雲端服務之資安治理

安碁資訊
吳乙南
5/2 , 2024

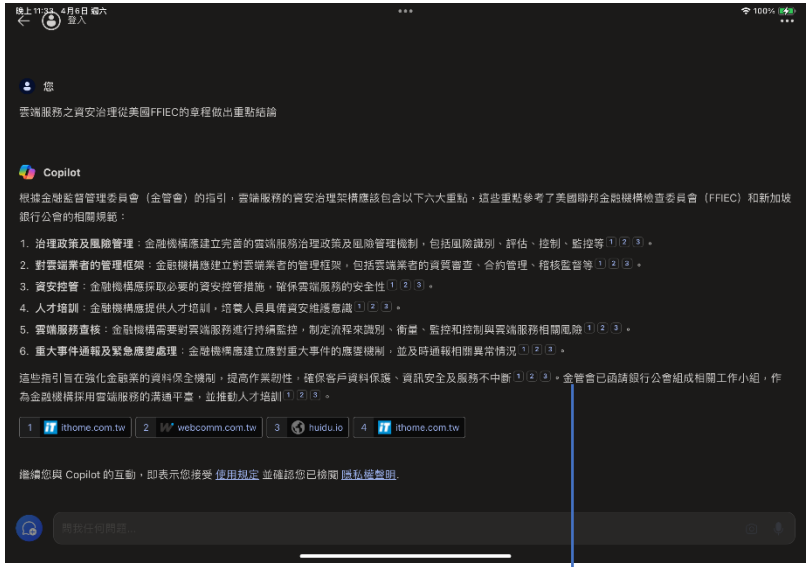
講師簡介

吳乙南

職務	安碁資訊股份有限公司 總經理 宏碁雲架構股份有限公司總經理，安碁學苑董事長
學歷	美國Syracuse University電腦資訊科學碩士 國立交通大學計算機工程學士
經歷	■ 交通大學資訊工程學系109年傑出系友 ■ 安碁資訊(ACSI)(股)公司 業務協理、副總經理、總經理 ■ BMC, Taiwan業務協理、總經理 ■ IBM, Taiwan 行銷經理
專長	■ 公司營運策略規劃 ■ 業務市場開發與銷售策略研擬 ■ 產品規劃暨市場行銷企畫 ■ 軟體工程

議題與GPT的回應

Copilot



SFCERT

1.使用雲端服務的治理框架，並考量使用雲端服務對金融機構治理和運營模式影響。

2.使用雲端服務的安全管理，應執行適當盡職調查及持續監控雲端服務安全性。

3.應制定流程來識別、衡量、監控和控制與雲端服務相關風險。

4.使用雲端服務應有資訊安全維護意識及人員培訓計畫。

5.金融機構和雲端服務業者的合約應明確說明雙方責任畫分。

重大事件通報以及緊急事件處理SF-CERT

2022.9.15

工商時報 A6 名家評論 https://ctee.com.tw 中華民國111年9月15日／星期四

觀念平台

審視證券期貨領域SF-CERT之任務

吳乙南■安碁資訊股份有限公司總經理

資安等同國安，資訊安全已是國家六大核心戰略重要產業發展面向，自今年2月俄烏開戰前夕資訊戰已經成為前哨戰；8月對岸啟動實體軍事演習之前，網路攻擊與認知作戰也同時開打，資訊戰已經成為現代化軍事行動的第四軍，不同於傳統武力所造成的人命傷害，但一樣可以達到擾亂民心以及讓人民對政府公權力的不安，網路資訊戰成為各國較forward）；專攻對手網路攻擊，但目的都在「持續應戰」，因此行政院資安處以資安資訊分享與分析中心（ISAC），電腦緊急應變支援小組（CERT）以及資安監控中心（SOC）來落實推動國家關鍵資訊基礎設施的護，金融業的資安防護計畫方面，比照有F-ISAC、F-CERT和F-SOC三項金融資安機制。

金融產業領域多元，跨金管會轄下的證券、期貨等產業在2021年11月30日正式成立「證券暨期貨市場電腦緊急應變支援小組」（Security and Future Computer Emergency Response Tean，SF-CERT），對象由最需證券交易所、臺灣期貨交易所、證券櫃檯買賣中心、臺灣集中保管結算所，以及相關同業公會所共同合作維運，自2022年開始辦理資安演練及相關教育訓練課程，全天候協助業者應變資安事件，包含事前提供資安事件應變以及已結保存處理指引，並且辦理四項資安演練，包括：資安通報、社交工程、資安事件應變桌面演練及DDoS防護演練，事中則有關聲協助、電話聯問諮詢、現場事件應變、數位證據保存以及鑑識調查，提升資安韌質，經由持續性的檢討、改善以及應變，精以提升資安防禦韌性。

在遭逢疫情的黑天鵝時期，數位化科技行生許多金融商品的創新，必須專注的行動以及因業提合作，金融交易系統在創新過程才會具韌性，證券、期貨交易的特性在於「即時性」、「公平性」以及「透明度」，投資大眾的信任及信心是金融交易的基礎。

