出國報告(出國類別：其他）

SEACEN
「銀行科技風險(包括網路安全)」
訓練課程出國報告

服務機關：中央銀行
姓名職稱：李瑞杷(副處長)、李典運(辦事員)
派赴國家：菲律賓
出國期間：106 年 10 月 22 日至 10 月 28 日
報告日期：107 年 1 月 10 日

摘要

隨著科技進步及環境競爭，金融機構為提高獲利、降低營運成本、提升作業效率以及提供客戶更方便的服務，對電腦、資訊與通訊等科技依賴度日益趨增，進而重新塑造金融服務營運模式，如網路銀行、行動支付、大數據、機器人理財等，該等科技之使用幾乎已滲透至金融機構內部各角落。惟近些年來，金融之資訊安全事件與網路犯罪新聞逐漸增多，且造成金額損失以及對客戶影響層面亦趨嚴重，如果全球性重要金融機構或者一國之金融體系受到嚴重網路攻擊，導致資訊系統癱瘓、運作停擺或鉅額損失，引發全球系統性風險亦不無可能。因此，為維護銀行體系能持續穩定擔任金融中介之重任，在此類風險事前防護與事後復原之管理與實踐成為現今金融監理單位與金融機構著重的課題，為讓會員瞭解當前該類風險管理之發展與應用，東南亞國家中央銀行聯合會(The South East Asian Central Banks, SEACEN)開立本次課程，進行會員間經驗分享與知識學習。

本次訓練課程探討銀行科技風險(包括網路安全)，並無涉及資訊與通訊科技(information and communication technology, ICT)相關技術，主要著重於 ICT 之風險監理與範疇、風險辨識及分類、風險分析、控制與稽核，以及風險評估與控管策略等相關風險管理程序與控制評估議題，課程講授內容大致參照歐美金融管理機關於 ICT 風險制定之指導方針與評等方法，依制定目的分成可用於金融機構自評或給予監理單位參考使用。

本報告共分 5 個章節，除前言外，第貳章簡介歐洲銀行管理局(European Banking Authority, EBA)監理審查評估程序下之 ICT 風險評估指導方針，第參章說明美國聯邦金融機構檢查委員會(Federal Financial Institutions Examination Council, FFIEC)之網路安全評估工具，第肆章為課程內容，最後第伍章為心得與建議。

目　次

表

圖

壹、 前言

「銀行科技風險(包括網路安全)」訓練課程係由 SEACEN 與菲律賓央行(Bangko Sentral ng Pilipinas, BSP)共同舉辦，於民國 106 年 10 月 23 日至 27 日在菲律賓馬尼拉舉行，為期 5 天。本訓練課程與會學員共計 46 位，分別來自各國央行及金融監理單位等 17 個機構，課程講師由 SEACEN 邀請專家與菲律賓央行代表擔任，大部分授課內容由菲律賓央行分享其在 ICT 風險監理架構與實踐之經驗。

ICT 已成為發展與支援銀行服務的一個關鍵資源，ICT 系統不只是機構策略的重要實現條件，全部銀行業務程序與服務通路幾乎由其構成，核心業務資料亦為支援自動化控制環境之基礎，因此 ICT 系統與服務在機構營運成本、投資與無形資產也占有重要比例。再者，從策略觀點來看，技術創新在銀行業務扮演決定性角色，以此為競爭優勢，並以新產品的開發，促成價值鏈再造與最佳化。隨著 ICT 對銀行產業重要性增加，同時也伴隨其他問題，如網路犯罪、網路恐怖主義和網路風險的浮現，以及對第三方和 ICT 服務外包依賴度增加所衍生的問題等。

由於 ICT 於金融機構的運作扮演重要角色，其產生的風險可能影響金融機構長期經營與生存，甚者可能造成系統性衝擊，因此部分金融監理機關，如歐洲銀行管理局(EBA)與美國聯邦金融機構檢查委員會(FFIEC)等，致力於 ICT 與網路安全之風險管理與評估，制定基本標準評估程序，提供監理單位評估金融機構 ICT 風險、與金融機構自行管理評估 ICT 風險之參考。

本次課程主要就上述兩個機關對 ICT 與網路安全之風險管理與評估之架構發表之文件進行講述，以下內容將對 EBA 及 FFIEC 發表之文獻先進行解說，而後再對本次上課內容進行說明。

