databricks

CUSTOMER COMPLIANCE MAPPING

Mapping FISC Security Guidelines to Databricks' Customer Capabilities

Version	
1.0	FISC Security Guidelines on Computer Systems for Financial Institutions, Thirteenth Edition (March 2025)

Contents

The FISC Security Guidelines on Computer Systems for Financial Institutions are organized into four primary divisions. This document walks each guideline unit and maps Databricks Data Intelligence Platform capabilities that help in-scope financial institutions meet the relevant control objectives.

Three-column reading guide. Each row pairs a FISC guideline number and category with the corresponding Databricks customer-capability mapping.

Shared responsibility. Refer to the Databricks Shared Responsibility Model alongside this guide. Customers remain accountable for organizational policies, contracts, and ongoing oversight.

N/A entries. Some guidelines fall outside the Databricks platform boundary (physical premises, branch operations, customer-managed procedures). Those rows are noted for completeness.

Cybersecurity & AI. The Thirteenth Edition strengthens cybersecurity requirements and introduces dedicated AI guidelines; both are mapped to Databricks platform capabilities.

01 GUIDELINE	02 CATEGORY	03 DATABRICKS CUSTOMER CAPABILITIES
C Common Standards		
C1 – C19	INTERNAL CONTROLS	N/A. Controls C1–C19 are internal management controls owned by the customer. Databricks provides supporting capabilities — Unity Catalog data governance, role-based access control, audit logging, and the Compliance Security Profile — but organizational policy, structure, and personnel management remain the customer's responsibility.
C1-1	CYBERSECURITY MANAGEMENT	▪ Policy ownership sits with the customer. Databricks supports operationalizing cybersecurity policy through the Databricks Security & Trust Center, the Shared Responsibility Model, and documented platform security baselines. ▪ Enforce policy technically with account- and workspace-level security settings, the Compliance Security Profile (CSP), and Enhanced Security Monitoring (ESM) for regulated workloads.
C1-2	CYBERSECURITY MANAGEMENT	▪ Codify cybersecurity rules as enforceable configuration: compute policies, Unity Catalog governance rules, IP access lists, and network/egress policies. ▪ Manage security configuration as code (Databricks Terraform provider and Asset Bundles) so rules are version-controlled, peer-reviewed, and applied consistently across workspaces.
C4-1	CYBERSECURITY MANAGEMENT	▪ Structure cybersecurity accountability using Databricks role separation — account admins, workspace admins, and Unity Catalog metastore admins — mapped to IdP groups via SCIM. ▪ Management and HR planning remain customer responsibilities; Databricks provides the role-based entitlements and admin governance to support them.
C4-2	CYBERSECURITY MANAGEMENT	▪ Continuously check platform security posture with system tables (system.access.audit, system.compute, etc.) and the Databricks Security Analysis Tool (SAT), which benchmarks workspace configuration against security best practices. ▪ Forward audit and configuration telemetry to your SIEM for ongoing control-effectiveness monitoring and alerting.
C5-1	CYBERSECURITY RISK MANAGEMENT	▪ Unity Catalog provides a central, governed inventory of data and AI assets (catalogs, schemas, tables, volumes, models, functions) with automated lineage and discovery. ▪ Use tags, Data Classification, and system.information_schema to identify and label sensitive assets so cybersecurity risk can be assessed against a complete asset inventory.
C5-2	CYBERSECURITY RISK MANAGEMENT	▪ Risk assessment and response planning are customer-owned processes; Databricks supplies the inputs — asset inventory and lineage (Unity Catalog), posture scoring (SAT), and threat telemetry (system tables, ESM). ▪ Response actions can be executed on-platform: revoke tokens and grants, disable principals, rotate customer-managed keys, and quarantine data via Unity Catalog.

01 GUIDELINE	02 CATEGORY	03 DATABRICKS CUSTOMER CAPABILITIES
C5-3	CYBERSECURITY RISK MANAGEMENT	▪ Databricks manages platform vulnerabilities: runtimes are regularly patched, and the Compliance Security Profile enforces CIS-hardened, FIPS 140-validated images with automatic security updates and automatic cluster (VM) update/restart. ▪ Constrain customer-introduced software with compute policies and allowlisted libraries; monitor Databricks security bulletins and use ESM host-level telemetry to detect vulnerable components.
C5-4	CYBERSECURITY RISK MANAGEMENT	▪ Cybersecurity exercises (tabletop and disaster-recovery drills) are customer-owned. Databricks supports failover and DR rehearsals through multi-region workspace deployments and Delta cross-region replication.
C5-5	CYBERSECURITY RISK MANAGEMENT	▪ Security-awareness education for the customer's workforce is a customer responsibility. Databricks provides product security documentation, the Security & Trust Center, and administrator training resources.
C20	OUTSOURCING MANAGEMENT	N/A. This control is an organizational outsourcingmanagement responsibility owned by the customer.
C21	OUTSOURCING MANAGEMENT	N/A. This control is an organizational outsourcingcontract responsibility owned by the customer.
C22	OUTSOURCING MANAGEMENT	N/A. Customers must still manage their own outsourcing, conduct risk assessments, and provide ongoing oversight.
C23	OUTSOURCING MANAGEMENT	N/A. This is a customer-managed control.
C24	USER OF CLOUD SERVICES	▪ Configure Databricks with cloud-specific controls: customer-managed VPC/VNet, PrivateLink, CMK, and cloud-native IAM roles for least-privilege access. ▪ Unity Catalog unifies governance and workspace isolation across multi-cloud deployments. For regulated workloads, enable ESM/CSP compute profiles.
C25	SHARED DATA CENTER	▪ Databricks is fully cloud-hosted on AWS, Azure, and GCP: no owned data centers. Physical security (biometric access, CCTV, power redundancy) is managed by each CSP under ISO 27001, SOC 1/2, and PCI-DSS; Databricks reviews CSP audit reports annually. ▪ Databricks security commitments are set out in the MCSA and Security Addendum, independently verified annually. See the Databricks Trust Center.
C26	SERVICES ON FINANCIAL INSTITUTIONS' MUTUAL SYSTEM NETWORK	▪ Connect mutual financial network data via private VPC/VNet with full audit logging. Unity Catalog enforces access control and lineage for mutual-network data. ▪ Use Delta Sharing and Clean Rooms for secure cross-institution analytics with strict row/column- level permissions and no data copying. ▪ For tighter runtime security, run workloads on ESM/CSP-enabled clusters.

