protiviti®
Face the Future with Confidence

Critical Information Infrastructure

As part of our series providing insights into the Cybersecurity Law of the People's Republic of China (PRC), this fourth installment focuses on the requirements in Section Two, Chapter Three, pertaining to Critical Information Infrastructure (CII) operators. According to the Cybersecurity Law, CII is defined as any information infrastructure that can endanger national security, national strategy, and civil welfare in the event of a data breach, compromised network, or system malfunction.

Overview of Critical Information Infrastructure

The Regulation for CII Security ("the Regulation") was drafted by the Cyberspace Administration of China (CAC), the agency responsible for compliance and enforcement of the Cybersecurity Law. The National Information Security Standardization Technical Committee of China, commonly referred to as TC260, is responsible for the associated technical standards, specifications, measures, and guidelines.

According to the CAC, critical systems across 11 major industries are considered CIIs. It's important to note that the definition of CII is not exhaustive and may also cover networks or applications whose failure could harm national security, national economy, or public interest. The Cybersecurity Law provides overarching principles and high-level requirements for CII compliance.

The scope of application, enforcement measures, technical specifications, and standards are stipulated by the State Council and industry regulatory ministries and commissions. Industry regulatory bodies are authorized to define detailed CII requirements and rules for companies in their respective industries according to the principles of the Regulation. Specific requirements and rules are published or released in multiple forms, from administrative orders and notifications to opinions, proposals, and provisions.

In addition to the State Council and industry regulatory bodies, local governments of major cities and provinces also have the authority to identify companies as CII operators and specific systems as CIIs. Companies determined to be CII operators must regularly follow the updates on the requirements and rules released by the industry regulatory bodies and local governments.

Identification of Critical Information Infrastructure

According to the Regulation, companies should consider three factors in determining which systems and applications could potentially be classified as CII.

1. Whether the business is classified as a critical business

The Regulation classifies businesses that fall within 11 industries as critical businesses. These industries include public communications, energy, finance, and public services, among others.
To determine whether all or part of their business is classified as a critical business, companies must consider the following:

- Do we have businesses or operations that are in the 11 pre-defined industries?
- Do we have businesses or operations that could be classified as critical businesses according to the definition set by different industry regulatory bodies?
- Do we have business or operations that could impact or harm national security, national economy, or public interest?

2. Whether systems are used to support a "critical business"

Organizations must identify whether any of their systems may be supporting CII operators that conduct critical business. The following questions can help determine which systems may be considered CIIs:

- Do the systems store and process important data as defined by industry regulatory bodies in mainland China? Examples of important data are listed in the table below.
- How many types of important data do the systems store and process?
- How frequently do systems process data?
- How much revenue is derived from the data processed by the systems?
- What are the consequences when systems are discontinued? For example, what would be the impact on reputation, the economy, lives, social order, or national security?
- How much is the loss or impact within the Maximum Tolerable Downtime (MTD)?
- Are there any alternative ways to run the business without the systems? If so, how sustainable are these alternatives?

Critical Industry	Critical Business	Important Data
Financial Services	• Banking • Securities & Futures • Clearing & Settlement • Insurance	• Business Operations • Security • Privacy & Credit • Organization • Analysis & Profiling
Medical & Healthcare	• Establishment Operations • Disease Control • Emergency Center Operations	• Health & Privacy • Medical Records • Clinical Trials • Traceable IDs • Emergency • Disease Control • Genetic Data
Manufacturing	• Business Operations • Intelligent Industry • Control of Dangerous Goods • High-Risk Facility Operations	• Industrial Statistics • Strategy & Planning • Production & Sales • Purchasing • Delivery • Market Analysis • Investment

* This is not an exhaustive list

3. Potential impact of a security incident in the system

The Regulation provides multiple criteria to determine whether the impact from system damage is severe enough to classify the systems as CIIs.

