金融監督管理委員會因公出國報告
出國類別：其他(國際研討會)

東南亞中央銀行(SEACEN)研訓中心舉辦銀行業資訊風險暨相關安全機制(Technology Risks in Banks, including Cybersecurity)訓練課程心得報告

服務機關：金融監督管理委員會銀行局
出國人姓名職稱：楊稽查光偉
出國地區：菲律賓馬尼拉
出國期間：106 年 10 月 22 日至 106 年 10 月 27 日
報告日期：107 年 1 月

目錄

壹、前言

本課程為東南亞國家中央銀行研訓中心(The South East Asian Central Banks (SEACEN) Research and Training Centre)與菲律賓央行聯合舉辦銀行業資訊風險暨相關安全機制(Technology Risks in Banks, including Cybersecurity)之訓練課程為期 5 天，在菲律賓馬尼拉舉辦。參加學員共 46 人，分別來自汶萊、柬埔寨、香港、印度、印尼、寮國、馬來西亞、蒙古、緬甸、尼泊爾、巴布亞新幾內亞、菲律賓、斯里蘭卡、泰國、越南及我國等 16 國家之中央銀行及銀行監理機關之人員。

本次課程講座主要由 SEACEN Centre 邀請專業講師授課，並由各國學員簡報及分享其機構有關資訊與通訊科技(information and communication technology, ICT)風險評估、風險管理品質及網路安全之經驗，再透過分組討論個案研討等方式進行。

課程目的係提供各國中央銀行與金融主管機關與會代表們，在監理審查及評估流程(Supervisory review and evaluation process, SREP)前提下，對 ICT 的評估能建立一個通盤的架構、程序及方法。

貳、課程內容摘要

一、 背景說明及基本認識

(一)背景說明：

1.近年來因科技的迅速發展，已徹底顛覆及重新形塑以往的金融服務型態，而銀行為避免被淘汰，並考量下列原因後，均採取擁抱新科技的態度：營運的效率性、電子(行動)商務的發展、客戶對於快速且隨時進行交易的需求增加，及希望將觸角延伸至以往非銀行客戶的普羅大眾等。

2.隨著科技的運用，資訊安全的威脅對銀行業日趨嚴重，而資訊安全的威脅大概能從遭遇攻擊的對象不同，區分為兩個層面：

	攻擊「金融機構基礎設施」	攻擊「客戶終端設備」
威脅	DDos、IP 詐騙(spoofing)、網址嫁接(pharming)、資料竊取及 SQL 攻擊等	釣魚網站(phishing)、使用者未更新(Drive-By Download)、鍵盤側錄(key logging)及身分資料竊取等
衝擊	營運中斷、機敏資料外洩、系統風險、財物損失及聲譽風險	未經授權轉帳、個資外洩、對金融產業失去信心

(二)基本認識

1.依據歐盟銀行監理機構(European Banking Authority, EBA)的 SREP 前提下，ICT 風險評估應列營運風險[1]評估項下，惟倘 ICT 風險過鉅時，可將 ICT 風險評估另外作為獨立風險進行評估項目。

2.當主管機關將銀行的ICT風險置於營運風險項下進行

[1] EBA's Guidelines on common procedures and methodologies for the supervisory review and evaluation process (SREP).(19 Dec 2014)

