INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-14 13:37 UTC

China Releases Data Classification Guidelines for Financial Information Services Sector

GOVERNANCE | MEDIUM

SCC Item ID	SCC-GOV-2026-0056
Type	Governance
Severity	MEDIUM
Affected Products	Financial information services sector, China-domiciled entities and operators
Published	2026-06-14
Discovery Source	Gemini

Executive Summary

China's cybersecurity regulators have issued a four-tier data classification and grading framework for the financial information services sector, aligning with China's Data Security Law. Organizations domiciled in China, or operating financial data services that touch Chinese markets, must now classify and govern data according to sensitivity and potential harm from unauthorized disclosure. Non-compliance carries regulatory risk in China; multinational firms should assess whether their China-side operations or data-sharing arrangements fall under this framework.

Technical Analysis

This is a regulatory governance development, not a technical vulnerability. No CVE, CWE, CVSS score, or exploit vector is associated with this item. China's financial sector regulators have issued guidelines establishing a four-tier data classification and grading scheme for financial information services providers. The framework maps data assets to tiers based on importance, sensitivity, and impact of unauthorized disclosure or leakage. The initiative operates under China's Data Security Law (DSL) and national cybersecurity policy. Affected entities must inventory, classify, and apply appropriate protective controls to financial data according to the tier assigned. No patch, signature update, or vendor advisory applies.

Action Checklist

1. Step 1: Scoping, Identify all China-domiciled legal entities, subsidiaries, joint ventures, or third-party service providers handling financial information data subject to Chinese regulatory jurisdiction. Document which data assets are in scope.

2. Step 2: Data Inventory, Per CIS 3.2 (Establish and Maintain a Data Inventory), conduct or update a sensitive data inventory for in-scope operations. Map existing data assets to the four-tier classification framework based on importance, sensitivity, and disclosure impact.
3. Step 3: Access Control Alignment, Per CIS 3.3 (Configure Data Access Control Lists) and NIST SI-7 (Software, Firmware, and Information Integrity), review and tighten access controls for data classified at higher tiers. Apply least-privilege principles and integrity verification where applicable.
4. Step 4: Retention and Disposal Review, Per CIS 3.4 (Enforce Data Retention) and CIS 3.5 (Securely Dispose of Data), validate that data retention schedules and disposal procedures align with the classification tier requirements mandated under the framework.
5. Step 5: Post-Assessment, Engage qualified legal counsel with China regulatory expertise to interpret specific compliance obligations. Document classification decisions, control mappings, and any gaps identified. Establish a review cadence as implementing rules are issued.

IR / Forensic Enrichment

Triage Priority	STANDARD
Escalation Criteria	Escalate to legal counsel and senior leadership immediately if any in-scope China-domiciled entity is identified as handling data that may qualify as 'Important Data' or 'Core National Data' under the DSL four-tier framework, or if a regulatory inquiry, audit notice, or data incident affecting classified financial information is received from PBOC, CSRC, or CAC before the classification and control alignment work is complete.
Recovery Notes	Post-assessment, verify that all higher-tier data assets have documented classification decisions, mapped controls, and closed or formally risk-accepted gaps before any regulatory submission or audit response. Monitor PBOC, CSRC, and CAC official channels on a monthly cadence for sector-specific implementing rules that may refine tier definitions or introduce new technical control obligations, and trigger a delta-review of the classification register each time new guidance is published. Retain all assessment artifacts — classification records, ACL snapshots, disposal certificates, legal counsel memos — for a minimum retention period consistent with DSL requirements and the organization's documented data management process.
Forensic Artifacts	China regulatory correspondence records: any notices, inquiries, or audit requests received from PBOC, CSRC, or CAC referencing the financial information services data classification framework — these establish the regulatory trigger timeline. | Data inventory snapshots: point-in-time exports of database schemas, file system directory listings, and cloud storage bucket inventories capturing the pre-assessment state of financial data assets subject to DSL tier classification. | ACL and permission exports: before-state permission reports from all data stores holding in-scope financial data (SQL `SHOW GRANTS` outputs, Linux `getfacl` exports, Alibaba Cloud RAM policy exports) documenting access posture prior to any remediation under Step 3. | Data disposal certificates: timestamped destruction records for any out-of-retention data disposed under Step 4, including file identifiers, checksums, disposal method, classification tier, and the regulatory basis for disposal. | Classification decision register: the version-controlled document produced in Step 5 mapping each data asset to its assigned DSL tier, with rationale, control mappings, identified gaps, and legal counsel review dates — the primary audit artifact for demonstrating DSL Article 21 and Article 27 compliance.