如果從數位科技發展的趨勢下，必須接受虛擬或是數位金融交易的新生態系，SF-CERT必須緊盯此一流數位轉型，避免讓惡意駭客趁此資訊取得優勢，進而阻止駭客對新生態系產生威脅以及破壞整體金融系統的可信度，協助維持金融穩定是SF-CERT的重要任務，尤其SF-CERT更應該系統性規劃並按照計畫期程落實資安情資、演練、通報以及應變處理。

國內業者的抗此合作期訪，並落實SF-CERT所訂定之規範並以執行，可以讓產業在遭遇大資安事件按照步驟應變，因為事前的四項資安演練就是

在了解自身遭遇該事件如何應變的同時，也檢驗自身的防護力是否需要再強化！

如能在發生資安事件之內的30分鐘內做到初步通報，後續的應變體系才可以7x24回應事件的處理，一再的反覆熟悉才可以發揮平時演練的韌性加以面對。

在全融交易推廣全球化的進程下，擴大國際合作可以借鏡其相關法律以及制度讓SF-CERT的執行更有效用，並且從實踐上的量化趨勢可以衡量國內應有的即時計畫，從而將SF-CERT成為各產業的典範，最終執行SF-CERT的需事人才以及人才可以讓大眾信任序，立基的臺灣。

1.系統性規畫並按照計畫期程落實資安情資、演練、通報以及應變處理

2.產業在遭遇重大資安事件按照步驟應變。

3.檢驗自身的防護力是否需要再強化。

4.發生資安事件之內的30分鐘內做到初步通報，後續的應變體系才可以7x24回應事件的處理。

5.一再的反覆熟悉才可以發揮平時演練的韌性加以面對。

資訊安全建立信賴機制

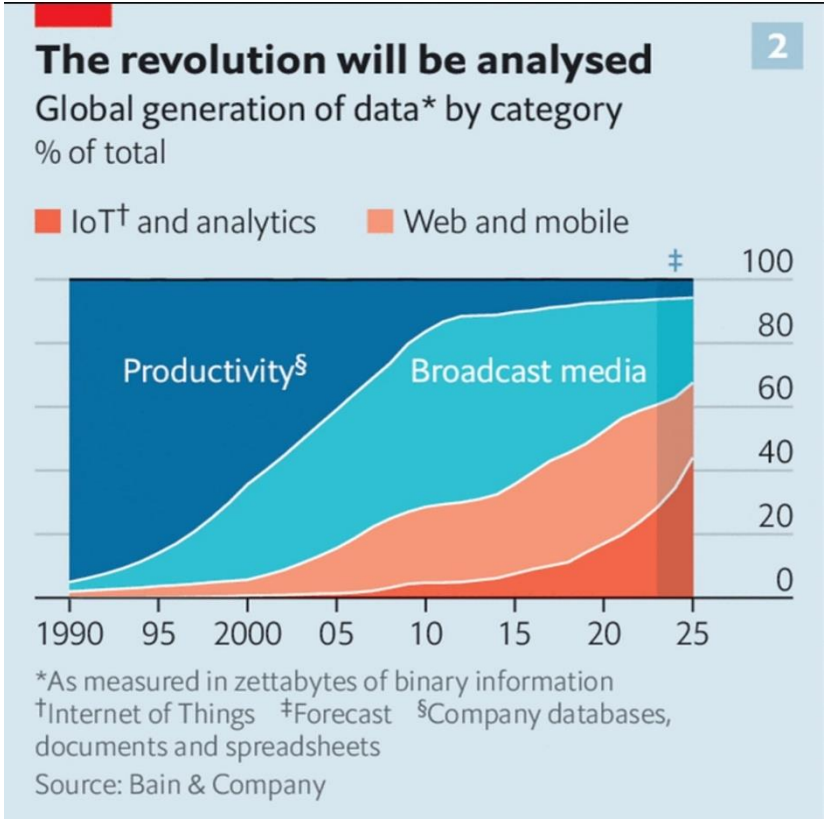
■證券、期貨交易的特性在於

- 「即時性」、
- 「公平性」、
- 「透明度」，

■必須建立讓投資大眾有信任以及信心，如果從數位科技數位發展的趨勢下，有可能使得之前的基礎架構，因應金融科技的發展。

Start with the Why?

10/5 , 2023經濟學人



- Data Sovereignty(資料主權)
  - 資料種類: 生產有關、媒體社群、IOT相關數據以及網頁、行動裝置。
  - 是否就近使用、儲存以及即時分析，一些比較沒那麼關鍵資料送雲端。
- 全球布局(地緣政治)
  - 產線或是數位法規因應各國政府的內政需求，必須透過雲端基礎擴大業務面的布局。
- AI運算
  - 動則數倍價格於現在的運算伺服主機，以及高耗能的AI設備(10-20倍的電力需求)，分散投資轉往雲端。
  - 支付成本含機房土地、電力等設施，以及維運人力。

