國際存款保險機構協會 (IADI) 亞太區域委員會 (APRC) 第 2 屆研習訪問會議暨國際研討會「存款保險機構之資安風險及企業風險管理」研討會摘要報告

本公司國關室、資訊處、風管處及業務處整理

壹、前言
貳、企業風險管理概述：如何在數位化金融來襲時維持穩定性
參、企業風險管理
肆、企業風險管理架構及網路安全應用
伍、企業風險管理案例分享
陸、區域性危機模擬經驗
柒、氣候風險納入金融監控政策：對於存款保險機構的考量及影響
捌、「提高綠色及轉型金融的市場透明度」報告概述
玖、減少碳足跡以實現永續性的創新改革
拾、心得與建議

壹、前言

本次會議為亞太區域委員會第 2 屆研習訪問會議暨國際研討會，探討議題主要包括：「存款保險機構之資安風險及企業風險管理」及「氣候變遷、減碳、永續發展及綠色經濟」。印尼專家學者分享印尼企業風險管理現行做法；巴基斯坦、馬來西亞、泰國等國簡介其企業風險管理架構及網路安全應用；另探討亞太區、南美區之危機模擬演練經驗。印尼存款保險公司、紐西蘭前總理 Ms. Helen Clark、世界銀行及亞太區域委員會存保同業代表等共同分享經驗及挑戰。與會者

藉此得以學習他國企業風險管理、網路安全及永續發展之經驗及作法，期盼邁向金融穩定、綠色金融轉型及全球永續發展之目標。

貳、企業風險管理概述：如何在數位化金融來襲時維持穩定性

講座：印尼存款保險公司研究顧問 Mr. Iwan Jaya Azis

由於金融環境持續變化及新冠肺炎疫情影響加速金融數位化轉型，進而促使企業營運風險型態不斷演變，使企業風險管理 (Enterprise risk management, ERM) 成為當前重要議題。企業風險範圍複雜且廣泛，包含企業內部風險、企業外部風險 (全球風險) 等，ERM 相關規範及原則應明確訂定「核心要素」、「管理架構」及「風險因應策略」，核心要素係指 ERM 規範與企業營運、職能、目標及企業文化，管理架構應包含企業內部控制制度及評估方法、有效內部控制防線 (含企業監督者、管理者及股東) 之溝通協調等，風險因應策略則包含潛在風險辨識、風險發生機率預估及風險損害控制等。

金融市場與商品市場不同處在於金融市場多了人為、行為及偏差 (bias) 等因素，造成資訊不對稱導致金融風險，更大的風險來自於不確定因素 (例如：新冠肺炎疫情大流行)，故需持續監控金融市場及其對銀行體質之影響，並避免影響擴大導致金融危機。

ERM 同時存在機會及挑戰，機會包含明確指導方針、經驗傳承與共享，並可利用數位科技監控風險，惟須注意加強管理及監控數位科技之相關應用，以避免非法行為、詐欺、個資安全、支付系統不穩定等風險。面對 ERM 之挑戰，企業應具備高度彈性、落實情境模擬分析、降低技術官僚主義 (less technocratic) 及創造更多互動、溝通及協調機會，並及時更新預期風險 (anticipated risks)，例如氣候變遷相關資訊，須同時致力於縮小數位落差 (digital gap)，善加利用分散式帳本 (distributed ledger)、智能合約 (smart contract)、金融科技等技術，另亦需考量政策不確定性，包含全球流動性及其風險、主權與銀行關係 (sovereign-bank nexus) 等因素。

儘管新冠肺炎疫情趨緩，政策制定者仍應對當前高度通貨膨脹、財政政策緊

縮、戰爭及地緣政治不穩定等問題保持警覺，各層面的危機及挑戰亦可能快速影響全球金融穩定；另政策制定者應綜合考量後制定解決方案，而非就單一問題提出解決方法。

由於金融科技及數位化持續發展，提高金融交易速度、減少交易摩擦，並優化內部風險管理之數據，反之，或將可能增加網路威脅 (cyber threats) 及隱私風險，技術專業人員、政策制定者及監理機關應適時檢視相關機制並妥適因應，並應避免過度管控及限制；另應妥善運用數位金融科技以實現更具現代化、更穩定的全球金融體系，並同時改善 ERM。

最後，金融機構及金融安全網成員 (包含存款保險機構)，應持續強化營運計畫以預防金融體系風險及機構內部風險，倘目前處於金融承平時期，仍需維持高度風險意識；目前全球金融體系仍面臨諸多不確定性，包含：通貨膨脹、政策緊縮、地緣政治不穩定等問題，各國存款保險機構應發揮資源及經驗分享的互助精神，共同合作，以維護國際及國內金融穩定。

參、企業風險管理

一、企業風險管理概述

講座：印尼人民銀行 (Bank Rakyat Indonesia, BRI) 銀行獨董 (Independent Commissioner BRI) Ms. Rofikoh Rokhim

傳統風險管理 (Traditional Risk Management, TRM) 係透過傳統工具管理企業「部分」風險。另企業風險管理 (ERM) 係一種共同及全面性方法，用以管理企業的風險，進而改善績效。此外，ERM 考量更多面向風險 (如：環境、法遵、財務及策略風險等)，藉以提升股東價值，即企業在創造及實現價值過程中，係依靠持續實施風險管理，並與策略制定及其落實企業文化等習習相關。

傳統風險管理 (TRM) 與企業風險管理 (ERM) 的比較：

比較項目	傳統風險管理	企業風險管理
性質	被動、獨立、防禦性	積極主動、相互依存、思想開明

比較項目	傳統風險管理	企業風險管理
方法	「穀倉」(註 1) (Silo) 方法	全面性 (Holistic) 方法
風險類別	純風險：危害 (hazard)、作業風險	更細緻的風險分類
策略	被動式	主動式
動機	法規或法遵所驅動	銀行競爭優勢、策略驅動

ERM 須能有效回應下列問題，具備正確的企業文化為其關鍵。

(一)壓力測試：企業面臨壓力事件的衝擊及風險因子間之關聯性。

(二)涵蓋範圍：企業策略及日常營運面臨的所有風險。

(三)風險胃納：可承擔的風險。

(四)治理及政策：在公司現行架構運作下，所呈現治理成效及政策推行過程。

(五)風險資訊及基礎架構：如何確認獲得正確資訊以管理風險。

(六)衡量、評估及溝通：瞭解風險規模、影響範圍及彙整相關分析報告。

(七)控制環境：管理風險。

(八)回應：採取因應措施。

ERM 面臨之挑戰：

挑戰	說明	潛在解決方案
時間範圍	取決於企業及其投注於風險管理之心力	可由短期間的風險評估，調整為長期 (或兼顧) 之解決方案
多種潛在情境	採用基本風險評估方法，準備各種風險、各類事件發生的可能性及嚴重程度等資料	針對問題，利用最基本及複雜等 2 種模擬分析

挑戰	說明	潛在解決方案
ERM 主導權	針對董事會、稽核小組或管理階層，何者具主導權，存在爭議且尚未明確	由部分主管監控風險、法遵情形
風險報告	報告應涵蓋哪些資訊，並應採何種方式傳達予內外部相關成員	風險資訊依收受報告者權責、風險類型，及對企業影響，產出各種型式報告
模擬及壓力測試	管理階層透過壓力測試評估企業遭受負面影響之程度	必須能衡量最糟情況，進一步預測惡化趨勢；另利用黑天鵝事件審視企業能採行之措施

ERM 的落實，需要企業內部共識、優秀執行能力，及對各種專案具敏感性等配合，其執行可讓企業專注並辨識出風險，進而保護其珍貴的資本，並促進股東權益的提升。

2022 年，因數位化及風險管理不同的發展面向，例如：治理、風險管理及法遵 (Governance, Risk and Compliance, GRC) 平台、成熟度架構 (maturity frameworks)、風險胃納聲明、資訊長 (Chief Information Officer, CIO) 角色，重塑了 ERM 態樣及提升其競爭優勢，列舉近期趨勢：風險成熟度架構 (包含工作流程)、ERM 精神融入 GRC、將 ERM 視為競爭優勢、風險胃納聲明用途廣泛、風險減緩及評估工具精進、GRC 達成環境保護、社會責任及公司治理 (Environment, Social and Governance, ESG) 目標、CIO 說服企業高層 (C-Level) 接受 ERM、網路與實體匯合；透過數位轉換達成整合性風險管理。

COSO 及 ISO31000 企業風險管理架構，均強調風險是價值創造的一部分，分述如圖一。

COSO 企業風險管理架構，包含 5 要素 23 項原則，分列如下：

(一)風險治理與文化 (Risk Governance and Culture)：實現董事會對風險的監督；建立治理及運作模式；定義對組織行為的期望；遵循誠實及道德的承諾；加強問責 (accountability)；吸引、發展及留住優秀人才。

圖一　ERM 架構


Risk Governance And Culture
1. Exercises Board Risk Oversight
2. Establishes Governance and Operating Model
3. Defines Desired Organizational Behaviors
4. Demonstrates Commitment to Integrity and Ethics
5. Enforces Accountability
6. Attracts, Develops, and Retains Talented Individuals
Risk, Strategy, and Objective-Setting
7. Considers Risk and Business Context
8. Defines Risk Appetite
9. Evaluates Alternative Strategies
10. Considers Risk while Establishing Business Objectives
11. Defines Acceptable Variation in Performance
ENTERPRISE RISK MANAGEMENT
Mission, Vision, and Core Values
Strategy and Business Objectives
Enhanced Performance
Risk in Execution
12. Identifies Risk in Execution
13. Assesses Severity of Risk
14. Prioritizes Risks
15. Identifies and Selects Risk Responses
16. Assesses Risk in Execution
17. Develops Portfolio View
Risk Information, Communication, and Reporting
18. Uses Relevant Information
19. Leverages Information Systems
20. Communicates Risk Information
21. Reports on Risk, Culture, and Performance
Monitoring Risk Management Performance
22. Monitors Substantial Change
23. Monitors Enterprise Risk Management

