NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document : Secure Controls Framework (SCF) version 2025.2
STRM Guidance: https://securecontrolsframework.com/set-theory-relationship-mapping-strm/

Focal Document: **China Cybersecurity Law of the People's Republic of China (2017)**
Focal Document URL: https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/
Published STRM URL: https://securecontrolsframework.com/content/strm/scf-strm-apac-china-cybersecurity-law-2017.pdf

Note: The Cybersecurity Law of the People's Republic of China (China Cybersecurity Law) is a dictate from the Chinese Communist Party (CCP) and should be viewed by western organizations as nothing more than an insincere façade that empowers the CCP with authority to do as it wishes under the guise of cybersecurity and national security. To comply with the China Cybersecurity Law, western organizations would be committed to fully exposing their networks and data to the CCP, as well as provide unfettered support for any investigations launched by CCP officials. Non-compliance with the China Cybersecurity Law should be considered as a viable option, since compliance with this law could lead to many negative consequences for an organization, including:
(1) non-compliance with actual data protection laws/regulations;
(2) potential human rights abuses by the CCP;
(3) compromise of an organization's networks by CCP actors; and/or
(4) loss of intellectual property to the CCP.

To demonstrate cybersecurity practices, organizations must be capable of following the rule of law according to a defined standard. Unfortunately, China is an authoritarian state that is ruled by the whims of the CCP and that makes the concept of "the rule of law" untenable under a legal system that is little more than a thinly disguised dictatorship. Given this reality, western organizations are highly encouraged to perform due diligence as to the true cost associated with compliance. The organization's Board of Directors (BoD) is ultimately be responsible to make the decision and cybersecurity practitioners should find ways to remind board members of their fiduciary duty to protect the organization given the grave implications of compliance with the CCP's vague cybersecurity guidelines that may easily be abused.

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
Article 1	N/A	This Law is formulated in order to: ensure cybersecurity; safeguard cyberspace sovereignty and national security, and social and public interests; protect the lawful rights and interests of citizens, legal persons, and other organizations; and promote the healthy development of the informatization of the economy and society.	Functional	no relationship	N/A	N/A	N/A		
Article 2	N/A	This Law is applicable to the construction, operation, maintenance, and use of networks, as well as to cybersecurity supervision and management within the mainland territory of the People's Republic of China.	Functional	no relationship	N/A	N/A	N/A		Article 2 defines the scope to include any business network that has a nexus (e.g., physical location) to mainland China.
Article 3	N/A	The State persists in equally stressing cybersecurity and informatization development, and abides by the principles of active use, scientific development, management in accordance with law, and ensuring security. The State advances the construction of network infrastructure and interconnectivity, encourages the innovation and application of network technology, supports the cultivation of qualified cybersecurity personnel, establishes a complete system to safeguard cybersecurity, and raises capacity to protect cybersecurity.	Functional	no relationship	N/A	N/A	N/A		Article 3 is factually incorrect. The lack of granular requirements, or alignment with existing standards, disproves a central claim that this law "establishes a complete system to safeguard cybersecurity." Interpretation of requirements is left to CCP officials.
Article 4	N/A	The State formulates and continuously improves cybersecurity strategy, clarifies the fundamental requirements and primary goals of ensuring cybersecurity, and puts forward cybersecurity policies, work tasks, and procedures for key sectors.	Functional	no relationship	N/A	N/A	N/A		
Article 5	N/A	The State takes measures for monitoring, preventing, and handling cybersecurity risks and threats arising both within and without the mainland territory of the People's Republic of China. The State protects critical information infrastructure against attacks, intrusions, interference, and destruction; the State punishes unlawful and criminal cyber activities in accordance with the law, preserving the security and order of cyberspace.	Functional	no relationship	N/A	N/A	N/A		
Article 6	N/A	The State advocates sincere, honest, healthy and civilized online conduct; it promotes the dissemination of core socialist values, adopts measures to raise the entire society's awareness and level of cybersecurity, and formulates a good environment for the entire society to jointly participate in advancing cybersecurity.	Functional	no relationship	N/A	N/A	N/A		
Article 7	N/A	The State actively carries out international exchanges and cooperation in the areas of cyberspace governance, research and development of network technologies, formulation of standards, attacking cybercrime and illegality, and other such areas; it promotes constructing a peaceful, secure, open, and cooperative cyberspace, and establishing a multilateral, democratic, and transparent Internet governance system.	Functional	no relationship	N/A	N/A	N/A		
Article 8	N/A	State cybersecurity and informatization departments are responsible for comprehensively planning and coordinating cybersecurity efforts and related supervision and management efforts. The State Council departments for telecommunications, public security, and other relevant organs, are responsible for cybersecurity protection, supervision, and management efforts within the scope of their responsibilities, in accordance with the provisions of this Law and relevant laws and administrative regulations. Cybersecurity protection, supervision, and management duties for relevant departments in people's governments at the county level or above will be determined by relevant national regulations.	Functional	no relationship	N/A	N/A	N/A		
Article 9	N/A	Network operators carrying out business and service activities must follow laws and administrative regulations, respect social morality, abide by commercial ethics, be honest and credible, perform obligations to protect cybersecurity, accept supervision from the government and public, and bear social responsibility.	Functional	subset of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.		
Article 10	N/A	The construction and operation of networks, or the provision of services through networks, shall be done: in accordance with the provisions of laws and administrative regulations, and with the mandatory requirements of national standards; adopting technical measures and other necessary measures to safeguard cybersecurity and operational stability; effectively responding to cybersecurity incidents; preventing cybercrimes and unlawful activity; and preserving the integrity, secrecy, and usability of online data.	Functional	intersects with	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.		Article 10 subject to interpretation from a CCP official, since the China Cybersecurity Law fails to provide required controls. This vagueness makes it more of a guideline, masquerading as a law. Obtaining actual compliance with this law is a fantasy, due to the lack of clear requirements.