To begin, companies must consider the following questions on information assets, customers and users, asset values, and incident frequency:

- In terms of number of people and percentage of population, who will be affected by security incidents or data breaches?
- What are the consequences of security incidents or data breaches, such as privacy data or company data leaks?
- How much damage will the company and national security suffer from security incidents or data breaches?

These three factors will help companies assess whether they and their systems are likely to be classified as CII operators and CIIs. Companies who are classified as CIIs will receive official notifications from the local police or industry regulatory bodies. They must open communication channels with the local police or industry regulatory bodies to confirm the official notification and coordinate the submission of compliance documents. CII operators should maintain regular contact with these organizations to stay up-to-date on the latest regulatory rules, which may often be presented as regulatory opinions, notifications, or even administrative orders.

Compliance Requirements for Critical Information Infrastructure

While technical standards and specifications are currently under development or being drafted for comment, industry regulatory bodies may also have specific industrial requirements. The following table summarizes the key requirements for CIIs.

Article	Legal Requirements
No. 32	The State Council and associated departments shall compile and organize security enforcement plans, as well as guide and supervise security protection efforts for critical information infrastructure operations.
No. 33	CIIs must have the capability to support business stability and sustain operations.
No. 34, Sec. 1	Set up a dedicated security management body with a designated security management leader; conduct security background checks on personnel in key positions.
No. 34, Sec. 2	Periodically conduct cybersecurity education, technical training, and skills evaluations for employees.
No. 34, Sec.3	Conduct disaster-recovery backups of critical systems and databases.
No. 34, Sec.4	Formulate emergency response plans for cybersecurity incidents and regularly organize drills.
No. 35	Network products and services purchased by CII operators that might impact national security will be subjected to a national security review by relevant departments.
No. 36	When purchasing network products and services, CII operators must follow relevant guidelines and sign a security and confidentiality agreement with the provider.
No. 38	Critical information infrastructure operators shall conduct testing and assessment of cybersecurity risks on critical information infrastructure.
No. 38	State cybersecurity departments shall conduct annual inspections and assessments of network security, as well as submit a cybersecurity report and proposed improvement measures to the departments responsible.

Compliance Considerations and Challenges

Compliance Enforcement from Industry Regulatory Bodies

Once a company is classified as a CII operator and has reported to the respective industry regulatory body, that regulatory body will be responsible for enforcing the company's CII compliance. When appropriate, the regulatory body may issue additional rules and requirements for the company as long as these do not conflict with the existing laws and regulations of the central government.

The regulatory body can also conduct inspections and assessments in accordance with these additional requirements and rules. If they believe the company is not fulfilling their obligations as a CII operator, they may issue various penalties. Penalties depend on the severity of the violation and may include administrative warnings and ordered rectification, business suspension, license or certificate revocation, and administrative fines.

CII operators have tougher requirements and stricter compliance processes than network operators. Severe consequences may occur if CII operators practice passive compliance—waiting for explicit remediation orders by regulatory bodies. Instead, companies are encouraged to align with key stakeholders to actively engage in compliance.

Adopting an Active and Proactive Compliance Approach

Considering the complex structure of CII compliance, both in terms of requirements and enforcement, CII operators should adopt an active, or even proactive, approach. An active approach entails identifying gaps between current practices and effective laws and regulations for future remediation and rectification. In this situation, compliance is seen as a separate process implemented to satisfy laws and regulations. In general, an active approach is considered good enough for normal compliance, although there might be a deviation between operational procedures and compliance requirements. However, this deviation is easily exposed through the technical tests and assessments that are part of the compliance process.

A proactive approach means implementing effective security measures in response to all potential security threats and legal concerns, even if those measures are not explicitly stated in the laws or regulations. While more expensive and technically demanding, a proactive approach may be more effective because of its focus on potential technical and legal concerns.

