Deloitte.
勤業眾信

CISA

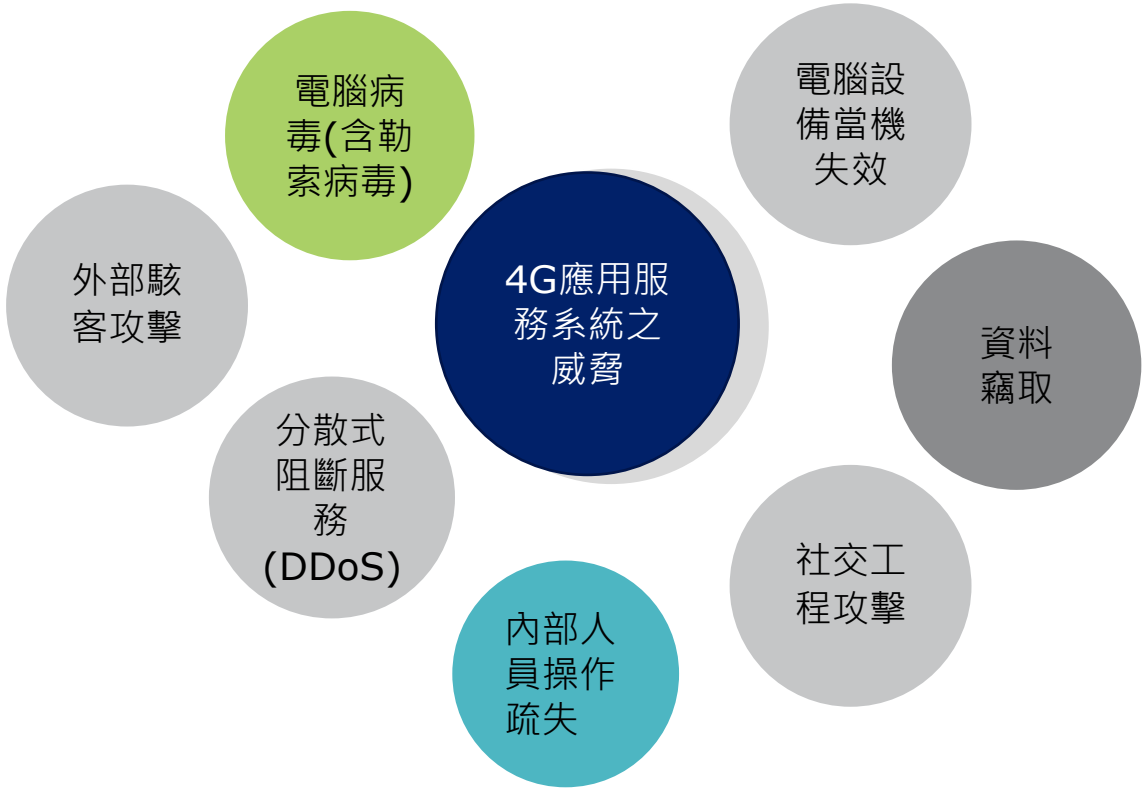
4G應用服務系統資安推動計畫成果分享
行動應用服務系統資安防護研討會
「剖析4G應用服務系統資安風險與對策」

