Deloitte.
勤業眾信

CISA

4G營運資安參考指引推廣說明會

Agenda

- 舉辦目的
- 4G應用服務系統基本介紹
- 剖析4G應用服務系統資安風險與對策
- 4G應用服務系統營運資安參考指引說明

說明會目的簡介

舉辦目的

政府於2013年釋出行動寬頻業務(4G)執照

行政院科技會報辦公室特別會同相關部會規劃「加速行動寬頻服務及產業發展方案」

「4G應用服務系統營運資安參考指引」係依循經濟部工業局之「4G應用服務系統資安推動計畫」研擬應用服務系統之營運資安參考指引

行政院科技會報辦公室特別會同相關部會規劃「加速行動寬頻服務及產業發展方案」

經濟部工業局之「4G應用服務系統資安推動計畫」為協助行政院「加速行動寬頻服務及產業發展方案」服務普及類計畫之「4G應用服務系統」提升資訊安全防護能力

目的

提供4G應用服務系統，包括Web應用服務系統、行動應用App軟體及其後端平臺供營運管理單位之相關資訊安全建議，協助4G應用服務系統營運相關人員提升資訊安全防護能力及品質。

適用對象

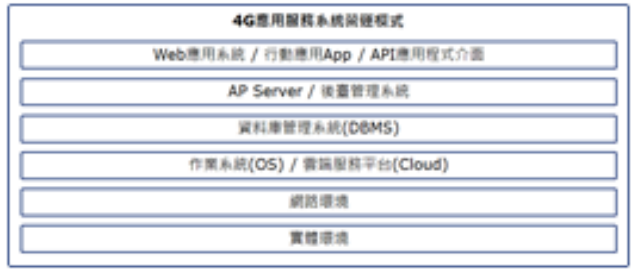
營運管理單位4G應用服務系統之

- **系統開發人員**
- **系統維運人員**
- **系統管理人員**
- **網路管理人員**
- **機房管理人員**
- **資安技術人員**

4G應用服務系統基本介紹

4G應用服務系統營運模式

4G應用服務系統營運端



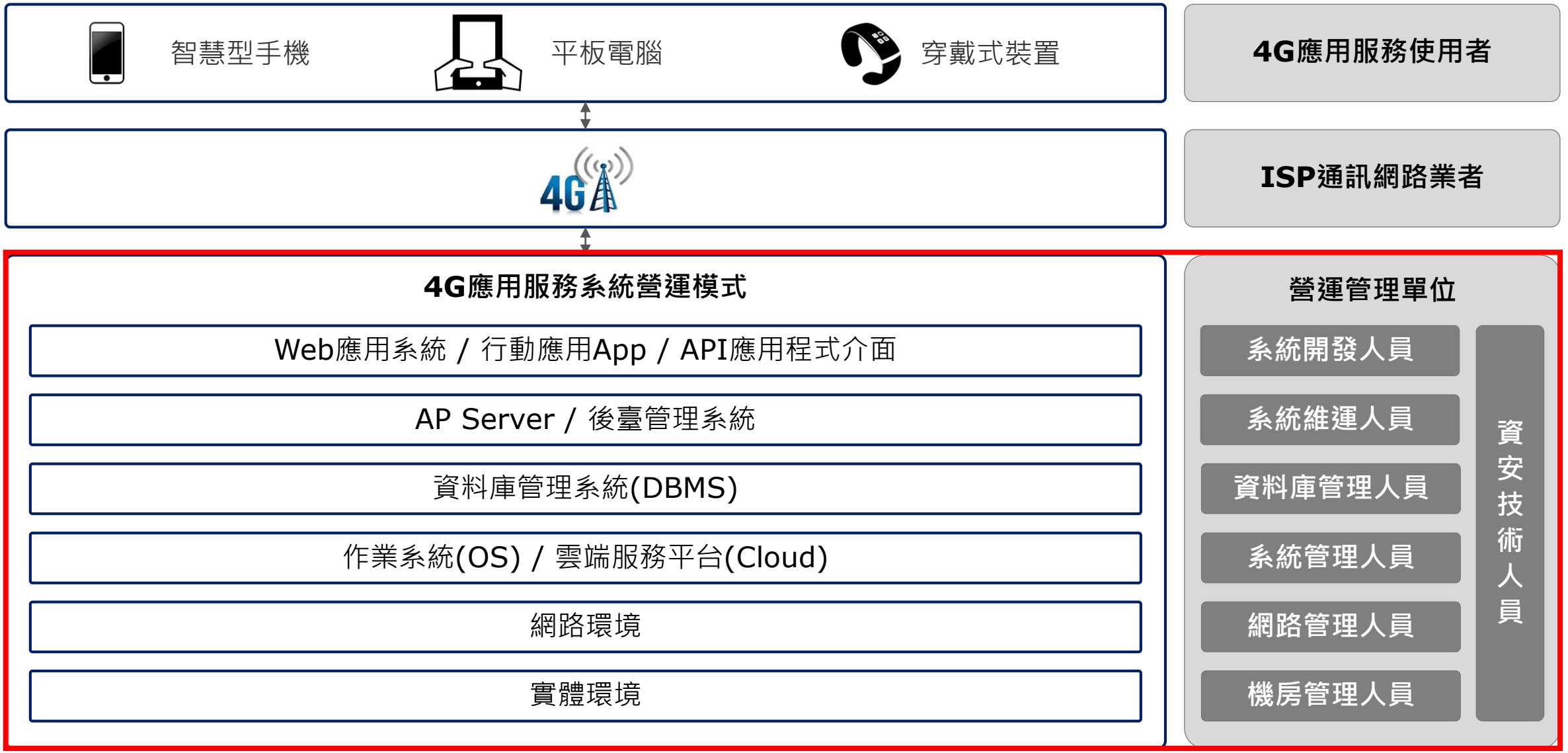
- 從使用終端蒐集資料，並將其存儲至伺服器環境中。
- 將資料呈現於多個使用者介面（如APP、網站等），讓使用者可瞭解該資料。
- **資料經常採用指標、參數或命令的形式**，也可以通過服務基礎設施中生成的 API 交給授權協力廠商。

通信網路

4G應用服務系統使用終端

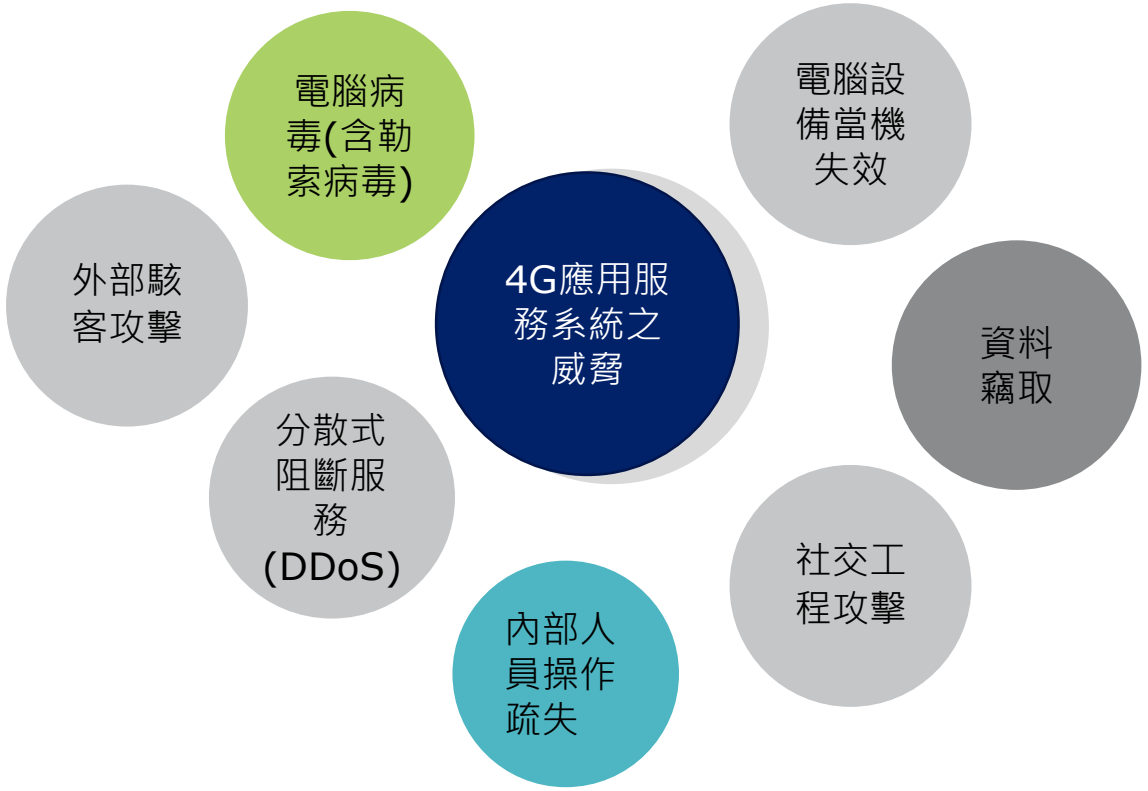
- 終端設備包括智慧型手機、平板電腦與運動感測器等。
- 通過多種有線和無線網路將真實世界連接數位世界。
- 從真實環境中收集指標，並以多種形式通過4G網路將資料傳輸至「4G應用服務系統營運端」。

4G應用服務系統營運管理角色

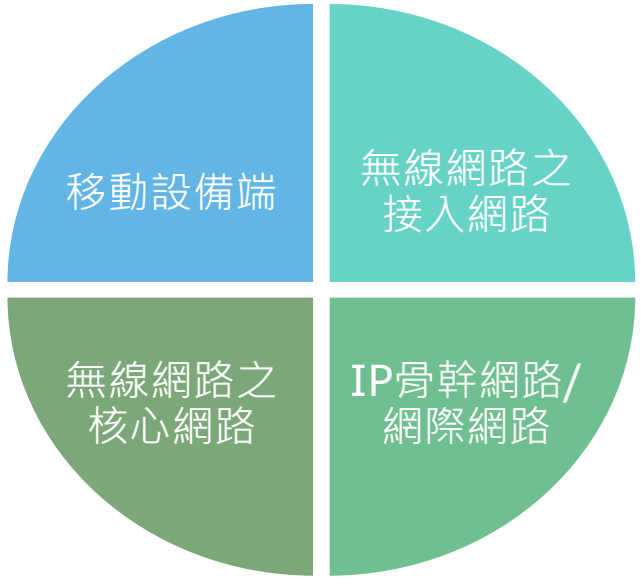


剖析4G應用服務系統資安風險與對策

4G應用服務系統面臨之資安威脅



無線網路元素及相關風險



[4G應用服務系統營運的安全議題]

存取控制 | 身分驗證 | 不可否認性 | 資料機密性 | 資料完整性 | 通訊安全 | 可用性 | 隱私保護

「4G應用服務系統營運端」- 網路基礎設施攻擊

攻擊方式

中間人攻擊(Man-in-the-middle attack , MITM) ：攻擊者與通訊的兩端分別建立獨立的聯繫，並交換其所收到的資料，使通訊的兩端認為正在通過一個私密的連線與對方直接對話，但事實上整個對談都被攻擊者完全控制。在中間人攻擊中，攻擊者可以攔截通訊雙方的通話並插入新的內容。

其他類似攻擊：針對正向加密和加密通信分析的攻擊、旁道攻擊

原因分析

- 實體通信網路之弱點
- 網路服務之漏洞

對策分析

- 利用相互驗證、正向加密、適當的加密協定和演算法，降低攻擊風險。

「4G應用服務系統營運端」- 雲服務或伺服器基礎設施攻擊

攻擊方式

雲服務或伺服器基礎設施攻擊假定攻擊者可控制與目標 VM 相同的物理伺服器上的 VM，攻擊者可能會使用多種方法攻破伺服器上的其他 VM：

1. 利用 VM 基礎設施的漏洞擺脫訪客身份限制進入主機系統
2. 利用旁道攻擊推斷另一訪客 VM 的金鑰
3. 利用伺服器上的大量資源，強制目標 VM 遷移至攻擊者具有更多控制的伺服器上

原因分析

- 利用特殊權限管理者地位，進入正在運行訪客虛擬機器 (Virtual Machine , VM) 系統的主機，使攻擊者有能力檢查並修改正運行的 VM 系統。

對策分析

- 基於架構和獨特的加密身份，該架構能夠將每個容器限定給特定用戶，借以削弱攻擊者濫用 VM 基礎設施同時訪問多個使用者或多項服務的能力。

「4G應用服務系統營運端」- 應用程式服務攻擊

攻擊方式

應用程式服務層級若遭受攻擊面臨的風險將最大，攻擊者會從對網路基礎設施的攻擊一路到對應用程式自身進行攻擊。

原因分析

- 使用終端之風險容易被忽略
- 應用程式代管道多元，攻擊者可由不同管道的弱點進行攻擊

對策分析

- 檢視現行應用程式執行架構，確保架構之安全度
- 定期針對應用程式進行弱點掃描，確保其安全性

「4G應用服務系統使用終端」對應之資安威脅 1/2

1. 平臺層面之風險
2. 作業系統漏洞
3. 多元應用管道
4. 使用者與服務設定者的資訊安全認知落差
5. 移動設備端之漏洞

A. 移動設備端於硬體層面，常見於平臺的架構中，對於完整性及驗證機制的考量，使其中的模組易因惡意攻擊而受竄改
B. 硬體於各種通訊埠較缺乏完整性與機密性之考量，使其資料易受竊聽或竄改
C. 既有的移動設備端平臺較缺乏存取控制機制，常使移動設備端的遺失所釀成的損失驚人