(二)風險、策略與目標設定 (Risk, Strategy, and Objective-Setting)：考慮風險及營業環境；定義風險胃納；評估替代策略；建立營業目標並同時考量風險；定義可接受的績效波動程度。

(三)執行時面臨的風險 (Risk in Execution)：辨識執行所面臨的風險；評估風險嚴重程度；區分解決風險的優先順序；辨識並選擇風險因應 (Risk responses)；評估執行時的風險；建立風險組合觀點。

(四)風險資訊、溝通及申報 (Risk Information, Communication, and Reporting)：使用相關資訊；利用資訊系統；溝通風險資訊；對風險、文化及績效進行報告。

(五)監控風險管理效果 (Monitoring Risk Management Performance)：對重大變化進行監控；對 ERM 進行監控。

新、舊版 ERM 重點內容：

重點內容	新版	舊版
架構	5 個構成元素 (包含風險治理與文化；風險、策略與目標設定；執行時面臨的風險；風險資訊、溝通及申報；監控風險管理效果)，細分為 23 條原則。	四大目標 (策略、營運、報導、法遵)、八個構成要素 (內部環境、目標設定、事件辨識、風險評估、風險因應措施、控制活動、資訊與溝通、監控)
定義	將企業的文化、能力及作法與策略制定及其績效作整合，組織藉以管理有關創造、維護及實現價值之風險 (註 2)。	是一種過程，受到該機構董事會、管理階層以及各級員工的影響，被應用在戰略設定上而且是超越企業層級的，被設計來辨識可能影響該機構的潛在事件，並且設法將風險管控在它的風險胃納之內，為其經營目標之達成提供合理的信心 (註 3)。
風險胃納 (Risk appetite)	即組織在追求價值時所願意承擔的風險類型及程度 (Accepted Variation in Performance)	願意損失的最大數量之金額。決定風險胃納量需要由上而下的方式、較為主觀的決定。

新版 ERM 架構與舊版之區別：

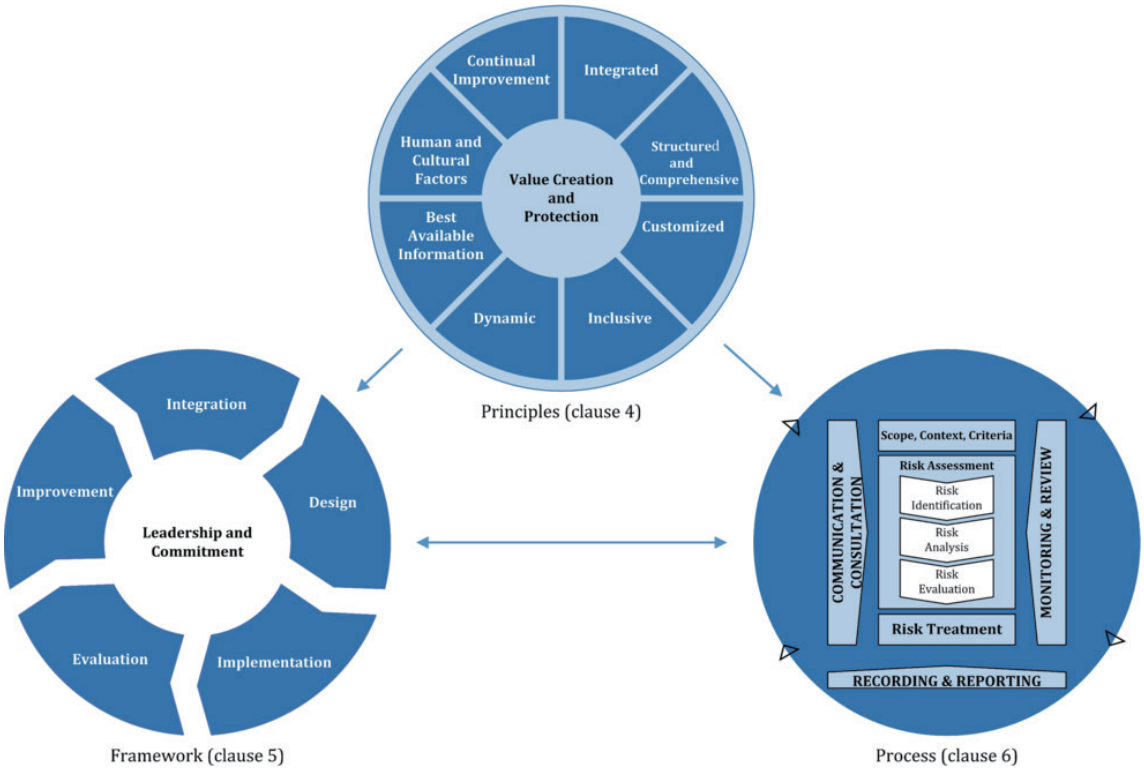
(一)新架構採用要素及原則的結構 (Components and Principles)：加強新架構的可讀性、可行性及一致性。

(二)修訂風險定義：舊定義只強調事件帶來負面影響的可能性，新定義則兼顧正面及負面影響。

(三)簡化及重新定義 ERM。

(四)強調風險與價值間的關聯：即 ERM 不是一項單獨活動或項目，而是整合體現於企業策略、日常營運中。

圖二　ISO31000 風險管理原則、架構及流程關係圖



ISO 31000[註4]標準：

(一)風險管理原則：核心內容為創造及保護價值，並延伸出八項原則，包括：整合性、結構化及全面性、客製化、包容性、動態、最佳有用資訊、人員及文化因素、持續改善。

(二)風險管理架構：核心為領導力與承諾，並透過五項步驟實現，包括：整合、設計、實踐、評估及改善。

(三)風險管理流程，包含：對範圍、內容及標準的定義；風險評估流程 (風險辨識、風險分析及風險評價)；風險處理；風險記錄與申報；溝通與諮詢；監控與審視。

ISO 31000 標準之重點：

(一)聚焦價值創造：與前述 ERM 架構相同，聚焦創造、保護及實現企業價值。

(二)以決策為核心：標準中強調風險管理對於決策之重要性，應妥善管理不確定性，進而做出良好的決策。

(三)著重於整合：前述的「原則」、「架構」，都將整合作為第一個要素，強調風險管理不是一項獨立的管理工作，而是與其他營運活動習習相關，換言之，風險管理工作應與企業其他管理工作整合。

(四)領導力：前述架構「領導力與承諾之核心」，強化高階管理階層角色及權責，同時也強調風險管理是企業管理不可分割的一部分。

在 ERM 架構下，進行風險管理之二種方法：

(一)透過作業面 (Operation) 之管理風險：在作業流程中，透過執行內部控制 (如：前、中、後台)，進而支持公司策略。

(二)透過資本規劃 (Capital) 之管理風險：確保銀行依其風險概況 (risk profile) 及風險性資產報酬率 (RoRWA)，評估並確保有足夠資本因應非預期損失。

二、企業風險管理實務

講座：印尼存款保險公司企業風險管理委員會成員 (ERM Committee Member), Dr. Agustinus Nicholas L Tobing

企業營運過程中，面臨各式各樣風險，可透過 ERM 工具，例如：風險控制自我評估 (Risk Control Self-Assessment, RCSA)、關鍵風險指標 (Key Risk Indicator, KRI)、事件管理、議題管理、內外部稽核等，達到控制遵循，並加以改善，其中，風險胃納聲明 (Risk Appetite Statement, RAS) 包含利害關係人目標，及當決定企業策略時，須瞭解企業風險胃納，擬定業務組合，設定關鍵績效指標，及風險容忍度。

問題的發生，代表一個內控弱點，突顯在管理渠等已辨識風險出現缺陷，目的在於提供資訊以幫助管理並減緩損失。

可信賴的數據及內部控制環境是有效 ERM 流程的基本要素，未來可關注之 ERM 工具與重點如下：

(一)鑒於個人資料保護法 (Personal Data Protection Act) 日漸受到關注、資料保護長 (Data protection Officer, DPO) 的設立、網路安全威脅等因素，將採取以資料為導向 (Data-Centric) 之方法作為因應。

(二)人工智慧 (Artificial Intelligence, AI) 與機器學習 (Machine Learning, ML) 為基礎之檢測工具，可應對企業環境的異常、模式及威脅，如：

1. 定期評估企業環境中敏感資料之儲存。
2. 網路威脅的資訊服務。
3. 以軟體即服務 (Software as a Service, SaaS) 或安全營運中心 (Security Operation Center, SOC) 監控服務[註5] 作為安全工具。

(三)為達持續的法令遵循，須整合安全、合規及風險管理各方面之工具，如：

1. 借助雲端共同合作、提供整合，產出符合全球 ISO 標準、支付卡產業資料安全標準 (Payment Card Industry Data Security Standard, PCI DSS)、SOC 監控服務等報告。

2.系統自動化因應異常事件、是否遵循內部規定，並充分清楚瞭解有無遵守企業控制架構。

肆、企業風險管理架構及網路安全應用

一、馬來西亞存款保險公司經驗分享

講座：馬來西亞存款保險公司 (Malaysia Deposit Insurance Corporation, PIDM) 風險管理主管 Mr. Zufar Suleiman Abu Bakar

本節為馬來西亞存款保險公司在企業風險管理及網路安全方面的概念及實作等議題，主要涵蓋「治理、風險及法遵」、「落實企業風險文化」、「企業持續營運管理的新模式」及「網路威脅應對方法」等四個面向，以下分別敘述。