簡報人：李民偉 顧問

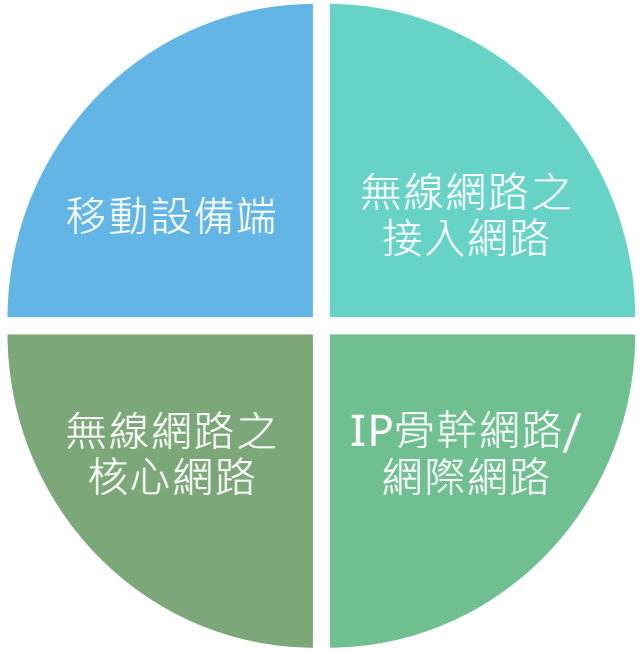
106年12月8日

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

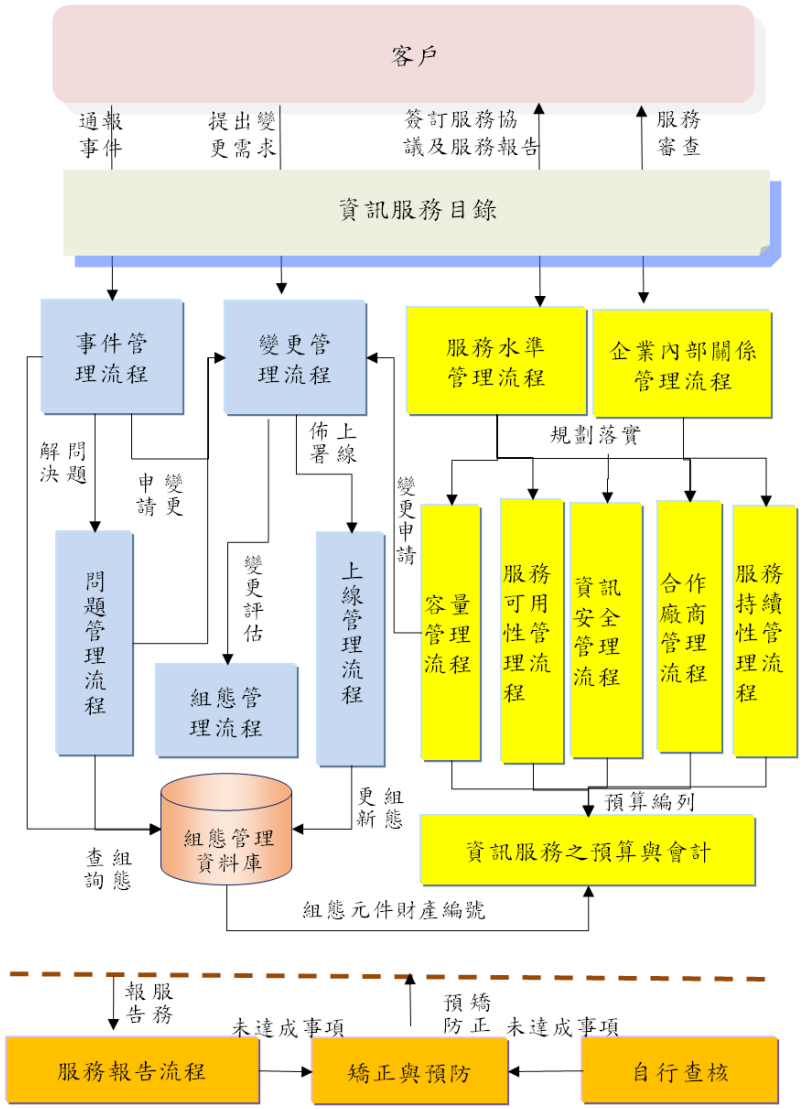
6 身分辨識之隱憂

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

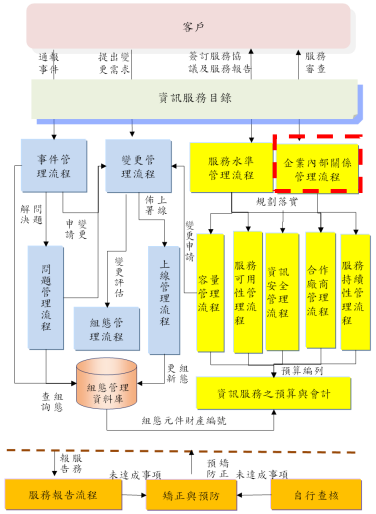
新服務或服務異動(含服務之終止)，以正式變更管理規劃

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：

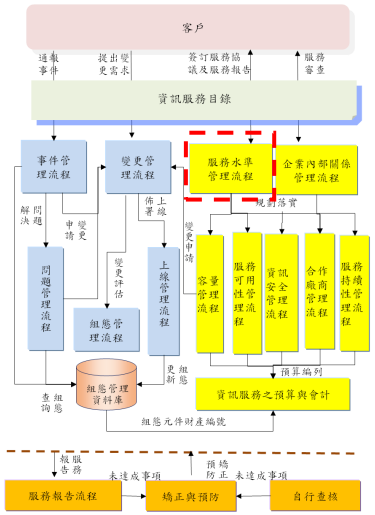
實施、操作及維護之角色與責任	對於資訊安全、資訊服務管理制度及資訊服務之影響	與利害相關團體之溝通結果
相關之時程、流程、監控方式、管理方法及工具	合約或服務水準協議修改之必要	針對新服務運作情形或預期效益，設定量化管理績效指標
新服務或服務異動完成後之驗用方法	新服務或服務異動之預算、人力需求	新服務或服務異動之技能及訓練需求

資訊服務管理建議 -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 -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。

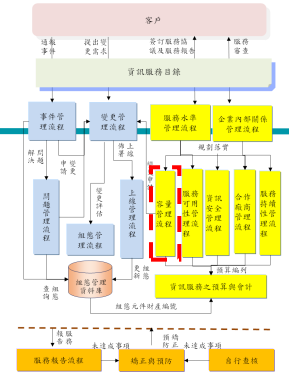
2 依據資訊服務水準協議，管理資訊服務流程，並確保資訊服務達成需求。

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 -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

