China's New Data Security Measures Mandate Annual Risk Assessments for Certain Enterprises

By Liza L.S. Mark, Maisy Chang | September 25, 2026

RELATED PRACTICES International

What is happening?

The Cyberspace Administration of China ("***CAC***"), the Ministry of Industry and Information Technology ("***MIIT***") and the Ministry of Public Security jointly promulgated the *Measures for Cybersecurity Data Security Risk Assessment* (the "***Measures***") on June 18, 2026, which took effect on Aug. 20, 2026.

The Measures do not create entirely new obligations. Rather, they translate the principle-based risk assessment requirements of the Data Security Law (the "***DSL***"), which went into effect on Sept. 1, 2021, and the Regulations on Network Data Security Management (the "***Regulations***"), which went into effect on Jan. 1, 2025, into concrete, actionable compliance regulations. Companies with operations or business in China should evaluate whether the Measures apply to them and, if so, understand what the new compliance requirements entail and what steps they should take now.

Key Takeaways

- *Mandatory obligation for important data processors*: Enterprises processing "important data" must conduct risk assessments annually and submit assessment reports to the competent authorities within 20 working days upon completion. As defined in the Regulations, important data refers to data that pertains to specific sectors, groups or regions, or that reaches a certain level of precision and scale, and that, if subjected to destruction, leakage or unlawful acquisition or use, may directly endanger national security, economic operation, social stability or public health and safety (e.g., human genetic resource data and large-scale health records collected through clinical trials or joint ventures by foreign-invested pharmaceutical companies). Specific assessments must also be conducted promptly when the security status of "important data" undergoes material changes (e.g., business model adjustments, significant growth in data volume, changes to system architecture or security incidents).
- *Encouraged (not mandatory) requirements for general data processors*: Enterprises that only process general data and do not process "important data" are encouraged to conduct risk assessments at least once every three years. This frequency of conducting risk assessments is not currently legally required.
- *Significantly strengthened regulatory oversight power*: Authorities at or above the provincial level may verify and inspect risk assessment reports. Where significant security risks or data breaches are identified, they may require enterprises to engage certified institutions to conduct reassessments. Those refusing to rectify noncompliance may be ordered to suspend "important data" processing activities.
- *Particular attention for foreign-invested enterprises in China*: Enterprises operating in sectors such as energy, transportation, finance, healthcare and industrial manufacturing, or those processing large volumes of personal information or data pertaining to specific regions or groups, are likely to be designated as "important data processors" and should initiate compliance preparations immediately.

What is changing?

Compared with the principle-based provisions previously scattered across the DSL and the Regulations, the Measures introduce substantive changes in the following respects:

1. Clarification of Assessment Frequency and Trigger Mechanisms

For the first time, the Measures translate the requirement for "regular risk assessments" into specific time frames and introduce a "material-change trigger" mechanism:

- Important data processors shall conduct risk assessments at least once annually (mandatory).
- Where the security status of important data undergoes material changes that may adversely affect data security (such as business model adjustments, rapid expansion of data volume, changes to system architecture or the occurrence of security incidents), ad hoc risk assessments shall be conducted promptly to assess both the changed portions of the data processing activities and how those changes affect the enterprise's overall data security posture (mandatory).
- General data processors are encouraged to conduct risk assessments at least once every three years (nonmandatory).

2. Specification of Rules for Submission and Retention of Assessment Reports

Articles 15 and 16 of the Measures set forth the requirements for the preparation, submission and retention of risk assessment reports:

