資通安全風險管理架構，訂定資通安全政策、具體管理方案及投入資通安全管理之資源

1. 風險管理架構

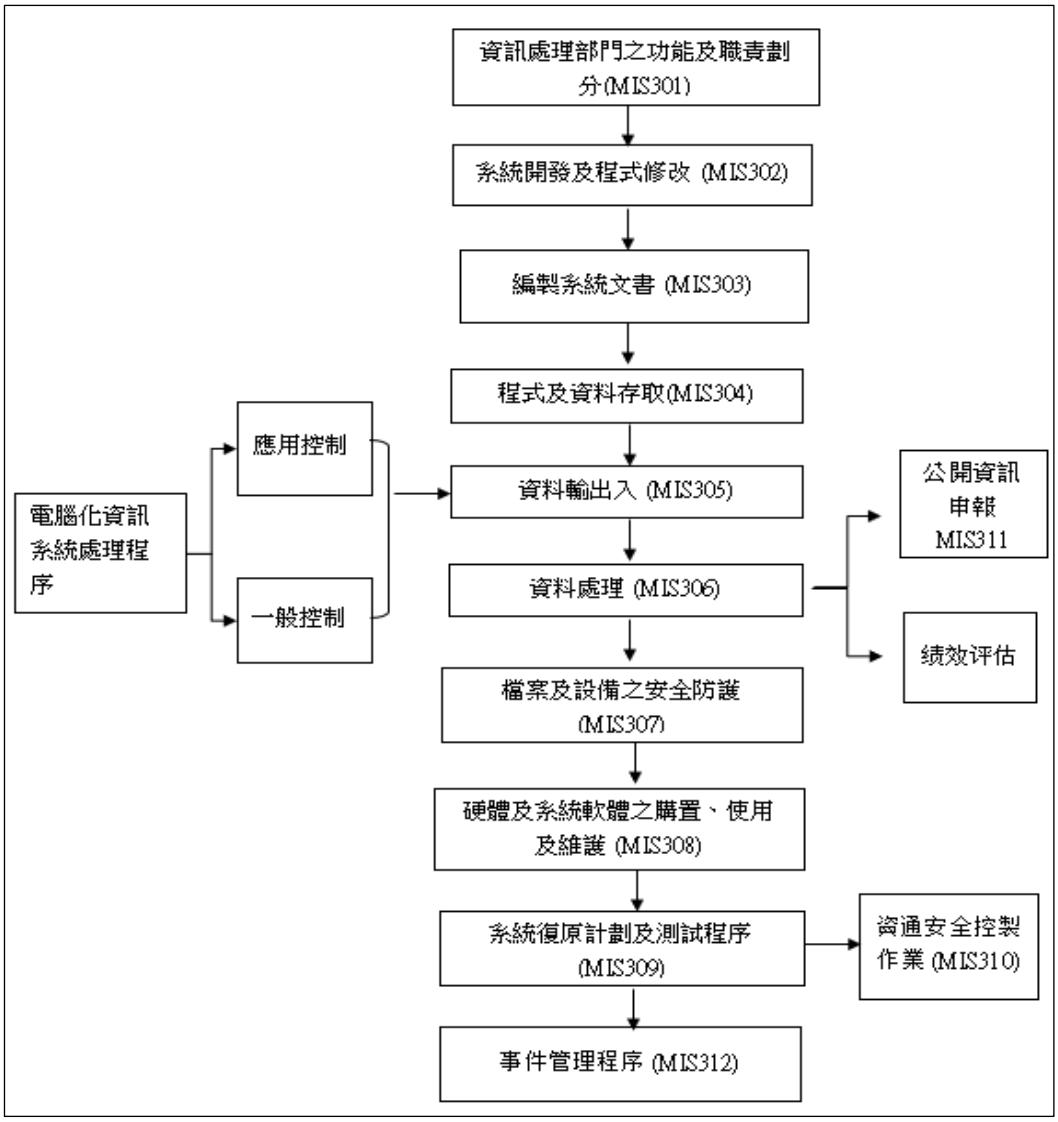
身處資訊化社會與全球化時代，人與電腦、網路的關係愈趨緊密、電子交易亦日趨普及，但也因此衍生出一些資訊安全或網路犯罪問題。惟本公司之生產與銷售並非線上即時作業系統，且公司設有資訊部，聘請相關專業人員協助管理公司的網路、主機與相關系統的權限設定，每天都會備份主機的資料，定期維護員工之電腦與安排掃毒偵測，並且加強機房各項模擬測試與緊急應變等演練以確保資訊系統之正常運作及資料保全，以降低意外或人為疏失所造成之系統中斷風險。