Article 11	N/A	Relevant Internet industry organizations, according to their Articles of Association, shall strengthen industry self-discipline, formulate cybersecurity norms of behavior, guide their members in strengthening cybersecurity protection according to the law, raise the level of cybersecurity protection, and stimulate the healthy development of the industry.	Functional	no relationship	N/A	N/A	N/A		Article 11 is nonsensical language. There is nothing for an organization to comply with, since it lacks any granular requirements or alignment with existing standards. This leaves the interpretation to a CCP official to define what it means.
Article 12	N/A	The State protects the rights of citizens, legal persons, and other organizations to use networks in accordance with the law; it promotes widespread network access, raises the level of network services, provides secure and convenient network services to society, and guarantees the lawful, orderly, and free circulation of network information. Any person and organization using networks shall abide by the Constitution and laws, observe public order, and respect social morality; they must not endanger cybersecurity, and must not use the Internet to engage in activities endangering national security, national honor, and national interests; they must not incite subversion of national sovereignty, overturn the socialist system, incite separatism, break national unity, advocate terrorism or extremism, advocate ethnic hatred and ethnic discrimination, disseminate violent, obscene, or sexual information, create or disseminate false information to disrupt the economic or social order, or information that infringes on the reputation, privacy, intellectual property or other lawful rights and interests of others, and other such acts.	Functional	no relationship	N/A	N/A	N/A		Article 12 is a "catch all" section that can ensnare any organization or individual with engaging in "activities endangering national security, national honor, and national interests." For an organization to engage in legitimate Environmental, Social and Governance (ESG) activities, that would run afoul of Article 12 for complying with the Uyghur Forced Labor Discloser Act (https://uhrp.org/bill-summary/uyghur-forced-labor-disclosure-act-h-r-1187/)
Article 13	N/A	The State encourages research and development of network products and services conducive to the healthy upbringing of minors; the State will lawfully punish the use of networks to engage in activities that endanger the psychological and physical well-being of minors; and the State will provide a safe and healthy network environment for minors.	Functional	no relationship	N/A	N/A	N/A		
Article 14	N/A	All individuals and organizations have the right to report conduct endangering cybersecurity to cybersecurity and informatization, telecommunications, public security, and other departments. Departments receiving reports shall promptly process them in accordance with law; where matters do not fall within the responsibilities of that department, they shall promptly transfer them to the department empowered to handle them. Relevant departments shall preserve the confidentiality of the informants' information and protect the lawful rights and interests of informants.	Functional	no relationship	N/A	N/A	N/A		

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
Article 15	N/A	The State establishes and improves a system of cybersecurity standards. State Council standardization administrative departments and other relevant State Council departments, on the basis of their individual responsibilities, shall organize the formulation and timely revision of relevant national and industry standards for cybersecurity management, as well as for the security of network products, services, and operations. The State supports enterprises, research institutions, schools of higher learning, and network-related industry organizations to participate in the formulation of national and industry standards for cybersecurity.	Functional	no relationship	N/A	N/A	N/A		
Article 16	N/A	The State Council and people's governments of provinces, autonomous regions, and directly-governed municipalities shall: do comprehensive planning; expand investment; support key cybersecurity technology industries and programs; support cybersecurity technology research and development, application, and popularization; promote secure and trustworthy network products and services; protect intellectual property rights for network technologies; and support research and development institutions, schools of higher learning, etc., to participate in State cybersecurity technology innovation programs.	Functional	no relationship	N/A	N/A	N/A		
Article 17	N/A	The State advances the establishment of socialized service systems for cybersecurity, encouraging relevant enterprises and institutions to carry out cybersecurity certifications, testing, risk assessment, and other such security services.	Functional	no relationship	N/A	N/A	N/A		
Article 18	N/A	The State encourages the development of network data security protection and utilization technologies, advancing the opening of public data resources, and promoting technical innovation and economic and social development. The State supports innovative methods of cybersecurity management, utilizing new network technologies to enhance the level of cybersecurity protection.	Functional	no relationship	N/A	N/A	N/A		
Article 19	N/A	All levels of people's governments and their relevant departments shall organize and carry out regular cybersecurity publicity and education, and guide and stimulate relevant units in properly carrying out cybersecurity publicity and education work. The mass media shall conduct targeted cybersecurity publicity and education aimed at the public.	Functional	no relationship	N/A	N/A	N/A		
Article 20	N/A	The State supports enterprises and education or training institutions, such as schools of higher learning and vocational schools, in carrying out cybersecurity-related education and training, and it employs multiple methods to cultivate qualified personnel in cybersecurity and promote the interaction of cybersecurity professionals.	Functional	no relationship	N/A	N/A	N/A		
Article 21	N/A	The State implements a cybersecurity multi-level protection system [MLPS]. Network operators shall perform the following security protection duties according to the requirements of the cybersecurity multi-level protection system to ensure the network is free from interference, damage, or unauthorized access, and to prevent network data leaks, theft, or falsification:	Functional	intersects with	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.		
Article 22	N/A	Network products and services shall comply with the relevant national and mandatory requirements. Providers of network products and services must not install malicious programs; when discovering that their products and services have security flaws or vulnerabilities, they shall immediately adopt remedial measures, and follow provisions to promptly inform users and report to the competent departments. Providers of network products and services shall provide security maintenance for their products and services, and they must not terminate the provision of security maintenance during the time limits or period agreed on with clients. If a network product or service has the function of collecting user information, its provider shall clearly indicate this and obtain consent from the user; and if this involves a user's personal information, the provider shall also comply with the provisions of this law and relevant laws and administrative regulations on the protection of personal information.	Functional	intersects with	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, processing, storage, sharing, updating and disposal of their Personal Data (PD), where prior to collection the data subject is provided with: (1) Plain language to illustrate the potential data privacy risks of the authorization; (2) A means for users to decline the authorization; and (3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.		Article 22 is nonsensical language. There is nothing for an organization to comply with, since it lacks any granular requirements or alignment with existing standards. This leaves the interpretation to a CCP official to define what it means.
