Provide one-stop compliance service on China Cybersecurity Law MLPS 2.0

China is an extremely important market, and for enterprises expanding or already operating inside Mainland China, it is imperative their digital transformation be in compliance with China Cybersecurity Law MLPS 2.0, the most up to date version of this mandatory regulation. To ensure not only an easier and smoother process to achieve this, but also more stringent and careful verification, CITIC Telecom CPC offers the China Cybersecurity Law MLPS 2.0 Compliance Service, a one-stop service covering every aspect and stage of the China Cybersecurity Law MLPS 2.0 process, including classification, registration, gap analysis, remediation and assessment. This important service is easy, reliable, and professionally administered to ensure an enterprise operates a robust, fully compliant MLPS 2.0 infrastructure.

Compliance Service Scope

Information System Survey
An initial survey is conducted, to assess the target Information System, covering physical location, network topology, personal information types, existing security devices, and other items.

Classification of Consequences
In the event of compromise of the Information System, levels of consequences are defined according to the official MLPS 2.0 Level Classification rule.

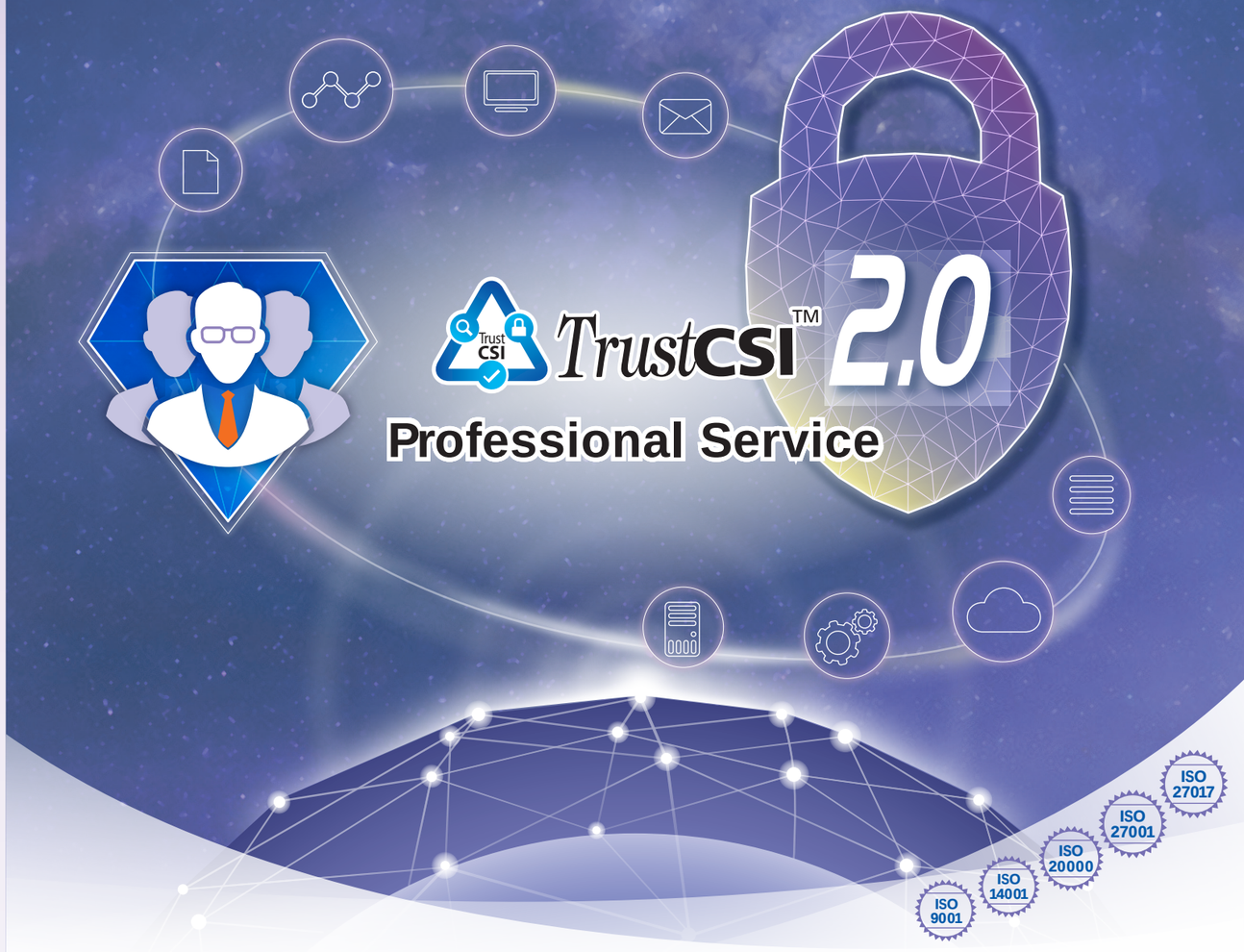
Materials Registration
All necessary materials such as appropriate documents and forms are prepared and submitted to the Local Internet Police.

Gap Analysis Reporting
A “Gap Analysis Report” is produced, according to non-compliance findings related to the current topology of the Information System (based on the MLPS 2.0 compliance table).

Remediation Planning
Based on the “Gap Analysis Report” a “Remediation Plan” will be carefully created, assisting the enterprise to properly and systematically close the identified security gaps using IT security best practices.