(一)治理、風險及法遵 (Governance, Risk and Compliance, GRC)

1.GRC 定義

GRC 係一套系統及規則，藉以幫助企業實現業務目標及任務、應對各種不確定性及機會，及促使企業的各種活動皆能符合道德與法律規範，增加營運韌性及信任度。

(1)治理 (Governance)

指系統化的方法，用以指導、管理或控制企業（含策略、政策、流程及控制措施），包含利害關係人之間的關係及企業的治理目標。

(2)風險 (Risk)

指風險管理 (Risk Management)，為一套規則、系統、方法及程序，用以識別、評估、管理、監控及陳報風險。

(3)法遵 (Compliance)

制定流程及程序規範，用以確保公司及其員工以合法及符合道德的方式執行其業務。

2.存款保險機構及企業個體於 GRC 實作上之差異比較表

存款保險機構	企業個體
• 有明確的任務 • 營運規模相對較小 • 員工相對較少 • 非營利 • 信任及信心 • 以公眾利益及金融穩定為主	• 各式各樣的業務 • 營運規模相對較大 • 員工相對較多 • 營利 • 產品及服務 • 以股東利益為主

通常存款保險機構內部的 GRC 相關職能是彼此獨立運作，但由於存款保險機構較小的規模及所擔負的具體責任，使得這些職能彼此之間可以有效的共享、協調與及時陳報。

3.從策略面看 GRC

馬來西亞存款保險公司在管理風險方面已將 GRC 運用於人員的協調、流程及技術上，以達成其業務目標，簡要說明其策略如下。

(1)治理

• 成為考量策略時不可或缺的部分。

• 關鍵在於維護商譽及發展與主要利害關係人之間的信任關係。

(2)風險管理

• 塑造企業的策略方向及焦點時納入風險概念。

• 在策略規劃過程中，檢視環境及考量主要的風險驅動因素。

(3)法遵

確保在營運上遵循政策及程序，這些政策及程序應遵循高治理標準以降低風險。

4.GRC 在企業內五項職能間需共享及相互整合

有關 GRC 各項職能 (如下表) 的重點及工作計畫皆需以風險為基礎發展，及將風險評鑑過程中的調查發現與報告一併納入考量。

企業職能	企業風險管理
	內部稽核
	法務
	誠信及治理
	資訊管理及安全

(1)製作以主題為基礎的風險報告。

(2)以風險為考量而得出內部稽核的重點項目。

(3)納入網路安全相關的趨勢發展、監控方法及弱點識別。

(4)撰寫法令遵循狀況及要保機構對監理規範遵循狀況報告。

(5)強化治理及誠信，並且實施企業內的活動偵測，以確認符合法令。

(二)落實企業風險文化

評估與降低風險為邁向 GRC 的要件，因此在企業內部需強化風險文化發展，使每個人將風險視為自身責任。

1.定義

風險文化係指企業的共同價值、利益、知識及具備對風險的充分認知能力，尤其是指企業的領導人及員工等群體之間必須要擁有相同之目的。

2.重點概念

(1)企業為達到目標就必須承擔相對應的風險。

(2)風險文化深深影響企業管理風險的能力。

(3)風險文化影響企業因承擔風險而進行的決策，以及承諾可履行績效目標的能力。

3.馬來西亞存款保險公司如何發展風險文化

使所有員工認知風險，並對其所承擔的風險負責，在企業中對風險抱持開放討論的態度，並在各部門間充分協調及運作以管理風險。

4.馬來西亞存款保險公司於疫情期間面臨的問題

近幾年 Covid-19 疫情而帶來的營業中斷現象，成為馬來西亞存款保

險公司營運所涵蓋區域內，最為顯著的改變 (指風險事件)，其中大多數是企業持續營運及網路科技方面所面臨的問題，馬來西亞存款保險公司對於類等改變及其不確定性相關面向，採取之應對方法如下表所列。

面向	變更及不確定項目應對方法
企業風險管理	• 企業持續營運管理 • 政府標準作業流程遵循 • 照顧員工健康及安全 • 網路風險監控 • 落實企業風險文化
資訊管理及安全	• 網路安全 • 資訊安全 • 資安管理系統 (ISMS)
內部稽核	• 稽核網路及資訊安全控管 • 滲透測試 • 資安管理系統
法務	• 會員機構法遵
誠信及治理	• 企業內部及員工法遵

(三)企業持續營運管理新模式

1.企業持續營運管理 (BCM) 定義

完整的企業持續營運管理程序係識別企業面臨的潛在威脅，以及這些威脅對企業營運的衝擊為何，衡量如果發生風險可能造成的損失，與具備有效率的因應能力，以保護關鍵利害關係人的利益、商譽、品牌及價值創造等活動，打造企業成為具有韌性的架構，使企業可以在災害或中斷發生時，延續其關鍵職能。

2.Covid-19 疫情發生後企業持續營運管理所產生的變化

(1)疫情發生前遇到災難發生時，所採取的對策是人員進駐至災害復原中

心 (Disaster Recovery Centre, DRC)。

(2)現行在採用新興科技 (如下列) 輔助下，企業得以持續營運。

- 雲端科技
- 高速網路
- 虛擬私人網路 (VPN)
- 電子郵件安全閘道器
- 雙因子驗證
- 視訊會議軟體 (例如 Microsoft Teams, Zoom, Skype, WebEx)

3.「遠距辦公」成為新的營運模式

(1)成為在疫情下最可行的工作方式。

(2)成為任何企業在面臨營運中斷情況下的主要選項。

4.被拆分的工作團隊仍可照常營業 (Business As Usual, BAU)

過去企業持續營運的管理模式，因新興科技的輔助，而得以實現照常營業 (BAU) 的新模式。

5.拜科技快速進步之賜，災害復原中心因科技輔助而更緊密結合，不再是獨立運作的單位，另因許多新興技術不斷產生，企業亦須側重：

(1)瞭解如何與新興科技併肩作戰。

(2)持續關注新興科技如何應用於企業持續營運管理。

(3)深入瞭解新興科技的優缺點。

(4)如何應用最能符合需求。

6.雲端環境、服務可提供企業更多的選擇。

7.企業持續營運的選項將隨科技進步而不斷增加。

(四)網路威脅應對方法

近幾年網路威脅逐漸升高，根據統計截至 2021 年已有高達 86.2% 的企業受到一次以上的網路攻擊，而受侵害所占的比例也逐年提升，在 2020 年疫情爆發的同時，受網路侵害事件造成的損失金額也隨之大幅增加 (據估計在 2018 年網路犯罪造成企業平均損失金額為 5,225 億美元，但 2020 年網路犯罪造成企業平均損失金額大幅成長至 9,450 億美元)，且為因應

網路威脅犯罪日增情況，網路安全相關產品或服務的市場規模預測至 2026 年時甚至將達到近 3,500 億美元的規模。

另外，除了網路威脅次數及所造成的損失持續增加外，隨著科技進步，網路威脅也不斷擴展其攻擊範疇，其主要攻擊對象已涵蓋物聯網 (IoT)、以 5G 為基礎的各式網路應用、雲端基礎設施即服務 (IaaS)（註 6）、平台即服務 (PaaS)（註 7）、公開資料中心、遠距人力資源及使用個人擁有的行動裝置來執行工作 (BYOD)（註 8）等。

網路威脅亦衝擊出其他的風險，也就是網路風險可能會與其他的風險產生連鎖反應，其他相關風險包括營運持續風險、資訊安全風險、商譽風險、法律風險、財務風險及其他風險等，例如企業一旦遭遇網路攻擊而造成資料被盜取、勒索贖金時，很有可能將多年辛苦經營的商譽毀於一旦，因此在面對網路威脅時，馬來西亞存款保險公司所採取的應對方法有以下幾種：

- 在進行風險評鑑時，將 IT 風險項下的網路風險另外區隔出來成為獨立的評鑑項目。
- 設置資訊管理、安全部門及資安長等職位。
- 通過 ISMS（註 9）相關認證 (如 ISO 27001 國際認證)。
- 施行預防、偵測及修正等控制措施，以因應相關風險，包括人員風險、惡意軟體風險、勒索軟體風險、網路釣魚風險及各種弱點與漏洞所造成的風險。

識別風險後，馬來西亞存款保險公司設置下列三道防線（註 10），以防禦資訊及網路威脅：

- 第一道防線 - 察覺及管理風險：持續維護有效的內部控制措施，以及做出風險管理決策。
- 第二道防線 - 綜觀風險：在企業風險管理及資訊安全管理層面，有關內部控制措施的有效性及法遵方面需受到監控，並鑑別出目前已知風險與找出逐漸浮現的風險，然後納入風險管理實務當中。
- 第三道防線 - 各自獨立確認：各風險是否已被適當的管理與處置，將由

內部稽核分別檢視及提供確認。

任何種類的網路安全相關應對措施，均須隨著網路環境的不斷發展，採取動態調整的管理方式，依以下三個步驟持續循環檢視及調整：

- 實行各項網路安全控制措施。
- 識別各項措施與現況的落差，並進行矯正以持續增強防禦措施。
- 經常重新檢視各項網路防禦措施是否適當。

二、 網路安全及數位轉型

講座：加拿大存款保險公司 (Canada Deposit Insurance Corporation, CDIC) 存款人解決方案及數位轉型部門主管 Ms. Alison Millard

當企業期望能以導入數位科技以改變或創造新的商業模式時，在進行數位轉型的過程中做好風險管理將是轉型成功與否的關鍵，尤其是在疫情爆發後，企業更需應用各種遠距數位輔助工具及雲端科技等以保持營運不中斷，因此相對投入更多的資源在推動網路安全相關的風險管理更是勢在必行，以下就可能面臨的狀況加以說明及探討如何採取應對方式。

