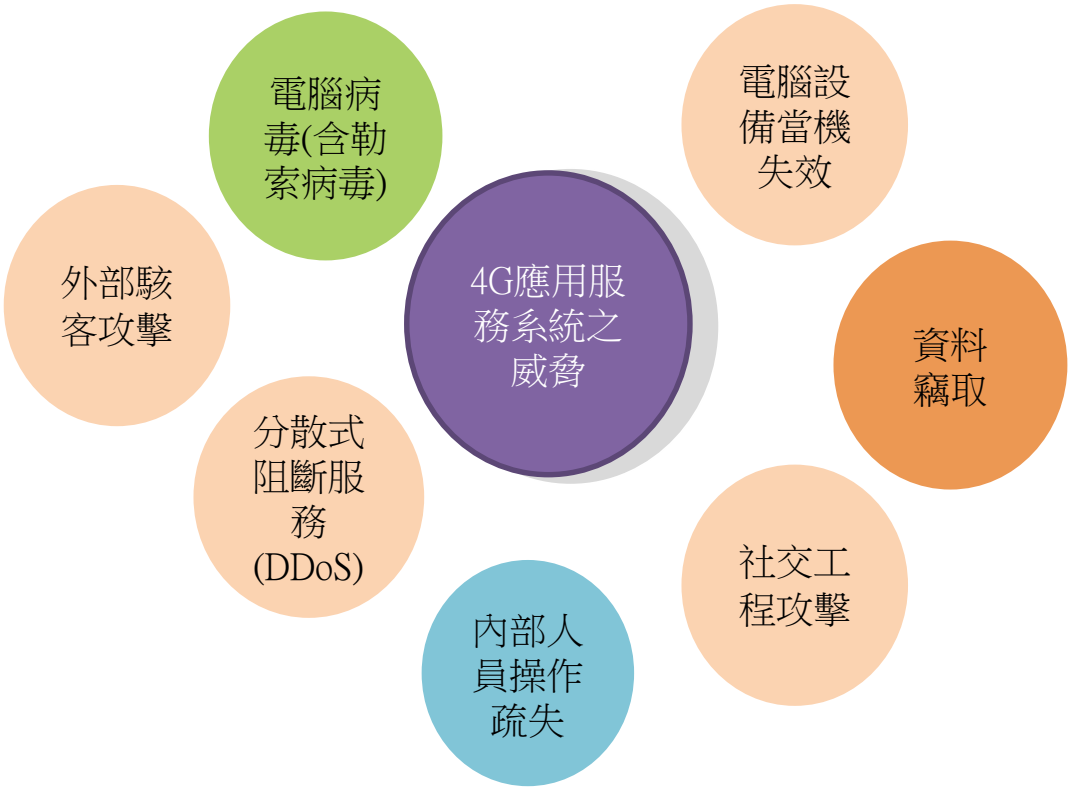
4G應用服務系統資安推動計畫

「4G應用服務系統營運資安參考指引」簡介

執行單位：財團法人資訊工業策進會、中華民國資訊軟體協會
報告人：李彥震 顧問

106年12月7日

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

「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

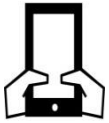
- 使用終端之風險容易被忽略
- 應用程式代管道多元，攻擊者可由不同管道的弱點進行攻擊

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應用服務系統營運管理角色


智慧型手機


平板電腦


穿戴式裝置

4G應用服務使用者

ISP通訊網路業者

4G應用服務系統營運模式

- Web應用系統 / 行動應用App / API應用程式介面
- AP Server / 後臺管理系統
- 資料庫管理系統(DBMS)
- 作業系統(OS) / 雲端服務平台(Cloud)
- 網路環境
- 實體環境

