Nuova legge sulla cybersicurezza: armonizzazione e adeguamento delle responsabilità

Il 28 ottobre 2025, la 18ª Sessione del Comitato Permanente della 14ª Assemblea Nazionale del Popolo ha approvato la Decisione del Comitato Permanente dell'Assemblea Nazionale del Popolo sull'emendamento della Legge sulla cybersicurezza della Repubblica Popolare Cinese.
L'emendamento comprende 14 disposizioni e mira a chiarire il ruolo della cybersicurezza nel più ampio contesto della sicurezza nazionale, a includere nuove tecnologie come l'intelligenza artificiale nell'ambito regolatorio e a rafforzare il sistema di responsabilità giuridica.

La nuova legge entrerà in vigore il 1° gennaio 2026, segnando una nuova fase di governance della cybersicurezza in Cina, più sistematica e precisa. Il presente articolo illustra i principali emendamenti e fornisce indicazioni pratiche per le imprese straniere operanti in Cina.

I. Panoramica delle modifiche e valutazione complessiva dell'impatto

Questo emendamento rappresenta la prima revisione sostanziale della Legge sulla cybersicurezza dalla sua entrata in vigore nel 2017 e intende rispondere alle nuove sfide in materia di sicurezza derivanti dal rapido sviluppo delle tecnologie digitali.

Gli articoli modificati sono distribuiti principalmente nei capitoli relativi alle Disposizioni generali, al Supporto e alla promozione della cybersicurezza, alla Sicurezza delle operazioni di rete, alla Sicurezza delle informazioni di rete e alla Responsabilità giuridica. In particolare, ben dieci modifiche riguardano la sezione sulla responsabilità giuridica, evidenziando la chiara intenzione del legislatore di rafforzare l'efficacia regolatoria attraverso un inasprimento delle conseguenze legali.

Per le imprese straniere operanti in Cina, l'emendamento non introduce obblighi completamente nuovi, ma rappresenta un approfondimento, una precisazione e un rafforzamento del quadro normativo esistente. I suoi effetti principali risiedono in: una maggiore operatività e prevedibilità delle norme giuridiche, una più chiara articolazione e specificità dei requisiti di compliance e un aumento significativo della certezza e della gravità dei costi derivanti dalle violazioni. Comprendere tali cambiamenti consente alle

imprese di trasformare la pressione della compliance in un'opportunità per migliorare la governance e rafforzare le capacità di gestione del rischio.

II. Inclusione dell'intelligenza artificiale nell'ambito di regolamentazione

La nuova Legge sulla cybersicurezza introduce l'Articolo 20, che stabilisce: "*Lo Stato sostiene la ricerca e lo sviluppo delle teorie di base e delle tecnologie chiave, quali gli algoritmi dell'intelligenza artificiale, promuove la costruzione di infrastrutture come le risorse di dati di addestramento e la capacità di calcolo, migliora le norme etiche per l'intelligenza artificiale, rafforza il monitoraggio e la valutazione dei rischi e la supervisione della sicurezza, e promuove l'applicazione e lo sviluppo sano dell'intelligenza artificiale. Lo Stato sostiene l'innovazione nei metodi di gestione della sicurezza delle reti, utilizza nuove tecnologie come l'intelligenza artificiale e innalza il livello di protezione della sicurezza delle reti*."

Questa disposizione, per la prima volta a livello legislativo, definisce esplicitamente l'intelligenza artificiale come una componente importante dell'infrastruttura digitale (inclusi algoritmi, risorse di dati di addestramento e capacità di calcolo) e stabilisce un orientamento regolatorio in cui "incoraggiamento all'innovazione" e "sviluppo regolamentato" procedono in parallelo.
Per le imprese che sviluppano o applicano tecnologie di IA, ciò implica integrare la compliance lungo l'intero ciclo di vita del prodotto e istituire meccanismi di controllo interno, in particolare in relazione a trasparenza degli algoritmi, governance dei dati, valutazione etica e monitoraggio continuo dei rischi.

