

WELCOME TO OUR NEW


支付應用 & 金融應用

以專業的產業知識與創新卓越的技术
專注於支付清算與資訊安全的系統研發

從作業風險談金融亂碼化 作業管理

Agenda

- ☒ 作業風險與服務品質
- ☐ 銀行資安與硬體亂碼化設備規範
- ☐ 亂碼化作業管理
- ☐ 低風險的亂碼化服務方案
- ☐ Q&A



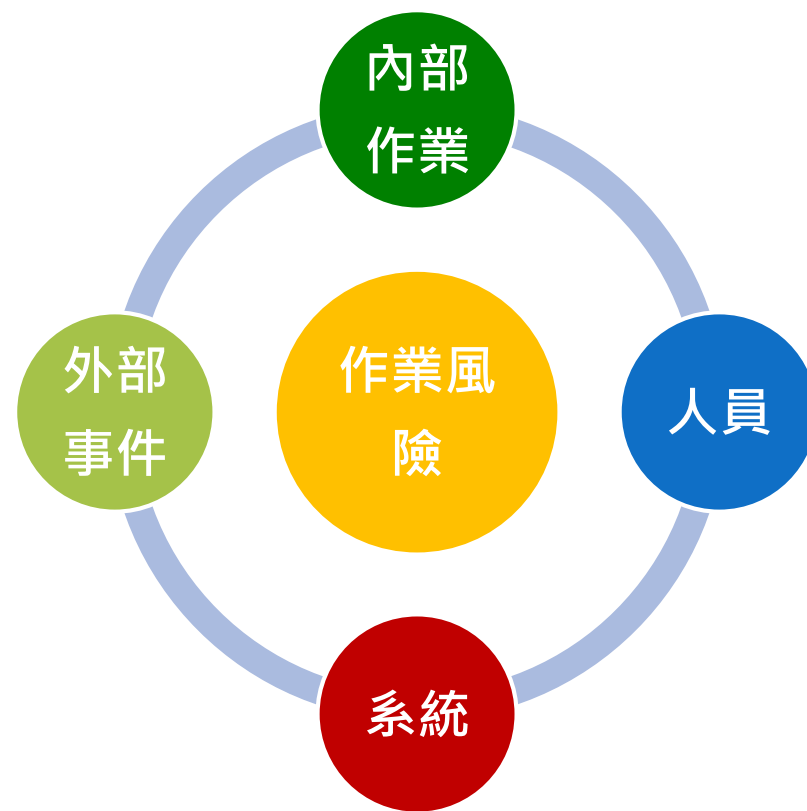
以「成就客戶」為經營理念，秉持著專業、誠信的理念服務客戶。

作業風險之定義

依據Basel之定義，作業風險係指「起因於銀行內部作業、人員及系統之不當或失誤，或因外部事件造成損失之風險，包括法律風險，但排除策略風險及信譽風險。」。

作業風險損失之型態：

事件型態	類別	說明
1.內部詐欺	未經授權/詐欺	舞弊案件
2.外部詐欺	資安/詐欺	駭客攻擊
3.雇用慣例、工作場所安全	環境安全/員工關係	工會活動
4.客戶、產品、營業行為	產品瑕疵/曝險	產品設計問題
5.人員或資產損失	災害	天然災害
6.營運中斷與系統當機	資訊系統	軟硬體故障
7.執行、運送及作業流程之管理	資料處理/作業問題	資料輸入錯誤