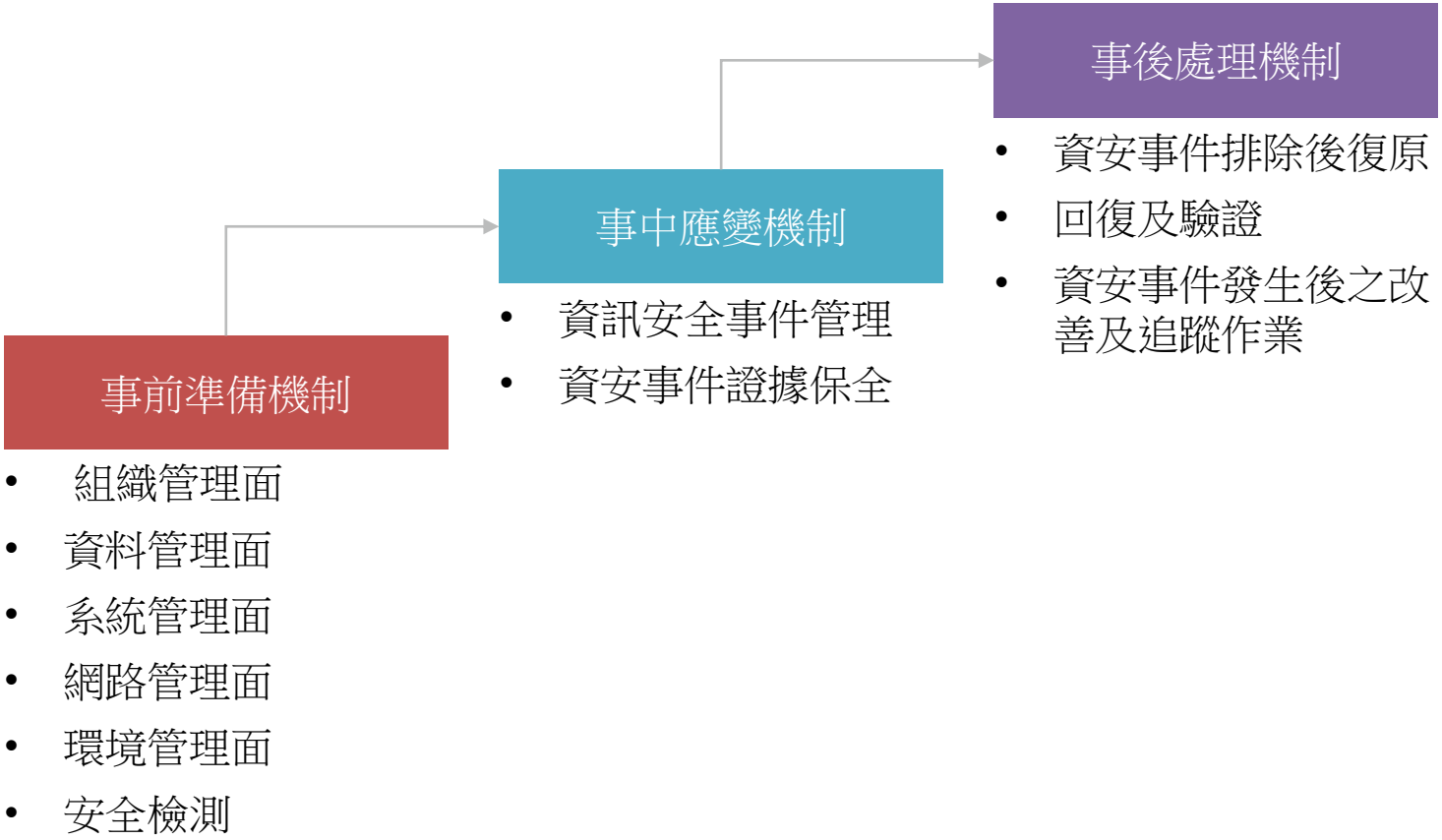
營運管理單位

- 系統開發人員
- 系統維運人員
- 資料庫管理人員
- 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應用服務系統營運資安參考指引摘要說明

