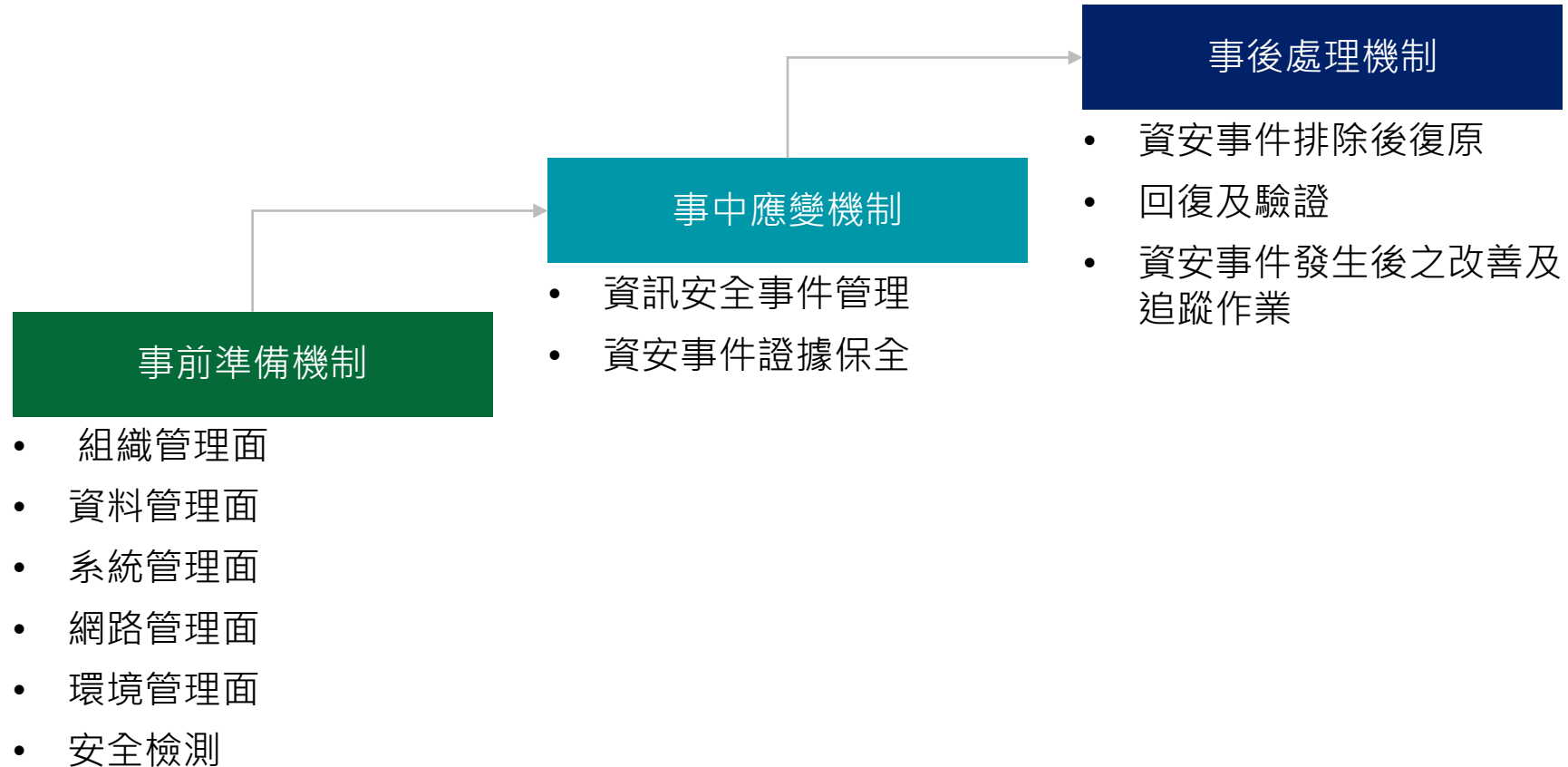


**4G應用服務系統資安推動計畫成果分享  
行動應用服務系統資安防護研討會  
「4G應用服務系統營運資安參考指引說明」**

簡報人：李民偉 顧問  
106年12月6日

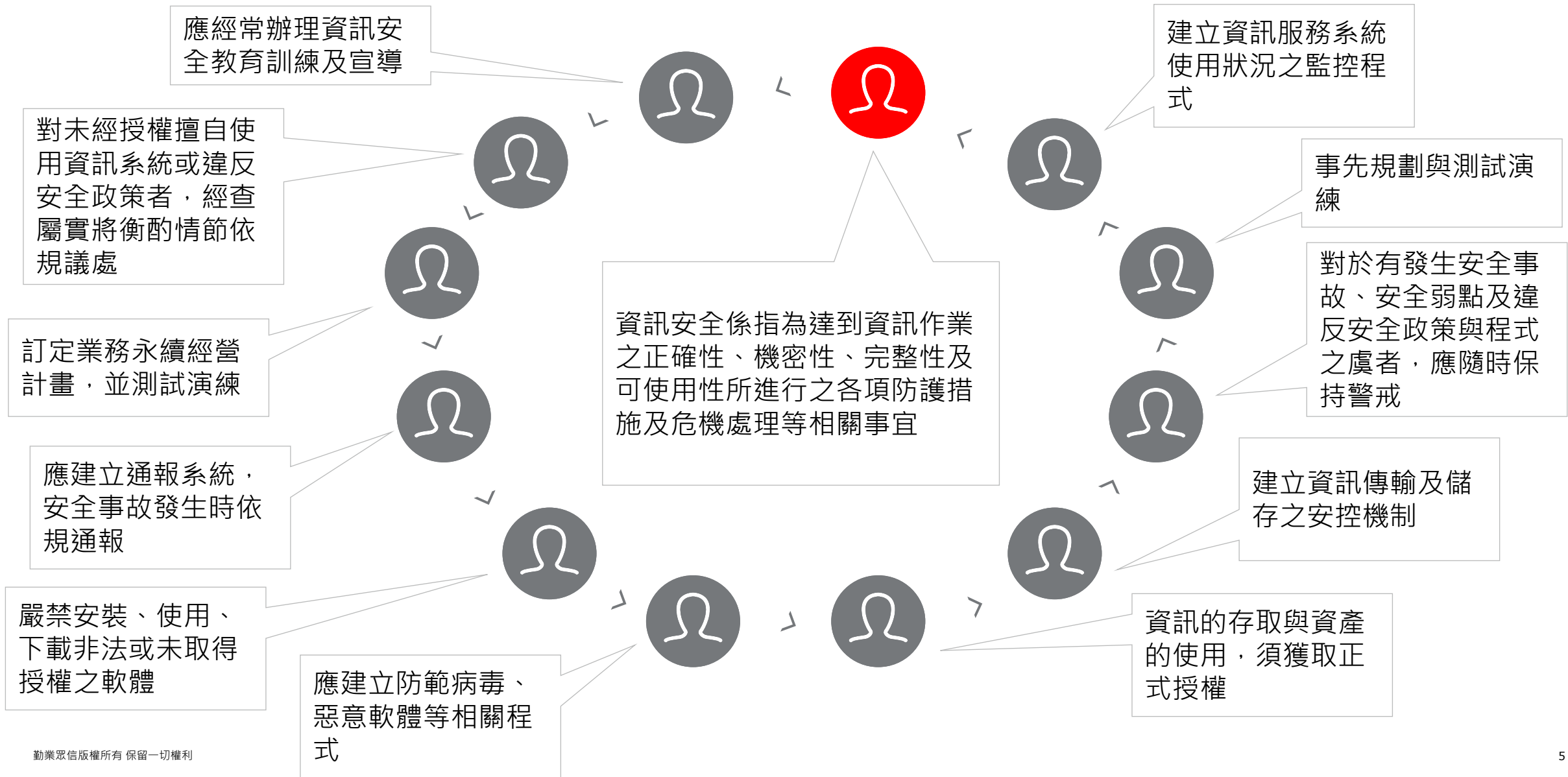
# 4G應用服務系統營運資安參考指引說明

# 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