01 GUIDELINE	02 CATEGORY	03 DATABRICKS CUSTOMER CAPABILITIES
C27	COOPERATION WITH FINANCIAL TECHNOLOGY (FINTECH) COMPANIES	N/A. This is a customer-managed control.
C28	SUPPLY CHAIN MANAGEMENT	▪ Databricks manages its own supply chain (sub-processors, third-party components) and evidences it through SOC 1/2, ISO 27001/27017/27018, and PCI-DSS attestations in the Trust Center; customers inherit these assurances under the shared responsibility model. ▪ Govern your own data and AI supply chain on-platform: control third-party data sources and models through Unity Catalog, Lakehouse Federation, Partner Connect, and Marketplace, with lineage and access controls applied uniformly.

MAPPING FISC SECURITY GUIDELINES · DATABRICKS' CUSTOMER CAPABILITIES

01 GUIDELINE	02 CATEGORY	03 DATABRICKS CUSTOMER CAPABILITIES
P	**Practical Guidelines**	
P1	DATA PROTECTION	▪ Integrate with your IdP via SSO with MFA enforced at the IdP. Use SCIM for user lifecycle management. ▪ Replace long-lived PATs with OAuth token federation for both users and service principals. Unity Catalog enforces least-privilege data access based on these identities.
P2	DATA PROTECTION	N/A. This is a customer-managed control. Databricks does not interact directly with terminals on public networks.
P3	DATA PROTECTION	▪ Enable at-rest encryption on cloud storage (S3/ADLS/GCS); use CMK for workspace and storage where required. Unity Catalog enforces RBAC, row filters and column masking, with catalog-to- workspace binding to restrict sensitive data to approved workspaces. ▪ Register external databases (PostgreSQL, Snowflake, etc.) as Lakehouse Federation foreign catalogs to apply the same UC policies without copying data. Use Data Classification and ABAC to automatically tag and protect sensitive columns.
P4	DATA PROTECTION	▪ Enforce TLS 1.2+ for all connections; use PrivateLink and private endpoints to keep traffic off the public internet. Apply IP access lists and context-based ingress policies. ▪ Use network policies (Serverless Egress Control) to enforce a deny-by-default outbound posture across serverless compute (notebooks, jobs, SQL, and model serving); some deny-by-default controls are in preview. Store credentials in Databricks Secrets rather than in code. ▪ Apply Unity Catalog least-privilege and row/column-level controls. Forward audit logs to your SIEM and alert on anomalous download patterns or egress denials.

01 GUIDELINE	02 CATEGORY	03 DATABRICKS CUSTOMER CAPABILITIES
P5	DATA PROTECTION	▪ Use Unity Catalog as the primary access layer: expose data as tables and volumes, granting fine- grained privileges (SELECT, MODIFY, OWNERSHIP) to approved users and service principals only. ▪ Combine with workspace ACLs and cloud-storage IAM. Enable audit logs and system tables to record object access. Run regulated workloads on ESM/CSP-enabled clusters.
P6	DATA PROTECTION	▪ Use Lakeflow Declarative Pipelines (formerly Delta Live Tables) expectations to drop, quarantine, or flag invalid records during ingestion. Delta Lake constraints (NOT NULL, CHECK) catch schema violations at write time. ▪ Lakehouse Monitoring continuously profiles tables for freshness, volume, and quality anomalies. Unity Catalog lineage traces defective data to upstream sources.
P7	DATA PROTECTION	▪ Use Delta Lake's ACID transaction log and time travel to detect unauthorized changes. Route audit logs to your SIEM with detection rules for anomalous write events. ▪ Register models in the Unity Catalog Model Registry (MLflow) for version-controlled promotion workflows with full audit trails per model transition. Enable CSP for FIPS 140-validated encryption and CIS-hardened OS images on compute.
P8	PREVENTION OF UNAUTHORIZED USE	▪ Integrate with your enterprise IdP via SSO; enforce MFA, conditional access, and device posture at the IdP. Manage identities via SCIM. ▪ Use OAuth token federation so users and service principals exchange IdP tokens for short-lived Databricks OAuth tokens. Enable single-use refresh tokens for U2M flows. Review and revoke PATs via the account-level token report. ▪ Run regulated workloads on ESM/CSP compute to correlate identity events with host-level telemetry.
P9	PREVENTION OF UNAUTHORIZED USE	▪ Configure MFA, risk-based conditional access, and prohibit shared credentials via your IdP. Use SCIM to deprovision identities promptly on role changes or departures. ▪ Replace PATs with OAuth token federation; enable single-use refresh tokens to prevent replay attacks. Regularly review the token report to revoke unused or non-expiring tokens. ▪ Unity Catalog limits blast radius via least-privilege access even when credentials are compromised.
P10	PREVENTION OF UNAUTHORIZED USE	▪ Enable account-level audit log delivery and the audit log system table to capture sign-ins, token use, cluster/job operations, SQL queries, and permission changes. Forward to cloud storage and your SIEM. ▪ Use the token report to audit PAT inventory across workspaces. Unity Catalog provides detailed data access records and lineage for full traceability.
P11	PREVENTION OF UNAUTHORIZED USE	▪ Use Unity Catalog privileges to limit operations per role: grant SELECT for read-only access; restrict INSERT, UPDATE, DELETE, and OWNERSHIP to controlled groups. Apply row filters and column masking to limit visible data per user. ▪ Use compute policies to restrict compute creation by role and SQL warehouse permissions to control warehouse access.

