**風險分析與管理**是**資訊安全**與**個資管理**的核心與最重要的工作之一，它必須與單位之日常管理及業務流程與活動相結合，而風險管理之要旨在於透過**系統化的機制**，經由事先建立之評定標準及方法，針對單位業務流程**鑑別資訊資產**，並**分析及評估**其可能面臨之**風險**（如威脅、弱點，業務面、法規及資安要求），以採取適切之**處理措施**（如避免、移轉、降低或接受等），制定適切之風險管理計畫，及對各項風險加以監控。

目前有四份國際標準(**ISO27001**、**ISO20000**、**BS25999**及**BS10012**)的核心要求均需要建立與執行風險管理機制，然而對企業而言還是不夠，例如**ISO27001對風險評鑑僅有提供原則性的要求內容(what)，卻沒有提供實務性的指南內容(How to do)**，而國際標準ISO27005：2008正好可以提供**技術性的支援**，為組織的資訊安全風險管理提供實務上的**執行指南(Guideline)**。

由於ISO27005標準整合了四個管理系統對**風險評鑑**的要求，因此以ISO27005：2008版（Information Technology–Security Techniques – Information Security Risk Management，資訊技術–安全技術–資訊安全風險管理）的實作指引或要求，來作為設計與輔導基礎的實務訓練課程，將是最能滿足各單位需求的訓練方案。

目前，「國防部及其所屬A、B、C及D級單位」以及「空軍司令部及其所屬A、B及C級單位」，共61個單位，均以部份範圍導入與建置ISO27005：2008版的要求，並要求以「一級輔導一級」與陸續擴大單位範圍的方式，分階段完成全組織導入與建ISO27005風險管理的工作。

資策會推出「ISO27005資訊安全與個人資料風險管理認證班」，透過說明講解與實作研討搭配的方式，闡述ISO27001 ISO20000、BS25999、BS10012及ISO27005之系統化風險管理的內涵，同時結合資訊安全管理（ISMS）、資訊技術服務管理（ITSM）、營運持續管理（BCMS）、個人資料管理（PIMS）及個人資料保護法、與其對風險評鑑的要求，教導風險評鑑的步驟，練習風險評鑑之詳細執行細節，以培養風險評鑑小組人員之建置與維運能力。此外，全程參與課程並通過考試者，將可於課程結束後獲頒國際驗證證書。