「4G應用服務系統使用終端」對應之資安威脅 2/2

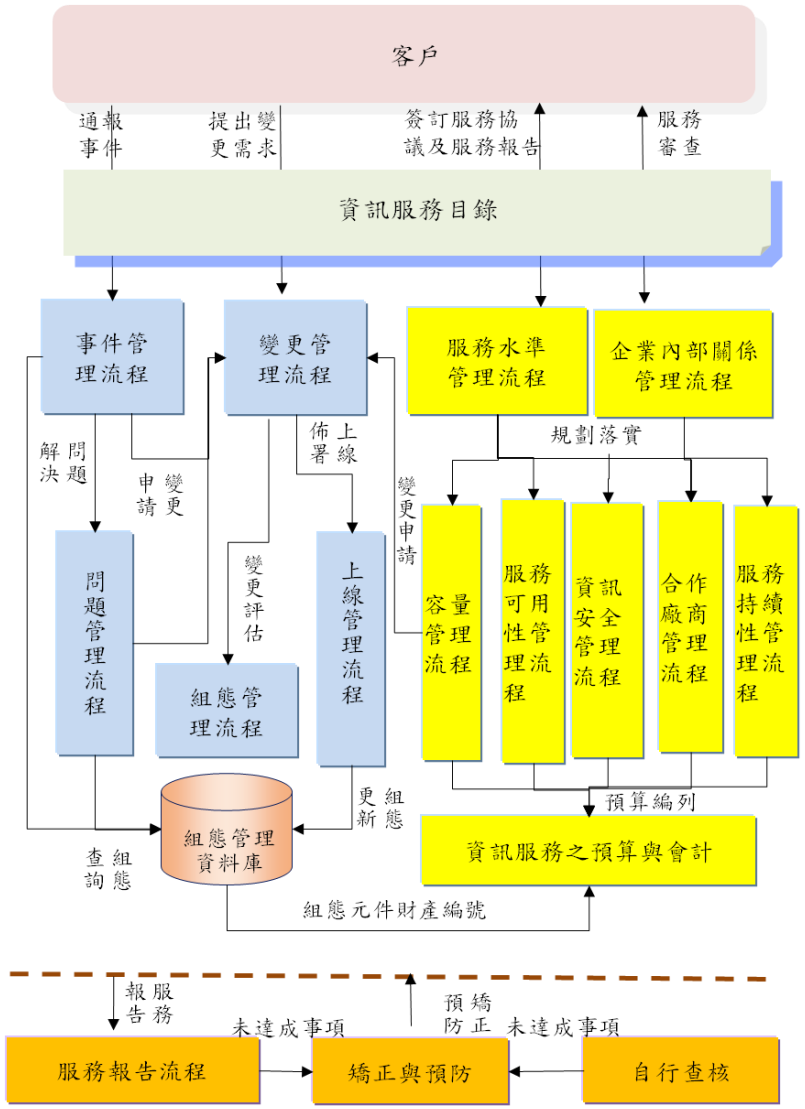
6 身分辨識之隱憂

7 防毒軟體之漏洞

8 網路服務之風險

9 無線網路架構間之安全機制

資訊服務管理流程



資訊服務支援（Service Support）管理流程

著重於提供反應式之資訊系統服務運行之作業流程，偏重操作面，代表回應使用者之需求，包括事件管理、問題管理、變更管理、上線管理及組態管理等流程，並以組態管理資料庫（Configuration Management DataBase：以下簡稱CMDB）作為各流程間以資訊服務為導向之組態資訊彙整平台，各流程則分別依流程特性訂定各類可量化之關鍵績效指標，作為具體評估資訊服務管理流程成效之依據，同時以服務窗口作為使用者與資訊服務平台間之主要聯繫管道。

資訊服務交付（Service delivery）管理流程

著重於提供主動式之監控與規劃作業流程，偏重於策略面， 代表主動提供給使用者適切之服務，用以達到資訊服務水準協議（Service Level Agreement：以下簡稱 SLA）所需執行之作業流程，包括服務水準管理、可用性管理、服務持續營運管理、容量管理及財務管理等流程，經由資訊4G應用服務系統營運管理單位與使用者代表研議訂定之 SLA 作為使用者所要求之業務整體服務品質具體指標，本類各項流程則為達到各 SLA 指標所需投入資源之規劃與管理程序。

資訊服務管理建議 -資訊服務之新增、終止及重大異動

針對資訊服務之新增及重大異動，事先進行可行性評估及前置作業規劃

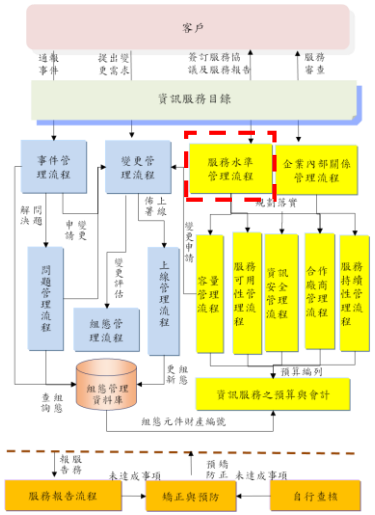
新服務或服務異動(含服務之終止)，以正式變更管理規劃

新服務或服務變更於正式環境實施前依循規範作業

事先擬定變更管理規劃，並須包含：

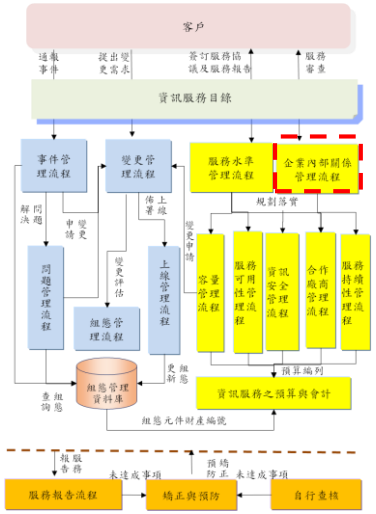
實施、操作及維護之角色與責任	對於資訊安全、資訊服務管理制度及資訊服務之影響	與利害相關團體之溝通結果
相關之時程、流程、監控方式、管理方法及工具	合約或服務水準協議修改之必要	針對新服務運作情形或預期效益，設定量化管理績效指標
新服務或服務異動完成後之驗用方法	新服務或服務異動之預算、人力需求	新服務或服務異動之技能及訓練需求

資訊服務管理建議 -服務水準管理



1. 透過資訊服務目錄說明提供之資訊服務與內容，訂定服務水準協議，取得對於資訊服務管理目標之共識。
2. 依據資訊服務水準協議，管理資訊服務流程，並確保資訊服務達成需求。
3. 服務水準協議之異動宜有正式之變更管理管控。
4. 服務水準協議宜定期進行審查，以確保服務水準協議維持在最新及有效狀態。
5. 服務水準宜進行監控並與目標進行比較，以顯示現況及趨勢資訊。

資訊服務管理建議 -企業內部關係管理



1. 4G應用服務系統營運管理單位宜鑑別及建立服務之利害關係人與客戶清單
2. 4G應用服務系統營運管理單位宜透過服務審查會議，討論服務績效、達成情況、問題與行動計畫；並於年度終了前討論服務範圍、服務水準協議、合約及企業需求之變更
3. 4G應用服務系統營運管理單位宜注意企業需求之重大異動，並做好回應之準備
4. 藉由了解使用者需求及其業務特性，與其建立並維持良好之互動關係
5. 4G應用服務系統營運管理單位宜建立適當之服務抱怨程序，並執行抱怨記錄、調查及結案程序；當無法透過正常管道解決時，4G應用服務系統營運管理單位宜提升處理層級
6. 4G應用服務系統營運管理單位宜指派專人負責管理客戶滿意度及企業內部關係流程，確保可從定期客戶滿意度中獲得回饋；並將任何已鑑別之措施紀錄，做為服務改善計畫之輸入

資訊服務管理建議 -容量管理

1. 宜分析現行資訊服務之容量狀況，並規劃未來使用資訊設備及資源需求，確保資訊服務符合需求之變動
2. 資訊服務之容量規劃宜考量其服務水準要求
3. 宜透過容量管理評估下列項目
4. 宜監控服務容量並調整服務效能，確保有適當容量提供服務之運作