貳、 EBA 監理審查評估程序下之 ICT 風險評估指導方針

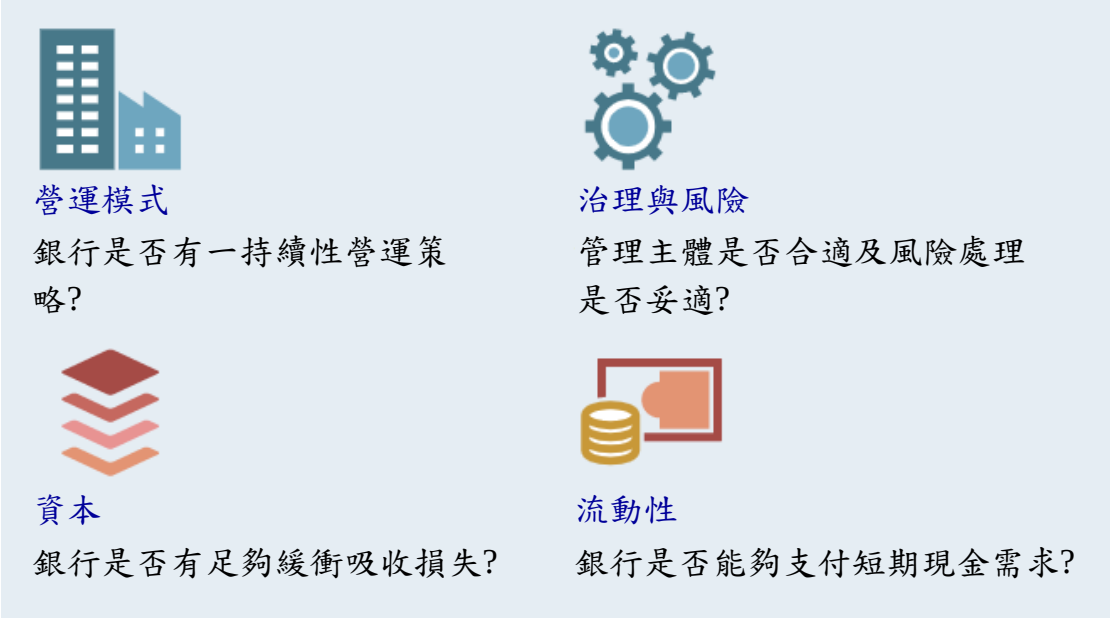
一、EBA 之監理審查評估程序

監理單位定期評估和衡量每家銀行風險之活動，EBA 稱之為監理審查評估程序(Supervisory review and evaluation process, SREP)，其總結了一年中所有調查結果，並給了銀行「家庭作業」。具體來說，SREP 指出銀行在計提資本和風險處理方面的程度，在程序最後部分，監理單位寄送給銀行 SREP 檢查結論，主要目的是為了處理已辨識出來之問題，銀行必須在指定期限內予以矯正。

(一)監理單位檢視要素

為確保公平，把同一標準應用於所有銀行至關重要，SREP 是監理單位用一套一致化之工具，從四個不同角度檢查銀行的風險概況 (圖 1)。

圖 1 SREP 檢視角度



資料來源：ECB 網站[1]。

1. 營運模式

監理單位評估每家銀行設置的可持續性，換句話說，銀行是否有廣泛的活動，抑或只關注少數業務。例如，一家只專注於航運的銀行，對於全球貿易放緩或者過度給予造船商

[1] European Central Bank (ECB), *What is the SREP?*, 6 June 2016. Retrieved from https://www.bankingsupervision.europa.eu/about/ssmexplained/html/srep.en.html (20 Dec 2017)

貸款，將有高度脆弱性，該銀行須管理此類風險。

2. 治理與風險管理

監理單位透過監控銀行管理主體與檢查其風險是否被適當管理之方式，檢視其組織架構。

3. 資本風險

監理單位分析銀行是否有一充分的安全網以吸收正在形成的損失，比如銀行 IT 系統遭到網路攻擊、油價崩跌或借款人無法準時償還貸款。

4. 流動性與籌資風險

監理單位檢查銀行支付特殊現金需求的能力，如經濟不穩定時期，存款人可能提領比平時更多現金。

(二)SREP 如何運作

歐洲央行和國家監管部門的監督人員組成的聯合監督小組(Joint Supervisory Teams, JSTs)持續執行 SREP，且每年籌劃一次個別的 SREP 檢查結論，而每家銀行都會收到下一年度需採取具體措施之通知。

SREP 檢查結論是針對每家銀行個別概況訂製，一般來說，每家銀行都必須遵守法規要求之最低資本，這常被稱為「第一支柱」。

針對個別銀行，在 SREP 檢查結論中，監理單位可以要求銀行持有額外資本且／或設定質化要求(通常稱為「第二支柱」)，質化要求可參考銀行的治理結構或其管理。

此外，個別 SREP 檢查結論支援其他監督活動，有助於對銀行進行全面和持續監控，並為即將到來的監督週期提供策略和作業規劃，直接影響一家特定銀行場外和場內監督活動之頻率和深度。

(三)SREP 對銀行的意涵

每家銀行都不相同，有些專注於傳統商業銀行業務，有些保管其他公司的財務資產；有些將其活動集中於特定部門，有些則將其活動廣泛分散在不同部門。雖然遵循一套共同方法以確保公平和一致之監督，但其中差異反映在每家銀行的個別審查程序之範圍、強度和頻率上。

通常情況下，監理單位要求銀行持有更多資本作為額外的安全網，或者出售某些貸款組合以降低其信用風險。在最極端的案例，監理單位可能會要求銀行改變管理方式，或者調整營運策略，以獲得更多利潤。