(一)網路安全與數位轉型在企業風險管理實際應用建議

根據調查企業已採用或計劃優先採用數位轉型者高達 89%，但數位轉型因風險識別、管理及減輕影響等處置不當而遭遇轉型失敗者卻也高達 70%，因此在企業打算進行數位轉型時需要考慮的關鍵法則有：

1. 轉型方向應契合目標業務。
2. 企業應對轉型過程採取合適的治理方式。
3. 在網路安全方面建議採取分散決策模式 (Distribute Decision Making)[註 11]，決策結果將更貼近實務作業。

(二)「數位創新」及「網路安全」二者於「風險承受」互相衝突

為提升業務面執行效率，在進行數位創新時，將導入應用較新技術與其他創新概念，然而在另一方面，由於應用創新概念或新的技術帶來網路安全漏洞或對 IT 系統的不當管理，以及對所依賴的外部供應商的不當管理，會對維持安全、可擴展及營運彈性的能力上產生負面的衝擊。

(三)建立合適的風險治理聲明

企業在評估數位轉型相關的風險承受度時，可參考下表建議，列舉風險偏好聲明，並依實務調整其風險承受度以及治理聲明，以切合自身需求建立風險治理聲明。

風險偏好評估項目	風險承受度	治理聲明
追求新技術與其他創新的導入，應用以提升業務執行效率	高	• 在預算上持續以百分比列示投入數位轉型或創新專案。 • 在擁抱新的科技及創新方面，可接納犯錯的風險，以及從錯誤中學習，作為經驗及增進能力，最終達成業務任務。 • 將焦點集中在能幫企業帶來最有價值產出的科技專案上。
網路漏洞或對 IT 系統的不當管理，以及對所依賴的外部供應商的不當管理，會對維持安全、可擴展及營運彈性的能力上產生負面衝擊	低	• 在預算上持續以百分比列示投入網路安全相關專案。 • 僅保留執行業務方面需要的關鍵資訊，以降低資訊洩露風險。 • 使用安全設計原則，以確保所有開發流程及技術都將安全性納入考量。

(四)培育領導者的責任感以建立網路安全風險承受能力

儘管網路安全為營運風險之一，但在實務上，企業很少願意參與其中並決定要承擔多少風險，所以企業風險管理領導者可以協助促進業務及技術領導者二者之間的討論，將業務及與其相關的網路風險偏好等網路安全管理作業擺放在業務決策的重心。

為了實現建立風險承受度之目標，企業領導者必須擁有共通的衡量單位以衡量網路安全風險，量化網路安全事件對業務的影響有多大，如此才有辦法具體建立企業風險承受能力，以下所列步驟可用來幫助企業建立風險承受能力。

1.明確的闡述各種風險對於業務的衝擊程度。

2.根據各種風險事件被量化後的結果，評估及發展風險承受能力。

3.為支持發展風險承受能力，對各項控制措施進行成本與效益分析。

4.針對風險承受能力、投資金額及衡量指標等三個面向，必須在業務面及技術面之間達成一致共識。

企業可參考以下三項 (或更多) 風險事件，將網路風險事件發生時，對於業務面所造成潛在衝擊一一列舉。

1.因資料外洩而可能被曝露出來的非公開資訊。

2.因網路風險事件無法提供服務而造成營運中斷，以及在不同種類的錯誤情況下所造成的不同衝擊。

3.不符合法規或監理要求的地方。

根據以上步驟所列舉出的風險，企業應再進一步依上述建立企業風險承受能力的四個步驟以評估衝擊程度 (詳如下表範例)。

網路風險	對業務衝擊	建立風險承受能力時的考量
因資料外洩而曝露的非公開資訊	財務面：對遭受侵害的個體提供的補償金額	• 是否願意支付被勒索軟體加密資料後，駭客所要求的贖金？以及願意支付多少金額？ • 是否投保網路安全相關保險？或自行承擔財務風險
	商譽面：損失名譽及公眾信任	• 災害發生時對於利害關係人溝通機制的成熟度如何？ • 是否建立追蹤信任度變化的衡量指標？
	法規面：隱私保護及揭露法規／義務	• 風險於法規面潛在的後果為何？ • 如有未合規的部份，所造成的衝擊為何？
	人資面：人才誘因	• 人才流失的衡量指標 • 對在職員工的溝通機制
	金融穩定面：資料外洩而造成金融穩定及效應擴散疑慮	• 目前持有可能導致潛在穩定性問題的任何資訊 (如持有金融機構弱點相關資訊)，檢視其風險能見度是否適足？

(五)重點回顧

1.企業必須在推動數位創新及維護有韌性且安全的技術環境二者間找到適當的平衡。

2.以適當的治理原則幫助領導者做出決策，在各種風險承受度間取得平衡。

3.由明確定義的業務面預期成果以驅動數位創新。

企業風險管理及網路安全的領導者，需要與所有的利害關係人共同建立安全的風險承受度，建立風險承受度指標，將網路風險明確量化為對企業的影響程度，據以制訂各項風險控制措施及進行相關的投資決策，以促成與確保完成整個企業的問責制度。

伍、企業風險管理案例分享

講座：世界銀行金融部門顧問 Mr. Nan Zhou

2019 年新冠肺炎疫情爆發後，世界各國政府機關為保護人民的健康實施各種防疫措施，例如自主或強制性的居家隔離及居家檢疫、限制出入境及防疫照顧假等，這些措施也直接影響企業營運，因此，企業紛紛著手制定相關對策應對，並且針對潛在風險進行鑑別與訂定因應方法，目的讓營運順利，存款保險機構亦然。

企業營運持續計劃（BCP）係先擬訂應變計畫以預防並降低緊急事故帶給企業的風險。換言之，各國存款保險機構亦應依自身業務性質、規模及複雜性，訂定適當的營運持續管理機制，運用合適的系統、資源及流程以維持營運不中斷。然而，為達到此目標，應以「風險管理」為基礎，建立切合組織目標與業務的營運持續計畫，並且依照適當的管理程序，定期測試與更新。

BCP 制定流程係根據風險管理的架構，其營運管理生命週期如下：

(一)風險評估 (Risk Assessment, RA) 及營運衝擊分析 (Business Impact Analysis, BIA)：RA 係鑑別、定義及評估所面對的威脅、弱點及風險，並對所有資產鑑別出的風險進行評估；BIA 的架構係建立在 ERM 的風險識別原則，其目的是為評估營運無法持續時的衝擊程度（亦即損失或中斷），與恢復

運作至最低標準的作業需求，藉此可以清楚了解企業的關鍵營運項目與流程，以及支持這些流程所需的要求，以協助評估復原所需要的時間與相關資源。

對於存款保險機構而言，為辦理 ERM 評估及營運衝擊分析，執行特定職務關鍵營運流程之考量重點包括：

1.應該涵蓋組織內部哪一個功能？這些功能的活動在營運流程如何運作？
2.如前所述，這些特定活動會存在那些風險？這些風險產生的原因？
3.如果風險無法即刻降低，將會為存款保險機構帶來何種衝擊？

(二)準備 (Preparedness)：對於存款保險機構而言，應鑑別營運中的關鍵項目 (Critical Process) 並分析潛在風險所帶來的衝擊，依照風險（弱點）排序並確立不可中斷項目、優先復原項目及可接受之復原時間，並能在災難發生時盡快地重啟營運，此階段衡量的標準如下：

1.最大可容忍停機時間 (Maximum Tolerable Downtime, MTD) 係為在衝擊發生時，存保機構營運系統完全停擺可容許的時間。
2.復原時間目標 (Recovery Time Objective, RTO) 係當營運系統遇災難時造成停機，透過擇定的復原程序或方法進行復原所需的最少時間。
3.復原點目標 (Recovery Point Objective, RPO) 係可容許的資料損失時間、資料量，以評估多久進行一次備份。
4.復原目標及關鍵程序所需最少資源：
(1)存款保險機構如何評估 MTD、RTO 以及 RPO 的流程？審視及核准主要考量的因素為何？
(2)考量關鍵人員及技術資源如何利用最少的資源維持存款保險機構正常營運。
(3)存款保險機構的指導原則如何在資源不足以應付緊急事件時，權衡需求及成本。

(三)回應 (Response) ：面對瞬息萬變的經營環境，無論是氣候變遷、法令法規的變更、全球化的營運模式等，任何一個危機交互相影響可能造成營運的重大衝擊，因此，模擬災害發生時的不同情境，讓相關人員進行營運持續

計畫演練，至關重要。另應擬訂計畫預防中斷及復原之執行措施，以及恢復正常營運之時程與策略，例如重大事件通報 (Event Reporting)、危機評估 (Crisis Evaluation)、啟動 (Activation) 以及危機分析及揭露 (Dislosure)。

1.危機演練、營運策略及步驟：

(1)存款保險機構在制定 BCP 時會考量哪些危機的情境？

(2)存款保險機構可以分享危機演練時所制定的營運不中斷策略及關鍵營運流程是什麼？

(3)執行 BCP 時會碰到哪些困難？如果以 ERM 的架構為基礎，這些困難如何解決？

(四)持續檢討與改善 (Improvement)：外在或內在環境都會因時間而變化，除定期檢視實體環境是否變動、BCP 是否隨變動調整架構外，另亦須不定期檢視，例如採購新的設備、人員與組織的調整變動、契約當事者或供應商的調整變動、業務流程的變動等；規劃及執行計畫是不同的任務，當緊急事件發生時，應依照 BCP 執行以發揮作用，而演練係確保計畫有效發揮作用且達成訂定的目標。演練之目的不僅是測試執行 BCP 的效果，且應隨時更新相關的演練經驗及事後檢討，演練的程序如下：