Article 22	N/A	Network products and services shall comply with the relevant national and mandatory requirements. Providers of network products and services must not install malicious programs; when discovering that their products and services have security flaws or vulnerabilities, they shall immediately adopt remedial measures, and follow provisions to promptly inform users and report to the competent departments. Providers of network products and services shall provide security maintenance for their products and services, and they must not terminate the provision of security maintenance during the time limits or period agreed on with clients. If a network product or service has the function of collecting user information, its provider shall clearly indicate this and obtain consent from the user; and if this involves a user's personal information, the provider shall also comply with the provisions of this law and relevant laws and administrative regulations on the protection of personal information.	Functional	intersects with	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of products and/or services across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.		Article 22 is nonsensical language. There is nothing for an organization to comply with, since it lacks any granular requirements or alignment with existing standards. This leaves the interpretation to a CCP official to define what it means.
Article 23	N/A	Critical network equipment and specialized cybersecurity products shall follow national standards and mandatory requirements, and be security certified by a qualified establishment or meet the requirements of a security inspection, before being sold or provided. The state cybersecurity and informatization departments, together with the relevant departments of the State Council, will formulate and release a catalog of critical network equipment and specialized cybersecurity products, and promote reciprocal recognition of security certifications and security inspection results to avoid duplicative certifications and inspections.	Functional	intersects with	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.		Article 23 is nonsensical language. There is nothing for an organization to comply with, since it lacks any granular requirements or alignment with existing standards. There is no established "security certification" for an organization to obtain. This leaves the interpretation to a CCP official to define what it means.
Article 24	N/A	Network operators handling network access and domain name registration services for users, handling stationary or mobile phone network access, or providing users with information publication or instant messaging services, shall require users to provide real identity information when signing agreements with users or confirming the provision of services. Where users do not provide real identity information, network operators must not provide them with relevant services. The State implements a network identity credibility strategy and supports research and development of secure and convenient electronic identity authentication technologies, promoting reciprocal acceptance among different electronic identity authentication methods.	Functional	intersects with	Potential Human Rights Abuses	PRI-16	Mechanisms exist to constrain the supply of physical and/or digital activity logs to the host government that can directly lead to contravention of the Universal Declaration of Human Rights (UDHR), as well as other applicable statutory, regulatory and/or contractual obligations.		Article 24 provides the CCP with authenticated identities, which could lead to human rights abuses. Depending on an organization's Environmental, Social and Governance (ESG) practices, complying with Article 24 could violate the organization's core beliefs about ethical and humane practices.
Article 25	N/A	Network operators shall formulate emergency response plans for cybersecurity incidents and promptly address system vulnerabilities, computer viruses, cyber attacks, network intrusions, and other such cybersecurity risks. When cybersecurity incidents occur, network operators should immediately initiate an emergency response plan, adopt corresponding remedial measures, and report to the relevant competent departments in accordance with relevant provisions.	Functional	intersects with	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.		

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
Article 26	N/A	Those carrying out cybersecurity certification, testing, risk assessment, or other such activities—or publicly publishing cybersecurity information such as system vulnerabilities, computer viruses, network attacks, or network incursions—shall comply with relevant national provisions.	Functional	intersects with	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.		Article 26 is nonsensical language. There is nothing for an organization to comply with, since it lacks any granular requirements or alignment with existing standards. This leaves the interpretation to a CCP official to define what it means.
Article 27	N/A	Individuals and organizations must not engage in illegal intrusion into the networks of other parties, disrupt the normal functioning of the networks of other parties, or steal network data or engage in other activities endangering cybersecurity; they must not provide programs, or tools specially used in network intrusions, that disrupt normal network functions and protection measures, steal network data, or engage in other acts endangering cybersecurity; and where they clearly are aware that others will engage in actions that endanger cybersecurity, they must not provide help such as technical support, advertisement and promotion, or payment of expenses.	Functional	intersects with	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.		
Article 28	N/A	Network operators shall provide technical support and assistance to public security organs and national security organs that are safeguarding national security and investigating criminal activities in accordance with the law.	Functional	intersects with	Forced Technology Transfer (FTT)	GOV-12	Mechanisms exist to avoid and/or constrain the forced exfiltration of sensitive / regulated information (e.g., Intellectual Property (IP)) to the host government for purposes of market access or market management practices.		Article 28 demands that organizations support investigations by the CCP, which could be intrusive of the organizations' network(s) and data.
Article 28	N/A	Network operators shall provide technical support and assistance to public security organs and national security organs that are safeguarding national security and investigating criminal activities in accordance with the law.	Functional	intersects with	State-Sponsored Espionage	GOV-13	Mechanisms exist to constrain the host government's ability to leverage the organization's technology assets for economic or political espionage and/or cyberwarfare activities.		Article 28 demands that organizations support investigations by the CCP, which could be intrusive of the organizations' network(s) and data.
Article 28	N/A	Network operators shall provide technical support and assistance to public security organs and national security organs that are safeguarding national security and investigating criminal activities in accordance with the law.	Functional	intersects with	Investigation Access Restrictions	CPL-05.2	Mechanisms exist to support official investigations by provisioning government investigators with "least privileges" and "least functionality" to ensure that government investigators only have access to the data and systems needed to perform the investigation.		Article 28 demands that organizations support investigations by the CCP, which could be intrusive of the organizations' network(s) and data.
Article 28	N/A	Network operators shall provide technical support and assistance to public security organs and national security organs that are safeguarding national security and investigating criminal activities in accordance with the law.	Functional	intersects with	Government Surveillance	CPL-06	Mechanisms exist to constrain the host government from having unrestricted and non-monitored access to the organization's systems, applications and services that could potentially violate other applicable statutory, regulatory and/or contractual obligations.		Article 28 demands that organizations support investigations by the CCP, which could be intrusive of the organizations' network(s) and data.