安碁資訊

雲端運算降低機會成本 - 紐約梅隆銀行

雲端策略

- 將雲端視為旅程，不是目的地。
- 利用公有雲的規模經濟，擷取業務價值、降低風險、提高彈性，並且大力確保基礎設施永遠維持最新的狀態。

多雲端環境中的治理

- 擴展延伸既有的治理流程，並且增強該流程以涵蓋雲端需求。

現代化之旅

- 雲端策略是整體技術和數位之旅的一部分

雲端如何增強彈性

- 下一代的需要的回復力（resiliency posture）。
- 雲端救生艇

雲端應用效果最好的地方

- 雲端在涉及實驗且機會成本高的任何領域，會有很好的效果。因為當你能夠實驗，就有潛在的機會迅速進軍新的業務、測試某個構想。

關於企業中的人工智慧

- AI 和 ML 終究不是魔法。它的核心是利用錯綜複雜的數學處理資料。
- 到頭來，你需要確保你的結果是可解釋的。

重點一：使用雲端服務的治理框架，並考量使用雲端服務對金融機構治理和運營模式影響

金管會自律規範五大重點

金融機構上雲八大重點

01 採取適當風險管控措施

02 金融機構有最終監督義務，但可委託專業第三人輔助監督作業

03 應確保金融機構監理機關或委外查核人員，可取得雲端委外作業的執行資訊，包括實地查核權

04 使用同一雲端供應商的金融機構，可聯合委託第三方查核雲端業者

05 明定資料傳輸及儲存上雲端要有保護措施和加密金鑰管理機制

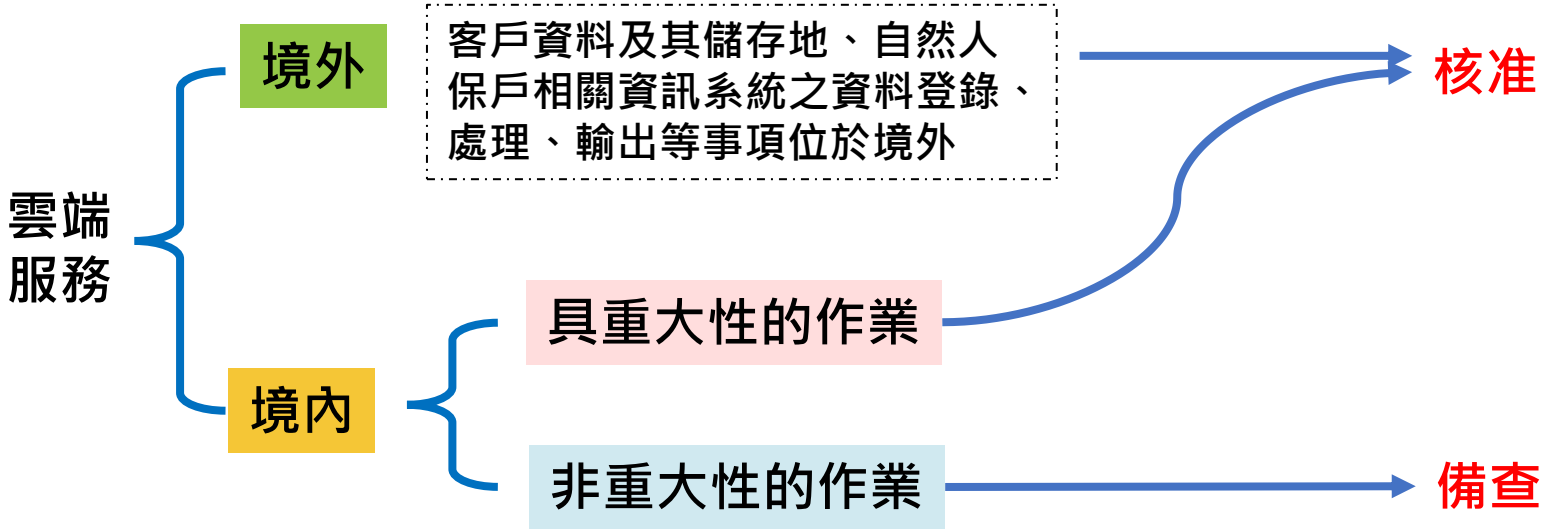
06 須確保雲端供應商不得有存取顧客資料的權限及用於非委託之用途

07 應訂定緊急應變計畫，涵蓋服務中斷委託結束後的轉移等，也要確保委外儲存的資料全數銷毀

08 租用境外雲端服務須符合 3 要求，可指定資料處理及儲存地、境外個資法規不得低於我國，及要有境內備份

金融機構委外作業涉及雲端申請規定

- 金管會將依照雲端作業委外的重大性與否，區分為「核准制」以及「備查制」。
- 作業委託他人處理涉及使用雲端服務，具重大性的委外作業，或將作業委託到境外者，應檢具書件向主管機關申請核准始得辦理，事先向金管會提出申請。
- 非以上範圍的委外作業（非重大性的委外作業），得檢附簡化申請書件報請備查。



