

Latest update of China Cyber Security Law

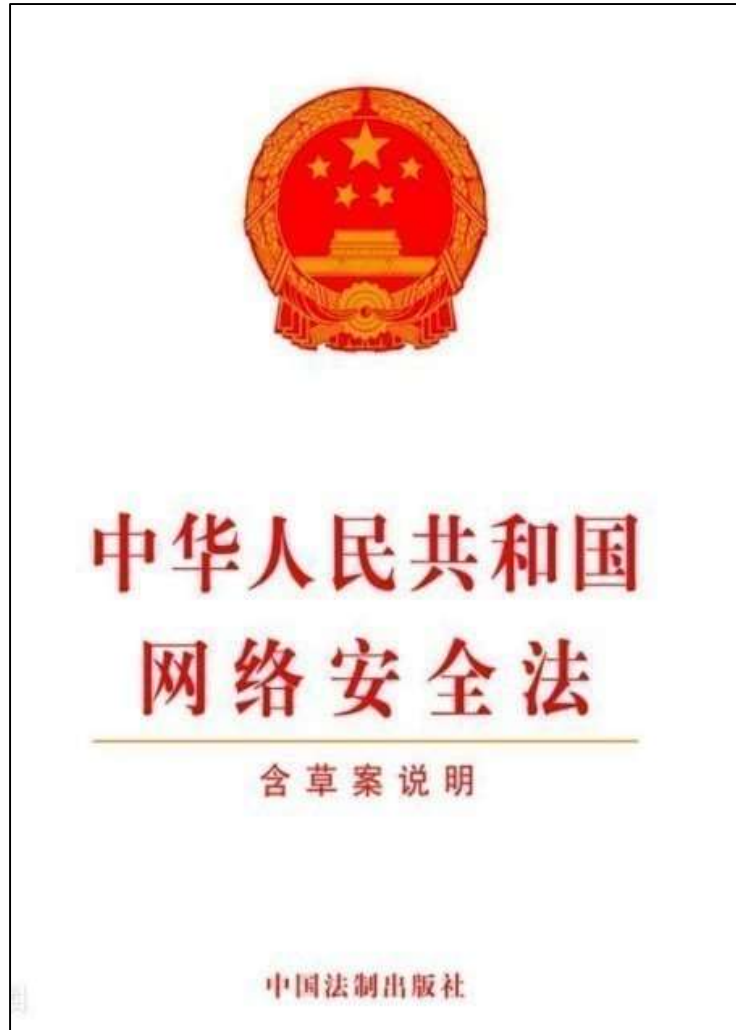
March 2018



The better the question. The better the answer.
The better the world works.

Quick Recap of the CSL – Effective on 1 June 2017

Key Contents



About this law

- ▶ The first comprehensive law **on cybersecurity** and **privacy protection** in China
- ▶ Include altogether 7 charters for **79** articles
- ▶ Was reviewed and discussed 3 times by the NPC Standing Committee

