1.2 or greater was implemented to protect the confidentiality and integrity of data being transmitted over the internet.	No exceptions noted.

Additional Considerations Related to the HIPAA Security and Breach Notification Requirements Provided Within 45 CFR Sections 164.308-316 and 164.400-414

Criteria	HIPAA Security and Breach Notification Requirements	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
		NET-12	Remote access to Databricks networks is restricted through an IT managed, encrypted VPN solution.	Inspected the VPN configuration and observed a user remotely VPN to determine whether remote access to the Databricks network and production environments are restricted through an encrypted VPN solution.	No exceptions noted.
				Observed a user attempt to access the Databricks network and production environments without VPN to determine whether the user was denied access.	No exceptions noted.
H55	§164.312(e)(2)(ii) Encryption: Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	CRY-03	TLS 1.2 is used to protect the confidentiality and integrity of data being transmitted over the internet.	Inspected the TLS certificates for the AWS, Azure, and GCP environments to determine whether TLS 1.2 or greater was implemented to protect the confidentiality and integrity of data being transmitted over the internet.	No exceptions noted.

Additional Considerations Related to the HIPAA Security and Breach Notification Requirements Provided Within 45 CFR Sections 164.308-316 and 164.400-414

Criteria	HIPAA Security and Breach Notification Requirements	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
		CRY-05	Databricks database systems are configured to store information encrypted.	Inspected the AWS database baseline template configuration and the AWS encryption configuration for a selected database to determine whether databases were encrypted, and inspected Azure and GCP vendor backup documentation to determine whether databases were encrypted by default.	No exceptions noted.
		NET-12	Remote access to Databricks networks is restricted through an IT managed, encrypted VPN solution.	Inspected the VPN configuration and observed a user remotely VPN to determine whether remote access to the Databricks network and production environments are restricted through an encrypted VPN solution.	No exceptions noted.
				Observed a user attempt to access the Databricks network and production environments without VPN to determine whether the user was denied access.	No exceptions noted.

Additional Considerations Related to the HIPAA Security and Breach Notification Requirements Provided Within 45 CFR Sections 164.308-316 and 164.400-414

Criteria	HIPAA Security and Breach Notification Requirements	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
H56	§164.314(a)(1) Business Associate Contracts or Other Arrangements: The contract or other arrangement between the covered entity and its business associate required by §164.308(b) must meet the requirements of paragraph (a)(2)(i) or (a)(2)(ii) of this section, as applicable.	TPM-502	Subcontractors or subprocessors that create, receive, maintain, or transmit ePHI on behalf of Databricks, have appropriate contractual agreements in place to protect ePHI.	Inspected the contractual agreements for a selection of subcontractors to determine whether they have agreements in place to protect ePHI.	No exceptions noted.
H57	§164.314(a)(2)(i) Business Associate Contracts: The contract between a covered entity and a business associate must provide that the business associate will: (A) Comply with the applicable requirements of this subpart; (B) In accordance with §164.308(b)(2), ensure that any subcontractors that create, receive, maintain, or	TPM-05	Third-party confidentiality, Nondisclosure Agreements, and other contracts that reflect the organization's needs to protect systems and data, are implemented, and updated as necessary.	Inspected the Data Processing Agreement and Master Supplier Agreement templates to determine whether contracts are implemented and updated as necessary.	No exceptions noted.
				Inspected signed contracts for a selection of new third parties to determine whether the confidentiality and Nondisclosure Agreements or other applicable contracts were signed, as necessary.	No exceptions noted.

Additional Considerations Related to the HIPAA Security and Breach Notification Requirements Provided Within 45 CFR Sections 164.308-316 and 164.400-414

Criteria	HIPAA Security and Breach Notification Requirements	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
	transmit electronic protected health information on behalf of the business associate agree to comply with the applicable requirements of this subpart by entering into a contract or other arrangement that complies with this section; and (C) Report to the covered entity any security incident of which it becomes aware, including breaches of unsecured protected health information as required by §164.410.	TPM-502	Subcontractors or subprocessors that create, receive, maintain, or transmit ePHI on behalf of Databricks, have appropriate contractual agreements in place to protect ePHI.	Inspected the contractual agreements for a selection of subcontractors to determine whether they have agreements in place to protect ePHI.	No exceptions noted.
H58	§164.314(a)(2)(ii) Other Arrangements: The covered entity is in compliance with paragraph (a)(1) of this Section If it has another arrangement in place that meets the requirements of §164.504(e)(3).	Not Applicable — The entity is not a government entity.			