重點二：使用雲端服務的安全管理，應執行適當盡職調查及持續監控雲端服務安全性

金管會自律規範五大重點

金融機構應定期對雲端服務進行查核

金融機構聯合委託具資訊專業之獨立第三人查核

可考量聯合查核（獨立第三人查核之要求）

- 鑒於雲端科技具相當專業複雜度，金融機構對受託機構進行查核，得自行或與其他金融機構聯合委託具資訊專業之獨立第三人查核為之；
- 考量雲端業者委託之獨立第三人，對於我國相關法規，銀行公會資安標準以及委託銀行本身之相關要求，似未較銀行自行委託者熟稔，我國相關法規及制度，仍以自行委託或與其他金融機構（聯合）委託為限。

金融機構所發起（聯合）委託之查核

直接引用雲端業者已有之證照或查核結果

金融雲端規定辦理事項與解決方案

政策
- 應訂定使用雲端服務之政策及原則，採取適當風險管控措施，並應注意作業委託雲端服務業者之適度分散。

監督
- 金融機構對雲端服務業者負有最終監督義務，並應具有專業技術及資源，監督雲端服務業者執行受託作業，並得視需要委託專業第三人以輔助其監督作業。

查核
- 金融機構得自行委託，或與委託同一雲端服務業者之其他金融機構聯合委託具資訊專業之獨立第三人查核

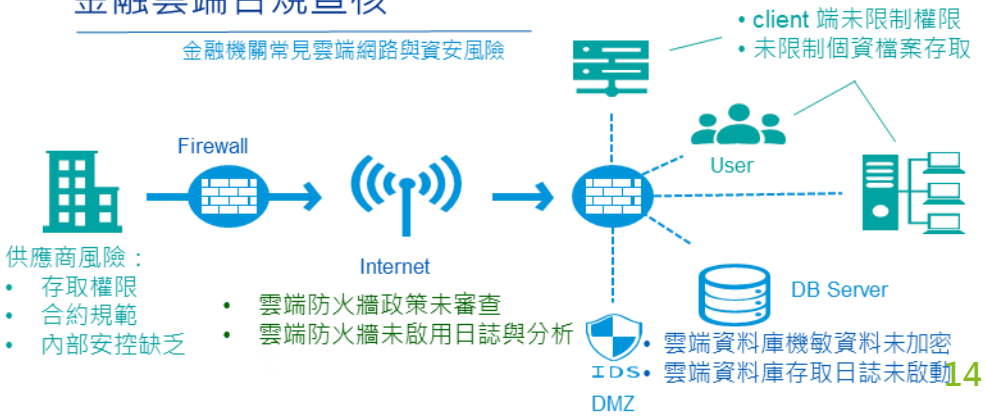
法源 ：金融機構作業委託他人處理內部作業制度及程序辦法 (§18)