評估時，至少應包含下列事項：

(1)營運持續性計畫及測試的有效性。

(2)對於系統及資料庫的內部及外部安全性。

(3)相關報告、風險管理及財務會計等數據資料的正確性及完整性。

(4)應變的敏捷性。

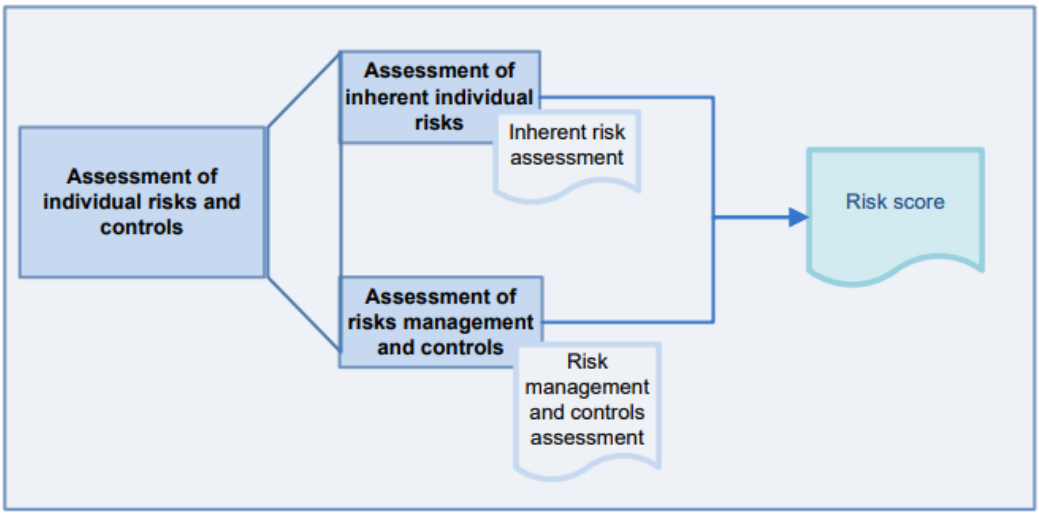


Figure 2: Assessment workflow for risks to capital- EBA's Guidelines on common procedures and methodologies for the supervisory review and evaluation process (SREP)

3.ICT 風險的管理應由上而下，董事會、CEO 及相關高階經理人應對資訊風險管理及消費者保護共同承擔高度責任，方生成效。

4.按 EBA 所發出對 ICT 風險評估指引的最終報告[2]，金融主管機關應注意下列事項：

(1)發現新種型態的資安風險或金融機構增加 ICT 服務的委外時，應對 ICT 風險評估提出特殊的指引。

(2)就金融機構高階管理層對內部監理及機構控制進行評估。

(3)就金融機構所訂 ICT 策略與金融機構經營模式的相當性進行評估。

[2] EBA's Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation process (SREP).(11 May 2017)

(4)對金融機構 ICT 風險的曝險情況及控制措施進行評估，並就前開評估所發現的風險事實給予不同權重及評分後，產出相關報告。

二、 ICT 之風險治理與策略

(一)金融主管機關應以風險基礎為原則之監理(risk-based supervision approach)方式，並透過風險辨識、評估、監測及控制的循環過程，督導金融機構建構滿足下列要件的 ICT 風險管理架構：

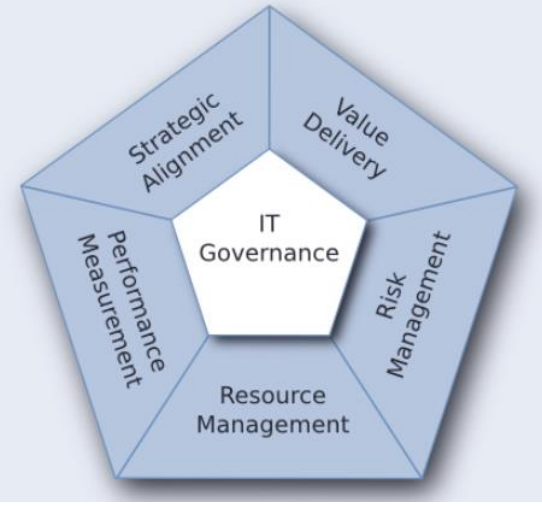
1.正確辨識、瞭解及監控 ICT 風險。

2.將 ICT 風險管理納入機構整體風險管理(Enterprise Risk management)的一環。

3.評估 ICT 風險可能造成的衝擊與機構之風險胃納(risk appetite)及承受度。

4.發展出適當的風險控管策略。

(二)按 EBA 所發出對 ICT 風險評估指引的最終報告，金融主管機關在監理金融機構之 ICT 治理及策略時，應評估金融機構總體治理(general governance)及內部控制架構能正確涵蓋 ICT 系統及相應而生之風險，且金融機構的管理階層能否適當處理可能發生之問題。



三、 ICT 風險辨識及分類

(一)金融機構進行 ICT 風險辨識時，應找出主要的 ICT 風險，瞭解 ICT 實體設備與其在組織運作之環境，辨識出關鍵系統與服務，以及影響 ICT 風險概況之因素。關鍵系統的判別標準如下：

1. 支援核心的商業營運及分銷通路(distribution channels)。
2. 支援治理流程(governance processes)及機構運作之重要功能。
3. 屬於法律規定或監理合規要求。
4. 處理或儲存機敏性資料。