二、最終報告-SREP 下之 ICT 風險評估指導方針

該指導方針，係 EBA 根據歐盟 2013/36 號指引(Directive 2013/36/EU)[2]第 97 條，在 SREP 架構下，推廣對 ICT 風險評估之一般程序與方法，並特別依照 Directive 2013/36/EU 第 107 條第 3 項制定之，將 ICT 風險評估補充與進一步明確評斷標準視為 SREP 之一般程序與方法指導方針(EBA/GL/2014/13)[3]中作業風險之一部分。最終報告之指導方針為依循 EBA/GL/2014/13 架構予以整合並制定之指導方針，因此使用上須參照 EBA/GL/2014/13。最終報告對於 ICT 風險評估，除依 EBA/GL/2014/13，提出一般性總則外，另有 2 大主題，大致說明如下：

(一)機構 ICT 治理與策略之評估

該評估主要集中於 ICT 策略、整體內部治理及機構風險管理架構之於 ICT 風險 3 方面，簡述如下：

1. ICT 策略

機構是否落實一套 ICT 策略，該策略除受管理階層適當監督與支援機構營運模式外，且必須與機構營運策略一致，特別是為了持續進行 ICT 更新及規劃，或者執行重要且複雜 ICT 更換之營運策略。

---

[2] Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC (1) – OJ L 176, 27.6.2013.

[3] EBA, *Guidelines on common procedures and methodologies for the supervisory review and evaluation process (SREP)*, 19 December 2014, (EBA/GL/2014/13).

考量 ICT 策略發展與適當性，監理單位應評估機構是否有落實一個與其本身 ICT 活動之本質、規模與複雜度相稱的架構，讓機構用以準備與發展 ICT 策略。

策略執行方面，應考量過程和預算之監控與報告的治理程序，以及相關主導單位，來有效支持 ICT 策略計畫之執行；執行獨立控制與內部稽核以確保與 ICT 策略執行有關之風險有被辨識、評量及有效減緩，以及執行 ICT 策略之治理架構是否有效；採行有彈性之規劃與其審查程序，以回應當遭遇到執行問題或營運環境、技術等等改變時，確保策略執行計畫能及時調整因應。

2. 整體內部治理

機構應闡述其對於 ICT，要有清楚責任劃分之穩健與透明組織架構，ICT 負責人對於管理階層有適當溝通管道，以確保重要 ICT 資訊與事件能夠於管理階層充分報告、討論與決定，且管理階層瞭解及處理與 ICT 有關之風險。進一步而言，監理單位應評估機構之 ICT 外包政策與策略是否考量其外包對機構營運之衝擊。

3. 機構風險管理架構之於 ICT 風險

監理單位應考量機構風險管理與內部控制架構是否足以防護與其規模、活動和風險概況相稱之 ICT 系統，特別是對於整體風險策略規定與內部資本規劃及評量，在預期及嚴峻情境下，其風險胃納是否能涵蓋 ICT 風險，以及在給定機構規模與風險概況下，獨立控制與內部稽核功能是否合適，以確保 ICT 與控制稽核功能間有足夠獨立程度。

(二)機構 ICT 風險暴險與控制之評估

機構能適當辨識、評量與減緩其 ICT 風險，其過程應為作業風險管理架構之一部分，且須與應用於作業風險之方法一致。監理單位首先應辨別機構主要 ICT 固有風險，並對減緩該等風險的管理架構、過程與控制之有效性進行評估，評估之執行應考量所有可用資訊，包括上陳給管理階層之 ICT 風險相關管理資訊、ICT 有關之內外部稽核查核結果，或 ICT 內部風險與控制之自我評估等，最後將評估結果納入作業風險分數評等的檢查結果摘要中。

1. 主要 ICT 固有風險之辨識

首先，監理單位參考所有有關 ICT 暴險之資訊，如 ICT 治理與策略、內外部稽核檢查

結果等，對機構 ICT 風險概況進行檢視；再者應檢視機構用以辨識重要 ICT 系統與服務之方法及程序；完成上述兩步驟後，監理單位應對會造成機構重要 ICT 系統與服務重大衝擊之主要 ICT 風險，給予意見，並且將已辨識出之 ICT 風險對應到相對之固有風險分類。

2. 對減緩主要 ICT 風險的控制之評估

監理單位藉由上述程序對機構辨識出的風險，監理單位應瞭解機構如何辨別、監控、評量與減緩這些風險，並用符合機構之活動本質、規模與複雜度，以及適合機構 ICT 風險概況的監督角度，對 ICT 風險管理政策、程序與風險容忍臨界值，組織管理與監督架構，內部稽核範圍與稽核報告，以及對已辨識出的主要 ICT 風險之特定風險控制等 4 方面進行審視。

3. 檢查結果與評等之摘要

經過上述評估之後，給予 ICT 分數評等，該評等共分 4 級，由 1(最好)至 4(最差)。監理單位在給予作業風險評等的同時，應將機構 ICT 風險意見反應在檢查結果摘要中。監理單位應基於其對主要 ICT 風險的觀點，斟酌風險、管理與控制兩大考量(表 1)，納入作業風險評估。