該部門於營運方面旨在為營運部門提供大量資料處理及查詢作業；提供營運部門所需各類報表，以簡化人工作業；減少重覆、繁雜之例行作業，以提高工作效益；配合各部門事務流程制度化以及表單格式的標準化；整合規劃全公司各部門業務所需之軟硬體設備管理及維護。於經營管理方面旨在促進各部門之協調溝通，使作業流暢及資料一致；提供各類管理資訊協助決策分析與管理，配合企業營運計劃，並協助稽核部門加強內部稽核控制，進一步提升企業競爭力。相關部門人員之功能及職責劃分如下：

資訊處理部門（MIS）	
經理	IT 人員
a. 協助公司規劃信息環境，設計，項目與執行（ERP， SFT， Payroll，FingerTech） b. 計劃公司的網絡基礎設施，確保計劃是最新的，可執行的和安全的 c. 與供應商就系統相關事宜進行溝通 d. 通過計算機信息系統協助內部控制和監控操作。確保數據的完整性和保密性。 e. 授權並跟進 IT 人員對公司硬件/軟件的需求、監控、維護和服務。 f. 系統培訓及會議 g. 系統恢復計劃和測試控制 h. 系統監控與維護	a. 辦公室的電腦，設備，軟件的管理（需求，監視，維護，服務） b. 網絡，文件共享，電郵，終端設置在辦公和生產區域 c. 數據庫備份和服務器存儲監控 d. 每日維護服務器檢查表 e. 系統監控與維護 f. 系統與電腦培訓

2. 資通安全政策

本公司編制“電腦化資訊系統處理循環（MIS cycle）”，並經董事會討論通過，以通過具體的管理方案進一步確保及強化管理資通安全。“電腦化資訊系統處理循環”敘明電腦化資訊系統處理循環內部控制流程圖中各個項目之控制作業與管理程序。例如，硬體及系統軟體之購置、使用、維護及報廢控制作業，程式及資料存取控制作業等。相關電腦化資訊系統處理循環內部控制流程圖如下：



3. 具體管理措施

為強化網路安全，資訊部採取多種網路安全防範措施，包含防火牆、防毒軟體等技術，又公司員工利用公司網路在瀏覽外部網頁時設有屏障，若是不明或惡意之網站將無法開啟鏈結。本公司內控系統中訂定有電腦化資訊系統處理相關的程序，相關的資訊使用辦法與注意事項也會以郵件方式公告予全體員工，並且資訊部也不定期會安排一些資訊安全相關的說明會，以提醒公司員工注意網路安全，宣導最新的資訊安全訊息。

綜上分析，本公司之資安風險評估層級屬於低風險。截至年報刊印日止，本公司並未發現任何重大的網路攻擊或事件、已經或可能對公司業務及營運產生重大不利影響，未曾涉入任何與此有關的法律案件或監管調查。

4. 投入資通安全管理之資源

（1）人員管理及教育訓練

A. 人員安全評估及管理
B. 員工維護資訊安全及公務機密責任
C. 資訊安全教育訓練

(2) 電腦化資訊系統安全管理

A. 電腦化資訊系統處理循環目錄
B. 電腦化資訊系統處理循環內部控制
C．資訊處理部門之功能及職責劃分
D. 系統開發及程式修改控制
E. 編制系統文書控制
F. 程式及資料存取控制
G. 資料輸出入控制
H. 資料處理控制
I. 檔案及設備之安全防護控制
J．硬體及系統軟體之購置、使用、維護及報廢控制
K．系統復原計劃製度及測試程序控制
L．資通安全控制
M．公開資訊申報
N．事件管理程序

The security risk of information technology structure and policy, specific management plans and resources invested in security risk of information technology, etc.