1.沙盤推演 (Walkthrough)：針對各種危機情況進行沙盤推演，確保並使所有計畫相關人員明確了解各業務 BCP 啟動時之職責與內容。

2.測試危機情境演練 (Dry Run of Crisis Scenario)：藉由不同情境演練過程，讓測試參與者，掌握計畫與特定事件間的關聯，並測試小組人員互相配合的能力。

3.功能測試 (Functional testing)：係測試 BCP 規劃流程的妥適性、有效性及處室間、存款保險機構主管與外部機構的協調性，亦盡可能在備援的網站上進行測試。

4.金融危機模擬演練測試 (Testing as part of financial crisis simulation exercise)：BCP 測試包含多種不同的模擬情境，但最重要的是存款保險機構、金融機構及主管機關共同參與解決危機的演練，並依據演練的結果，持續檢討及修正存保機構的營運流程。

ERM 之目的係協助存款保險機構透過風險識別、監控、回報以及回應流程，除將負面衝擊影響降到最低，也致力貫徹達成業務目標；除此之外，BCP 係協助存款保險機構遭遇突發事件衝擊時，透過鑑別關鍵營運、回應、復原以及重建架構降低營運中斷風險。綜上所述，ERM 結合 BCP 能夠為存款保險機構創造綜效，同時藉由分析流程改善組織通報、溝通、協調、整合等決策能力。

透過風險管理及 BCP 的運行，存款保險機構不僅能夠降低危機衝擊，且能協助強化金融體系。

陸、區域性危機模擬經驗

一、亞太區

講座：奧緯財顧公司 (Oliver Wyman Financial Services) 合夥人 Dr. Oliver Wuensch

近年來，各國主管機關針對清理系統性重要銀行時，不致對金融穩定產生影響，取得實質性的進展，其中對建構復原及清理計畫 (Recovery and Resolution planning, RRP)，意味著國內外主管機關對跨境銀行的清理，協調程度有顯著程度的提升。然而幸運的是，迄今尚未爆發系統性危機，進而對現行架構產生考驗，無法確知是否有能力去處理。近期國際間零星的個案，明確指出每個危機是不同的，且限縮所能準備的範圍。近期工作重點由政策面及金融機構潛在風險，轉移至各機構 (包含銀行、主管機關及週邊機構) 危機處理能力，目的在確認面臨高度動態環境及極度不確定性下，各機構是否有能力處理。模擬測試是有效的工具，藉由測試各參與者之能力及瞭解經驗上所欠缺部分，歸結出應改善之處。

近期模擬測試所觀察到的測試著重於各國主管機關間跨國合作上的效率，然而成功的跨國合作，取決於彼此間對現況、相關議題及處理策略上，有無明確一致的觀點，以下為近期模擬測試所觀察到的現象：

(一)跨國合作

各國主管機關主動積極參與，但隨著時間壓力而面臨挑戰；儘管所有

參與者都積極做出貢獻並聽取彼此意見，惟經濟體大國仍承擔更多責任；最終達成協議之解決方案，而單邊解決方案是所有國家的次佳選擇。

(二)國內合作

相關部門各司其職，權責明確，經由正式 (如：危機處理小組) 及非正式管道溝通，資訊分享非常頻繁。

(三)清理架構及工具

1.對於所有參與國家，可採用之政策工具，足以處理模擬情景，然而制定完善的關鍵協議，更對決策大有助益，例如及時啟動緊急流動性援助 (Emergency Liquidity Assistance, ELA)。

2.對國內架構 (如：觸發機制、政策工具等) 有清晰的認識，但缺乏對跨境間架構的理解，協調議題自始便極為重要，且在模擬過程中不斷磨合。

(四)清理計畫

1.預擬的清理計畫，且能為所有參與之主管機關共同遵循，將是順利完成模擬測試目標之關鍵。模擬強調制訂合理的清理計畫以應對並減緩不斷變化的危機。

2.在各種危機情景 (如：總體經濟面向、特殊 (idiosyncratic) 風險、資訊安全面等) 下進行可行性評估，即時調整清理計畫及提升危機處理能力仍很重要。

3.簡言之，危機情境越嚴峻，主管機關及相關單位的迴旋餘地越少，且單方面的行動帶來的風險也較高。

二、南美區

講座：國際清算銀行 (Bank for International Settlements, BIS) 資深顧問 Ruth Walters

(一)依據成本及複雜程度，測試及模擬態樣可分為：

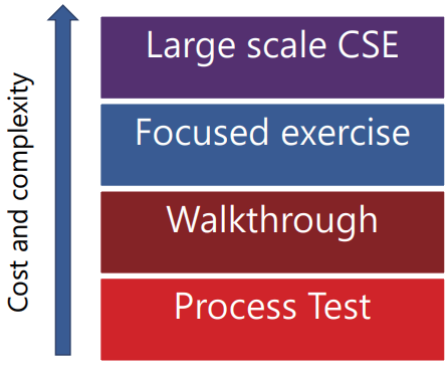
1.流程測試 (Process Test)：需制定技術測試模板及具備內部管理工具知識。

2.沙盤推演 (Walkthrough)：檢視重大關鍵內部流程、文件，對於面臨危機

時的反應，而不是建構在情境上的模擬。

3. 聚焦測試 (Focused exercise)：針對預設之情境進行演練，特別專注於制定決策之內部流程。
4. 大規模危機情境測試 (Large scale CSE)：決策制定及溝通過程尤為重要，需考量各種因素，如各種資料來源、判斷能力，及機關間(包含跨國機構)的溝通。

圖三　測試及模擬態樣



圖四　BSF 營運範圍

(二)案例探討：拉丁美洲 BSF[註 12] 銀行

1. 特徵：
   (1)屬系統性重要 (Systemically important) 銀行，據點涵蓋南美多數國家。
   (2)近年規模快速擴張。
   (3)重大暴險項目
   - 非城市地區對中小企業及零售債權。
   - 仰賴國外投資之重大投資專案。
   - 部分國家較為熱絡之房貸市場。
2. 策略：
   (1)推出高利率快速達到存款目標額，輔以集團內部自有資金。
   (2)除提供各行業企業貸款外，對家戶、中小企業及公司提供各類金融商品，以達積極成長目標。
   (3)辦理與伊泰普水電站專案 (Itapúa Dam Project) 相關的基礎設施融資，

積極努力擴大市場占有率，並從該地區的外國投資中獲利。

3.隱憂：

(1)分析師對南美銀行業前景堪慮。

(2)環保人士抗議推遲伊泰普水電站擴張。

(3)媒體報導 BSF 子公司在公司治理及風險管理等面向缺陷。

(4)由於伊泰普水電站專案暫停，使得中小企業面臨困境，違約率不斷上升。

由於不斷接踵而來的挑戰與壓力，導致 BSF 銀行倒閉，除評估其自救可行性外，決定策略、工具及採行時機，須權衡各種可能性後執行。

4.因應 BSF 銀行倒閉，各面向所側重要點彙整：

(1)清理立場及授權：部分清理架構側重於清算，缺乏可行的政策工具，如：資本重建 (Bail-in)、過渡銀行 (Bridge Bank) 等，尚不足以應付系統性銀行的倒閉。

(2)清理計畫及可行性評估：大多數參與國尚未進行，且未充分考量營運不中斷因素，主管機關的事先準備及能力可透過協議、指導手冊得到改善。

(3)清理過程所需資金：對提供流動性缺乏指引，並過度仰賴存款保險基金，仍有資金缺口，在缺乏明確的復原協議 (recovery arrangements) 或架構，最後需由公共資金挹注。

(4)國內協調工作：在部分國家，主管機關間的協調、分工並不明確，且有未及時提供資訊予存款保險機構之情形。

(5)跨國合作 (Cross-border cooperation)：目前合作架構側重於監理資訊交流，而在資金分擔、政策工具及權責劃分等方面，仍有重重困難待克服。

5.後續應採取改善的措施：

(1)立法解決目前架構上不足之處，並完善復原及清理計畫 (RRP) 的規定及步驟。

(2)更新國內主管機關間的備忘錄，將危機管理及緊急流動性援助 (ELA)

等流程明文化。

(3)審視並補充內部作業手冊，包括溝通及決策流程。

(4)制定區域性主管機關間之合作協議。

6.從模擬中獲得的經驗：

(1)模擬的事先準備：明確目標，及勿低估所需資源與時間。

- 提前決定模擬目標，並務實決定資料來源。
- 充分瞭解受測地區之政經環境，並確保所用資料與當地主管機關習習相關。
- 排練 (Dry-runs) 極為重要，應早於模擬前一個月，以便有充分時間調整資料。

(2)危機情境測試 (CSE)：確認所有主管機關皆參與，但避免過度複雜。

- 確認資料來源真實性，並與主管機關有關聯，且儘可能保持簡單。
- 鼓勵透過跨國對話，以減輕彼此間訊息不對稱，並增進團隊成員彼此依存度。
- 聚焦測試 (Focused exercise)：從過程失敗之處出發，提供足夠時間對各項清理方案進行討論。

(3)模擬形式：保持動態，並儘可能彈性調整

- 充分利用角色扮演以增加模擬的動態，並由觀察中獲益。
- 定量資料應力求簡單，並對所做決策有所裨益。
- 不同模擬間，可針對部分資料做必要調整。

(4)執行及報告：有效率的團隊及優秀的觀察員

- 確保團隊有足夠能力，對模擬各項活動充分掌握與監控，並扮演稱職的利害關係人 (如：財政部長、投資人或潛在購買人)。
- 觀察員適時提供明確指引，並熟悉所觀察國家之法律架構。