雲端資料分析

依據雲端業務流程特性，進行雲端資料分布，符合組織雲端安全政策規範

金融雲端合規查核

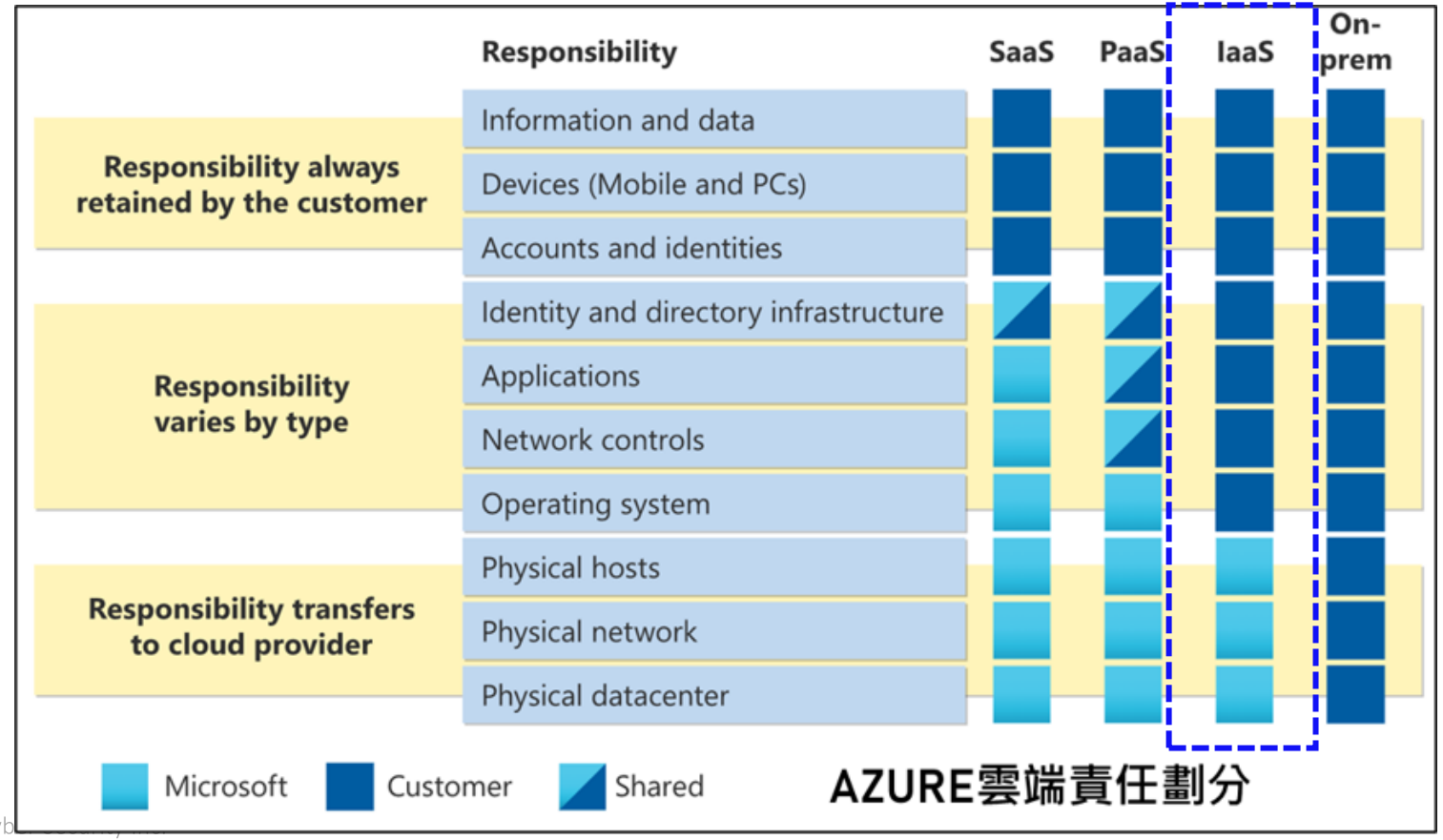
金融機關常見雲端網路與資安風險



持續監控，及時應對，重大事件通報及緊急應變機制

雲地聯防 Cloud SOC

Cloud SOC – Hybrid Cloud



安碁資訊布局雲地聯防架構（組合式方案）

多雲 + 地端，高度複雜環境

雲地整合，單一 SOC 監控中心

服務環境

SIEM

Cloud

Azure

aws

Google Cloud

多種公有雲環境

雲到雲

Microsoft Sentinel

IBM ArcSight

QRadar splunk>

雲端 SIEM 平台

SIEM

雲到地

地到雲

On-Premise

Firewall

WAF

Server

Mail Spam

多種地端設備

地到地

IBM ArcSight

QRadar splunk>

多種 SIEM 平台

SIEM

彙整

ACSI SOC

安碁資安監控中心

大數據關聯分析平台