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

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

重要職務人員應設置代理人制度，以確保營運作業不中斷

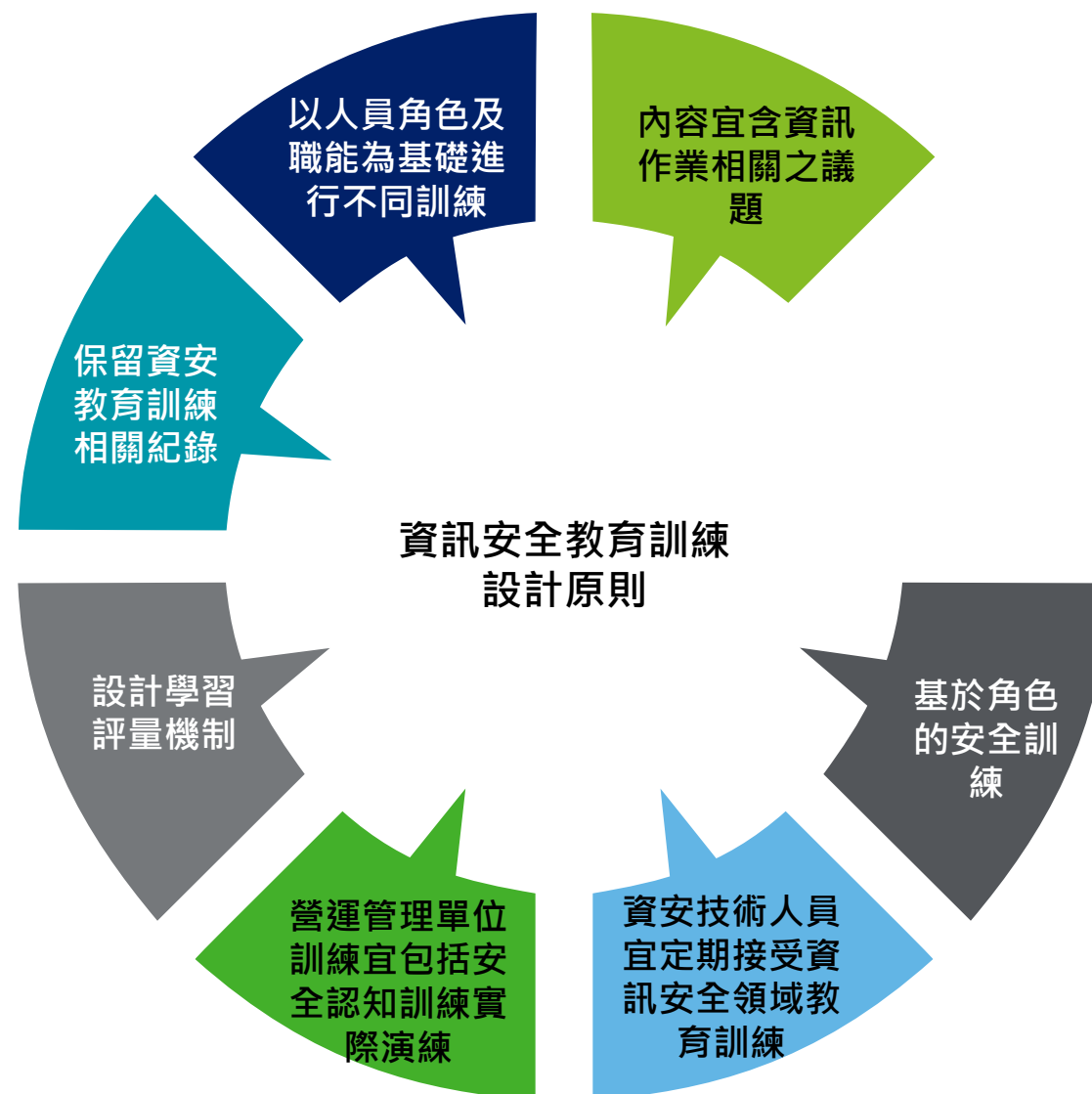
營運管理單位所有員工對於與工作上資訊安全相關之法令要求，應有所瞭解並依據相關規定辦理