資料來源：銀行局作業風險分組第一階段研究報告

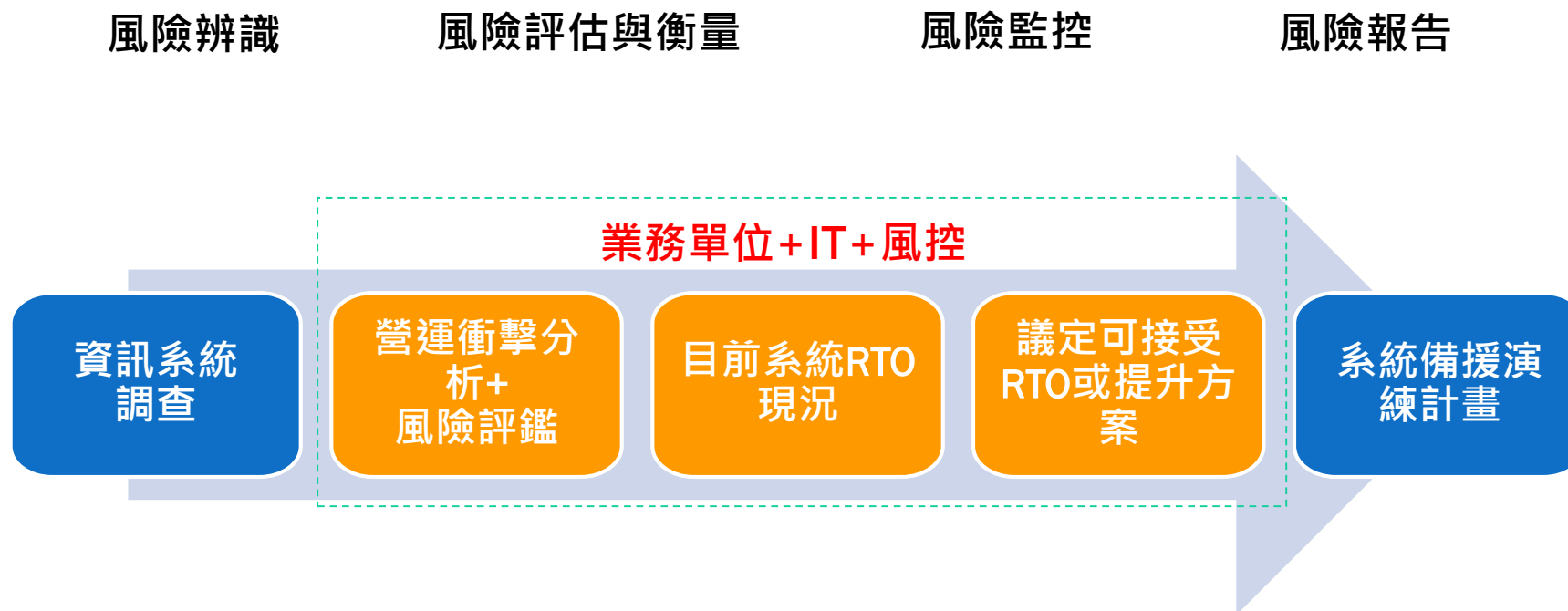
近期重大作業風險事件

事件日期	銀行	事件說明	金管會
2021-10-18	國泰世華銀行	系統升級發生異常交易事件： 於110年10月18日及19日部分時段發生系統異常致影響網路銀行(含行動銀行APP)、自動櫃員機(ATM)近4萬筆跨行交易受影響事件	<ul style="list-style-type: none"> 該行郭董事長等人到金管會報告，由主委黃天牧親自主持，聽取該行應變處理檢討情形外，並要求該行儘速對外說明。 受影響國泰世華銀客戶一年台幣跨行免5次手續費，包括轉帳、提款估計賠償金額約千萬元
2020-10-10	台北富邦銀行	<p>辦理轉帳業務時，因系統異常導致系統連接問題，該行未能完善辦理系統轉帳業務，規劃、評估、測試及檢覈等作業缺失，有礙該行健全經營之虞。</p> <p>商譽損失無法估算</p>	依銀行法第61條之1第1項規定，予以糾正。結果： 應予糾正 。
2018-08-18	財金公司	因IBM大型主機連線管理系統程式(IMS系統)異常，導致ATM跨行提款或轉帳交易無法使用。	財金公司對於提供金融服務之資訊系統廠商，未能妥適監督，致跨行系統發生服務中斷事件，影響民眾便利性違反銀行法第47條之3第1項授權訂定之第31條規定， 核處150萬元罰鍰

資料來源：金管會銀行局

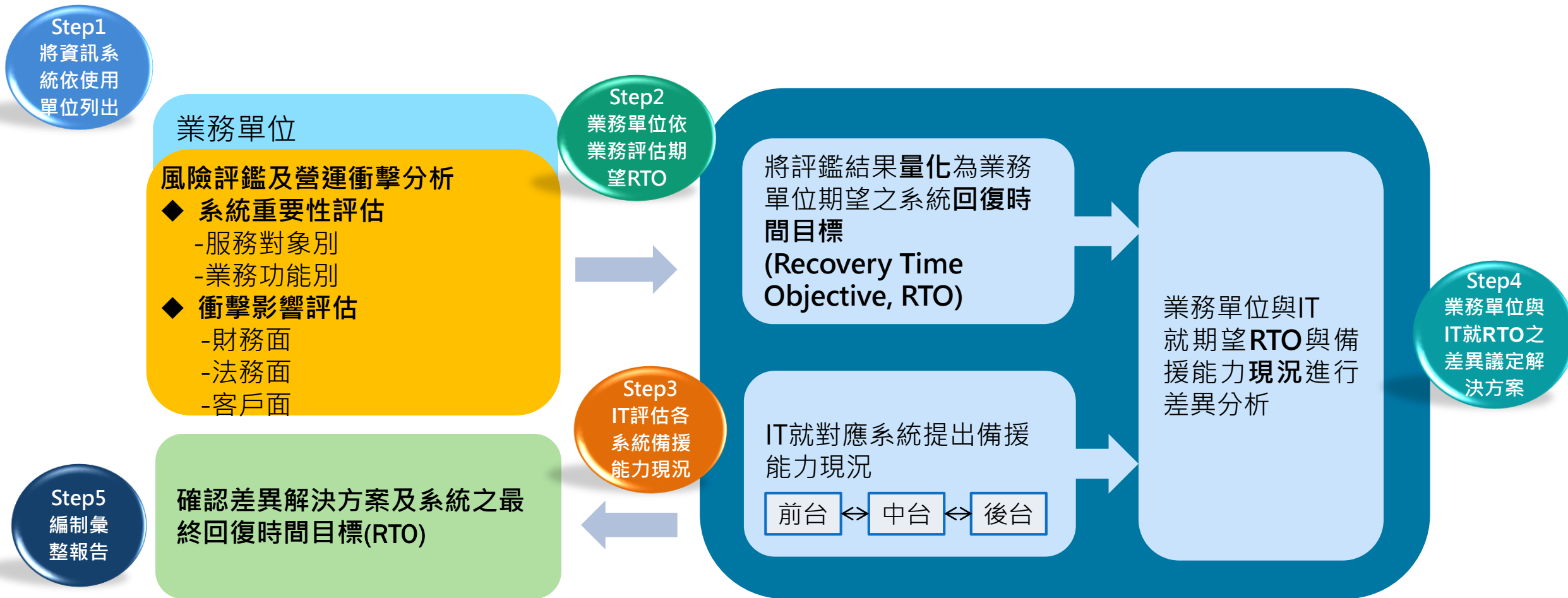
作業風險與系統備援

應用系統備援機制應經由資訊部門與業務主管單位就業務重要性共同決定，依銀行之『營運衝擊分析(BIA)及風險評鑑(RA)機制』，建立系統備援機制，降低銀行營運作業風險