01 GUIDELINE	02 CATEGORY	03 DATABRICKS CUSTOMER CAPABILITIES
P12	PREVENTION OF UNAUTHORIZED USE	▪ Cancel active job runs and stop clusters via the Jobs and Clusters APIs during incidents. Use Unity Catalog to revoke INSERT/UPDATE/DELETE/MODIFY privileges on affected tables. ▪ Use audit logs to identify which principals performed actions at incident time. Use Delta Lake time travel to restore data to a pre-incident state.
P13	PREVENTION OF UNAUTHORIZED USE	▪ Databricks delegates key storage to cloud KMS (AWS KMS, Azure Key Vault, GCP Cloud KMS). Configure CMK with least-privilege IAM roles so only designated workspaces can perform wrap/unwrap operations. ▪ Unity Catalog external locations govern access to CMK-protected storage without distributing keys to users. Use Lakehouse Federation to connect to external sources without sharing credentials.
P14	PREVENTION OF UNAUTHORIZED ACCESS FROM EXTERNAL NETWORKS	▪ Enforce SSO with MFA and conditional access via your IdP. Manage identities centrally via SCIM and prefer OAuth token federation over long-lived PATs. ▪ Monitor logins, token usage, and admin changes via audit logs. Revoke unused credentials regularly. Run regulated workloads on CSP/ESM-enabled compute.
P14-1	PREVENTION OF UNAUTHORIZED ACCESS FROM EXTERNAL NETWORKS	▪ Enhanced Security Monitoring (ESM) adds host-level monitoring agents — antivirus, file-integrity monitoring, and vulnerability scanning — plus advanced threat detection on hardened classic compute for regulated workloads. ▪ Stream audit logs and system tables to your SIEM and apply correlation rules to detect early indicators of compromise — privilege escalation, anomalous geographies, unusual service-principal activity, and abnormal data egress.
P14-2	PREVENTION OF UNAUTHORIZED ACCESS FROM EXTERNAL NETWORKS	▪ Databricks performs regular independent penetration tests and vulnerability assessments of the platform; results are summarized in SOC 2 and available under NDA via the Trust Center. ▪ Customers may run their own vulnerability scans and penetration tests of their workloads in line with the Databricks penetration testing policy; CSP-hardened images reduce the platform attack surface.
P15	PREVENTION OF UNAUTHORIZED ACCESS FROM EXTERNAL NETWORKS	▪ Restrict access to approved networks via PrivateLink, IP access lists, and context-based ingress. Use customer-managed VPCs and compute policies to avoid public IPs on compute. ▪ Replace long-lived PATs with OAuth token federation to reduce credential exposure. Bind sensitive Unity Catalog catalogs to designated workspaces. Enable ESM/CSP for host-level security on exposed workloads.
P16	MEASURES TO DETECT UNAUTHORIZED ACCESS	▪ Enforce PrivateLink, compute policies, and context-based network policies to prevent direct internet egress. Use network policies (Serverless Egress Control) for a deny-by-default egress posture across serverless compute; some controls are in preview. ▪ Route audit logs and system tables to your SIEM for anomaly detection. Unity Catalog constrains which data objects are accessible from externally-connected workspaces. Enable ESM/CSP for host-level telemetry.

01 GUIDELINE	02 CATEGORY	03 DATABRICKS CUSTOMER CAPABILITIES
P17	MEASURES TO DETECT UNAUTHORIZED ACCESS	▪ Use Databricks SQL and Lakehouse Monitoring to detect anomalous transaction patterns (e.g., isolation-forest models on streaming or batch data). Configure SIEM alerts from audit logs. ▪ Unity Catalog lineage attributes unusual transactions to upstream jobs or users. Enable ESM/CSP for additional host-level behavioral telemetry.
P18	MEASURES TO DETECT UNAUTHORIZED ACCESS	▪ Build exception-monitoring pipelines (SQL queries or streaming jobs filtering threshold breaches) and expose results via dashboards and alerts. Use audit logs and system tables with your SIEM to detect bulk exports or mass updates. ▪ Unity Catalog fine-grained access control and lineage help focus monitoring on high-sensitivity catalogs. Enable ESM/CSP for host-level telemetry.
P19	RESPONSE MEASURES FOR UNAUTHORIZED ACCESS	▪ On detection, revoke tokens, disable accounts, rotate credentials, and reconfigure workspace or network settings. Sync users and groups via SCIM. ▪ Use Delta Lake time travel to restore data to a pre-incident state. Unity Catalog lets you revoke all privileges for compromised users and rebuild tables from trusted sources.
P20	MEASURES AGAINST MALICIOUS PROGRAMS	▪ Follow secure-coding guidelines in notebooks and jobs. Unity Catalog limits blast radius by restricting what data a compromised workload can access or write. ▪ Enable ESM/CSP, which adds hardened OS images, antivirus/malware detection, file-integrity monitoring, and host-level security telemetry forwarded to your SIEM.
P21	MEASURES AGAINST MALICIOUS PROGRAMS	▪ Use compute policies to restrict allowed compute images, libraries, and init scripts; limit package installation to approved sources. Unity Catalog enforces least-privilege access to tables, volumes, and external locations. ▪ Enable ESM/CSP for antivirus/malware detection, behavioral monitoring, file-integrity monitoring, and vulnerability reporting on compute nodes.
P22	MEASURES AGAINST MALICIOUS PROGRAMS	▪ Restrict runtimes and libraries via compute policies; minimize outbound internet access. Apply Unity Catalog least-privilege permissions to limit data exposure. Enable ESM/CSP for antivirus/malware detection and file-integrity monitoring. ▪ Recover corrupted data using Delta Lake time travel and versioned tables, complemented by backups in your cloud account.
P23	DOCUMENTATION	N/A. This is a customer-managed control.
P24	DOCUMENTATION	N/A. This is a customer-managed control.
P25	MANAGEMENT OF ACCESS RIGHTS	▪ Assign account roles, workspace entitlements, and Unity Catalog privileges via IdP-synced SCIM groups. Use OAuth token federation so users and service principals exchange IdP tokens for short-lived Databricks OAuth tokens. ▪ Enable Databricks-native MFA only when SSO is not configured. Apply CSP on workspaces handling regulated data. Use Lakehouse Federation for governed access to external data systems.

