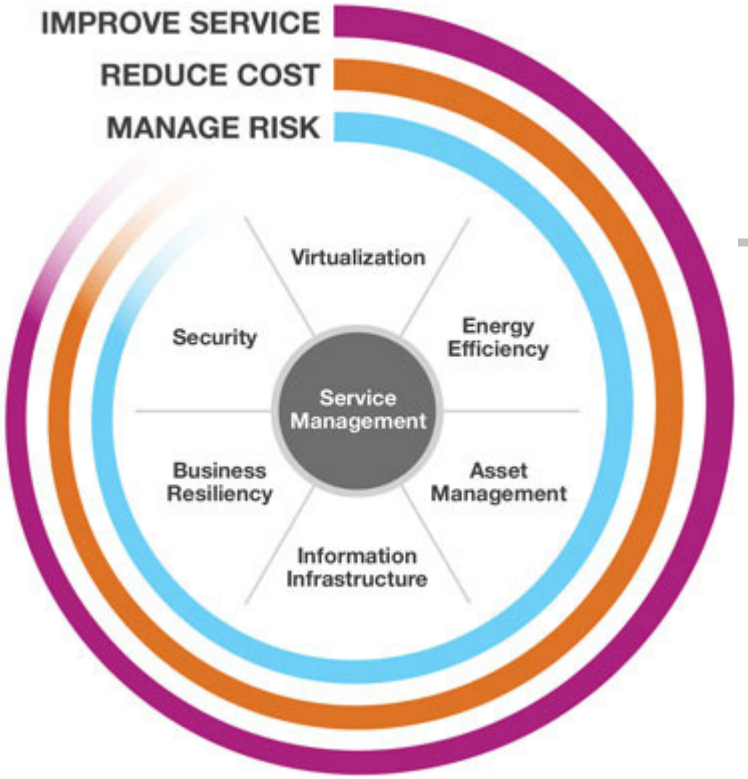
Colin Yao – Solution Design Team, GTS
2010/06

妙計4：節點資料洩漏保管策略分析

端點及移動媒體資料
洩漏保護策略分享



A Smarter Planet

SmarterSecurity&Resilience

Smarter Security and Resilience

An intelligent approach to risk management reveals opportunities for innovation

Agenda：

- **簡單回顧：節點資料保護概念**
- 節點資料保護技術核心策略
- 導入資料保護方案前之關鍵問題
- 總結

個資洩漏的相關統計資訊及研究報告：主要事件來源

個資洩漏事件，最主要可粗分為下列幾種事件來源：

節點防護不足

- 筆記型電腦或個人電腦的遺失或被竊取
- 遺失或被竊取的儲存媒體

未有整體防禦架構

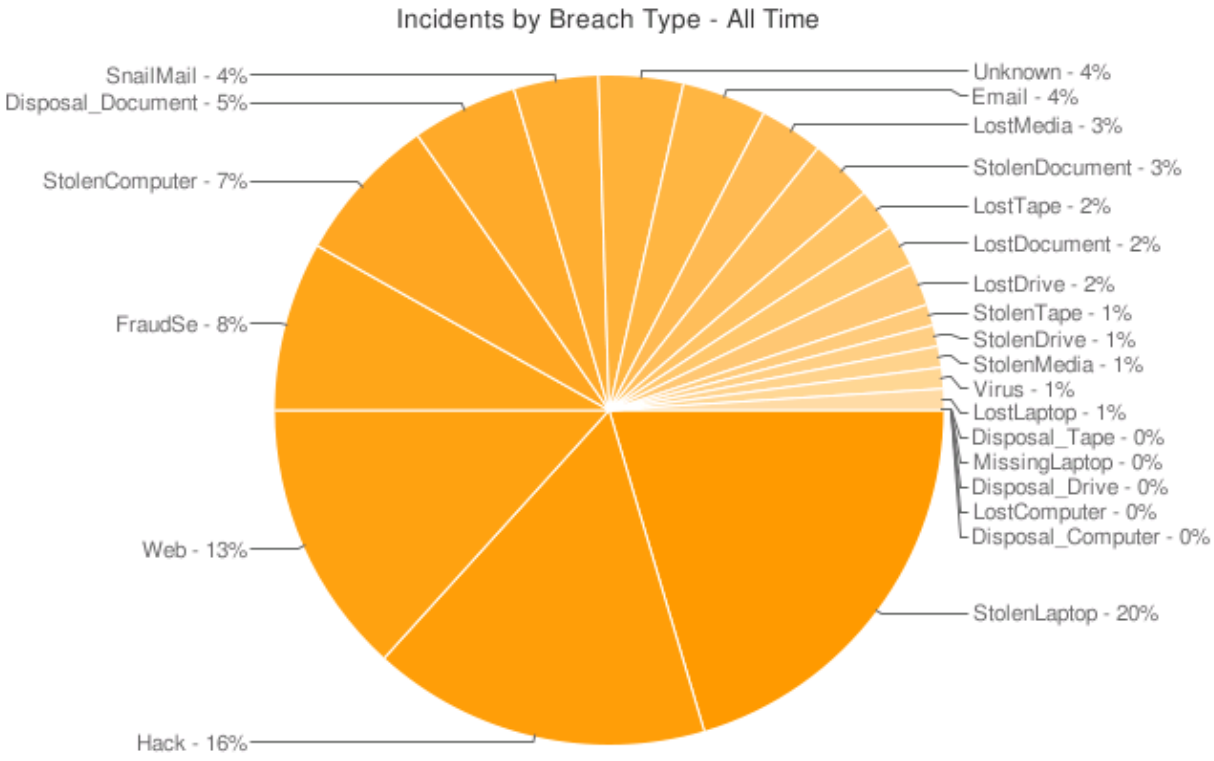
- 外部駭客攻陷Web應用程式或資料庫，抓取個資

缺乏資料運用政策

- 惡意的高權限內部系統管理者或維護廠商

未具備資料外洩處理分析能力

- 惡意的內部使用者



這些於節點發生之個資或資料保護相關問題極可能發生在貴公司

- 惡意員工進行個資或營運秘密備份，於在職時或離職後洩漏給競爭廠商，成立新公司，或出售以得到個人的利益
- 企業發生重大個資或營運秘密洩漏情事，但無法得到有利之稽核證據，或具備有效的管控機制
- 惡意高技術員工利用各種管道突破現有之資料管控機制。
- 員工不知道他們有意或無意之行為已違背企業個資暨資料保護政策而持續進行