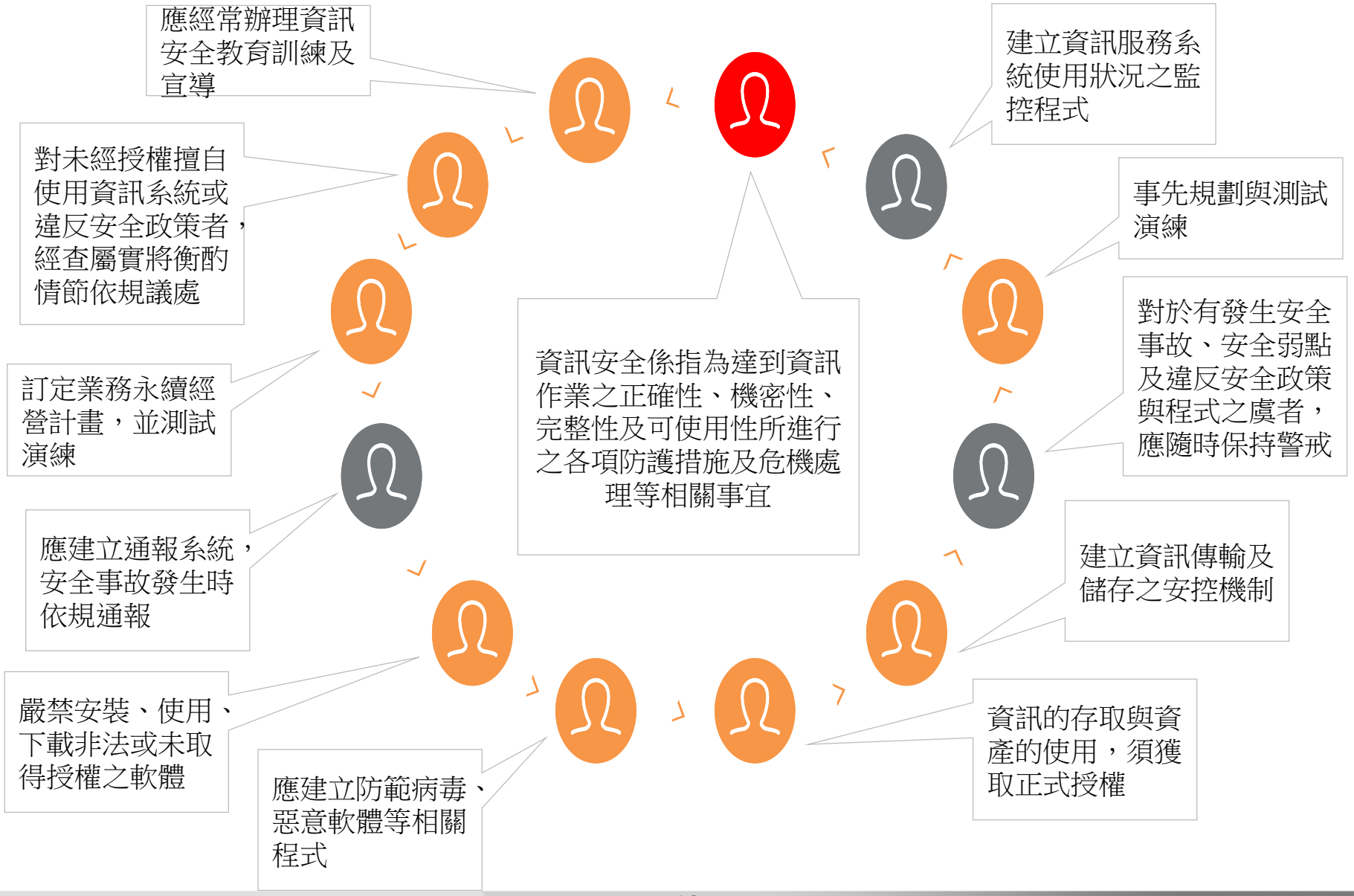
4G應用服務系統營運資訊安全要求