人工智慧AI分析平台

資安情資與威脅獵捕

Hybrid Monitor

Ticket system

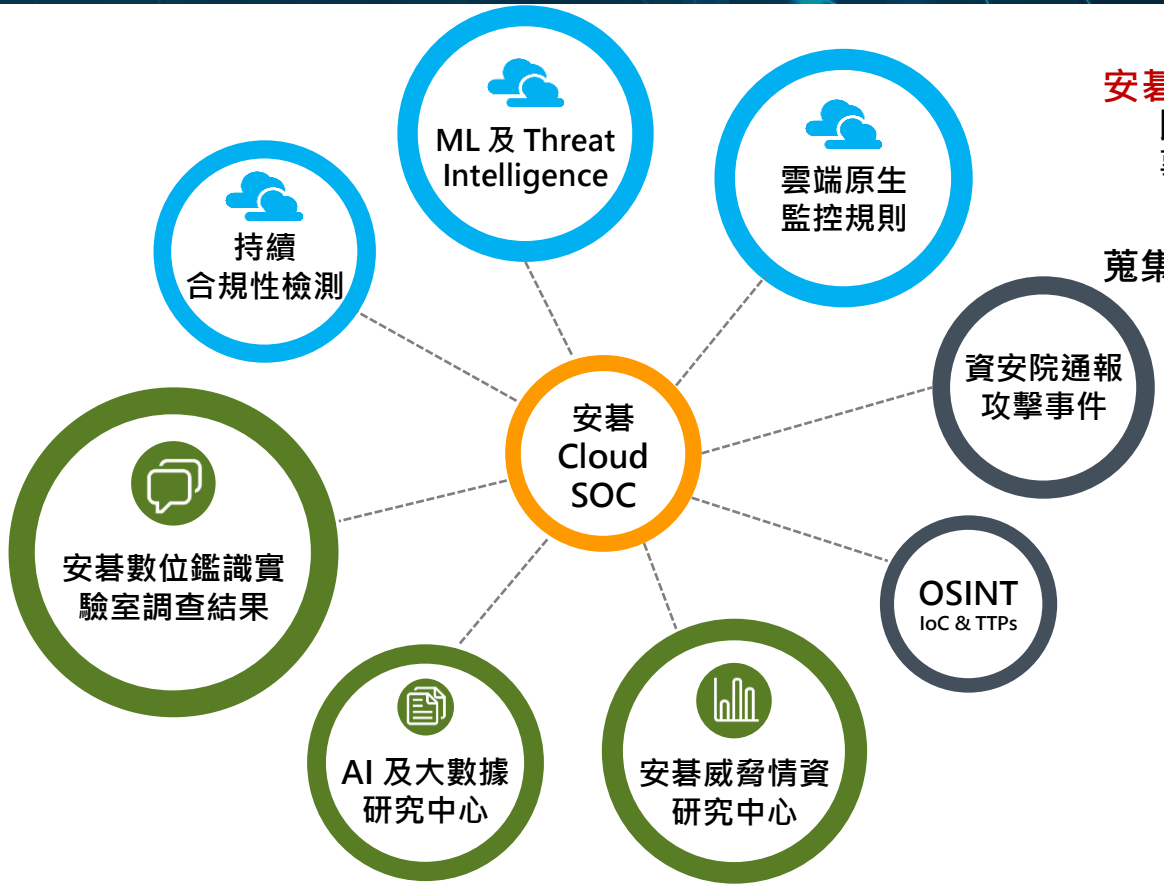
資安儀表板

事件通報

客戶通報對象

SIEM: Security Information and Event Management

整合雲地資源，持續監控雲地端服務



安碁透過多種來源蒐集新型態攻擊資訊，並即時新增、調整規則，以因應新型態攻擊事件

蒐集與分析新型態資安資訊之方法為：

- 分析所蒐集之資安資訊，據以研究駭客如何應用**新型態攻擊手法**
- 辨識何種資安設備或設備日誌，可偵測此類之新型態攻擊事件
- 整合**雲地情資進行比對**，並進行關聯分析
- 實際測試並分析資安設備所回傳之日誌內容，據以**新增、調整規則**，以偵測新型態攻擊事件
- 根據偵測事件，比對**合規性檢測**，降低整體風險

重點三：應制定流程來識別、衡量、監控和控制與雲端服務相關風險

金管會自律規範五大重點

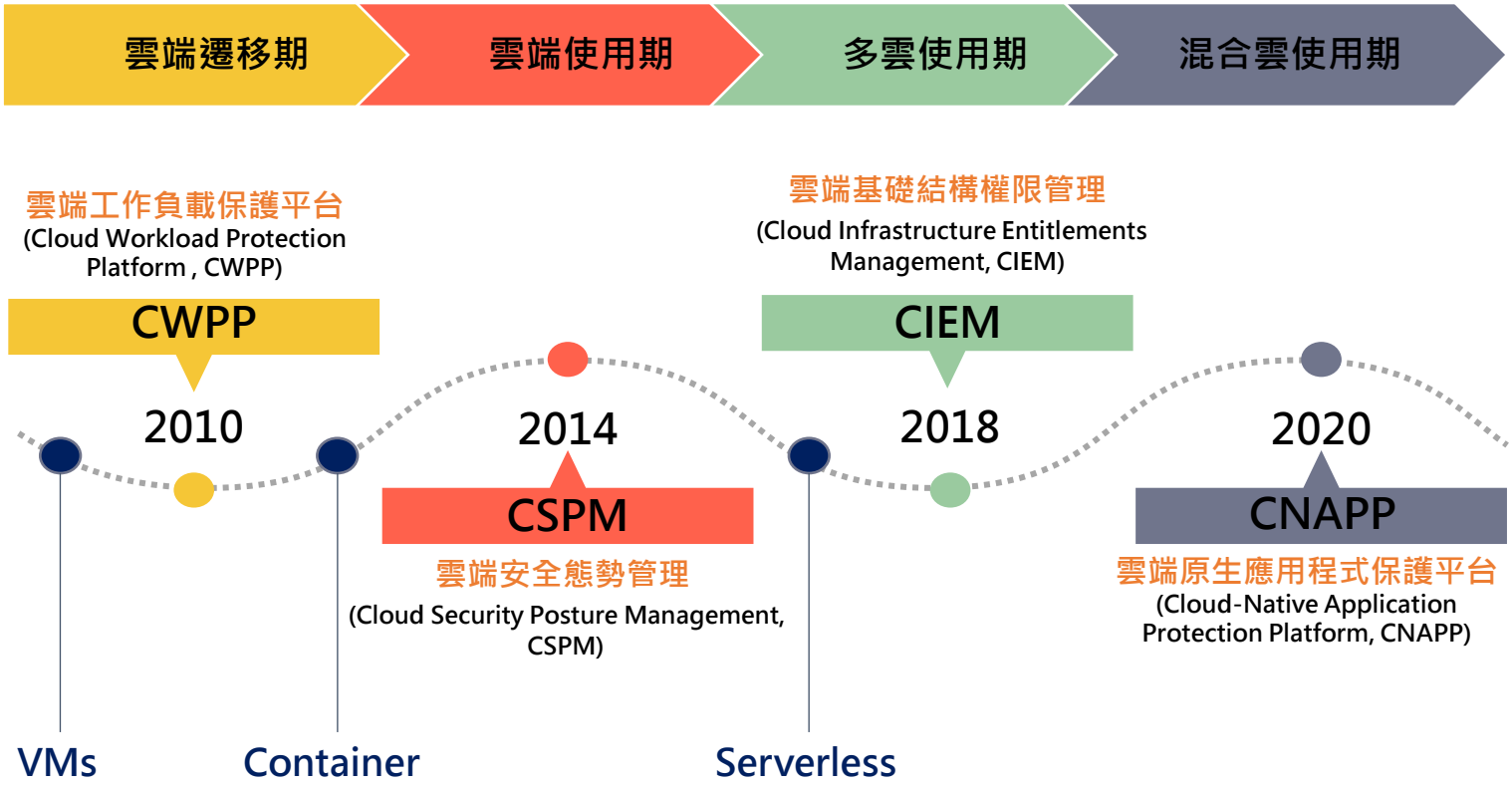
雲端資安的威脅(風險)