表 1 風險、管理與控制考量

風險考量	機構 ICT 風險概況與暴險
	辨識關鍵 ICT 系統與服務
	就關鍵 ICT 系統而言，重要 ICT 風險
管理與控制考量	機構 ICT 風險管理政策及策略，與其整體策略及風險胃納是否一致
	ICT 風險管理組織架構之穩健，在風險持有人、管理及控制功能間，是否有清晰責任和任務分工
	ICT 風險測量、監控與回報系統是否合適
	主要 ICT 風險控制架構是否穩固

資料來源：EBA/GL/2017/05。

參、 FFIEC 之網路安全評估工具

有鑑於網路威脅之數量與複雜度日益增加，FFIEC 整合 FFIEC Information Technology(IT) Examination Handbook 中網路安全相關原則與規範指導，以及包含美國標準技術研究院(National Institute of Standards and Technology, NIST)的 Cybersecurity Framework 等其他產業標準之概念，發展出一套可重複且可計量之網路安全評估工具，幫助機構辨識自身風險與確定自身網路安全準備情形。評估包含兩部分：網路風險有關之固有風險概況與網路安全當前準備情形之成熟度。藉由檢視機構固有風險概況與每個領域成熟度等級，管理階層能夠確定其成熟度等級相較於其風險是否恰當；如果為否，機構應該採取降低風險等級，抑或增加成熟度等級之行動。

一、固有風險概況

一個機構之運作包含許多活動、服務與產品，惟項目繁多，故 FFIEC 將網路風險有關之風險辨識分為 5 類固有風險，各分類中之活動、服務與商品，就機構運作以及對機構直接威脅之類型、量(業務量、設備數量等)與複雜度，定義出不同風險等級並加以敘述，進行風險等級評等，最後產出固有風險概況(表 2)。風險等級描述中之參數並非固定，但已有相當程度的參考性；如果在評等每一活動、服務與商品時，風險等級介於兩種等級間，管理階層應以保守原則，選擇較高風險等級。

需注意的是，固有風險評等應於機構在執行風險管理之控制程序前即進行，也就是說，在未包含減緩控制之下進行風險評等。以下就固有風險之分類、風險等級，以及決定固有風險概況等加以描述：

(一) 固有風險之分類

1. 技術與連接類型(technologies and connection types)

某些種類之技術與連接類型，會因特定技術與商品兩者之複雜度與成熟度、連接數，以及本質，而暴露出較高之固有風險，此分類包含網際網路連線服務公司(internet service provider, ISP)與第三方連接數量、系統主機運作為內部或外包、非安全性連結數量、無線存取之使用、網路裝置數量、商品壽命終止系統、雲端服務範圍與個人裝置使用等。

表 2 固有風險概況評估表之設計範例

活動、服務或商品

分類：技術與連結類型	風險等級				
	極低	輕微	中等	顯著	極高
ISP 總連接數	無	輕微複雜(1-20)	中度複雜(21-100)	顯著複雜(101-200)	著實複雜(>200)
非安全性外部連結，非使用者連接數(如 FTP、Telnet)	無	極少數非安全性連接事例(1-5)	些許非安全性連結事例(6-10)	顯著非安全性連結事例(11-25)	多個非安全連結事例(>25)
無線網路存取	無	區隔客戶與公司之無線基地台(access point, AP)	客戶與公司無線網路存取理論上區隔，有限使用者數量與 AP 數量(1-250 使用者；1-25AP 數)	共用無線網路存取，顯著使用者數量與 AP 數量(251-1,000 使用者；26-100AP 數)	共用無線網路存取，所有員工皆可存取，大量 AP 數量(>1,000 使用者；>100AP 數)

資料來源：FFIEC, Cybersecurity Assessment Tool, May 2017。

2. 服務管道(delivery channels)

固有風險隨金融服務管道多樣化與數量增加而增加，此分類包含處理商品與服務之取得，是否透過線上與行動裝置傳輸通道，以及自動櫃員機操作範圍等。

3. 線上／行動裝置商品與技術服務(online/mobile products and technology services)

機構提供之商品與技術服務不同，固有風險亦有不同，此分類包含多樣化之支付方式，如簽帳卡、信用卡、點對點支付、媒體交換自動轉帳服務(automated clearing house, ACH)、小額電匯、大額支付、遠端支票存款、財務金融服務與客戶信託服務、全球匯款、通匯業務、信用卡收單活動等。此分類亦考量是否對其他組織提供技術服務。

4. 組織特徵(organizational characteristics)

此分類考慮到之組織特徵包括企業併購、直屬員工與網路安全承包商數量、安全人員配置更換、擁有高度權限存取之使用者數量、資訊科技環境改變、業務營運地理範圍，以及作業與資料中心之位置等。

5. 外部威脅(external threats)

企圖攻擊或攻擊成功之數量與種類，影響機構固有風險暴險，此分類以機構作為目標進行攻擊之複雜度與數量為考量。

(二) 風險等級

1. 極低固有風險(least inherent risk)