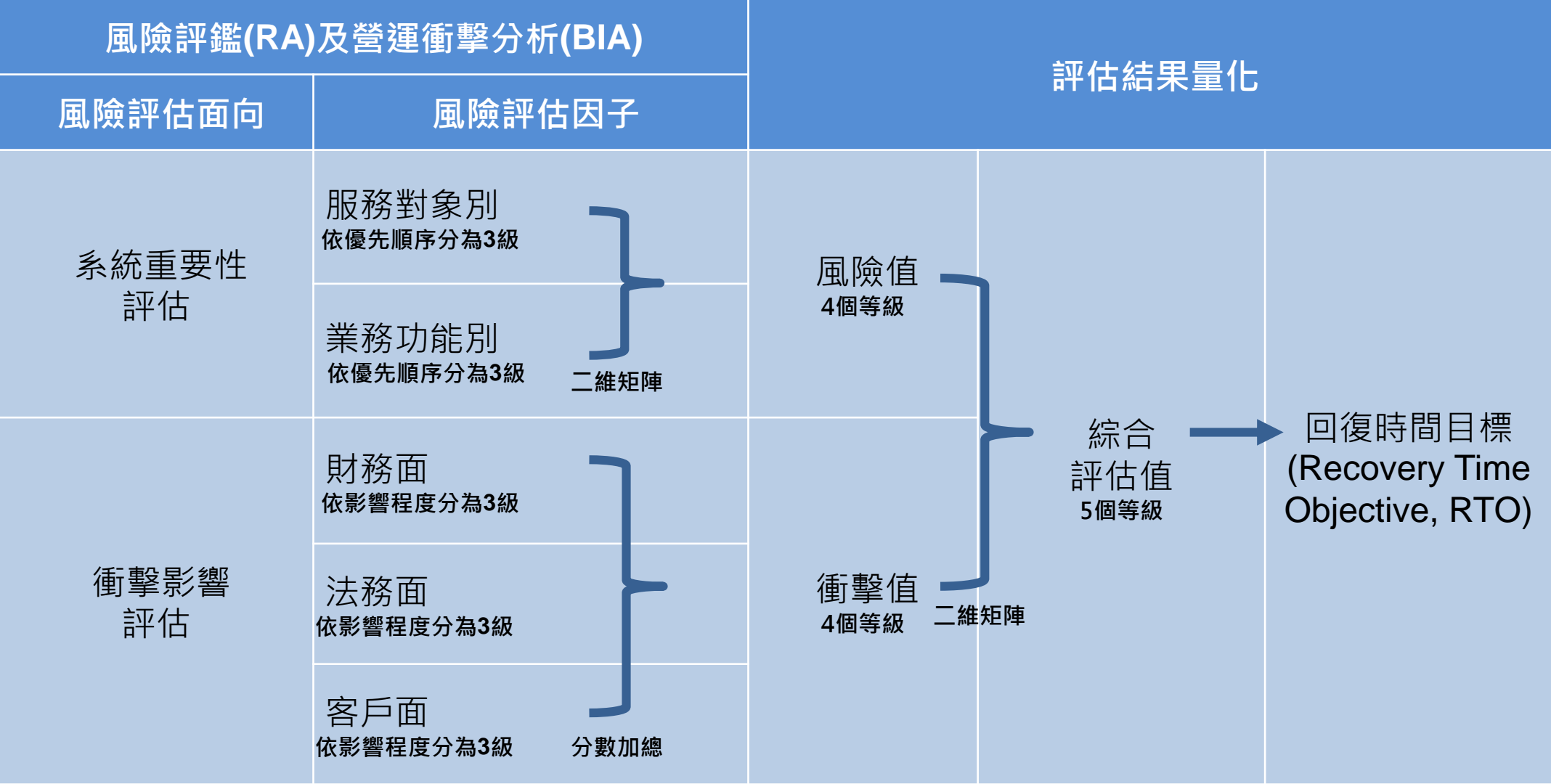
營運衝擊分析及風險評鑑機制

Business Impact Analysis(BIA) & Risk Assessment(RA)

