艾訊資訊安全政策
Axiomtek Information Security Policy

一、資訊安全政策方針 (Guidelines)

為了提升客戶信心，保護客戶資訊，強化資訊安全管理體系，強化企業資安韌性，促使企業永續發展，艾訊導入 ISO 27001:2022 標準建立專責的資安組織與適當的管理程序，以確保公司資訊資產之機密性、完整性與可用性，並重視與保障使用者與客戶資料隱私，完善安全措施，提高系統可用度與信任度。

To enhance customer confidence, protect customer information, strengthen information security management systems, bolster organizational cyber resilience, and foster sustainable development, Axiomtek Company has implemented the ISO 27001:2022 standard. This initiative involves establishing a dedicated cybersecurity organization and implementing appropriate management procedures to ensure the confidentiality, integrity, and availability of the company's information assets. Additionally, there is a strong emphasis on safeguarding user and customer data privacy, enhancing security measures, improving system availability, and building trust.

導入適當的 IT 備份機制與雲端備份解決方案，排定定期災害復原演練，當公司發生不可預期的營運中斷時，能迅速還原，控制於設定目標範圍內。

Implementing appropriate IT backup mechanisms and cloud backup solutions, scheduling regular disaster recovery drills. In the event of unforeseen operational disruptions, the company can swiftly restore operations, maintaining control within the defined target scope.

艾訊總部與製造工廠的重要營運核心系統與營運活動定期取得第三方資安認證以確保系統持續改進與有效性。

Axiomtek ensures the continuous improvement and effectiveness of its crucial operational systems and activities at both the headquarters and manufacturing facilities by obtaining regular third-party cybersecurity certifications.

二、資訊安全政策 (Policy)