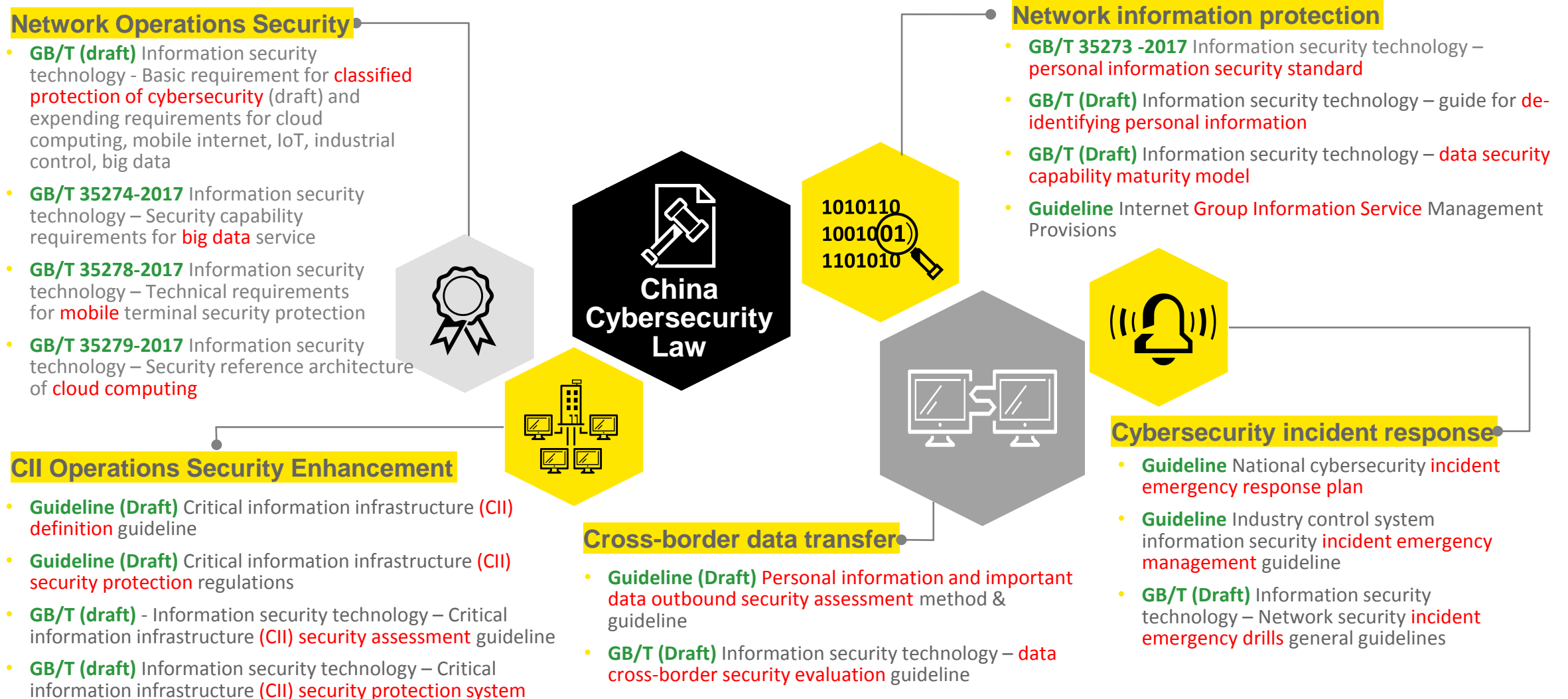
Main government bodies

- ▶ Cyberspace Administration of China (**CAC**)
- ▶ The Ministry of Public Security of China (**MPS**)
- ▶ The Ministry of Industry and Information Technology of China (**MIIT**)






Key requirements

- ▶ **Network Operator** shall fulfill security duties based on **classified cybersecurity protection** system and formulate emergency response plan for cybersecurity incidents.
- ▶ **Critical Information Infrastructure (CII)** shall enhance operation security, implement **data localization** solution and conduct **risk assessment before cross-border data transfer**.
- ▶ **Personal information** shall be protected by network operators following **legitimacy, rightness and necessity** principles in all data handling activities.
- ▶ **Cyber defense systems** shall be established in form of security risk assessment, monitoring, surveillance, warning, emergency response, etc.

A series of supporting regulations and national standards (GB, GB/T) are established to support CSL implementation



What areas should be **focused** on and how to stay compliant with relevant requirements?