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。

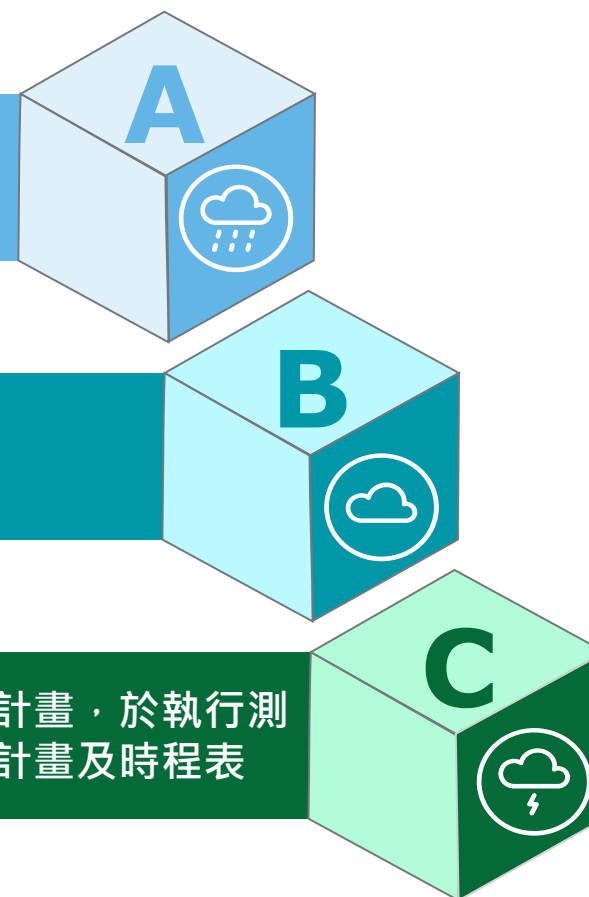
營運管理單位宜與負責相關計畫的部門  
協調營運持續計畫的制定

- 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

訂定演練模式及週期

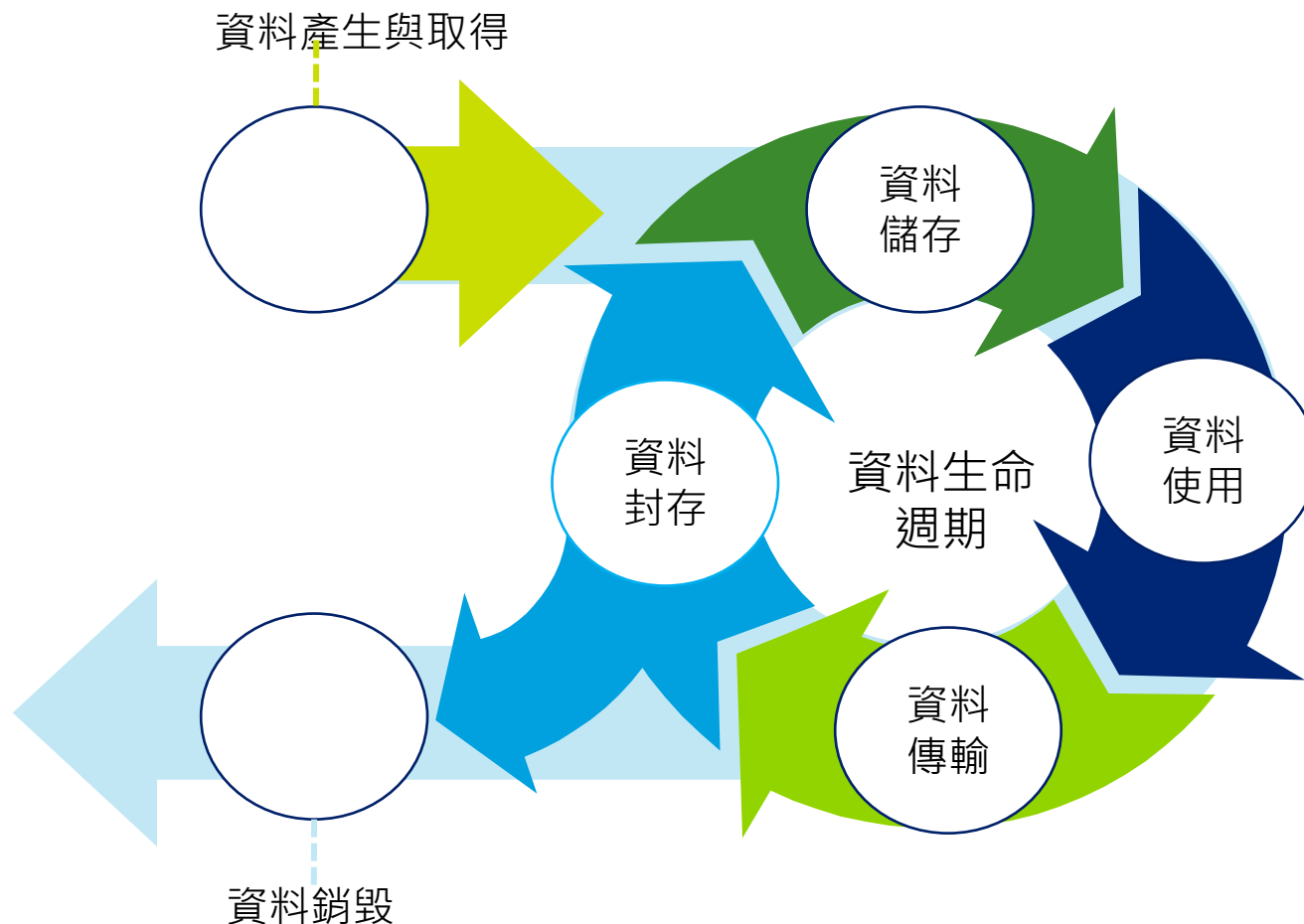
營運管理單位進行營運衝擊分析時，應判斷各項資訊資產與業務服務流程中斷時，產生對於各項業務服務流程所造成之影響及衝擊程度，據以判斷最大可容忍中斷時間(MTPD)、系統復原時間目標(RTO)以及資料復原點目標(RPO)等，並分別給予重要分級

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



# 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

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

儲存

使用

傳輸

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



## 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<br>系統管理   | 資料庫帳號及存<br>取權限管理 |
| 資料庫實體檔案<br>目錄管理 | 資料管理             |

