Time will tell:
Perspectives of Network Data Security Risk Assessment

By Xun Yang | Echo Li

Whilst compliance audits for personal information protection are taking into shape, network data security risk assessment is now on the horizon. Is this an unbearable burden for enterprises, or can it be a convenient way to meet compliance requirements?

On the night before the Dragon Boat Festival, June 18, 2026, the Cyberspace Administration of China, the Ministry of Industry and Information Technology, and the Ministry of Public Security jointly issued the Measures for *Network Data Security Risk Assessment* (hereinafter referred to as the "**Measures**"), which will take effect on August 20, 2026. The promulgation of these Measures marks the imminent implementation of China's data security risk assessment system. But what do the Measures actually mean for enterprises?

I. The Nature of the Measures for Network Data Security Risk Assessment

From the perspective of legislative hierarchy, the Measures constitute a managerial rule, with superior legal bases including the Data Security Law of the People's Republic of China, the Cybersecurity Law of the People's Republic of China, and the Regulations on Network Data Security Administration (State Council Order No. 790, hereinafter referred to as the "**Regulations**"). Specifically, the Data Security Law, as a congress-made law, establishes in Article 30 the fundamental system that "processors of important data shall conduct risk assessments of their data processing activities on a regular basis in accordance with regulations"; the Regulations, as an administrative regulation, further refine in Articles 31 and 33 the specific requirements for special assessments and annual assessments; while the Measures, building upon the former two, provide systematic provisions on operational matters such

For more Llinks publications, please contact:

Publication@llinkslaw.com

as the organization and implementation of risk assessments, procedural workflows, report preparation, and institutional management, constituting the most practically enforceable subordinate legal norm within the three-tier normative system of "statute—administrative regulation—departmental regulation."

From the perspective of regulatory content, the Measures do not create new substantive obligations but rather provide procedural implementation of existing statutory obligations. They clarify the definition of risk assessment (Article 2), the subjects of assessment (Article 5), the methods of assessment (Article 7), reporting requirements (Articles 15 and 16), management of third-party institutions (Articles 8 through 14), and supervision and inspection mechanisms (Articles 19 through 22). Notably, Article 6 of the Measures explicitly provides that risk assessment work shall "be conducted with reference to relevant national standards on data security risk assessment," and where relevant competent authorities have separate provisions, such provisions shall prevail. This means that national standards such as GB/T 45577-2025 Data Security Technology — Methods for Data Security Risk Assessment (the "Assessment Methods National Standard") have de facto normative effect at the assessment methodology level, and data processors should follow them when performing assessments.

From the perspective of relationship with other compliance requirements, the Measures constitute an important component of China's data security governance system, interconnecting with systems such as cybersecurity classified protection assessment, personal information protection compliance audits, and personal information protection impact assessments, jointly regulating enterprises' data processing activities from different angles.

II. Who Must Conduct Network Data Security Risk Assessments?

Article 5 of the Measures clarifies the scope of obligated subjects for risk assessment, including mandatory assessment and encouraged assessment.

"Important data processors" are the subjects of mandatory assessment. According to Article 62 of the Regulations, important data refers to "data in specific fields, relating to specific groups, in specific regions, or reaching a certain level of precision and scale, which, once tampered with, destroyed, leaked, or illegally obtained or utilized, may directly endanger national security, economic operation, social stability, public health, and safety." Because the data they process involves public interests or national interests, important data processors are legally required to conduct risk assessments on an annual basis. Furthermore, Article 28 of the Regulations provides that data processors processing personal information of more than 10 million individuals shall also comply with the provisions of Articles 30 and 32 of the Regulations applicable to important data processors, meaning that ultra-large personal information processors are likewise subject to annual risk assessment obligations.

Other ordinary " data processors" are the subjects of encouraged assessment. Paragraph 3 of Article 5 of the Measures explicitly "encourages network data processors processing ordinary data to conduct risk assessments at least once every three years." General data processors typically involve only private interests;

the law does not mandate them to conduct assessments but encourages them to enhance their data security safeguards through periodic assessments. This institutional design reflects the principle of proportionality—imposing strict obligations on important data processors involving public interests while granting more autonomy to ordinary data processors.

The identification of important data imposes a major practical challenge. Currently, there are three identification pathways: first, direct regulatory stipulation, such as the *Provisions on Management of Automotive Data Security (Trial)* defining data related to autonomous driving vehicles; second, designation by competent authorities, such as the National Financial Regulatory Administration's identification and designation of important data for banks and insurance institutions; and third, enterprise self-assessment, whereby network data processors identify and declare important data in accordance with relevant state regulations, which is then confirmed by relevant regions or departments and communicated or publicly announced (Article 29 of the Regulations). For data not yet explicitly included in industry catalogues of important data, enterprises should establish internal data classification and grading systems, proactively carry out important data identification work, and avoid missing assessment obligations due to identification oversights.

III. When Should Network Data Security Risk Assessments Be Conducted?

The Measures and the Regulations establish a trigger mechanism of "special assessment" and "routine assessment," corresponding to two types of timing requirements: "ex-ante milestones" and "annual routines."