屬於此類之風險，機構對於電腦科技之使用極為有限，極少數量之電腦、應用程式、系統，並且電腦間與系統間無任何連接。商品與服務單純，機構服務區域與員工數有限。

2. 輕微固有風險(minimal inherent risk)

屬於此類之風險，機構就其使用之技術來說，複雜度有限，提供些許低度風險商品與服務。機構關鍵業務系統外包，且主要使用已建置開發完成之技術，在有限複雜度下，對客戶或第三方保持少數類型之連接。

3. 中度固有風險(moderate inherent risk)

屬於此類之風險，就數量與複雜性而言，機構使用稍微複雜之技術。機構可能外包關鍵業務系統與應用程式，以及能內部維持元件技術。透過多種管道提供較大量多樣之商品與服務。

4. 顯著固有風險(significant inherent risk)

屬於此類之風險，就範圍與複雜性而言，機構使用複雜之技術。機構可能使用新興技術提供高風險商品與服務，機構內部可能提供顯著數量之應用程式。機構允許使用大量個人裝置，抑或多樣裝置類型，並對客戶與第三方維持大量連接。機構自身提供多樣支付服務而非透過第三方，且可能有顯著交易量。

5. 極高固有風險(most inherent risk)

屬於此類之之風險，機構使用極度複雜之技術傳遞各式各樣商品與服務，多數商品與

服務，包含提供予其他組織，皆在最高等級風險。新興技術被使用於多樣服務管道。機構可能外包某些關鍵業務系統或應用程式，但主要由內部自行主導。機構與客戶和第三方間資料傳輸維持多種連接類型。

(三) 決定整體固有風險概況

管理階層基於在每個風險等級應用說明之數量來決定機構整體固有風險概況(表 3)，舉例來說，當主要活動、商品或服務落於中等固有風險等級，管理階層可決定機構為一中等固有風險概況。然而，每一分類可能顯現出不同等級之固有風險，因此管理階層亦能考量評估特定分類是否顯現出額外風險。

表 3 固有風險一覽

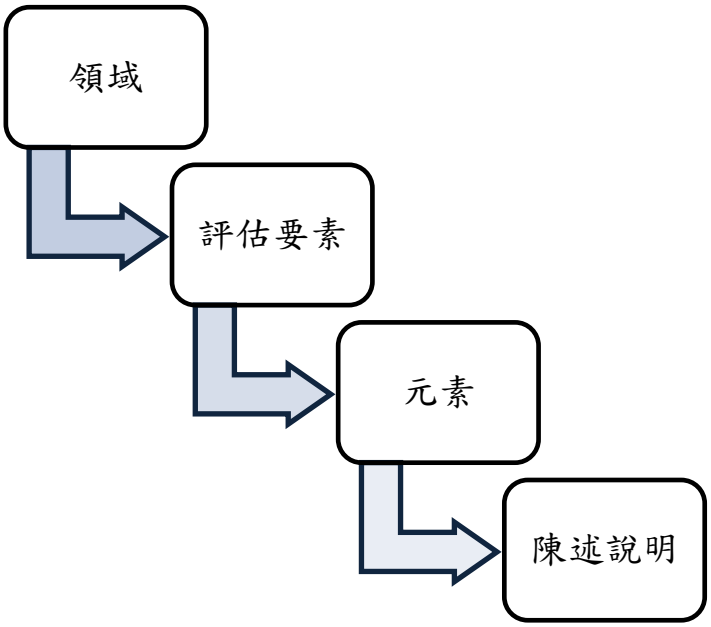
	風險等級				
	極低	輕微	中等	顯著	極高
每一風險等級被選取之說明總數量					
基於被選取個別風險等級，指定一固有風險概況	極低	輕微	中等	顯著	極高

資料來源：FFIEC, Cybersecurity Assessment Tool, May 2017。

二、網路安全成熟度

網路安全成熟度可協助管理階層判斷機構管理網路風險之相對應控制，也就是說，機構現有網路安全準備狀況之行為、落實與程序，其「成熟度」為何。FFIEC 將機構網路安全準備狀況分成 5 個領域，評估不同領域內評估要素中之個別成分，每個成分透過其在 5 個成熟度等級之陳述說明(圖 2)，辨識出恰當符合機構現有之特定控制與落實(表 4)。

圖 2 網路安全成熟度架構



資料來源：FFIEC, Cybersecurity Assessment Tool Presentation, 30 Jun 2015.