III. Aumento significativo della gravità delle sanzioni

L'Articolo 61 modificato integra e aggiorna i precedenti articoli 59 e 60, prevedendo quattro livelli di sanzioni in base alle conseguenze delle violazioni:

- per violazioni generali, ammenda da 10.000 a 50.000 RMB;
- in caso di rifiuto di apportare correzioni o qualora siano arrecati danni, ammenda da 50.000 a 500.000 RMB, e ammenda da 10.000 a 100.000 RMB per i soggetti direttamente responsabili;
- in caso di danni gravi, ammenda da 500.000 a 2 milioni di RMB, ammenda da 50.000 a 200.000 RMB per le persone fisiche responsabili, nonché possibile sospensione dell'attività, sospensione per rettifica o revoca di licenze o permessi;
- in caso di danni particolarmente gravi, ammenda da 2 a 10 milioni di RMB, ammenda da 200.000 a 1 milione di RMB per le persone fisiche responsabili, e applicazione di misure quali la sospensione dell'attività o la revoca di certificati o licenze.

L'articolo modificato innalza in modo significativo i limiti massimi delle sanzioni per condotte quali l'inadempimento degli obblighi di protezione della sicurezza da parte

degli operatori di rete e le violazioni da parte degli operatori di infrastrutture informative critiche, introducendo un meccanismo sanzionatorio graduato in funzione della gravità delle conseguenze. Tale struttura delimita i confini della responsabilità in modo particolarmente chiaro.

IV. Maggiore armonizzazione delle norme

Un altro aspetto rilevante delle modifiche è il rafforzamento sistematico della responsabilità, ottenuto attraverso una più chiara integrazione e connessione tra diverse normative, creando un sistema di responsabilità più rigoroso.

Il nuovo comma aggiunto all'Articolo 42 stabilisce che:
"*Quando gli operatori di rete trattano dati personali, devono rispettare la presente legge e le disposizioni del Codice Civile della Repubblica Popolare Cinese, della Legge sulla protezione delle informazioni personali della Repubblica Popolare Cinese e di altre leggi e regolamenti amministrativi*."
Ciò chiarisce i requisiti di coordinamento tra le varie leggi in materia di trattamento dei dati personali e garantisce la coerenza nella tutela dei diritti relativi alle informazioni personali. Le imprese sono quindi tenute a implementare una gestione integrata della compliance, assicurando che ogni attività di trattamento dei dati soddisfi molteplici standard giuridici.

In linea con l'obiettivo di unificare la tutela dei diritti sulle informazioni personali, la Legge sulla cybersicurezza modificata ha inoltre accorpato i precedenti Articoli 64, 66 e 70 nel nuovo Articolo 71, il cui secondo comma prevede che "*in caso di violazione dei diritti sulle informazioni personali, il trattamento e le sanzioni saranno effettuati conformemente alle leggi e ai regolamenti amministrativi pertinenti*", creando un'armonizzazione con le disposizioni sanzionatorie contenute nella Legge sulla protezione delle informazioni personali ed evitando zone grigie nell'applicazione della legge.

V. Responsabilità più dettagliate per gli operatori di infrastrutture critiche

Il nuovo Articolo 67 modifica il precedente articolo 65 stabilendo che: *Qualora un operatore di infrastrutture informatiche critiche utilizzi prodotti o servizi di rete che non sono stati sottoposti a revisione di sicurezza o che non hanno superato tale revisione, le autorità competenti ordinano la cessazione dell'uso e infliggono un'ammenda compresa tra una e dieci volte l'importo dell'appalto, mentre alle persone direttamente responsabili viene inflitta un'ammenda compresa tra 10.000 e 100.000 RMB*.