這些於節點發生之個資或資料保護相關問題極可能發生在貴公司

- 紀錄個資或重要營業秘密之資訊設備或媒體遺失或失竊
- 紀錄個資或重要營業秘密之媒體銷毀時未能完全清除資料
- 須提供維護廠商或內部員工遠端接取核心系統，但難以保證個資或重要營業秘密不會由此途徑洩漏

節點資料保護核心需求

節點資料保護技術核心需求：

1. 企業可稽核使用者於端點上之資料使用行為
2. 企業可限制使用者於端點上之資料保護政策違反行為
3. 記錄重要個資或營運秘密的設備或移動媒體，沒有經過適當的認證及授權，他人無法讀取內部的資訊

Smarter Security and Resilience

An intelligent approach to risk management reveals opportunities for innovation

Agenda：

- 簡單回顧：節點資料保護概念
- **節點資料保護技術核心策略**
- 導入資料保護方案前之關鍵問題
- 總結

節點資料洩漏保護技術之三大核心策略

- 節點資料保護技術核心策略

① **策略一：**

利用雲端桌面技術，讓使用者無法直接接觸資料

② **策略二：**

於使用者端點設備進行機敏資料之使用稽核、政策管控、與加密保護

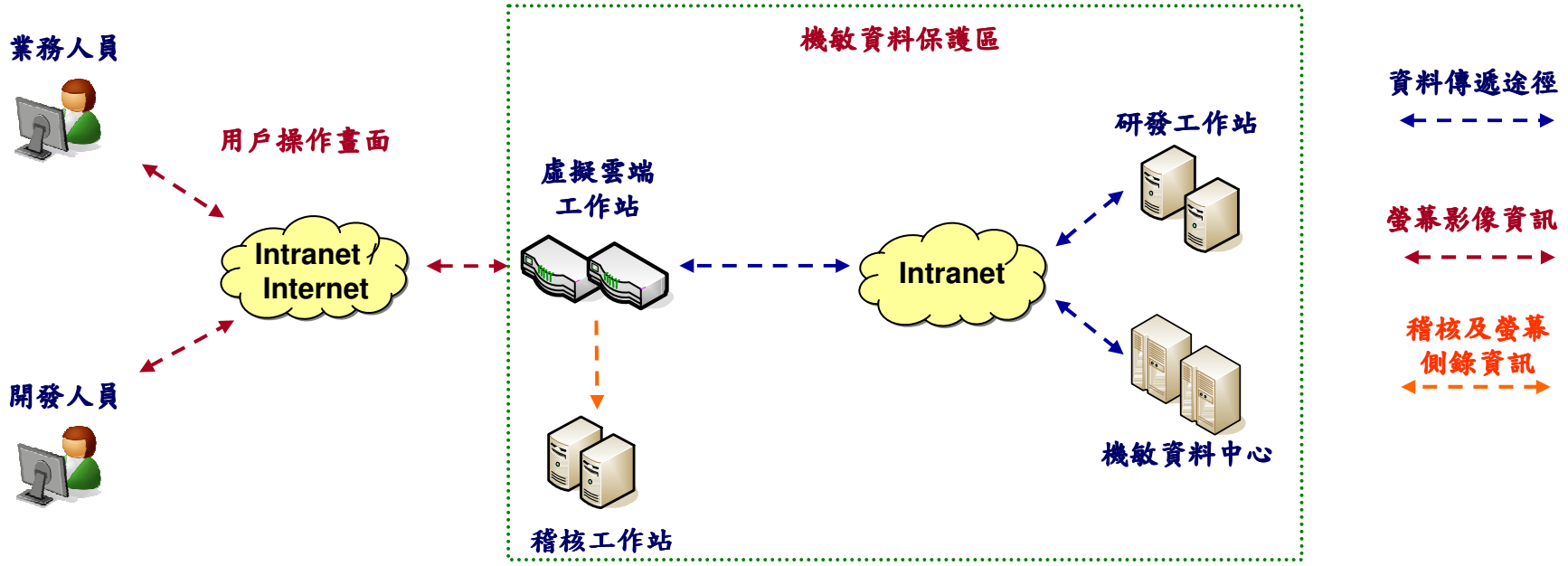
③ **策略三：**