Article 29	N/A	The State supports cooperation between network operators in areas such as the gathering, analysis, reporting, and emergency handling of cybersecurity information, increasing the security safeguarding capacity of network operators. Relevant industrial organizations are to establish and complete mechanisms for standardization and coordination of cybersecurity for their industry, strengthen their analysis and assessment of cybersecurity, and periodically conduct risk warnings, support, and coordination for members in responding to cybersecurity risks.	Functional	intersects with	Government Surveillance	CPL-06	Mechanisms exist to constrain the host government from having unrestricted and non-monitored access to the organization's systems, applications and services that could potentially violate other applicable statutory, regulatory and/or contractual obligations.		Similar to Article 28, Article 29 demands that organizations support investigations by the CCP, which could be intrusive of the organizations' network(s) and data. Article 29 also contains nonsensical language, since it lacks any granular requirements or alignment with existing standards. This leaves the interpretation to a CCP official to define what it means.
Article 30	N/A	Information obtained by cybersecurity and informatization departments and relevant departments performing cybersecurity protection duties can only be used as necessary for the protection of cybersecurity, and must not be used in other ways.	Functional	no relationship	N/A	N/A	N/A		
Article 31	N/A	The State implements key protection on the basis of the cybersecurity multi-level protection system for public communication and information services, power, traffic, water resources, finance, public service, e-government, and other critical information infrastructure which—if destroyed, suffering a loss of function, or experiencing leakage of data—might seriously endanger national security, national welfare, the people's livelihood, or the public interest. The State Council will formulate the specific scope and security protection measures for critical information infrastructure. The State encourages operators of networks outside the [designated] critical information infrastructure systems to voluntarily participate in the critical information infrastructure protection system.	Functional	no relationship	N/A	N/A	N/A		
Article 32	N/A	In accordance with the duties and division of labor provided by the State Council, departments responsible for security protection work for critical information infrastructure are to separately compile and organize security implementation plans for their industry's or sector's critical information infrastructure, and to guide and supervise security protection efforts for critical information infrastructure operations.	Functional	no relationship	N/A	N/A	N/A		
Article 33	N/A	Those constructing critical information infrastructure shall ensure that it has the capability to support business stability and sustained operations, and ensure the synchronous planning, synchronous establishment, and synchronous application of security technical measures.	Functional	intersects with	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).		
Article 34	N/A	In addition to the provisions of Article 21 of this Law, critical information infrastructure operators shall also perform the following security protection duties:	Functional	intersects with	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.		
Article 34(1)	N/A	Set up specialized security management bodies and persons responsible for security management, and conduct security background checks on those responsible persons and personnel in critical positions;	Functional	intersects with	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.		
Article 34(2)	N/A	Periodically conduct cybersecurity education, technical training, and skills evaluations for employees;	Functional	intersects with	Cybersecurity & Data Privacy-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.		
Article 34(3)	N/A	Conduct disaster recovery backups of important systems and databases;	Functional	intersects with	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfying Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).		
Article 34(4)	N/A	Formulate emergency response plans for cybersecurity incidents, and periodically organize drills;	Functional	intersects with	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).		
Article 34(4)	N/A	Formulate emergency response plans for cybersecurity incidents, and periodically organize drills;	Functional	intersects with	Contingency Plan Testing & Exercises	BCD-04	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.		
Article 34(5)	N/A	Other duties provided by law or administrative regulations.	Functional	intersects with	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.		Article 34(5) is nonsensical language. There is nothing for an organization to comply with, since it lacks any granular requirements or alignment with existing standards. This leaves the interpretation to a CCP official to define what it means.
Article 35	N/A	Critical information infrastructure operators purchasing network products and services that might impact national security shall undergo a national security review organized by the State cybersecurity and informatization departments and relevant departments of the State Council.	Functional	intersects with	Assessments	IAO-02	Mechanisms exist to formally assess the cybersecurity & data privacy controls in systems, applications and services through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.		Article 35 is nonsensical language. There is nothing for an organization to comply with, since it lacks any granular requirements or alignment with existing standards. This leaves the interpretation to a CCP official to define what it means.
Article 36	N/A	Critical information infrastructure operators purchasing network products and services shall follow relevant provisions and sign a security and confidentiality agreement with the provider, clarifying duties and responsibilities for security and confidentiality.	Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.		

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
Article 37	N/A	Critical information infrastructure operators that gather or produce personal information or important data during operations within the mainland territory of the People’s Republic of China, shall store it within mainland China. Where due to business requirements it is truly necessary to provide it outside the mainland, they shall follow the measures jointly formulated by the State cybersecurity and informatization departments and the relevant departments of the State Council to conduct a security assessment; where laws and administrative regulations provide otherwise, follow those provisions.	Functional	intersects with	Data Localization	DCH-26	Mechanisms exist to constrain the impact of "digital sovereignty laws," that require localized data within the host country, where data and processes may be subjected to arbitrary enforcement actions that potentially violate other applicable statutory, regulatory and/or contractual obligations.		Article 37 pertains to "data localization" where data must reside within the geographic boundaries of mainland China.
Article 38	N/A	At least once a year, critical information infrastructure operators shall conduct an inspection and assessment of their networks’ security and risks that might exist, either on their own or through retaining a cybersecurity services organization; CII operators should submit a cybersecurity report on the circumstances of the inspection and assessment as well as improvement measures, to be sent to the relevant department responsible for critical information infrastructure security protection efforts.	Functional	intersects with	Independent Assessors	CPL-03.1	Mechanisms exist to utilize independent assessors to evaluate cybersecurity & data protection controls at planned intervals or when the system, service or project undergoes significant changes.		
Article 38	N/A	At least once a year, critical information infrastructure operators shall conduct an inspection and assessment of their networks’ security and risks that might exist, either on their own or through retaining a cybersecurity services organization; CII operators should submit a cybersecurity report on the circumstances of the inspection and assessment as well as improvement measures, to be sent to the relevant department responsible for critical information infrastructure security protection efforts.	Functional	intersects with	Cybersecurity & Data Privacy Status Reporting	GOV-17	Mechanisms exist to submit status reporting of the organization's cybersecurity and/or data privacy program to applicable statutory and/or regulatory authorities, as required.		