Questo emendamento collega l'ammontare delle sanzioni al valore dell'approvvigionamento, allineando la responsabilità alla dimensione dell'attività economica. Ciò implica che le imprese — in particolare quelle che potrebbero essere qualificate come operatori di infrastrutture informatiche critiche — debbano

considerare la revisione della sicurezza informatica come una componente centrale della gestione della supply chain nell'acquisto di apparecchiature o servizi di rete fondamentali. Nella selezione dei fornitori (in particolare dei fornitori di servizi cloud), le capacità di sicurezza e compliance dovrebbero costituire criteri di valutazione essenziali, con una chiara definizione delle responsabilità nei contratti.

Conclusioni

Nel complesso, gli emendamenti alla Legge sulla cybersicurezza promuovono la governance della cybersicurezza in Cina verso una fase più matura e raffinata, attraverso un rafforzamento della posizione strategica, l'inclusione della regolamentazione delle nuove tecnologie e l'inasprimento delle responsabilità: enfatizzando la sicurezza senza rinunciare allo sviluppo, chiarendo le responsabilità e, al contempo, prevedendo meccanismi di flessibilità.

Per le imprese straniere operanti in Cina, questo emendamento rappresenta più una chiarificazione del quadro giuridico che un irrigidimento della normativa, contribuendo alla creazione di un contesto imprenditoriale con regole più chiare e un'applicazione del diritto più prevedibile. Le imprese dovranno mantenere solide capacità di governance delle reti e dei dati, monitorare costantemente l'evoluzione delle politiche e garantire uno sviluppo sostenibile, stabile e di lungo periodo delle proprie attività in Cina.

New Cybersecurity Law: Coordination and Upgrading of Liabilities

On October 28, 2025, the 18th Session of the Standing Committee of the 14th National People's Congress approved the Decision of the Standing Committee of the National People's Congress on Amending the Cybersecurity Law of the People's Republic of China. This amendment includes 14 provisions and aims to clarify cybersecurity's role within the broader context of national security, incorporate new technologies like artificial intelligence into the regulatory scope, and enhance the legal liability system.

The new law takes effect on January 1, 2026, signaling a new phase of more systematic and precise cybersecurity governance in China. This article **outlines** the key amendments and provides **practical guidance** for foreign companies operating in China.

I. Overview of the Amendments and Overall Impact Assessment

This amendment is the first major revision of the Cybersecurity Law since its implementation in 2017, aiming to address new security challenges arising from the rapid development of digital technologies.

The amended contents are mainly distributed across the chapters of General Provisions, Cybersecurity Support and Promotion, Cyber Operation Security, Cyber Information Security, and Legal Liability, among which the amendments to the "Legal Liability" section amount to as many as ten, highlighting the clear intention of the legislators to enhance regulatory effectiveness by strengthening legal consequences. For foreign enterprises operating in China, this amendment does not create entirely new obligations but represents a deepening, refinement, and strengthening based on the existing regulatory framework. Its core impacts lie in: enhanced operability and predictability of legal rules, clearer layering and specificity of compliance requirements, and significantly increased certainty and severity of the costs of violations. Understanding these changes helps enterprises turn compliance pressure into an opportunity to improve governance and enhance risk management capabilities.

II. Inclusion of Artificial Intelligence within the Scope of Regulation

The new Cybersecurity Law adds Article 20, which provides: "*The state supports the research and development of basic theories and key technologies such as algorithms*

for artificial intelligence, promotes the construction of infrastructure such as training data resources and computing power, improves ethical norms for artificial intelligence, strengthens risk monitoring and assessment, and security supervision, and promotes the application and healthy development of artificial intelligence. The state supports innovation in network security management methods, uses new technologies such as artificial intelligence, and enhances the level of network security protection."

This provision, for the first time at the legal level, explicitly defines artificial intelligence as an important component of digital infrastructure (including algorithms, training data resources, and computing power) and establishes a regulatory tone in which "encouraging innovation" and "regulated development" proceed in parallel. For enterprises that develop or apply AI technologies, this means embedding compliance design throughout the entire product lifecycle and establishing internal control mechanisms, particularly regarding algorithm transparency, data governance, ethical review, and continuous risk monitoring.