Key areas to focus	Relevant guidance and standards
 Cross-border Data Transfer <p>Article 37 (CSL): A security assessment shall be conducted if CII operators transfer personal information and important data out of mainland China. Article 2 (Data Outbound Provision Assessment Method-DRAT): Network operator need to conduct security assessment for data cross-border transfer.</p>	<ul style="list-style-type: none">• Guideline (DRAFT) - Personal information and important data outbound security assessment method & guideline• GB/T (DRAFT) - Information security technology – data cross-border security evaluation guideline
 Data Storage Localization <p>Article 37 (CSL): Personal information and important data collected and produced by CII operators shall be stored in Mainland China. Article 2 (Data Outbound Provision Assessment Method-DRAT): Non-CII also need to fulfill data storage localization requirement</p>	<ul style="list-style-type: none">• Guideline (DRAFT) - Critical information infrastructure definition guideline• Guideline (DRAFT) - Personal information and important data outbound security assessment method & guideline• GB/T (DRAFT) - Information security technology – data cross-border security evaluation guideline
 Classified Cybersecurity Protection Framework <p>Article 21 (CSL): All network operators shall fulfill security protection duties according to the requirements of classified cybersecurity protection system.</p>	<ul style="list-style-type: none">• GB/T (DRAFT) - Information security technology - Basic requirement for classified protection of cybersecurity (draft) and expending requirements for cloud computing, mobile internet, IoT, industrial control, big data
 Real name identity <p>Article 24 (CSL): Network shall require users to provide real identity information when providing network access or information release service.</p>	<ul style="list-style-type: none">• Guideline Administrative Provisions on the Account Names of Internet Users• Guideline Administrative Measures for Internet Information Services
 Personal Information Security and Compliance <p>Article 41 (CSL): Network operator shall preserve the confidentiality of user information they collect, following principles of legality, legitimacy and necessity, and obtaining consents from data subjects.</p>	<ul style="list-style-type: none">• GB/T 35273 -2017 Information security technology – personal information security standard• GB/T (DRAFT) - Information security technology – guide for de-identifying personal information

What areas should be **focused** on and how to stay compliant with relevant requirements?

Key areas to focus

Cross-border Data Transfer

Article 37 (CSL): A security assessment shall be conducted if CII operators transfer personal information and important data out of mainland China.
Article 2 (Data Outbound Provision Assessment Method-DRAT): **Network operator** need to conduct security assessment for data cross-border transfer.



Data Storage Localization

Article 37 (CSL): Personal information and important data collected and produced by CII operators shall be stored in Mainland China.
Article 2 (Data Outbound Provision Assessment Method-DRAT): Non-CII also need to fulfill data storage localization requirement



Classified Cybersecurity Protection Duties

Article 21 (CSL): All network operator shall fulfill security protection duties according to the requirements of classified cybersecurity protection system.



Real name identity

Article 24 (CSL): Network shall require users to provide real identity information when providing network access or information release service.



Personal Information Security and Compliance

Article 41 (CSL): Network operator shall preserve the confidentiality of user information they collect, following principles of legality, propriety and necessity, and obtaining consents from data subjects.

Recommended actions

- 1. Identify and understand existing cross-border data transfer scenarios**
 - Business purposes
 - Data type (personal information, personal sensitive information) and amount
 - Data flow
 - Consent status
- 2. Perform self risk evaluation based on national guideline and identify gaps:**
 - Impact level
 - Security capability of data senders and recipients
- 3. Conduct remedial actions to mitigate risk level to ensure data can be allowed to transfer overseas**
 - Obtain consents from data subject
 - Decrease data volume or transmission frequency
 - Perform de-identification on personal data
 - Establish data cross-border management system
 - Etc.

What areas should be **focused** on and how to stay compliant with relevant requirements?

Key areas to focus

Cross-border Data Transfer

Article 37 (CSL): A security assessment shall be conducted if CII operators transfer personal information and important data out of mainland China.
Article 2 (Data Outbound Provision Assessment Method-DRAT): Network operator need to conduct security assessment for data cross-border transfer.

Data Storage Localization

Article 37 (CSL): Personal information and important data collected and produced by CII operators shall be stored in Mainland China.
Article 2 (Data Outbound Provision Assessment Method-DRAT): Non-CII also need to fulfill data storage localization requirement

Classified Cybersecurity Protection Duties

Article 21 (CSL): All network operator shall fulfill security protection duties according to the requirements of classified cybersecurity protection system.