01 GUIDELINE	02 CATEGORY	03 DATABRICKS CUSTOMER CAPABILITIES
P26	MANAGEMENT OF ACCESS RIGHTS	▪ Centralize authentication via IdP SSO and SCIM; avoid local Databricks credentials. Use OAuth token federation for service principals to eliminate PAT management. Enable single-use refresh tokens and configurable session lifetimes for U2M flows. ▪ Store credentials in Databricks Secrets rather than in notebooks or job configurations. Review and revoke unused PATs via the token report.
P27	MANAGEMENT OF ACCESS RIGHTS	▪ Implement joiner/mover/leaver workflows by syncing your IdP to Databricks via SCIM, assigning roles and entitlements per approved access requests. Use audit logs and system tables to evidence authentication and privilege changes for periodic access reviews. ▪ Centralize data authorization via Unity Catalog grants; include Lakehouse Federation foreign catalog privileges in the same review process. Enable CSP on workspaces handling regulated data.
P28	MANAGEMENT OF ACCESS RIGHTS	▪ Use Unity Catalog to organize and govern data as catalogs, schemas, tables, views, and volumes, managing permissions via grants. Use SQL warehouses as the governed query interface. ▪ Register external JDBC databases as Lakehouse Federation foreign catalogs and manage access through Unity Catalog grants. Use Delta Sharing to govern external data sharing without copying underlying data.
P29	DATA MANAGEMENT	▪ Use Delta Lake's versioned tables, ACID transaction log, and time travel as the technical basis for data revision control. Use Git Folders and Declarative Automation Bundles (DABs) for controlled ETL promotion across environments. ▪ Unity Catalog centralizes ownership and lineage for data-level revision. Register models in the Unity Catalog Model Registry (MLflow) for version-controlled promotion workflows with full audit trails.
P30	DATA MANAGEMENT	▪ Configure CMK with cloud KMS for workspace and storage encryption. Use audit logs and cloud KMS logs together to verify keys are used per operational procedures. ▪ Unity Catalog ensures only CMK-protected storage locations are used for sensitive catalogs. Enable CSP for stricter baselines on cryptographic operations.
P31	DATA MANAGEMENT	N/A. This is a customer-managed control.
P32	COMPUTER ANTIVIRUS PROTECTION	▪ Enforce compute policies to constrain runtime versions, images, and init scripts; restrict package installation to curated private repositories. Unity Catalog limits blast radius via fine-grained permissions on catalogs, schemas, tables, volumes, and external locations. ▪ Enable ESM/CSP for antivirus/malware detection, file-integrity monitoring, and vulnerability scanning on compute nodes, with security events forwarded to your SIEM.
P33	EXTERNAL CONNECTION MANAGEMENT	▪ Implement external connection conditions through customer-managed VPCs, PrivateLink or private endpoints, and IP access lists so only approved networks reach Databricks. ▪ Bind sensitive Unity Catalog catalogs to specific workspaces to align data boundaries with network rules. Use audit logs and system tables to demonstrate that external access follows agreed-upon conditions. Mandate ESM/CSP clusters for externally-connected workloads.

01 GUIDELINE	02 CATEGORY	03 DATABRICKS CUSTOMER CAPABILITIES
P34	EXTERNAL CONNECTION MANAGEMENT	▪ Monitor approved external connections by reviewing audit logs and system tables for anomalous access patterns. Periodically review IP access lists and PrivateLink endpoint configurations. ▪ Validate via the token report that only approved principals hold credentials with external-access scope.
P35	MANAGEMENT OF OPERATIONS	▪ Tie high-privilege roles (account admin, workspace admin, compute policy admin) to specific IdP groups so only qualified staff can be added. Require all operator credentials to be issued via OAuth token federation, gating service principal access on IdP group membership. ▪ Use the token report in periodic operator-qualification reviews alongside IdP group membership audits. Unity Catalog ownership and privileges distinguish data stewards from general users.
P36	MANAGEMENT OF OPERATIONS	▪ Govern Databricks role and group assignments through ITSM/IdP change-management workflows, validated via audit logs and system tables. Include the token report as a mandatory step in both provisioning (verify new operator token appears with expected scope/expiry) and deprovisioning (verify tokens are revoked). ▪ Unity Catalog supports procedure-driven operations via SQL scripts or automated pipelines for grants and ownership changes.
P37	MANAGEMENT OF OPERATIONS	▪ Structure operations teams using Databricks account admin, workspace admin, and metastore admin roles mapped to SCIM groups. Unity Catalog formalizes data governance responsibilities via ownership and privilege control at catalog, schema, and table levels.
P38	MANAGEMENT OF OPERATIONS	▪ Audit logs and system tables record all operations: cluster/job management, SQL queries, permission changes, workspace configuration. Forward to cloud storage or SIEM for long-term retention and alerting. ▪ Schedule regular token report exports as a supplementary credential-layer operational record. Unity Catalog provides detailed records of grants, revocations, and data-access operations.
P39	DATA FILE MANAGEMENT	N/A. Customers are responsible for implementing data backup and recovery strategies appropriate to their business and compliance requirements.
P40	PROGRAM FILE MANAGEMENT	▪ Manage notebooks, jobs, and libraries using Git Folders with workspace folder permissions. Use compute policies to define approved library sources and versions, and branch-based workflows with CI/CD for dev/test/prod promotion.
P41	PROGRAM FILE MANAGEMENT	▪ Use Git Folders as the source of truth for notebooks, jobs, and code, with branch-based versioning backed by your Git provider. Export non-Repo workspace objects (legacy notebooks, job definitions) regularly via APIs to cloud storage.
P42	NETWORK CONFIGURATION MANAGEMENT	▪ Manage VPCs/VNets, subnets, security groups, and PrivateLink endpoints in your cloud account; track configuration in your CMDB or IaC tooling. Unity Catalog catalog bindings help map data domains to specific network segments.