表 4 網路安全成熟度評估表範例

領域一：網路風險管理與監督			
評估要素：治理			
元素	成熟度等級	Y, Y(C), N	陳述說明
監督	基本		對於執行及管理資訊安全與營運持續計畫，董事會指派管理人員負責。 當顯見網路事件或規範警示發生時，管理階層舉行會議討論資訊安全風險。 管理階層至少每年提供資訊安全與營運持續計畫之整體狀況報告予董事會。 預算編列過程包含資訊安全相關費用與設施。 管理階層考量到因其他關鍵基礎設施對機構造成之風險。
	初階		董事會至少每年檢視與批准機構之網路安全計畫。

			管理階層負責確認網路安全有關之法遵與規範規定。 透過預算程序要求網路安全設施與人員。 預算編列過程，有一程序正式討論與評估關於網路安全事件潛在費用。

資料來源：FFIEC, Cybersecurity Assessment Tool, May 2017。

需注意的是，在某個成熟度等級的全部陳述說明，以及低於該等級之全部陳述說明，皆必須達成並且維持，該領域才算達到此成熟度等級，也就是在某一成熟度等級中及該等級以下之每一等級，每一個陳述問題需要肯定回答「是(Yes, Y)」或者「以補償控制達成(Yes with Compensating Controls, Y(C))」，機構才算達到該成熟度(圖 3)。某些陳述說明清楚表明無法應用到所有機構時，就不影響成熟度等級之決定。

圖 3 網路安全成熟度等級

資料來源：FFIEC, Cybersecurity Assessment Tool, May 2017。

以下就 5 個領域、成熟度等級，以及完成網路安全成熟度評等加以描述：

(一) 網路安全準備狀況之領域

1. 網路風險管理與監督(cyber risk management and oversight)

一套有效的全企業層面網路安全計畫，說明董事會之監督與管理階層之發展與執行，並有全面性政策與過程，以建立合適的當責與監督。評估要素包含治理、風險管理、資源，以及員工訓練與文化。

2. 威脅情報與合作(threat intelligence and collaboration)

有效地發現、分析和瞭解網路威脅，並具有在內部和適當第三方共享信息能力之程序。評估要素包含威脅情報、監控與分析，以及資訊分享。

3. 網路安全控制(cybersecurity controls)

藉由透過持續自動化防護與監控方式來強化機構防禦態勢，用以保護資產、基礎設施、資訊之做法與程序。評估要素包含預防控制、偵測控制，以及修正控制。

4. 外部依賴管理(external dependency management)

對於監控與管理存取機構技術資產和資訊之外部連接與第三方關係，建立與維持一套全面性計畫。評估因素包含連接及關係管理。

5. 網路事件管理與復原能力(cyber incident management and resilience)

建立、辨識與分析網路事件；優先考慮機構的遏制或緩解措施；並將資訊向上陳報並及於適當的利害關係人。復原能力包括規劃和測試，期以在網路事件期間和事件後，能夠維持和回復正在進行之操作。

(二) 網路成熟度等級

1. 基本(baseline)

達到法律和法規，或在所建議監理指導下之最小期望，此級別包括法規遵循目標，管理階層已審查和評估規定之指導原則。

2. 初階(evolving)

形成尚未被要求之額外文件化程序和政策。已落實風險驅動目標，網路安全責任正式分配並擴大至客戶資訊保護範圍，包含整合資訊資產和系統。

3. 中階(intermediate)

程序詳細、正式，控制被驗證且一致。風險管理落實和分析整合至營運策略中。

4. 高階(advanced)

網路安全落實和分析以跨事業方式整合至不同事業線。大部分風險管理流程皆自動化，並且包含持續性流程改進。前線事業單位之風險決策責任被正式指派。

5. 革新(innovative)

對機構和產業而言，藉由驅動人員、程序與技術創新來管理網路風險。這可能需要開發新的控制手段、新的工具、或創造新的資訊共享群組，且可自動回應即時、預測性分析。

三、解釋與分析評估結果

固有風險概況為整體機構會遭遇到的風險分析，網路安全成熟度等級為機構當前執行的管理控制程序，故管理階層能夠檢視機構固有風險概況相對於每個領域成熟度是否匹配，表 5 描述兩者關係。

越高的風險越需要相對應的成熟度，當兩者不能匹配時，管理階層應考量降低固有風險，抑或開發一套改進成熟度等級之策略，這過程包含決定目標成熟度等級、產出差異分析、優先考量與規劃行動、執行變更、隨時重新評估、傳達結果。因此當環境變更、提供新服務或商品，或當引用新技術時，皆可重新評估機構固有風險與成熟度等級，以瞭解機構控制程序是否到位，進而制訂與執行必要之修正策略。

表 5 風險／成熟度關係

		固有風險等級				
		極低	輕微	中度	顯著	極高
每一領域網路成熟度等級	革新				■	■
	高階			■	■	■
	中階		■	■	■	
	初階	■	■	■		
	基本	■	■			

資料來源：FFIEC, Cybersecurity Assessment Tool, May 2017。

肆、 課程內容

一、ICT 風險監理與範疇

基於風險導向之監理方式，管理架構包含風險確認、評估、監測及控制的循環過程，評量影響金融機構營運健全的主要風險，分析機構對於各類風險之風險管理品質、風險胃納(risk appetite)及暴險程度，並發展出風險控管策略。