Article 39	N/A	State cybersecurity and informatization departments shall coordinate relevant departments in employing the following measures for critical information infrastructure security protection:	Functional	no relationship	N/A	N/A	N/A		
Article 39(1)	N/A	Conduct spot testing of critical information infrastructure security risks, put forward improvement measures, and when necessary they can retain a cybersecurity services organization to conduct testing and assessment of cybersecurity risks;	Functional	no relationship	N/A	N/A	N/A		Article 39(1) opens the door for state-sponsored espionage through "spot testing" of cybersecurity practices.
Article 39(2)	N/A	Periodically organize critical information infrastructure operators to conduct emergency cybersecurity response drills, increasing the level, coordination, and capacity of responses to cybersecurity incidents.	Functional	no relationship	N/A	N/A	N/A		
Article 39(3)	N/A	Promote cybersecurity information sharing among relevant departments, critical information infrastructure operators, and also relevant research institutions and cybersecurity services organizations.	Functional	no relationship	N/A	N/A	N/A		
Article 39(4)	N/A	Provide technical support and assistance for cybersecurity emergency management and recovery, etc.	Functional	intersects with					
Article 40	N/A	Network operators shall strictly maintain the confidentiality of user information they collect, and establish and complete user information protection systems.	Functional	intersects with	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.		
Article 40	N/A	Network operators shall strictly maintain the confidentiality of user information they collect, and establish and complete user information protection systems.	Functional	intersects with	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.		
Article 41	N/A	Network operators collecting and using personal information shall abide by the principles of legality, propriety, and necessity; they shall publish rules for collection and use, explicitly stating the purposes, means, and scope for collecting or using information, and obtain the consent of the persons whose data is gathered. Network operators must not gather personal information unrelated to the services they provide; must not violate the provisions of laws, administrative regulations or agreements between the parties to gather or use personal information; and shall follow the provisions of laws, administrative regulations, and agreements with users to process personal information they have stored.	Functional	intersects with	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.		
Article 41	N/A	Network operators collecting and using personal information shall abide by the principles of legality, propriety, and necessity; they shall publish rules for collection and use, explicitly stating the purposes, means, and scope for collecting or using information, and obtain the consent of the persons whose data is gathered. Network operators must not gather personal information unrelated to the services they provide; must not violate the provisions of laws, administrative regulations or agreements between the parties to gather or use personal information; and shall follow the provisions of laws, administrative regulations, and agreements with users to process personal information they have stored.	Functional	intersects with	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, updating and/or sharing Personal Data (PD) to: (1) The purpose(s) originally collected, consistent with the data privacy notice(s); (2) What is authorized by the data subject, or authorized agent; and (3) What is consistent with applicable laws, regulations and contractual obligations.		
Article 42	N/A	Network operators must not disclose, tamper with, or destroy personal information they gather; and, absent the consent of the person whose information was collected, must not provide personal information to others. However, this is the case with the exception that information can be provided if after processing there is no way to identify a specific individual, and the identity cannot be recovered. Network operators shall adopt technical measures and other necessary measures to ensure the security of personal information they gather and to prevent personal information from leaking, being destroyed, or lost. When the leak, destruction, or loss of personal information occurs, or might have occurred, remedial measures shall be immediately taken, and provisions followed to promptly inform users and to make a report to the competent departments in accordance with regulations.	Functional	intersects with	Security of Personal Data (PD)	PRI-01.6	Mechanisms exist to ensure Personal Data (PD) is protected by logical and physical security safeguards that are sufficient and appropriately scoped to protect the confidentiality and integrity of the PD.		
Article 43	N/A	Where individuals discover that network operators have violated the provisions of laws, administrative regulations, or agreements between the parties to gather or use their personal information, they have the right to demand the network operators delete their personal information; where discovering that personal information gathered or stored by network operators has errors, they have the right to demand the network operators make corrections. Network operators shall employ measures for deletions and corrections.	Functional	intersects with	Correcting Inaccurate Personal Data	PRI-06.1	Mechanisms exist to establish and implement a process for: (1) Data subjects to have inaccurate Personal Data (PD) maintained by the organization corrected or amended; and (2) Disseminating corrections or amendments of PD to other authorized users of the PD.		
Article 43	N/A	Where individuals discover that network operators have violated the provisions of laws, administrative regulations, or agreements between the parties to gather or use their personal information, they have the right to demand the network operators delete their personal information; where discovering that personal information gathered or stored by network operators has errors, they have the right to demand the network operators make corrections. Network operators shall employ measures for deletions and corrections.	Functional	intersects with	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to complaints, concerns or questions from authenticated data subjects about how the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes of their Personal Data (PD).		
Article 43	N/A	Where individuals discover that network operators have violated the provisions of laws, administrative regulations, or agreements between the parties to gather or use their personal information, they have the right to demand the network operators delete their personal information; where discovering that personal information gathered or stored by network operators has errors, they have the right to demand the network operators make corrections. Network operators shall employ measures for deletions and corrections.	Functional	intersects with	Right to Erasure	PRI-06.5	Mechanisms exist to maintain a process to erase a data subject's Personal Data (PD), in accordance with applicable laws, regulations and contractual obligations pertaining to the retention of their PD.		
Article 44	N/A	Individuals or organizations must not steal or use other illegal methods to acquire personal information, and must not unlawfully sell or unlawfully provide others with personal information.	Functional	intersects with	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, updating and/or sharing Personal Data (PD) to: (1) The purpose(s) originally collected, consistent with the data privacy notice(s); (2) What is authorized by the data subject, or authorized agent; and (3) What is consistent with applicable laws, regulations and contractual obligations.		
