一、 資通安全管理策略與架構：

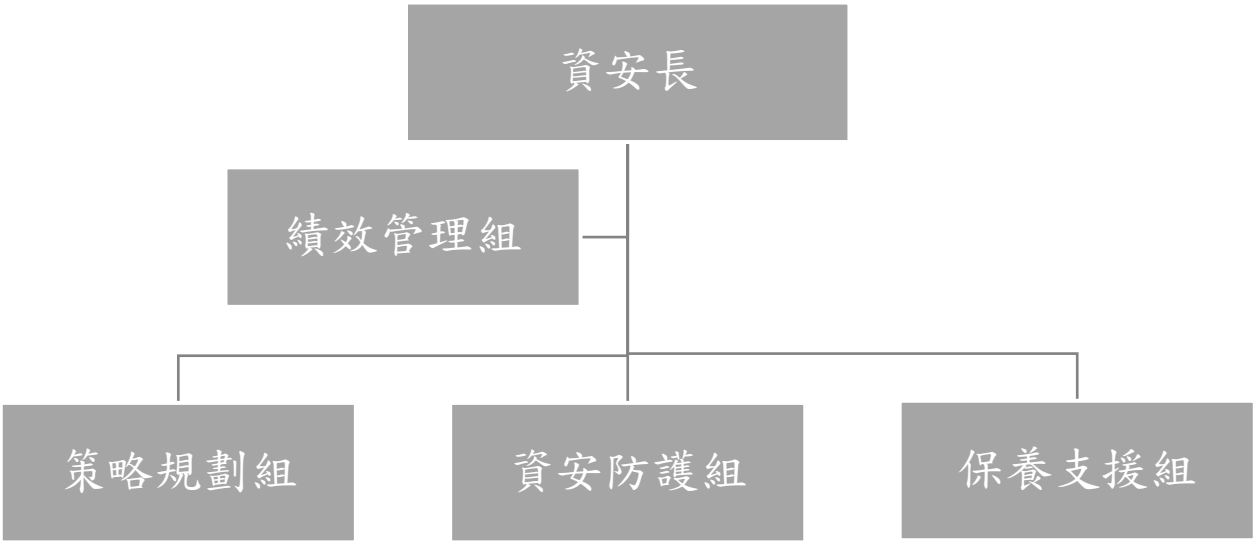
台塑石化股份有限公司於民國109年11月依「資通安全管理法」(下稱資安法)指定為「關鍵基礎設施提供者」，資通安全責任等級B級，依據資安法相關規範並酌衡本公司之業務需求依法訂定「資通安全防護計劃」，計劃內規劃依不同面向的資安管理架構(如下圖所示)，並依此建立資訊安全政策，以強化資訊安全管理，建構資訊資產之風險管理，並確保本公司資訊資產之機密性、完整性、可用性符合相關法規之要求，使其免於遭受內、外部的蓄意或意外之資安事件威脅。資訊安全政策每年配合政府法令、環境、業務與技術之變動評估檢討，其修正經公司核定後公告實施。

(一)資通安全風險管理架構

1. 公司資訊安全治理組織

本公司依資安法資通安全責任等級B級，設立「資通安全推動小組」，統籌資訊安全及保護相關政策制定、執行、風險管理與法規遵循度查核，由本公司「資安長」定期向公司會彙報資安管理成效、資安相關議題及方向。本公司總經理室負責監督治理公司資訊安全之責，依「資安法實行細則」每年辦理內部資通安全稽核，用以評核台塑石化公司資訊與網路安全管理機制及方向，並於接獲主管機關資安情資通報時，評估該情資內容採行最適當之因應方式。

2. 公司企業資訊安全組織架構



(二)資通安全政策

1. 公司資訊安全管理策略與架構

為使本公司業務順利運作，防止資訊或資通系統受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，並確保其機密性、完整性及可用性，本公司特制訂明列於「資通安全維護計劃」中的資安政策如下：

- 應遵守政府資通安全相關法規要求，如：資通安全管理法、國家機密保護法、個人資料保護法、著作權法等。
- 應建立資通安全風險管理機制，定期因應內外在資通安全情勢變化，檢討資通安全風險管理之有效性。
- 應保護機敏資訊及資通系統之機密性與完整性，避免未經授權的存取與竄改。
- 應強固核心資通系統之韌性，確保公司業務持續營運。
- 應因應資通安全威脅情勢變化，辦理資通安全教育訓練，以提高員工之資通安全意識。
- 應建立資通安全事件通報及應變機制，確保資安事件儘速妥善回應、控制損害及復原，降低事件影響。
- 針對辦理資通安全業務有功人員應進行獎勵。

2.公司資訊安全風險管理與持續改善架構

- 資訊安全之權責單位為「資通安全推動小組」，負責規劃、執行及推動資訊安全管理事項，並推展資訊安全意識。
- 本公司總經理室為資訊安全監理之查核單位，若查核發現缺失，旋即要求受查單位提出相關改善計畫並呈報，且定期追蹤改善成效，以降低內部資安風險。
- 組織運作模式-採 PDCA（Plan-Do-Check-Act）循環式管理，確保可靠度目標之達成且持續改善。

