KPMG

個人資料稽核實務與困境

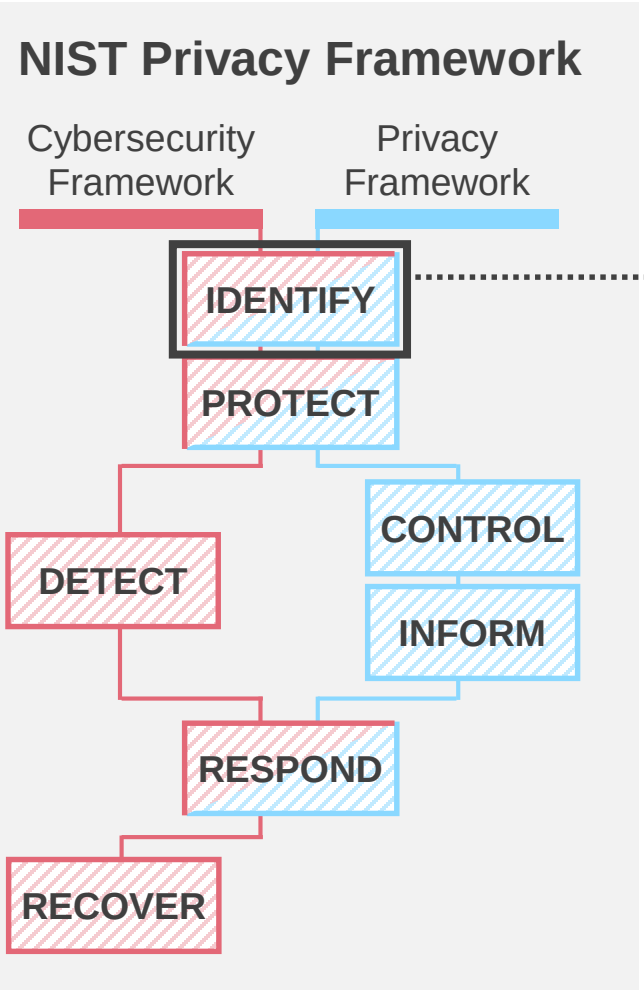
November 2019

KPMG Advisory

KPMG

3G/4G 時代的個資稽核常見發現

3G/4G 時代的個資稽核常見發現

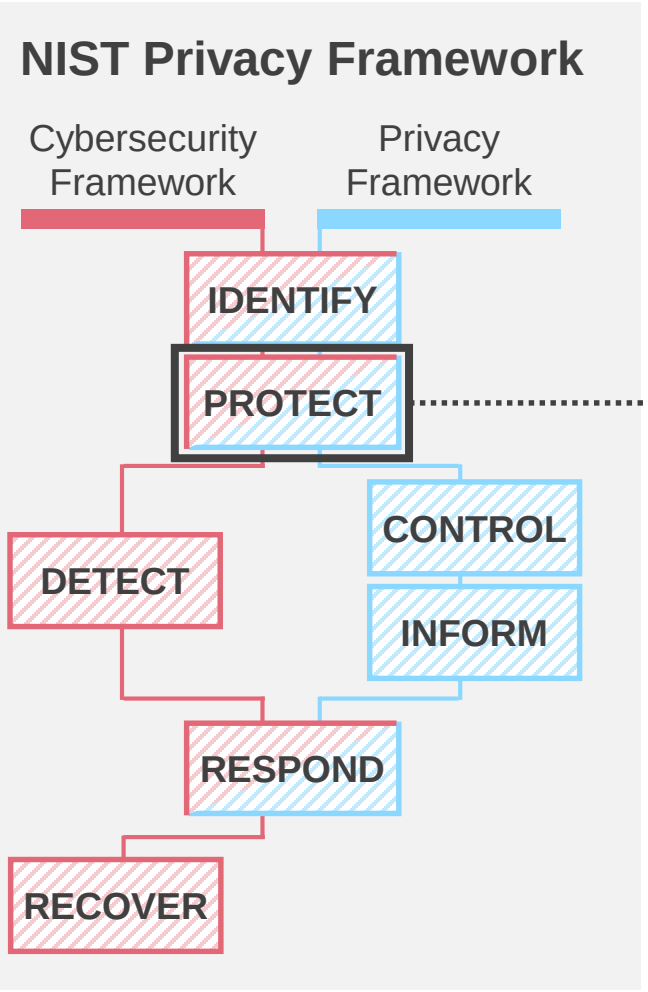


識別

- 未將資訊資產列冊控管及未妥善盤點資料備份儲存媒體

Source: https://www.cybersaint.io/blog/what-the-nist-privacy-framework-draft-means-for-privacy-and-cybersecurity