Real name identity

Article 24 (CSL): Network shall require users to provide real identity information when providing network access or information release service.

Personal Information Security and Compliance

Article 41 (CSL): Network operator shall preserve the confidentiality of user information they collect, following principles of legality, propriety and necessity, and obtaining consents from data subjects.

Recommended actions

1. Conduct personal information and important data mapping, understanding data storage location and data flow (how to collect, store, use and transfer)

System name	Business Users	Contact Person	Type of personal information	Data Subject	Collection methods	Consents obtained?
Amount of PII records	Type of important data	Hosting Location	Data Interfaces	Any interfaces transferring data to 3rd parties	Any interfaces transferring data overseas	

2. Plan to setup infrastructure in localizing the personal and important data

Guiding Law & Guideline

	Cyber Security Law of the People's Republic of China	Personal Information and Important Data Outbound Security Assessment Method & Guideline (Draft)

PII & Critical Data Cross-Border Provision Principles

Data Cross-Border Provision Requirements (Elements)	Network Operator	CII
PII & Critical Data localization in principle	Optional (Under CSL guideline)	Required (Under CSL article)
PII Data cross-border provision in principle	Allowed (with security self-assessment)	Prohibited (with Gov approval obtained)
Critical data cross-border provision in principle	Allowed (with security self-assessment)	Prohibited (with Gov approval obtained)
Security Assessment/Approval in principle	By self or government assessment (Under SOCS PII)	By government assessment only

What areas should be **focused** on and how to stay compliant with relevant requirements?

Key areas to focus



Cross-border Data Transfer

Article 37 (CSL): A security assessment shall be conducted if CII operators transfer personal information and important data out of mainland China.
Article 2 (Data Outbound Provision Assessment Method-DRAT): Network operator need to conduct security assessment for data cross-border transfer.



Data Storage Localization

Article 37 (CSL): Personal information and important data collected and produced by CII operators shall be stored in Mainland China.
Article 2 (Data Outbound Provision Assessment Method-DRAT): Non-CII also need to fulfill data storage localization requirement



Classified Cybersecurity Protection Framework

Article 21 (CSL): All network operator shall fulfill security protection duties according to the requirements of classified cybersecurity protection system.



Real name identity

Article 24 (CSL): Network shall require users to provide real identity information when providing network access or information release service.



Personal Information Security and Compliance

Article 41 (CSL): Network operator shall preserve the confidentiality of user information they collect, following principles of legality, propriety and necessity, and obtaining consents from data subjects.

Recommended actions

1. Conduct shadow IT discovery on Internet-facing websites, and develop an application inventory to ensure all IT assets are under proper control.
2. Classify all applications and perform gap analysis from both managerial and technical perspectives
 - Management**
 - Security Strategy and Management Policy
 - Security Management Organization and People
 - Security Development
 - Security Operation
 - Technical**
 - Physical and Environment
 - Network and Communication
 - Device and Computing
 - Application and Data
3. Perform penetration testing and vulnerability scanning to ensure the security of applications, especially Internet-facing websites.
4. Conduct remediation based on the priority of systems and prepare for official MLPS registration and evaluation.

What areas should be **focused** on and how to stay compliant with relevant requirements?

Key areas to focus



Cross-border Data Transfer

Article 37 (CSL): A security assessment shall be conducted if CII operators transfer personal information and important data out of mainland China.
Article 2 (Data Outbound Provision Assessment Method-DRAT): Network operator need to conduct security assessment for data cross-border transfer.



Data Storage Localization

Article 37 (CSL): Personal information and important data collected and produced by CII operators shall be stored in Mainland China.
Article 2 (Data Outbound Provision Assessment Method-DRAT): Non-CII also need to fulfill data storage localization requirement



Classified Cybersecurity Protection Duties

Article 21 (CSL): All network operator shall fulfill security protection duties according to the requirements of classified cybersecurity protection system.