4G應用服務系統營運資訊安全要求

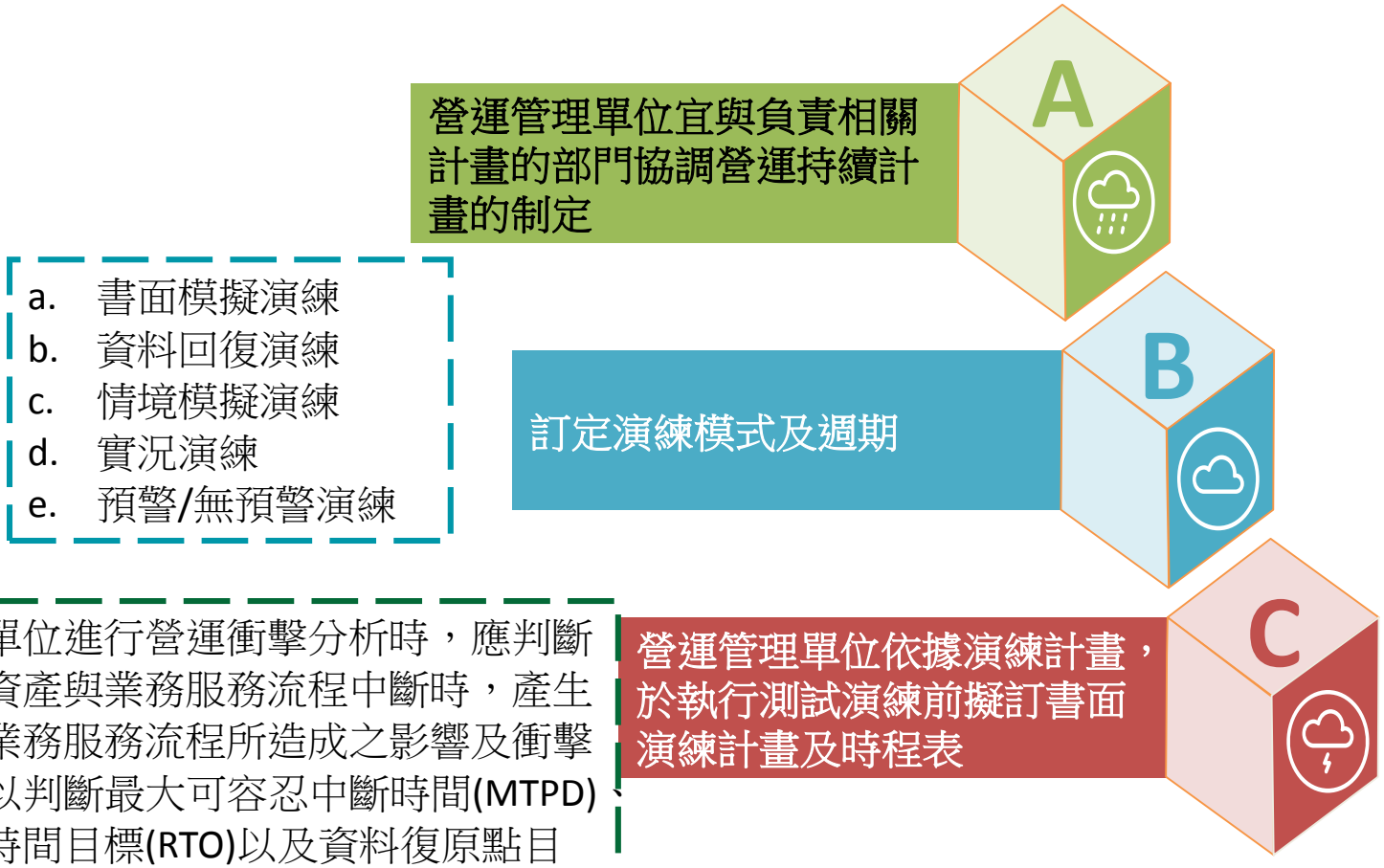
事前準備機制(摘要說明)