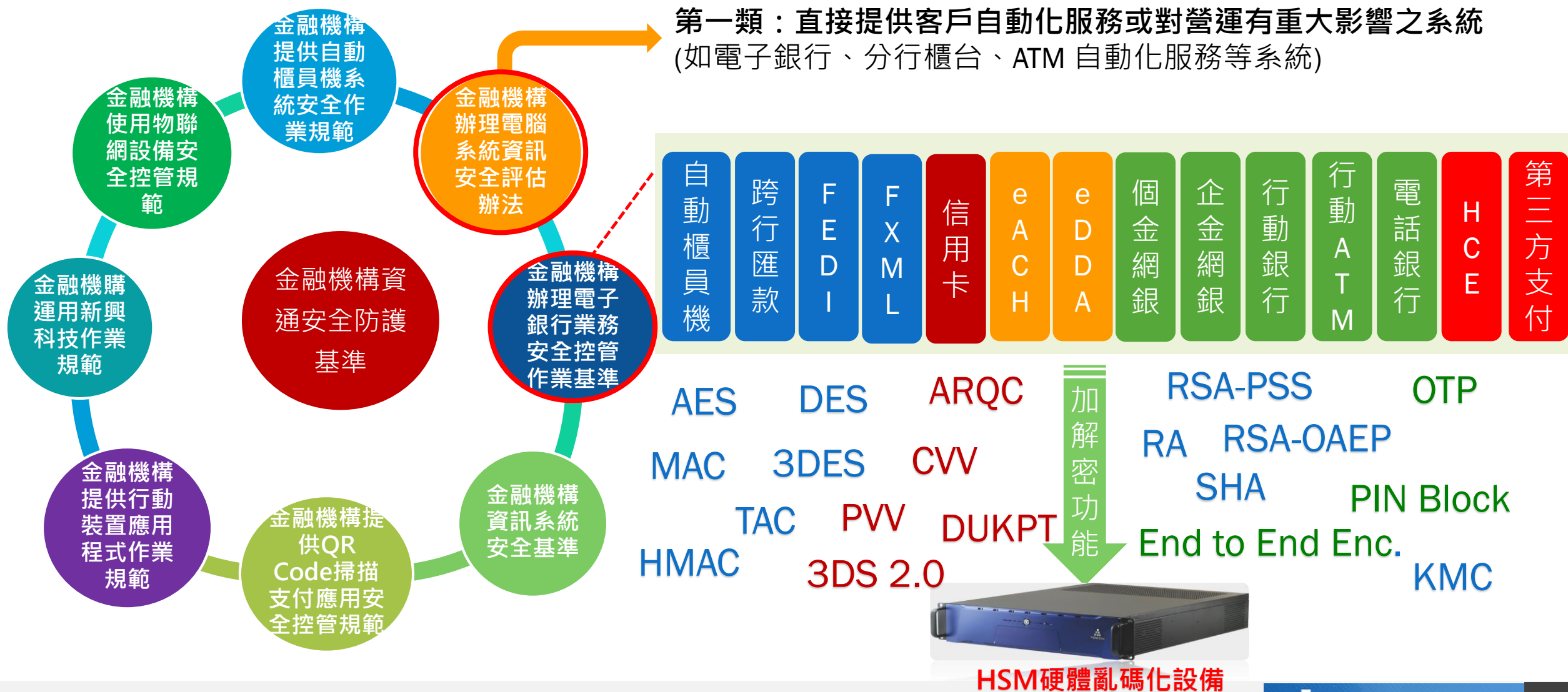


前、中、後台系統需同時評估，並取系統復原時間最長者為其備援能力，同時找出最重要的共用設備。

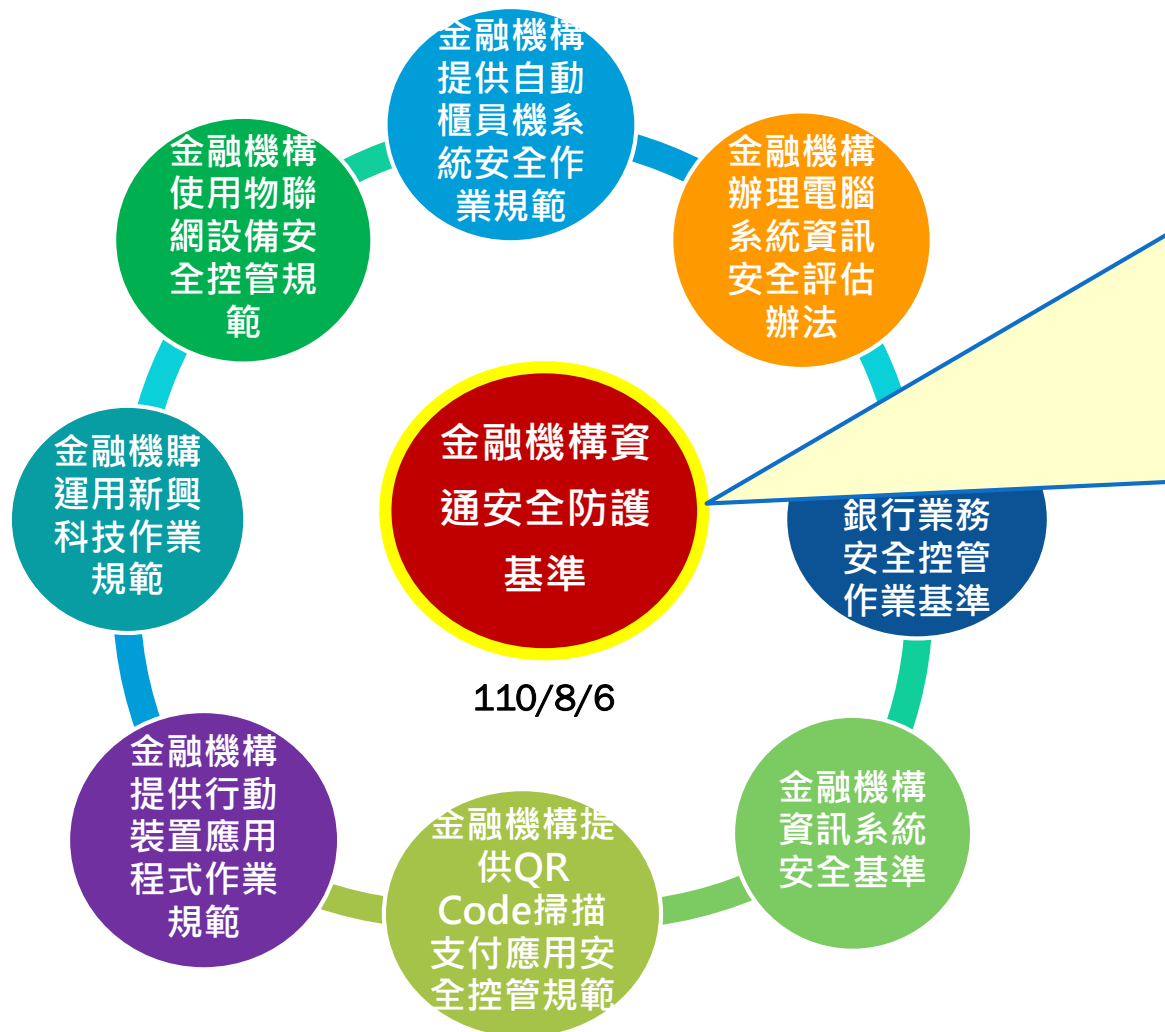
營運衝擊分析及風險評鑑機制之量化流程



BIA及RA與電子銀行應用(1/2)



BIA及RA與電子銀行應用(2/2)



- RTO 2 小時/4小時?
- 第十八條「營運持續管理應符合下列要求」之第二款：
「應建立對於重大資訊系統事件或天然災害之應變程序，並確認相對應之資源，以確保重大災害對於重要營運業務之影響在其**合理範圍**內」。
- 重點在於不要影響客戶權益，即**避免客訴**。
- 因應國泰世華系統升級事件，金管會已責成銀行公會修訂「金融機構資通安全防護基準」，將非核心資訊系統但對會影響客戶權益(資訊安全評估中的第一類系統)之重要軟體，比照核心系統辦理。

Agenda



- ☐ 作業風險與服務品質
- ☒ 銀行資安與硬體亂碼化設備規範
- ☐ 亂碼化作業管理
- ☐ 低風險的亂碼化服務方案
- ☐ Q&A

銀行資安與硬體亂碼化設備規範



金融資訊系統硬體亂碼化設備規範(1/4)

- ◆ 財政部於82年要求各金融機構：金融卡密碼相關交易處理應使用**硬體亂碼化設備**。
- ◆ 財金公司83年制定「**金融資訊系統硬體亂碼化設備規範**」，函送各金融機構，作為採購硬體亂碼化設備之參考，主要內容：
 - 設備**專屬專用**，不得用於處理與資料亂碼化無關之作業
 - 設備所提供之各種亂碼化功能原則上應於**設備內**一次處理完畢
 - 主基碼(Master Key)必須儲存於**設備內**
 - 設備不得具備可將基碼以**明碼格式**或以已知內容之基碼亂碼後輸出之功能
 - 除執行密碼產製外，客戶密碼應經**格式化**並**亂碼後**始得輸出
 - 設備之基碼管理，應達除非串通至少二位基碼安全 控管人員否則基碼不會外洩之標準
 - 設備應具備嚴謹之安全防護措施，於外力侵入或破壞防護措施時，能消除儲存於設備中之所有可能洩漏之秘密資料及基碼



金融資訊系統硬體亂碼化設備規範(2/4)

- ◆ 銀行公會於99年訂定「**金融機構辦理電子銀行業務安全控管作業基準**」，函送各金融機構，作為執行電子銀行業務系統之安控標準
- ◆ **電子銀行(Electronic Banking)業務**：係指在金融機構與客戶，透過各種電子設備及通訊設備，客戶無須親赴金融機構櫃台，即可直接取得金融機構所提供之各項金融服務
- ◆ 本安控基準使用之密碼學演算法：
 - (一) **對稱性加解密系統**：採用資料加密標準(DES/3DES)及進階資料加密標準(AES)等運算進行資料加密
 - (二) **非對稱性加解密系統**：採用 RSA 加密演算法、橢圓曲線密碼學(ECC)等運算進行簽章加密
 - (三) **訊息鑑別系統**：採用訊息鑑別碼(MAC、HMAC)、雜湊函式(Hash Function；如 SHA256)等運算
- ◆ 交易面之安全需求依安全防護措施之不同分述如下：
 - (一) **訊息隱密性(Confidentiality)**：訊息不會遭截取、窺竊而洩漏資料內容致損害其秘密性
 - (二) **訊息完整性(Integrity)**：訊息內容不會遭篡改而造成資料不正確性，即 訊息如遭篡改時，該筆訊息無效
 - (三) **訊息來源辨識(Authentication)**：傳送方無法冒名傳送資料
 - (四) **訊息不可重複性(Non-duplication)**：訊息內容不得重複
 - (五) **無法否認傳送訊息(Non-repudiation of sender)**：傳送方無法否認其傳送訊息行為
 - (六) **無法否認接收訊息(Non-repudiation of receiver)**：接收方無法否認其接收訊息行為