(5)危機情境測試 (CSE) 的設計原則

- 明確目標及範圍：事先決定測試目標，在能力所及下，於設定範圍內進行模擬測試。
- 後續流程：從模擬測試中，發現不足之處，在機構支持下展開改善

流程。

- 參與程度：參與者須目標一致，更重要的是，需有財政部長的參與。
- 情境與資料：簡單為佳，過度複雜會降低效率；資料聚焦於所要測試目標，而決策表可幫助確認資料是否與決策相關；保持動態調整資料。

柒、氣候風險納入金融監控政策：對於存款保險機構的考量及影響

一、圓桌會議：英國駐雅加達領事館處長 Ms. Amanda McLoughlin

氣候變遷對於世界各地的影響逐漸加劇，天災帶來的人員與財產損失也日益嚴重，為因應氣候風險所帶來的衝擊，英國政府刻不容緩並將此列為國家首要目標，該國除是全世界首位將減排目標納入法規並提出碳預算的國家，且自 2021 年起提出重大的倡議，如格拉斯哥氣候協定 (Glasgow Climate Pact)，各國最終達成協議，也是史上首次明確表達減少使用煤炭的計畫，並為發展中國家提供財務援助協助其適應氣候變遷。

英國央行 (Bank of England) 要求銀行及保險公司審視氣候變遷帶來之挑戰、對其業務、客戶及環境造成之衝擊，以及如何管理與因應措施，例如英國政府承諾在 5 年內，將在整個英國經濟體系中強制推行與 TCFD 氣候相關的訊息揭露。

自 2021 年 6 月起英國央行針對金融機構及保險公司進行首次壓力測試，該測試檢驗英國大型的金融機構及保險公司在面對未來零碳排經濟的過渡期及極端氣候影響壓力下的韌性。

英國政府於 2021 年啟動百萬城市氣候行動計畫 (Urban Climate Action Programme, UCAP)，在英國提供 27.5 億英鎊資金，城市氣候行動計畫將扶持非洲、亞洲和拉丁美洲多個國家解決氣候變遷議題，打造綠色環境；英國駐雅加達大使館自 2013 年在印尼地區開始實施與氣候相關的政策，如提升建築物及能源效率、氣候融資，以及森林和自然保護的措施，旨在減緩氣候變遷的衝擊及與燃燒化石燃料而造成的空氣污染。

英國政府也投入資金於東協基礎建設基金（ASEAN Infrastructure Fund, AIF）發起成立的東協推動綠色金融機構（ASEAN Catalytic Green Finance Facility, ACGF），資金挹注對印尼政府相當重要，該機構可協助印尼政府在減碳上建立長遠目標，藉此逐步達成 2050 年淨零碳排的國際共同目標。

二、 圓桌會議：美國氣候政策倡議組織資深研究員 Mr. Luthfyana Larasati

印尼身為東南亞國協國家重要成員，其經濟成長速度全球第二，惟在面對人口、經濟快速成長，以及推動國家邁向工業化過程中，面臨氣候變遷的嚴重威脅，洪水肆虐、海平面上升等災害為當前重要的議題。為解決前述問題，印尼政府近年來已陸續發布與永續發展和綠色金融等議題相關政策。

2015 年 9 月 25 日聯合國 193 個會員國通過 17 項永續發展目標 (Sustainable Development Goals, SDGs)，計畫於 2050 年達到零碳排目標。為達成共同的目標需仰賴各國政府、國際機構、民間社會和其他機構等共同落實永續發展行動。

2017 年印尼政府發布總統令第 59 條，制定國家及地方性行動計畫，以促進 SDGs 的實施，該計畫清楚規範政府和非政府活動及相關可持續發展目標，同時印尼金融服務管理局 (Otoritas Jasa Keuangan, OJK) 於同年再發布第 51 號及 60 號條文，前者係規範 11 項綠色商業活動，其中投資組合揭露，同時並要求上市公司及金融機構依該項規範揭露可持續性獨立報告或部分報告之年度報告；而 60 號 OJK 係涵蓋綠色債券發行及條款，其旨在鼓勵開發環境友善金融產品，也刺激銀行發行創新可持續金融產品，以共創綠色金融生態圈。

印尼證交所於 2022 年發布 ESG 領導者指標 (Leaders Index)，該指標係衡量一間公司企業社會責任績效，做為投資人選股衡量之指標。指標分為「環境 (Environmental)」、「社會 (Social)」、「公司治理 (Governance)」3 項指標，當中「環境」方面包括氣候變遷、溫室氣體排放等與環境有關議題，「社會」方面係指勞工問題影響當地社區、消費者權益等社會議題。至於「公司治理」方面，包括行政人員薪酬、董事會架構、組織稅務策略等。

另印尼於 2022 年發布綠色經濟活動分類目錄 (Green Taxonomy)1.0 版本，主要將營運活動 (Business Activities) 依據對環境的破壞程度，以綠、黃、紅燈顏色，

區分為三大經濟活動 (共 919 個細項) ：

(一)綠色 (15 個細項)：指營運活動對環境有正面影響且無重大的破壞，並能加速達成國際可持續性目標。

(二)黃色 (422 個細項)：指為達到國際永續目標進行營運活動的轉型，對於環境沒有造成重大的破壞。

(三)紅色 (482 個細項)：指營運活動對環境有重大破壞。

印尼 Green Taxonomy 1.0 版本與歐盟綠色分類標準 (EU Taxonomy Regulation) 結合有助於提高可信度，且如能在全球經濟中提供可預測之相關政策並降低審查及盡職調查成本，將吸引國內外綠色投資資金的流入。

相較於 2017 年 OJK 發布的條例，目前印尼所發布之 Green Taxonomy 1.0 版含括更廣泛綠色細項。該分類規範與相關區域性分類規範的定期評估及協調亦相當重要；東南亞國家協會 (Association of Southeast Asian Nations, ASEAN) 並訂有分類規範，旨在為所有成員國提供可持續金融的共同語言，以減少溝通摩擦，並在該地區創造更多的經濟機會。

印尼政府為使 Green Taxonomy 有效推動企業轉型，要求當前黃色類別下的行業必須制定戰略、行動計畫、時間表和明確的轉型目標，讓投資者了解哪些產業正在進行轉型，並攜手企業發掘新商機共同邁向低碳綠色金融生態系。

捌、「提高綠色及轉型金融的市場透明度」報告概述

講座：國際清算銀行 (Bank for International Settlements, BIS) 亞太區代表處 (Representative Office for Asia and the Pacific) 區域顧問，Mr. Frank Packer

一、背景及動機

「提高綠色及轉型金融的市場透明度」(Enhancing market transparency in green and transition finance) 報告參考及調查綠色金融體系網路 (Network for greening the

financial System, NGFS)[註 13] 成員及許多中央銀行、監理機關及國際金融機構之經驗及資料。

全球金融家及投資者致力於擴大綠色金融規模，要求其投資及購買的資產標的在環境永續方面保持透明度，並以實現綠色標籤 (green labels) 為目標，達成環境友善的市場發展及投資策略 (例如：減少溫室氣體排放)，另希冀永續投資及氣候轉型計畫，降低各行業碳排放程度。

二、本報告架構

(一)分類法 (Taxonomies)：定義綠色標準以有效辨識具有環境效益或成本的資產、專案及活動的分類系統。

(二)綠色外部審查及評估：綠色外部審查為確保正確應用綠色原則、標準及分類法，從而提高市場透明度。

(三)氣候轉型指標、架構及市場產品：藉由使用市場基礎方法 (market-based approaches) 以評估重要轉型工具。

(四)總結及結論性觀點部分，摘錄及參考決策者的共同觀點及建議，另於「提高綠色及轉型金融的市場透明度」報告之附件中提供具體國家案例。

三、綠色分類法 (Green Taxonomies)

在新興市場及發展中市場，許多國家對降低全球溫室氣體排放的貢獻度仍低，且易受到氣候變化影響 (包含實體風險及轉型風險)，新興市場預估每年需要 1 兆美元才能逐步邁向低碳經濟，而明確定義綠色資產、活動及專案有助於投資及融資策略轉向氣候友善的資產項目及達成環境永續發展目標。

歐盟分類法 (EU Taxonomy) 係建立在歐盟基礎上的法規及目標，由於社會經濟發展、環境及轉型途徑的差異，歐盟法規及目標不完全適用於新興市場。另鑒於上述興新市場具龐大資金需求，決策者意識到需要跨國投資助益，以有效且快速達成綠色金融目標。

此外，新興市場分類法 (emerging market taxonomy) 的制定者正試圖反映其自

身綠色轉型發展的環境目標及流程，並在術語及指標部分盡可能保持與歐盟分類法具有一定程度的可比較性 (comparability) 及一致性。世界銀行 (World Bank) 亦指導新興市場根據其國家環境優先原則制定分類法，並須與當地法規保持一致性。

四、 分類法的相互作用性 (Interoperability of taxonomies)

跨司法管轄區及大型司法管轄區內以一致的方式制定分類法有助於提高跨市場的可比較性及透明度，亦能擴大綠色資金跨境流動。

中國人民銀行 (People’s Bank of China, PBC)、國家發展及改革委員會 (National Development and Reform Commission) 及中國證券監督管理委員會 (China Securities Regulatory Commission, CSRC) 合作更新 2015 年目錄，並於 2021 年 4 月發布《中國綠色債券認可專案目錄》(China Green Bond Endorsed Projects Catalogue)，更新後的目錄刪除清潔煤 (clean coal)，將減緩氣候變化作為環境目標，另包含預防環境污染、有效利用資源，及引入「不造成重大傷害」原則 (Do No Significant Harm Principle)。