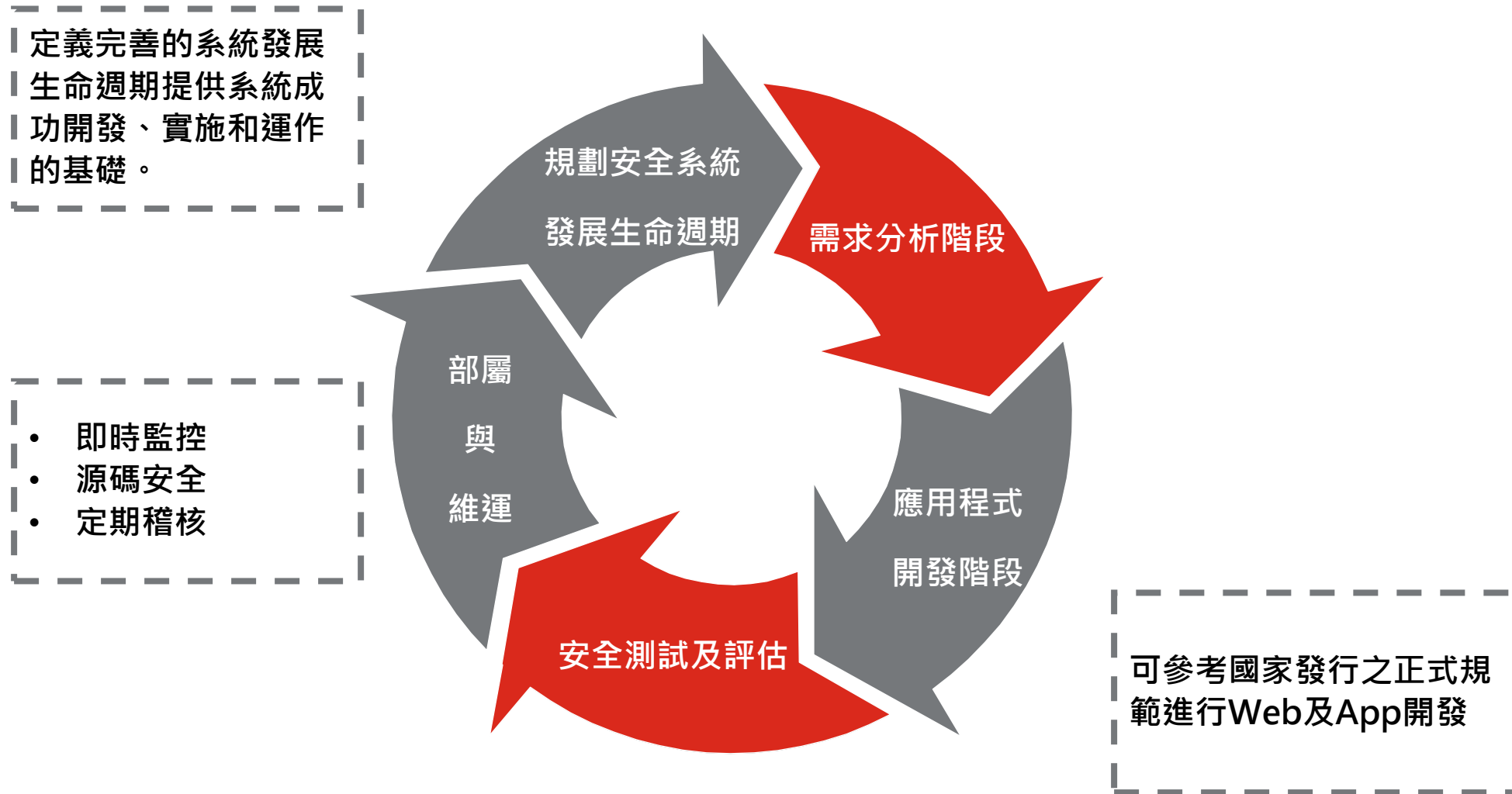
2. 資料備份作業原則如下：

- 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商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