- **企業需求**

A. 目前與預測之容量與效能要求

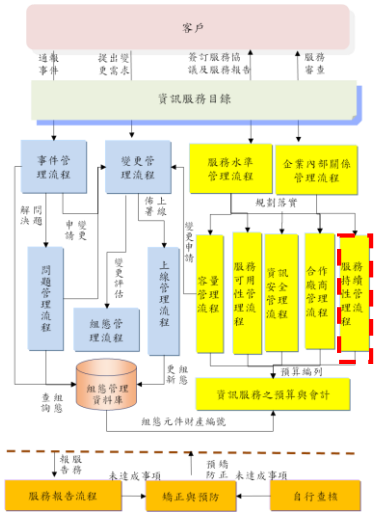
B. 鑑別升級時所需時程、臨界值與成本

C. 鑑別升級時所需時程、臨界值與成本

D. 預測外部變更之衝擊，如：法令

E. 可用於能夠執行預測性分析之資料與流程

資訊服務管理建議 -服務持續性與可用性管理



1 確保協議之服務水準，滿足企業服務持續運作及其可用性

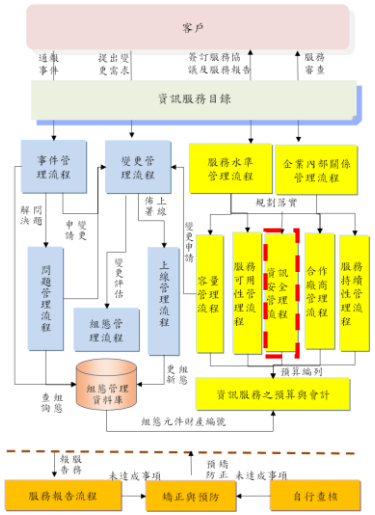
2 宜考量其資訊服務水準要求

3 宜發展可用性與服務持續計畫，確保內容已考量從一般異常到服務中斷之不同狀況，並應執行年度審查

4 可用性和服務持續計畫宜於業務環境發生重大變化時重新測試

5 宜確保當辦公場所無法使用時，服務持續計畫、聯絡清單與組態管理資料庫仍可被取得

資訊服務管理建議 -資訊安全管理



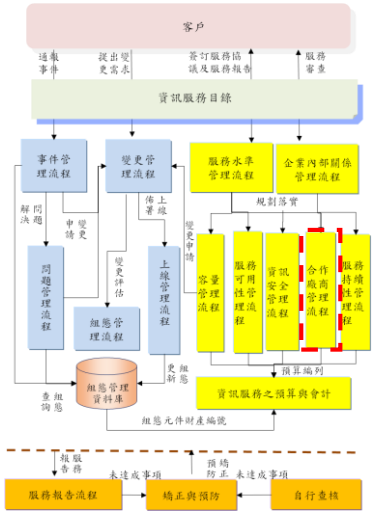
1 宜依資訊安全管理制度，管理各項資訊服務所涵蓋之資訊安全議題

2 應執行資訊安全控制措施，管理與資訊服務相關之風險

3 宜依據事件管理流程通報並記錄資訊安全事件;且有適當程序以確保所有資訊安全事件被調查，並採取相關行動

4 宜有適當機制以量化並監控資訊安全事件與故障之類型、數量及衝擊

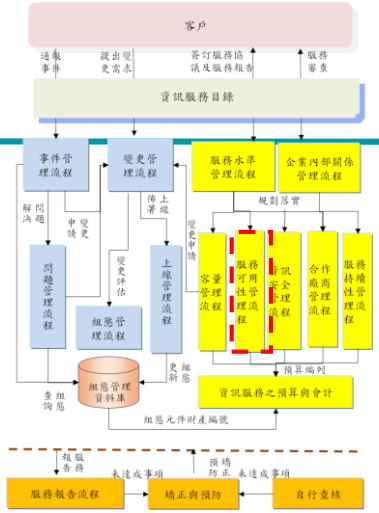
資訊服務管理建議 -合作廠商管理

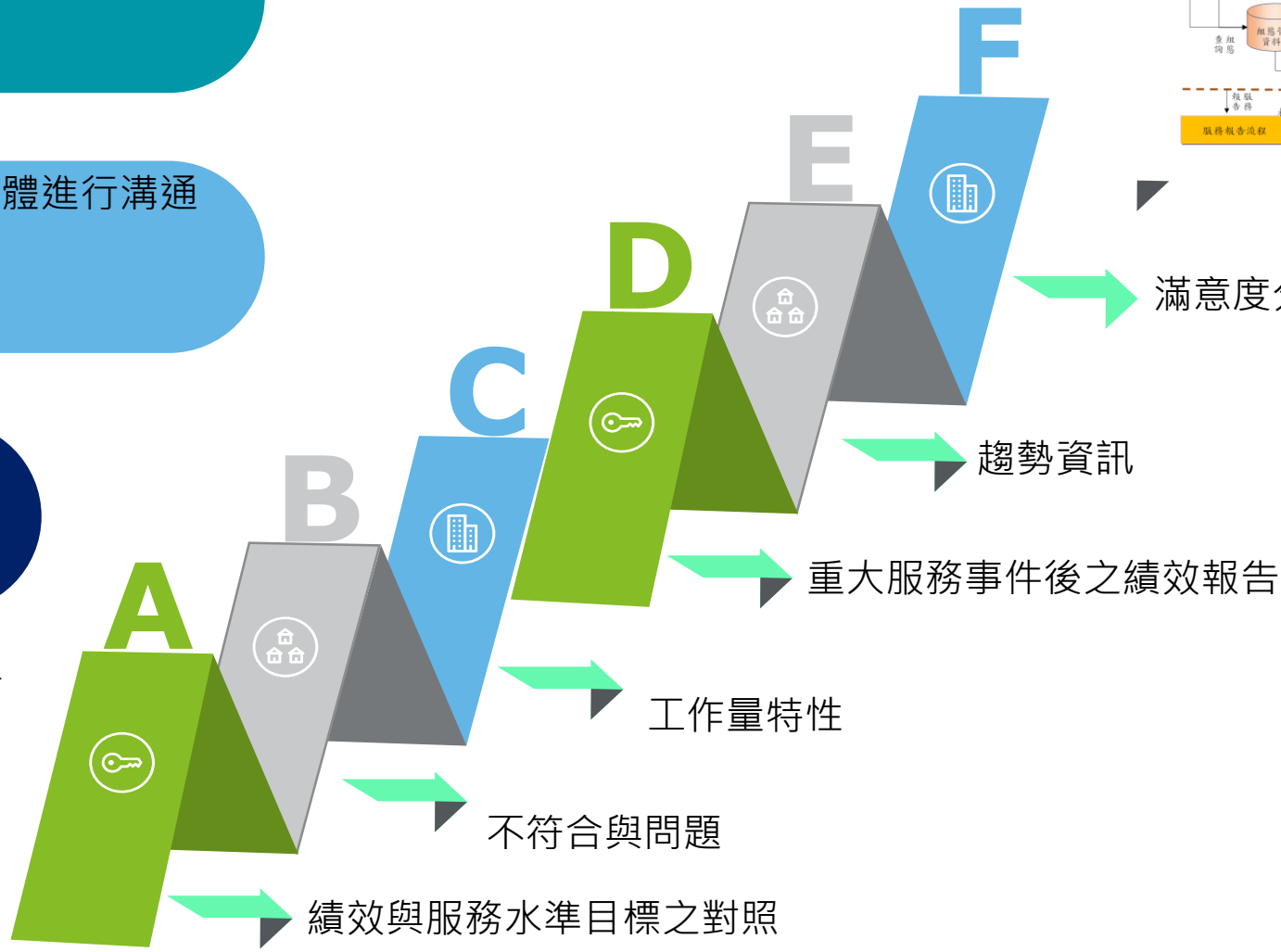


1. 宜有書面化之管理流程，以維持高品質之資訊服務
2. 宜有效協調使其合約協議與服務水準協議一致
3. 宜將其與分包廠商之角色及關係書面化；其對分包廠商履約之部分，應負完全責任
4. 針對資訊服務合作廠商之契約，宜定期進行一次審查，確保契約與本行需求間之適用性
5. 宜採用適當程序處理其服務之正常結束及提前結束
6. 宜依據其服務等級目標進行監測並審查績效

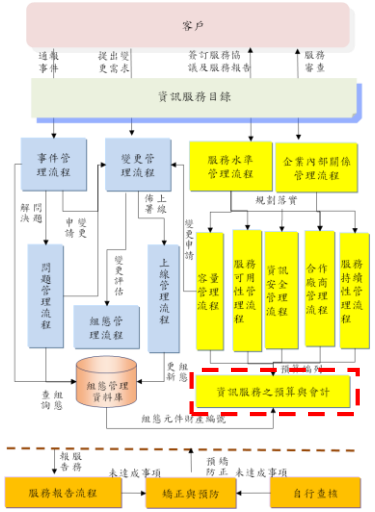
資訊服務管理建議 –服務可用性管理

1. 宜定期產出資訊服務報告，用以促進管理階層制定決策與進行有效之溝通
2. 服務報告中之發現事項宜與相關團體進行溝通
3. 服務報告宜內容應包含以下事項





資訊服務管理建議 -資訊服務預算與會計管理



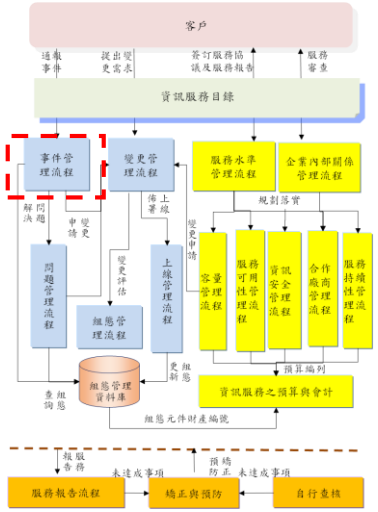
1 4G應用服務系統營運管理單位對於下列事項宜有明確之程序

2 4G應用服務系統營運管理單位宜彙整資訊服務預算，以做為有效之財務控制與決策

3 宜檢視資訊服務的財務預測與成本支出，用以分配資訊服務的預算與成本之編列；資訊服務的預算宜適度考量服務水準要求

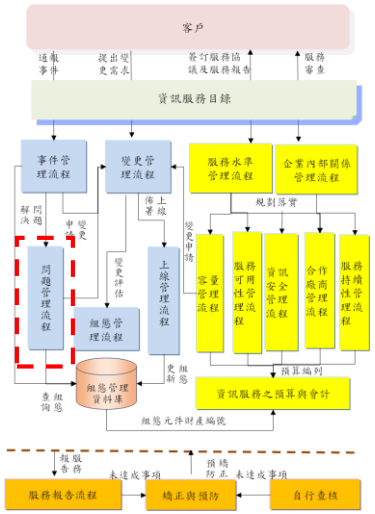
- 有效之財務控制及授權
- 分攤專屬成本及分配共用成本至資訊服務
- 與資訊服務相關資源(例：人力、軟硬體等)之預算與會計

資訊服務管理建議 -事件管理



1. 宜記錄所有事件，並透過有效之管理程序，儘速將資訊服務回復至正常運作狀態
2. 宜確認程序已定義事件記錄、優先順序、企業衝擊、分類、更新、升級、事件解決及事件結束之流程活動
3. 宜回覆客戶已通報事件或請求之進度；若可能無法達到服務水準時，應通知客戶並採取適當行動
4. 宜確保所有涉及事件管理之同仁可存取相關資訊，包括：已知錯誤、問題解決方案及組態元件資料庫
5. 重大事件宜根據已制定之流程進行分類與管理

資訊服務管理建議 -問題管理



1 宜記錄所有問題，並以根因分析及管理機制，降低服務中斷之情形及異常事件之發生

2 宜確認程序已定義問題記錄、分類、更新、升級、解決與結束之流程活動

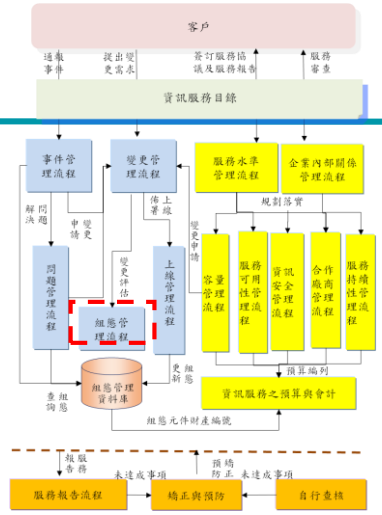
3 宜採取預防措施以減少潛在問題，如進行趨勢分析

4 透過變更管理流程採取矯正潛在根因或解決該問題所需之變更

5 宜監測、審查及報告問題解決之有效性

6 問題管理宜負責確保事件管理可使用已知錯誤及已矯正問題等最新資訊

資訊服務管理建議 -組態管理



資訊服務與基礎架構中之組態元件宜能被鑑別、控制及追蹤；控制程度應滿足企業需求、失效之風險、關鍵性服務

宜在資訊服務重大異動前執行組態元件之基準點(Baseline)

宜定義與控制支援資訊服務之重要組態元件，並維持其正確性

組態元件宜定義財務資產會計流程之介面

組態管理

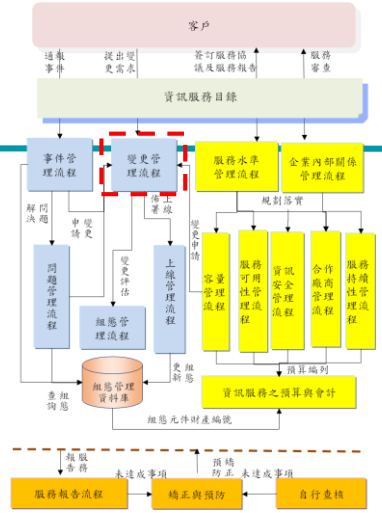
宜將組態元件之實體置於管制環境中

宜提供變更管理流程對資訊服務與基礎架構之變更衝擊資訊。在適當情況下，宜可追蹤及查核組態元件之變更

宜確保每一組態元件為唯一可識別，並記錄於受管制之組態管理資料庫中，且該組態管理資料庫已被確保其可靠性與正確性，並提供下列資訊：

A.組態元件之狀態及關聯性
B.組態元件之版本
C.組態元件之位置
D.相關變更與問題
E.相關之文件

資訊服務管理建議 -變更管理



對於服務與系統架構之變更，宜具有明確書面化定義之範圍

變更紀錄宜被定期分析以偵測變更之增加、經常重複發生之類型、浮現之趨勢及其他相關資訊；並將變更分析之結果及結論予以記錄

宜記錄所有變更請求並加以分類，並應對變更請求評估其風險、衝擊與企業利益

變更管理

所有已核可之變更及其提議實施之時程宜予以維護，並向所有相關團體溝通

流程中宜包含變更失敗時之還原或補救方式

宜制定程序以控制緊急變更之授權與實施

變更宜被核准並以可控制之方法實施

資訊服務管理建議 -上線管理

將變更管理所變更之組態元件，發佈至正式環境運作

宜擬定上線管理書面程序

4G應用服務系統營運管理單位宜規劃服務、系統及軟硬體之發佈；並與相關團體協議上線計畫

上線計畫宜包含如何取銷及補救上線方法、上線日期暨可交付之事項

上線計畫宜提及相關之變更需求、已知錯誤問題；上線管理流程應提供適當資訊至事件管理流程

宜建立受控管之可接受測試環境(Acceptance Test Environment)