Per-Action IR Details

Step 1: Scoping — Identify all China-domiciled legal entities, subsidiaries, joint ventures, or data-processing operations that handle financial information services data subject to Chinese regulatory jurisdiction. Document which data assets are in scope.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Establishing the organizational inventory and scoping boundaries necessary to respond to a regulatory compliance event before obligations become enforceable.

Controls: CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 3.2 (Establish and Maintain a Data Inventory)

Compensating: For a 2-person team without enterprise asset management tooling: export entity and subsidiary lists from corporate registries or HR systems into a spreadsheet; cross-reference with network topology diagrams to identify data-processing nodes with Chinese IP ranges or regulatory nexus. Use a shared document (e.g., Git-tracked markdown) to record each entity, its data categories, and jurisdictional basis. Free tool: OpenRefine for deduplicating and normalizing asset/entity lists from multiple exports.

Evidence: This is a preparation step that does not alter live system state, so no volatile capture is required before execution. However, document the current state of entity registrations, data-processing agreements, and network architecture diagrams as baseline records — these will serve as audit evidence if regulators request proof of scoping diligence under China's Data Security Law (DSL) Article 21 tiered classification requirements.

Step 2: Data Inventory — Per CIS 3.2 (Establish and Maintain a Data Inventory), conduct or update a sensitive data inventory for in-scope operations. Map existing data assets to the four-tier classification framework based on importance, sensitivity, and disclosure impact.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Building the data classification baseline that enables accurate detection and scoping of future regulatory non-compliance events or data incidents involving classified financial information.

Controls: CIS 3.2 (Establish and Maintain a Data Inventory), CIS 3.3 (Configure Data Access Control Lists), NIST SI-12 (Information Management And Retention)

Compensating: For teams without a commercial DLP or data catalog: run targeted filesystem and database scans using open-source tools — use `grep -rE` or PowerShell `Get-ChildItem` with regex patterns matching Chinese financial data identifiers (bank account numbers, securities codes, RMB transaction fields) against known data-store paths. For structured databases, execute schema-level queries (`INFORMATION_SCHEMA.COLUMNS`) to surface columns likely holding regulated financial data. Document outputs in a version-controlled spreadsheet mapping each dataset to the four-tier classification (Core National Data, Important Data, Sensitive Personal Information, General Data) with the DSL harm-impact rationale for each tier assignment.

Evidence: No live system state is altered by this step, so no volatile capture prerequisite applies. Preserve point-in-time snapshots of database schema exports and directory listings at the time of classification — these create an audit trail demonstrating the classification baseline existed prior to any regulatory inquiry. If data stores are cloud-hosted in China (e.g., Alibaba Cloud OSS, Tencent COS), capture current bucket/container ACL exports as evidence of pre-assessment access posture.

Step 3: Access Control Alignment — Per CIS 3.3 (Configure Data Access Control Lists) and NIST SI-7 (Software, Firmware, and Information Integrity), review and tighten access controls for data classified at higher tiers. Apply least-privilege principles and integrity verification where applicable.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Hardening access controls for higher-tier classified financial data before a compliance audit or data incident occurs, reducing blast radius if unauthorized access is discovered.

Controls: CIS 3.3 (Configure Data Access Control Lists), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 6.1 (Establish an Access Granting Process), CIS 6.2 (Establish an Access Revoking Process), NIST SI-7 (Software, Firmware, And Information Integrity)

Compensating: For teams without PAM or enterprise IAM tooling: generate ACL and permission reports from data stores directly — for Linux file systems use `getfacl -R /path/to/data > acl_baseline.txt`; for SQL Server/MySQL run

`SHOW GRANTS` or `sys.database_permissions` queries; for Alibaba Cloud OSS use the RAM (Resource Access Management) console export. Compare outputs against the classification tier assignments from Step 2 and revoke permissions exceeding least-privilege using native CLI (`setfacl`, `REVOKE` statements, RAM policy edits). For integrity verification without enterprise tooling, use `sha256sum` or PowerShell `Get-FileHash` to baseline critical financial data files and store hashes in a write-protected log.

Evidence: Before modifying any ACLs or revoking access accounts, capture a complete export of current permission states as a before/after audit record — this is required evidence for DSL compliance demonstration. If any accounts being revoked are currently authenticated to systems holding Tier 3 or Tier 4 classified data, capture active session listings first (`who`, `w`, `netstat -an`, or cloud console active session exports) to document what access was live at the time of remediation. These session records establish that no unauthorized data exfiltration occurred concurrently with the access change.