Additional Considerations Related to the HIPAA Security and Breach Notification Requirements Provided Within 45 CFR Sections 164.308-316 and 164.400-414

Criteria	HIPAA Security and Breach Notification Requirements	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
H59	§164.314(a)(2)(iii) Business Associate Contracts with Subcontractors: The requirements of paragraphs (a)(2)(i) and (a)(2)(ii) of this section apply to the contract or other arrangement between a business associate and a subcontractor required by §164.308(b)(4) in the same manner as such requirements apply to contracts or other arrangements between a covered entity and business associate.	TPM-05	Third-party confidentiality, Nondisclosure Agreements, and other contracts that reflect the organization's needs to protect systems and data, are implemented, and updated as necessary.	Inspected the Data Processing Agreement and Master Supplier Agreement templates to determine whether contracts are implemented and updated as necessary.	No exceptions noted.
				Inspected signed contracts for a selection of new third parties to determine whether the confidentiality and Nondisclosure Agreements or other applicable contracts were signed, as necessary.	No exceptions noted.
		TPM-502	Subcontractors or subprocessors that create, receive, maintain, or transmit ePHI on behalf of Databricks, have appropriate contractual agreements in place to protect ePHI.	Inspected the contractual agreements for a selection of subcontractors to determine whether they have agreements in place to protect ePHI.	No exceptions noted.
H60	§164.314(b) Group Health Plans	Not Applicable — Databricks is not a group health plan.			

Additional Considerations Related to the HIPAA Security and Breach Notification Requirements Provided Within 45 CFR Sections 164.308-316 and 164.400-414

Criteria	HIPAA Security and Breach Notification Requirements	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
H61	§164.316(a) Policies and Procedures: Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in §164.306(b)(2)(i), (ii), (iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.	GOV-02	Security policies and procedures are documented, communicated, made available on the internal Databricks network to appropriate personnel, and versions are maintained.	Inspected the internal Databricks network and the security policies and procedures to determine whether they are formally documented, maintained, and made available to Databricks personnel.	No exceptions noted.
				Inspected the annual security policy certification to determine whether the security policy has been communicated as part of the annual security training.	No exceptions noted.
		GOV-03	Security policies and procedures are reviewed and approved at least annually or if significant changes occur.	Inspected the DocuSign approval by the CSO to determine whether security policies and procedures have been reviewed and approved within the last year.	No exceptions noted.

Additional Considerations Related to the HIPAA Security and Breach Notification Requirements Provided Within 45 CFR Sections 164.308-316 and 164.400-414

Criteria	HIPAA Security and Breach Notification Requirements	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
H62	§164.316(b)(1)(i) Documentation: Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form	GOV-02	Security policies and procedures are documented, communicated, made available on the internal Databricks network to appropriate personnel, and versions are maintained.	Inspected the internal Databricks network and the security policies and procedures to determine whether they are formally documented, maintained, and made available to Databricks personnel.	No exceptions noted.
				Inspected the annual security policy certification to determine whether the security policy has been communicated as part of the annual security training.	No exceptions noted.
		GOV-03	Security policies and procedures are reviewed and approved at least annually or if significant changes occur.	Inspected the DocuSign approval by the CSO to determine whether security policies and procedures have been reviewed and approved within the last year.	No exceptions noted.
H63	§164.316(b)(1)(ii) Documentation: if an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.	GOV-02	Security policies and procedures are documented, communicated, made available on the internal Databricks network to appropriate personnel, and versions are maintained.	Inspected the internal Databricks network and the security policies and procedures to determine whether they are formally documented, maintained, and made available to Databricks personnel.	No exceptions noted.
				Inspected the annual security policy certification to determine whether the security policy has been communicated as part of the annual security training.	No exceptions noted.

Additional Considerations Related to the HIPAA Security and Breach Notification Requirements Provided Within 45 CFR Sections 164.308-316 and 164.400-414

Criteria	HIPAA Security and Breach Notification Requirements	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
		GOV-03	Security policies and procedures are reviewed and approved at least annually or if significant changes occur.	Inspected the DocuSign approval by the CSO to determine whether security policies and procedures have been reviewed and approved within the last year.	No exceptions noted.
H64	§164.316(b)(2)(i) Time Limit: Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.	DCH-18	A records retention policy exists that establishes retention requirements in accordance with applicable statutory, regulatory, and contractual obligations.	Inspected the Data Retention Policy to determine whether requirements surrounding data retention had been established and documented.	No exceptions noted.
		GOV-02	Security policies and procedures are documented, communicated, made available on the internal Databricks network to appropriate personnel, and versions are maintained.	Inspected the internal Databricks network and the security policies and procedures to determine whether they are formally documented, maintained, and made available to Databricks personnel.	No exceptions noted.
				Inspected the annual security policy certification to determine whether the security policy has been communicated as part of the annual security training.	No exceptions noted.
H65	§164.316(b)(2)(ii) Availability: Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.	GOV-02	Security policies and procedures are documented, communicated, made available on the internal Databricks network to appropriate personnel, and versions are maintained.	Inspected the internal Databricks network and the security policies and procedures to determine whether they are formally documented, maintained, and made available to Databricks personnel.	No exceptions noted.