01 GUIDELINE	02 CATEGORY	03 DATABRICKS CUSTOMER CAPABILITIES
P43	NETWORK CONFIGURATION MANAGEMENT	• Use IaC (Terraform/CloudFormation/ARM) and version control as the primary backup for cloud network configuration. Export workspace networking settings (IP access lists) via APIs or IaC templates. Maintain catalog-to-workspace bindings under version control as part of your network-to-data mapping.
P44	DOCUMENT MANAGEMENT DURING SYSTEM OPERATION	• Store operational runbooks, diagrams, and configuration baselines in Git or Confluence. Host technical runbooks as notebooks in Databricks Git Folders. Use Unity Catalog to attach documentation to data assets for discoverability alongside the datasets they support.
P45	DOCUMENT MANAGEMENT DURING SYSTEM OPERATION	• Back up operational documents in redundant Git repositories or document management systems. Sync Databricks notebooks and queries to Git via Git Folders. Export Unity Catalog metadata via APIs/SQL for backup and DR planning.
P46	MONITORING OF OPERATIONS	• Query system tables (billing.usage, compute logs, job run histories, data quality results, access.audit) via Databricks SQL to build operational dashboards and alerts. Export insights to observability or SIEM platforms. • Enable CSP/ESM on critical workspaces to ensure dashboards reflect a secure and compliant infrastructure baseline.
P47	RESOURCE MANAGEMENT	N/A. This is a customer-managed control.
P48	RESOURCE MANAGEMENT	• Databricks is a PaaS deployed entirely on AWS, Azure, and GCP. Physical hardware and device maintenance are governed by those CSPs under ISO 27001, SOC 1/2, and PCI-DSS: Databricks reviews CSP audit reports annually. • At the software layer, Databricks maintains an ISMS, documented change management, a secure SDLC (SAST/DAST, vulnerability scanning), and customer commitments under the MCSA and Security Addendum (SOC 1/2 Type II, ISO 27001/27017/27018, HIPAA, PCI-DSS). Details: Databricks Trust Center.
P49	DEVICE MANAGEMENT	N/A. This is a customer-managed control.
P50	DEVICE MANAGEMENT	N/A. This is a customer-managed control.
P51	DEVICE MANAGEMENT	N/A. This is a customer-managed control.
P52	DEVICE MANAGEMENT	N/A. Databricks does not operate its own physical data centers; production services are hosted in data centers managed by AWS, Microsoft Azure, and Google Cloud Platform, and physical security and environmental controls for those facilities are therefore provided by these cloud service providers.
P53	DEVICE MANAGEMENT	N/A. This is a customer-managed control.

01 GUIDELINE	02 CATEGORY	03 DATABRICKS CUSTOMER CAPABILITIES
P54	MAINTENANCE AND MANAGEMENT OF COMPUTER-RELATED EQUIPMENT	N/A. This is a customer-managed control.
P55	MAINTENANCE AND MANAGEMENT OF COMPUTER-RELATED EQUIPMENT	N/A. This is a customer-managed control.
P56	PHYSICAL ACCESS CONTROL (BUILDING AND ROOMS)	N/A. This is a customer-managed control.
P57	PHYSICAL ACCESS CONTROL (BUILDING AND ROOMS)	N/A. This is a customer-managed control.
P58	PHYSICAL ACCESS CONTROL (BUILDING AND ROOMS)	N/A. This is a customer-managed control.
P59	PHYSICAL ACCESS CONTROL (BUILDING AND ROOMS)	N/A. This is a customer-managed control.
P60	PHYSICAL ACCESS CONTROL (BUILDING AND ROOMS)	N/A. This is a customer-managed control.
P61	MONITORING	▪ Define operational authority using RBAC (account/workspace admin roles, Unity Catalog privileges, group-based entitlements). Treat admin credentials as operator-level access governed by formal approval, stored in Databricks Secrets, and periodically recertified via the token report. ▪ Enable audit logging and system tables; forward to SIEM with alerts for high-risk actions (bulk exports, privilege escalations). Validate data input via Unity Catalog privileges, Delta Lake constraints, and Lakehouse Monitoring.
P62	MONITORING	N/A. This is a customer-managed control.
P63	MONITORING	N/A. This is a customer-managed control.
P64	MONITORING	N/A. This is a customer-managed control.
P65	MONITORING	N/A. This is a customer-managed control.

01 GUIDELINE	02 CATEGORY	03 DATABRICKS CUSTOMER CAPABILITIES
P66	MONITORING	N/A. Databricks does not provide full DLP for off-platform exports (email, print). Customers must enforce downstream controls for printed or exported data.Databricks compute policies restrict allowed images, libraries, and init scripts, while workspace export controls (notebook exports, result downloads, dashboard creation) limit the introduction and movement of malicious files. Unity Catalog enforces least-privilege access with fine-grained row/column filtering, masking, and centralized audit of read operations.Furthermore, customers may use Databricks Data Classification to detect and tag sensitive columns (PII, financial data, confidential) without manual intervention. Automatic classification feeds into Attribute-Based Access Control (ABAC) policies (Public Preview), enabling row filters, column masks, and workspace bindings to be applied based on classification labels rather than hand-maintained lists. Classification results should be reviewed periodically by data stewards and reconciled with your data inventory for FISC evidence. For high-risk or regulated workloads, run compute on ESM/CSP-enabled clusters, which provide hardened images, host-based antivirus/malware detection, file-integrity monitoring, and vulnerability scanning. Security events feed into audit logs and system tables that can be streamed to a SIEM to detect suspicious script execution, library downloads, and anomalous exports. Complement this with network egress controls such as PrivateLink and IP access lists.
P67	MONITORING	▪ Management of physical printed forms is outside the Databricks platform and must be governed by your organization's records management policy. For digital equivalents (report templates, notebook-generated reports), manage in Git Folders and restrict access via workspace permissions. ▪ Unity Catalog controls access to underlying datasets referenced by such forms.
P68	MONITORING	N/A. This is a customer-managed control.
P69	MONITORING	▪ Enforce SSO/MFA, least-privilege groups, and workspace security baselines (PrivateLink, compute policies, Databricks Secrets, controlled export paths). Enable encryption at rest and in transit; route audit logs to a SIEM. ▪ Unity Catalog provides centralized access control, row filters/column masking, data classification, lineage, and system tables for audit and usage tracking. Run regulated workloads on ESM/CSP- enabled clusters.
P70	USE OF SYSTEMS	▪ Databricks does not prescribe incident communication runbooks, but customers can use platform signals as inputs: subscribe to the Databricks status page, configure job/cluster/SQL warehouse alerts, and integrate audit logs and system tables into your SIEM. ▪ Unity Catalog maps data products to their owners and stewards, facilitating rapid identification of responsible parties during incidents. For platform incidents, use Databricks Support and the Trust Center.
P71	MEASURES FOR HANDLING FAILURES AND DISASTER-RESPONSIVE MEASURES	▪ Deploy primary and secondary Databricks workspaces in different AWS regions with cloud-native storage replication meeting your RPO/RTO. Back up critical notebooks, workflows, and configuration artifacts using Git Folders and DABs. ▪ Unity Catalog supports DR via per-region metastores, enabling reconstruction of catalogs, access controls, and data locations during failover. Enable CSP/ESM on both primary and DR workspaces for a consistent hardened baseline.