資安防護不中斷 - Continuous Security Protection

風險控管要持續 - Persistent Risk Management

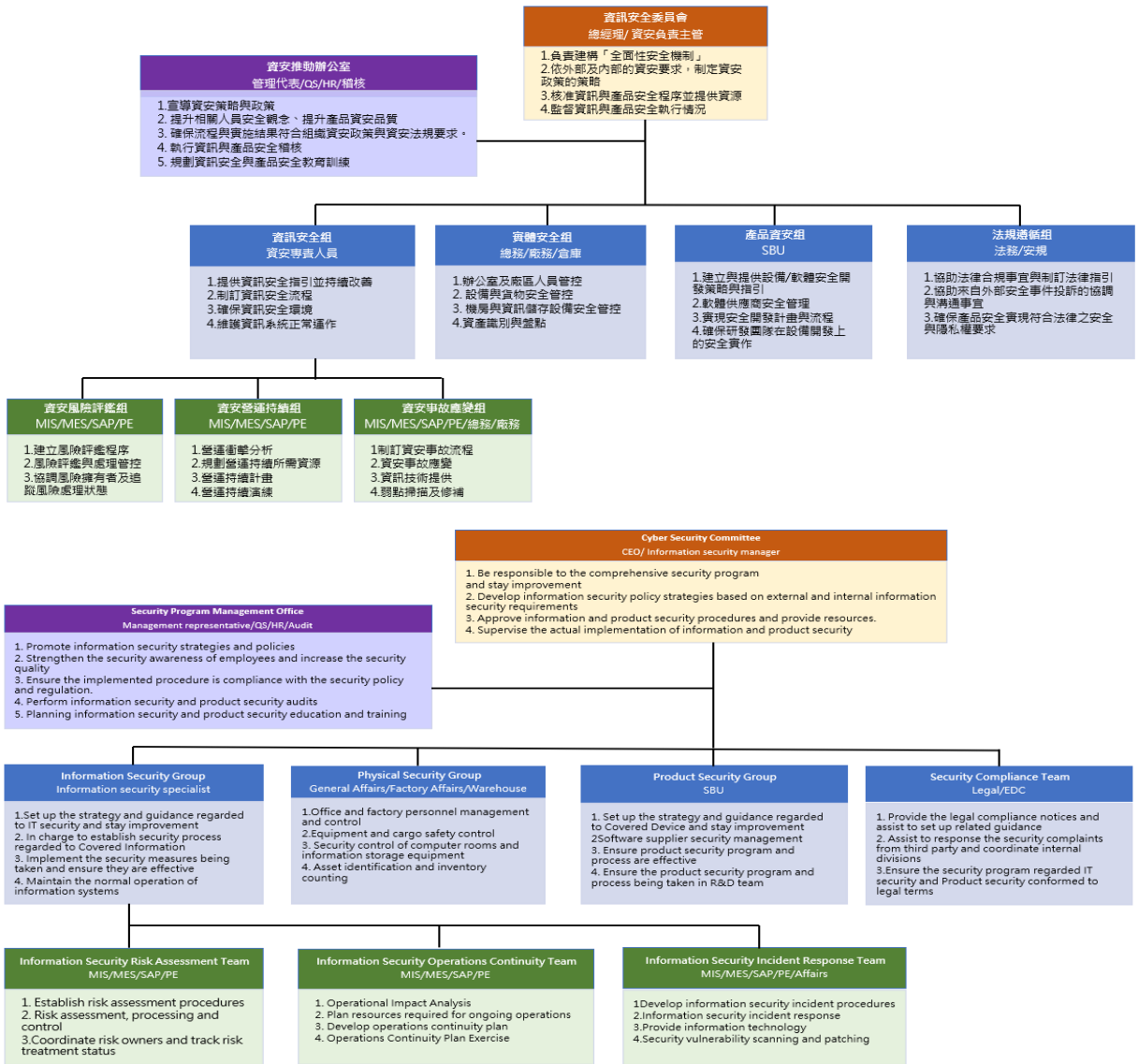
企業營運有保障 - Assured Business Operations

Axiomtek Co., Ltd.
8F., No.55, Nanxing Rd., Xizhi Dist., New Taipei City 221, Taiwan
TEL +886-2-8646-2111 FAX +886-2-8646-2555
www.axiomtek.com

三、資安治理組織 (Organization)

艾訊設有資訊安全委員會(IT Security Committee)，設置資安專責主管及資安專責人員，負責資訊安全政策與制度之規劃、監控及管理作業，並與公司資訊技術及相關單位組織合作，強化資訊安全防護及管理機制，詳見下圖。

Axiomtek has established an Information Security Committee (IT Security Committee) responsible for the planning, monitoring, and management of information security policies and systems. The committee includes a dedicated Information Security Officer and personnel, tasked with collaborating with the company's information technology and relevant units to enhance information security protection and management mechanisms, See details below:

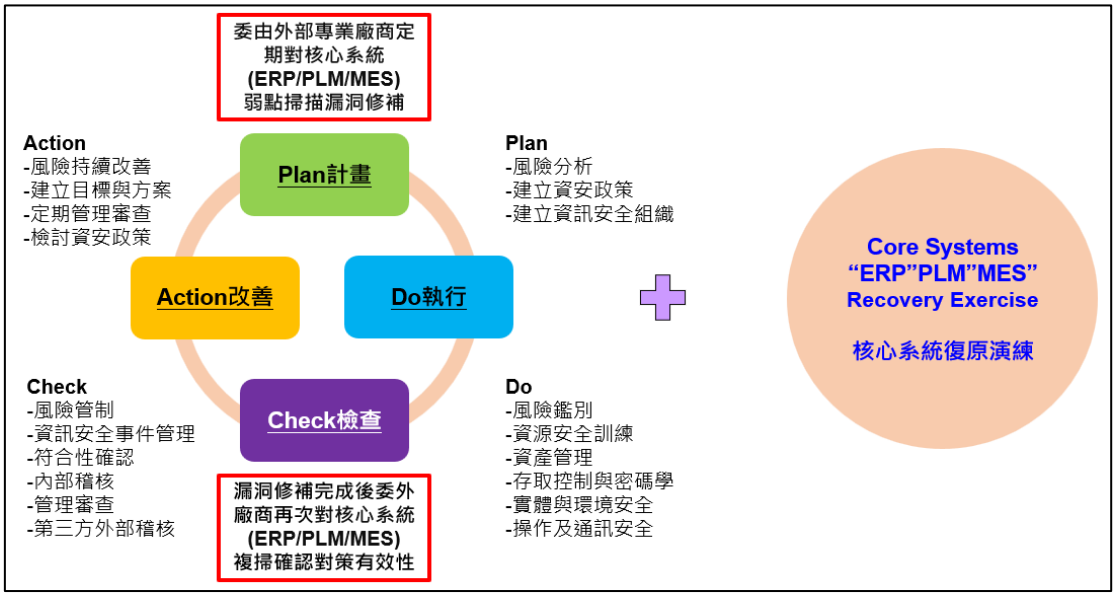


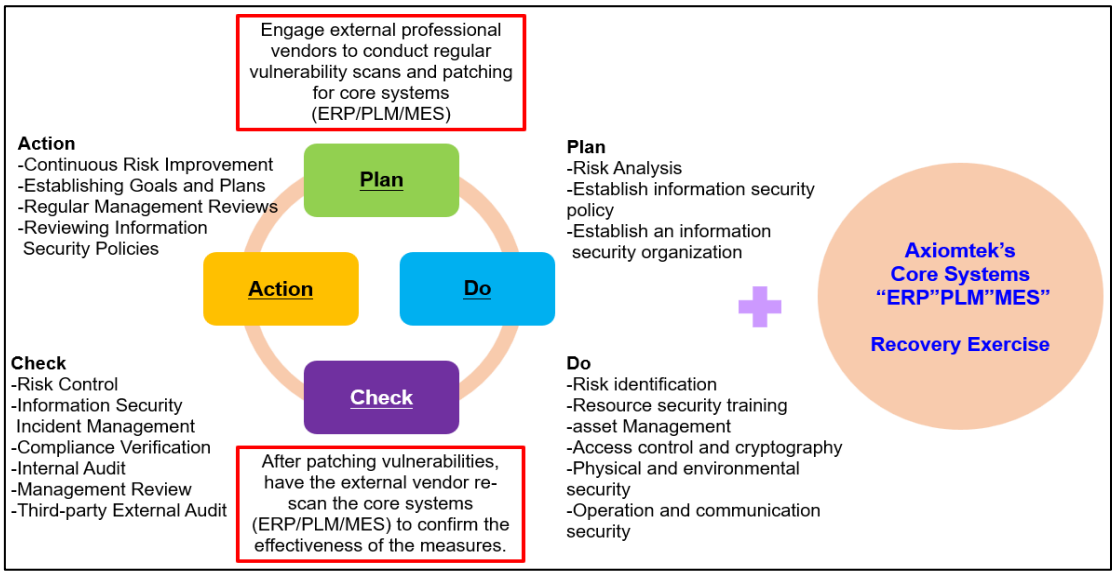
Axiomtek Co., Ltd.
8F., No.55, Nanxing Rd., Xizhi Dist., New Taipei City 221, Taiwan
TEL +886-2-8646-2111 FAX +886-2-8646-2555
www.axiomtek.com

四、資安治理運作模式 (Operation mode)

艾訊根據 ISO/IEC 27001:2022 標準的要求，建立、實施、保持和持續改進資訊安全管理體系(ISMS)，公司全體員工都將有效地貫徹執行這個體系並持續改進，以確保其有效性，資訊安全管理制度(ISMS)所涉及的過程基於以下 PDCA (Plan-Do-Check-Act)模式，詳見下圖。

Axiomtek has established, implemented, maintained, and continuously improved an Information Security Management System (ISMS) in accordance with the requirements of ISO/IEC 27001:2022. All employees of the company will effectively implement and continuously improve the ISMS to ensure its effectiveness. The processes involved in the Information Security Management System (ISMS) are based on the Plan-Do-Check-Act (PDCA) model, as detailed in the diagram below.





Axiomtek Co., Ltd.
8F., No.55, Nanxing Rd., Xizhi Dist., New Taipei City 221, Taiwan
TEL +886-2-8646-2111 FAX +886-2-8646-2555
www.axiomtek.com

五、資訊安全管理與執行重點 (Key Points in Information Security Management and Implementation)

1. 資訊安全管理(Information Security Management)
2. 資訊安全政策管理(Information Security Policy Management)
3. 資訊安全組織管理(Information Security Organization Management)
4. 人力資源安全管理(Human Resources Security Management)
5. 資訊資產管理(Information Asset Management)
6. 存取控制管理(Access Control Management)
7. 密碼管理(Password Management)
8. 實體與環境安全管理 (Physical and Environmental Security Management)
9. 作業安全管理(Operation Security Management)
10. 通訊安全管理(Communication Security Management)
11. 資訊系統獲取、開發及維護管理(Information System Acquisition, Development, and Maintenance Management)
12. 供應商關係管理(Supplier Relationship Management)
13. 資訊安全事件管理(Information Security Incident Management)
14. 業務持續管理(Business Continuity Management)
15. 遵循性(適法性)管理(Compliance Management)
16. 資料安全管理(Data Security Management)
17. 變更與組態管理(Change and Configuration Management)
18. 雲端服務管理(Cloud Service Management)

六、資安事件處理與通報 (Information Security Incident Handling and Reporting)

艾訊已成立資訊安全應變中心與資訊安全事件管理程序，明訂相關流程與措施，包含資安事件通報程序、指派負責人員處理重大資通安全事件、評估遭受損失及進一步的必要因應措施、評估資安風險可能對公司財務與營運的影響及其因應措施。

Axiomtek has set up an Information Security Incident Response Center and associated procedures, outlining processes for reporting incidents, assigning responsibilities, assessing losses, determining response measures, evaluating potential impacts on financial and operational aspects, and implementing necessary actions.

Established on January 31, 2024 Version: V1.0

Axiomtek Co., Ltd.
8F., No.55, Nanxing Rd., Xizhi Dist., New Taipei City 221, Taiwan
TEL +886-2-8646-2111 FAX +886-2-8646-2555
www.axiomtek.com