3G/4G 時代的個資稽核常見發現

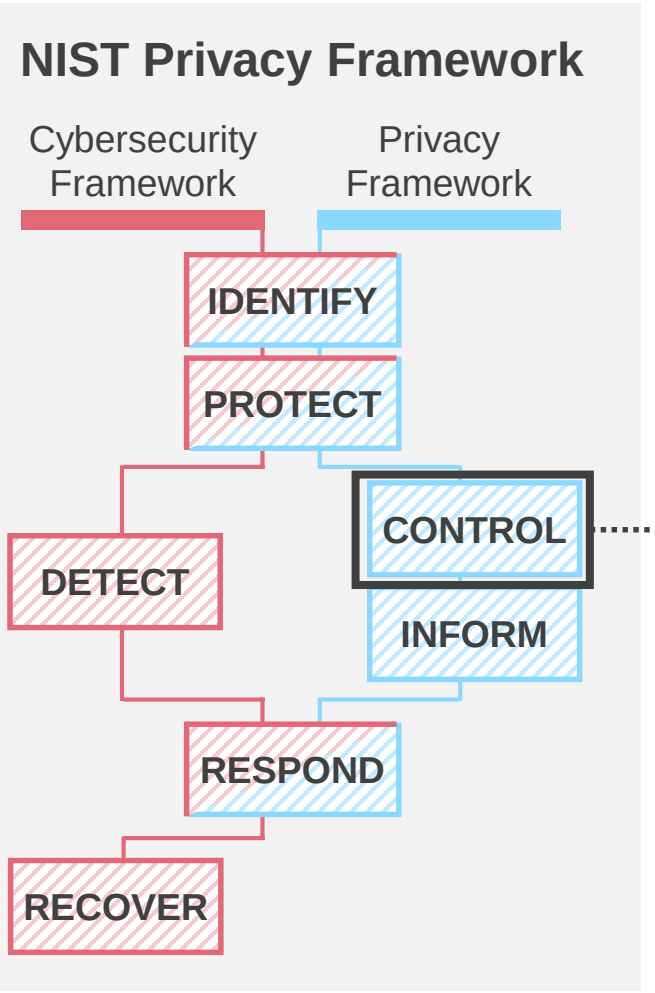


保護

- 業務使用之行動 APP，無帳號密碼即可下載瀏覽，且人員可將客戶個人資料儲存至非公司控管之雲端空間
- 防火牆已開放利用其他通訊埠對外傳輸內含個資檔案，尚未建立過濾或管控其適當性之機制
- 辦理網路相關規劃管理作業，FTP 伺服器未依規定置放
- 資料庫存取授權未符合最小授權原則
- 對存放客戶個資檔案之共用檔案伺服器，檔案可讀取設定欠妥適

Source: https://www.cybersaint.io/blog/what-the-nist-privacy-framework-draft-means-for-privacy-and-cybersecurity

3G/4G 時代的個資稽核常見發現



控制 - 資料管理

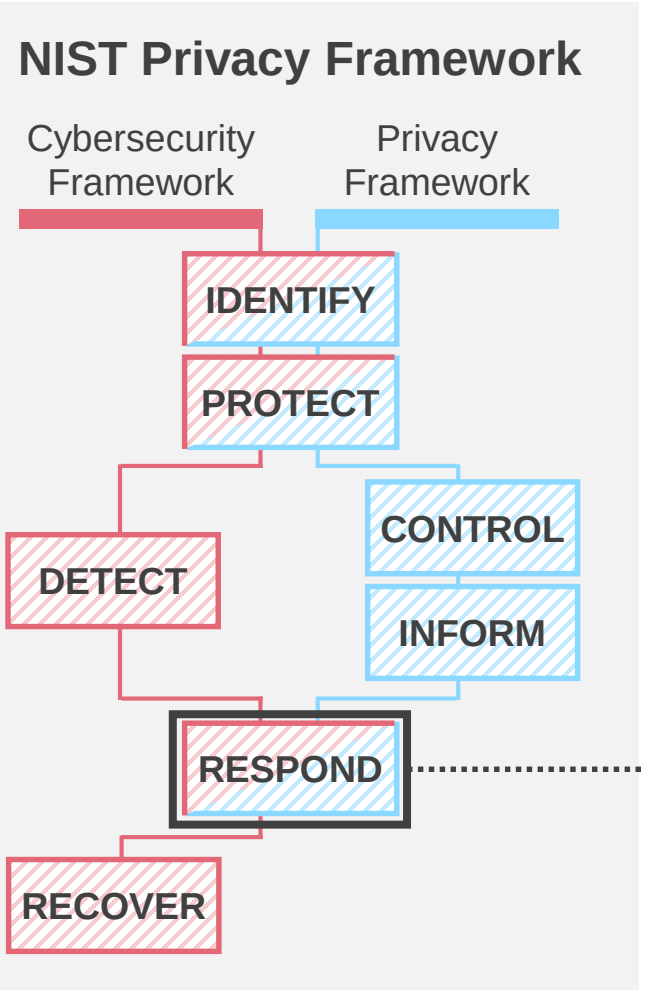
- 業務使用之個資可複製至個人電腦，並無稽核軌跡及管控措施
- 將正式作業主機之個資檔案及資料庫複製至開發測試主機作業，有未去識別化之情形
- 電子商務系統之安全設計涉及個人資料，尚未妥適隱碼顯示
- 委託其他公司辦理行銷活動參加者之個人資料蒐集作業，有對個人資料事項有未落實辦理查核
- 未將複委託之對象納入監督
- 未依內部規範將要保人之金流資料加密儲存
- 對於應收集、監控之系統稽核軌跡或日誌紀錄 (log) 範圍尚未明確規範
- 所訂應用系統安全管理作業手冊及各應用系統開發手冊等規範內容有欠完備，不利確保應用程式變更之正確性及系統維運安全
- **含個資之電子郵件外寄管理有疏漏之情事，有礙健全經營之虞**
- 以個人行動裝置通訊軟體將因公務取得之個人資料外洩予第三人，未能有效落實管理客戶資料