Article 45	N/A	Departments lawfully having cybersecurity supervision and management duties, and their staffs, must keep strictly confidential personal information, private information, and commercial secrets that they learn of in performing their duties, and they must not leak, sell, or unlawfully provide it to others.	Functional	no relationship	N/A	N/A	N/A		

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
Article 46	N/A	All individuals and organizations shall be responsible for their use of websites and must not establish websites or communications groups for use in perpetrating fraud, imparting criminal methods, the creation or sale of prohibited or controlled items, or other unlawful activities, and websites must not be exploited to publish information related to perpetrating fraud, the creation or sale of prohibited or controlled items, or other unlawful activities.	Functional	intersects with	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of products and/or services across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.		
Article 47	N/A	Network operators shall strengthen management of information published by users and, upon discovering information that the law or administrative regulations prohibits the publication or transmission of, they shall immediately stop transmission of that information, employ handling measures such as deleting the information, prevent the information from spreading, save relevant records, and report to the relevant competent departments.	Functional	intersects with	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.		Article 47 deals more with censorship that cybersecurity or data privacy. The CCP is requiring organizations to have a method to self-censor.
Article 48	N/A	Electronic information sent, or application software provided by any individual or organization, must not install malicious programs, and must not contain information that laws and administrative regulations prohibit the publication or transmission of. Electronic information distribution service providers, and application software download service providers, shall perform security management duties; where they know that their users have engaged in conduct provided for in the preceding paragraph, they shall: employ measures such as stopping provision of services and removal of information or malicious programs; store relevant records; and report to the relevant competent departments.	Functional	intersects with	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of products and/or services across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.		
Article 49	N/A	Network operators shall establish network information security complaint and reporting systems, publicly disclose information such as the methods for making complaints or reports, and promptly accept and handle complaints and reports relevant to network information security. Network operators shall cooperate with cybersecurity and informatization departments and relevant departments in conducting implementation of supervision and inspections in accordance with the law.	Functional	no relationship	N/A	N/A	N/A		Article 49 has nothing to do with cybersecurity or data privacy. It is a requirement to have a support line to intake customer complaints.
Article 50	N/A	State cybersecurity and informatization departments and relevant departments will perform network information security supervision and management responsibilities in accordance with law; and where they discover the publication or transmission of information which is prohibited by laws or administrative regulations, shall request that network operators stop transmission, employ disposition measures such as deletion, and store relevant records; for information described above that comes from outside the mainland People's Republic of China, they shall notify the relevant organization to adopt technical measures and other necessary measures to block transmission.	Functional	intersects with					Article 50 authorizes the CCP to supervise cybersecurity activities, which could lead to state-sponsored espionage under the banner of "information security supervision" activities.
Article 51	N/A	The State will establish a cybersecurity monitoring, early warning, and information communication system. The State cybersecurity and informatization departments shall do overall coordination of relevant departments to strengthen collection, analysis, and reporting efforts for cybersecurity information, and follow regulations for the unified release of cybersecurity monitoring and early warning information.	Functional	no relationship	N/A	N/A	N/A		
Article 52	N/A	Departments responsible for critical information infrastructure security protection efforts shall establish and complete cybersecurity monitoring, early warning, and information reporting systems for their respective industry or sector, and report cybersecurity monitoring and early warning information in accordance with regulations.	Functional	no relationship	N/A	N/A	N/A		
Article 53	N/A	State cybersecurity and informatization departments will coordinate with relevant departments to establish and complete mechanisms for cybersecurity risk assessment and emergency response efforts, formulate cybersecurity incident emergency response plans, and periodically organize drills. Departments responsible for critical information infrastructure security protection efforts shall formulate cybersecurity incident emergency response plans for their respective industry or sector, and periodically organize drills. Cybersecurity incident emergency response plans shall rank cybersecurity incidents on the basis of factors such as the degree of damage after the incident occurs and the scope of impact, and provide corresponding emergency response handling measures.	Functional	no relationship	N/A	N/A	N/A		
Article 54	N/A	When the risk of cybersecurity incidents increases, the relevant departments of people's governments at the provincial level and above shall follow the scope of authority and procedures provided, and employ the following measures on the basis of the characteristics of the cybersecurity risk and the damage it might cause:	Functional	intersects with	N/A	N/A	N/A		
Article 54(1)	N/A	Require that relevant departments, institutions, and personnel promptly gather and report relevant information, and strengthen monitoring of the occurrence of cybersecurity risks;	Functional	intersects with					
Article 54(2)	N/A	Organize relevant departments, institutions, and specialist personnel to conduct analysis and assessment of information on the cybersecurity risk, and predict the likelihood of incident occurrence, the scope of impact, and the level of damage;	Functional	no relationship	N/A	N/A	N/A		
Article 54(3)	N/A	Issue cybersecurity risk warnings to the public, and publish measures for avoiding or reducing damage.	Functional	no relationship	N/A	N/A	N/A		
Article 55	N/A	When a cybersecurity incident occurs, the cybersecurity incident emergency response plan shall be immediately initiated, an evaluation and assessment of the cybersecurity incident shall be conducted, network operators shall be requested to adopt technical and other necessary measures, potential security risks shall be removed, the threat shall be prevented from expanding, and warnings relevant to the public shall be promptly published.	Functional	intersects with	Investigation Access Restrictions	CPL-05.2	Mechanisms exist to support official investigations by provisioning government investigators with "least privileges" and "least functionality" to ensure that government investigators only have access to the data and systems needed to perform the investigation.		Article 28 demands that organizations support investigations by the CCP, which could be intrusive of the organizations' network(s) and data.
Article 56	N/A	Where, while performing cybersecurity supervision and management duties, relevant departments of people's governments at the provincial level or above discover that networks have a relatively large security risk or the occurrence of a security incident, they may call in the legal representative or responsible party for the operator of that network to conduct interviews in accordance with the scope of authority and procedures provided. Network operators shall follow requirements to employ procedures, make corrections, and eliminate hidden dangers.	Functional	intersects with	Investigation Access Restrictions	CPL-05.2	Mechanisms exist to support official investigations by provisioning government investigators with "least privileges" and "least functionality" to ensure that government investigators only have access to the data and systems needed to perform the investigation.		Article 28 demands that organizations support investigations by the CCP, which could be intrusive of the organizations' network(s) and data.