- **設備、用戶缺乏可視度**
  - 因為可能從第三方網路進入
- **多租戶**
  - 共享
- **設備無法控管**
  - BYOD
- **對第三方的法規稽核有難度**
  - 國外雲服務商
- **配置政策不洽當**
  - 管控不佳、權限不當

雲端資安健診

基於雲端安全組態，精準診斷，全面保護

雲端原生安全的發展時間線



比較表：CWPP、CSPM 以及 CIEM

功能/服務	CWPP	CSPM	CIEM
功能	漏洞管理、運行時保護、應用程式控制、資料保護	安全配置評估、風險管理、合規性檢測	權限審核、遵循最小權限原則、身份和權限分析
目的	是**內部**的，用於在雲端執行的軟體中尋找威脅，確保工作負載安全性	是**外部**的，用於尋找雲端資源配置錯誤以及合規性違規	**最小化**濫用/誤用雲端權限的風險
應用範圍	保護**應用程式**和**工作負載**	減少**雲端資源配置**錯誤的風險	管理和監視**雲端基礎架構的權限**
自動化	提供自動化的漏洞修復和威脅應對	強調自動化的安全配置修復	支援自動化權限管理和審核
合規性	**支援**滿足行業和法規合規性	**提供**合規性檢測和管理	**支援**權限合規性審核和報告

雲端資安健診檢測八大項目

01 **雲端身份識別與權限管理**

監視和更新使用者權限，以確保與其職責相符。

02 **雲端安全組態掃描**

掃描雲端資源組態，確保符合安全最佳實踐。

03 **雲端儲存體惡意活動檢視**

檢查是否存在未經授權的訪問或意外公開的檔案或文件。

04 **雲端資料庫安全檢視**

確保資料庫的訪問權限和身份驗證機制得到妥善配置和管理。

05 **威脅檢測**

使用行為分析檢測來辨識潛在威脅

06 **法規合規性檢測**

檢查雲端環境的組態和操作是否符合相關法規和合規性標準。

07 **工作負載弱點掃描與惡意活動檢視**

監視工作負載，檢測異常活動和惡意行為。

08 **軟體安全性檢測 (開發環境)**

檢查程式碼中的潛在漏洞和安全弱點。

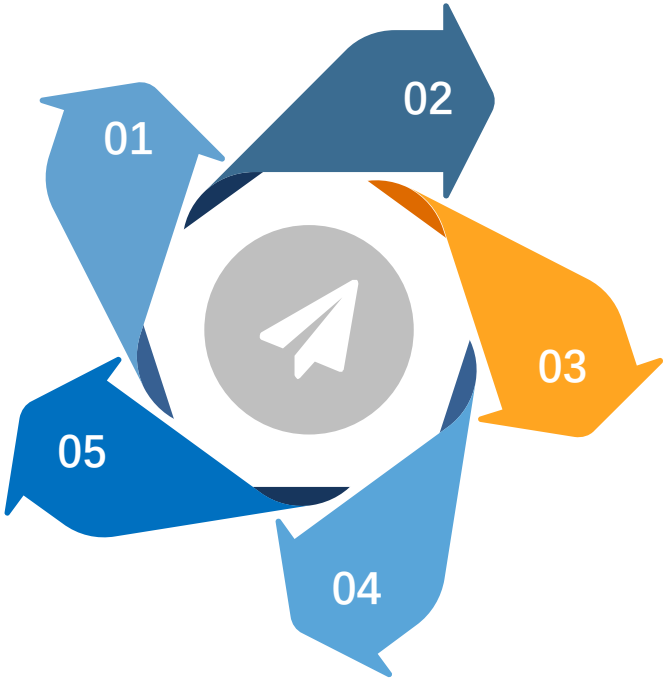
雲端資安健診為金融機構帶來之效益

符合法規及合規性

- 確保雲端資源的設定，符合法規框架基準及合規性要求
- 資安政策的制定與優化

態勢管理

- 識別雲端資產
- 清查雲端資源的使用情況
- 確保資安政策的落實
- 涵蓋身份識別、安全組態檢測、軟體安全性檢視等



降低資安風險

- 識別安全漏洞或錯誤設定造成的資安風險和漏洞
- 提高整體雲端環境安全性

防範資料外洩

- 監控雲端設定，減少資料外洩的風險

提高資安意識

- 分析雲端環境弱點，促使對資安的重視
- 提高人員資安意識

重點四：使用雲端服務應有資訊安全維護意識及人員培訓計畫

金管會自律規範五大重點

雲端服務安全教育訓練

雲端資訊安全人力培訓

安碁學苑：雲端服務安全教育訓練

https://www.acsiacad.com/course_list/1021

雲端安全人才培育

Certificate of Cloud Security Knowledge (CCSK)

- 完整包含 14 個雲端資安知識領域
- 快速幫您建構完整雲端安全知識
- 通過測驗，即獲頒 CSA 原廠's CCSK 國際認證

晉身國際雲端資安認證專家

展現雲端安全專業知識技能

建立廣泛完整雲端資安職能

哪些人適合?