硬體亂碼化設備



金融資訊系統硬體亂碼化設備規範(3/4)

◆ 「金融機構辦理電子銀行業務安全控管作業基準」對HSM規格之要求：

- 採用加密演算法者，其金鑰應儲存於經第三方認證(如 **FIPS 140-2 Level 3** 以上)之**硬體安全模組**內並限制明文匯出功能
- 開立第一類帳戶並採用高風險之介面安全設計進行身分驗證者，憑證私鑰 應儲存於經第三方認證之硬體裝置
- 該裝置之**晶片**應符合我國國家標準 CNS 15408 EAL 4+.....或 **FIPS 140-2 Level 3** 以上或其他相同安全強度之認證，以防止該私鑰被 匯出或複製
- 硬體設備為防止敏感資料外洩得採用資料輸出管控機制、**破壞偵測與歸零清除保護機制**、或其他足以保護設備內敏感資料之安全設計
- 傳輸敏感資料時，應提供端點對端點加密機制(如 end-to-end encryption, E2EE)，傳送至金融機構端符合 **FIPS 140-2 Level 3** 以上之硬體安全模組(如 HSM)內進行解密

金融資訊系統硬體亂碼化設備規範(4/4)

◆ 銀行公會參照ISO27001及相關資安規範訂定「金融機構資通安全防護基準」，於110/08/06公告，作為未來金檢查核重點

一. 資訊安全政策、內部組織及資產管理

十一.網路管理

二. 營運環境管理人員

十二.系統生命週期管理

三. 個人資料保護

金鑰應 儲存於經第三方認證並符合 NIST FIPS 140-2 L3 之硬體安全模組內 並限制明文匯出功能

四. 機敏資料隱密及金鑰管理

十四.供應商管理

五. 營運環境之實體安全

於營運環境採用硬體安全模組保護金鑰者，該金鑰應由非系統開發及維護單位之二個單位以上產製，並分持管理其產製之基碼單

六. 營運管理

十六.營運持續管理

七. 核心資通系統、第一類電腦系統之營運環境容量管理

十七.法令遵循管理

八. 脆弱性管理

九. 測試環境管理

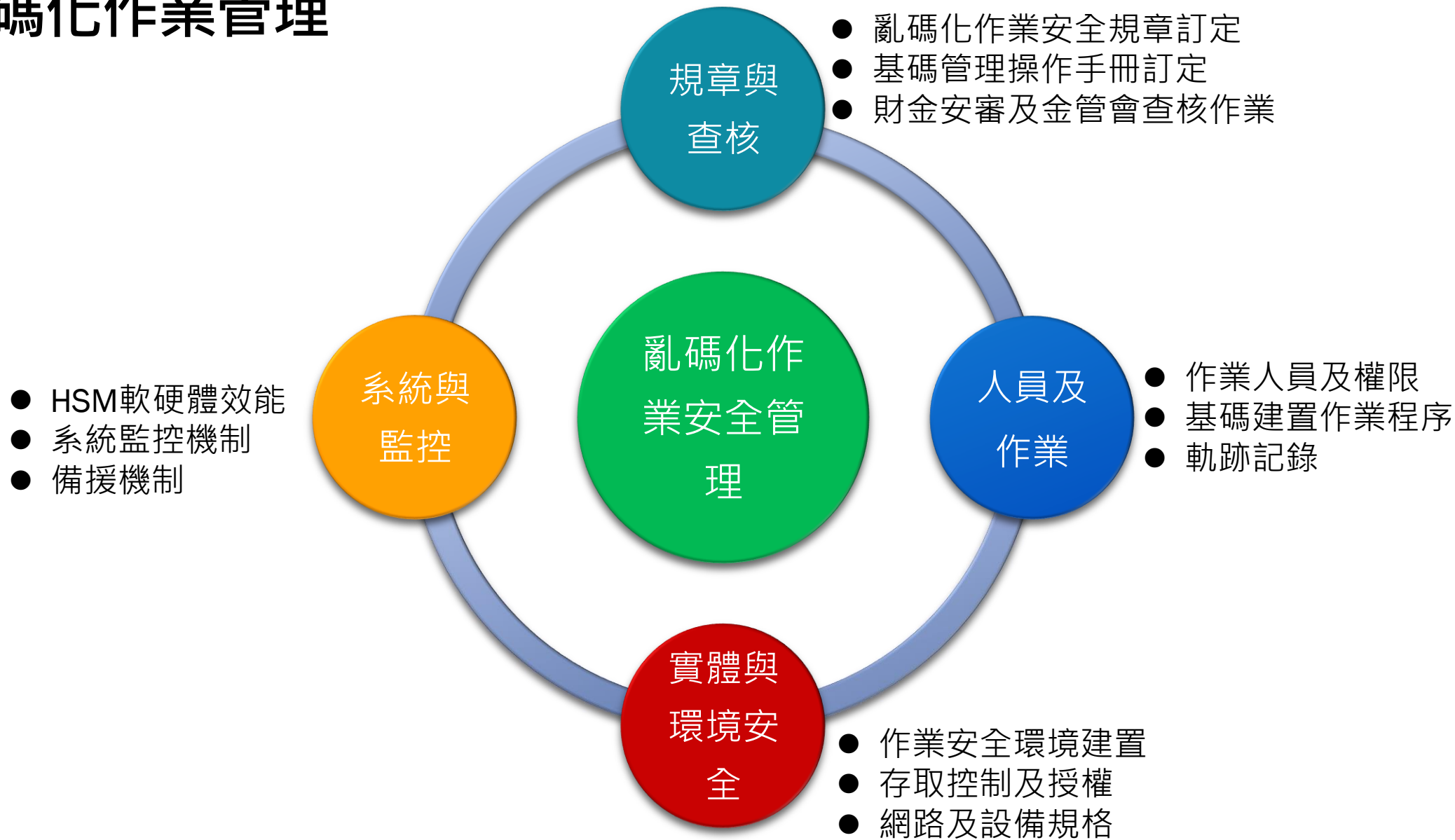
十. 辦公環境管理

Agenda



- ☐ 作業風險與服務品質
- ☐ 銀行資安與硬體亂碼化設備規範
- ☒ 亂碼化作業管理
- ☐ 低風險的亂碼化服務方案
- ☐ Q&A