於中心儲存媒體端進行資料加密，保護儲存媒體免於遺失或被竊取之風險

節點資料保護技術核心策略一：
雲端桌面保護機制

資料保護技術核心策略一：

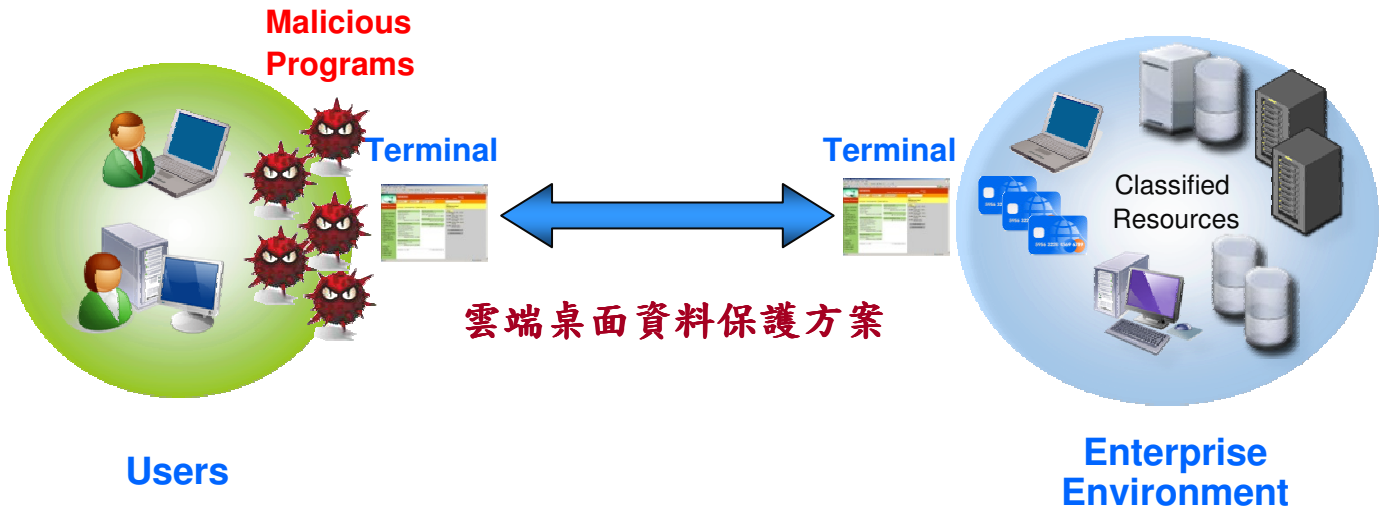
利用雲端桌面技術，讓使用者無法直接接觸資料



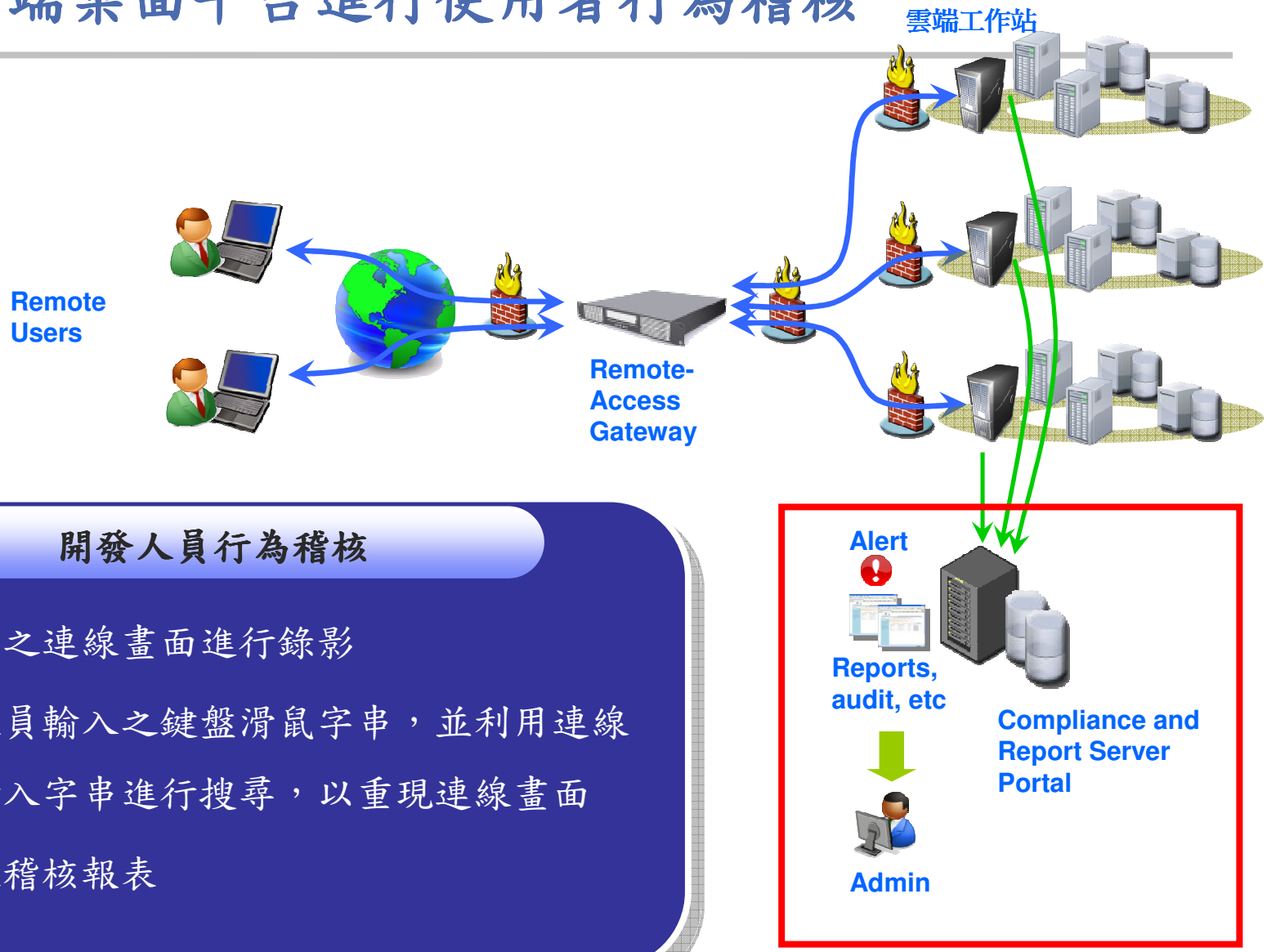
使用者僅看到畫面，不直接接觸實體資料

雲端桌面資料保護方案

- 僅允許螢幕影像傳輸而非實際資料檔案傳輸，避免機敏資料洩漏
- 阻擋使用者進行檔案複製、下載
- 使用者本機不儲存機敏資料



可利用雲端桌面平台進行使用者行為稽核



開發人員行為稽核

- 可將人員之連線畫面進行錄影
- 可紀錄人員輸入之鍵盤滑鼠字串，並利用連線資訊及輸入字串進行搜尋，以重現連線畫面
- 人員連線稽核報表

雲端桌面保護機制可滿足節點資料保護核心需求

資料保護需求	雲端桌面保護機制
企業可稽核使用者於 端點上之資料使用行為	支援
企業可限制使用者於 端點上之資料保護政策違反行為	強大
記錄重要個資或營運秘密的設備或移動媒體，沒有經過適當的認證及授權，他人無法讀取內部的資訊	強大
適合對象	適合各種企業，尤其是主要位於LAN網路內之員工
不適合對象	長期在外之主管與業務人員
方案最重要風險	端點架構改變、如何滿足不同員工之資訊使用需求
其他優點	強大的端點管理、節能