(1) Security risk of information technology structure

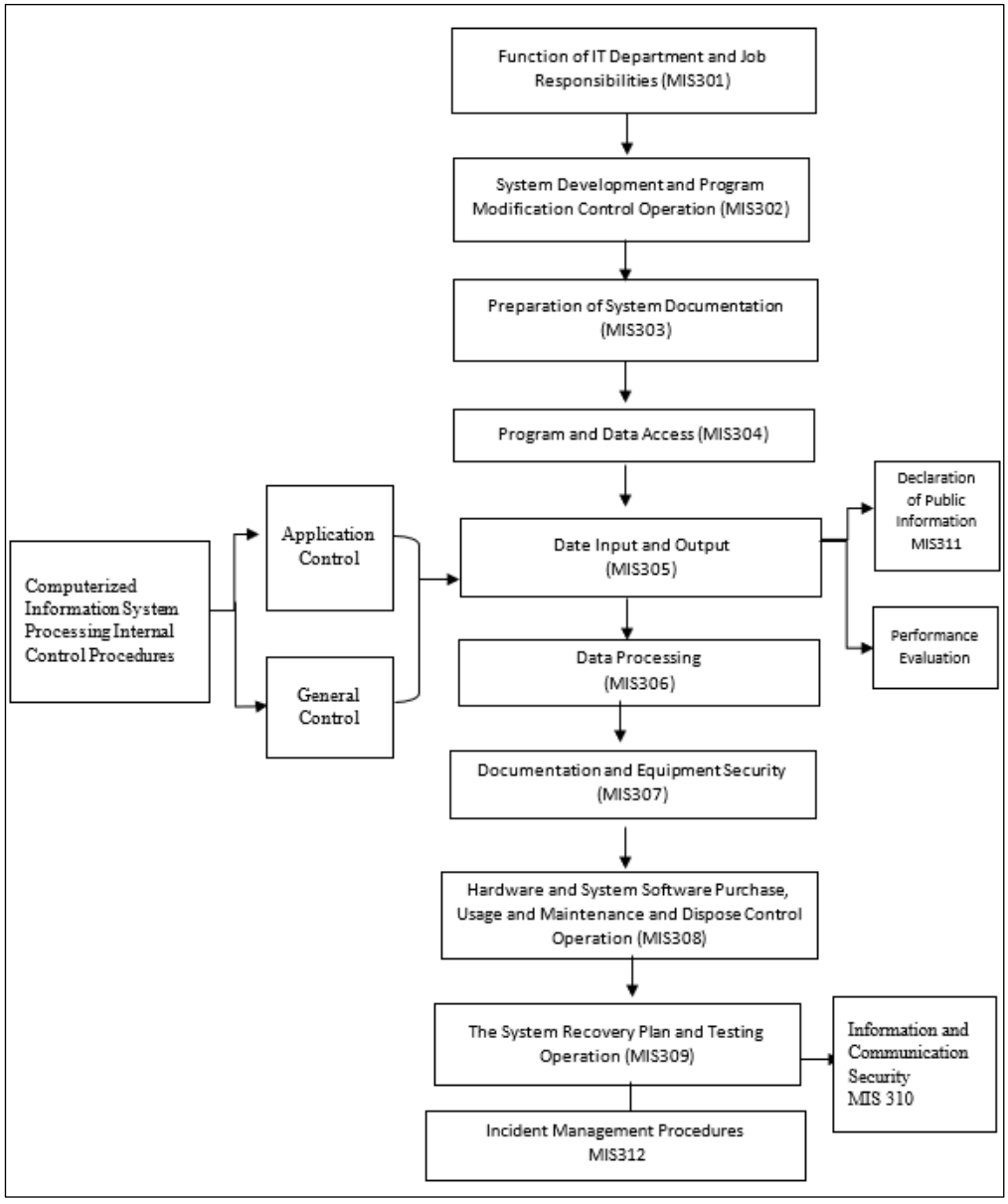
In the era of information society and globalization, the relationship between people and computers and the Internet is becoming more and more close, and electronic transactions are becoming more and more popular. However, the company's production and sales are not online real-time operating systems, and the company has an information department that hires relevant professionals to assist in the company's management network, host and related systems. Computer and arrange anti-virus detection, and strengthen various simulation tests and emergency response drills in the computer room to ensure the normal operation of the information system and data preservation, to reduce the risk of system interruption caused by accidents or human negligence.