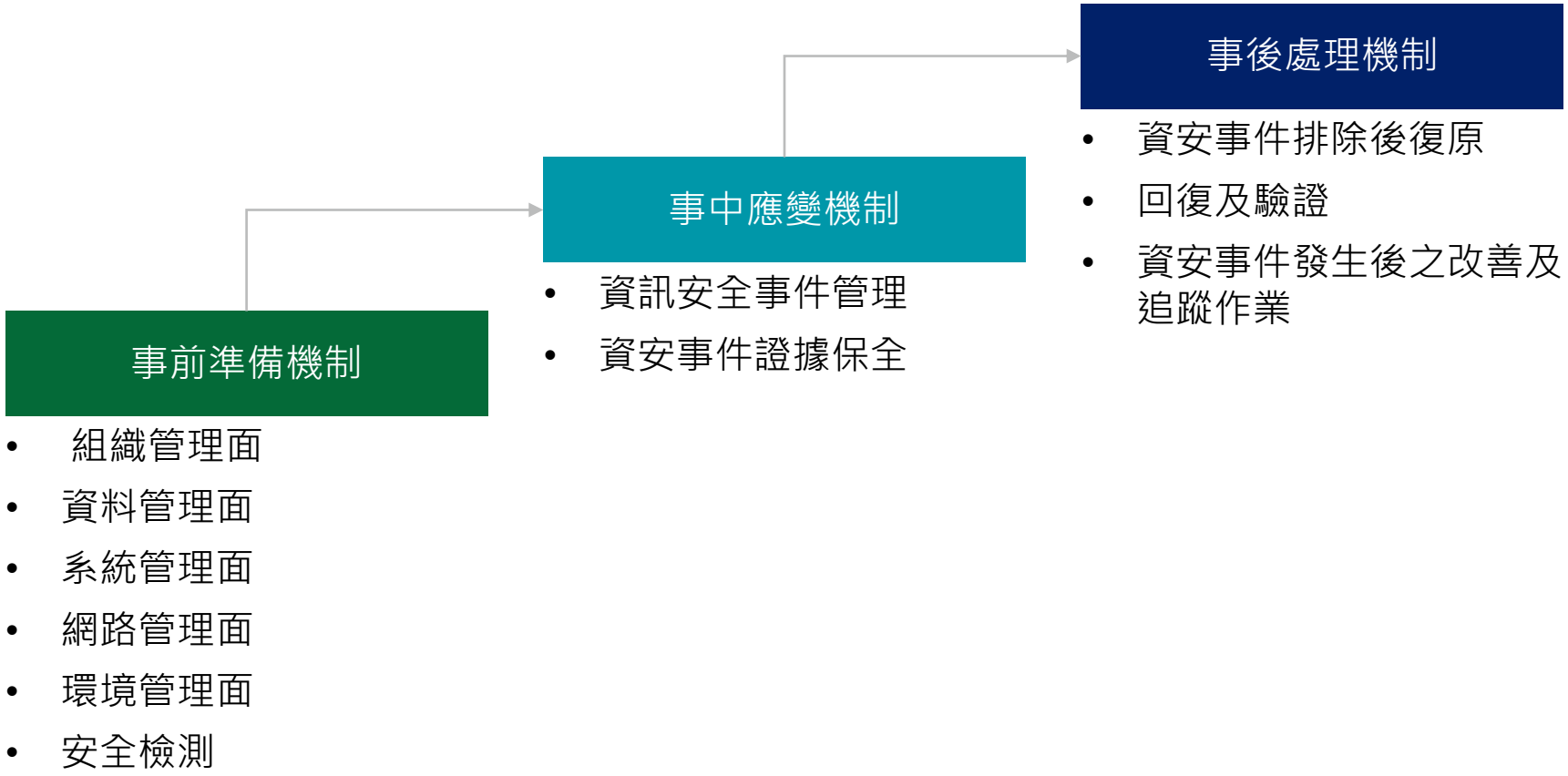
宜制定程序以控制緊急上線之授權及實施

上線與發佈活動宜被設計及實施，以確保在安裝、處理、封裝、交付時，能保持軟硬體之完整性

宜量測上線之成功與失敗，包括：在上線之後與上線有關之事件、評估對企業、資訊營運與支援人力資源之衝擊；並將結果輸入改善服務之計畫

4G應用服務系統營運資安參考指引說明

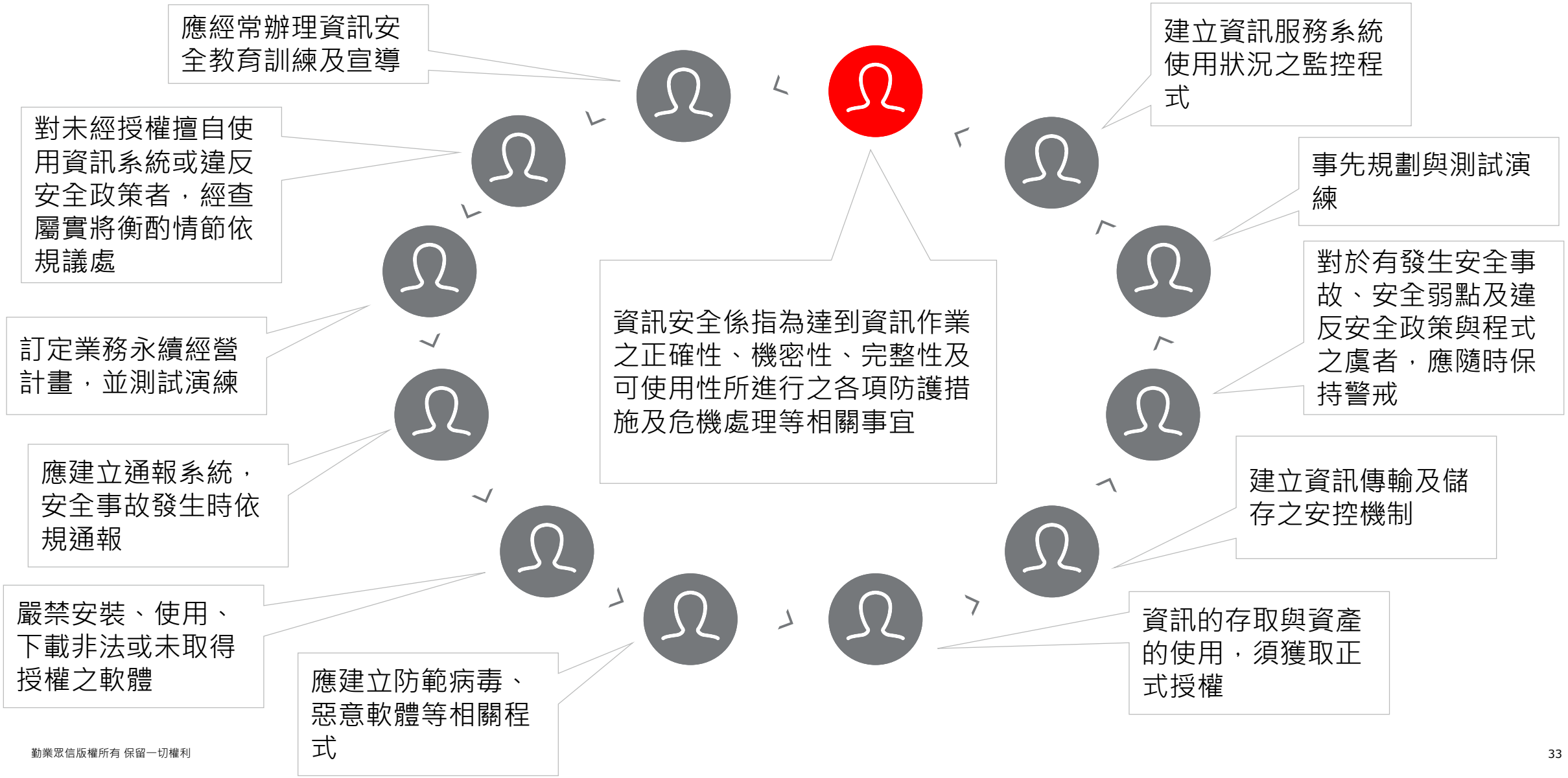
4G應用服務系統營運資訊安全要求



4G應用服務系統營運資訊安全要求

事前準備機制

組織管理面 -資訊安全政策



組織管理面 -資訊安全管理權責

組織管理面 -人員安全管理

重要職務人員應設置代理人制度，以確保營運作業不中斷

營運管理單位各項資訊作業活動之工作分配應依員工個人之專業技能做適當權責分工，並預防未經授權存取之行為，以杜絕舞弊

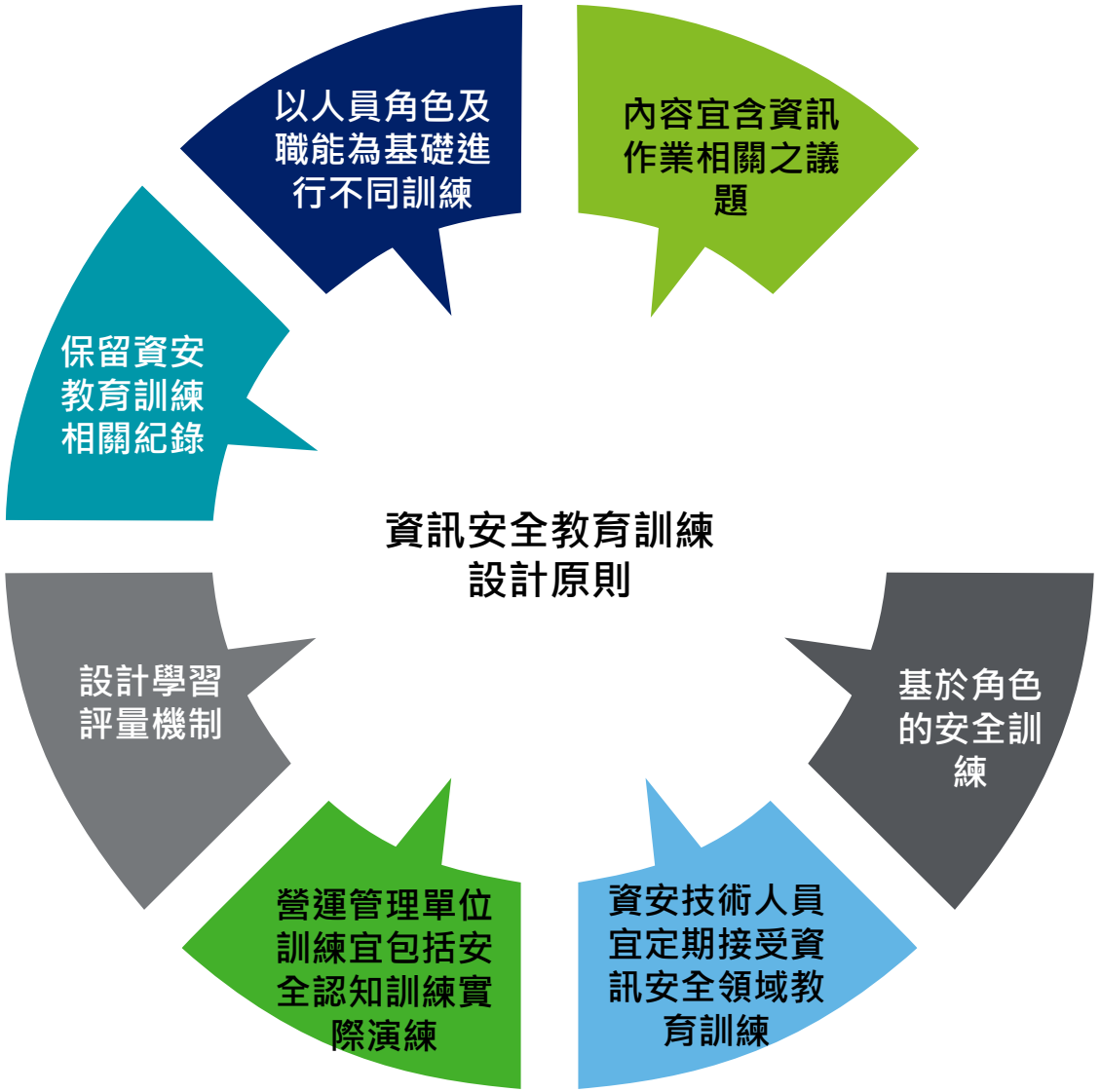
營運管理單位所有員工對於與工作上資訊安全相關之法令要求，應有所瞭解並依據相關規定辦理

若因人力不足而有兼任之情形時，須採取適當之補償性控制措施，如留存操作稽核軌跡或人員陪同作業等

協力廠商人員安全

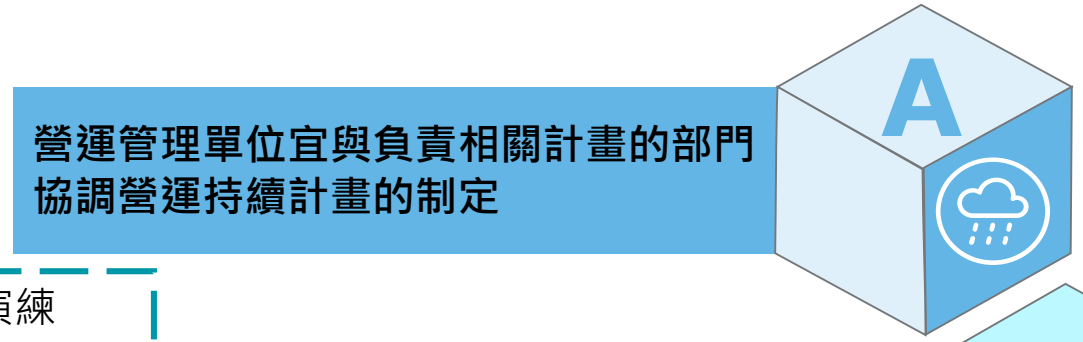
人員離(調)職應辦理移交事項及帳號權限之移除作業

組織管理面 -資訊安全教育訓練

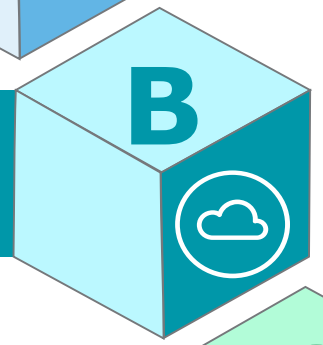


組織管理面 -營運持續管理：營運持續計畫/與相關計畫協調及容量管理計畫

為降低4G應用服務系統遭遇突發緊急危難或異常事件所可能造成資訊作業之衝擊，並規劃相關應變策略與處理計畫，以確保關鍵性資訊作業持續運作。

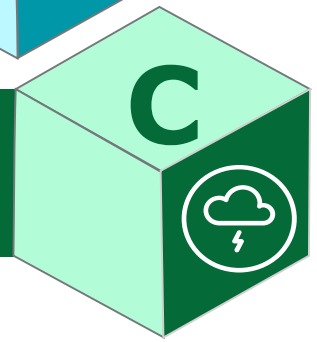


營運管理單位宜與負責相關計畫的部門協調營運持續計畫的制定



訂定演練模式及週期

a. 書面模擬演練
b. 資料回復演練
c. 情境模擬演練
d. 實況演練
e. 預警/無預警演練

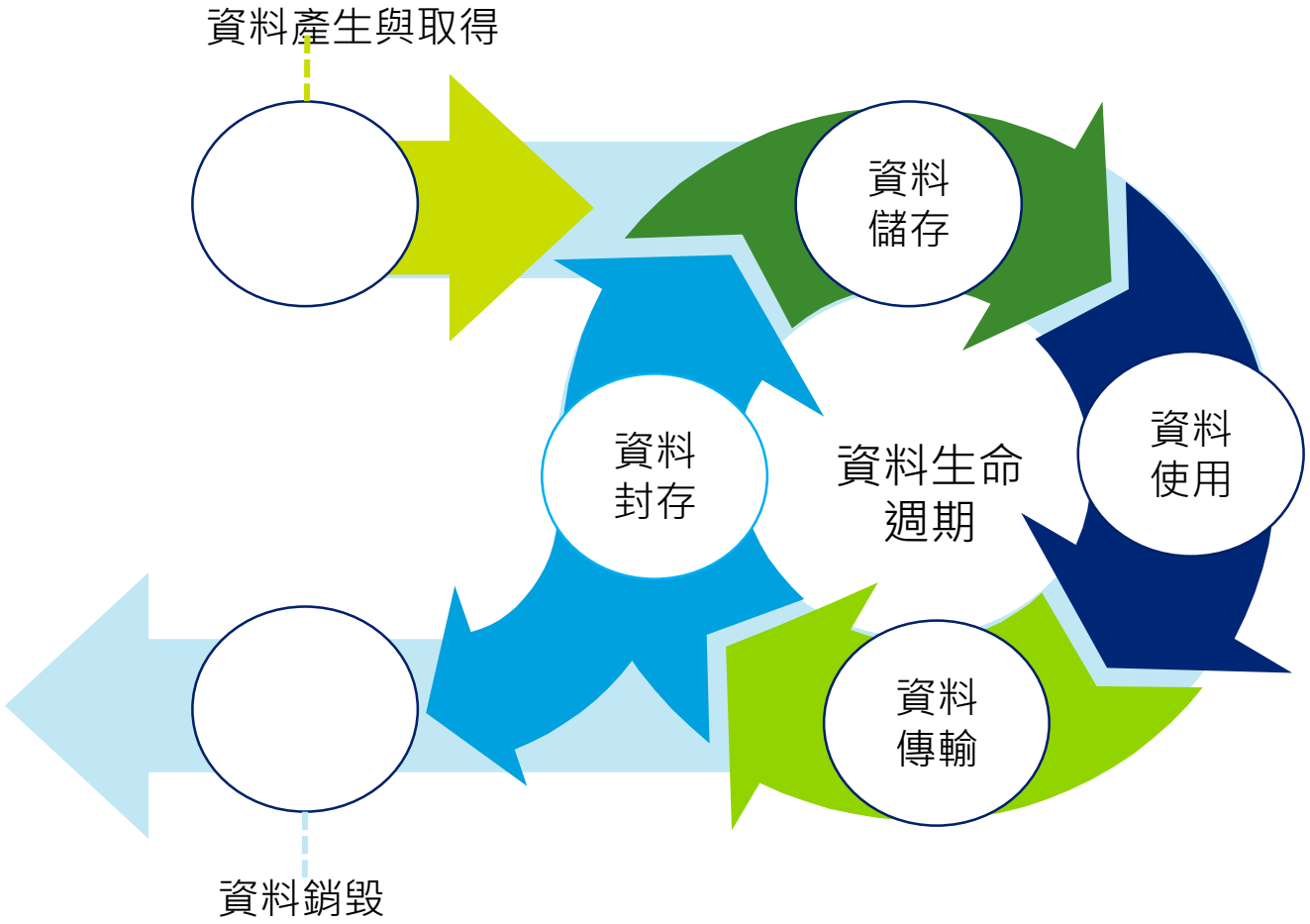


營運管理單位依據演練計畫，於執行測試演練前擬訂書面演練計畫及時程表

營運管理單位進行營運衝擊分析時，應判斷各項資訊資產與業務服務流程中斷時，產生對於各項業務服務流程所造成之影響及衝擊程度，據以判斷最大可容忍中斷時間(MTPD)、系統復原時間目標(RTO)以及資料復原點目標(RPO)等，並分別給予重要分級