組織管理面 -資訊安全政策



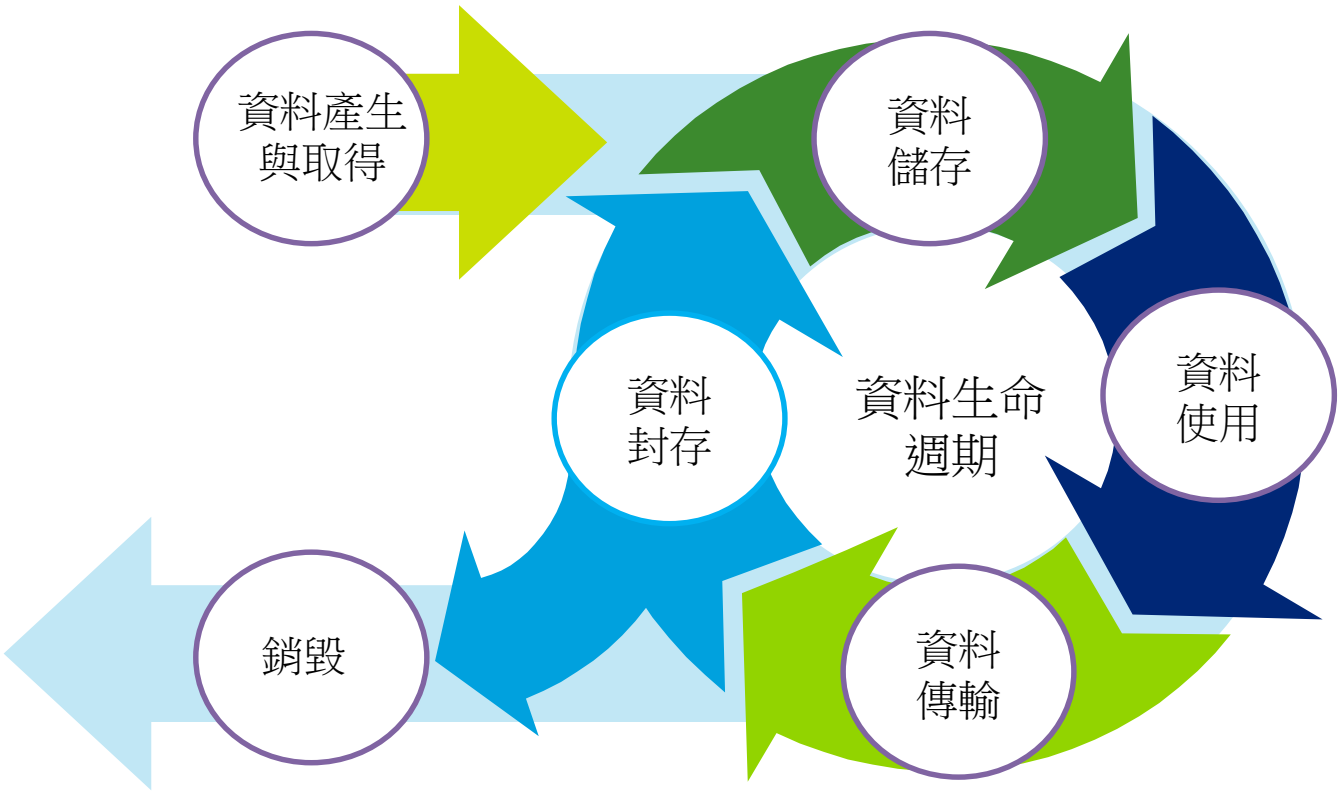
組織管理面 -營運持續管理：營運持續計畫/與相關計畫協調及容量管理計畫

- 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。



資料管理面

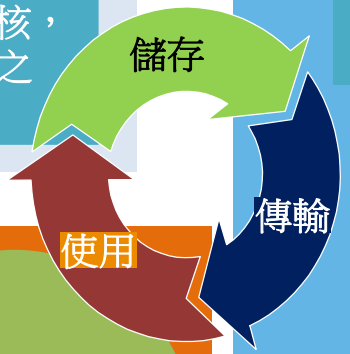
- 資料管理面將會從資料生命週期管理（Information Lifecycle Management）的角度，來探討4G應用服務系統從資料的產生與取得、資料儲存、資料使用、資料傳輸、資料封存到資料銷毀這整個過程中的資訊安全管理機制，資料生命週期如下圖所示。



資料管理面 -資料儲存、使用及傳輸

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

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

1

透過FTP線上傳輸方式應使用加密機制或專線等機制

2

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

3