01 GUIDELINE	02 CATEGORY	03 DATABRICKS CUSTOMER CAPABILITIES
P72	ESTABLISH PROCESSES FOR RECOVERY FROM SYSTEM FAILURES AND DISASTERS	▪ Use cluster, job, and SQL warehouse logs, system tables, and audit logs to diagnose failures (configuration errors, resource exhaustion, code bugs). Forward events to observability tools for cross-system correlation. ▪ Unity Catalog lineage identifies upstream causes and blast radius in data pipeline failures. Run DR investigation workloads on CSP/ESM-enabled workspaces.
P73	DEVELOPMENT OF CONTINGENCY PLANS	▪ Define a contingency plan covering DR triggers, roles, communication paths, and failback steps. Leverage secondary workspaces in different regions, Delta Lake backup/restore procedures, and Jobs/workflow failover runbooks. ▪ Use audit logs and system tables to validate the plan and refine RPO/RTO through DR tests. Unity Catalog per-region metastores and Delta Sharing enable structured data access continuity. Run DR procedures on CSP/ESM-enabled workspaces.
P73-1	DEVELOPMENT OF CONTINGENCY PLANS	▪ Databricks operates a documented security incident response program and notifies affected customers in accordance with the Security Addendum. ▪ Build cyber-specific contingency plans on-platform: cross-region workspace/DR failover, Delta Lake time travel and restore for ransomware or tampering recovery, and SIEM-driven detection feeding your incident-response runbooks.
P74	BACKUP CENTERS	▪ Deploy separate Databricks workspaces in multiple AWS regions as logical primary and DR centers. Enable cross-region replication or periodic backups of Delta Lake tables and workspace configuration (via IaC and Databricks APIs). ▪ Unity Catalog requires a separate metastore per region, each acting as an independent governance center. Enable CSP/ESM on both primary and backup workspaces for consistent hardened baselines.
P75	MANAGEMENT OF THE DEVELOPMENT AND MODIFICATION OF THE SYSTEM	▪ Define SDLC using Git Folders (branching, pull requests, code review) and Declarative Automation Bundles (DABs) to promote notebooks, workflows, compute policies, and SQL objects across dev/test/prod workspaces. ▪ Enforce separation of duties via workspace permissions (restrict production deployments to service principals) and compute policies. Unity Catalog supports governed SDLC via separate catalogs per environment and workspace-catalog bindings.
P76	MANAGEMENT OF THE DEVELOPMENT AND MODIFICATION OF THE SYSTEM	▪ Establish separate dev, test, and staging workspaces from production. Use Git Folders plus DABs to promote code and configurations only after automated tests and approvals. Unity Catalog provides environment isolation via separate catalogs and workspace-catalog bindings. ▪ Manage production workspaces via IaC with audit logs and system tables providing deployment evidence. Enable CSP/ESM on all SDLC workspaces that process regulated data.
P77	MANAGEMENT OF THE DEVELOPMENT AND MODIFICATION OF THE SYSTEM	N/A. This is a customer-managed control.

01 GUIDELINE	02 CATEGORY	03 DATABRICKS CUSTOMER CAPABILITIES
P78	DOCUMENT MANAGEMENT DURING DEVELOPMENT AND MODIFICATION	▪ Manage development documentation via Git Folders, which version notebooks, SQL files, and pipeline definitions in an external Git provider. Use DABs for infrastructure-as-code artifact versioning and lifecycle management.
P79	DOCUMENT MANAGEMENT DURING DEVELOPMENT AND MODIFICATION	N/A. This is a customer-managed control.
P80	PACKAGE INSTALLATION	▪ Restrict library installation to an approved set using compute policies that auto-install allowlisted libraries and block ad-hoc user installs. Connect to private package repositories via Databricks Secrets and workspace configuration. ▪ Unity Catalog workspace-catalog bindings isolate evaluation clusters to non-sensitive catalogs. Enable ESM/CSP on evaluation and production clusters for runtime antivirus and file-integrity monitoring.
P81	PACKAGE INSTALLATION	N/A. This is a customer-managed control.
P82	DISPOSAL OF SYSTEMS	▪ Execute disposal plans using admin UI, APIs, and CLI to delete workspaces, clusters, jobs, and workspace objects. Use Delta Lake lifecycle controls (VACUUM, retention configuration) and cloud-storage lifecycle policies to physically remove retired data. ▪ Unity Catalog provides governed disposal via catalog/schema/table drops and privilege revocation through SQL, CLI, or Terraform: preventing post-disposal access via orphaned objects or stale permissions. Enable ESM/CSP on final disposal/migration workloads.
P83	DISPOSAL OF SYSTEMS	N/A. This is a customer-managed control.
P84	BACKUP FOR HARDWARE	N/A. This is a customer-managed control.
P85	BACKUP FOR HARDWARE	N/A. This is a customer-managed control.
P86	BACKUP FOR HARDWARE	N/A. This is a customer-managed control.
P87	BACKUP FOR HARDWARE	N/A. This is a customer-managed control.
P88	BACKUP FOR HARDWARE	N/A. This is a customer-managed control.