Real name identity

Article 24 (CSL): Network shall require users to provide real identity information when providing network access or information release service.



Personal Information Security and Compliance

Article 41 (CSL): Network operator shall preserve the confidentiality of user information they collect, following principles of legality, propriety and necessity, and obtaining consents from data subjects.

Recommended actions

- 1. Identify scenarios which need real name identity and methods, including:**
 - Websites / Application registration
 - Information release functions
 - Network access
- 2. Register the websites and implement control functions:**
 - ICP/MPS/AIC registration
 - Keep logs for no less than 6 months
 - Monitoring and filtering on information release functions
 - Implement real name identity solution for network services provided

What areas should be **focused** on and how to stay compliant with relevant requirements?

Key areas to focus



Cross-border Data Transfer

Article 37 (CSL): A security assessment shall be conducted if CII operators transfer personal information and important data out of mainland China.
Article 2 (Data Outbound Provision Assessment Method-DRAT): Network operator need to conduct security assessment for data cross-border transfer.



Data Storage Localization

Article 37 (CSL): Personal information and important data collected and produced by CII operators shall be stored in Mainland China.
Article 2 (Data Outbound Provision Assessment Method-DRAT): Non-CII also need to fulfill data storage localization requirement



Classified Cybersecurity Protection Duties

Article 21 (CSL): All network operator shall fulfill security protection duties according to the requirements of classified cybersecurity protection system.



Real name identity

Article 24 (CSL): Network shall require users to provide real identity information when providing network access or information release service.



Personal Information Security and Compliance

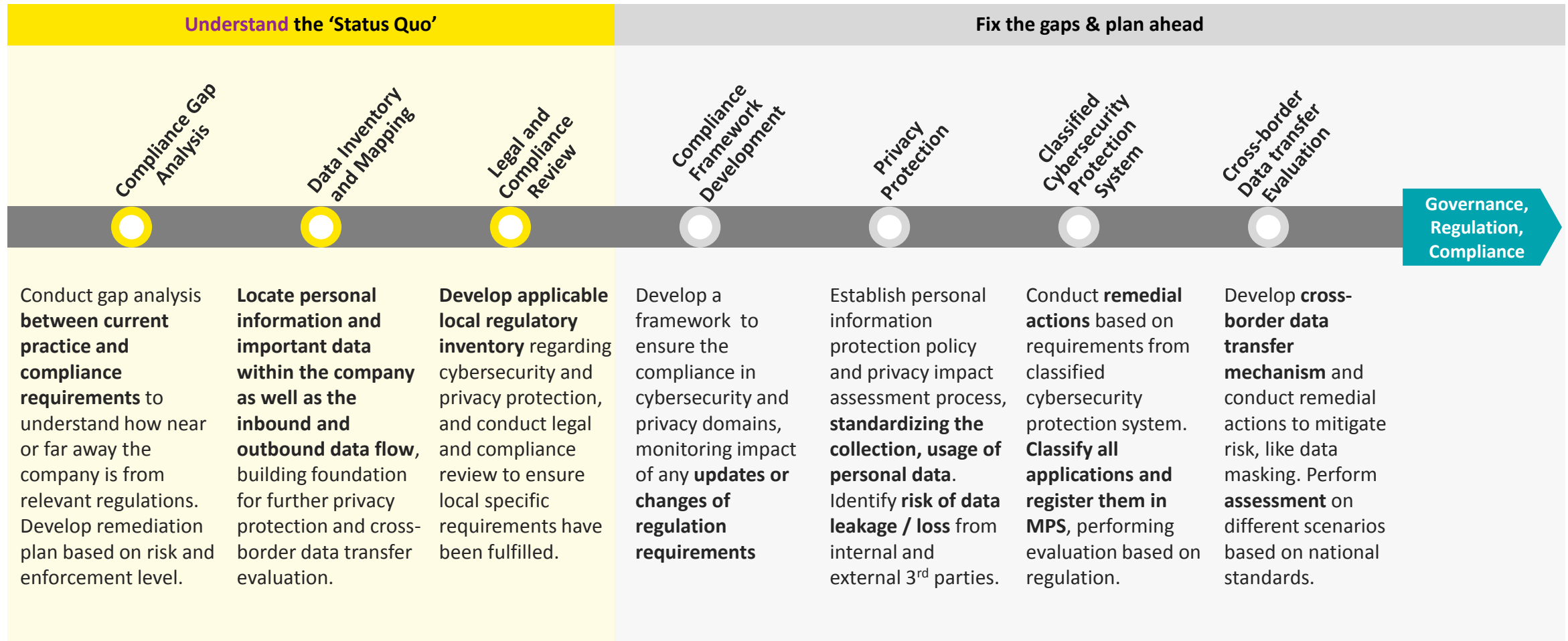
Article 41 (CSL): Network operator shall preserve the confidentiality of user information they collect, following principles of legality, propriety and necessity, and obtaining consents from data subjects.