III. Significant Increase in Penalty Severity

Revised Article 61 integrates and upgrades former Articles 59 and 60 and sets out four levels of penalties based on the consequences of violations:

- For general violations, a fine of between RMB 10,000 and RMB 50,000 shall be imposed;
- For refusal to make corrections or where harmful consequences are caused, a fine between RMB 50,000 and RMB 500,000 shall be imposed, and the directly responsible persons shall be fined between RMB 10,000 and RMB 100,000;
- Where serious harm is caused, a fine between RMB 500,000 and RMB 2 million shall be imposed, individuals shall be fined between RMB 50,000 and RMB 200,000, and suspension of relevant business, suspension for rectification, or revocation of permits or business licenses may also be ordered;
- Where particularly serious harm is caused, a fine between RMB 2 million and RMB 10 million shall be imposed, individuals shall be fined between RMB 200,000 and RMB 1 million, and measures such as business suspension or revocation of certificates or licenses may likewise apply.

The revised provision comprehensively raises the upper limits of fines for acts such as network operators' failure to perform security protection obligations and violations by critical information infrastructure operators, and introduces a tiered penalty mechanism linked to the severity of the consequences of violations. This tiered design makes the boundaries of liability highly clear.

IV. Clearer Alignment of Rules

Another notable part of this amendment is the systematic strengthening of legal liabilities. It clearly aligns the rules of different laws through logical consolidation and connection, creating a more rigorous liability system.

The added paragraph in Article 42 provides: "*When network operators handle personal information, they shall comply with this Law and the provisions of the Civil Code of the People's Republic of China, the Personal Information Protection Law of the People's Republic of China, and other laws and administrative regulations.*" This paragraph clarifies the alignment requirements between multiple laws relating to the handling of personal information and ensures the consistency of personal information rights protection. This requires enterprises to carry out integrated compliance management, and any data processing activities must meet multiple legal standards.

Under the overall tone of unifying personal information rights protection, the newly revised Cybersecurity Law merges former Articles 64, 66, and 70 into new Article 71 and provides in Paragraph 2 of this article that "*where personal information rights are infringed, handling and punishment shall be carried out in accordance with the relevant laws and administrative regulations*," thereby achieving seamless connection with the liability provisions of the Personal Information Protection Law and avoiding grey areas in the application of the law

V. More Detailed Responsibilities for Critical Information Infrastructure Operators

Revised Article 67 amends former Article 65 to: *Where a critical information infrastructure operator uses network products or services that have not undergone security review or have failed security review, the competent authorities shall order cessation of use and impose a fine of between one and ten times the procurement amount, and the directly responsible persons shall be fined between RMB 10,000 and RMB 100,000*.

This amendment links the fine standards to the procurement amount, achieving alignment between liability and business scale. This means that enterprises, especially those that may be identified as critical information infrastructure operators, must treat cybersecurity review as a key component of supply chain management when procuring core network equipment or services. When selecting suppliers (especially cloud service providers), their security and compliance capabilities should be taken as important evaluation indicators, and relevant responsibilities should be clearly defined in contracts.

Conclusion

Overall, the amendments to the new Cybersecurity Law promote China's cybersecurity governance toward a more mature and refined stage by elevating strategic positioning,

incorporating new technology regulation, and strengthening legal liabilities: emphasizing security while also encouraging development; clarifying responsibilities while also providing buffer mechanisms.

For foreign enterprises in China, this amendment is more a clarification of the legal framework than a tightening of the regulatory environment, representing the formation of a business environment with clearer rules and more predictable law enforcement. Enterprises need to maintain robust network and data governance capabilities, continuously monitor policy developments, and ensure the long-term, stable, and successful development of their business in China.