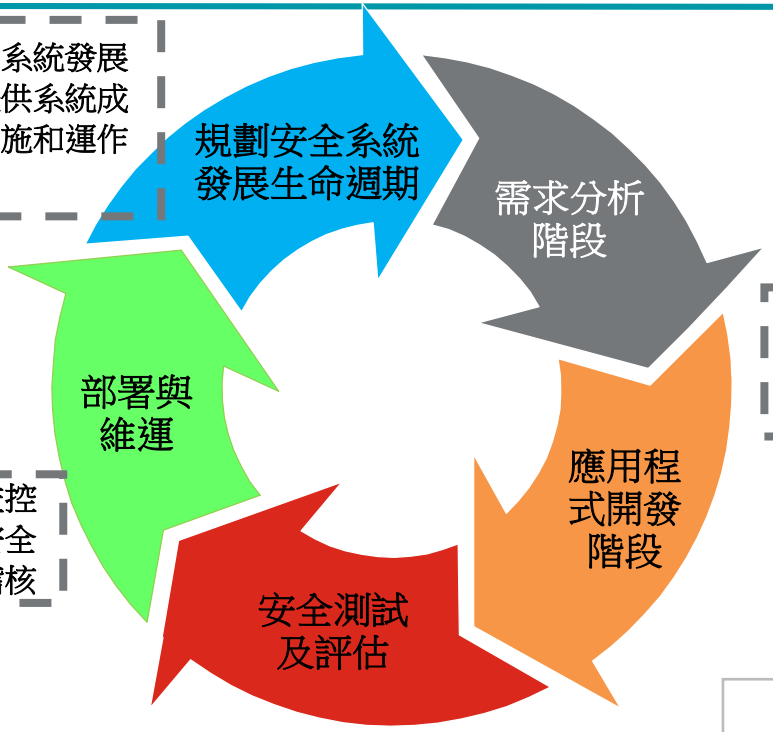
對個人資料或機敏性資料應在使用過程中以加密方法保護，並決定採取適當等級的安全保護措施

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

系統管理面 -系統安全開發管理

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。



可參考國家發行之正式規範進行Web及App開發

- 即時監控
- 源碼安全
- 定期稽核

區隔系統測試與開發環境

安全測試及評估

伺服端安全檢測

- 靜態代碼分析(（static code analysis）
- 威脅和弱點分析
- 人工源碼審查(code review)
- 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

系統管理面 -網路安全架構

(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 -委外廠商管理

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(摘要說明)