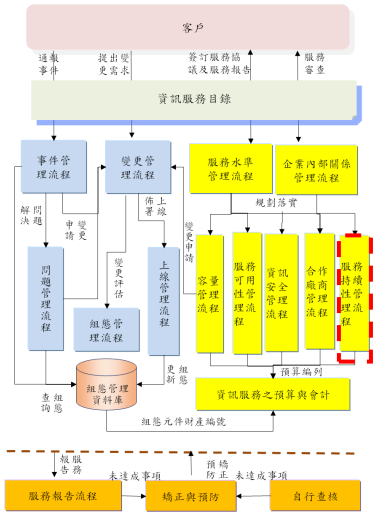
B 鑑別升級時所需時程、臨界值與成本

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

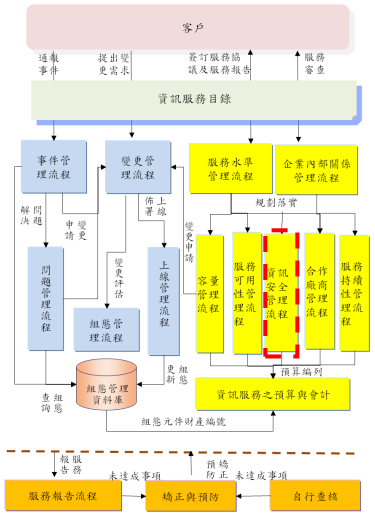
2 宜考量其資訊服務水準要求

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



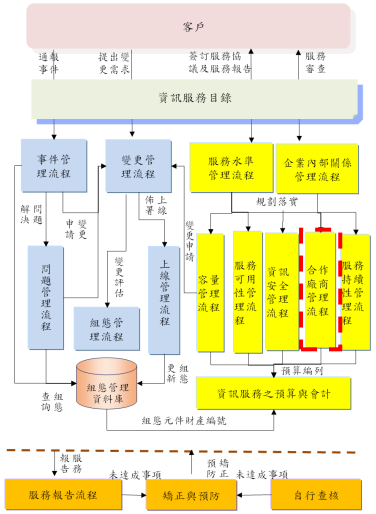
1 宜依資訊安全管理制度，管理各項資訊服務所涵蓋之資訊安全議題

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

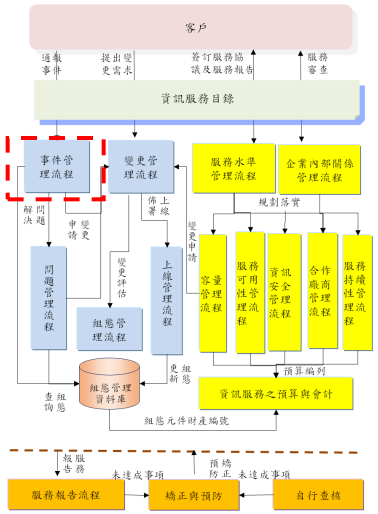
4 宜有適當機制以量化並監控資訊安全事件與故障之類型、數量及衝擊

資訊服務管理建議 -合作廠商管理



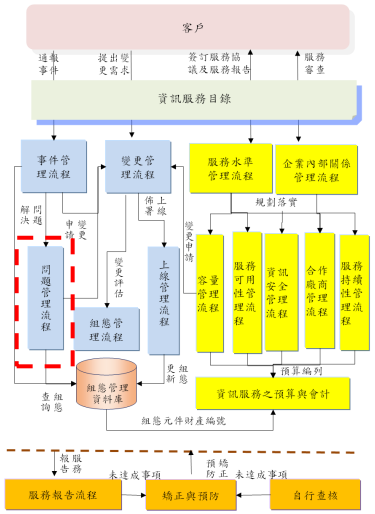
1. 宜有書面化之管理流程，以維持高品質之資訊服務
2. 宜有效協調使其合約協議與服務水準協議一致
3. 宜將其與分包廠商之角色及關係書面化；其對分包廠商履約之部分，應負完全責任
4. 針對資訊服務合作廠商之契約，宜定期進行一次審查，確保契約與本行需求間之適用性
5. 宜採用適當程序處理其服務之正常結束及提前結束
6. 宜依據其服務等級目標進行監測並審查績效

資訊服務管理建議 -事件管理



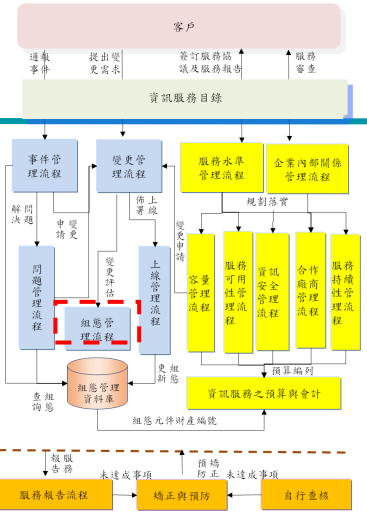
1. 宜記錄所有事件，並透過有效之管理程序，儘速將資訊服務回復至正常運作狀態
2. 宜確認程序已定義事件記錄、優先順序、企業衝擊、分類、更新、升級、事件解決及事件結束之流程活動
3. 宜回覆客戶已通報事件或請求之進度；若可能無法達到服務水準時，應通知客戶並採取適當行動
4. 宜確保所有涉及事件管理之同仁可存取相關資訊，包括：已知錯誤、問題解決方案及組態元件資料庫
5. 重大事件宜根據已制定之流程進行分類與管理

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



宜在資訊服務重大異動前執行組態元件之基準點(Baseline)