Principali impatti dell'attuazione della Legge IVA della RPC sulle operazioni aziendali

A decorrere dal 1° gennaio 2026, sono ufficialmente entrate in vigore la Legge sull'Imposta sul Valore Aggiunto della Repubblica Popolare Cinese e i relativi Regolamenti di Attuazione; contestualmente, le Misure per l'Amministrazione della Registrazione dei Contribuenti Ordinari IVA sono state abrogate.

Questo cambiamento segna il passaggio del sistema IVA cinese da un regime disciplinato principalmente da regolamenti amministrativi a un quadro centrato sulla legge statutaria, introducendo requisiti di conformità più chiari e strutturati per le imprese.

1.Gestione dei contribuenti ordinari IVA

In base alle precedenti misure amministrative, lo status di contribuente ordinario fungeva in gran parte da classificazione amministrativa. Nella pratica, le imprese determinavano spesso il trattamento IVA verificando innanzitutto se possedessero i requisiti per tale qualifica.
Tuttavia, con la nuova Legge IVA:

- Le regole pertinenti sono incorporate direttamente nel quadro legale.
- Viene posta maggiore enfasi sul fatto che la transazione stessa costituisca un'attività imponibile.
- Le imprese devono concentrarsi sull'effettivo verificarsi di una transazione imponibile, sul metodo di tassazione applicabile e sul corretto adempimento degli obblighi di dichiarazione e fatturazione, piuttosto che basarsi esclusivamente sullo status di contribuente.

2. Pagamenti di commissioni per servizi transfrontalieri

La Legge IVA fornisce un quadro più chiaro per determinare se i servizi siano "consumati in Cina":

- Pagamenti a fornitori esteri: Quando le imprese della RPC pagano commissioni (come spese di consulenza, servizi tecnici, gestione o abbonamenti SaaS) a fornitori esteri, tali servizi possono essere considerati imponibili in Cina se utilizzati o consumati internamente.
- Obbligo di ritenuta: Se il fornitore estero non è registrato ai fini IVA in Cina, il pagatore cinese è tenuto a trattenere e versare l'IVA in conformità alla legge.
- Servizi digitali: I servizi digitali, di piattaforma o di supporto tecnico online forniti da imprese estere a clienti cinesi possono essere considerati imponibili se il luogo effettivo di consumo è la Cina. Gli obblighi IVA non possono essere esclusi solo perché il fornitore si trova all'estero o i pagamenti avvengono tramite canali transfrontalieri.

3. Valutazione di beni immateriali e servizi digitali

L'attuazione della legge ha reso cruciale la valutazione IVA per i beni immateriali e i servizi digitali.

- Le transazioni riguardanti licenze software, servizi dati e diritti d'uso di piattaforme devono essere valutate in base al luogo di utilizzo o consumo.
- I pagamenti per spese quali commissioni di gestione, servizi e competenze tecniche sono ora soggetti a maggiore scrutinio.

Conclusione

La logica fondamentale dell'amministrazione IVA si sta spostando da un approccio "basato sull'identità" a uno "basato sulla transazione". I rischi fiscali derivano sempre più dalla sostanza delle operazioni commerciali, dagli accordi contrattuali e dalle prestazioni effettive.

Si consiglia alle imprese di revisionare proattivamente i propri modelli di business, specialmente quelli che coinvolgono attività transfrontaliere e digitali, per allinearsi al nuovo quadro legale.

Key Impacts of the PRC VAT Law New Implementations

Effective from 1 January 2026, the Value-Added Tax Law of the People's Republic of China and its Implementation Regulations have officially come into force, and the Measures for the Administration of VAT General Taxpayer Registration have been repealed. This change marks a shift in China's VAT system from one primarily governed by administrative regulations to a framework centered on statutory law, bringing clearer and more structured compliance requirements for enterprises.

