1. Introduction

As global enterprises expand into the Chinese market, ERP (Enterprise Resource Planning) systems must comply with China's cybersecurity and data protection regulations. This report outlines the key regulatory requirements enterprises must follow when selecting and deploying ERP systems and provides compliance recommendations.

2. Applicable Chinese Security Regulations

ERP systems in China must comply with multiple legal and regulatory requirements, including:

2.1 Cybersecurity Law

Effective Date: June 1, 2017
Key Requirements:

- Critical data and personal information must be stored within China.
- Critical Information Infrastructure Operators (CIIOs) must undergo security reviews.
- Enterprises must implement data security measures, such as access controls and encryption.
- Resource from：https://www.cac.gov.cn/

2.2 Data Security Law

Effective Date: September 1, 2021
Key Requirements:

- Data must be classified and graded based on different protection levels.
- Important data requires government approval before cross-border transfer.
- Non-compliance may result in fines, business suspension, or license revocation.
- Resource from：https://www.npc.gov.cn/

2.3 Personal Information Protection Law (PIPL)

Effective Date: November 1, 2021
Key Requirements:

- Collecting and processing personal information requires user consent.
- Cross-border transfer of personal information requires a security assessment.
- Organizations must provide mechanisms for deleting, modifying, and accessing personal data.
- Resource from：https://www.cac.gov.cn/

2.4 Regulations on the Security Protection of Critical Information Infrastructure

Effective Date: September 1, 2021
Key Requirements:

- Critical infrastructure (such as finance, telecom, and energy sectors) must implement strict security protection measures.
- If an ERP system is used in critical infrastructure, it must meet higher security standards.
- 官方来源：https://www.miit.gov.cn/

2.5 Multi-Level Protection Scheme (MLPS 2.0)

Key Requirements:

- Applies to all enterprise IT systems, categorized from Level 1 to Level 5.
- ERP systems typically require **at least MLPS Level 2** certification.
- Includes identity authentication, access control, intrusion detection, and encryption measures.
- 官方来源：https://www.mps.gov.cn/

2.6 Industrial Enterprise Data Classification and Grading Guidelines

Key Requirements:

- ERP data must be classified according to **industrial enterprise data classification guidelines**.
- Different levels of data require different security management measures.
- 官方来源：https://www.miit.gov.cn/

3. ERP Compliance Requirements

3.1 Data Storage and Cross-Border Transfer

- Ensure ERP data is stored within China.
- If cross-border data transfers are needed, undergo **security assessments** or use **contractual safeguards** (e.g., Standard Contractual Clauses, SCCs).

3.2 Access Control and Identity Management

- Implement **Zero Trust Architecture** and **Multi-Factor Authentication (MFA)**.
- Enforce fine-grained access controls, adhering to the **Principle of Least Privilege**.

3.3 Data Encryption and Security Protection

- Use **Chinese commercial cryptographic algorithms** (such as SM2, SM3, SM4) for encryption.
- Ensure data transmission uses **TLS 1.2/1.3** or higher security protocols.

3.4 Multi-Level Protection Scheme (MLPS 2.0)

- Ensure the ERP system meets **at least MLPS Level 2** technical requirements.
- Implement logging, intrusion prevention, and disaster recovery solutions.

3.5 Security Incident Response and Compliance Audits

- Establish a **Security Incident Response Mechanism** to address data breaches or attacks promptly.
- Conduct regular security audits to ensure the ERP system remains compliant.

4. Conclusion and Recommendations

To ensure ERP system compliance in the Chinese market, we recommend:

1. Choosing an ERP vendor that meets **Cybersecurity Law, Data Security Law, and PIPL** requirements.
2. Ensuring ERP deployment complies with **MLPS 2.0** certification.
3. Establishing a **cross-border data transfer management framework** and conducting security assessments.
4. Using **localized encryption solutions** that align with national cryptographic standards.

5. Performing **regular compliance audits** to ensure the ERP system adheres to the latest regulations.

By following these guidelines, enterprises can mitigate legal risks and ensure the secure and stable operation of their ERP systems in the Chinese market.

Prepared by: Tingting Huang
Submission Date: 2025-02-06