Official Assessment Assistance
For the final submission of the “Official Assessment Report” to the local Network Police for endorsement, CITIC Telecom CPC’s experts will assist the enterprise with every step of the official assessment process.

CITIC TELECOM CPC



World-class Security Talent at Your Service

Your Global Local ICT Solutions Partner

CITIC Telecom CPC
W: www.citictel-cpc.com
Asia Pacific: info@citictel-cpc.com
Europe and CIS: info-eu@citictel-cpc.com

Hong Kong T: 852 2170 7101
Japan T: 81 3 5339 1968
Estonia T: 372 622 33 99
Russia T: 7 495 981 5676
Taiwan T: 886 2 6600 2588
Malaysia T: 603 2280 1500
Poland T: 48 22 630 63 30
The Netherlands T: 31 20 567 2000
Mainland China (Toll Free): 400 651 7550
Singapore T: 65 6220 6606

TPS2010EN

中信國際電訊(信息技術)有限公司
CITIC TELECOM INTERNATIONAL CPC LIMITED
中信國際電訊集團成員
A member of CITIC Telecom International

Dedicated team of security professionals for managing your mission-critical cybersecurity tasks

To gain productivity and competitiveness, enterprises of all scales are adopting digital transformation strategies, leveraging cutting-edge technologies to empower and extend their business opportunities. Yet, as these organizational networks become more complex and cover more markets, their vulnerability also increases. Network attacks are no longer simply nuisances, but cause far-ranging damage to business operations and even reputation. Additionally, with geographic expansion comes the need to comply with various data and privacy security regulations, such as China Cybersecurity Law requirements.

To help companies address and manage all these concerns, CITIC Telecom CPC created **TrustCSI™ Professional Service**, offering a range of mission-critical cybersecurity-related tasks performed by top-notch security professionals, including vulnerability assessment, penetration testing, security device migration and China Cybersecurity Law MLPS 2.0 compliance. It can be cost prohibitive, and very difficult, to hire world-class security professionals to work as in-house IT staffing, but through TrustCSI™ Professional Service, any company can leverage the expertise of CITIC Telecom CPC's extensively trained and industry-certified security experts to pinpoint vulnerabilities in the enterprise network, assist with network strengthening, and help support smooth business expansion into new geographies.

TrustCSI™ IAS

Information Assessment Service

Thorough analysis and identification of network weaknesses through deep vulnerability assessment

To thoroughly analyze and identify enterprise network vulnerabilities, our IT security professionals adopt a 4-tiered systematic and disciplined approach which can uncover security weaknesses, and deliver insights into an organization's security posture and effectiveness of countermeasures.

1 Systematic Service Planning

To ensure TrustCSI™ IAS is properly customized and meets the requirements of a particular business and network topology, CITIC Telecom CPC's certified security professionals will first consult with customers regarding the service schedule and assessment scope.

2 Wide Spectrum Risk Assessment

To ensure security vulnerabilities are thoroughly identified and risk levels properly assessed, TrustCSI™ IAS leverages the industry's most comprehensive IT security knowledge base and leading vulnerability management toolset to analyze web applications, network equipment and IT infrastructure.

3 Risk Reporting and Recommendations

After deep analysis of the enterprise network, CITIC Telecom CPC security professionals will present the findings via a detailed report, which covers all identified risks (and predicted consequences if they are exploited), plus expert recommendations to close these loopholes, and other risk remediation insights.

4 Optional Re-auditing

An optional re-auditing stage can be performed as an after-action assessment, to check whether updates to the network have properly secured previously identified security gaps, and if any new vulnerabilities have appeared because of the infrastructure modifications.

A damage-free penetration testing to evaluate the sufficiency of security measures under real-world attacks

Where Vulnerability Assessment is a more passive and analytical process, Penetration Testing is an active attempt to break through network defenses (ethical hacking), focusing attack attempts on the network, web applications and other organizational applications and entry points. This is a damage-free exercise, only to test if security measures are sufficient against a simulated real-world attack.

External Penetration Testing

To uncover what information (public or private) an attacker can gain from an organization via an attack originating externally, this External Penetration Testing will be conducted without any internal access "assistance" to simulate exploits against Internet-facing digital assets (e.g., web applications, web servers, network endpoints, VPN, e-mail servers). The majority of hacking attempts are simulated by this external test.

Internal Penetration Testing

To simulate "insider attacks" (e.g., guests entering the organization's physical boundaries including wireless range, malicious staff or other insiders, and even the scope of access an attacker gains once the external defenses are breached), this Internal Penetration Testing is performed within premises. Focus is on workstations, internal applications, access controls, domains, and internal documents, to identify vulnerabilities of sensitive information and controls.

Results from both External and Internal Penetration exercises will form the basis of remedial recommendations from CITIC Telecom CPC's IT security experts. These will be in the form of an on-site presentation, and cover identified assets, threats, vulnerabilities, impacts and suggestions.

A purpose-designed security device migration service to best fit your business and security needs

Enterprise networks often grow organically as business needs arise, with new technologies, new locations, and new connectivity methods, including wireless access. Yet this expansion leads to an increasing number of entry points and potential vulnerabilities. CITIC Telecom CPC's professional service team helps organizations migrate to a purpose-designed, more innovative security infrastructure designed from scratch to best fit business and security needs. The security team will ensure clarity on the risk factors of the original network, and explain an optimized migration strategy for a smooth and reliable process, with detailed planning and conscientious change management.

4-Step Security Device Migration