資料管理面

資料管理面將會從資料生命週期管理（Information Lifecycle Management）的角度，來探討4G應用服務系統從資料的產生與取得、資料儲存、資料使用、資料傳輸、資料封存到資料銷毀這整個過程中的資訊安全管理機制，資料生命週期如下圖所示。



資料管理面 -資料產生與取得

應用服務系統於蒐集個人資料前，應取得使用者同意，並進行個資告知聲明。

依據個資法第八條之要求，**向當事人蒐集其個資時，應明確進行個資告知聲明**，其告知內容應包含：

1) 蒐集個資之機關名稱
2) 蒐集目的
3) 蒐集之個資類別
4) 個資利用期間、地區、範圍
5) 當事人可行使之權利
6) 當事人保有自由選擇提供個人資料之權利，如不提供，將對其權益之影響

另外，若**符合以下狀況者，得免告知**，可直接向當事人進行個人資料之蒐集：

1) 依法律規定得免告知。
2) 個人資料之蒐集係公務機關執行法定職務或非公務機關履行法定義務所必要。
3) 告知將妨害公務機關執行法定職務。
4) 告知將妨害公共利益。
5) 當事人明知應告知之內容。
6) 個人資料之蒐集非基於營利之目的，且對當事人顯無不利之影響

資料管理面 -資料儲存、使用及傳輸

1. 對於存放個人資料或機敏性檔案的系統，應建立資料外洩防護與網站管理機制

2. 對於存放個人資料或機敏性檔案的系統應定期進行資料稽核，使用紀錄、軌跡資料及證據之保存都必須被完整保留

單位間進行資料或軟體交換，應訂定正式的協定，將機敏性資料的安全保護事項及有關人員的責任列入

透過FTP線上傳輸方式應使用加密機制或專線等機制

透過電子郵件傳輸個資或機敏性資料，應對檔案本身施予加密或編碼等保護機制

對個人資料或機敏性資料應在使用過程中以加密方法保護，並決定採取適當等級的安全保護措施

營運管理單位應遵守資料保密規範，對於測試用之個人資料或機敏性資料，應先進行資料遮蔽處理或管制保護

在使用真實的個人資料或機敏性資料進行測試時，應採行適當之保護措施

資料管理面 -資料封存及銷毀

資料封存

1. 應準備適當及足夠的備援設施，定期執行必要的資料及軟體備份和備援測試演練作業，以便發生災害或是儲存媒體失效時，可迅速回復正常作業

資料庫管理系統管理	資料庫帳號及存取權限管理
資料庫實體檔案目錄管理	資料管理

2. 資料備份作業原則如下：

A. 正確及完整的備份資料

B. 備份資料應有適當的實體及環境保護，其安全標準應盡可能與主要作業場所的安全標準相同。

C. 應定期測試備份資料，以確保備份資料之可用性

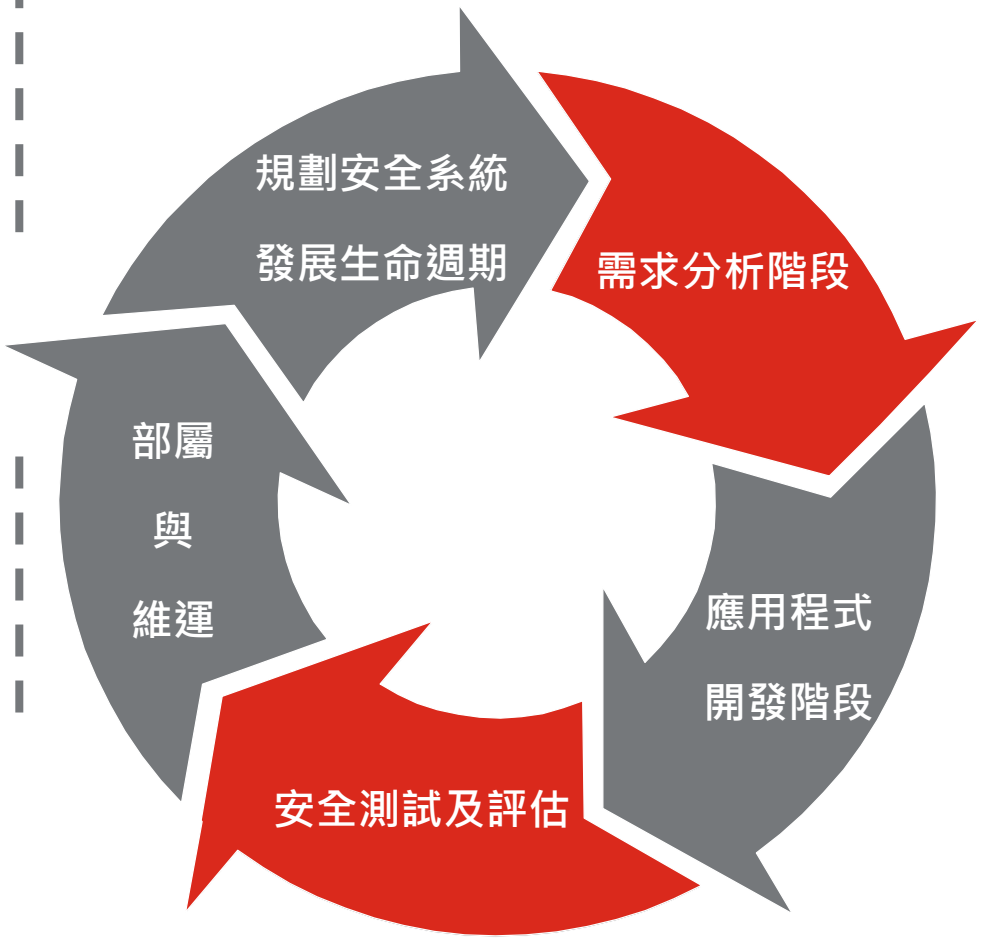
資料銷毀

1. 完成銷毀與刪除作業後，個資或機敏性資料檔案應不復存在
2. 不可再復原及留存備份個資或機敏性資料檔案
3. 進行個資或機敏性資料銷毀與刪除作業時，應確保該資料檔案上之資訊無法再利用
4. 謹慎選擇有適切控制措施及經驗之協力廠商委外廠辦理個資或機敏性資料檔案銷毀與刪除作業
5. 應要求協力廠商委外廠商提供個資或機敏性資料檔案已實際被銷毀或刪除之證明

系統管理面 -系統安全開發管理 1/3

定義完善的系統發展生命週期提供系統成功開發、實施和運作的基礎。

- 即時監控
- 源碼安全
- 定期稽核



可參考國家發行之正式規範進行Web及App開發

系統管理面 -系統安全開發管理 2/3

在分析與描述安全的軟體需求時，系統開發人員應掌握SMART+原則具體描述

S Specific：明確的，不模糊的。需求必須提供詳細的說明，同時包含一致的專業用語

M Measurable：可量化、可量測的。需求必須可以被分析與測試

A Appropriate：適當、符合所需的。需求必須被驗證以確保符合真正需要

R Reasonable：有依據、具合理性。需求執行前最好參照類似專案

T Traceable ：可追蹤 、有建檔 及有紀錄可循。需求必須融入開發生命週期以容易追蹤或驗証

系統管理面 -系統安全開發管理 3/3

區隔系統測試與開發環境

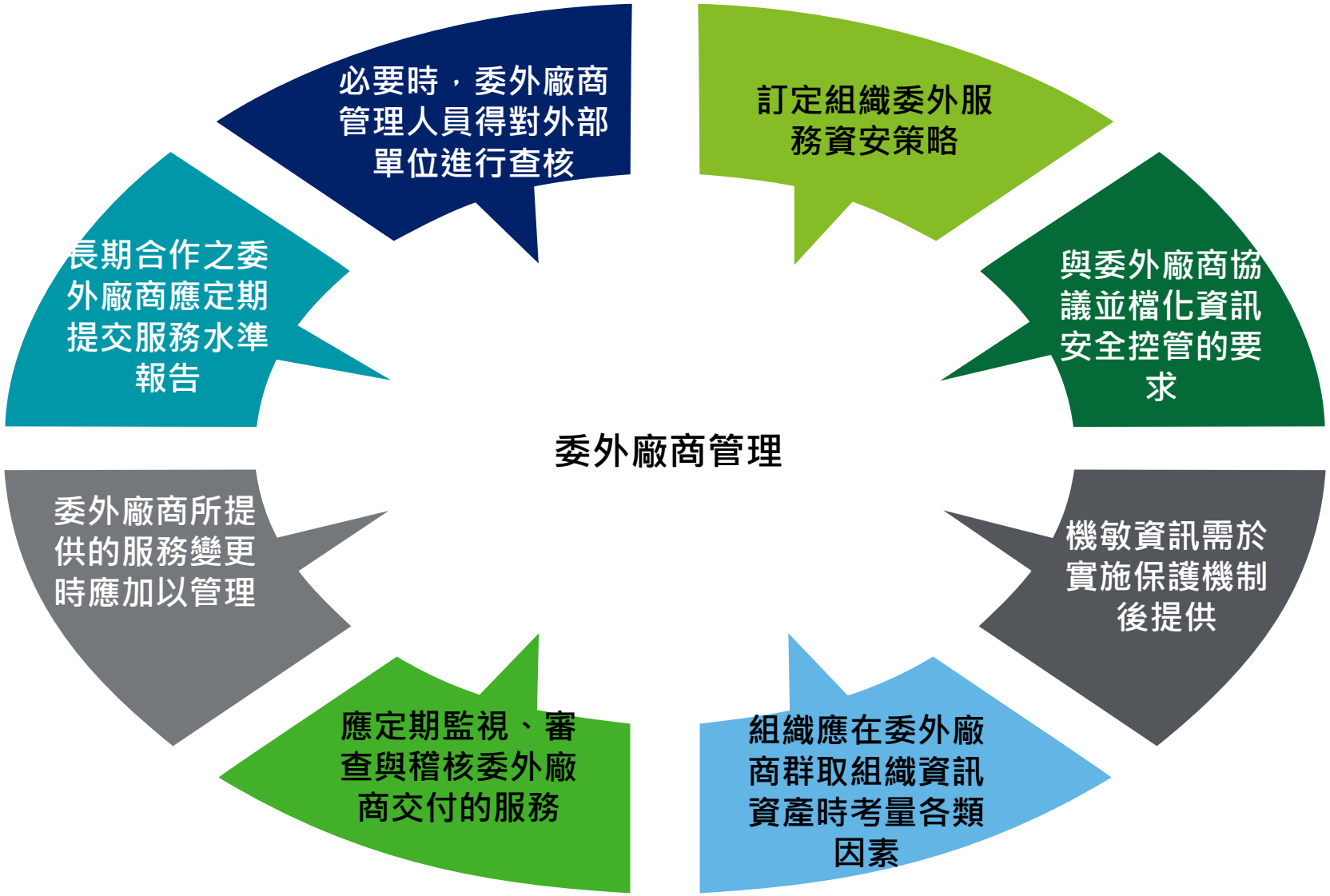
安全測試及評估

- 靜態代碼分析
- 威脅和弱點分析
- 人工代碼審查
- 滲透測試/分析
- 攻擊面審查
- 驗證測試/評估範圍
- 動態代碼分析

系統開發人員

伺服端安全檢測

系統管理面 -委外廠商管理



系統管理面 -雲端環境安全管理 1/2

根據美國國家標準技術研究所NIST的定義，雲端運算是一個支援方便性與即時性的網路存取模式，使用者可自行調控所需的運算資源；另一方面，4G應用服務系統營運管理單位能有效地管理整個可共用與可調整的運算資源，以達到降低管理成本、彈性提升計算處理能力及易於量測服務等目的

系統管理面 -雲端環境安全管理 2/2

雲端服務的5個基本特徵

1 **隨需隨用(On-demand self-service)：**使用者可以單方面的使用其計算能力，並能自動的得到所需要的資料，不需要隨時與服務供應商互動。

2 **廣泛的網路連接(Broad network access)：**使用者可以使用各種平臺來連接網路，如智慧型手機、筆記型電腦、桌上型電腦、穿戴式裝置及平板電腦或物聯網智慧裝置等