## 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，同時包含一致的专业用語

**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

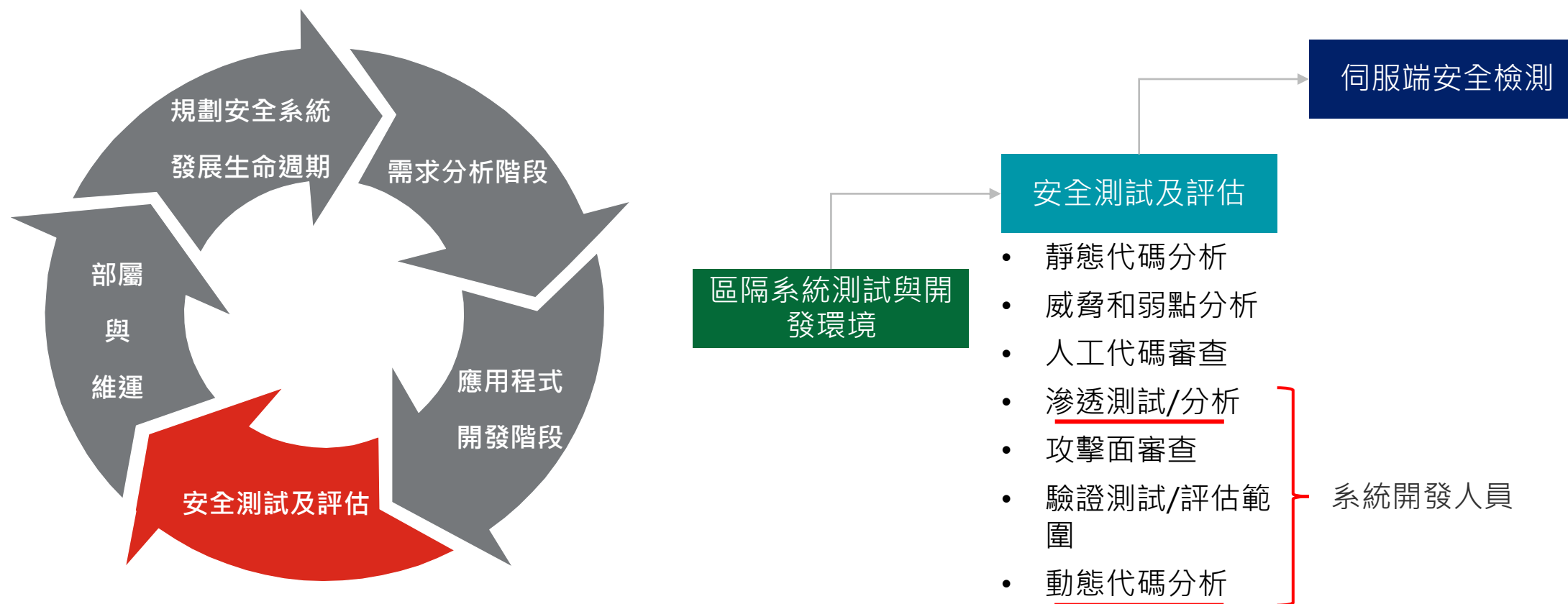
**R**

**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證

## 系統管理面 - 系統安全開發管理 3/3





## 系統管理面 - 委外廠商管理

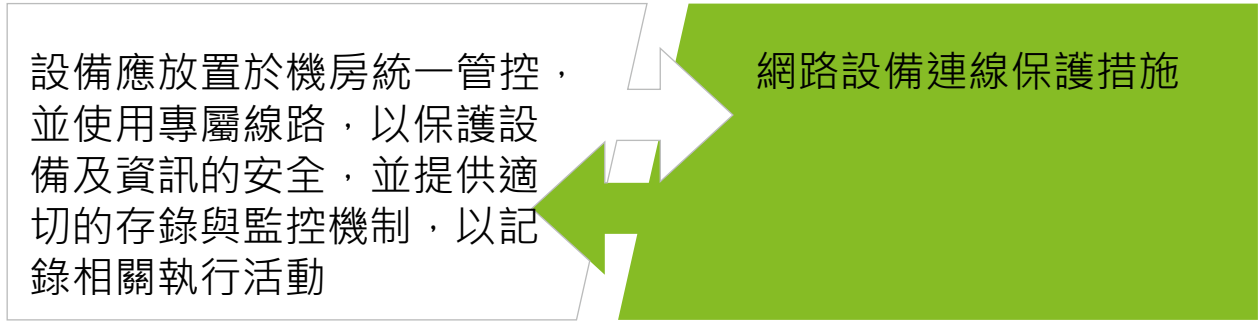


# 系統管理面 - 網路安全架構 1/3

## (1) 網路規劃與建置



## (2) 網路設備管理



## (3) 防火牆管理及入侵偵測防禦系統

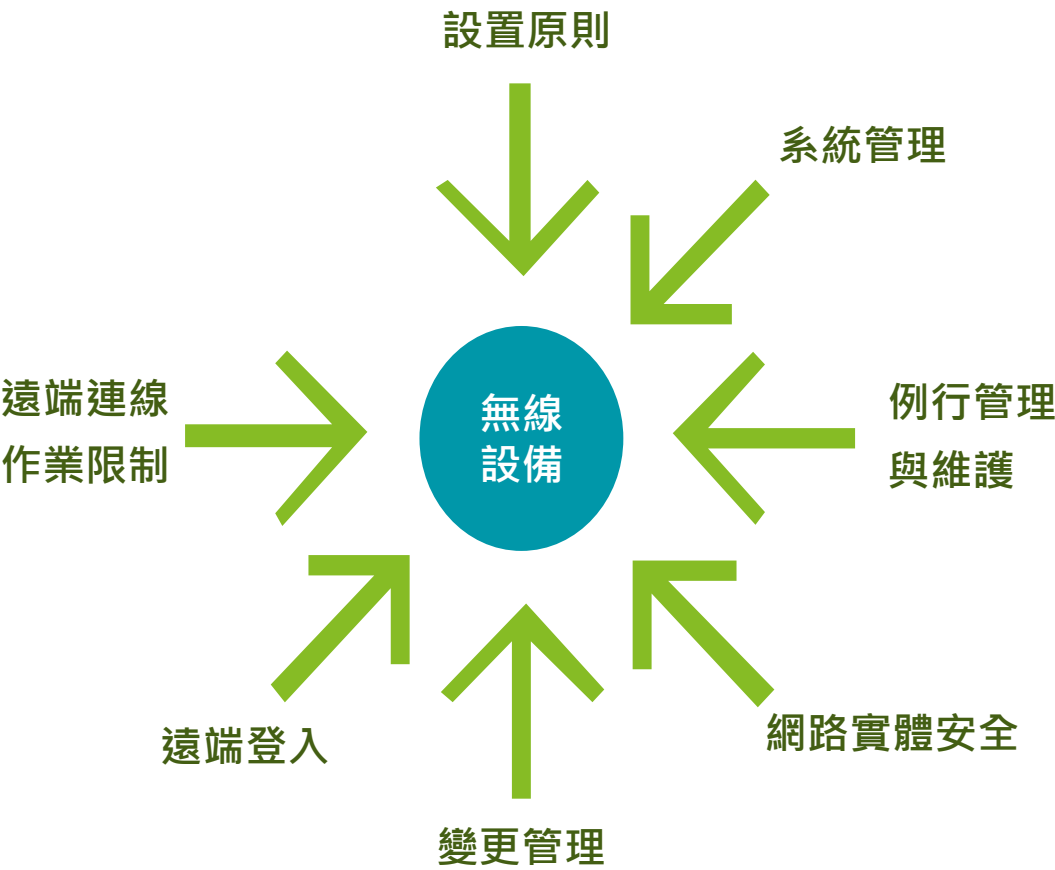


# 系統管理面 - 網路安全架構 2/3

## (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

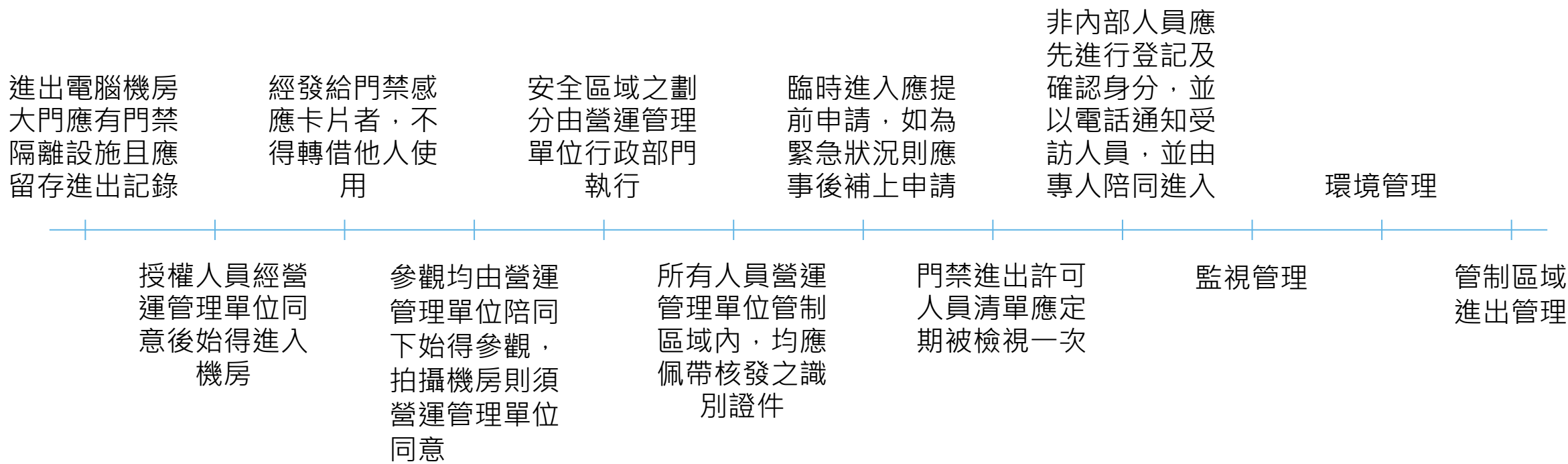
### (11)網路檔案服務(Network File Service, NFS)