First, with respect to general VAT taxpayer management, under the former administrative measures, general taxpayer status functioned largely as an administrative classification. In practice, enterprises often determined VAT treatment by first considering whether they qualified as general taxpayers. Under the VAT Law, however, the relevant rules are incorporated directly into the legal framework, placing greater emphasis on whether a transaction itself constitutes a taxable activity. Enterprises are now required to focus on whether a taxable transaction has occurred, which taxation method applies, and whether VAT declaration and invoicing obligations are properly fulfilled, rather than relying solely on taxpayer status.

Second, regarding cross-border service fee payments, the VAT Law provides a clearer framework for determining whether services are "consumed within China."

On one hand, where PRC enterprises pay service fees—such as consultancy fees, technical service fees, management fees, or SaaS subscription fees—to overseas suppliers, such services may constitute taxable services within China if they are used or consumed domestically. If the overseas service provider is not registered for VAT in China, the PRC payer is required to withhold and remit VAT in accordance with the law.

On the other hand, where overseas enterprises provide digital services, platform services, or online technical support to PRC customers and charge fees accordingly, such services may also be regarded as taxable if their actual place of consumption is in China. VAT obligations cannot be excluded solely because the service provider is located overseas or payments are made through cross-border settlement channels.

In addition, following the implementation of the VAT Law, VAT assessment for intangible assets and digital services has become increasingly important. Transactions

involving software licensing, data services, and platform usage rights must be evaluated based on their place of use or consumption to determine whether they are subject to VAT in China. At the same time, expense-type payments such as management fees, service fees, and technical fees are more likely to attract scrutiny from a VAT perspective, and enterprises should ensure that the relevant tax treatments are properly applied.

Overall, the core logic of VAT administration is shifting from an "identity-based" approach to a "transaction-based" approach. VAT risks for enterprises are increasingly derived from the substance of business transactions, contractual arrangements, and actual performance, rather than from registration status alone. Enterprises are therefore advised to proactively review their existing business models—particularly those involving cross-border and digital activities—to better align with the new VAT legal framework.

Vuoi fare business in Cina? Non trascurare gli adempimenti annuali di compliance obbligatoria

In conformità alle leggi e ai regolamenti della Repubblica Popolare Cinese, sia le imprese domestiche sia le **imprese a capitale estero (Foreign-Invested Enterprises – FIEs)** sono tenute a rispettare specifiche procedure annuali di compliance, tra cui **la revisione contabile annuale, gli adempimenti fiscali e il reporting annuale**, al fine di soddisfare i requisiti legali, finanziari e regolamentari. Tali attività non rappresentano esclusivamente un obbligo normativo, ma costituiscono anche un'opportunità per le imprese di valutare in modo più approfondito la propria situazione operativa e finanziaria.

Come indicato sopra, i tre principali adempimenti sono i seguenti:

1. Revisione contabile annuale
Ogni società è tenuta a sottoporre i propri bilanci a una revisione contabile annuale. Tale revisione è condotta da una società di revisione cinese abilitata (Chinese Certified Public Accountant – CPA) e ha l'obiettivo di garantire che l'informativa finanziaria sia conforme alla normativa cinese. Sebbene i requisiti siano più stringenti per le FIEs, è generalmente raccomandato che tutte le imprese effettuino una revisione annuale al fine di garantire trasparenza e una solida governance finanziaria.
Per le FIEs, i precedenti fondi di riserva e i fondi per lo sviluppo dell'impresa sono stati unificati nelle **riserve legali** e nelle **riserve discrezionali**; eventuali adeguamenti devono essere integralmente indicati nella relazione di revisione annuale.

2. Adempimenti fiscali annuali
Le società sono tenute a versare l'Imposta sul Reddito delle Società (Corporate Income Tax – CIT) con cadenza trimestrale. Inoltre, devono completare la riconciliazione fiscale annuale entro il **31 maggio dell'anno successivo**. Una volta completato tale adempimento, le imprese a capitale estero possono procedere alla distribuzione e al rimpatrio degli utili.