此外，國際永續金融平臺 (International Platform on Sustainable Finance, IPSF) 於 2019 年正式成立，引領全球邁向綠色經濟轉型，為綠色及永續發展活動制定共同原則及指標，這將促進全球市場分類法的可比較性 (comparability) 及相互作用性 (interoperability)。在國際永續金融平臺中，中國及歐盟於 2020 年成立分類法工作小組，目標係制定共同基礎分類法 (Common Ground Taxonomy)，該工作小組於 2021 年首次對歐盟和中國分類法進行全面性逐項審視及比較。經檢視，歐盟及中國分類法間存在部分重疊，雙方專家在普遍適用的分類架構下確立共同的技術標準。

五、 建立綠色外部審查制度

多數人對於綠色標籤 (green labels) 的可靠性及可比較性存在疑慮，特別是在環境保護、社會責任及公司治理 (ESG) 評級部分，各界呼籲針對綠色外部審查及評估流程進行有效監理，並建立綠色外部審查制度。

建立綠色外部審查制度的目標是發展適當的法規及原則，廣納專業且合格的私人審查者或審查單位，確保獨立且專業評估的公平競爭環境，藉此落實綠色經濟目標、綠色定義標準及提高外部審查的透明度。部分國家 (例如：中國及歐盟) 已經開始建立或提升綠色外部審查監理架構，並指導私人或私部門從事外部審查工作。

六、 具備內建目標工具 (built-in targets)：以可持續發展連結債券為例

可持續發展連結債券 (Sustainability-Linked Bond, SLB) 係根據特定的可持續發展績效目標 (Sustainability Performance Target, SPT) 對未來表現進行嵌入式評估的金融工具，績效目標包括發行人承諾實現與 ESG 相關的關鍵績效指標 (Key Performance Indicators, KPI)，若發行人未達績效目標，將以票面利率遞增 (step-up coupon)、溢價贖回 (redemption premium) 或抵銷機制 (offset mechanism) 的形式向債券持有人支付額外款項。可持續發展連結債券 (SLB) 與綠色或社會債券 (green or social bonds) 不同之處在於，SLB 籌集的資金未限制資金用途，可用於一般融資目的。

部分市場已發展出標準化原則，最著名的是國際資本市場協會 (International Capital Market Association, ICMA) 於 2020 年 6 月發布的可持續發展連結債券原則 (Sustainability-Linked Bond Principles, SLBP)，SLBP 屬自願性準則，概述金融工具納入 ESG 評估考量，並透過解釋 SLB 的發行方式，促進 SLB 市場發展的健全與誠信。SLBP 為所有 SLB 發行人提供發行關鍵指引，並提倡發行人問責制度，及要求發行人提供必要的投資相關資訊，以保障投資者權益。

自 2019 年起，SLB 市場迅速擴張，歐洲表現尤其強勁，企業及主權發行人積極進入該市場，惟 SLB 市場仍具許多挑戰及優化空間，簡述如下：

(一)投資者對於支持降低溫室氣體排放的資產及標的保持高度興趣。

(二)確保 SLB 發行人使用的績效指標及目標具備高可信度。

(三)制定簡單易懂的績效指標應優先於複雜的績效指標，例如：溫度指標或 ESG 評級。

(四)針對特定行業的績效指標制定應提供更多的指導及原則，以落實高度標準化。例如：全球許多權威機構實施 ESG 揭露架構 (ESG disclosure frameworks) 及科學基礎減量目標倡議 (Science Based Targets initiative) 等，皆可為訂定關鍵績效指標 (KPI) 及可持續發展績效目標 (SPT) 提供具體指引。

(五)為提高關鍵績效指標 (KPI) 及可持續發展績效目標 (SPT) 的可信度，可依據全球報告標準制定機構 (global reporting standards setters) 所推動的指標，並與遵守上述標準的非 SLB 發行人進行比較。

七、 技術提升與數據收集

為確實審查環境相關績效目標的達成結果，需要更多高品質及精確的統計數據佐證。藉由提升技術運用，強化永續發展資訊揭露管理，以提高市場透明度，並即時或以較高頻率收集數據及資訊。

部分司法管轄區已開始利用新技術加強數據收集及儲存，例如：2021 年，在歐盟企業永續報告指令 (EU Corporate Sustainability Reporting Directive) 提案中，歐盟委員會 (European Commission) 提議要求企業對報告資訊進行數位標記 (digitally tag)，歐盟委員會的提案預期將增加永續資訊的數位化，並確保永續資訊易於上傳至資本市場聯盟行動計畫 (Capital Markets Union Action Plan) 所設計的歐盟單一窗口 (European Single Access Point, ESAP)。另外，2021 年 12 月，世界銀行集團 (World Bank Group) 的國際金融公司 (International Finance Corporate, IFC)、香港交易及結算所、許多銀行及資產管理公司等共同發行 ESG 手冊 (ESG Book)，為大眾提供及整合數位企業永續發展的資訊及來源。

八、 政策建議

本報告研究主題包含分類法、綠色外部審查及氣候轉型指標及原則，目的皆為促進綠色金融市場透明度，雖然具體的政策建議不可避免因地域及司法管轄區而有所不同，但仍提出與決策者有關的共同及一般性意見，簡述如下：

(一)為避免不同綠色分類法、標準及原則導致分析結果有所差異，應提升分類法及轉型架構或原則的可比較性及相互作用性，以強化共識，並為綠色外部審查提供一致的基礎。

(二)建立專業的外部審查及評估，是提升市場可信度的關鍵。

(三)投資者應實地查核 (Due diligence) 及評估發行人的可信度，例如：環境永續相關基金的投資者應留意基金的前瞻性目標及未來投資計畫與策略，同時比較基金過去投資紀錄是否具一致性，亦需評估發行者與被投資對象的關係及其代理投票模式 (proxy-voting pattern)。

玖、減少碳足跡以實現永續性的創新改革

一、 搭建資本市場、永續發展與氣候行動 (Climate Actions)[註14] 之間的橋樑

講座：Kehati 基金會執行董事會主席 Mr. Riki Frindos

Kehati 基金會是 1994 年成立的非政府組織，目前已獲得總額超過 2.5 億美元的援助，組織運用各方援助者的資金來支援進行印尼各項環境計畫。由於資本市場的投資者目的是促進商業與經濟繁榮並從中獲得利益，非政府組織則是以公平正義、人權與環境保護為出發點，投資者及非政府組織通常處於對立面，故該組織希望可以搭建雙方溝通的平台，及建立起大家共同生存與共同面臨相同威脅 (如氣候變遷、浪費及污染及自然生態破壞) 的共識，訴求在商業利益及對環境衝擊中間找到平衡點，並提出二項主要倡議如下：

(一)不傷害 (Do No Harm)：鼓勵投資者與企業採用 ESG 或資助 ESG 相關基金。

(二)做好事 (Do Good)：設立相關慈善基金，培育挑選出的受資助對象，使商業計畫成為可行，及鼓勵投資者投資因堅持 ESG 理念而受到衝擊的企業。

該組織並於 2014 年在印尼資本市場上創建 SRI KEHATI 指數，該指數以在資本市場上挑選 25 檔辦理 ESG 績效最佳的股票作為其成份股，在東南亞是第一個以永續責任為理念的 ESG 指數，並與基金管理公司合作設立共同基金來投資 Kehati 挑選的 ESG 企業相關股票，基金管理公司也會將部份手續費回饋予該組織，

目前已與 12 家基金管理機構採取這種合作模式。

於此商業模式下，目前已取得具體成效的案例有印尼的弗洛雷斯島 (Flores Island)，該島因地勢易受氣候影響，故面臨日益嚴重的氣候變遷威脅及糧食安全問題，該組織協助農民投資種子開發及品種改良、栽培等，以振興長期廢棄的高粱產地與進行市場開發，解決長期以來當地的糧食安全問題。

該組織也為加入 Kehati 的 ESG 計畫的企業設定長期目標 (如下列)，企業並可獲得全球認可的認證標章或獎項等榮譽。

(一)鼓勵成為資本市場上擁有 ESG 友善卓越績效的標竿企業。

(二)鼓勵與激勵上市公司將永續發展的理念融入其企業營運當中。

(三)促進投資者投資對環境及社會友善的企業，以及實踐更完善治理的企業。

(四)為資本市場上的投資者提供直接參與實際永續發展及氣候行動的機會。

二、存款保險與 ESG：是被炒作或是新興議題？

講座：IADI 研究處資深研究與政策顧問 Mr. Bert Van Roosebeke

本節對 ESG 議題在國際上所面臨的現況進行簡介，進而分析 IADI 對會員機構所做以 ESG 為主題的問卷調查結果，據以觀察會員機構所採取的作法與呈現的態度等整體概況，惟講座特別強調這些分析屬於個人研究意見，不代表 IADI 或任何合作夥伴的立場。

(一)ESG 的概念

ESG 提供一個涵蓋廣泛議題的討論架構，且這些議題通常與銀行業的商業上沒有直接關聯，所以存款保險機構長期以來從未將 ESG 視為其核心任務，然而，近期非金融相關產業的企業目標似乎有朝 ESG 方向進行改變的跡象，這些受到關注的 ESG 相關主要議題如下表。

ESG	主要議題	
環境 (E)	• 能源效率 • 溫室氣體排放 • 森林砍伐	• 循環經濟 • 水資源管理
社會 (S)	• 多元及包容 • 工作條件 • 雇傭關係	• 公眾關係 • 人權問題
治理 (G)	• 風險管理 • 高階管理階層薪酬 • 報告與揭露事項	• 董事會結構 • 網路安全