ICT 風險為何屬於作業風險之一環？根據巴賽爾銀行監理委員會(Basel Committee on Banking Supervision)對作業風險之定義[4]：因不適當或無效之內部程序、人員、系統或外部事件導致直接或間接損失的風險稱之。就 ICT 而言，從組織外部網路攻擊或內部心生不滿員工造成 ICT 資產或系統損失就符合這項定義，除此之外，ICT 於現今金融機構高滲透度與對其營運重要性，相關事件發生可能對其造成潛在重大衝擊，故 EBA 將其評估從作業風險中獨立分離，評估範圍至少需包含營運持續性規劃與測試、內外部存取系統資料、資料正確完整狀況，以及系統轉換管理等，皆屬作業層面。

二、ICT 風險辨識及分類

ICT 風險辨識，應找出主要 ICT 風險實例，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，並將找出的 ICT 風險一一對應到固有風險分類。

EBA 將 ICT 固有風險分為 5 類，每一分類中皆有與之對應的 ICT 風險成分，並對成分做風險描述，每一成分列舉相關範例，下表 5 於每一固有風險各列舉一成分說明：

表 6 ICT 風險分類法

固有風險分類	ICT 風險[5]	風險描述	範例
1. 系統與資料之效能及可用性受到衝擊之可用性與持續性風險(availability and	ICT 系統癱瘓	因硬體問題導致可用性喪失	因缺乏維護導致儲存裝置、伺服器或其他 ICT 設備故障／失常

[4] Basel Committee on Banking Supervision(2001), *Consultative Document on Operational Risk*, January 2001.
[5] 置於此分類之 ICT 風險表示對其固有風險分類衝擊最大，但也可能對其他分類造成衝擊。

continuity risk)			
2. 系統及資料未授權存取之安全風險(security risk)	網路攻擊或其他外部 ICT 攻擊	因不同目的(如詐欺、間諜活動、破壞行動、網路恐怖行動等)，利用各種技術(如社交工程、部署惡意軟體等)從網際網路或外部網絡進行攻擊，而取得內部 ICT 系統控制權	為了取得內部系統控制或竊取資訊(如身分竊盜、信用卡資訊等)，而進行之進階持續性滲透威脅(Advanced Persistent Threat, APT)
3. 及時可控方式管理系統異動之變更風險(change risk)	對 ICT 系統異動及開發之控制不適當	變更後，因未偵測到之錯誤或脆弱性導致事件發生，	由於缺乏適當測試環境而未落實足夠之測試
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(data integrity risk)	ICT 資料處理不正常	由於系統、通訊、應用程式之錯誤或失常，或錯誤執行資料擷取、轉換或載入程序，造成資料毀損或遺失	資料備份錯誤導致遺失
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外包風險(outsourcing risk)	第三方或其他群組實體服務之復原能力不適當	關鍵業務外包之 ICT 服務、通信服務失靈 委託給服務供應商之關鍵／敏感資料遺失或毀損	因外包 ICT 系統或應用失常，導致核心服務中斷

資料來源：EBA/GL/2017/05。

三、ICT 風險分析評估、控制與稽核

經過風險辨識與分類後，將各種固有風險之發生機率和對營運之衝擊做分級，最後所有固有風險得出一個淨風險，分為複雜(complex)、適度(moderate)或單純(simple)。

控制層面，對各種固有風險，依序利用辨識、保護、偵測、回應及復原等 5 大步驟，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與封鎖等。

基於風險導向，ICT 稽核包含風險評估、稽核規劃、稽核工作實行、報告、回饋監控之循環程序，ICT 稽核為促進穩健 ICT 控制、確保稽核與控制不足能及時解決、通知董事會及管理階層關於 ICT 風險管理落實之有效性。

四、ICT 風險評等與控管策略

菲律賓央行風險評等之方式如同 CAMELS，進行綜合評分，共分 4 級，由高(最好)至低(最差)分別為 4 到 1。

評等成份有 3 類：ICT 治理，如 ICT 監督與作業管理、ICT 風險管理；控制設計、落實與監控，如資訊安全、系統發展與整合、營運連續性；ICT 稽核與法遵等。

綜合評分後，將其所得分數與風險分析中所屬級別進行分類，可得固有風險經過控制後屬高度(high)、中等(moderate)、低度(low)風險 (表 7)，進而決定監理與監控強度。

表 7 ICT 評等與固有風險概況矩陣

ICT 評等	固有風險概況		
	複雜	適度	單純
4	中等	低度	低度
3	高度	中等	低度
2	高度	中等	低度
1	高度	高度	中等

資料來源：本次訓練課程資料。

伍、 心得與建議

一、課程心得

(一)ICT 風險管理與評估漸受重視

本次課前參考與準備資料為美國國家標準技術研究院(NIST)、歐洲銀行業管理局(EBA)及美國聯邦金融監理委員會(FFIEC)等 3 機構有關 IT 風險管理指導原則、SREP 架構下 ICT 風險評估之最終指導原則、網路安全評估工具等 3 篇文件，解釋何謂 ICT 風險，如何建置風險管理程序，以及有哪些評估工具。除此之外，香港金融管理局、新加坡金融管理局及菲律賓央行等機構亦建置其 ICT 風險管理規範原則。隨 ICT 產業進步，為達快速、低成本、便利及規模經濟，金融監理單位及金融機構使用 ICT 已無可避免，但對 ICT 領域之瞭解仍有限，這亦是各國金融監理單位目前關注重點之一。