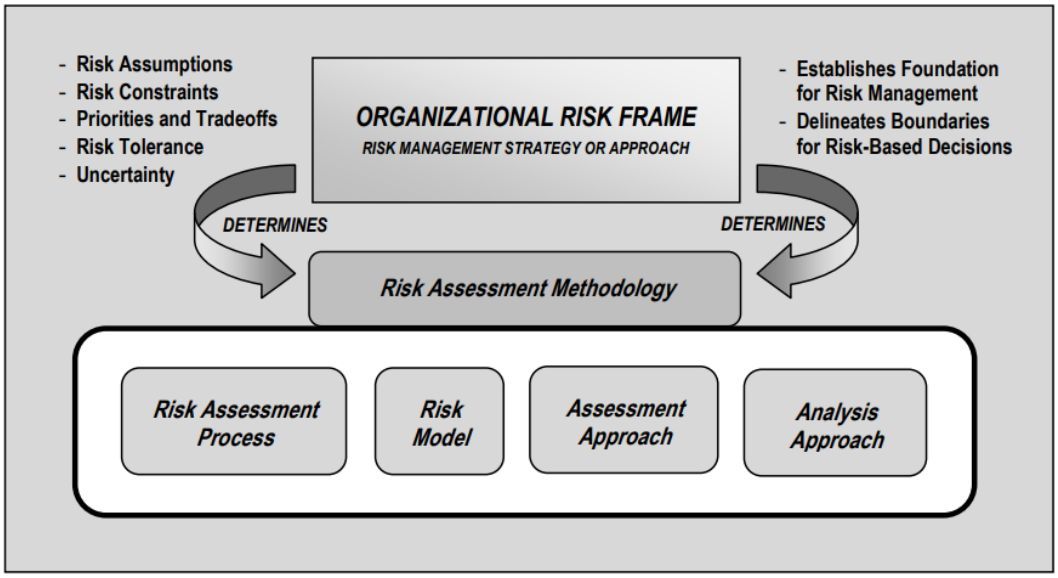


Figure 2: RELATIONSHIP AMONG RISK FRAMING COMPONENTS.- NIST's Guide for Conducting Risk Assessments.-

(二)ICT 風險主要可分為 5 類：

1. 系統與資料的效能及可用性受到衝擊之可用性與持續性風險(IT availability and continuity risk)。
2. 系統及資料未授權存取之安全風險(IT security risk)。
3. 系統轉換時失控之轉換風險(IT change risk)。
4. 系統儲存與處理資料不完整、不正確或資料跨系統間

不一致之資料完整性風險(IT data integrity risk)。

5.第三方提供系統或相關服務對機構效能和風險管理產生衝擊之委外風險(IT outsourcing risk)。

(三)另按 EBA 解釋,「資訊風險分類學(IT Risk Taxonomy)」係指藉由不同的特定(non-exhaustive)資訊風險類型案例，協助他人能對各類主要類型資訊風險達成一致性的理解(uniform understanding)。

(四)例如 2013 年 12 月蘇格蘭皇家銀行(RBS)因系統當機造成超過 1 百萬的客戶無法取款或支付款項，且電子(或行動)銀行也同樣無法進行交易，究其主因，係該行(1)未對資訊系統投入足夠資金(under-investment in technology)，並將關鍵系統委外予印度；(2)使用過時且難以更新的系統程式(outdated and complex patchwork of system)，致該行花費近 28 天的系統恢復期。而由前開案例觀之，RBS 未能有效識別關鍵核心系統，並管控 ICT 風險中的持續性風險及外包風險。

四、 ICT 風險分析與稽核

(一)金融機構經過風險導向分析方式進行風險辨識[3]後，應依金融機構之實體環境、商業作業流程及業務性質、潛在威脅發生的關聯性等，辨識固有風險(inherent risks)，並按固有風險發生之可能性及對營運衝擊之嚴重性進行風險評分後，進行分級。

(二)營運的衝擊嚴重程度應判斷風險發生時，對金融機構造成的財務衝擊性、潛在的營運中斷影響性、潛在的

[3] 現行風險分析方法論，包含威脅導向分析(threat-oriented)、資產(衝擊)導向分析(asset/impact-oriented)及弱點導向分析(vulnerability-oriented)等分析基礎，而威脅導向分析主要應先識別威脅的來源及相關情事，並專注於威脅情事之後續發展、衝擊及威脅事件的弱點分析等。P15,Information Security-Guide for Conducting Risk Assessments from NIST Special Publication 800-30(Sep 2012)

聲譽衝擊性、合規衝擊及是否影響達成經營策略目標。

(三)金融機構將固有風險分配於所屬 5 大風險分類中，利用辨識、保護、偵測、回應及復原等 5 大功能，找出相對應可落實之控制，如辨識網路或外部 ICT 攻擊屬安全風險，保護控制如防火牆，偵測控制如資安監控中心，回應控制如有效之事件處理，復原控制如災害回復等。