資訊安全事件管理

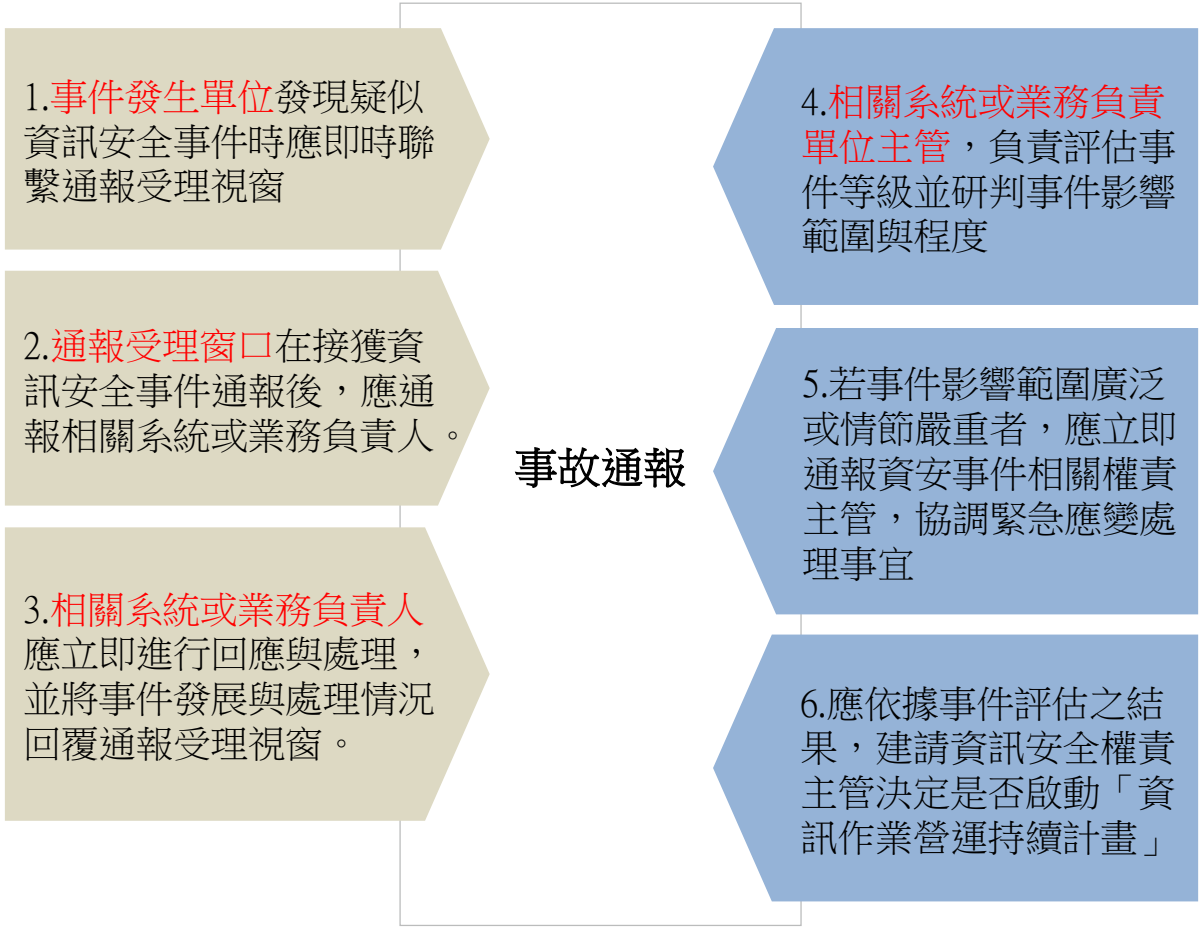
- 以委外方式辦理個人資料或機敏性檔案銷毀或刪除作業時，應要求協力廠商委外廠商執行銷毀或身除作業後，檢附個資或機敏性資料檔案已實際被銷毀或刪除之證明文件或檔案，以及執行銷毀中的資料檔案照片，或者資料銷毀或刪除執行的影片，除留存紀錄證明資料已按照標準流程進行銷毀或刪除以供備查外，同時也能監督協力廠商委外廠商是否有依照合約內容履行其所應交付的服務。

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

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

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

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

4G應用服務系統營運資安參考指引說明

事後處理機制(摘要說明)

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，辨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

