POINT OF VIEW - SEPTEMBER 2026

China: From Regulatory Obligation to Board-Ready Evidence.

Connected controls for banking, securities, cybersecurity and personal data

China's framework combines central-bank and financial-supervision requirements with securities governance, national cybersecurity duties and personal-information protection. Enterprises need documented risk tolerances, internal controls, independent assurance, incident response and accountable remediation across this perimeter.

REGION
APAC

REGULATORY HUB
CHN

China

Country in Brief

4	6	4	3
Regulatory authorities profiled	Official regulatory sources mapped	Supervisory priorities operationalised	Connected TransVare platforms

01 China Regulatory Landscape

China's framework combines central-bank and financial-supervision requirements with securities governance, national cybersecurity duties and personal-information protection. Enterprises need documented risk tolerances, internal controls, independent assurance, incident response and accountable remediation across this perimeter.

PBOC

People's Bank of China

Industries Regulated

Banking and lending

NFRA

National Financial Regulatory Administration

Industries Regulated

Banking and lending, Insurance

CSRC

China Securities Regulatory Commission

Industries Regulated

Capital markets and listed companies

CAC

Cyberspace Administration of China

Industries Regulated

Government and critical infrastructure

02 Supervisory Priorities

The applicable perimeter depends on entity type, licence and sector. These priorities provide a practical starting point for programme design and evidence management.

01	Risk tolerance and board oversight
02	Internal-control evaluation
03	Cyber incident response
04	Personal-information governance

03 From Obligation to Board-Ready Evidence

Use one traceable workflow to translate requirements, manage execution and demonstrate oversight.

01

Catalogue Obligations

Structure local requirements by entity, licence, authority and accountable owner.

02

Connect Operational Evidence

Link obligations to risks, controls, incidents, tests, findings and remediation.

03

Monitor and Assure

Track KRIs, control status, audit coverage, incidents and action closure continuously.

04

Report to Leadership

Turn current operational evidence into traceable executive and board oversight.

04 China Regulation and Product Map

Each official requirement below is translated into an operational GRC focus. Only platforms with a defensible workflow or evidence role are shown as a primary or supporting fit.

Guidelines for Internal Control of Commercial Banks

PBOC and banking supervisor

Applies To	Commercial banks operating in China
Operational Focus	Board-approved risk tolerance, control responsibilities, internal-control evaluation, internal audit, emergency arrangements and tracked correction of deficiencies.
ERMCare® **Primary Fit**	Risk and control registers, assessments, appetite or limits, KRIs, treatments, approvals and board reporting.
AuditCare® **Primary Fit**	Audit universe, risk-based planning, RCM-linked testing, working papers, evidence, findings and follow-up.
Scope Boundary	Workflow and evidence support only. Applicability and legal interpretation remain with the organisation and its advisers.
Official Source	**Open Official Source**

Commercial Bank Law and Banking Supervision Framework

PBOC and NFRA

Applies To	Commercial banks and supervised banking institutions
Operational Focus	Prudent operations, governance, risk controls, supervisory reporting, examination evidence and corrective measures.
ERMCare® **Primary Fit**	Risk and control registers, assessments, appetite or limits, KRIs, treatments, approvals and board reporting.
AuditCare® **Supporting Fit**	Risk-based assurance, control design and effectiveness testing, evidence, findings and action follow-up.
Scope Boundary	Notification workflow and evidence can be configured. Submission to an authority requires an approved process or integration.
Official Source	**Open Official Source**

Guidelines for Governance of Listed Companies
CSRC

Applies To	Companies listed on Chinese securities markets
Operational Focus	Board and committee accountability, internal controls, risk oversight, disclosure, audit supervision and follow-up of governance issues.
ERMVare® **Primary Fit**	Risk and control registers, assessments, appetite or limits, KRIs, treatments, approvals and board reporting.
AuditVare® **Supporting Fit**	Risk-based assurance, control design and effectiveness testing, evidence, findings and action follow-up.
Scope Boundary	Notification workflow and evidence can be configured. Submission to an authority requires an approved process or integration.
Official Source	**Open Official Source**