01 GUIDELINE	02 CATEGORY	03 DATABRICKS CUSTOMER CAPABILITIES
P89	MEASURES TO IMPROVE THE QUALITY OF SOFTWARE	▪ Implement a secure SDLC using Git Folders, DABs, and Unity Catalog governance across all environments. In design, define architecture as code with PR-based review and least-privilege policies built in. In implementation, use protected branches with required reviews and SAST/DAST in CI. ▪ Deploy to non-production workspaces via DABs with automated tests (unit, integration, data- quality) before production promotion. Standardize on Databricks Runtime LTS releases. Restrict library sources via compute policies. ▪ Enable ESM/CSP on all environments handling regulated workloads for consistent antivirus, file- integrity, and vulnerability scanning across the full SDLC.
P90	MEASURES TO IMPROVE THE QUALITY OF SOFTWARE	N/A. This is a customer-managed control.
P91	MEASURES TO IMPROVE THE QUALITY OF SOFTWARE	N/A. This is a customer-managed control.
P92	MEASURES TO IMPROVE THE QUALITY OF SOFTWARE	N/A. This is a customer-managed control.
P93	MEASURES TO IMPROVE THE QUALITY OF SOFTWARE	N/A. This is a customer-managed control.
P94	MEASURES TO IMPROVE THE QUALITY OF SOFTWARE	N/A. This is a customer-managed control.
P95	MEASURES TO IMPROVE THE QUALITY OF SOFTWARE	N/A. This is a customer-managed control.
P96	MEASURES TO IMPROVE THE QUALITY OF SOFTWARE	N/A. This is a customer-managed control.
P97	BACKUP FOR HARDWARE	▪ Use workspace file ACLs (VIEW/RUN/EDIT/MANAGE), cloud-storage IAM, PrivateLink, and IP access lists to restrict workspace and storage access. Unity Catalog enforces exclusive data access via fine-grained privileges, row/column-level policies, and Delta Lake ACID transaction log with schema enforcement and lineage. ▪ Enable ESM/CSP for hardened, auditable compute on backup, matching, and reconciliation workloads.
P98	BACKUP FOR HARDWARE	N/A. This is a customer-managed control.

01 GUIDELINE	02 CATEGORY	03 DATABRICKS CUSTOMER CAPABILITIES
P99	MEASURES TO IMPROVE OPERATIONAL RELIABILITY	▪ The Databricks control plane spans multiple availability zones with automatic zonal failover. Clusters and SQL warehouses autoscale (including scale-to-zero) and Lakeflow Jobs handles scheduling, retries with exponential backoff, and self-recovery. ▪ System tables (365-day retention) and Lakehouse Monitoring provide data quality, lineage, and SLA tracking. Enable ESM/CSP for regulated workloads.
P100	MEASURES TO IMPROVE OPERATIONAL RELIABILITY	N/A. This is a customer-managed control.
P101	MEASURES TO IMPROVE OPERATIONAL RELIABILITY	N/A. This is a customer-managed control.
P102	FUNCTIONS FOR EARLY FAILURE DETECTION AND RECOVERY	▪ Lakeflow Jobs and Lakeflow Declarative Pipelines (formerly Delta Live Tables) emit structured run status, error codes, and event logs per task to trigger alerts. Lakehouse Monitoring catches freshness, volume, and quality anomalies before bad data propagates downstream. ▪ System tables and audit logs unify job runs, cluster events, SQL activity, and configuration changes for SIEM root-cause isolation. Unity Catalog lineage identifies affected downstream assets. Delta Lake time travel enables rollback to a known-good state.
P103	FUNCTIONS FOR EARLY FAILURE DETECTION AND RECOVERY	▪ Configure job-level alerts, event-log monitoring, and dashboards to detect failures in jobs, clusters, and SQL workloads. Drill into job, cluster, and system table logs to isolate the failing component. ▪ With Unity Catalog enabled, use object-level audit logs, access history, and data lineage to identify which user, service principal, or upstream job caused a pipeline failure. Enable ESM/CSP for additional host-level telemetry.
P104	FUNCTIONS FOR EARLY FAILURE DETECTION AND RECOVERY	▪ Reduce or shut down operations during failure by pausing/disabling job schedules, stopping clusters, and applying workspace-level restrictions via the Jobs and Clusters APIs. Redirect workloads to alternate workspaces or regions as needed. ▪ Unity Catalog enables rearrangement by reconfiguring access policies to restrict write access and switching consumers to read-only or backup data locations. Enable ESM/CSP on shutdown and recovery workloads.
P105	FUNCTIONS FOR EARLY FAILURE DETECTION AND RECOVERY	▪ Implement read-only mode during incidents by pausing job runs and stopping clusters via the Jobs and Clusters APIs. Use Unity Catalog to revoke INSERT/UPDATE/DELETE privileges on critical tables. ▪ Enable ESM/CSP on failure-management workloads for hardened images and security telemetry.