Article 57	N/A	Where sudden emergencies or production security accidents occur as a result of cybersecurity incidents, they shall be handled in accordance with the provisions the "Emergency Response Law of the People's Republic of China," the "Production Safety Law of the People's Republic of China," and other relevant laws and administrative regulations.	Functional	no relationship	N/A	N/A	N/A		
Article 58	N/A	To fulfill the need to protect national security and the social public order, and to respond to the requirements of major security incidents within the society, it is possible, as stipulated or approved by the State Council, to take temporary measures regarding network communications in a specially designated region, such as limiting such communications.	Functional	no relationship	N/A	N/A	N/A		

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
Article 59	N/A	Where network operators do not perform cybersecurity protection duties provided for in Articles 21 and 25 of this Law, the competent departments will order corrections and give warnings; where corrections are refused or it leads to harm to cybersecurity or other such consequences, a fine of between RMB 10,000 and 100,000 shall be levied; and the directly responsible management personnel shall be fined between RMB 5,000 and 50,000. Where critical information infrastructure operators do not perform cybersecurity protection duties as provided for in Articles 33, 34, 36, and 38 of this Law, the competent departments will order corrections and give warnings; where corrections are refused or it leads to harm to cybersecurity or other such consequences, a fine of between RMB 100,000 and 1,000,000 shall be levied; and the directly responsible management personnel shall be fined between RMB 10,000 and 100,000.	Functional	no relationship	N/A	N/A	N/A		
Article 60	N/A	Where Article 22 Paragraphs 1 or 2 or Article 48 Paragraph 1 of this Law are violated by any of the following conduct, the relevant competent departments shall order corrections and give warnings; where corrections are refused or it causes harm to cybersecurity or other consequences, a fine of between RMB 50,000 and 500,000 shall be levied; and the persons who are directly in charge shall be fined between RMB 10,000 and 100,000:	Functional	no relationship	N/A	N/A	N/A		
Article 60(1)	N/A	Installing malicious programs;	Functional	no relationship	N/A	N/A	N/A		
Article 60(2)	N/A	Failure to immediately take remedial measures for security flaws or vulnerabilities that exist in products or services, or not informing users and reporting to the competent departments in accordance with regulations;	Functional	no relationship	N/A	N/A	N/A		
Article 60(3)	N/A	Unauthorized ending of the provision of security maintenance for their products or services.	Functional	no relationship	N/A	N/A	N/A		
Article 61	N/A	Network operators violating Article 24 Paragraph 1 of this Law in failing to require users to provide real identity information or providing relevant services to users who do not provide real identity information, are ordered to make corrections by the relevant competent department; where corrections are refused or the circumstances are serious, a fine of between RMB 50,000 and 500,000 shall be levied, and the relevant competent department may order a temporary suspension of operations, a suspension of business for corrections, closing down of websites, cancellation of relevant operations permits, or cancellation of business licenses; persons who are directly in charge and other directly responsible personnel shall be fined between RMB 10,000 and 100,000.	Functional	no relationship	N/A	N/A	N/A		
Article 62	N/A	Where Article 26 of this Law is violated in carrying out cybersecurity certifications, testing, or risk assessments, or publishing cybersecurity information such as system vulnerabilities, computer viruses, cyber attacks, or network incursions, corrections are to be ordered and a warning given; where corrections are refused or the circumstances are serious, a fine of between RMB 10,000 and 100,000 shall be imposed, and the relevant competent department may order a temporary suspension of operations, a suspension of business for corrections, closing down of websites, cancellation of relevant operations permits, or cancellation of business licenses; persons who are directly in charge and other directly responsible personnel shall be fined between RMB 5,000 and 50,000.	Functional	no relationship	N/A	N/A	N/A		
Article 63	N/A	Where Article 27 of this Law is violated in engaging in activities harming cybersecurity, or by providing specialized software or tools used in engaging in activities harming cybersecurity, or by providing others engaging in activities harming cybersecurity with assistance such as technical support, advertising and promotions, or payment of expenses, and where this does not constitute a crime, public security organizations shall confiscate unlawful gains and impose up to 5 days detention, and may levy a fine of between RMB 50,000 and 500,000; and where circumstances are serious, shall impose between 5 and 15 days detention, and may levy a fine of between 100,000 and 1,000,000 RMB. Where units have engaged in the conduct of the preceding paragraph, public security organizations shall confiscate unlawful gains and levy a fine of between RMB 100,000 and 1,000,000, and the directly responsible persons in charge and other directly responsible personnel shall be fined in accordance with the preceding paragraph. Where Article 27 of this Law is violated, persons who receive public security administrative sanctions must not engage in cybersecurity management or key network operations positions for 5 years; those receiving criminal punishments will be subject to a lifetime ban on engaging in work in cybersecurity management and key network operations positions.	Functional	no relationship	N/A	N/A	N/A		
Article 64	N/A	Network operators, and network product or service providers violating Article 22 Paragraph 3 or Articles 41-43 of this Law by infringing on personal information that is protected in accordance with law, shall be ordered to make corrections by the relevant competent department and may, either independently or concurrently, be given warnings, be subject to confiscation of unlawful gains, and/or be fined between 1 to 10 times the amount of unlawful gains; where there are no unlawful gains, the fine shall be up to RMB 1,000,000, and a fine of between RMB 10,000 and 100,000 shall be given to persons who are directly in charge and other directly responsible personnel; where the circumstances are serious, the relevant competent department may order a temporary suspension of operations, a suspension of business for corrections, closing down of websites, cancellation of relevant operations permits, or cancellation of business licenses. Where Article 44 of this Law is violated in stealing or using other illegal means to obtain, illegally sell, or illegally provide others with personal information, and this does not constitute a crime, public security organizations shall confiscate unlawful gains and levy a fine of between 1 and 10 times the amount of unlawful gains, and where there are no unlawful gains, levy a fine of up to RMB 1,000,000.	Functional	no relationship	N/A	N/A	N/A		