節點資料保護技術核心策略二：
端點設備資料保護機制

IBM

資料保護技術核心策略二：

於使用者端點設備進行機敏資料之使用稽核、政策管控、與加密保護

Host IDP&FW

Patch Management

Data / HD Encryption

Virus/Malware Protection

Endpoint Data Loss Protection

節點資料保護技術核心策略二：端點設備資料保護機制

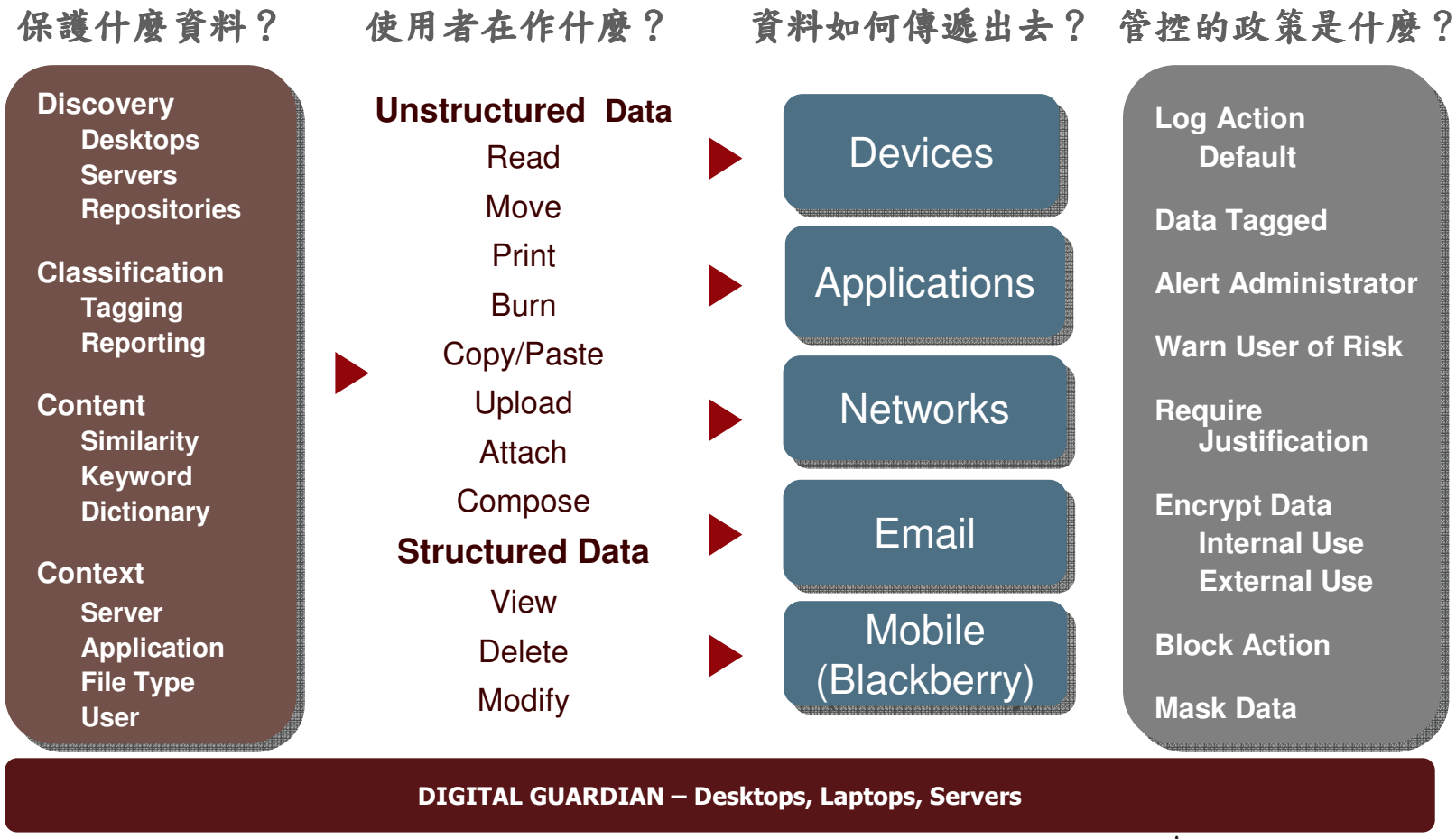
Data / HD Encryption

- **硬碟加密機制之主要資料保護功能**
  - 針對移動式的用戶端系統進行全硬碟加密以降低設備遺失導致的資料外洩風險
  - 使用者無法自行將硬碟攜出安裝至另一台電腦進行讀取

端點資料洩漏保護
- 進行端點機敏資料保護與行為稽核

Endpoint Data Loss Protection

- **端點DLP機制之主要資料保護功能：**追蹤控制對資料之存取行為，主動阻擋非授權行為，保留完整之資料使用過程



端點資料洩漏保護機制可滿足節點資料保護核心需求

資料保護需求	雲端桌面保護機制
企業可稽核使用者於 端點上之資料使用行為	強大
企業可限制使用者於 端點上之資料保護政策違反行為	強大
記錄重要個資或營運秘密的設備或移動媒體，沒有經過適當的認證及授權，他人無法讀取內部的資訊	強大
適合對象	適合各種企業，尤其是在外之主管與業務人員
不適合對象	無
方案最重要風險	於同一端點上佈建多個方案之衝突與管理問題
其他優點	無

節點資料保護技術核心策略三：儲存媒體保護機制

資料保護技術核心策略三：

於中心儲存媒體端進行資料加密，保護儲存媒體免於遺失或被竊取之風險

節點資料保護技術核心策略三：儲存媒體保護機制

- **儲存媒體保護機制之主要資料保護功能**
  - 資料中心的儲存媒體，含硬碟與磁帶，仍為移動性媒體，可能在移動或儲存過程中遺失，或於廢棄時未完全將資料移除
  - 藉由加密技術，保護紀錄企業最核心個資或營運資訊的媒體，即使於運送或棄置時遺失或被竊取，仍可確保機敏資料不會被讀取

Smarter Security and Resilience

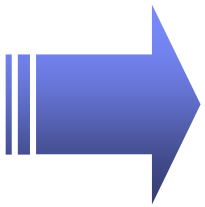
An intelligent approach to risk management reveals opportunities for innovation