- *Submission deadline*: Important data processors shall submit their reports to the competent authorities within 20 working days upon completion of the annual risk assessment.
- *Submission channels*: Where the competent authority is clearly identified, reports shall be submitted to that authority. Where no competent authority is clearly identified, reports shall be submitted to the provincial-level cyberspace administration or the CAC.
- *Preparation requirements*: Important data processors shall prepare annual risk assessment reports in accordance with the requirements of the competent industry authorities. Where no special requirements are prescribed by the competent authorities, reports may be prepared by reference to national standards such as *GB/T 45577-2025, Data Security Technology — Data Security Risk Assessment Methodology*.
- *Retention period*: Risk assessment reports shall be retained for at least three years.
- *Inter-regulatory departments sharing*: Competent authorities shall, within 10 working days after receiving a report, circulate it to the local cyberspace administration (i.e., provincial-level branches of the CAC) at the same administrative level as the competent authority that received the report. The CAC shall aggregate relevant reports and share them with authorities, including MIIT, the Ministry of Public Security and national security authorities (sharing is mandatory and automatic). Enterprise reports therefore fall within the regulatory purview of multiple agencies.

3. Establishment of a Regulatory Framework for Third-Party Assessment Institutions

The Measures systematically regulate third-party assessment institutions, an area that prior legislation had not expressly addressed:

- *Certification encouraged*: Assessment institutions are encouraged to obtain certification under the Regulations of the People's Republic of China on Certification and Accreditation, effective Nov. 1, 2003, to demonstrate their service capabilities.
- *Prohibition on subcontracting*: Assessment institutions shall not subcontract assessment engagements to other institutions.
- *Confidentiality obligations*: Data, trade secrets and confidential business information obtained during the assessment process shall be kept confidential in accordance with law. Upon conclusion of the assessment, such information shall be promptly deleted or duly disposed of in accordance with contractual arrangements.
- *Risk notification obligation*: Where material data security risks are identified during the assessment, the institution's primary obligation under the Measures is to notify the enterprise promptly. The enterprise must then address the risk and may have separate reporting obligations to authorities under applicable data security incident reporting requirements.

4. The "Mandatory Assessment" Mechanism — A Key Regulatory Instrument

Article 17 of the Measures introduces an important regulatory instrument: Where authorities at or above the provincial level, including cyberspace administrations, telecommunications authorities and public security organs, identify any of the following circumstances during report verification or supervisory inspections, they may require an enterprise to engage a certified assessment institution to conduct a risk assessment (a "***Mandatory Assessment***"):

- The network data processing activities present significant security risks that may endanger national security or public interests.
- A network data security incident has occurred, resulting in the leakage or theft of important data or large-scale personal information.
- Other circumstances prescribed by the relevant authorities.

Enterprises subject to a Mandatory Assessment shall fulfill stringent obligations: Providing the assessment institution with necessary system access and data permissions; completing the assessment within the prescribed time limit; submitting the assessment report, signed and sealed by the institution, to the relevant authorities; and rectifying identified issues and submitting a rectification report within 15 working days of completing rectification.

The Measures also include safeguards against regulatory abuse: An enterprise shall not be required repeatedly to engage an assessment institution with respect to the same network data security incident or risk.

5. Legal Consequences

Failure to conduct risk assessments in accordance with applicable provisions will be addressed under laws and regulations, including the DSL and the Regulations. Where authorities find that important data processing activities may endanger national security or public interests, they shall order rectification. If an enterprise refuses to rectify or fails to meet rectification requirements, authorities may order suspension of important data processing activities. This is an exceptionally severe consequence because suspension could effectively halt core business operations. A manufacturing enterprise dependent on processing production, supply chain or quality control data classified as important data could be forced to cease production entirely. A suspension order may therefore amount to a forced cessation of business operations in China.

Who should be prepared?

Important Data Processors — Subjects of Mandatory Obligations

This is the core category of entities to which the Measures apply. Determining whether an enterprise qualifies as an "important data processor" hinges on whether the data it processes constitutes "important data."

For foreign enterprises operating in China, the following circumstances warrant particular vigilance regarding potential designation as important data processors:

- *Sectoral dimension*: Enterprises operating in critical sectors such as energy, transportation, water conservancy, finance, defense science, technology and industry, telecommunications, public services and healthcare.
- *Data dimension*: Enterprises processing large-scale personal information (e.g., where the user base reaches a certain volume), geospatial data for specific regions, health or biometric data of specific groups, industrial production and operation data or critical supply chain data.
- *Scale dimension*: Data that reaches a certain level of precision and scale (e.g., high-resolution map data covering specific regions, or industry-wide statistical data).