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

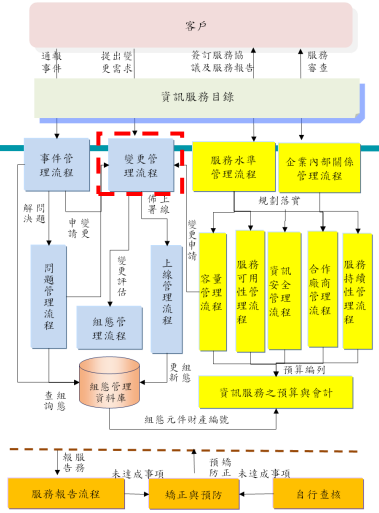
宜將組態元件之實體置於管制環境中

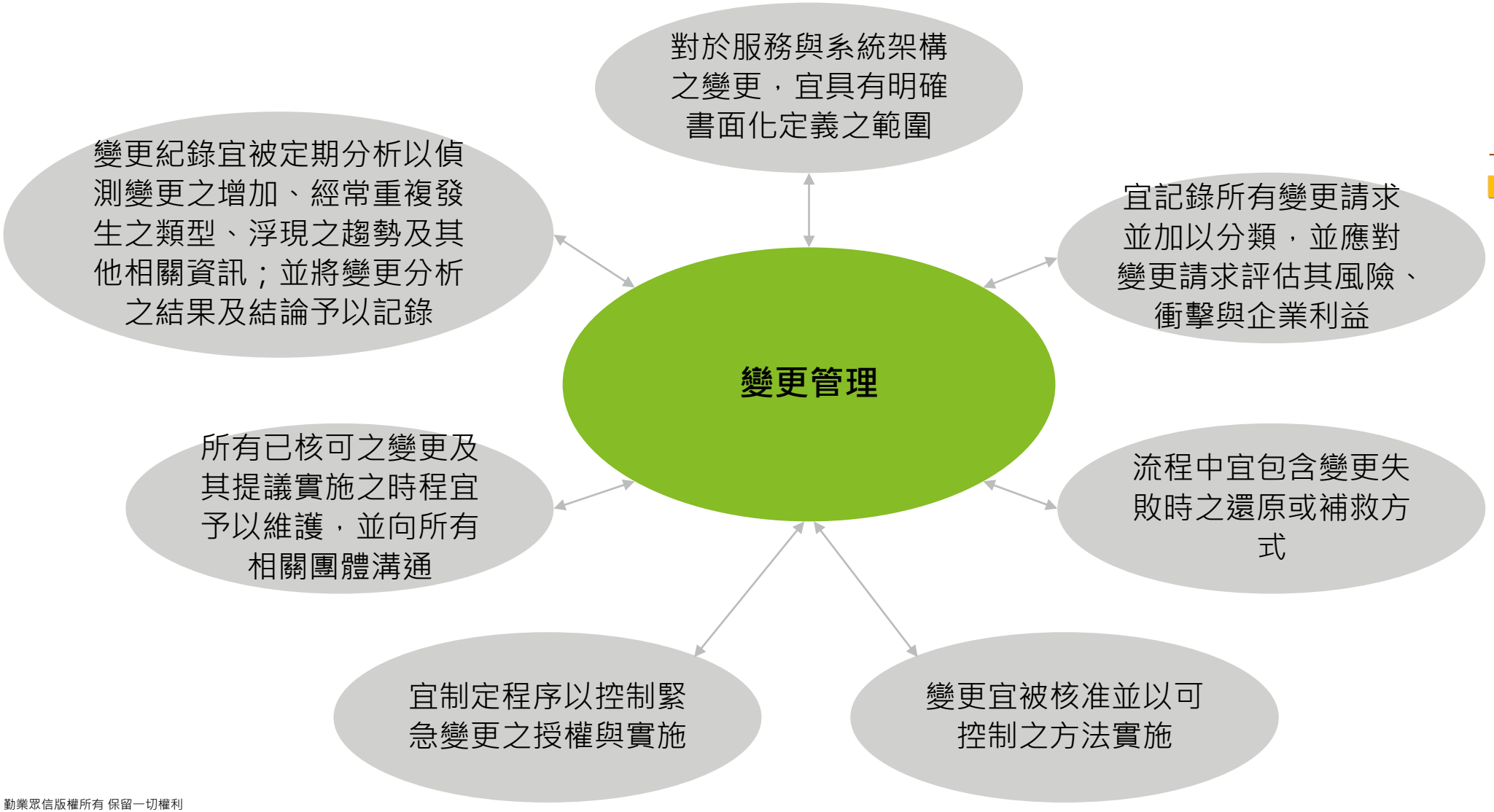
宜提供變更管理流程對資訊服務與基礎架構之變更衝擊資訊。在適當情況下，宜可追蹤及查核組態元件之變更

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





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

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。