The company has an IT department to ensure the security risk of information technology. In terms of operations, the function of the IT department is to: provide the operational department with data processing and inquiry; provide various reports required by the operation department to simplify manual work; reduce complicated and duplicated routine procedures to increase work efficiency; coordinate with other departments to standardize the transaction procedure document format. Integrate and plan the management and maintenance of all departments' required software and hardware. In terms of operation and management, it aims to stimulate coordination and communication among the departments to have a smooth operation and enhance data consistency; provide management information to help analyze and manage decisions and coordinate with the enterprise's operating plan; assist the audit department and strengthen internal audit control; and enhance the enterprise's competitiveness. The operating procedures for the personnel of the relevant departments are:

Management Information System (MIS)	
Manager	IT executive
a. Assist company to plan the information environment, design, project execution (ERP, SFT, Payroll, FingerTech). b. Plan company's network infrastructure and ensure the plan is up to date, executable and secure. c. Dealing with the vendor/ supplier for related matters about system. d. Assist in internal control and monitor the operation through computer information system. Ensure the data integrity and data confidentiality. e. Authorize and follow up with IT executive regrading requisition, monitoring, maintenance, service of hardware/software in company. f. system training & meeting. g. System monitoring and maintenance.	a. Management of the Office's Computer equipment/ software (requisition, monitoring, maintenance, service). b. Network/ File sharing/ Email/ Terminal setting in office and production area. c.Database backup and server storage monitoring. d. Update Server Checking List every day. e. System monitoring and maintenance. f. System and computer training.

(2) Security risk of information technology policy

The company has also compiled a "computerized information system processing cycle (MIS cycle)", which has been discussed and approved by the board of directors, to further ensure and strengthen the management of information security through specific management plans. The "MIS cycle" describes the control operations and management procedures for each item in the computerised information system processing flow chart. For example, hardware and system software purchase, usage, and maintenance, and disposal control operations, programme and data access control procedures, etc. The computerised information system processing flow chart is as follows:



(3) Specific management plans

The MIS Department has adopted a variety of network security precautions, including firewalls, anti-virus software and other technologies, and the company employees use the

company network to set up barriers when browsing external web pages to strengthen network security. If the website is unknown or malicious, the link will not be opened. The company's internal control system has procedures related to computerized information system processing, and we will also announce relevant information use methods and precautions to all employees by email, and the information department will also arrange some information security-related briefings from time to time. To remind company employees to pay attention to network security, and to promote the latest information security information.

The company's security risk of IT assessment is low. As of the publication of the annual report, the company has found no major cyberattacks or incidents that have or may have a significant adverse impact on the company's operations and has not been involving in any legal cases or regulatory investigations related to this.

(4) Resources invested in security risk of information technology

(1) Employee management and education training

A. Personnel safety assessment and management

B. Staff responsibility for maintaining information security and official confidentiality

C. Information Security Education and Training

(2) Computerized Information System Security Management

A. Content for Computerized Information System Processing Internal Control

B. Computerized Information System Processing Flow Chart

C・Function of IT Department and Job Responsibilities

D. System Development and Program Modification Control Operation

E. Preparation of System Documentation Control

F. Program and Data Access Control

G. Data Input and Output Control

H. Data Processing Control

I. Documentation & Equipment Security Control

J. Hardware and System Software Purchase, Usage, Maintenance and Dispose Control

K・The System Recovery Plan and Testing Control

L・Information and Communication Security

M・Declaration of Public Information Operation

N・Incident Management Procedures