(四)基於風險導向，ICT 稽核包含風險評估、稽核規劃、稽核工作情況、稽核報告、回饋監控之循環程序，ICT 稽核為促進穩健 ICT 控制、確保當稽核與控制不足時能及時解決、通知董事會及管理階層等關於 ICT 風險管理落實之有效性。

五、 ICT 風險控管

(一)金融機構建立 ICT 風險治理策略並進行風險範圍的定義，進行 ICT 風險辨識及分類，及 ICT 風險分析後，應採取 ICT 風險管控措施，以消除、避免或移轉 ICT 風險。

(二)以泰國中央銀行對 ICT 風險的控管機制為例，說明如下：

	風險情事	可能的控管機制
可用性與持續性風險	1. 缺乏財務資源。 2. 軟體/硬體當機。 3. 無效的商業持續計畫(BCP)及災害復原計畫(DRP) 。 4. 惡意軟體攻擊。	1. 建立充足人員及系統的財務資源計畫。 2. 購置備援系統/主機及進行演練。 3. 有效的偶發事件處理機制、災害復原計畫及完善的內部溝通管道。 4. 惡意軟體的監測及預警機制。
安全風	1. 外在的 ICT 攻擊。	1. 防火牆、入侵預防系統(IPS)、備

	風險情事	可能的控管機制
險	2. 不充分的內部及實體ICT資料存取控管機制。	援及演練。 2. 導入進階持續性滲透攻擊(Advanced Persistent Threat, APT)或安全營運中心(Security Operations Center, SOC)、資料外洩防護(DLT)等相關監控及預警機制。
轉換風險	1. 對ICT轉換的控制不充足。 2. 不充足的系統更新管理及生命週期管理。	1. 明確的職責系統分工(segregation of duty)及系統轉換監控機制等。 2. 存取權限管理、系統更新管理(patch management)。
資料完整性風險	1. 失能的ICT資料處理及程序。 2. 不完善的資料管理架構、流程及索引(data dictionaries)。	1. 建立(或由專業機構協助建立)妥善的資料庫架構及相關資料處理程序。 2. 使用數位簽章、資料存取監控與預警機制。 3. 存取權限管理、資料加密。
委外風險	1. 受委託的第三方機構未建置完整的復原機制。 2. 對受委託機構不建立完善的監管機制。	1. 瞭解整體數位供應鏈的風險，並適當的使用多家系統服務商。 2. 建立網路權限控制機制(network access control)。 3. 對ICT的委外建立管理機制及指引。

六、 ICT 風險評鑑

(一)金融機構於充分瞭解資訊安全環境並辨識固有風險，再完成風險分析並採用適當的 ICT 風險管理及控制機制後，將針對剩餘的淨風險進行評分及分級。

(二)以菲律賓中央銀行對 ICT 風險評分為例，說明如下：

1.金融機構應評鑑範圍至少包含 3 大部分：

(1)ICT 治理：

a. ICT 監督與作業管理：包含資訊架構及查核；資訊策略、程序及標準；人員的適格性及訓練；資訊系統的管理機制；針對資訊營運、委外廠商及電子銀行的相關控制措施等。

b. ICT 風險管理：建構資訊風險管理流程並書面化一切評估標準，如風險辨識、評估、管理及監督措施等。

(2)ICT 風險的控制設計、落實與監控：包括資訊安全(information security)、系統發展與整合(development and acquisition)及營運持續性(business continuity)。

(3)ICT 稽核與法遵：資訊稽核架構、有相當專業及經驗的稽核人員、資訊內部控制及內部稽核計畫、監理及追蹤活動、資訊政策之合規流程等。

2.依前開範圍檢視固有風險屬於的資訊程度(IT Profile)態樣：

(1)複雜(complex)：金融機構將科技廣泛運用於關鍵商業流程、金融商品跟服務；金融機構擁有廣大的通路且各類數位金融產品；商業策略主要著重於提供資訊平台且數位創新服務；積極利用新興科技等。

(2)適度(modrate)：金融機構會運用科技於分行通路及資訊架構等，但運用之強度及範圍不若複雜態樣；會將資訊系統及科技融入營運模式中，但主要作為輔助傳統金融商品及服務；僅提供基礎的電子商品及服務給部分的客戶。

(3)單純(simple)：金融機構很少利用科技方式與客戶或其他機構互動；資訊運用及系統各自獨立且很少將科技運用於金融商品或服務；資訊部門人員及使用科技的客戶很少。