3.具體管理方案

- 本公司導入AEO資通安全管理機制及遵循「資通安全管理法」、「個人資料保護法」及相關法令執行。
- 訂定及執行「資通安全防護計畫」及通報、應變機制，並採取適當之防護措施。
- 透過資訊資產盤點有效管理資訊資產，評估各種人為或天然災害之影響，持續執行風險評鑑、應變演練據以修訂「資通安全防護計畫」，以確保核心業務可持續運作。
- 企業集團提供對外建置防火牆可阻檔一般常見的網路攻擊及E-Mail病毒控管，並提供企業網域安全監控及異常偵測。本公司各部門另訂定相關措施，諸如密碼設定、機房門禁管理、資料存取傳輸之管制、伺服器管理…等安全管理措施。
- 落實資通安全教育訓練，以提高員工之資訊安全意識。每年透過教育訓練、內部會議、電子公佈函等方式，向公司內所有人員及委外廠商進行宣導，並檢視執行成效。
- 辦理資通系統之委外建置時，考量委外項目之性質及資通安全需求，要求承攬商簽立保密切結書，並監督其資通安全維護情形。
- 資通系統變更時，須依據變更管理辦法提出申請，透過風險評估及審查程序，確保所有潛在之危害與風險已被鑑別與評估，並研擬適當防範措施。
- 為即時掌控資通安全事件，並有效降低其所造成之損害，本公司訂定資通安全事件通報、應變及演練相關機制。

- 符合「個人資料保護法」之規定加強資訊安全管理：
  - ✓ 針對寄送至企業外的郵件含有個人資料者進行控管並完整的備存保留5年。
  - ✓ 多功能事務機列印次數異常通報並將列印檔案自動備存。
- 推動「資訊安全管理系統(Information Security Management System,ISMS)」導入作業，透過管理制度之建置及人員參與實行，建構更完善之個人資料保護機制及資訊環境，為導入ISO 27001安全管理系統如下：
  - ✓ 自109年1月起著手準備製程管理核心系統驗證工作，113年7月12日順利通過艾法諾國際股份有限公司查證作業，並通過審核推薦取得ISO/IEC 27001:2022 Information Security Management Systems Certification。114年10月15日通過ISO27001：2022續評。
  - ✓ 自111年3月起著手準備泰山機房驗證工作，113年11月19日順利通過台灣檢驗科技股份有限公司(SGS)查證作業，並通過審核推薦取得ISO/IEC 27001:2022 Information Security Management Systems Certification。
- 每年接受主管機關能源局依據資通安全管理法及其子法、國家資通安全發展方案(114年至117年)、資訊安全管理系統國家標準 CNS 27001:2022或資訊安全管理系統國際標準 ISO 27001:2022、IT服務管理系統國際標準 ISO 20000-1:2018等標準，稽核本公司辦理資安相關法遵事項之落實情形，經由外部稽核本公司資通安全維護計畫實施情形，改善並強化資通安全防護工作。
- 導入安全資訊及事件管理系統(SIEM)與資安監控平台(SOC)。
- 定期委託外部專家執行紅隊演練。

4.投入資通安全管理之資源

114年本公司資訊安全措施推動執行成果:

面向	工作項目	完成時間
管理面	訂定資安政策並提交資安防護計劃	114/01/31
	實施資通系統盤點、分級、風險評鑑	114/05/21
	訂定資安事件通報機制及應變演練	114/12/24
	委外廠商(盟立自動化)資安稽核	114/06/23
	通過 ISO27001：2022 續評	114/10/15
	辦理資安業務持續演練	114/06/25
	辦理資安內部稽核	114/09/11
	辦理能源署外部稽核(桌推)	114/08/15
	召開管審會議	114/09/17
	公告限制使用危害國家資通產品	114/12/30
訓練面	員工實施釣魚郵件測試	114/06/20
	員工線上資安通識訓練及專業訓練(每人通識:3HR/年、專業 3HR/2 年)	全公司完成通識課程及專業課程。
	二年內取得資通安全專業人員證照	4 人取得證照
技術面	設立資安監控中心(SOC)及持續運作	111/05/01
	資通安全弱點通報(VANS)	114/11/17
	資安治理成熟度評估資料提報	114/09/30
	實施資通安全健診(每 2 年 1 次)	114/12/02
	實施系統弱點掃描	114/10/01
	實施系統滲透測試(每 2 年 1 次)	113/10/08

二、 資通安全風險與因應措施：：

本公司依資安法其管理措施符合主管機關所訂定「經濟部能源及水資源領域工業控制系統資安防護基準」，基準明訂定相關作法有存取控制構面、稽核與可歸責性構面、識別與鑑別構面、營運持續計畫構面等，本公司符合基準並明確實施如密碼設置的規定、帳號管理的權限、稽核紀錄的保存、端點偵測及應變機制等。