Tests and Assessments from Regulatory Bodies

Industry regulatory bodies are authorized by Article 39 of the Cybersecurity Law to initiate a variety of tests and assessments of CII operators. These include on-site inspections and remote penetration testing. CII operators may be informed before the tests and assessments to allow for last-minute preparations, but these warnings are not guaranteed, and organizations should be prepared for surprise inspections.

The best compliance strategy is to always be prepared for sudden assessments. If the actual operation procedures of CII operators are different from their designed procedures, operators won't have time to do last-minute preparations. It's important for security policies and procedures to be well-designed, documented, and communicated. Frequent spot inspections and reviews, along with a checklist, will also help ensure compliance with designed procedures. These can ensure that good security practices are executed every single day.

Another key factor to ensuring satisfactory results from assessments is communication, especially when a company is not familiar with—or unprepared for—unexpected assessments. A typical mistake is allowing frontline staff to handle inspections directly. This may result in misunderstandings and miscommunication since frontline staff is often not fully informed about compliance requirements and processes.

Protiviti Cybersecurity and Privacy Protection Services

IT Specialized Audit	• Often included in the overall audit co-sourcing or outsourcing program • More in-depth and technical than Information Technology General Control (ITGC) audit • Often focused on a specific part of IT operations such as Cybersecurity or Disaster Recovery
Security Risk and Compliance Assessment	• International Security Standards: ISO/IEC 2700x, NIST Cybersecurity Framework, CSA Cloud Control Matrix • Payment Card Security Standards: PCI DSS 3.x • Other Regulations/Standards: China Cybersecurity Law, HKMA, SFC, MAS, COSO SOX, ISO/IEC 27701
Data Privacy Services	• Compliance assessment against privacy regulations: Hong Kong PDPO Cap.486, China Personal Information Protection, EU GDPR, US CCPA • Managed privacy services: Privacy-as-a-service • Personal data inventory advisory
Attack and Penetration Service	• Vulnerability scan and penetration test • Source code review • Red team test • Phishing and social engineering test
Security Program and Strategy Design	• Design and revision of cybersecurity strategy and program • Design and revision of security policies, such as data and information classification • Design, revision, and implementation of security procedures
Security Architecture and Control Design	• System hardening review and enhancement • Security architecture design: on-premise, cloud platform • Security control design and review: firewall, data loss prevention, privileged access management, event log analyzer
Security Implementation Services	• Security tools design and selection • Project management and support for security tools implementation • Leverage Protiviti global partnerships with OneTrust, SailPoint, CyberArk, Palo Alto, ServiceNow, Carbon Black, Splunk, LogRhythm, etc.
Managed Security Services	• Security resource augmentation • Managed security operations • Third-party risk outsourcing
Incident Response and Forensics	• Security incident response advisory and support • Security incident investigation and root-cause analysis • Compromise assessment
Security Awareness and Capability Advisory	• Blueteam security assessment and advisory (e.g. SOC, MSSP) • Cyber incident handling and mitigation review • Security awareness assessment and support

How Protiviti Can Help

Protiviti aids businesses in ensuring that their IT services meet legal requirements and regulatory rules on both national and industry-specific levels. With a team of IT security professionals, compliance experts, auditors, and other professionals, Protiviti keeps track of evolving regulations based on industry innovations, environmental trends, and emerging risks.

Protiviti security and privacy services will evaluate your current compliance according to relevant legal requirements and regulatory rules and develop technical solutions that correspond with your current technology, procedures, and resources competency. We will close gaps in your IT technology and processes in line with your budget plan, as well as prevent disruptions to normal IT and business operations from compliance activities.

Contacts

Michael Pang
Managing Director, Technology Consulting
Mobile (HK): +852 9211 9853
Mobile (PRC): +86 131 4399 6166
michael.pang@protiviti.com

Jonathan Hsieh
Associate Director, Technology Consulting
Office: +86 21 5153 6900
Mobile: +86 138 1745 5636
jonathan.hsieh@protiviti.com

Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.