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：

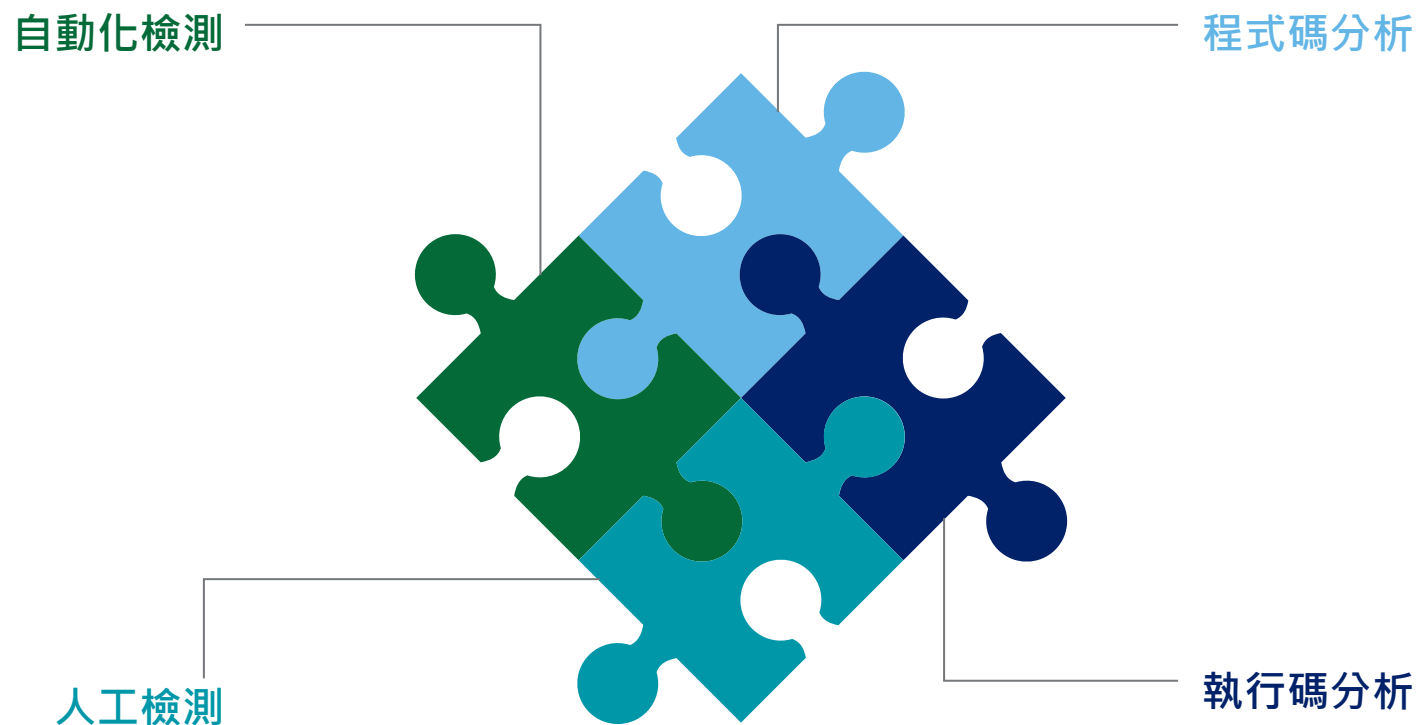
| 五大面向           | 說明  |
|----------------|---|
| 行動應用程式發布安全     | 主要適用於發布行動應用程式之相關資訊安全檢測基準，包括發布、更新與問題回報等                                    |
| 敏感性資料保護        | 主要適用於敏感性資料與個人資料保護之相關資訊安全檢測基準，包括敏感性資料蒐集、利用、儲存、傳輸、分享及刪除等                    |
| 付費資源控管安全       | 主要適用於付費資源使用及控管  |
| 身分認證、授權與連線管理安全 | 主要適用於行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

