

China Cybersecurity Law (CSL) – 2016

China Cybersecurity Law sets national rules for network security, personal data protection, data localization, and critical infrastructure oversight.



What it is

China Cybersecurity Law (CSL) is a national regulatory framework that establishes legal requirements for protecting network security, safeguarding personal information, and maintaining the integrity of critical information infrastructure within China. The CSL aims to enhance data protection, mitigate cybersecurity risks, and ensure the safe operation of digital systems.

Issued by the Standing Committee of the National People’s Congress, the CSL applies to all network operators, service providers, and organizations that process personal or important data within China. It covers areas such as security controls for networks and systems, data localization, real-time monitoring, and incident reporting, and places obligations on organizations to strengthen cybersecurity practices and regulatory compliance.

At a glance

PUBLISHER National People's Congress (NPC)	TYPE Framework	VERSION Cybersecurity Law of the People's Republic of China
EFFECTIVE June 1, 2017	DOMAIN Cybersecurity	FAMILY Global Privacy Regulations
REGION China	ADOPTION MODEL Regulatory Compliance	IMPLEMENTATION COMPLEXITY High

Source: https://www.npc.gov.cn/englishnpc/c23934/202112/t20211209_385109.html

Why it matters

- **Strengthen cybersecurity governance** Drive more structured oversight of network security responsibilities and accountability across all organizational levels.
- **Enhance data protection practices** Support implementation of robust technical and organizational controls to better secure personal and important information.
- **Improve regulatory compliance** Facilitate alignment with national legal requirements, reducing exposure to financial penalties and enforced remedial actions.
- **Increase audit readiness** Provide clear criteria for documenting controls and security activities to streamline internal and external review processes.

How SmartSuite supports CSL

Cybersecurity Control and Compliance Framework Structure CSL requirements with ownership, scope, and implementation tracking across systems.	Data Classification and Localization Management Track data classification, storage locations, and localization requirements for critical data.	Access Control and Network Security Governance Manage identity, authentication, and network protection controls aligned to CSL expectations.
Critical Infrastructure Security Management Identify and manage security controls for systems designated as critical infrastructure.	Incident Response and Regulatory Reporting Track security incidents and manage reporting obligations to Chinese authorities.	CSL Compliance Monitoring and Audit Readiness Provide dashboards showing control coverage, data governance posture, and CSL compliance readiness.

Common framework mappings

- APEC PF
- CIS Controls v8.1
- GDPR
- ISO 27001:2022
- ISO 27701
- MLPS 2.0
- NIST CSF 2.0
- PIPL

Official resources

China Cybersecurity Law (CSL) Official Text
Defines the legal requirements for cybersecurity and data protection in China.
npc.gov.cn/englishnpc/c23934/202112/t20211209_385109.html

Frequently asked questions

- What is the China Cybersecurity Law (CSL) used for?**
The China Cybersecurity Law (CSL) is used to establish legal requirements for protecting network security, personal information, and critical information infrastructure in China. Its primary goals are to enhance data protection, reduce cybersecurity risks, and ensure the safe operation of digital and networked systems.
- Is compliance with the China Cybersecurity Law mandatory?**
Yes, compliance with the CSL is mandatory for organizations operating within China, including all network operators and entities processing personal or important data. Non-compliance can result in regulatory actions, fines, or business restrictions.
- Who does the China Cybersecurity Law apply to?**
The CSL applies to network operators, service providers, and organizations that collect, process, or store personal and important data within China. This includes both domestic and international companies providing services or handling data in the Chinese market.
- What are key compliance requirements under the China Cybersecurity Law?**
Key requirements include implementing technical and organizational security controls, conducting cybersecurity risk assessments, establishing monitoring and incident response mechanisms, localizing certain data within Chinese territory, and fulfilling breach notification obligations to authorities.
- How does an organization implement the China Cybersecurity Law?**
Organizations should translate legal requirements into operational controls by classifying systems, assessing risks, developing governance policies, and conducting regular audits. Building an incident response plan and continuously monitoring security controls are also essential for compliance.

How does the China Cybersecurity Law relate to other standards such as ISO 27001?

The CSL can be integrated with global standards like ISO 27001, leveraging common control domains such as risk management, incident response, and data protection. However, CSL includes specific, country-level requirements—such as data localization—not present in international standards.

What are the ongoing compliance obligations for organizations under the CSL?

Ongoing obligations include maintaining up-to-date security controls, performing periodic risk assessments, keeping accurate records of data processing, monitoring for and reporting incidents, and ensuring employee training and awareness of cybersecurity responsibilities.

How would SmartSuite support China Cybersecurity Law (CSL)?

SmartSuite supports CSL compliance by enabling organizations to manage risk registers, build and map control libraries to CSL requirements, collect and retain evidence of security activities, facilitate audit readiness, track remediation efforts, and generate reporting dashboards to monitor and demonstrate regulatory compliance.

License included / downloadable: Yes The Cybersecurity Law of the People's Republic of China is publicly available through official Chinese government publications.

Full framework page and mappings: smartsuite.com/frameworks/china-cybersecurity-law-csl-2016