3 **資源共用(Resource pooling)：**所提供的運算資源可依使用者的需求自動動態分配，使用者無須也無法控制服務資源來源

4 **快速彈性(Rapid elasticity)：**所提供的服務是快速且有彈性的，對於使用者而言，可配置的功能似乎是無限的

5 **測量服務(Measured Service)：**雲端運算提供服務時，會計量、監控資源的使用，以達到雲端系統自動控制與優化的目的

系統管理面 -網路安全架構 1/3

(1)網路規劃與建置

(2)網路設備管理

設備應放置於機房統一管控，並使用專屬線路，以保護設備及資訊的安全，並提供適切的存錄與監控機制，以記錄相關執行活動

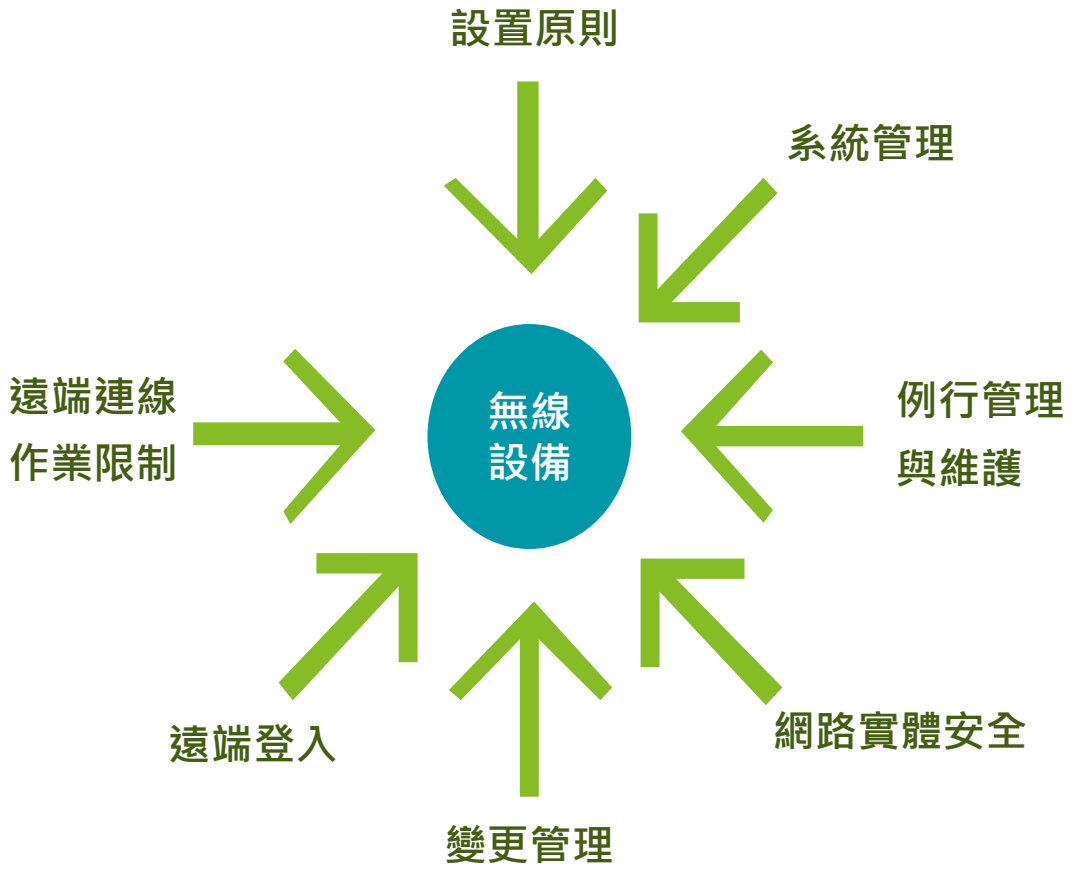
網路設備連線保護措施

(3)防火牆管理及入侵偵測防禦系統

系統管理面 -網路安全架構 2/3

(5)路由器及交換器

(6)無線設備



系統管理面 -網路安全架構 3/3

(8)通訊協定傳輸安全考量

- 考量傳輸內容之正確與完整性，且確保其不被未經授權存取
- 傳輸重要資料時，應將傳輸資料之傳輸途徑予以適當加密
- 加密技術及安全機制須先經資訊安全人員評估
- 稽核軌跡與網路資安事件處理

(9)網路介接管理

- 與其他電信業者介接之網路，應明訂網路介接責任點
- 部維護與其他業者之互連網路架構圖，並標示責任介接點
- 建立互連網路之監控運機制

(10)網路風險管理

- 應設定使用者電信服務供應商的提示以資識別
- NMC網域啟用Anti-spoofing功能，偵測IP spoofing
- 採用適當的鑑權機制以防範來源造假

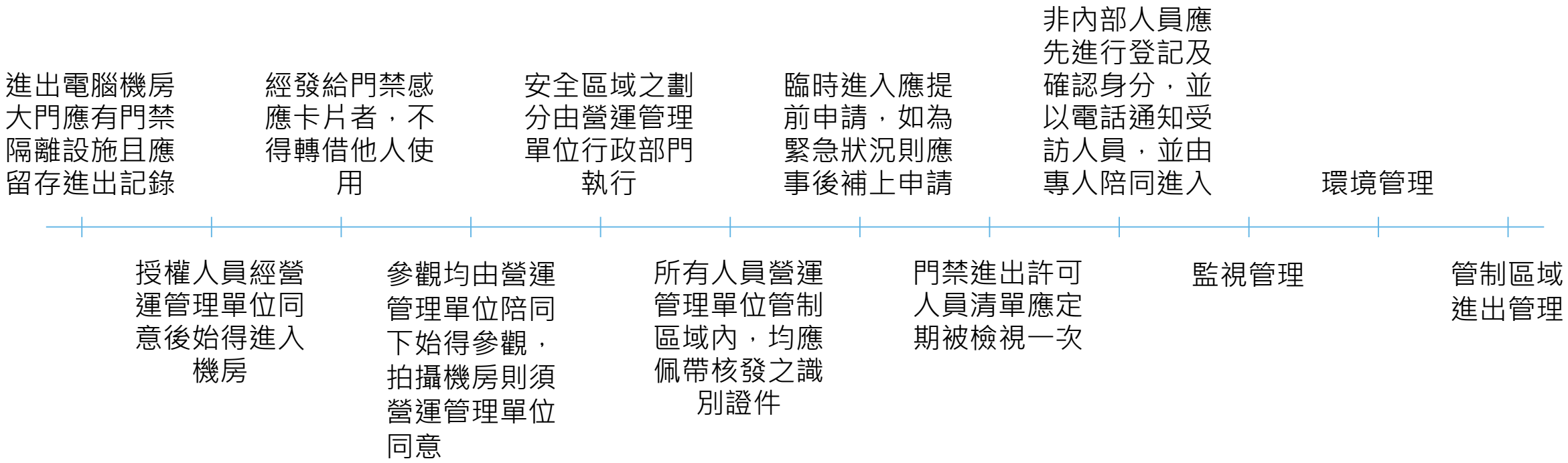
(11)網路檔案服務(Network File Service, NFS)

- 除經適當授權外，電腦主機嚴禁存取NFS伺服器
- 應限定各主機存取檔案系統之類型
- 禁止將NFS伺服器開放給任何放在外部網路的電腦主機存取
- 禁止未經授權於內部網路當中進行檔案分享
- 除經適當授權外，所有檔案分享應透過檔案伺服器

(12)網路流量管理

- 除經適當授權外，電腦主機嚴禁存取NFS伺服器
- 應限定各主機存取檔案系統之類型
- 禁止將NFS伺服器開放給任何放在外部網路的電腦主機存取
- 禁止未經授權於內部網路當中進行檔案分享
- 除經適當授權外，所有檔案分享應透過檔案伺服器

環境管理面 -電腦機房實體環境管理



環境管理面 -資訊設備管理

(1)設備管理

資訊設備應放置於安全且有人管理處

資訊設備進行維護時應留下相關紀錄及資料

資訊設備移動時應有專人陪同

資訊設備不堪使用時，須依循規定進行汰換

(2)媒體管理

磁帶置放之場所應留意其實體安全控制措施

定期進行NAS備份，同時每週將NAS資料手動備份到磁帶

定期進行備份媒體之盤點

每隔週進行備份媒體異地儲存

機器設備之維護作業，須由設備保管人員或機房操作員陪同維護廠商工程師辦理

(3)資訊設備報廢

資訊設備經評估不堪使用或不擬使用時，應確保資料不可讀方可報廢

資訊設備進行移交時，應予以清除資料方可移交

測試設備使用完畢後歸還廠商時，需確認資料皆予以清除方可歸還

環境管理面 -安全檢測要求

為有效瞭解及管理行動應用App之安全弱點，須定期行動應用App進行安全檢測，並產生檢測評估報告，列舉所發現的安全弱點並描述對行動應用App安全影響程度，而負責開發行動應用App之單位應針對弱點項目擬定改善方式，降低弱點被利用進行攻擊App的可能性。

檢測安全等級如下:

檢測安全等級	檢測內容
初級	主要檢測無連網之基礎功能安全性，檢測方式可採自動化工具檢測，並輔以適當之人工檢測，或純人工檢測
中級	主要檢測連網及認證安全性，檢測方式採人工檢測方式為主
高級	主要檢測付費資源安全性，檢測方式採人工檢測方式為主

行動應用程式規範分類與基準分級檢測對應如下：

	初級檢測功能相關之安全性	中級檢測連網及認證安全性	高級檢測交易相關之安全性
純功能性	★	V	V
具認證功能與連網行為	-	★	V
具交易功能	-	-	★
★代表為必要送測之檢測等級，V為可自由選擇通過之檢測等級			

環境管理面 -安全檢測要求：行動應用App安全檢測 1/3

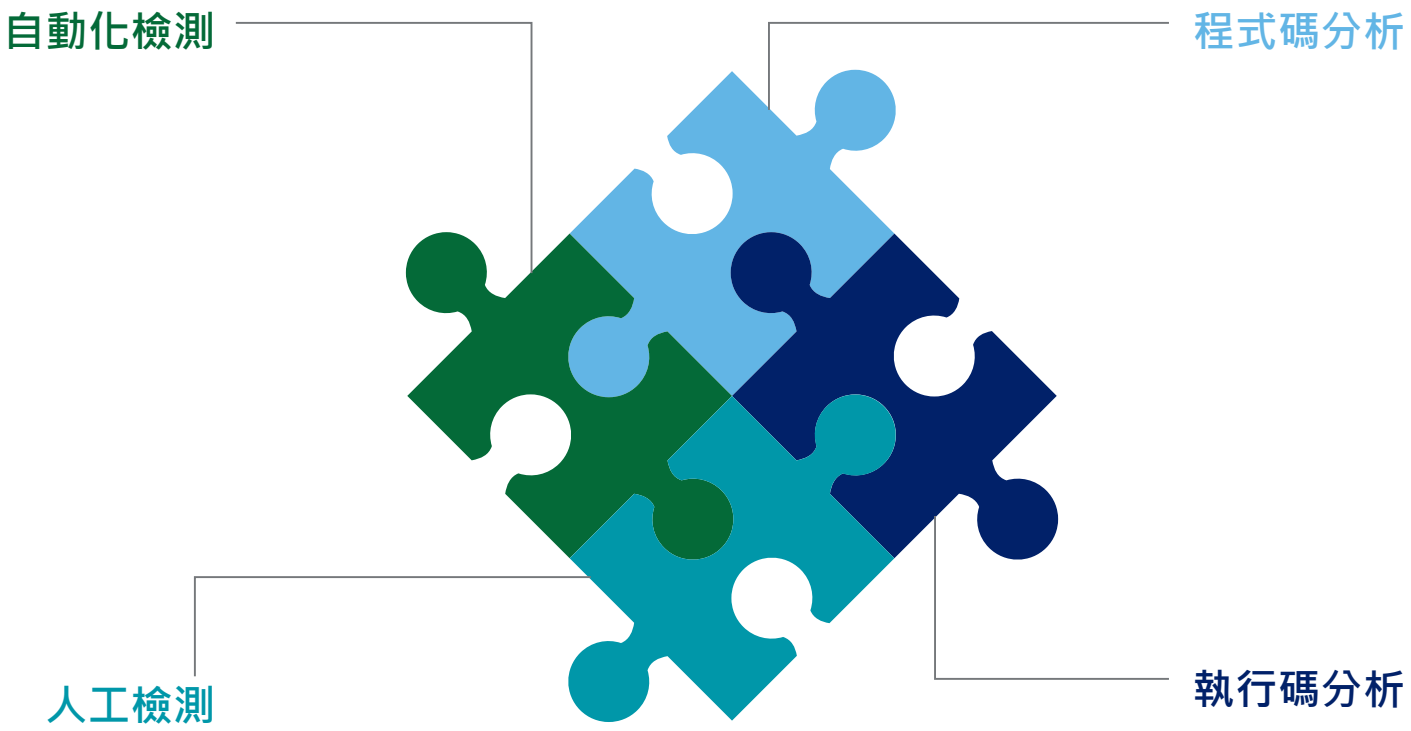
資安技術人員應針對每一檢測項目，訂定其檢測編號、檢測項目、檢測分級、檢測依據、技術要求、檢測基準及檢測結果等欄位，且應依照行動應用程式安全訂定基本資安檢測基準的五大面向:**行動應用程式發布安全**、**敏感性資料保護**、**付費資源控管安全**、**行動應用程式使用者身分認證**、**授權與連線管理安全及行動應用程式碼安全進行檢測**，其五大面向說明如下:

五大面向	說明
行動應用程式發布安全	主要適用於發布行動應用程式之相關資訊安全檢測基準，包括發布、更新與問題回報等
敏感性資料保護	主要適用於敏感性資料與個人資料保護之相關資訊安全檢測基準，包括敏感性資料蒐集、利用、儲存、傳輸、分享及刪除等
付費資源控管安全	主要適用於付費資源使用及控管
身分認證、授權與連線管理安全	主要適用於行動應用程式身分認證、授權與連線管理之相關資訊安全檢測基準，包括使用者身分認證與授權及連線管理機制等
行動應用程式碼安全	主要適用於行動應用APP開發之相關資訊安全檢測基準，包括防範惡意程式碼與避免資訊安全性漏洞、行動應用APP完整性、函式庫引用安全與使用者輸入驗證等

環境管理面 -安全檢測要求：行動應用App安全檢測 2/3

檢測方式

資安技術人員在未取得原始碼情況下進行測試，初級檢測以自動化工具進行檢測，中級、高級檢測以自動化工具及人工方式檢測，並進行逆向工程取得程式碼後檢測，使用原始碼掃描工具進行掃描並搭配人工分析。針對各級檢測使用之方式進行說明。