Additional Considerations Related to the HIPAA Security and Breach Notification Requirements Provided Within 45 CFR Sections 164.308-316 and 164.400-414

Criteria	HIPAA Security and Breach Notification Requirements	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
				Inspected the annual security policy certification to determine whether the security policy has been communicated as part of the annual security training.	No exceptions noted.
H66	§164.316(b)(2)(iii) Updates: Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.	GOV-03	Security policies and procedures are reviewed and approved at least annually or if significant changes occur.	Inspected the DocuSign approval by the CSO to determine whether security policies and procedures have been reviewed and approved within the last year.	No exceptions noted.
H67	§164.400 Applicability.	Note — Requirements are specified in the sections that follow.			
H68	§164.402 Definitions.	Note — This section is informational. Requirements are specified in the sections that follow.			
H69	§164.404 Notification to Individuals: §164.404(a) General Rule and Breaches Treated as Discovered §164.404(b) Timeliness of Notification §164.404(c) Content of Notification §164.404(d) Methods of Individual Notification	Not Applicable — The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers. Refer to §164.410 Notification by a Business Associate requirements below.			

Additional Considerations Related to the HIPAA Security and Breach Notification Requirements Provided Within 45 CFR Sections 164.308-316 and 164.400-414

Criteria	HIPAA Security and Breach Notification Requirements	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
H70	§164.406 Notification to the Media: (a) For a breach of unsecured protected health information involving more than 500 residents of a State or jurisdiction, a covered entity shall, following the discovery of the breach as provided in §164.404(a)(2), notify prominent media outlets serving the State or jurisdiction. (b) Timeliness of notification. Except as provided in §164.412, a covered entity shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a breach. (c) Content of notification. The notification required by paragraph (a) of this section shall meet the requirements of §164.404(c).	Not Applicable — The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.			

Additional Considerations Related to the HIPAA Security and Breach Notification Requirements Provided Within 45 CFR Sections 164.308-316 and 164.400-414

Criteria	HIPAA Security and Breach Notification Requirements	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
H71	§164.408 Notification to the Secretary: (a) A covered entity shall, following the discovery of a breach of unsecured protected health information as provided in §164.404(a)(2), notify the Secretary. (b) For breaches of unsecured protected health information involving 500 or more individuals, a covered entity shall, except as provided in §164.412, provide the notification required by paragraph (a) of this section contemporaneously with the notice required by §164.404(a) and in the manner specified on the HHS Web site.	Not Applicable — The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.			

Additional Considerations Related to the HIPAA Security and Breach Notification Requirements Provided Within 45 CFR Sections 164.308-316 and 164.400-414

Criteria	HIPAA Security and Breach Notification Requirements	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
	(c) For breaches of unsecured protected health information involving less than 500 individuals, a covered entity shall maintain a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, provide the notification required by paragraph (a) of this section for breaches discovered during the preceding calendar year, in the manner specified on the HHS web site.				
H72	§164.410(a)(1) Notification by a Business Associate: A business associate shall, following the discovery of a breach of unsecured protected health information, notify the covered entity of such breach.	IRO-01	A policy and procedure exist that establishes security incident response requirements.	Inspected the Security Incident Management Policy and Procedure to determine whether security incident response requirements are established.	No exceptions noted.
		IRO-10	Applicable security and privacy incidents are reported to internal stakeholders, affected clients, third parties, and regulatory authorities.	Inspected the Databricks Security Incident Management Procedure to determine whether Databricks has a procedure for reporting applicable security and privacy incidents to internal stakeholders, affected clients, third parties, and regulatory authorities.	No exceptions noted.

Additional Considerations Related to the HIPAA Security and Breach Notification Requirements Provided Within 45 CFR Sections 164.308-316 and 164.400-414

Criteria	HIPAA Security and Breach Notification Requirements	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
				Inspected tickets for a selection of security and privacy incidents to determine whether appropriate stakeholders were notified.	No exceptions noted.
H73	§164.410(a)(2) Breaches Treated as Discovered: For purposes of paragraph (a)(1) of this section, a breach shall be treated as discovered by a business associate as of the first day on which such breach is known to the business associate or, by exercising reasonable diligence, would have been known to the business associate. A business associate shall be deemed to have knowledge of a breach if the breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agent of the business associate (determined in accordance with the Federal common law of agency).	IRO-01	A policy and procedure exist that establishes security incident response requirements.	Inspected the Security Incident Management Policy and Procedure to determine whether security incident response requirements are established.	No exceptions noted.
		IRO-10	Applicable security and privacy incidents are reported to internal stakeholders, affected clients, third parties, and regulatory authorities.	Inspected the Databricks Security Incident Management Procedure to determine whether Databricks has a procedure for reporting applicable security and privacy incidents to internal stakeholders, affected clients, third parties, and regulatory authorities.	No exceptions noted.
				Inspected tickets for a selection of security and privacy incidents to determine whether appropriate stakeholders were notified.	No exceptions noted.
		IRO-501	Security and privacy incidents are documented, tracked, and a root cause analysis is performed.	Inspected the tickets for a selection of security and privacy incidents to determine whether incidents were documented, tracked, and a root cause analysis was performed.	No exceptions noted.