Special assessments apply before specific data processing activities occur. Article 31 of the Regulations provides that important data processors shall conduct risk assessments before providing, entrusting the processing of, or jointly processing important data, except where this is necessary for performing statutory duties or obligations. This article also enumerates six key assessment contents, including the legality, legitimacy, and necessity of the purposes, methods, and scope of data processing; risks of data leakage; the integrity and law-abiding record of the recipient; the binding effect of contractual constraints; and the effectiveness of technical and managerial measures. Additionally, according to Article 37 of the Regulations, where important data collected and generated during domestic operations must be provided overseas, network data processors shall undergo data export security assessment organized by the national cyberspace administration—this constitutes a more stringent national security review procedure, distinct in nature and procedure from the general risk assessments provided for in the Measures. Article 5 of the Measures further supplements that "where significant changes in the security status of important data may adversely affect data security, risk assessments shall be promptly conducted on the changed parts and their impacts," providing a basis for dynamic assessment.

Routine assessments apply to periodic review of data processing activities. Article 33 of the Regulations and Articles 5 and 16 of the Measures all require that important data processors conduct risk assessments of their network data processing activities on an annual basis, and submit risk assessment reports to relevant competent authorities at or above the provincial level upon completion of the assessment. The reports

should include basic information about the data processor, the purposes and methods of data processing, security management systems and technical measures, identified risks and incidents, and data export situations (Article 33 of the Regulations). The annual assessment has a fixed cycle and comprehensive content, aiming to form a normalized risk monitoring mechanism.

A question worth pondering is how to coordinate between special assessments and routine assessments. If an important data processor shortly after its annual assessment engages in important data transfer activities such as provision or entrusted processing, is a separate special assessment still required? From the literal meaning of the legislation, special assessments emphasize the "ex-ante" timing, while annual assessments emphasize the "routine" timing; each has independent trigger conditions, and in principle they should be conducted separately. However, Article 52 of the Regulations requires "avoiding repetitive assessments." In practice, for assessments conducted in close succession, supplementary assessments for newly added transfer matters may be conducted within the framework of the annual assessment to improve efficiency and reduce costs.

IV. What Is the Objective of Network Data Security Risk Assessment?

To understand the objective of data security assessment, it is necessary to place it within the overall framework of China's data protection legal system for comparative analysis. The Personal Information Protection Law establishes two systems: "personal information protection impact assessment" (PIA) and "personal information protection compliance audit." The former focuses on assessing the legality, legitimacy, and necessity of specific personal information processing activities, identifying risks, and proposing mitigation measures; the latter focuses on systematically reviewing the compliance and risk vulnerabilities of the entire process of personal information processing activities. By comparison, network data security assessment (targeting important data and other non-personal data) appears to combine the objectives of the above two systems, yet possesses its own unique institutional connotations.

According to Article 2 of the Measures, risk assessment refers to "activities of risk identification, risk analysis, and risk evaluation of the security of network data and network data processing activities." This definition is highly consistent with the core logic of the Assessment Methods National Standard, namely, taking data processing activities as the core, identifying risk sources, analyzing the degree of harm and likelihood of occurrence, evaluating risk levels, and ultimately answering fundamental questions such as "are there risks, what are the risks, where are the risks, and how significant are the risks."

From the perspective of objective levels, data security risk assessment encompasses at least three dimensions: the compliance dimension, namely reviewing whether data processing activities comply with mandatory requirements of laws, administrative regulations, and national standards; the risk dimension, namely identifying and evaluating the likelihood of data security incidents and their harmful consequences; and the governance dimension, namely discovering management loopholes, optimizing security strategies, and enhancing overall data security governance capabilities through assessment. Its ultimate objective is to provide a reference basis for risk management by the decision-making level of the entity and by industry regulatory authorities.

V. Who Should Conduct Network Data Security Risk Assessments?

Article 7 of the Measures grants data processors the option to conduct risk assessments on their own or to entrust third-party assessment institutions to conduct them. Each model has its advantages and disadvantages; in practice, a comprehensive judgment should be made based on the data processor's capabilities, the sensitivity of the data, and the complexity of the assessment.

Enterprise self-assessment has significant advantages. Data processors are most familiar with their own business scenarios, data flow paths, and system architectures, and can accurately identify internal risk points; at the same time, self-assessment avoids exposing sensitive data to external institutions, providing the greatest guarantee of information confidentiality. Article 7 of the Measures requires that entities conducting self-assessments "shall designate a specific person to be responsible," meaning that enterprises need to establish an internal assessment responsibility system to ensure that assessment work has a clear responsible party. However, self-assessment also has limitations: internal personnel may lack independence and thus find it difficult to objectively identify deep-seated problems; technical teams may lack a legal compliance perspective, while legal teams may lack technical detection capabilities.