環境管理面 -安全檢測要求：行動應用App安全檢測 3/3

檢測結果與產出

檢測結果產出，應包含在測試過程中的所有紀錄與結果，並應依所有檢測項目判定標準說明測試標的檢測結果為「符合要求或不符合要求」檢測結果與產出應包含但不限於：

環境管理面 -安全檢測要求：應用系統弱點掃描

為避免4G應用服務系統因為自身弱點成為駭客攻擊對象，資安技術人員須定期對4G應用服務系統伺服器進行弱點掃描，並於弱點掃描報告說明所發現的弱點對系統帶來的影響以及建議改善的方式。

定期掃描
資安技術人員應定期執行4G應用服務系統伺服器弱點掃瞄，評估是否應採取適當的管控措施，以處理所面臨之風險

弱點控管
若4G應用服務系統主機存在之弱點需採取管控措施，應經過適當的評估並留下相關紀錄

修補弱點
修補系統主機所存在之弱點時，應優先修補高風險(含)以上的弱點。經評估若有無法修補之高風險項目，應提出補償性措施來控制風險，避免該高風險項目成為駭客攻擊目標

選定弱點掃描工具
使用弱點掃描工具應確認工具本身的版本及弱點資料庫是否為最新，避免使用到過期的資料庫進行掃描，使得產出的掃描結果失真

撰寫弱點掃描報告
當弱點掃描完成後，應將產出的結果於報告中呈現，其報告內容應包含目標基本資訊、執行時間、工具的版本、工具的弱點資料庫版本、弱點風險等級、弱點說明及改善建議

4G應用服務系統營運資安參考指引說明

事中應變機制

(一)資訊安全事件管理

以委外方式辦理個人資料或機敏性檔案銷毀或刪除作業時，應要求協力廠商委外廠商執行銷毀或身除作業後，檢附個資或機敏性資料檔案已實際被銷毀或刪除之證明文件或檔案，以及執行銷毀中的資料檔案照片，或者資料銷毀或刪除執行的影片，除留存紀錄證明資料已按照標準流程進行銷毀或刪除以供備查外，同時也能監督協力廠商委外廠商是否有依照合約內容履行其所應交付的服務。

1. 事故之定義、目的、範圍、角色、責任、管理承諾、與各機關間之協調及符合性
2. 制訂相關程式，並促進事故應變政策及各項控制措施之實作
3. 應定期審查事故應變政策及事故應變程式等相關檔，確保制度之合適性及程式之完整性