(二)風險導向監理，仍有許多挑戰

以風險導向角度切入，ICT 風險為作業風險之一環，即使透過風險管理程序將已知固有風險控制後，仍有殘餘風險，但對於未知的風險仍是不清楚，如美國前國防部長 Donald Rumsfeld 對知的層次提出「未知的未知」—我們不知道我們所不知道之事物，在還沒有 ICT 之前，紙本作業就有不少作業風險，隨科技進步，ATM、信用卡，至網路銀行等，仍是有弊端發生，況且 ICT 屬於高度專業之產業，未知風險仍是監理單位及金融機構一大課題。

(三)ICT 之專業人才不可或缺

本次課程主要講述 ICT 風險之管理程序，對於 ICT 技術層面較少著墨，惟如對 ICT 運作及系統架構建置原理未深入理解，對於 ICT 風險之防範依然止於表面，故需有 ICT 專業人員指出風險發生之技術成因，才能對技術層面風險有效控制。

(四)加強資安意識、形塑資安文化，以降低風險

資安控制措施必須要考量風險大小與使用者感受。控制措施太嚴，容易造成使用者抗拒或規避，而難落實；措施不夠嚴謹，則無法消除資安威脅，故常在權衡下，接受風險。因此積極加強人員資安意識、形塑組織資安文化，是降低風險的重要工作。

(五)委外管理日益重要

資訊業務龐雜，囿於人力及經濟規模，部分工作或服務往往需要委外，如設備維護、系統開發、雲端服務等；但相關之風險責任仍須機構自行承擔，對於委外作業人員、程序等之管理、資料可否存放於由資訊業巨擘(如 Amazon)經營的公共雲端(public cloud)等，宜有妥善評估、規劃，以及確實執行。

二、建議

(一)以原則規範取代規則基礎規範

規則基礎(rule-based)為將每種發生之已知狀況加以敘明進行規範，既可涵括所有已知之控制與事件，又有法可循；然而，條列式規範過於繁瑣，易造成監理無效率，最大問題是過於詳細的規則，可讓有心人士知曉監理單位對 ICT 之瞭解程度，以及著重的規則，因此更輕易找出金融機構 ICT 之弱點，並進行攻擊。基於 ICT 為專業度極高的產業，監理上採用原則規範較能保持在 ICT 風險措施上之機密性。

(二)規範制定、風險控制對於金融服務須取得平衡點

正常狀況，報酬皆伴隨風險，風險之損失程度、發生機率及可控制方式皆不相同，如 Apple pay 遭盜刷、e-Bill 扣帳系統程式設計瑕疵導致錯帳、銀行帳務核心系統過載而中斷等，造成之損失與控制方法皆不相同；為了強調降低風險而在風險控制上制定過於繁雜或嚴苛規範，必然造成金融機構成本增加，如為避免系統中斷而擴增過多系統資源、網路銀行登入程序與密碼設定過於複雜以致客戶使用不便等。ICT 之使用是為增進作業效率及便利性，因此規範制定與風險控制應適當，以達金融產業與 ICT 產業結合之正向綜效。

(三)監理單位與金融機構各司其職，各負其責，以達相互發展

監理單位之監理宗旨在於促進金融穩定與發展，而金融機構之經營目的在於股東利益極大化。因此監理單位在 ICT 風險監理上，需有 ICT 專業與金融監理專業整合之人才或團隊，給予金融機構可信服之監理；金融機構為了股東利益極大化，亦不可能輕忽自身 ICT 風險管理，任其造成損失。因此監理單位與企業本身各司其職，不可因監理失能將責任歸咎於金融機構之內稽內控不良，亦不能因金融經營失敗將責任歸咎於監理單位之監理不

足。在兼顧有能之監理與合理之金融機構利益之下，以達金融穩定與發展。

(四)適時參採國際資安規範，精進本行資安管理

本行一向注重資安，已實施 ISO27001 資訊安全管理制度(ISMS)多年；惟資安管理沒有最好，只有更好，對於相關之國際資安規範宜時時涉獵，以補充、修正本行制度及規範。如 FFIEC 之網路安全評估工具，對於資安管理成熟度(cybersecurity maturity)之評估，有詳細說明且可指引改善方向，可作為本行資安管理自評及改善之參考。

參考資料

1.本次訓練課程主辦單位提供講義資料。

2.Accenture(2016), *The Convergence of Operational Risk and Cyber Security*. Retrieved from https://www.accenture.com/t20170803T055319Z__w__/us-en/_acnmedia/PDF-7/Accenture-Cyber-Risk-Convergence-Of-Operational-Risk-And-Cyber-Security.pdf (Dec 22,2017)

3.European Banking Authority (EBA), Final report: Guidelines on ICT risk assessment under the Supervisory Review and Evaluation process (SREP), 11 May 2017, (EBA/GL/2017/05).

4.Federal Financial Institutions Examination Council(FFIEC), Cybersecurity Assessment Tool, May 2017.