(二)國際概況

1.國際清算銀行、國際貨幣基金、世界銀行及民營顧問公司都曾發表關於 ESG 相關主題的文章，皆強調應將 ESG 理念導入金融市場的急迫性。

2.綠色金融體系網路 (Network for Greening the Financial System , NGFS) 是由世界上超過 100 家的中央銀行及金融監理機關組成，其目的在於促進調撥及投注資金於廣泛的低碳 (綠色) 經濟及環境永續發展方面的相關工作。

3.IADI 前於 2021 年時，將 ESG 中有關環境 (E) 議題的部分，納入存款保險機構新興議題的二份政策簡報中。

(三)現行 IADI 核心原則 [註 15] 與 ESG 有關聯的項目：

1.核心原則 1 (公共政策目標)：公共政策目標所有項目。

2.核心原則 3 (存款保險機構之治理)：聯結有關治理 (G) 的部分。

3.核心原則 9 (存款保險基金之來源及運用)：在資金來源及用途方面聯結有關環境 (E) 的部分。

4.核心原則 10 (存款保險制度之公眾意識)：在公眾意識方面聯結有關社會 (S) 的部分。

(四)IADI 對會員機構所作的問卷調查結果

IADI 在 2022 年第 3 季曾對會員機構進行 ESG 相關議題問卷調查，總計有 40 個會員機構回覆，相當於有半數的會員機構參與調查，調查結果應可視為具有代表性，其中有四分之三的存款保險機構認為，未來二年將會增加與 ESG 相關的重要議題，本次調查結果揭露值得關注的議題如下：

1.正式採用 ESG 政策的程度

三分之一的存款保險機構已經正式制定至少與 ESG 其中一項相關的政策，但僅四分之一的存款保險機構對外公開這些政策。而在 ESG 之中又以治理 (G) 方面最優先被考量制定為正式的政策，例如有關出差、採購、資訊揭露及實施相關公司治理架構等方面的政策，另外，四分之一的存款保險機構預計在未來二年內將制定與 ESG 相關的政策。

2.傳達 ESG 目標時採用的管道

有四分之一的存款保險機構，會強制要求要保機構必須透過公開管道揭露其有關 ESG 方面的目標。

3.考量將 ESG 納入關鍵績效指標 (KPI)

只有十分之一的存款保險機構考量將 ESG 相關的績效項目 (無論該項目是否可被量化衡量) 直接納入關鍵績效指標內。

4.面對氣候投資政策的態度

在未來制定有關氣候方面的投資政策，三分之二的存款保險機構表示「不太可能」或「非常不可能」，僅有三分之一表示「可能」，表示氣候問題尚未在存款保險機構主要政策中占有一席之地。

5.持續關注 ESG 議題

五分之三的存款保險機構認為 IADI 應對 ESG 相關主題進行進一步研究。

(五)未來方向

本節旨在介紹幾個較為關鍵的議題，IADI 研究處於未來即將發布的文章，將提出更多基於對全球存款保險機構在 ESG 問卷調查結果中所呈現的相關議題，並且會根據目前調查結果，對未來研究方向進行調整，惟研究處現階段只著重於如實分析及呈現調查結果，不會對調查結果做出任何價

值判斷，以維持中性客觀的研究立場。

拾、心得與建議

一、各國政府對於 ESG 的規範及定義不一致，影響金融機構在 ESG 資訊揭露及相關金融監理之可比較性，建議持續與各國存保機構合作交流，以掌握國際發展趨勢

近年來 ESG 議題已經是全球潮流，我國政府並將其列為施政政策，成為企業發展趨勢與金融監理機關關注之重點，對於銀行業授信及營運活動產生重大衝擊。我國政府機關持續研擬 ESG 相關規範或監理政策，惟各國對於該議題如 ESG 申報與資訊揭露、綠色分類標準、ESG 評鑑等，定義不盡相同，對於金融監理機關及存保機構之相關監理亦帶來挑戰，建議持續與各國存保機構交流，強化研究發展，以掌握國際發展趨勢。

二、科技轉型與資安仍充滿挑戰，資訊人才養成耗時，宜積極培育及延攬資訊人才，以提升資安控管

隨著 Covid-19 疫情轉變工作型態，進而對遠距上班的需求增加，及金融科技發展推動金融機構轉型趨勢，資訊安全成為金融機構重要核心，也直接影響存保機構營運風險，因此，對專業資訊人才之需求大為提升，惟培育該領域人才需耗費長時間，目前人才供給仍顯不足，存保機構宜積極培育及延攬資訊人才，以提升自身資安控管及對要保機構資安風險監控的能力。

三、因應網路上的威脅種類與攻擊事件逐漸增加，宜適時檢視網路安全相關風險評鑑項目內容是否適宜，使網路安全風險管理更加完備

Covid-19 疫情發生後，金融機構等企業為避免發生營運中斷，對虛擬辦公室及遠距辦公等需求大幅提升，由於企業對於網路服務及網路科技工具的倚賴漸深，新興工作模式於疫情降溫後仍然成為許多企業的標準工作模式之一，故建立在以網際網路通訊為基礎上的服務或產品所帶來的網路安全威脅等議題，應適時

重新檢視原風險評鑑項目之適用性是否仍屬妥當或宜調整修正，以避免因評鑑項目不合宜致未能於事前防範，而發生相關風險事件，對金融機構營運造成衝擊。

四、 金融安全網成員於金融機構進行數位轉型創造新興商業模式時，宜適時檢視相關風險控管，以避免風險事件影響金融穩定

金融機構因面對市場激烈競爭，為提升各項業務執行效率及提升服務品質，進行各項數位轉型計畫已然成為必要選項，但伴隨著數位轉型的過程或成果而來的風險事件卻也時有所聞，相關金融安全網成員對於金融機構數位轉型的相關風險，應適時介入了解其風險事件發生時對業務造成的衝擊程度，審慎評估金融機構是否已具備面對衝擊時的因應措施及風險承受能力，以避免危機擴大而影響金融市場穩定。

五、 強化永續報告書之揭露內容，並透過重大議題分析，辨識未來發展重點

ESG 為本公司近年重點政策與工作項目之一，除於 110 年成立永續委員會外，並自 111 年起著手編製永續報告書，由整體角度考量營運績效與風險，透過內外部持續且即時的溝通、鑑別利害關係人及蒐集其對各項永續相關議題關注程度、對本公司實質與潛在正／負面衝擊程度之矩陣分析等方式，分析各面向之重大永續議題，達到風險管理及公司治理 (或公司文化) 的融合，不僅可豐富本公司永續報告書之資訊揭露內容，並利辨視未來業務與管理發展重點。

六、 宜將要保機構 ESG 執行情形納入本公司要保機構申報評等管理能力評估指標，以引導要保機構重視永續發展

根據聯合國 2004 年發布的報告「Who Cares Wins」首次提出，ESG 能影響長期財務表現，依主管機關規定 2023 年起，對國內金融機構辦理永續金融評鑑，建議將評鑑結果或其他 ESG 受評結果，例如：Sustainalytics ESG 風險評分、FTSE Russell ESG 評級、ISS 環境揭露評級等，納入本公司要保機構申報評等管理能力評估指標，以適時將財務分析以外不同面向納入風險差別費率架構，以引導要保

機構重視永續發展。

註釋

註 1： 指企業分工過細，部門間不願分享資訊。

註 2： 資料來源：《企業風險管理》正體中文版，第 93 頁。

註 3： 資料來源：《臺灣保險業企業風險管理》，第 2 頁。

註 4： 即風險管理原則及指導綱要 (Risk management – principles and guidelines)。

註 5： 即資通安全威脅偵測管理服務。

註 6： 基礎設施即服務 (Infrastructure as a Service, IaaS)：雲端服務模式的一種，提供透過網際網路以使用 IT 基礎設施的服務，包括運算能力、儲存、備份及網路。

註 7： 平台即服務 (Platform as a Service, PaaS)：雲端服務模式的一種，提供可以在上面執行軟體的作業平台，而無需額外關注硬體及作業系統建置。

註 8： 自攜裝置 (Bring Your Own Device, BYOD)：允許使用者攜帶個人的行動裝置處理公務，例如員工使用筆記型電腦、手機與平板電腦來處理工作，存取企業內部資訊及使用應用系統。

註 9： 資訊安全管理系統 (Information Security Management System, ISMS)：以系統化方法分析及管理資訊安全相關事務，源自英國 BS-7799 標準，如今成為 ISO 27000 系列的 ISMS 標準。

註 10：此三道防線的策略又稱為縱深防禦，以多層的防禦科技層層保護資訊資產，加深入侵者攻擊的難度及降低風險事件所造成的傷害。

註 11：分散決策（或稱非集中決策）係指在機構內的不同位置分散進行決策，如高階主管授權給較低階的主管或一般員工等進行決策 (參考網址 https://zh.wikipedia.org/zh-hant/ 分散決策)。

註 12：Banco São Francisco(BSF)，係配合虛擬測試之虛構銀行 (Fictional Bank)。

註 13：綠色金融系統網路 (Network for Greening the Financial System, NGFS)：是由多國中央銀行及金融監理機關所組成，承諾互相分享好的實作方法，並促進有關氣候及環境變遷相關風險管理的發展，以及支持永續性經濟發展。(參考官方網站網址：https://www.ngfs.net/ngfs-scenarios-portal/about/)

註 14：氣候行動 (Climate Actions)：是依「巴黎協議」的內容，採取對地球環境問題的

拯救行動。

註 15：國際存款保險協會 (IADI) 核心原則：為設立或改革存款保險制度而建立的重要參考基準 (參考網址：https://www.iadi.org/en/core-principles-and-guidance/core-principles/)。