3. Reporting annuale
I report devono essere completati e presentati alle autorità governative competenti entro il **30 giugno**. Il reporting include le informazioni di base della società e i relativi aggiornamenti; a seconda della natura dell'attività svolta, potrebbe essere richiesta documentazione aggiuntiva.

I report annuali delle FIEs e le dichiarazioni relative agli investimenti esteri sono ora integrati e presentati tramite uno **sportello unico** all'interno del **National Enterprise Credit Information Publication System (NECIPS)**, eliminando la necessità di presentazioni duplicate.

Anche gli **Uffici di Rappresentanza esteri (Representative Offices – ROs)** sono soggetti a questi tre principali adempimenti di compliance. Nel periodo compreso tra il **1° marzo e il 30 giugno**, i ROs devono inoltre presentare alle autorità locali della **State Administration for Market Regulation (SAMR)** la documentazione attestante lo status giuridico della società madre estera.

Principali differenze tra FIEs e imprese domestiche

Sebbene il processo di compliance di base sia simile, le FIEs sono generalmente soggette a requisiti più stringenti, mentre le imprese domestiche affrontano un livello inferiore di oneri burocratici. Le principali differenze includono:

- **Reporting annuale**
  Le FIEs sono tenute a includere, oltre al report NECIPS, anche le comunicazioni per il **Ministero del Commercio (MOFCOM)** e per la **State Administration of Foreign Exchange (SAFE)**. Le imprese domestiche, di norma, devono presentare esclusivamente il report NECIPS.
- **Reporting SAFE**
  Le FIEs devono comunicare le operazioni in valuta estera, i movimenti di capitale e il rimpatrio degli utili. Le imprese domestiche non sono tenute a presentare report SAFE, salvo nel caso di operazioni transfrontaliere. Il reinvestimento domestico degli utili da parte delle FIEs può beneficiare di procedure semplificate, a condizione che i dati relativi ai flussi di capitale transfrontalieri siano comunicati in modo accurato e tempestivo.
- **Compliance fiscale**
  Sia le FIEs sia le imprese domestiche devono presentare la dichiarazione CIT. Le FIEs sono inoltre tenute a predisporre una relazione di revisione e ad applicare le ritenute fiscali sugli utili rimpatriati. Le imprese domestiche devono adempiere a tali obblighi aggiuntivi solo in presenza di operazioni transfrontaliere.
- **Revisione contabile annuale**
  La revisione è obbligatoria per tutte le FIEs. Per le imprese domestiche, la revisione è facoltativa per le piccole e medie imprese (PMI), mentre è obbligatoria per le grandi imprese.
- **Documentazione sui prezzi di trasferimento (Transfer Pricing – TP)**
  Le FIEs sono soggette a requisiti più rigorosi, in particolare in relazione alle operazioni infragruppo transfrontaliere. Sebbene le imprese domestiche siano soggette a controlli meno stringenti, sono comunque tenute a predisporre la documentazione TP in caso di operazioni con parti correlate.

- **Reporting sulla corporate governance**
  Le FIEs devono comunicare eventuali variazioni relative ad amministratori, azionisti e struttura del capitale. Le imprese domestiche sono soggette a minori restrizioni, salvo nei casi in cui operino in settori regolamentati.
- **Reporting del personale**
  Sia le FIEs sia le imprese domestiche devono includere nei report annuali le informazioni relative a lavoro dipendente, contributi previdenziali e fondi per l'edilizia abitativa. Questo aspetto è particolarmente rilevante per le FIEs che impiegano personale straniero, mentre risulta più semplice per le imprese domestiche che impiegano esclusivamente personale locale.

In conclusione, sebbene la compliance annuale obbligatoria si applichi a entrambe le tipologie di imprese, le **FIEs sono generalmente soggette a un livello di controllo più elevato**. Il rispetto puntuale di tali adempimenti e l'adozione di procedure specifiche per le attività transfrontaliere sono fondamentali per garantire la conformità normativa e migliorare la trasparenza finanziaria.