資訊安全事件定義

凡於作業環境中，因下列事項導致資訊資產之機密性、完整性、可用性遭受影響，足以危害內部運作與權益之事件。

A.內部資安事件：發現（或疑似）遭內部人為惡意破壞毀損、作業不慎等事件

B.外力入侵事件：發現（或疑似）電腦病毒感染、駭客攻擊（或非法入侵）等事件

天然災害：颱風、水災、地震、雷擊等

突發事件：火災、爆炸、重大建築災害、電力中斷及資訊網路骨幹（主幹寬頻）中斷事件等

事故應變之角色權責及通報程序

資訊安全事件管理應制定相關權責，將管理機制流程化，確保職權獨立性分工及事件之可追蹤性。主要可劃分成下列幾種角色權責，各角色在事故通程序中的權責也各不相同：

角色	權責
事件發生單位	通報
通報受理窗口	受理、 通知相關人等
相關系統或業務負責人	處理、回報結果
相關系統或業務負責人主管	分析、追蹤

事故處理 1/4

資訊安全事件之處理階段

資訊安全事件之處理應包含抑制、消除及回復等三階段；處理資訊安全事件時，應辨識資訊安全事件之發生來源，並考慮根除資訊安全事件因素及回復資訊資產。

a

抑制

指降低資訊安全事件所造成之危害與損失如隔離中毒之設備

b

消除

指移除資訊安全事件對資訊資產所造成之威脅，如清除病毒、切換至備援線路

c

回復

指將受資訊安全事件所影響之資訊資產回復至正常狀況，如系統回復、重新連結網路等

事故處理 2/4

資訊安全事件之處理程序

資訊安全事件處理程序

1.營運管理單位應建立資訊安全事件的通報程式及管道

2.營運管理單位所有相關人員應隨時注意系統或資訊服務設施之安全弱點以及可能面臨之威脅

3.營運管理單位全體人員及其相關人員，應隨時保持警戒並進行通報

4.營運管理單位受理窗口，於評估資訊安全事件等級並研判影響範圍與程度後，依照通報程序進行通報

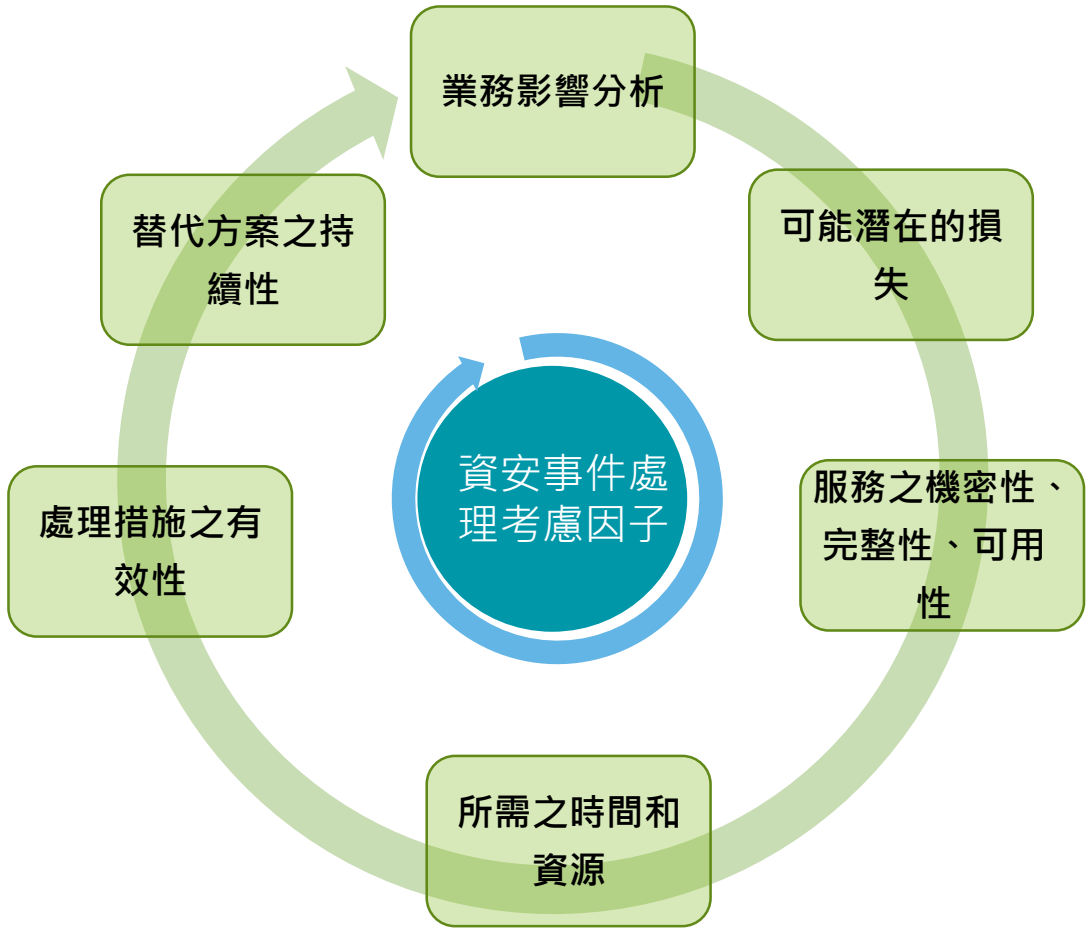
5.所有資訊安全事件均應立即通報並留下紀錄

6.事件紀錄應包含必要之資訊

7.資訊安全事件如涉及法令、法規，須確認處理措施是否合規

8.資訊安全事件於緊急應變處理結束後，採取必要之矯正措施並留存相關紀錄

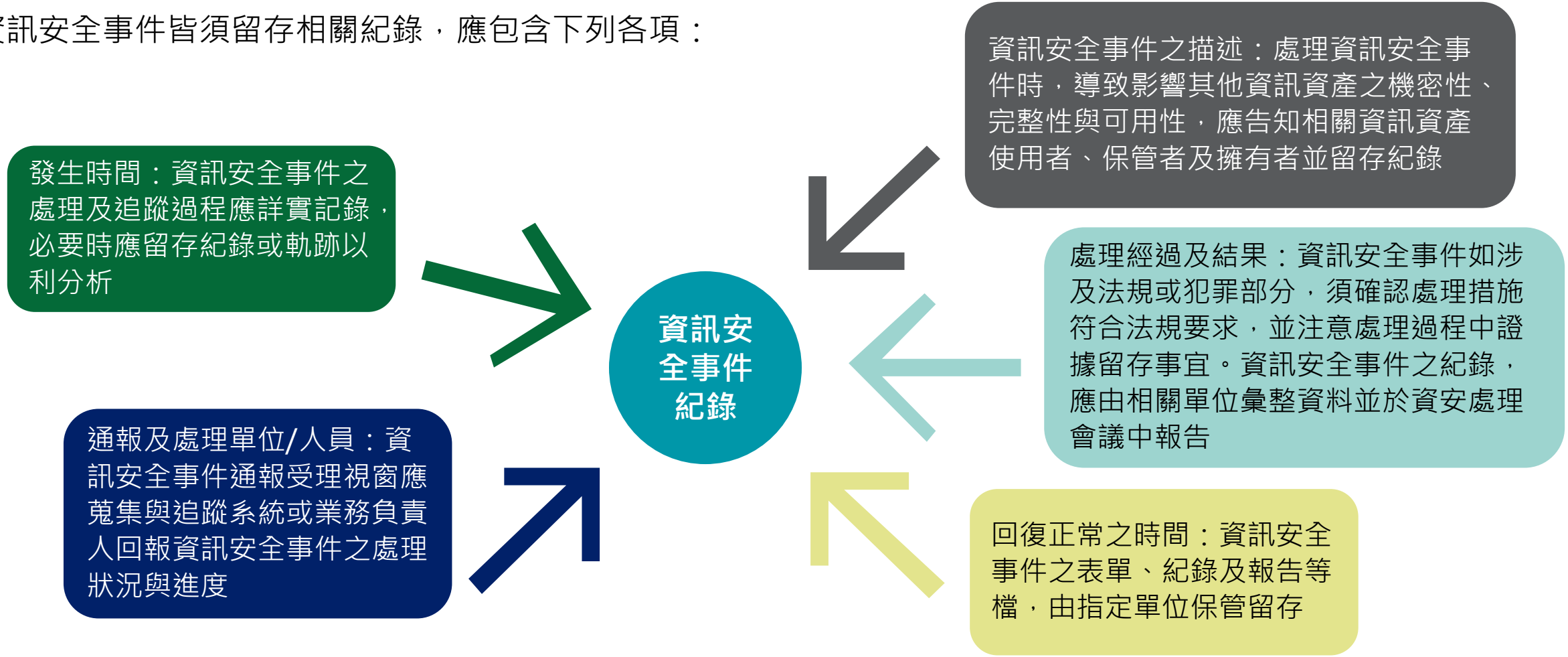
資訊安全事件處理需考慮因素



事故處理 3/4

資訊安全事件之記錄及追蹤

資訊安全事件皆須留存相關紀錄，應包含下列各項：

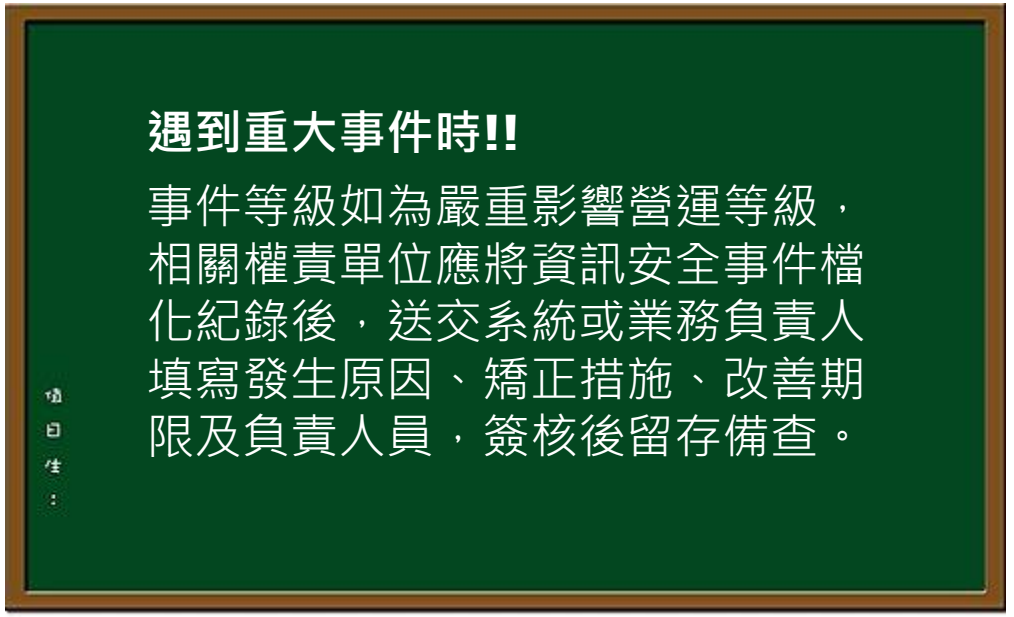


事故處理 4/4

資訊安全事件改善及回饋

資訊安全事件回復後，相關單位須審視資安事件通報及處理相關表單，並考量下列措施：

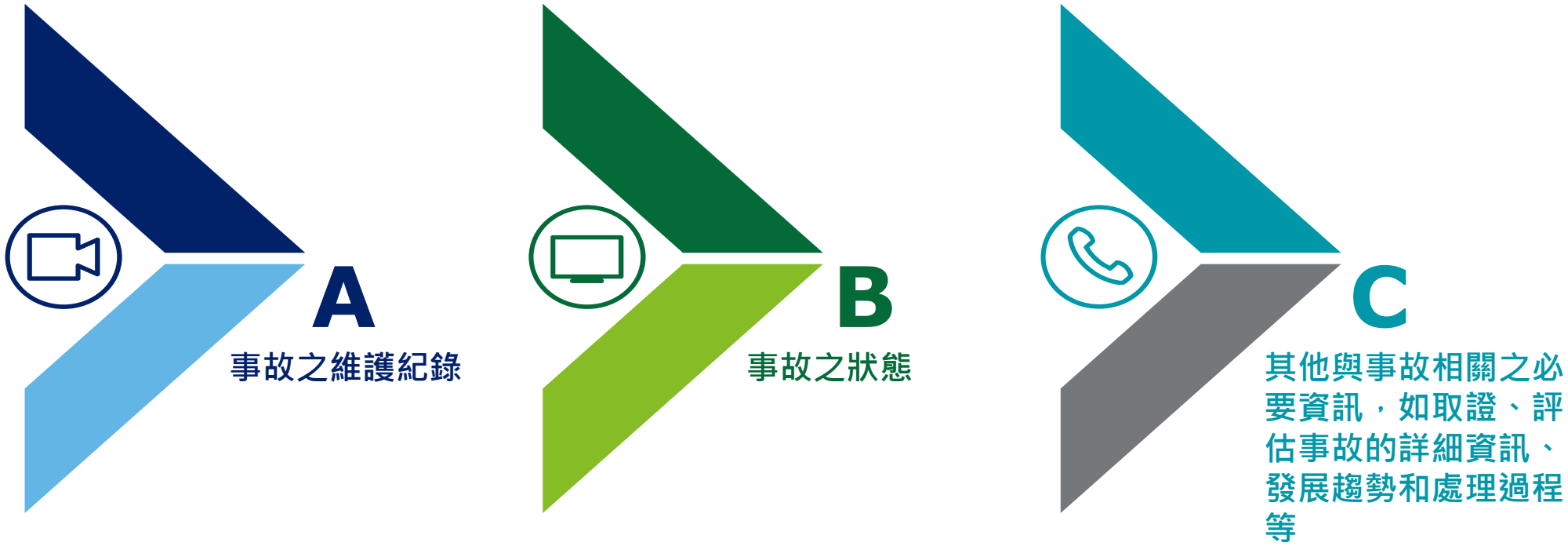
1. 重新審視資訊安全管理制度，檢驗是否有不足之處，並建議改善或新增控管措施
2. 重新設計控管措施時，應注意控管措施之有效性
3. 人為因素造成之資訊安全事件，應由各單位權責主管對相關失職人員採取適當之改善措施
4. 資訊相關單位應定期彙整資訊安全事件紀錄，定期檢閱資訊安全事件之有無再發生，並考量建構知識庫與監控規則。
5. 系統或業務負責人之權責主管應對發生頻率較高或投入復原成本較高之資訊安全事件提出改善計畫



事故監控

可考慮採用自動化機制來協助安全事故的追蹤及事故資訊的收集和分析，除此之外，也應定期追蹤事故後續發展及確保檔化資訊系統的安全事故。

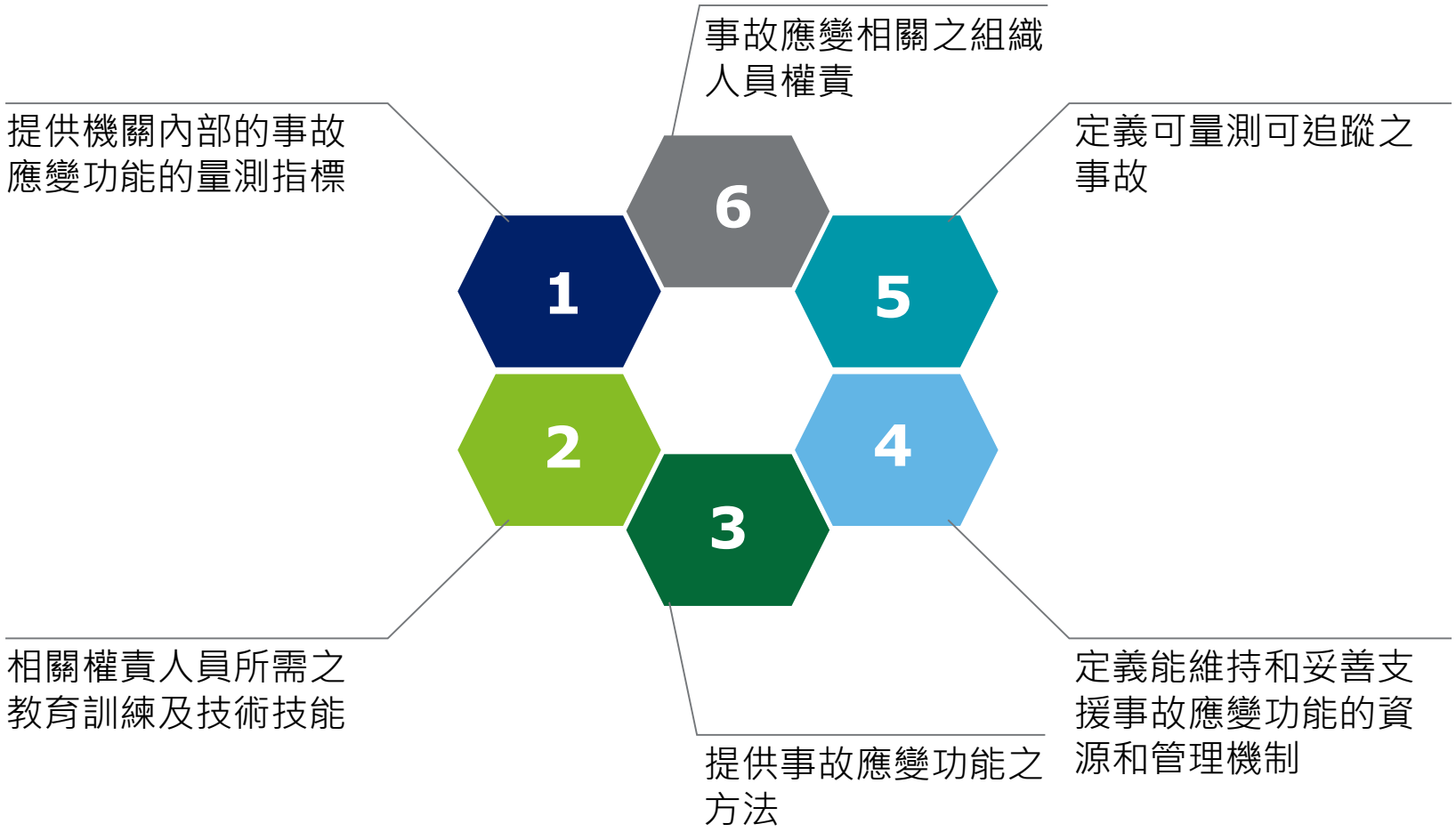
其中，檔化之資訊系統安全事故報告檔內容需包括以下內容：



事故應變

事故應變計畫

機關應擬定事故應變計畫，其內容應包含以下幾點：



(二)資安事件證據保全

數位證據有容易複製、容易修改及不易追溯等特性，因此在數位證據採集及保存上更需小心謹慎，方可顧及證據之完整性及正確性。

電子儲存媒介或系統中所存放的數位證據

1. 文字資料
2. 聲音或影像
3. 圖片、符號或其他資料

保存數位資料之設備

1. 電腦、周邊設備及數位儲存媒體
2. 網路連線設備
3. 監視錄影系統
4. 其他能儲存數位資料之裝置

(二)資安事件證據保全

數位證據取得要遵循合法、自願、真實的原則，因此當機關發生資安事件之際，需以有效的方式蒐集證據，且於第一時間進行數位證據保全，維持原證據的狀態確保後續件事分析工作能有效進行。

數位證據取得需注意以下原則：

	數位證據取得之原則
1.	為避免爭議，不以未經授權之方式取得證據。
2.	於蒐集證據當下，應確保相關第三公正方於現場一同檢視，避免後續作業產生之誤解及爭議。
3.	證據之蒐集應於事件發生後盡快完成，確保數位證物維持原本狀態。
4.	將證據蒐集及保全之過程留存檔化紀錄。
5.	注意數位證據儲存放置之實體環境。
6.	應進行證據備份機制，避免原始證據於採集及保全階段遭到破壞。

人員職掌

於數位證據的保全過程中，依照不同角色指派工作可確保過程中之環結辨識，保障證據之原始性及完整性。證據保全程式中主要的角色如下：

(1)現場記錄人員：

於現場狀況協助證據保全人員於證據蒐集及運送的過程中，進行過程之紀錄。

(2)證據保全人員：

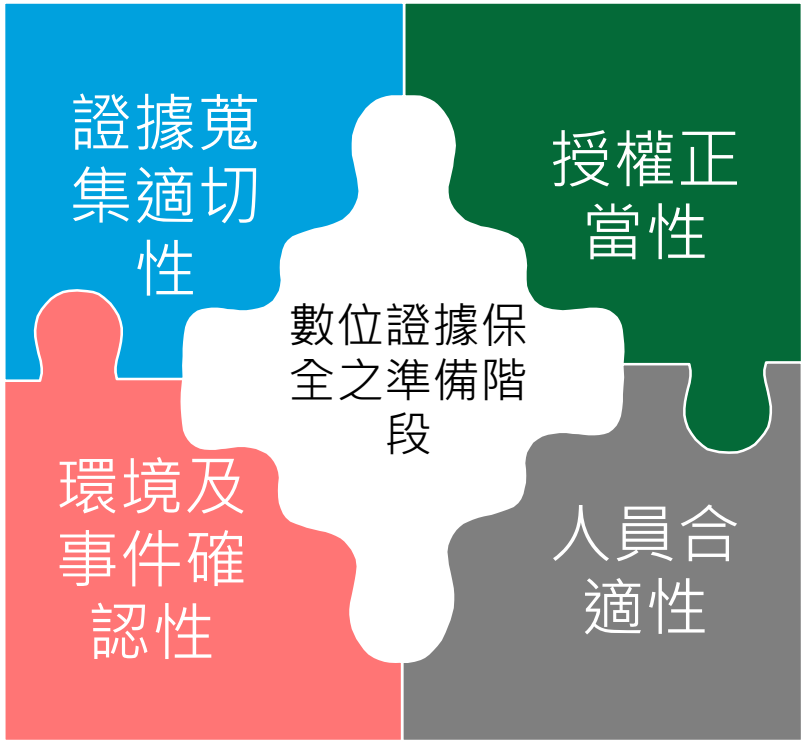
執行數位證據辨識、採集、封存及運送作業。

證據保全準備階段

於環境中正式進行數位證據採集之前，必須進行必要之安全防護措施，相關之準備措施如下：

預備合適採集工具及相關設備

事先了解事件狀況



符合正當之授權程序及採證許可

指派適當人員之角色權責

4G應用服務系統營運資安參考指引說明

事後處理機制

(一)資安事件排除後復原、回復及驗證

資安事件發生後應根據事件類別採取相對應之處理措施，辦識資安事件之發生來源進行處理，並考慮根除資安事件因素及回復資訊資產

1 **抑制**：
指降低資通安全事件所造成之危害與損失

2 **消除**：
指移除資通安全事件對資訊資產所造成之威脅

3 **回復**：
指將受資通安全事件所影響之資訊資產回復至正常狀況，

(二)資安事件發生後之改善及追蹤作業

資安事件之處理及追蹤過程應詳實記錄，必要時應蒐集相關資料或軌跡進行記錄與分析，以作為研擬矯正措施之參考

1. 資安事件應變處理完成後，盡速完成資安事件處理報告
2. 事件處理報告應包含事件發生簡述、事件應變過程及時序、資安事件根因分析、檢討、改善方案與計畫等
3. 定期追蹤實施改善措施的成效
4. 應考量建立當次資訊安全事件相關監控規則，以利未來類似事件發生之偵測與處理
5. 應檢視制度規範的完備性及對資訊業務單位提供必要的資安訓練與宣導，並提出制度規範修改建議

問題與討論

Deloitte.

勤業眾信

About Deloitte
Deloitte 泛指Deloitte Touche Tohmatsu Limited(即根據英國法律組成的私人擔保有限公司，簡稱"DTTL")，以及其一家或多家會員所。每一個會員所均為具有獨立法律地位之法律實體。Deloitte("DTTL")並不向客戶提供服務。請參閱 www.deloitte.com/about 了解更多有關Deloitte及其會員所。

Deloitte為各行各業的上市及非上市提供審計、稅務、風險諮詢、財務顧問、管理顧問及其他相關服務。Fortune Global 500大中，超過80%的企業皆由Deloitte遍及全球逾150個國家的會員所，以世界級優質專業服務，為客戶提供因應複雜商業挑戰中所需的卓越見解。如欲進一步了解Deloitte約245,000名專業人士如何致力於”因我不同，惟有更好”的卓越典範，歡迎瀏覽我們的Facebook、LinkedIn、Twitter專頁。

About Deloitte Taiwan
勤業眾信(Deloitte & Touche)係指Deloitte Touche Tohmatsu Limited(“DTTL”)之會員，其成員包括勤業眾信聯合會計師事務所、勤業眾信管理顧問股份有限公司、勤業眾信財稅顧問股份有限公司、勤業眾信風險管理諮詢股份有限公司、德勤財務顧問股份有限公司、德勤不動產顧問股份有限公司、及德勤商務法律事務所。

勤業眾信以卓越的客戶服務、優秀的人才、完善的訓練及嚴謹的查核於業界享有良好聲譽。透過Deloitte資源整合，提供客戶全球化的服務，包括赴海外上市或籌集資金、海外企業回台掛牌、中國大陸及東協投資等。