It should be particularly noted that various regions and departments are in the process of formulating specific catalogs of important data for their respective regions and industries in accordance with the data classification and grading protection system. Enterprises should closely monitor the publication of such catalogs in their respective industries and regions.

General Data Processors — Not Mandatory but Proactive Preparation Advised

For enterprises operating in China that do not process "important data" but do process general network data (including personal information), the Measures encourage (but do not require) risk assessments at least once every three years. A Mandatory Assessment may nevertheless be triggered if authorities identify risks during inspections. A risk assessment under the Measures generally entails evaluating the legality, legitimacy and necessity of data processing; the security of processing systems and technical safeguards; data-access controls and management measures; risks of leakage, tampering, loss or misuse; and the effectiveness of incident-response capabilities. It can also support compliance with other requirements, including *Personal Information Protection Impact Assessments* ("***PIAs***") and security assessments for cross-border data transfers. Accordingly, foreign enterprises processing a significant volume of data should consider incorporating regular data security ***risk*** assessments into their compliance programs.

What steps should be taken now?

For business operators, management and legal counsel of U.S. enterprises operating in China, the following steps are recommended:

Step 1: Data Asset Inventory and Important Data Identification

Enterprises should inventory data collected, stored, processed or transmitted in China and assess whether it may be "important data" based on sector, type, volume, precision and geographic coverage. Certain sectors have begun formulating or publishing catalogs — for example, *Guidelines for Identification of Key Data in Telecommunication Field (YD/T 3867-2024)* (effective on Oct. 1, 2024) and *Guideline for Identification of Key Data in Industrial Field (YD/T 4981-2024)* (effective on April 1, 2025). Because many sectors have not finalized their catalogs,

enterprises should monitor developments in their industries and update their analyses. Where uncertainty exists, enterprises should consult competent authorities or qualified professionals.

Step 2: Establishing Risk Assessment Policies and Procedures

Enterprises should formulate internal risk assessment management policies, clarifying the division of responsibilities, assessment frequency, procedures and mechanisms for report preparation and submission. Dedicated personnel should be designated to oversee risk assessment work — a statutory requirement for self-assessments. Enterprises should select between self-assessment and engagement of third-party institutions based on their own capabilities. Where third-party engagement is chosen, selection criteria and contract templates should be established, with clear provisions on confidentiality obligations, report accountability and data disposal. Assessment work should be conducted by reference to national standards, principally *GB/T 45577-2025, Data Security Technology — Data Security Risk Assessment Methodology*, and *GB/T 45389-2025, Information Security Technology — Capability Requirements for Data Security Assessment Institutions*.

Step 3: Cross-Departmental Coordination and Communication with the Parent Company

Within the entity's China operations, departments including legal, IT security, business and human resources should establish coordination mechanisms. At the same time, the foreign parent company or headquarters should be promptly informed of China's data security compliance requirements. Risk assessment reports may need to be submitted to Chinese regulatory authorities, raising sensitivities concerning data sovereignty and cross-border information sharing. The assessment process may require granting system access and data permissions to third-party institutions, necessitating an evaluation of the impact on the parent company's global data governance framework. If ordered to suspend important data processing activities, the operational impact on the China business will be enormous, requiring a pre-established business continuity plan.

Conclusion

Effective on Aug. 20, 2026, the Measures move China's data security framework from principle-based legislation toward concrete compliance rules and operational requirements. For foreign enterprises operating in China, annual risk assessments are mandatory for important data processors and noncompliance may lead to administrative penalties or orders to suspend important data processing activities.

Multinational enterprises should therefore establish and maintain their China data security management frameworks in accordance with the Measures and integrate those frameworks into their global compliance and business continuity systems.

For more information, please contact Liza L.S. Mark and Maisy Chang.