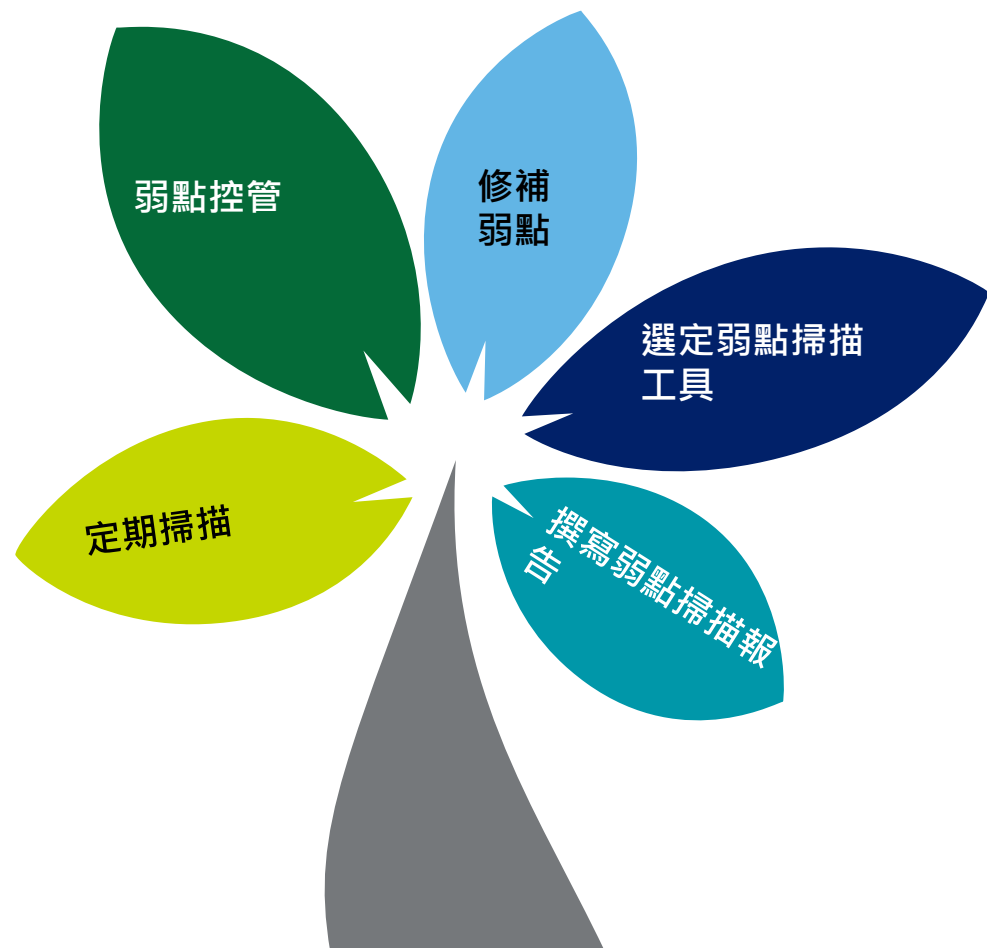
### 檢測結果與產出

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描，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

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：

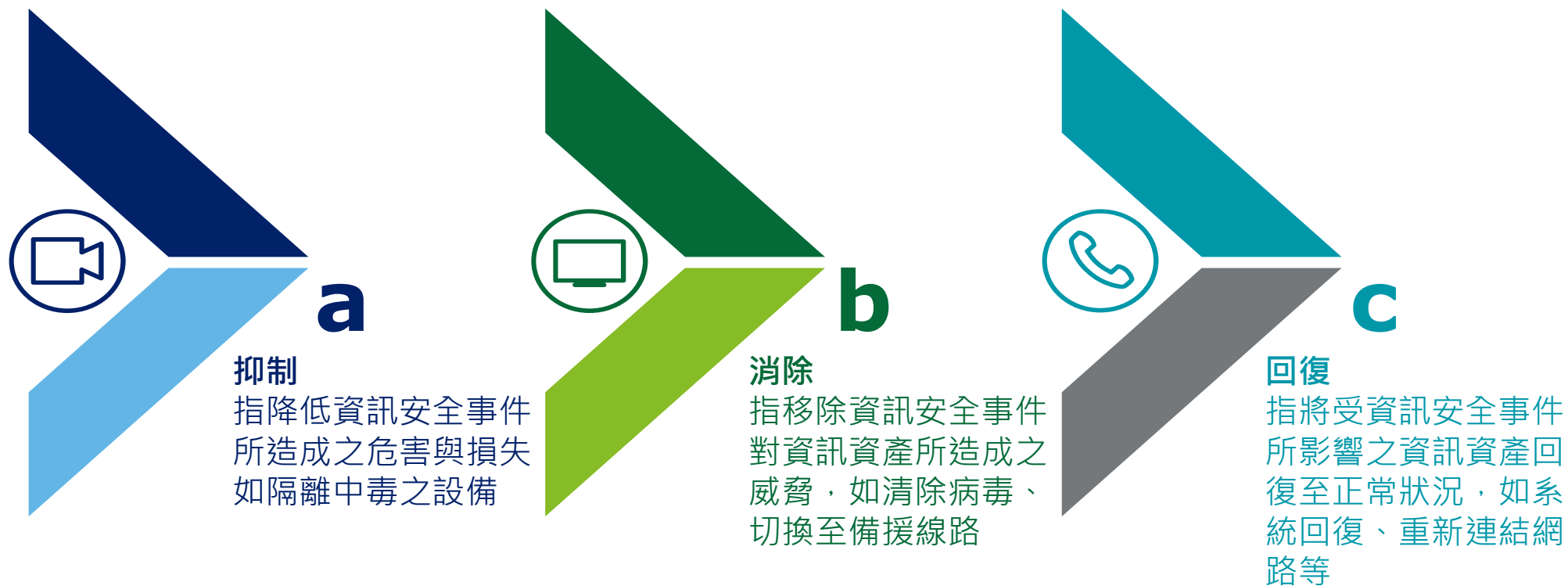
| 角色           | 權責        |
|--------------|-----------|
| 事件發生單位       | 通報        |
| 通報受理窗口       | 受理、通知相關人等 |
| 相關系統或業務負責人   | 處理、回報結果   |
| 相關系統或業務負責人主管 | 分析、追蹤     |



# 事故處理 1/4

## 資訊安全事件之處理階段

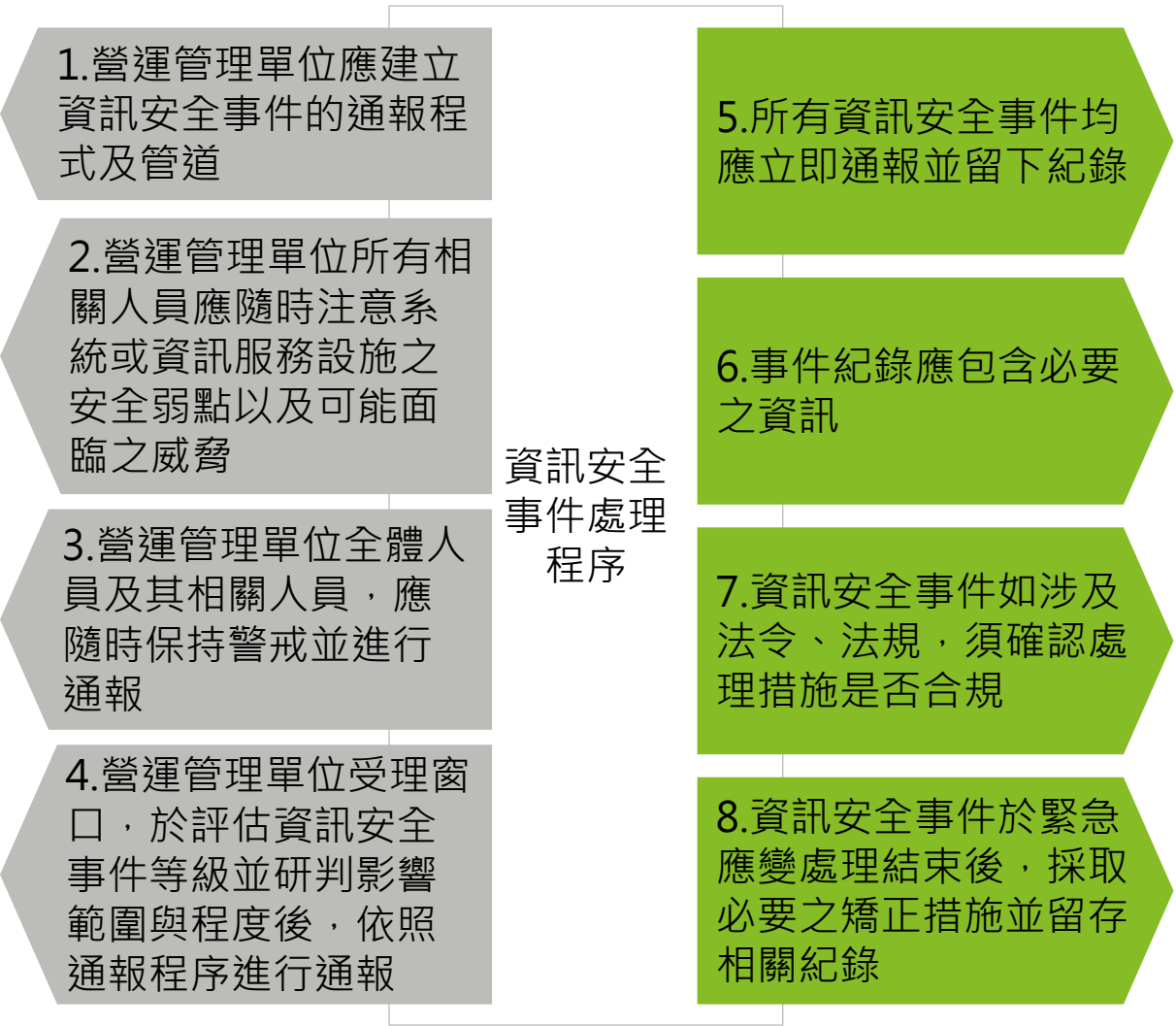
資訊安全事件之處理應包含抑制、消除及回復等三階段；處理資訊安全事件時，應辨識資訊安全事件之發生來源，並考慮根除資訊安全事件因素及回復資訊資產。