Agenda：

- 簡單回顧：節點資料保護概念
- 節點資料保護技術核心策略
- **導入資料保護方案前之關鍵問題**
- 總結

企業導入資料保護方案前之關鍵問題

企業導入資料保護方案前的關鍵問題



1. 企業高階主管對於營運秘密及個資之保護需求是否已了解並建立共識？
2. 企業是否已有針對資料分級、管理與保護的政策？這些政策是否完整涵蓋公司需保護的關鍵資訊，如研發、成本、製程等？
3. 公司是否明確定義營運秘密暨個資分級及管理政策，並告知員工知曉且落實執行？
4. 企業的營運秘密或包含個資的資訊在哪裡？誰會接觸到？會有哪些潛在的洩漏途徑？
5. 企業選擇進行營運秘密或個資保護之策略為何？是採取直接阻擋之方式或利用稽核紀錄的方式？
6. 企業的基礎資訊安全架構是否已經完善，可抵禦大部分的外部駭客攻擊？

可利用顧問服務進行各資料保護關鍵問題先期評估

營運秘密暨個資保護關鍵問題

- **R.1** 企業高階主管對於營運秘密及個資之保護需求是否已了解並建立共識？
- **R.2** 企業是否已有針對資料分級、管理與保護的政策？
- **R.3** 公司是否明確定義營運秘密暨個人資料分級及管理政策，並告知員工知曉且落實執行？
- **R.4** 企業的營運秘密或包含個資的資訊在哪裡？誰會接觸到？會有哪些潛在的洩漏途徑？
- **R.5** 企業選擇進行營運秘密保護之策略為何？是採取直接阻擋之方式或利用稽核紀錄的方式？
- **R.6** 企業的基礎資訊安全架構是否已經完善，可抵禦大部分的外部駭客攻擊？

營運秘密暨個資保護顧問服務

- 高階主管資料保護教育訓練
- 資料文件分級分類研討
- 資料保護現況訪查及風險分析
- 高風險流程評估、選擇、及資料流分析
- 企業個資保護政策制定暨改善藍圖建議