- 資安分析師、資安架構師、資安工程師、資安管理師、資安顧問、法令遵循主管、系統工程師，資安長 …

重點五：金融機構和雲端服務業者的合約應明確說明雙方責任畫分

金管會自律規範五大重點

雲端委外服務提供商查核主要依據與合約要求

- 台灣國內目前針對雲端應用之安全要求主要以金管會修訂之《金融機構作業委託他人處理內部作業制度及程序辦法》及銀行公會訂定之《金融機構運用新興科技作業規範》為主。
- 其中雲端服務提供業者應遵循之事項如下：

金融機構作業委託他人處理內部作業制度及程序辦法

- 不得有存取客戶資料之權限，且不得為委託範圍以外之利用
- 資料保護措施
- 定期報告與操作紀錄
- 資料刪除/銷毀作業及其記錄
- 內部資安管理與風險控管作業
- 境外廠商特別規範

金融機構運用新興科技作業規範

- 服務協議簽訂
- 提供給委託者之雲端資源與其他委託者獨立
- 資料保護措施
- 緊急應變計畫
- 資料取得權力
- 資安事件通報程序
- 資料刪除
- 境外雲端服務提供商作業要求

金融機構與雲端服務業者間的雲端服務合約

- 客戶資料保密
- 風險管理、內部控制稽核制度
- 重大異常或缺失通知機制
- 消費者爭端解決機制
- 聘僱人員之管理
- 契約終止或解約之條款
- 其他契約重要約定事項

共同供應契約採購(雲端服務)

✓ 廠商履約內容涉及資通安全者，應符合 ISO 27001（或 CNS 27001）、 ISO 27017（或 CSA STAR）、ISO 27018 所定標準。

服務水準管控	資通安全責任	契約終止
本署得派員或採用技術、設 備監看、檢查或稽核廠商提供之服務狀況況，廠商應以合作之態度在合理 時間內提供相關書面資料，或協助約談相關當事人或配合並提供必要資源。	遵守資通安全管理法、其相關子法及數位發展部資通安全署所頒 訂之各項資通安全規範及標準，並遵守機關資通安全管理及保密相關規 定。	廠商應依約定或機關指定之期間內，返還以前 持有屬於機關所有之資料，或經機關同意在其監督下以自己之費用銷毀 所有屬於機關之資料。
有關履約期間以下都必須進行通報，因資本額變動而有成為第三區有陸資成分者，資料存取、備份及備援之實體所在地為大陸地區、資料傳輸途徑與流向經過大陸地區，專案成員、設備為陸籍以及大陸廠牌。	數位發展部資通安全署籌組專案團隊稽核或其他適當方 式執行相關稽核或查核的權利。	
本署依照辦理稽核時，得委由專業之第三人稽核廠商提供之服務，費 用由本署負擔。 廠商作業經本署檢查或稽核結果不符合本契約規定者，需於接獲本署通 知期限內改善。	廠商提供服務前，應先行檢查所使用之軟硬體有無內藏惡意程式及隱密通道（covert channel）。	
	如違反資通安全相關法令、知悉機關或廠商發生資安事 件時，均必須於 1 小時內通報機關及本署軟體採購辦公室。	


THE BEST IS YET TO COME
工商服務

公司簡介

公司成立：2000年

上櫃日期: 2019.10.30(國內唯一資安服務公司)

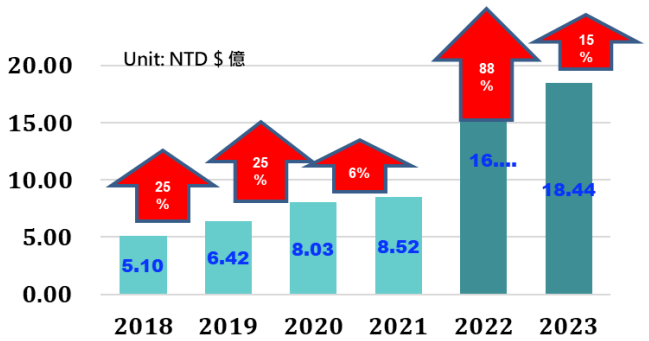
資本額：新台幣 2.22億

員工 數： 601 (ACSI+ACAD+eDC)

董事長：施宣輝

總經理：吳乙南

財務主管：譚百良



Since 2001/10

宏碁股份有限公司
Acer Inc.
(AI)

安碁資訊股份有限公司
(ACSI)

100 %(持股)

100 %(持股)

安碁學苑
股份有限公司
(ACAD)

宏碁雲架構服務
股份有限公司
(eDC)