一、 資通安全管理策略與架構：

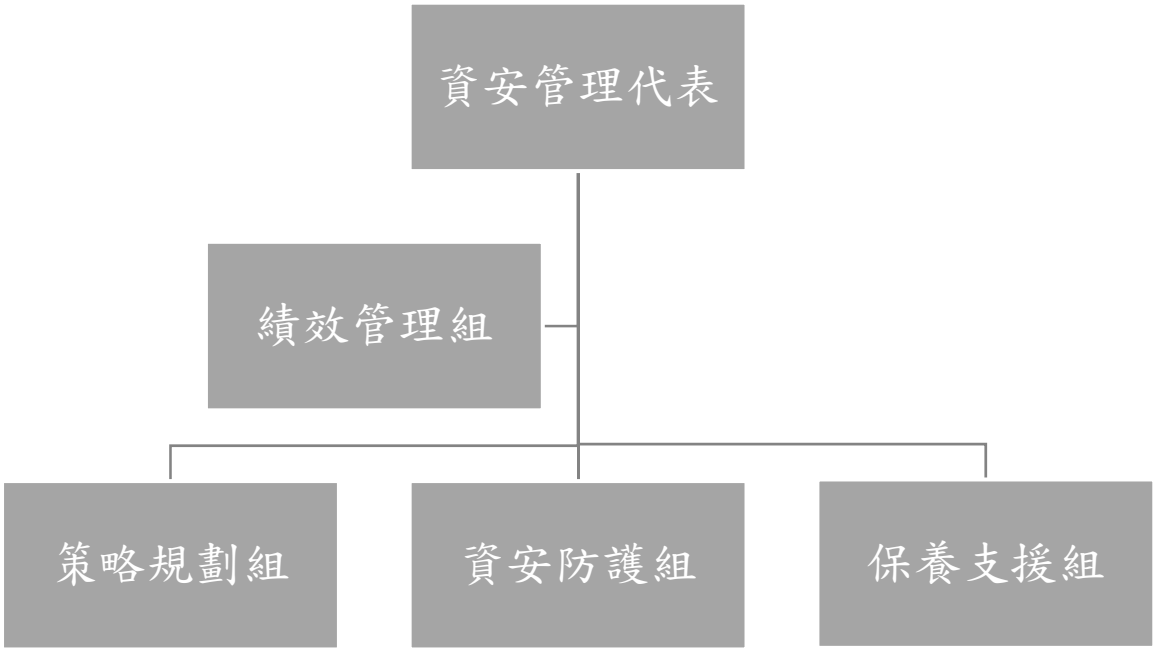
台塑石化股份有限公司於民國109年11月依「資通安全管理法」(下稱資安法)指定為「關鍵基礎設施提供者」，資通安全責任等級B級，依據資安法相關規範並酌衡本公司之業務需求依法訂定「資通安全防護計劃」，計劃內規劃依不同面向的資安管理架構（如下圖所示），並依此建立資訊安全政策，以強化資訊安全管理，建構資訊資產之風險管理，並確保本公司資訊資產之機密性、完整性、可用性符合相關法規之要求，使其免於遭受內、外部的蓄意或意外之資安事件威脅。資訊安全政策每年配合政府法令、環境、業務與技術之變動評估檢討，其修正經公司核定後公告實施。

(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「資安管理代表」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一次，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，確保機關業務持續營運。
- 應因應資通安全威脅情勢變化，辦理資通安全教育訓練，以提高本機關同仁之資通安全意識。
- 針對辦理資通安全業務有功人員應進行獎勵。
- 勿開啟來路不明或無法明確辨識寄件人之電子郵件。
- 禁止多人共用單一資通系統帳號，但24小時有人職守之OT系統除外。

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。

- 110年辦理本公司員工資通安全訓練執行情形：
  - ✓ 110年度辦理通識課程「何謂資訊安全及重大資安事件分享」3小時實體及線上學習課程，全體員工共4,429人參與。
  - ✓ 110年度辦理專業課程「工控資安管理」3小時及「工控資安國際標準」3小時實體及線上學習課程，全體員工共537人參與。

4.投入資通安全管理之資源

民國110年本公司資訊安全措施推動執行成果:

面向	工作項目	台塑石化煉油廠
管理面	訂定資安政策並提交資安防護計劃	已完成
	實施資通系統盤點、分級、風險評鑑	已完成
	完成資通安全防護基準	已完成
	訂定資安事件通報機制及應變演練	已完成
	訂定資訊委外廠商等管理制度及稽核	已完成系統盤點、風險評鑑、委外廠商等管理辦法
	辦理資安攻防演練	配合國土安全辦公室於110/11/25進行資訊安全攻擊及人為破壞等二項應變演練
	辦理資安外部稽核	配合經濟部10/28資安稽核並提交煉油廠稽核改善報告
訓練面	員工實施釣魚郵件測試	110/01/E已完成
	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)	全公司通識課程已完成人數4,429人，專業課程已完成人數537人。
	二年內取得資通安全專業人員證照	2人取得證照
技術面	設立資安監控中心並實施安全健診	已委外安碁公司輔導認證，並設立監控中心實施安全健診
	導入國際標準完成第三方之認證	

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。