Step 4: Retention and Disposal Review — Per CIS 3.4 (Enforce Data Retention) and CIS 3.5 (Securely Dispose of Data), validate that data retention schedules and disposal procedures align with the classification tier requirements mandated under the framework.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Establishing compliant data lifecycle controls for classified financial information before regulatory enforcement actions or audit inquiries target retention and disposal practices.

Controls: CIS 3.4 (Enforce Data Retention), CIS 3.5 (Securely Dispose of Data), NIST SI-12 (Information Management And Retention), NIST AU-11 (Audit Record Retention)

Compensating: For teams without enterprise DLP or automated retention enforcement: create a retention register mapping each data asset (identified in Step 2) to its classification tier and the corresponding minimum/maximum retention period required under the DSL framework and any sector-specific implementing rules. Enforce deletion schedules via cron jobs or scheduled tasks running `shred -u` (Linux) or `cipher /w` (Windows) against identified out-of-retention data paths. For cloud storage (Alibaba Cloud OSS, Tencent COS), configure native object lifecycle policies to enforce tier-appropriate expiration. Document each disposal event with timestamp, method, and data description for audit evidence.

Evidence: This step involves modifying data (deletion/disposal), which is an irreversible action. Before executing any disposal, capture an inventory snapshot of the data to be disposed — file names, sizes, checksums, classification tier, and the regulatory basis for disposal — as an auditable destruction certificate. This is not a volatile-evidence concern in the traditional forensic sense, but it is a compliance-evidence obligation: regulators under China's DSL may require proof that disposal was performed on the correct data, using a method appropriate to its classification tier, and not prematurely.

Step 5: Post-Assessment — Engage qualified legal counsel with China regulatory expertise to interpret specific compliance obligations. Document classification decisions, control mappings, and any gaps identified. Establish a review cadence as implementing rules are issued.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Conducting a structured lessons-learned and gap-documentation process following the initial compliance assessment, and establishing ongoing improvement cycles as the regulatory framework matures.

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST AU-6 (Audit Record Review, Analysis, And Reporting), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For a 2-person team without a GRC platform: maintain the compliance record in a version-controlled document repository (Git or SharePoint with change history enabled) capturing: each data asset, its assigned tier, the control mapped to it, any identified gap, the gap owner, and the target remediation date. Set calendar-based review triggers aligned to PBOC/CSRC implementing rule publication cycles — subscribe to official regulatory RSS feeds or mailing lists (e.g., CSRC, PBOC, CAC official sites) to detect new implementing guidance. Flag each open gap with a risk-acceptance sign-off from the appropriate data owner.

Evidence: No volatile system state is altered by this step. The primary evidence obligation is documentation integrity: all classification decisions, gap findings, legal counsel interpretations, and control mapping outputs produced during this assessment must be preserved in a tamper-evident, version-controlled format. These records constitute the organization's demonstrable compliance posture under DSL Article 27 (organizational accountability) and will be the first items requested in any PBOC, CSRC, or CAC regulatory examination or data incident investigation.

Detection Guidance

This item has no technical exploitation vector; standard IOC-based detection does not apply. For compliance monitoring purposes: audit data access logs (NIST AU-2, AU-6) for in-scope China-side systems to establish a baseline before classification controls are applied. Review NIST AU-3 audit record content to ensure logs capture sufficient detail to demonstrate data handling compliance under the framework. Monitor regulatory publications from China's National Financial Regulatory Administration and the Cyberspace Administration of China for implementing rules and enforcement guidance. No specific log queries, event IDs, or behavioral indicators are relevant to this governance item.

Framework Mappings

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities

Sources

Source	URL	Tier
China issues guidelines on financial services data amid ...	https://www.facebook.com/Reuters/posts/china-issues-guidelines-on-f...	T3
Vulnerabilities in China's Financial System and Risks for ...	https://www.uscc.gov/sites/default/files/2020-12/Chapter_2_Section_...	T1
China Cybersecurity Law: Key Takeaways for Financial...	https://www.dechert.com/knowledge/onpoint/2017/6/china-cybersecurit...	T3
How Do Financial Risks Threaten China's Economic Security?	https://chinapower.csis.org/china-financial-security/	T3
China issues guidelines on financial services data amid ...	https://wtvbam.com/2026/06/13/china-issues-guidelines-on-financial-...	T3

Generated 2026-06-14 13:37 UTC by TJS Security Command Center