Article 65	N/A	Where critical information infrastructure operators violate Article 35 of this Law by using network products or services that have not had security inspections or did not pass security inspections, the relevant competent department shall order the usage to stop and levy a fine in the amount of 1 to 10 times the purchase price; the persons who are directly in charge and other directly responsible personnel shall be fined between RMB 10,000 and 100,000.	Functional	no relationship	N/A	N/A	N/A		
Article 66	N/A	Where critical information infrastructure operators violate Article 37 of this Law by storing network data outside the mainland territory, or provide network data to those outside of the mainland territory, the relevant competent department: shall order corrective measures, provide warning, confiscate unlawful gains, and levy fines between RMB 50,000 and 500,000; and may order a temporary suspension of operations, a suspension of business for corrective measures, closing down of websites, revocation of relevant operations permits, or cancellation of business licenses. Persons who are directly in charge and other directly responsible personnel shall be fined between RMB 10,000 and 100,000.	Functional	no relationship	N/A	N/A	N/A		

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
Article 67	N/A	Where Article 46 of this Law is violated by establishing a website or communications group used for the commission of illegal or criminal activities, or the network is used to publish information related to the commission of illegal or criminal activities, but a crime has not been committed, public security organizations shall impose up to 5 days detention and may levy a fine of between RMB 10,000 and 15,000; and where circumstances are serious, they may impose between 5 and 15 days detention, and may give a fine of between 50,000 and 500,000 RMB. They may also close websites and communications groups used for illegal or criminal activities. Where units have engaged in conduct covered by the preceding paragraph, a fine of between RMB 100,000 and 500,000 shall be levied by public security organizations, and the principal responsible managers and other directly responsible personnel shall be fined in accordance with the preceding paragraph.	Functional	no relationship	N/A	N/A	N/A		
Article 68	N/A	Where network operators violate Article 47 of this Law by failing to stop the transmission of information for which transmission and publication are prohibited by laws or administrative regulations, failing to employ disposition measures such as deletion or failing to preserve relevant records, the relevant competent department shall order correction, provide warning, and confiscate unlawful gains; where correction is refused or circumstances are serious, fines between RMB 100,000 and 500,000 shall be imposed, and a temporary suspension of operations, a suspension of business to conduct correction, closing down of websites, cancellation of relevant operations permits, or cancellation of business licenses may be ordered; and persons who are directly in charge and other directly responsible personnel are fined between RMB 10,000 and 100,000. Where electronic information service providers and application software download service providers do not perform their security management duties provided for in Paragraph 2 of Article 48 of this Law, punishment shall be in accordance with the provisions of the preceding paragraph.	Functional	intersects with	N/A	N/A	N/A		
Article 69	N/A	Network operators violating the provisions of this Law, who exhibit any of the following conduct, will be ordered to make corrections by the relevant competent departments; where corrections are refused or the circumstances are serious, a fine of between RMB 50,000 and 500,000 shall be imposed, and directly responsible management personnel and other directly responsible personnel are to be fined between RMB 10,000 and 100,000:	Functional	intersects with	N/A	N/A	N/A		
Article 69(1)	N/A	Not following the requirements of relevant departments to adopt disposition measures such as stopping dissemination or deleting information for which laws or administrative regulations prohibit publication or dissemination;	Functional	intersects with	N/A	N/A	N/A		
Article 69(2)	N/A	Refusal or obstruction of the competent departments in their lawful supervision and inspection;	Functional	intersects with	N/A	N/A	N/A		
Article 69(3)	N/A	Refusing to provide technical support and assistance to public security organs and state security organs.	Functional	intersects with	N/A	N/A	N/A		
Article 70	N/A	Publication or transmission of information prohibited by Article 12 Paragraph 2 of this Law or other laws or administrative regulations shall be punished in accordance with the provisions of the relevant laws and administrative regulations.	Functional	no relationship	N/A	N/A	N/A		
Article 71	N/A	When there is conduct violating the provisions of this Law, it shall be recorded in credit files and made public in accordance with relevant laws and administrative regulations.	Functional	no relationship	N/A	N/A	N/A		
Article 72	N/A	Where state organization government affairs network operators do not perform cybersecurity protection duties as provided by this Law, the organization at the level above or relevant organizations will order corrections; sanctions will be levied on the directly responsible managers and other directly responsible personnel.	Functional	intersects with	Legal Assessment of Investigative Inquires	CPL-05	Mechanisms exist to determine whether a government agency has an applicable and valid legal basis to request data from the organization and what further steps need to be taken, if necessary.		Article 72 enables the CCP to require corrective actions to be implemented. Non-compliance should be considered if there is any potential risk to the organization's systems, data, personnel or clients.
Article 73	N/A	Where cybersecurity and informatization and other relevant departments violate the provisions of Article 30 of this Law by using personal information acquired while performing cybersecurity protection duties for other purposes, the directly responsible persons in charge and other directly responsible personnel shall be given sanctions. Where cybersecurity and informatization departments and other relevant departments' personnel neglect their duties, abuse their authority, show favoritism, and it does not constitute a crime, sanctions will be imposed in accordance with law.	Functional	intersects with	N/A	N/A	N/A		
Article 74	N/A	Where violations of the provisions of this Law cause harm to others, civil liability is borne in accordance with law. Where provisions of this Law are violated, constituting a violation of public order management, public order administrative sanctions will be imposed in accordance with law; where a crime is constituted, criminal responsibility will be pursued in accordance with law.	Functional	intersects with	N/A	N/A	N/A		
Article 75	N/A	Where foreign institutions, organizations, or individuals engage in attacks, intrusions, interference, damage, or other activities the endanger the critical information infrastructure of the People's Republic of China, and cause serious consequences, legal responsibility is to be pursued in accordance with the law; public security departments under the State Council and relevant departments may also decide to freeze institutional, organization, or individual assets or take other necessary punitive measures.	Functional	intersects with	N/A	N/A	N/A		