Additional Considerations Related to the HIPAA Security and Breach Notification Requirements Provided Within 45 CFR Sections 164.308-316 and 164.400-414

Criteria	HIPAA Security and Breach Notification Requirements	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
H74	§164.410(b) Timeliness of Notification: Except as provided in §164.412, a business associate shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.	IRO-10	Applicable security and privacy incidents are reported to internal stakeholders, affected clients, third parties, and regulatory authorities.	Inspected the Databricks Security Incident Management Procedure to determine whether Databricks has a procedure for reporting applicable security and privacy incidents to internal stakeholders, affected clients, third parties, and regulatory authorities.	No exceptions noted.
				Inspected tickets for a selection of security and privacy incidents to determine whether appropriate stakeholders were notified.	No exceptions noted.
H75	§164.410(c)(1) Content of Notification: The notification required by paragraph (a) of this section shall include, to the extent possible, the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the business associate to have been, accessed, acquired, used, or disclosed during the breach.	IRO-10	Applicable security and privacy incidents are reported to internal stakeholders, affected clients, third parties, and regulatory authorities.	Inspected the Databricks Security Incident Management Procedure to determine whether Databricks has a procedure for reporting applicable security and privacy incidents to internal stakeholders, affected clients, third parties, and regulatory authorities.	No exceptions noted.
				Inspected tickets for a selection of security and privacy incidents to determine whether appropriate stakeholders were notified.	No exceptions noted.

Additional Considerations Related to the HIPAA Security and Breach Notification Requirements Provided Within 45 CFR Sections 164.308-316 and 164.400-414

Criteria	HIPAA Security and Breach Notification Requirements	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
H76	§164.410(c)(2) Content of Notification: A business associate shall provide the covered entity with any other available information that the covered entity is required to include in notification to the individual under §164.404(c) at the time of the notification required by paragraph (a) of this section or promptly thereafter as information becomes available.	IRO-10	Applicable security and privacy incidents are reported to internal stakeholders, affected clients, third parties, and regulatory authorities.	Inspected the Databricks Security Incident Management Procedure to determine whether Databricks has a procedure for reporting applicable security and privacy incidents to internal stakeholders, affected clients, third parties, and regulatory authorities.	No exceptions noted.
				Inspected tickets for a selection of security and privacy incidents to determine whether appropriate stakeholders were notified.	No exceptions noted.
H77	§164.412 Law Enforcement Delay: If a law enforcement official states to a covered entity or business associate that a notification, notice, or posting required under this subpart would impede a criminal investigation or cause damage to national security, a covered entity or business associate shall:	IRO-01	A policy and procedure exist that establishes security incident response requirements.	Inspected the Security Incident Management Policy and Procedure to determine whether security incident response requirements are established.	No exceptions noted.

Additional Considerations Related to the HIPAA Security and Breach Notification Requirements Provided Within 45 CFR Sections 164.308-316 and 164.400-414

Criteria	HIPAA Security and Breach Notification Requirements	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
	(a) If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or (b) If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described in paragraph (a) of this Section Is submitted during that time.				
H78	§164.414(a) Administrative requirements. A covered entity is required to comply with the administrative requirements of §164.530(b), (d), (e), (g), (h), (i), and (j) with respect to the requirements of this subpart.	Not Applicable — Databricks is not a covered entity.			

Additional Considerations Related to the HIPAA Security and Breach Notification Requirements Provided Within 45 CFR Sections 164.308-316 and 164.400-414

Criteria	HIPAA Security and Breach Notification Requirements	Control Number	Controls Specified by Databricks, Inc.	Tests of Controls Performed by BDO USA, P.A.	Results of Tests
H79	§164.414(b) Burden of Proof - In the event of a use or disclosure in violation of subpart E, the covered entity or business associate, as applicable, shall have the burden of demonstrating that all notifications were made as required by this subpart or that the use or disclosure did not constitute a breach, as defined at §164.402.	IRO-10	Applicable security and privacy incidents are reported to internal stakeholders, affected clients, third parties, and regulatory authorities.	Inspected the Databricks Security Incident Management Procedure to determine whether Databricks has a procedure for reporting applicable security and privacy incidents to internal stakeholders, affected clients, third parties, and regulatory authorities.	No exceptions noted.
				Inspected tickets for a selection of security and privacy incidents to determine whether appropriate stakeholders were notified.	No exceptions noted.