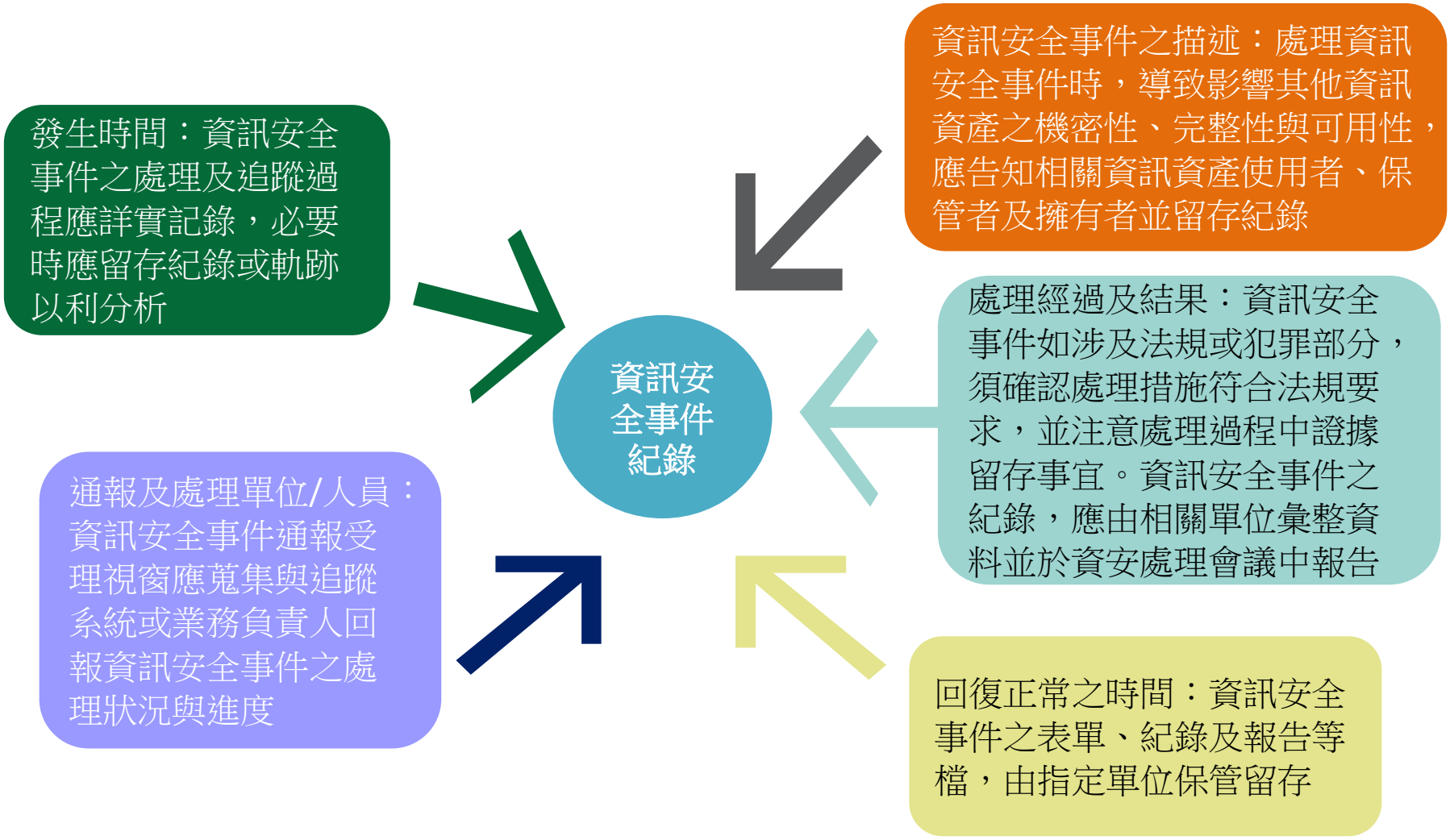
1 **抑制：**
指降低資通安全事件所造成之危害與損失

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，

資訊安全事件之記錄及追蹤

- **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：



事故應變計畫檢討

- 事故應變計畫，其內容應包含以下幾點：

Thank you