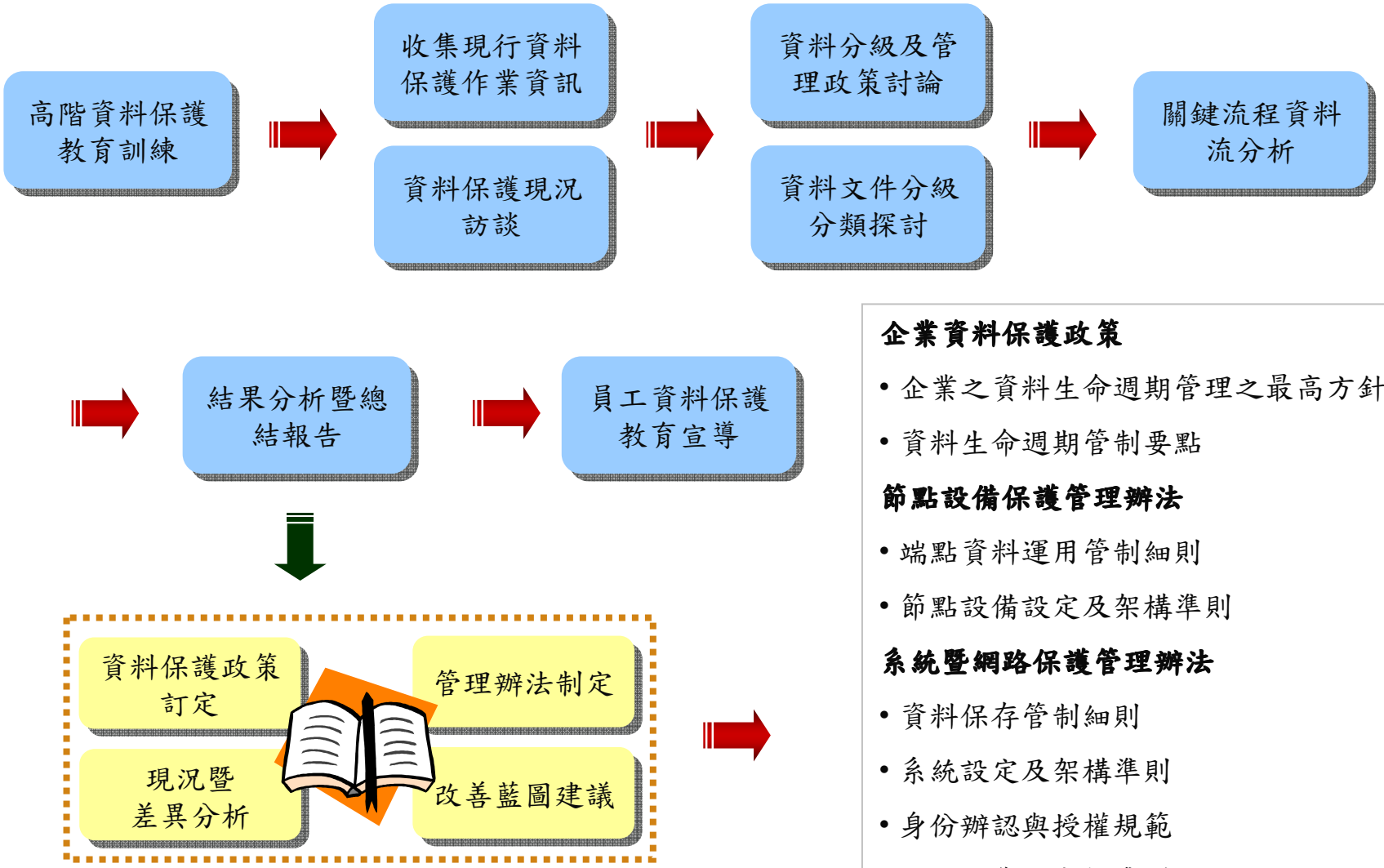
營運秘密暨個資保護解決方案

- 各種營運秘密暨個資保護機制

資訊安全現況評估暨分析顧問服務

- 資安現況分析
- 資安架構分析

建議之個資暨資料保護顧問服務流程與項目



企業資料保護政策

- 企業之資料生命週期管理之最高方針及基準
- 資料生命週期管制要點

節點設備保護管理辦法

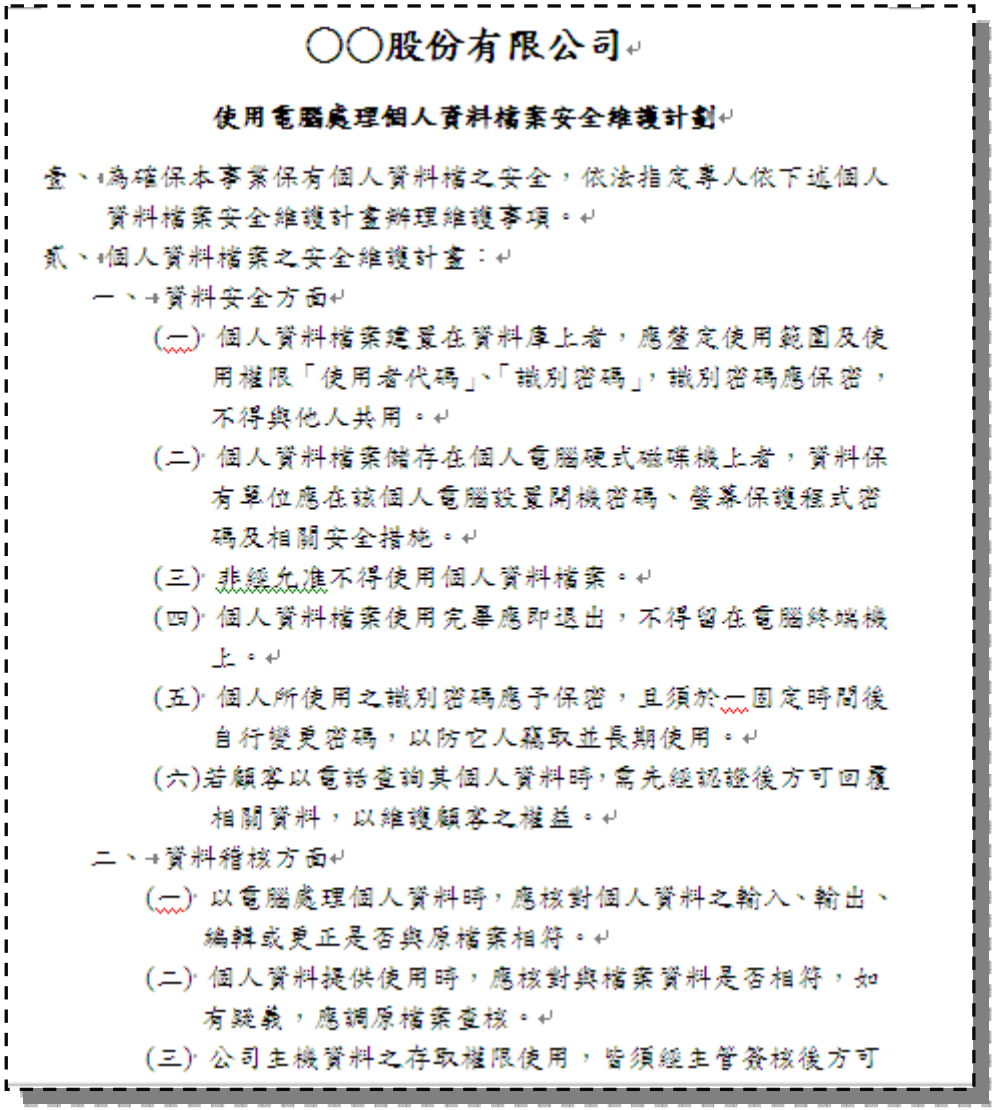
- 端點資料運用管制細則
- 節點設備設定及架構準則

系統暨網路保護管理辦法

- 資料保存管制細則
- 系統設定及架構準則
- 身份辨認與授權規範
- 日誌收集及分析準則

協助訂定企業個人資料的保護政策暨安全維護計劃

- 重點涵蓋：
  - 個人資料安全
  - 個人資料稽核
  - 相關設備管理
  - 其他安全維護事項



○○股份有限公司

使用電腦處理個人資料檔案安全維護計劃

壹、為確保本事業保有個人資料檔之安全，依法指定專人依下述個人資料檔案安全維護計畫辦理維護事項。

貳、個人資料檔案之安全維護計畫：

一、資料安全方面

(一) 個人資料檔案建置在資料庫上者，應整定使用範圍及使用權限「使用者代碼」、「識別密碼」，識別密碼應保密，不得與他人共用。

(二) 個人資料檔案儲存在個人電腦硬式磁碟機上者，資料保有單位應在該個人電腦設置開機密碼、螢幕保護程式密碼及相關安全措施。

(三) 非經允准不得使用個人資料檔案。

(四) 個人資料檔案使用完畢應即退出，不得留在電腦終端機上。

(五) 個人所使用之識別密碼應予保密，且須於一固定時間後自行變更密碼，以防它人竊取並長期使用。

(六)若顧客以電話查詢其個人資料時，需先經認證後方可回覆相關資料，以維護顧客之權益。

二、資料稽核方面

(一) 以電腦處理個人資料時，應核對個人資料之輸入、輸出、編輯或更正是否與原檔案相符。

(二) 個人資料提供使用時，應核對與檔案資料是否相符，如有疑義，應調原檔案查核。

(三) 公司主機資料之存取權限使用，皆須經主管簽核後方可

資料/文件分類定義

	A 級	B 級	C 級	D 級
研發	• 研發圖面 • 研發中之BOM • 客戶提供或要求保密之研發資料			
業務		• 廠商主檔 • 產品售價 • 合約 • 報關資訊	• 訂單資訊 • 發票資訊 • 交易紀錄 • 銷售預測	• 產品目錄
製造	• 製造成本 • 採購成本	• 製造圖面 • 量產後之BOM	• 庫存資訊 • 貨品運送狀態 • 生產預測 • 不良品資訊	