亂碼化作業管理



亂碼化作業管理—規章與查核

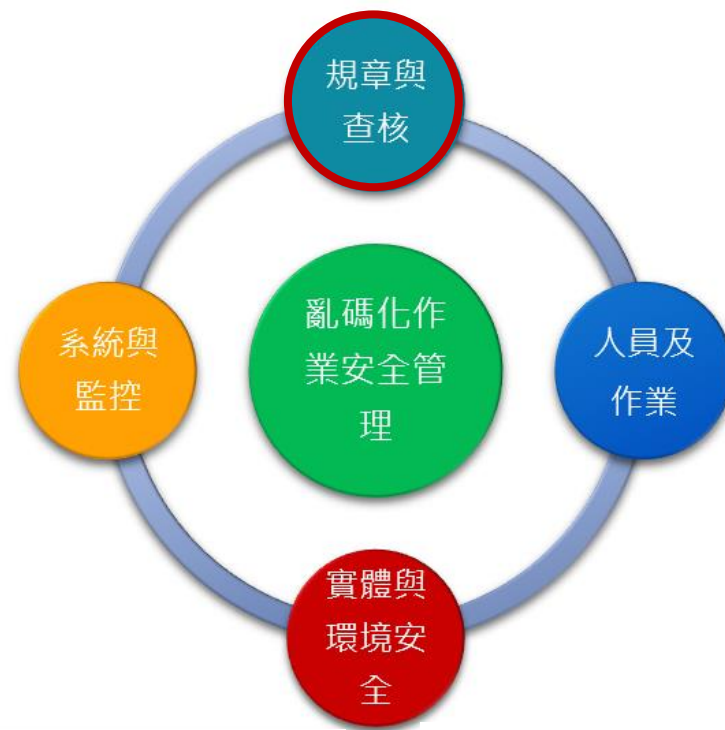
◆ 亂碼化作業安全規章之內容應包括：

- 明確規範作業人員之指派及工作職掌
- 系統主基碼及基碼檔安全控管作業
- 亂碼化設備及程式控管機制說明
- 落實文件及記錄控管
- 系統故障之回復機制規劃
- 系統開發廠商管理

◆ 基碼管理操作手冊訂定

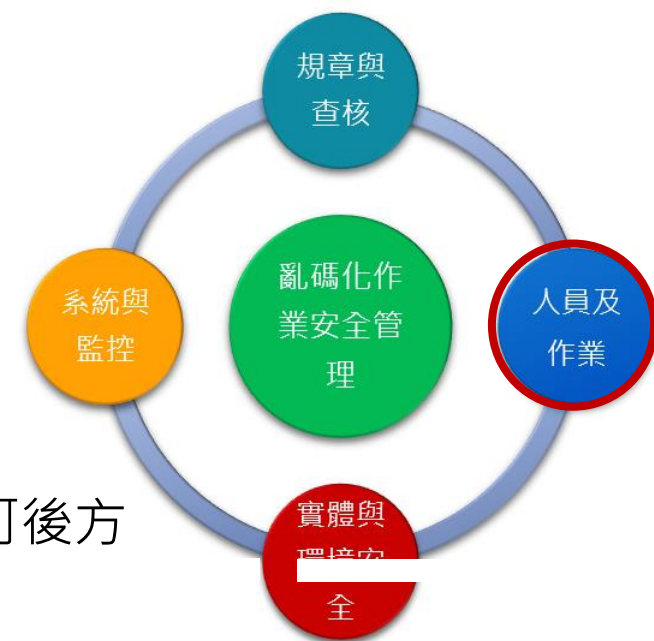
- 各類基碼列印/建置及交換程序
- 操作記錄留存及查詢作業

◆ 金管會檢查局與財金安審及實地查核作業



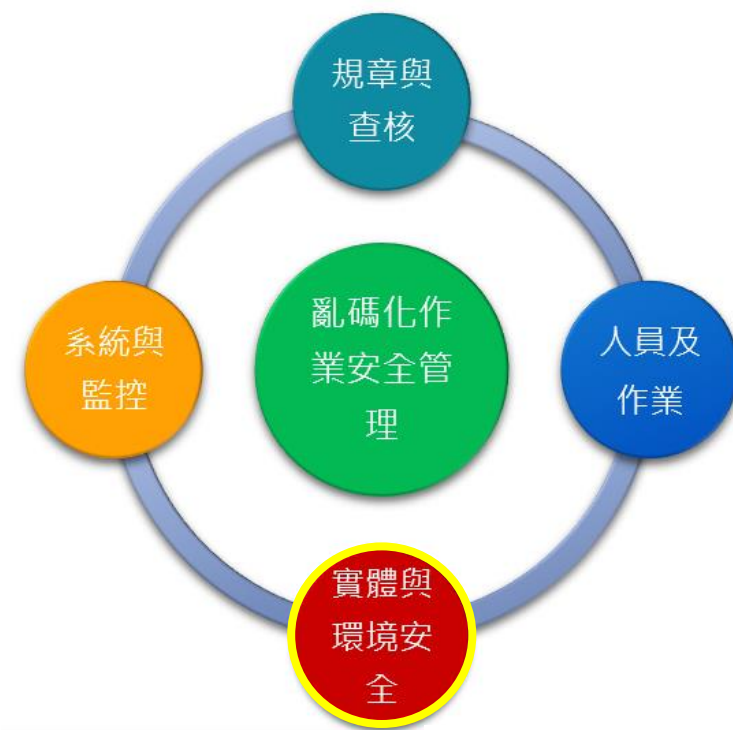
亂碼化作業管理—人員及作業管理

- ◆ 相關人員權責需於「亂碼化作業安全規章」載明，列冊及設定代理人
- ◆ 安全控管人員應包括：
 - 安全監督人員(電腦稽核或營業單位高階主管)
 - 基碼建置人員(A/B/C 3 Part，會計部/業務單位/IT 主管)
 - 安全控管人員(IT安控人員)
 - 亂碼化介面程式開發人員(IT專屬開發人員)
- ◆ 亂碼化介面程式之維護變更需經一定層級之主管(如安全控管人員)核可後方可變更
- ◆ 碼單列印及基碼建置作業需設簿登記，並經相關作業人員簽名備查
- ◆ 亂碼化介面程式及集體指令需設定存取權限(ACL)，非經授權使用者不得存取使用
- ◆ 提供相關作業人員完整的教育訓練



亂碼化作業管理—實體與環境安全

- ◆ 亂碼化設備(運算模組)符合**FIPS 140-2 Level 3**及破壞偵測與歸零清除保護機制
- ◆ 搭配相關之實體機制 (或增加本設備之重量、或鎖於櫃內、或固定於架上、或安裝於主機中)
- ◆ 亂碼化設備及基碼建置需在安全環境下作業：
 - **獨立空間**，設有**門禁管制**，經授權人員方可進入
 - 設有人員進出登記簿，所有進出人員均需登記
 - **獨立網段**，未經授權不可存取該網段設備
 - 設有**CCTV**(進出門及設備區)，錄影資料至少保留三個月
 - 基碼列印及建置設備不使用時要關機
- ◆ 亂碼化設備屬專用設備，非經授權不得使用(白名單控管機制)
- ◆ 基碼建置及列印需進行通道加密，以防止基碼外露