3.中央銀行針對風險評分之方式如同 CAMELS，對金融機構進行綜合評分，共分 4 級，由高至低分別為 4(強健)、3(滿足)、2(低於滿足)到 1(缺乏)。

(三)就評鑑範圍的不同項目，依照各項目的資訊程度及評分，配合前述風險分析進行分類，評斷固有風險經控制後所得之風險等級，再據以決定是否監理及應施予的監控強度。

	Inherent Risk (IT Profile)		
IT Rating	**Complex**	**Moderate**	**Simple**
4	Moderate Risk	Low Risk	Low Risk
3	High Risk	Moderate Risk	Low Risk
2	High Risk	Moderate Risk	Low Risk
1	High Risk	High Risk	Moderate Risk

叁、心得及建議事項

一、 金融主管機關對金融機構的 ICT 管理由上而下貫徹：

依照 SEACEN 的講師及新加坡、泰國及菲律賓等國家中央銀行的經驗分享，金融機構對 ICT 的管理及策略應由最高階的董事會及高階經理層級，逐漸向下延伸至各部門及人員，因為只有具決策權層級人員的重視，再透過強而有力的領導方式，訂定正確的 ICT 風險策略及治理，檢視機構內部制度、人員、財務是否有不足之處，持續落實管控機制及檢討修正，才有可能真正建立資訊安全管理強健的金融機構。

二、 金融主管機關應善用外部專家學者資源及資安標準機制：

(一)鑒於金融科技的快速發展，與會各國中央銀行代表無論於研討會議中或私底下討論時，多表示針對資訊安全人才均處於人力短缺的情況[4]，且雖然各國均已採內部培訓或外部招募方式，希望積極補充人才缺口，卻也都承認各國資訊安全人才的數量、素質及經驗與預設標準頗有落差。

(二)針對此普遍的資安人才缺口問題，與會的專業講師表示，資深且具經驗的專業資訊安全人才之薪酬較高，通常非各國金融主管機關所能負擔，故主管機關較可行的方式係於制定相關資安法規時，除要求金融機構應取得國際專業資訊安全認證機構之認可外，應定期要求專業會計師事務所之資訊安全技術部門等專業資安檢測機構向金融機構進行滲透測試、黑箱測試等資

[4] 除印度央行代表表示因該國資訊專才人數較充足，且該國重要銀行數目較少，故實務上係由中央銀行內部資訊人員直接測試該國銀行的 ICT 管理是否足夠，如與會代表所處部門將直接對銀行進行弱點測試，找出銀行的資訊系統弱點後，要求銀行進行補強或系統更新。

安檢測，藉由外部專業機構協助填補主管機關資安人力資源不足的缺口。

三、 金融主管機關應注意金融機構將資訊軟、硬體委託他人處理之風險：

金融機構為降低資訊系統成本，通常會將部分資訊軟、硬體委託他人協助處理，而隨著科技的進步，近年來金融機構也開始思考將資料庫委外予維運成本較低的 google 或 amazon 的雲端資料庫，但前開雲端資料庫營運商均不同意金融主管機關進行實地檢查(on site investigation)，故各國目前針對是類委外案件均採較為謹慎的態度[5]。另與談專業講師提醒主管機關即使同意金融機構將資料處理委託予雲端資料庫營運商處理，應委託予安全性較高的私有雲(private cloud)而非公有雲(public cloud)，且不應涉及客戶個人資料[6]。

肆、結論

科技的發展刻正快速改變金融產業面貌，新興科技與技術之運用雖為金融機構帶來正面的影響，如降低金融機構營運及人力成本、提供客戶更全面且快速的服務，卻也同時伴隨著潛在的威脅，如孟加拉中央銀行及遠東銀行的 SWIFT 資安事件、第一銀行 ATM 遭駭事件等。

觀察國內外發展趨勢，金融科技存在的價值並不僅止於創造，而是在於融合，金融科技必須發揮與結合「金融」與「科技」各自的特色及專長，才能長久共存。基

[5] 如大陸、澳洲、泰國及印尼之金融主管機關均不同意金融機構將客戶個人資料委託至雲端資料庫的營運商，而歐盟雖允許金融機構使用雲端資料庫，但建議應使用私有雲。

[6] 金融機構如擬將客戶個人資料委託至雲端資料庫營運商，亦應由金融機構進行自行加密後方可上傳儲存，惟實務上金融機構加密客戶個人資料上傳後，再於交易時下載加密資料自行解密之程序，所耗時間過長而影響交易進行，故仍不可行。

此，金融主管機關除鼓勵金融與科技業者積極發展金融科技創新，並擁抱科技發展的好處外，同時亦重視金融科技發展下的風險控管及民眾權益保護，認為必須在「負責任創新(responsible innovation)」的概念下推動金融科技創新，才能保護消費者權益、落實風險控管，讓金融科技的推動兼顧效率、安全及公平。