01 GUIDELINE	02 CATEGORY	03 DATABRICKS CUSTOMER CAPABILITIES
P106	FUNCTIONS FOR EARLY FAILURE DETECTION AND RECOVERY	• Use Delta Lake time travel, restore from cross-region backup storage, and rerun ETL/ELT pipelines to restore affected tables and jobs. Unity Catalog centralizes metadata and privileges for reconstructing the logical environment (catalogs, schemas, grants) during recovery. • Enable ESM/CSP on recovery workloads for consistent hardened baselines and forensic telemetry.
P107 – P111	CARD TRANSACTION SERVICE	N/A. Card transaction services fall outside the Databricks platform boundary and are customer-managed.
P112 – P118	INTERNET AND MOBILE SERVICES	N/A. Internet and mobile banking channel controls are customer-managed and outside the Databricks platform boundary.
P119 – P124	CD/ATM AND UNMANNED TERMINALS	N/A. CD/ATM and unmanned-terminal controls are customer-managed physical-channel controls outside the Databricks platform boundary.
P125 – P131	IN-STORE BRANCHES	N/A. In-store branch and convenience-store ATM controls are customer-managed and outside the Databricks platform boundary.
P132 – P137	DEBIT CARD AND PREPAID SERVICES	N/A. Debit-card, prepaid-payment, and electronic-value controls are customer-managed and outside the Databricks platform boundary.
P138 – P139	USE OF E-MAIL AND INTRANET	N/A. E-mail and intranet usage policies are customer-managed; Databricks is not an e-mail or web-browsing service.
P140 – P141	BIOMETRIC AUTHENTICATION	N/A. Biometric authentication is handled at the customer's identity provider; Databricks integrates via SSO but does not provide biometric authentication.
P142 – P144	QR CODE PAYMENT	N/A. QR-code payment services are outside the Databricks platform boundary and are customer-managed.
P145 – P148	REMOTE WORKING	N/A. Remote-working device and channel controls are customer-managed.
P149	MOBILE-BRANCH VEHICLE SERVICES	N/A. This is a customer-managed control.
P150	USE OF AI	• Govern AI as first-class assets in Unity Catalog: models, functions, features, and vector indexes carry the same access controls, ownership, and lineage as data — the technical foundation for AI-use policy and accountability. • Use the MLflow Model Registry for governed, version-controlled model promotion and the Unity AI Gateway (formerly Mosaic AI Gateway) to centrally define and enforce AI usage policies (permitted models, rate limits, logging). Appoint asset owners in Unity Catalog to fulfill accountability; policy formulation itself remains a customer responsibility.

01 GUIDELINE	02 CATEGORY	03 DATABRICKS CUSTOMER CAPABILITIES
P151	USE OF AI	▪ Operate AI transparently: MLflow captures model versions, parameters, and lineage from training data to endpoint; Unity AI Gateway logs inference requests and responses; and inference tables retain payloads for review. ▪ Monitor quality, drift, and bias with Lakehouse Monitoring and evaluate models and agents with MLflow 3 GenAI evaluation (mlflow.genai, formerly Mosaic AI Agent Evaluation), so unfair, incorrect, or biased AI behavior can be detected and remediated.
P152	USE OF AI	▪ Apply Unity AI Gateway service policies (guardrails) — PII detection and masking, safety and topic filters, and prompt-injection mitigations — on model-serving endpoints. ▪ Secure the AI stack with Unity Catalog access control over training data and models, private networking for model serving, and CSP/ESM for regulated AI workloads to prevent unauthorized operation, data leakage, and unintended behavior.
P153	USE OF AI	▪ User education on responsible AI use is a customer responsibility. Databricks supports it with product documentation and responsible-AI guidance, and with Unity AI Gateway service policies (guardrails) that can surface usage constraints and block unsafe prompts.

MAPPING FISC SECURITY GUIDELINES · DATABRICKS' CUSTOMER CAPABILITIES

01 GUIDELINE	02 CATEGORY	03 DATABRICKS CUSTOMER CAPABILITIES
F	**Reference Standards · Facilities**	
F1 – F83	DATA CENTER FACILITIES	N/A. Databricks operates no data centers. Physical facilities are provided by AWS, Azure, and GCP under ISO 27001, SOC 1/2, and PCI-DSS, and are reviewed by Databricks annually. These controls fall to the cloud service provider.
F84 – F138	HEAD & BRANCH OFFICE FACILITIES	N/A. These are customer- and CSP-managed physical facility controls outside the Databricks platform boundary.

01 GUIDELINE	02 CATEGORY	03 DATABRICKS CUSTOMER CAPABILITIES
A	**Auditing Standards**	
A1	SYSTEM AUDITING	▪ Databricks provides a unified audit and observability framework that supports regulated and financial workloads by capturing control plane, data plane, and AI/BI activity across accounts and workspaces in system tables such as system.access.audit, lineage, compute, Lakeflow jobs, billing/usage, Apps, AI/BI Genie, and Vector Search. The system.access.audit table retains up to 365 days of authentication, authorization, configuration, and data-access activity, while customers may extend retention by exporting these logs to encrypted cloud storage and a SIEM with their own multi-year lifecycle, immutability, and integrity controls. ▪ Audit events from Databricks system tables and diagnostic logs can be configured to continuously ingest logs to your centralized SIEM, where correlation rules and alerting are implemented for high-risk actions such as privilege escalation (e.g., changes to high-privilege groups or Unity Catalog grants on sensitive schemas), creation or modification of model serving endpoints that touch regulated data, changes to workspace and account-level security configurations, and anomalous access patterns from unusual geographies or service principals. Operational procedures define a structured review cadence: daily triage of critical alerts; weekly review of anomalous activities; monthly configuration and API usage review; quarterly access recertification for privileged roles and service principals; and an annual control-effectiveness review with documented outcomes and remediation tracking. ▪ For regulated and financial workloads, the Compliance Security Profile (CSP) is required, and Enhanced Security Monitoring (ESM) is enabled on all eligible (classic) compute so that all actions occur on hardened, monitored infrastructure with FIPS-validated cryptography, host-level telemetry, and advanced threat detection. Serverless and any other planes not yet covered by ESM are still in scope for auditing via system tables and log export, with documented compensating controls and monitoring in the SIEM to ensure consistent visibility across all Databricks services.
A1-1	CYBERSECURITY AUDITING	▪ Databricks provides the evidence base for internal cybersecurity audits: system.access.audit (retained up to 365 days) plus lineage, compute, and Lakeflow jobs system tables, exportable to immutable cloud storage and SIEM for multi-year retention. ▪ Support a structured audit cadence — daily alert triage, weekly anomaly review, monthly configuration/API review, quarterly privileged-access recertification, and annual control-effectiveness review — and evidence platform controls through independent SOC/ISO/PCI audits and the Compliance Security Profile.

databricks

END OF MAPPING

Mapping FISC Security Guidelines to Databricks' Customer Capabilities

REFERENCE EDITION

FISC Security Guidelines on Computer Systems for Financial Institutions, Thirteenth Edition (March 2025)

DOCUMENT VERSION

Version 1.0

SECURITY & COMPLIANCE

Databricks Security & Trust Center

PLATFORM DOCUMENTATION

docs.databricks.com