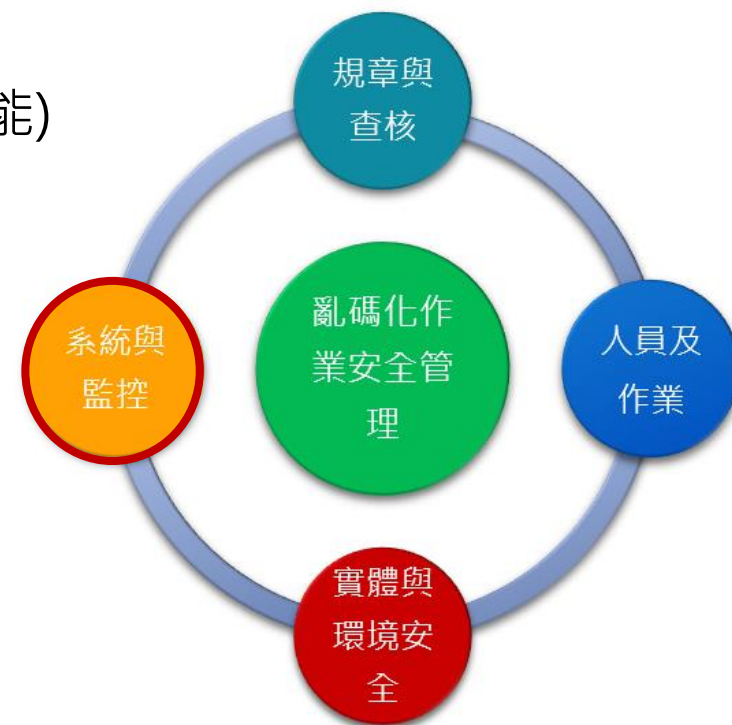
亂碼化作業管理—系統與監控

◆系統功能及維運

- 系統功能需符合財金公司「硬體亂碼化設備問卷調查表」相關規定，如：
 - 基碼以明碼方式建置時，須有**二位以上**之安全控管人員產生、建置與保存
 - 系統功能之變動與調整均須經正常的變更程序控管，且皆須有明確的紀錄可供查核
 - 須經過**授權之使用者**與程式，才可使用亂碼化設備之功能、、等
- 可提供完整的金融業務功能(含Payment 及GP HSM功能)
- 專業廠商支援服務
 - 亂碼化技術開發及研發能力
 - 完整的金融業務系統Domain Knowhow
 - 即時的維運支援能力

◆系統監控及備援

- 提供完整的監控及應變機制(含軟硬體服務)
- 完善的系統備援 (A/A 或A/S mode)及基碼同步機制



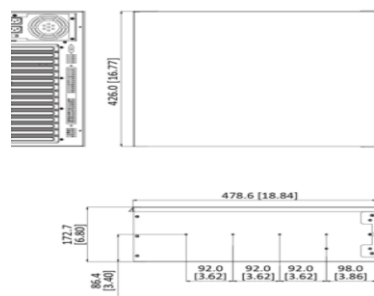
Agenda



- ☐ 作業風險與服務品質
- ☐ 銀行資安與硬體亂碼化設備規範
- ☐ 亂碼化作業管理
- ☒ 低風險的亂碼化服務方案
- ☐ Q&A

堅固安全的硬體(1/2)

ProHSM™ HSM Appliance Box



ProHSM™ Platform in IPC

24hrs Durable Industry PC

Dural Power Supply & Fans

Double Security, Physical Key & IC Chip Authentication

More Than 20 Years Experiences (Design by PIC)

符合銀行公會「金融機構辦理電子銀行業務安全控管作業基準」 **FIPS 140-2 Level 3** 之安全規範

堅固安全的硬體(2/2)

ProHSM™ HSM Appliance Box



- ◆ 提供四個獨立高速網路埠
- ◆ 將對外交易、連接HSM、管理、Heatbeat以實體網段分離
- ◆ 不相互影響流量，並提升系統安全性



ProHSM© KMC 基碼管理系統

- KMC操作手冊



提供簡單易操作的介面，讓您快速地、安全地鍵置您的基碼，是搭配 ProHSM™ 各系列亂碼化設備的必要套裝軟體

- ◆符合基碼以明碼方式建置時，須有二位以上之安全控管人員產生、建置相關規範
- ◆並通過財金公司安審及金管會實地查核作業



ProHSM™ M10K產品型號 & 效能

產品型號：

Model Name	Performance Model
ProHSM M10K	Standard
ProHSM M10K	Premium

效能：

Performance	Standard	Premium
3DES Encryption	600	2500
AES Encryption	600	2500
RSA 2048 Sign	12	60
PIN Translation	300	1200