Want to Do Business in China? Don't Miss Your Annual Statutory Compliance Steps!

In accordance with the laws and regulations of the People's Republic of China, both domestic and foreign-invested enterprises (FIEs) must adhere to specific annual compliance procedures—including annual audits, tax filings, and annual reporting—to meet legal, financial, and regulatory standards. These activities are not only a legal obligation but also an opportunity for companies to understand their own operational and financial health.

As mentioned above, the three primary steps are:

1. Annual Audit: Every company is required to undergo an annual audit of its financial statements. This audit is conducted by a Chinese Certified Public Accountant (CPA) firm to ensure the company's financial reporting complies with Chinese regulations. While these requirements are stricter for FIEs, it is generally recommended that all companies conduct an annual audit to maintain transparency and sound financial governance. For FIEs, former reserve funds and enterprise development funds are now unified under statutory and discretionary surplus reserves; any related adjustments must be fully disclosed in the annual audit.

2. Annual Tax Filing: Companies must pay Corporate Income Tax (CIT) on a quarterly basis. Additionally, they must complete the annual tax reconciliation by May 31 of the following year. Once this step is completed, foreign companies can proceed with the distribution and repatriation of profits.

3. Annual Reporting: Reports must be completed and submitted to government authorities by June 30. This includes basic company information and updates. Depending on the nature of the business, additional documentation may be required. FIE annual reports and foreign investment information reports are now integrated; they are submitted via a "single window" through the National Enterprise Credit Information Publication System (NECIPS), eliminating the need for duplicate submissions.

Foreign representative offices (ROs) also require these three main compliance steps. Between March 1 and June 30, ROs must submit proof of the legal status of their overseas parent organization to the local State Administration for Market Regulation (SAMR).

Key Differences Between FIEs and Domestic Companies

While the core compliance process is similar, FIEs often face stricter requirements, whereas domestic companies may encounter fewer bureaucratic hurdles. Key differences include:

- Annual Reporting: FIEs are expected to include reports for the Ministry of Commerce (MOFCOM) and the State Administration of Foreign Exchange (SAFE), alongside the NECIPS report. Domestic companies typically only need to submit the NECIPS report.
- SAFE Reporting: FIEs must report on foreign exchange, capital transactions, and profit returns. Domestic companies do not need to submit SAFE reports unless they engage in cross-border transactions. Domestic reinvestment of profits by FIEs can benefit from simplified procedures, provided that relevant cross-border fund flow data is reported accurately and on time.
- Tax Compliance: Both FIEs and domestic companies must file CIT returns. FIEs must also complete an audit report and withhold taxes on repatriated profits. Domestic firms only need to complete this step if they are involved in cross-border transactions.
- Annual Audit: Audits are mandatory for all FIEs. For domestic companies, audits are optional for Small and Medium Enterprises (SMEs) but mandatory for large enterprises.
- Transfer Pricing (TP) Documentation: FIEs face more rigorous requirements, particularly regarding cross-border related-party transactions. While domestic companies face less scrutiny, they must still provide TP documentation if involved in related-party dealings.
- Corporate Governance Reporting: FIEs must report any changes to directors, shareholders, and capital structure. Domestic companies have fewer restrictions in this regard unless they operate in a regulated industry.
- Employee Reporting: Both FIEs and domestic companies must include annual labor, social insurance, and housing fund information in their reports. This is particularly critical for FIEs employing foreign nationals, whereas it is simpler for domestic companies employing only local staff.

Overall, while mandatory annual compliance applies to both, FIEs generally face more stringent oversight. Following these key steps and establishing specific procedures for cross-border activities is essential for ensuring legal compliance and improving financial transparency.

circumstances, constitute a legal opinion on the matters addressed, nor can it give rise to any legitimate expectations or be relied upon as the basis for legal action.For any further clarification, please contact: ipr.pechino@ice.it or visit the website: https://www.ice.it/it/mercati/cina/pechino/desk-tutela-proprieta-intellettuale