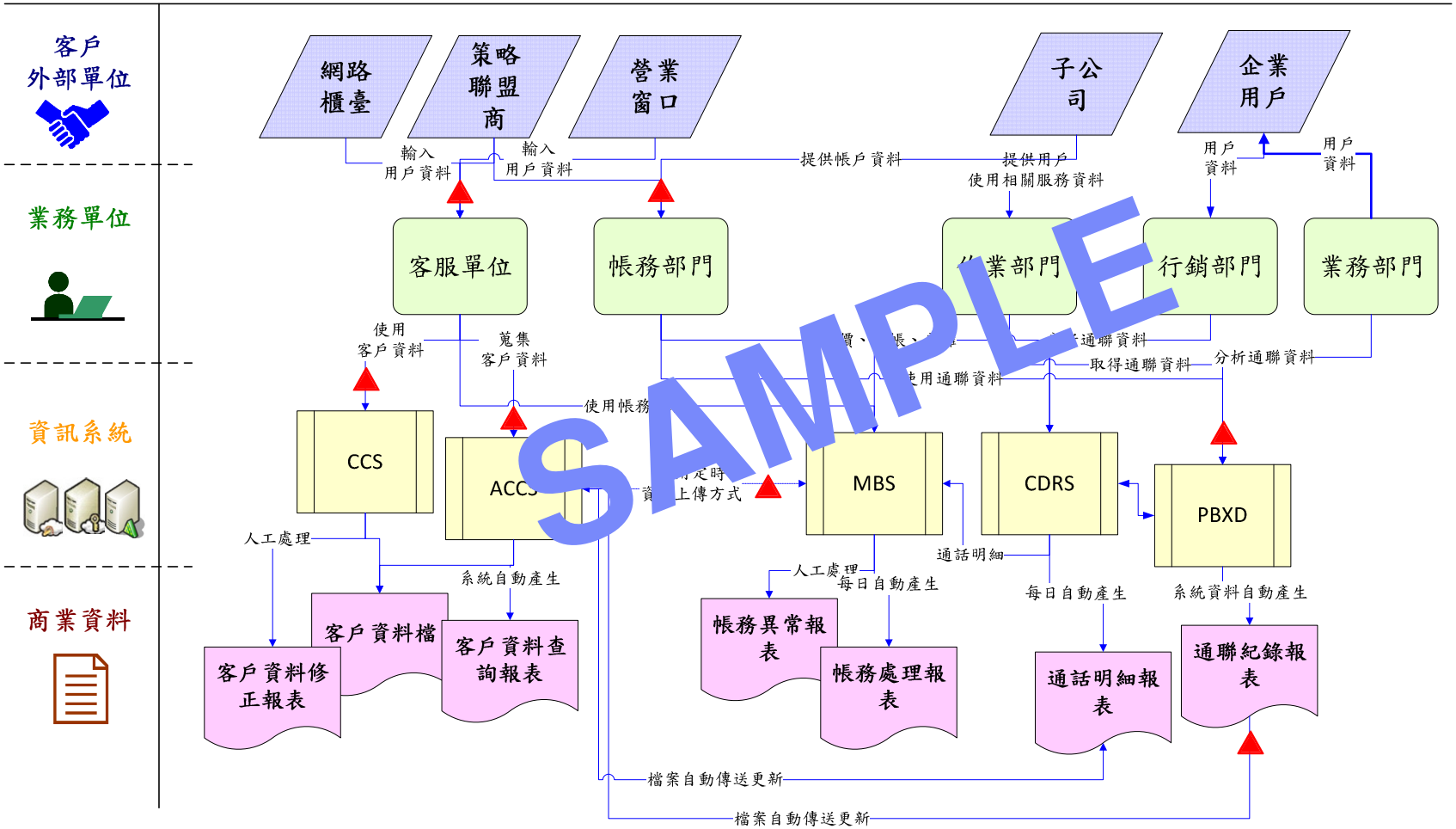
資料分級分類使用原則

項目	內/外	管道	A	B	C	D
檔案			需加密*，命名只能用代號	需加密	No limitation	No limitation
分發			需建立使用者清單，強制限制存取人員 Read Only/No print	Need to Know	Need to Know	Need to Know
傳遞	Internal	By email	需使用加密郵件功能	一般郵件	一般郵件	一般郵件
		Share folder	Not Allowed	目錄需有權限控管	目錄需有權限控管	No limitation
	External	By email	Not Allowed (Exception must use PDF only)	附檔要加密，不可寄個人信箱	一般郵件，不可寄個人信箱	一般郵件
		其他公司核准的管道	Not Allowed	附檔要加密	No limitation	No limitation

隱私資訊流評估範例

某電信單位商業作業流程範例

IBM Line of Visibility Engineering Methodology (LoVEM Chart)