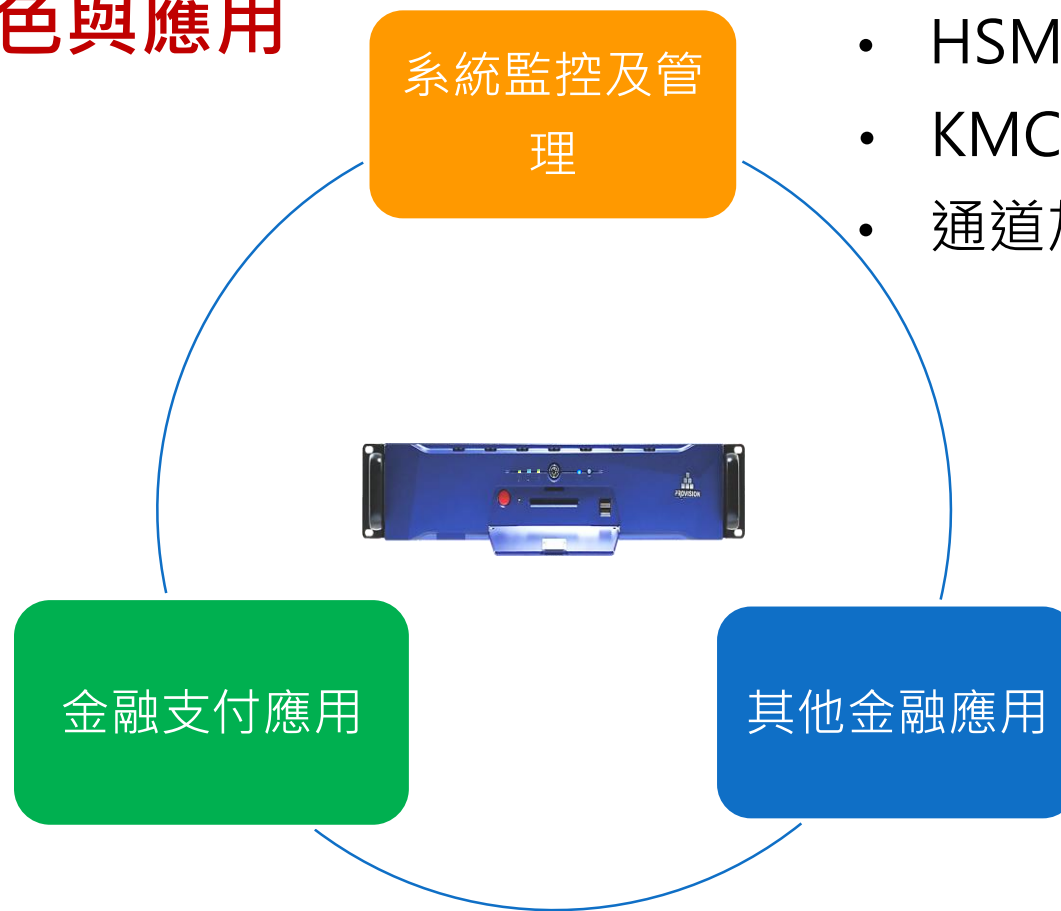
※使用 Variant LMK Scheme Benchmark

單位:TPS

完整的應用及系統監控

ProHSM™產品特色與應用

- 通匯
- ATM
- FXML/FEDI
- eDDA/eACH
- 信用卡
- 網路銀行
- 行動銀行
- 電子支付
- 行動支付



- HSM 監控系統
- HSM 安控模組
- KMC 金鑰管理
- 通道加密傳輸

- 雙因子認證
- 端點對端點加密
- 資料庫加密
- 行員晶片認證

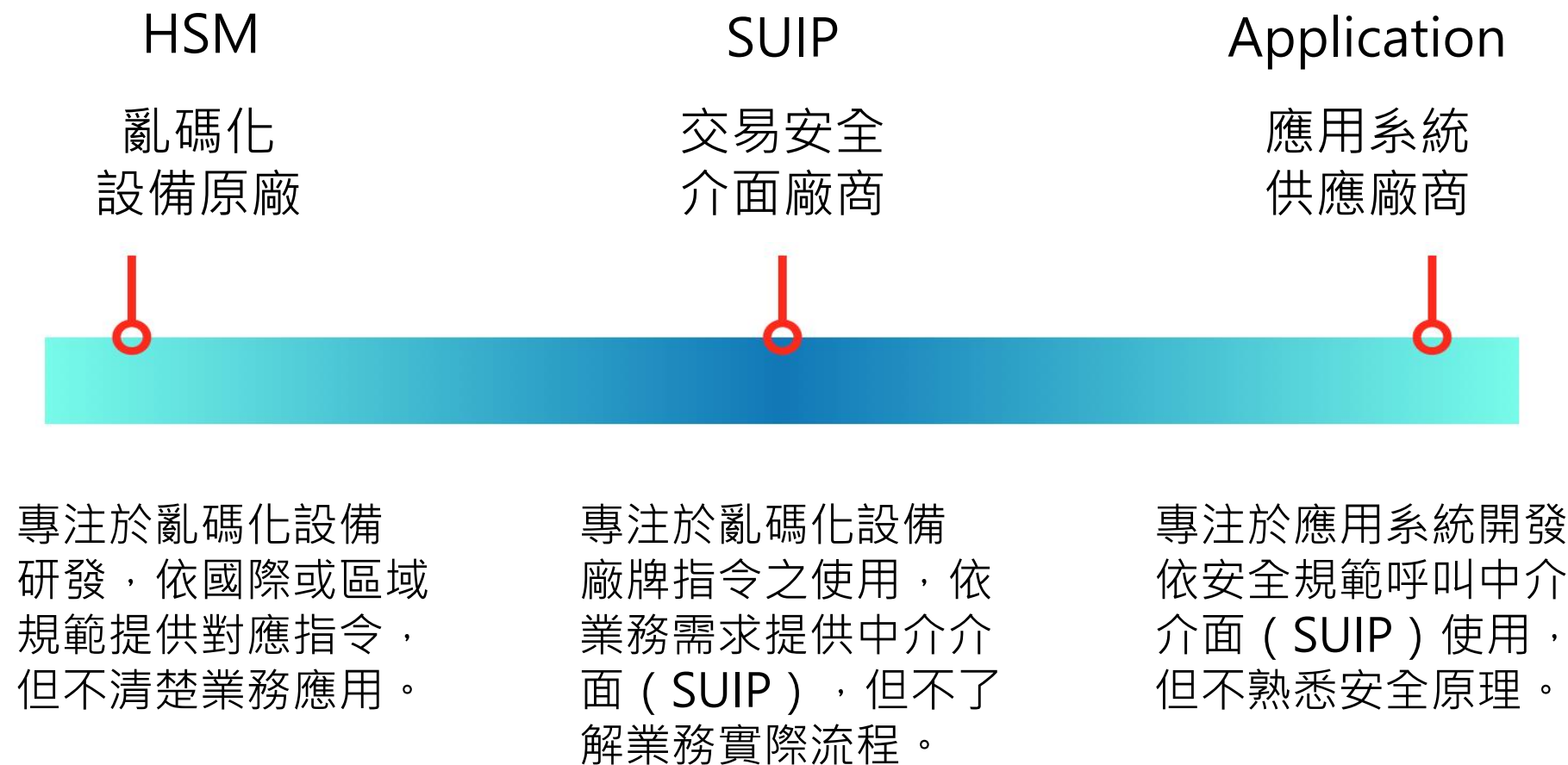
可靠的合作廠商—豐富的建置經驗與即時的維護服務

普鴻 HSM 產品指標型客戶

類別	信用卡 (前五大發卡行佔三家)	金融卡 IBRS ATM eACH
主管機關		   
金控/民營	   	     
外商		     

- 普鴻 HSM國內共有30多家金融業客戶
- 不論在ATM/匯款/信用卡/FEDI/FXML/eACH/eDDA等業務HSM均有豐富的建置經驗
- 堅強的研發團隊，提供即時的在地服務
- ◆ 提供7 X 24線上即時叫修維護服務
- ◆ 協助客戶財金安審作業及同異地備援演練
- ◆ 定期(每半年)提供客戶亂碼化作業教育訓練

整合服務、降低風險(1/2)



SUIP : Secure User Interface Program

整合服務、降低風險(2/2)



Q&A



感謝您

普鴻資訊團隊

886-2-2345-2366

sales@provision.com.tw

Provision.com.tw