Entrusting third-party assessments can compensate for the above disadvantages, but it remains unclear who is qualified to serve as a competent third party. Although GB/T 45389-2025 Data Security Technology — Requirements for Data Security Assessment Institutions has been implemented since October 1, 2025, setting capability benchmarks for assessment institutions from dimensions including basic conditions, management capabilities, technical capabilities, human resource capabilities, and site and equipment resource capabilities, the Measures do not explicitly limit which types of institutions possess assessment qualifications, merely "encouraging relevant assessment institutions to obtain certification" (Article 8 of the Measures). In reality, data security risk assessment is a comprehensive issue spanning technology, management, and law—assessments must review not only technical measures such as encryption, access control, and data masking, but also determine the "legality, legitimacy, and necessity" of data processing, and evaluate harm risks and the legal environment. Teams with a single background often struggle to provide comprehensive coverage.

Therefore, a more realistic path may be: taking the enterprise itself as the leading entity, assembling a cross-departmental assessment team (covering business, security, legal, and compliance functions), and bringing in external experts for supplementation when technical testing or legal argumentation is needed. For important data processors, especially when data security incidents occur or significant security risks exist, competent authorities may require them to entrust certified assessment institutions to conduct assessments (Article 17 of the Measures).

VI. How Should Data Security Assessments Be Conducted?

The Assessment Methods National Standard provides a standardized methodological framework for data security risk assessment, which can be summarized as five stages: assessment preparation, information

investigation, risk identification, risk analysis and evaluation, and assessment summary.

In the assessment preparation stage, it is necessary to determine the assessment objectives (such as comprehensively mapping data assets, identifying compliance risks, or reviewing specific data processing activities), define the assessment scope, assemble a cross-departmental team, and formulate an assessment plan. In the information investigation stage, it is necessary to verify the basic circumstances of the data processor, business and information systems, data assets (including classification and grading status), the full process of data processing activities, and existing security protection measures, forming a data asset inventory and data flow diagrams. In the risk identification stage, risk sources are investigated from four dimensions: data security management, data processing activity security, data security technology, and personal information protection, covering the full lifecycle of systems and processes, organizational structures, personnel management, data collection, storage, transmission, use, provision, public disclosure, and deletion. In the risk analysis and evaluation stage, identified risk sources are categorized, the degree of harm is analyzed (classified into five levels: low, medium, relatively high, high, and very high) and the likelihood of occurrence is analyzed (classified into three levels: low, medium, and high), and ultimately risk levels are determined and a risk inventory is formed. In the assessment summary stage, a risk assessment report is prepared, rectification recommendations are proposed, and residual risks are analyzed.

In practice, the author is often asked: does data security risk assessment overlap with personal information protection compliance audits? From an institutional design perspective, the subjects and objectives of the two are indeed different—data security assessment focuses on "important data and other non-personal data," emphasizing risk identification and evaluation; personal information protection compliance audit focuses on "personal information," emphasizing legality and compliance review. However, for most data processors, important data and personal information are often intertwined within the same business systems and data processing workflows; the work of mapping data assets, investigating data processing activities, and reviewing security measures is highly common. Therefore, if both tasks can be completed in a single coordinated operation, it is a pragmatic and efficient choice.

Conclusion

Let's allow the dust to settle and see where we land!

If compliance is merely viewed as an isolated task, enterprises will inevitably be overwhelmed; if enterprises merely follow various regulations and national standards, playing compliance whack-a-mole, enterprises' compliance work will likewise be unsustainable. The only viable path is to embed data compliance work into overall workflows and SOPs, and to place data security considerations at the forefront of the entire business process—incorporating a security perspective into every stage of data collection, storage, transfer, and productization. When assessing financial risks and weighing benefits against costs, treat data security as a mandatory item; in daily operations, continuously establish mechanisms for recording and reviewing data flows. In this way, whether it is personal information protection audits or data security risk assessments, they will come naturally for enterprises rather than being last-minute cramming.

If you would like to know more information about the subjects covered in this publication, please contact:

Xun Yang
+86 21 3135 8799
xun.yang@llinkslaw.com

SHANGHAI

19F, ONE LUJIAZUI
68 Yin Cheng Road Middle
Shanghai 200120 P.R.China
T: +86 21 3135 8666
F: +86 21 3135 8600

BEIJING

30F, Central Tower, China Overseas Plaza, 8 Guanghuadongli, Chaoyang District
Beijing 100020 P.R.China
T: +86 10 5081 3888
F: +86 10 5081 3866

SHENZHEN

18F, China Resources Tower
2666 Keyuan South Road, Nanshan District
Shenzhen 518063 P.R.China
T: +86 755 3391 7666
F: +86 755 3391 7668

HONG KONG

Room 3201, 32/F, Alexandra House
18 Chater Road
Central, Hong Kong
T: +852 2592 1978
F: +852 2868 0883

LONDON

1/F, 3 More London Riverside
London SE1 2RE
United Kingdom
T: +44 (0)20 3283 4337
D: +44 (0)20 3283 4323

www.llinkslaw.com

Wechat: LlinksLaw

WE LINK LOCAL LEGAL INTELLIGENCE WITH THE WORLD