Recommended actions

- 1. Review and update privacy policy to end users, including:**
 - Consumers
 - Employees
 - HR Candidates
- 2. Conduct remediation from technical perspectives, like adding privacy policy in websites, privacy policy update notification and message, etc.**
- 3. Develop on-going personal information protection mechanisms, including:**
 - Personal Information Protection Policy
 - Privacy Impact Assessment Process
 - Guideline on collection, storage, usage and transfer of personal information
 - Awareness training and workshop

Time to establish a framework to ensure continuous compliant with regulation in cybersecurity and privacy practices

Understand “Where you are” is the first step towards compliance, and then take remedial actions according to different priorities while developing a continuous governance framework to ensure the company stay compliant with all regulation requirements.



Key challenges and recommendations when moving towards compliance for multinational companies



Key challenges

- ▶ **UNCERTAINTIES** exist in current version of CSL supporting documents, which requires close monitor of the regulatory progress and react accordingly.
- ▶ **COLLABORATION FROM DIFFERENT DEPARTMENTS**, especially IT, legal, compliance, business department, is needed to ensure the completeness and accuracy of the assessment result.
- ▶ **IMPACT ON 'BUSINESS AS USUAL'** since the potential effort required to be invested into the assessment and associated remediation, which might have impact on existing IT environment and business process.
- ▶ **COMMUNICATION AND ALIGNMENT WITH GLOBAL** might take great efforts and time to ensure full understanding and support from global, which is significant to fulfill local regulatory requirements.
- ▶ **REMEDATION ACTION PLANS HAVE TO BE SENSIBLE & ACTIONABLE** with resources to be spent on issues that really matter.



Recommendations

- ▶ **BE PREPARED AND BE FLEXIBLE:** we recommend to collect the info. & data according to requirements from CSL and relevant regulatory, and keep pace with the development, thus to adjust the priority in a timely manner.
- ▶ **CROSS-FUNCTION COMPLIANCE COMMITTEE** with clear roles and responsibilities defined to ensure adequate support and resource are available, as well as keeping the progress on track.
- ▶ **IMPACT ON EXISTING BUSINESS ENVIRONMENT AND PROCESSES** should be taken into considerations when designing remedial tasks, developing actionable plan to minimize the potential negative impact.
- ▶ **GLOBAL' S WELL UNDERSTANDING** of CSL, especially its applicability, impact and enforcement, is critical for MNCs to understand current status and conduct implementation.
- ▶ **REMEDATION ACTIONS PLANNING** is essential to ensure risks, time, costs, effort and constraints are considered into action prioritization and planning.

EY | Assurance | Tax | Transactions | Advisory

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

© 2018 Ernst & Young (China) Advisory Ltd
All Rights Reserved.

APAC no. 03006415
ED MMY

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.

ey.com/china