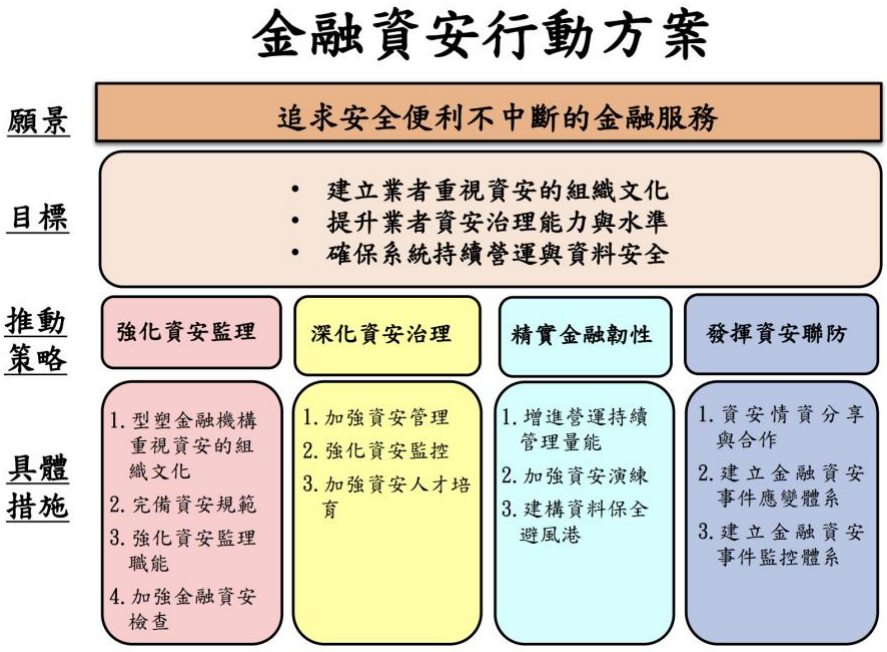
因應金融創新科技，改變營運模式的資安新思維

如何提供穩定不中斷的金融服務，更保護金融消費者的財產與隱私

金管會於 109 年 8 月 6 日推動『強化金融資安行動方案』，旨在提供民眾安心便利、穩定不中斷的金融服務。

該計畫之推動以二至四年為期，保護金融消費者的財產與隱私，資安行動方案從四個面向切入：強化主管機關資安監理、深化金融機構資安治理、精實金融機構資安作業韌性、發揮資安聯防功能 (架構圖如下圖一)，亦提出 36 項資安措施。



更從二方面提供指引功能：

(一)現有資安再優化精進措施：如檢視資安風險因子與金融監理工具連結之有效性、增修訂新興金融科技資安規範等。

(二)規劃資安新思維方向：如推動一定規模金融機構或純網銀設置資安長，強化金融資安韌性，建立資安應變體系。

本篇將特別著重於「新興金融科技資安規範」，提出具體行動方案與建議：

依據金融資安行動方案執行措施表內資訊，針對構面一、強化資安監理中，增修以下兩個工作小項，提出工作說明重點：

構面	工作項目	工作小項	執行措施	執行期程	說明
一、強化資安監理	2.完備資安規範	2.2 增修訂新興金融科技資安規範	增修訂資安自律規範，納入行動應用程式(APP)、雲端服務、開放銀行 OPEN API、物聯網、網路身分驗證(eKYC)等新興科技安控規範。	二年	金融機構已逐步運用新興科技發展金融創新業務，為金融機構運用新興科技時，能預先考量相關風險因子兼顧資安防護，爰規劃配合金融科技的發展與金融業務的陸續開放，就行動應用程式(APP)、雲端服務、開放銀行 Open API、網路身分驗證(eKYC)等當前關注議題增修資安自律規範，同時也持續關注未來環境變化進行滾動檢討。
		2.3 增修訂供應鏈風險管理規範	增修訂資安自律規範，納入核心資訊系統供應商及跨機構資訊服務之風險評估及查核等管理機制	二年	因應近期以委外廠商、軟硬體供應商等為跳板攻擊漸增之趨勢， G7 及美國、歐盟金融監理機關均提出應加強第三方服務供應商之風險評估與委外管理；我國資通安全管理法施行細則亦揭示委外辦理資通訊系統之建置、維運或資通服務之提供，於選任及監督受託者時應注意事項，行政院也已將供應鏈風險管理列為重點項目。因應金融服務委外及跨業之型態發展(如雲端服務、行動支付等)，為強化金融供應鏈體系之風險評估與管理，爰規劃增修訂資安自律規範，納入核心資通訊系統之軟硬體供應與維運商、跨機構合作夥伴等之風險評估、邊際防護及委外稽核等。

就上述兩項規範，格外著重於「新興科技安控」與核心資訊系統供應鏈之風險評估管理要求，於此，CyberArk 身分安全平台中，提供以下安控與稽核建議：

一、執行與落實零信任安全存取：

在創新金融發展下，多元化的新興科技持續導入，從過去的邊際防護到縱深防禦的做法，以不足以抵禦來自於多方的攻擊與入侵，為了建構強而有效的核心與交易系統防護控制點，唯有執行「零信任的身分識別」才是關鍵，具體可執行的建議如下：

- Human Identity：ID + Password + MFA + PAM → Login success
- Machine Identity：UID + Password + AP Secretless Broker → Authentication successful

二、建立供應鏈與維運商零信任安全存取：

- 無論供應鏈或維運商自內部進行連線操作時，必須是由廠商以個人帳號進行多因子身分驗

證，確保登入前的身分驗證安全。

- 若供應鏈或維運商自外部網路連入系統進行維運時，必須避免在遠端連線設備上輸入帳密(尤其是特權帳密)，且採行更加嚴謹的「生物識別驗證機制」，確保遠端連入時的驗證，並且建立外網連線的 Terminal gateway，完整留存系統維運時的操作記錄與影像擷取，作為日後稽核與備查。

預期效益：

透過上述的建議與作為，除可落實資安行動方案的要求外，共創以下「金三角」目標：

1. 金融機構：

   健全資安管理制度，提升資安防護能量；並得以在資通安全的基礎上，運用新興科技發展金融業務，提供消費者更安心、便利與多樣之金融服務，讓您完全無後顧之憂、勇往直前、再創營收佳績。

2. 金融產業：

   透過供應鏈與維運商的安全存取與管控機制，建構金融資安聯防體系，厚植金融體系防禦能量，營造安全的金融服務發展環境，奠定金融科技創新及發展之根基。

3. 金融消費者：

   安心使用更加便利、不中斷的數位化金融服務，並在保障財產與隱私安全情況下，獲得金融消費者更高的評價與服務滿意度提升。

[撰文者：力悅資訊 王甯申]

更多方案內容，請參閱以下官網資訊：

CyberArk https://www.cyberark.com/zh-hant/

力悅資訊 http://www.cyberview.com.tw/cyberark/