# 事故處理 2/4

## 資訊安全事件之處理程序



## 資訊安全事件處理需考慮因素



# 事故處理 3/4

## 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

### 遇到重大事件時!!

事件等級如為嚴重影響營運等級，相關權責單位應將資訊安全事件檔化紀錄後，送交系統或業務負責人填寫發生原因、矯正措施、改善期限及負責人員，簽核後留存備查。

值日生：

## (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：

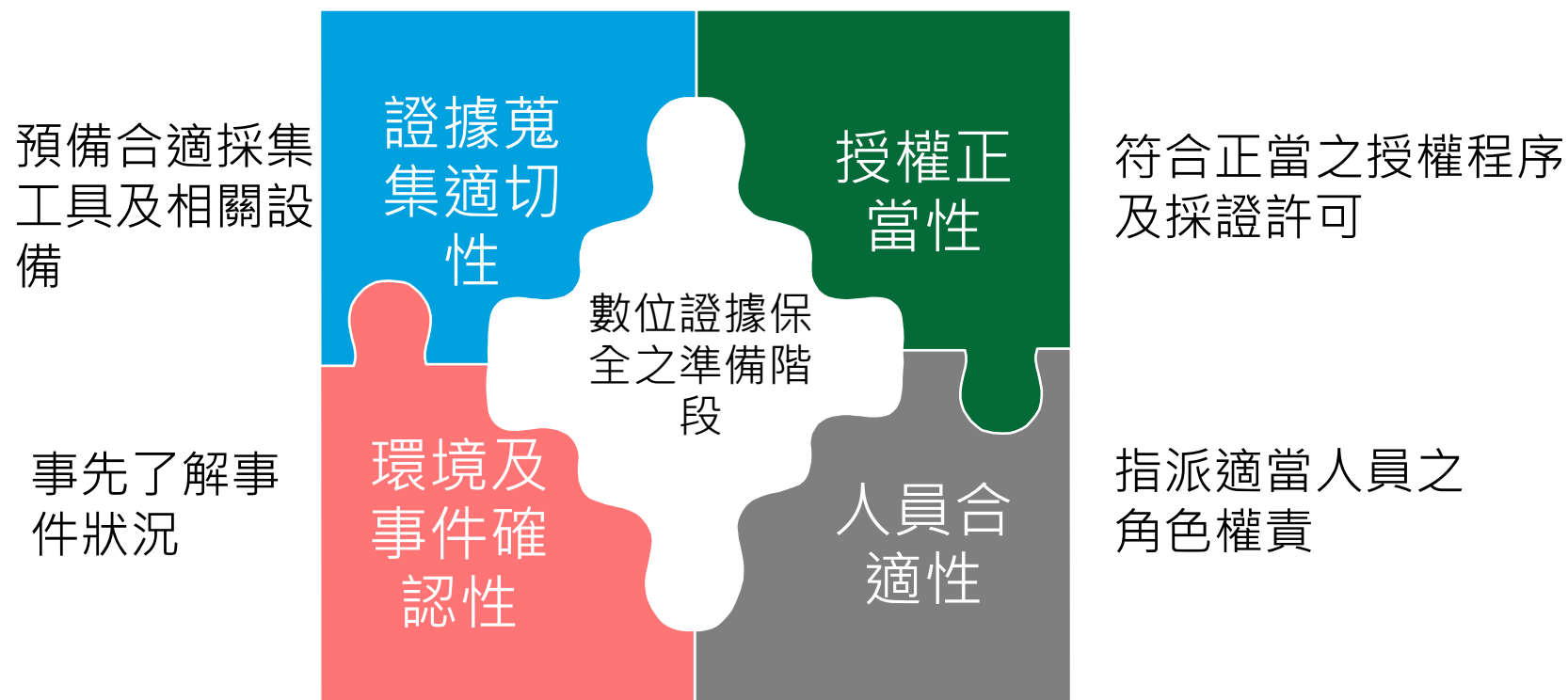
於現場狀況協助證據保全人員於證據蒐集及運送的過程中，進行過程之紀錄。

(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：



# 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，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，



## (二)資安事件發生後之改善及追蹤作業

### 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：



# 問題與討論

## 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](http://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。

本出版物係依一般性資訊編寫而成，僅供讀者參考之用。Deloitte及其會員所與關聯機構(統稱“Deloitte聯盟”)不因本出版物而被視為對任何人提供專業意見或服務。在做成任何決定或採取任何有可能影響企業財務或企業本身的行動前，請先諮詢專業顧問。對信賴本出版物而導致損失之任何人，Deloitte聯盟之任一個體均不對其損失負任何責任。