Smarter Security and Resilience

An intelligent approach to risk management reveals opportunities for innovation

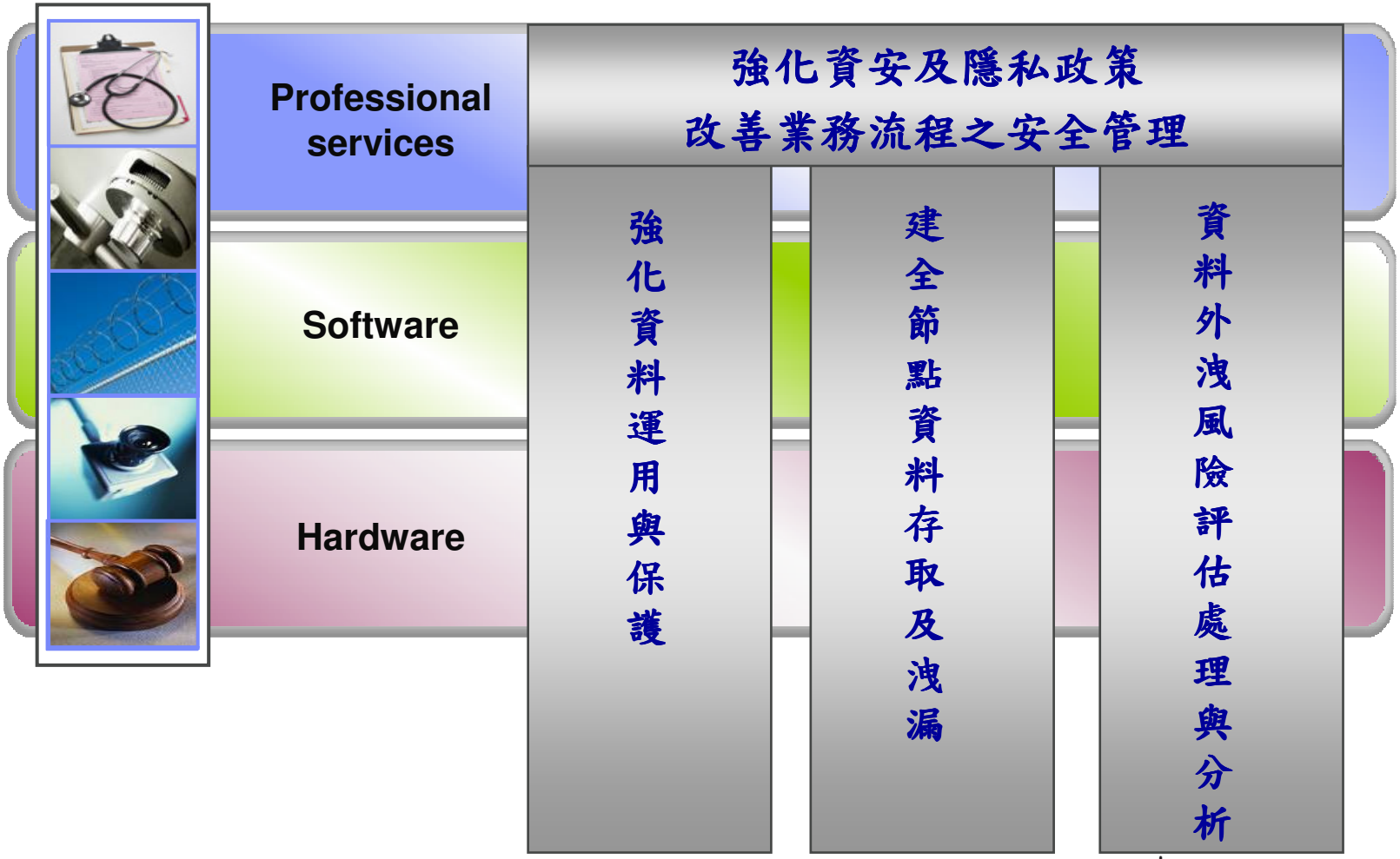
Agenda：

- 簡單回顧：節點資料保護概念
- 節點資料保護技術核心策略
- 導入資料保護方案前之關鍵問題
- **總結**

因應『新版個資法』的 法規要求及對IT系統影響；IBM從資料處理流程的控管角度，針對所涉及三大IT議題，提出因應方針及相關流程整合 解決方案。

IBM

To address the most critical client security needs, IBM focuses on three key pain points

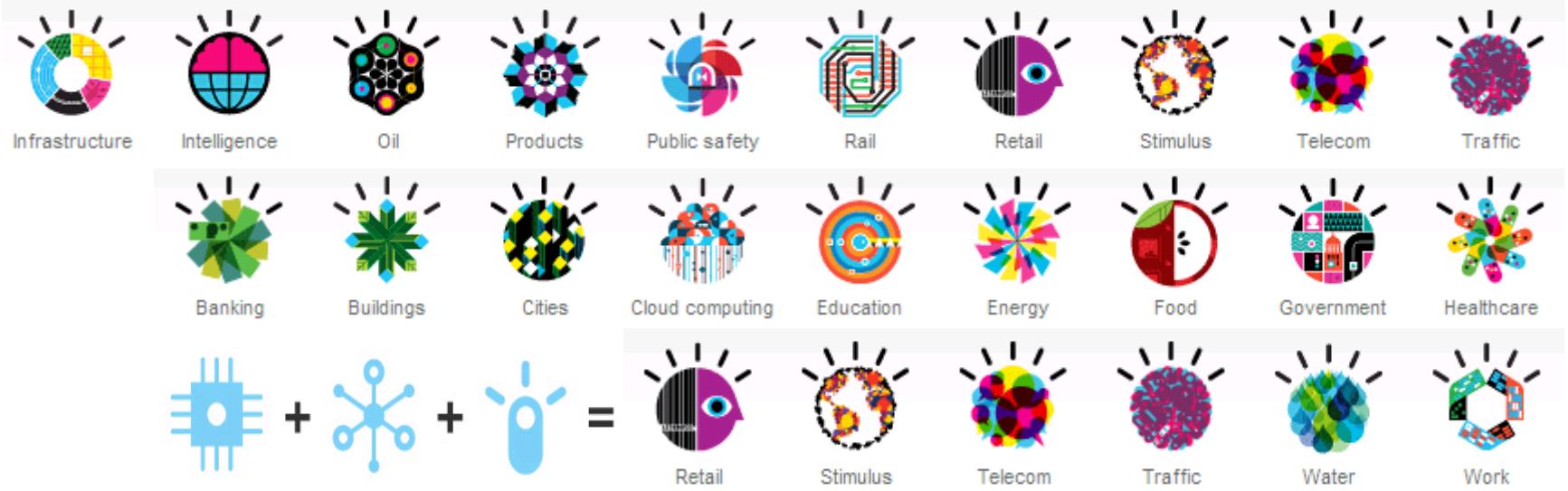


IBM提供全面向，由顧問服務至產品導入之完整資料保護服務，由IBM資訊安全專家帶領整個專案之完善進行，並確保專案內由前期顧問服務與規劃至產品佈建之知識完整轉移

法規要求	解決方案套餐	IBM 解決方案
應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏	**資料運用與保護**	• 入侵防禦弱點評估諮詢與設計服務 • 開發測試階段資料保護弱點評估諮詢與設計服務 • 網頁應用程式保護機制與開發規範暨安全性檢測服務 • 主動式入侵防禦及弱點保護系統規劃與建置服務 – XML/ WS 防火牆規劃與建置服務
	節點資料洩漏保管	• 雲端桌面資料保護解決方案 • 端點設備資料外洩預防規劃與建置服務 • 端點設備資料加密規劃與建置服務 • 磁帶機加密與保管解決方案
資料外洩損害賠償，非公務機構需證明「無故意或過失責任」，才能免責	**資料外洩風險評估與處理分析**	• 個資文件與資料分類分析與保護政策的訂定 • 企業個人資料保護政策諮詢顧問與設計服務 • 內部使用者行為稽核規劃與建置服務 • 資料庫稽核與防護系統規劃與建置服務 • 日誌集中管理及分析系統規劃與建置服務 • 身分辨認與授權管理規劃與建置服務

Q & A

The technology is here.
The people are ready.
The time is now.



IBM Global Services
3-4F, No.7, Song Ren Road,
Taipei, Taiwan

Produced in Taiwan

-

Colin Yao