Cybersecurity Law
CAC

Applies To	Network operators and critical information infrastructure operators within scope
Operational Focus	Security governance, risk controls, monitoring, incident plans, response, reporting and supply-chain oversight.
ERMVare® **Primary Fit**	Risk and control registers, assessments, appetite or limits, KRIs, treatments, approvals and board reporting.
InciVare® **Primary Fit**	Cyber-event intake, escalation, investigation, root cause, corrective action, recovery tracking and audit trail.
Scope Boundary	GRC workflow and evidence support only. The platforms do not replace technical security monitoring, detection or protection tools.
Official Source	**Open Official Source**

Rules on Data Security of Banking and Insurance Institutions

NFRA

Applies To	Banking and insurance institutions within the Rules' scope
Operational Focus	Data-security governance, classification, risk assessment, access controls, third-party data risk, security incidents, audit and supervisory reporting.
ERMVare® **Primary Fit**	Third-party risks, controls, assessments, treatments, approvals, KRIs and oversight reporting.
InciVare® **Primary Fit**	Incident reporting, triage, investigation, root cause, corrective action, escalation and closure.
Scope Boundary	Notification workflow and evidence can be configured. Submission to an authority requires an approved process or integration.
Official Source	**Open Official Source**

Personal Information Protection Law

CAC

Applies To	Personal-information handlers within the Law's scope
Operational Focus	Processing records, impact assessment, security controls, processor governance, breach response and corrective action.
InciVare® **Primary Fit**	Incident intake, assessment, investigation, notification workflow, corrective action, escalation and closure evidence.
AuditVare® **Supporting Fit**	Risk-based assurance, control design and effectiveness testing, evidence, findings and action follow-up.
Scope Boundary	Workflow and evidence support only. Applicability and legal interpretation remain with the organisation and its advisers.
Official Source	**Open Official Source**

Research Review	Primary Fit	Supporting Fit	Not Shown
Official-source and product-fit review completed 1 September 2026.	Directly manages a central process or evidence set.	Contributes linked evidence, oversight or follow-up.	Weak or unsubstantiated relationships are omitted.

05 Brochure-Validated Product Capability

The mapping uses capabilities documented in the current TransVare solution briefs. It does not extend the platforms beyond their stated functional scope.

ERMVare®

Risk and Control Intelligence

Enterprise risk ownership, risk and control registers, assessments, appetite and tolerances, KRIs, treatments, approvals, dashboards and board reporting.

Central risk and control register | KRI threshold alerts | Treatment action tracking | AI-assisted drafting and classification

AuditVare®

Independent Assurance

Audit universe, risk-based planning, engagement execution, RCM-linked control testing, evidence, findings, approvals and follow-up.

Risk-based audit planning | ToD and ToE procedures | Working papers and evidence | GIAS 2024 observation drafting

InciVare®

Incident Response and Closure

Incident intake, triage, investigation, root-cause analysis, escalation, notifications, corrective action, closure and lessons learned.

Central incident register | Investigation and root cause | Escalation and notifications | Corrective-action tracking

Scope Boundary

The platforms support governance workflows, accountability, evidence and reporting. They do not calculate regulatory capital or liquidity, replace technical cybersecurity monitoring, provide legal interpretation, issue external-audit opinions or automatically file statutory notifications unless an approved integration and process are configured.

06 Sources, Scope and Next Step

Official sources used in this report are linked directly from each regulation summary. The mapping is an implementation aid and not legal advice.

01	**Guidelines for Internal Control of Commercial Banks** PBOC and banking supervisor	**Official Source**
02	**Commercial Bank Law and Banking Supervision Framework** PBOC and NFRA	**Official Source**
03	**Guidelines for Governance of Listed Companies** CSRC	**Official Source**
04	**Cybersecurity Law** CAC	**Official Source**
05	**Rules on Data Security of Banking and Insurance Institutions** NFRA	**Official Source**
06	**Personal Information Protection Law** CAC	**Official Source**

THE NEXT STEP

Build a Connected GRC Operating Model for China.

See how TransVare can support local regulatory readiness while preserving regional visibility and board oversight.

TransVare US: Delaware
8 The Green, Street R
Dover, Kent 19901, State of Delaware
United States of America

For Local Alliance Partner and Sales Contact:
Connect@TransVare.com
TransVare.com