控制 - 弱點管理

- 僅就「高」以上風險等級系統弱點評估是否修補，對其他風險等級弱點則未有相關控管機制。
- 弱點掃描及滲透測試作業範圍尚欠完備，且對掃描發現之漏洞修補及追蹤處理未訂定作業規範等情事，有礙公司健全經營之虞。

Source: https://www.cybersaint.io/blog/what-the-nist-privacy-framework-draft-means-for-privacy-and-cybersecurity

3G/4G 時代的個資稽核常見發現



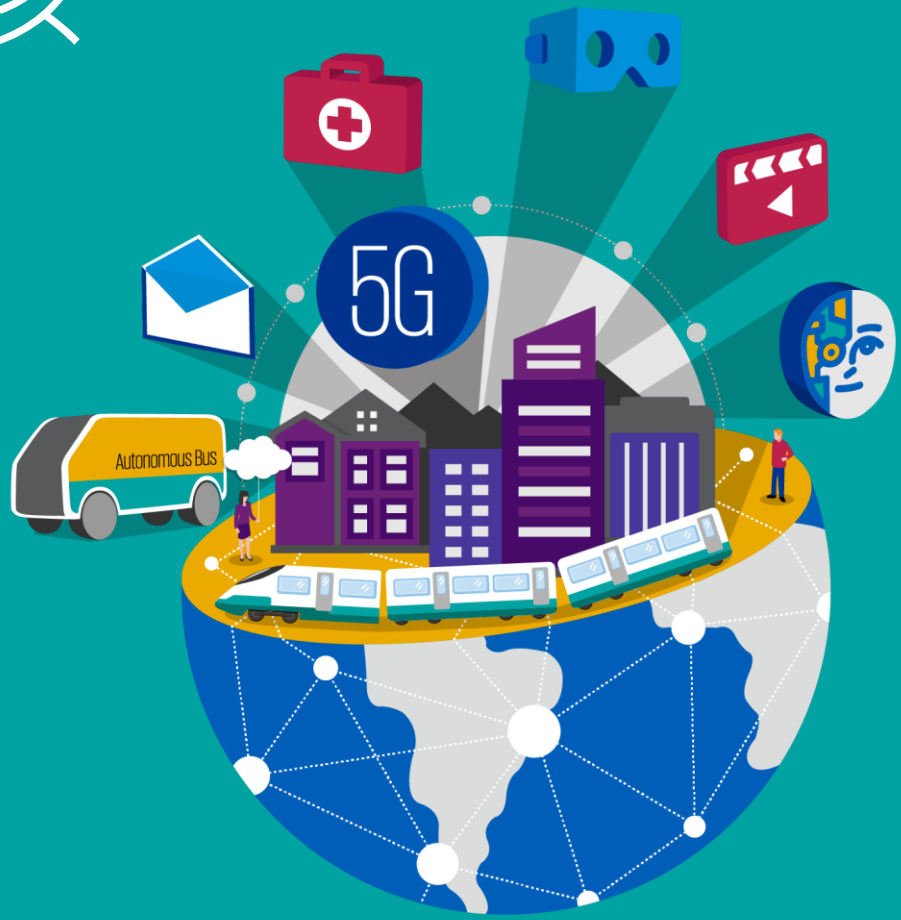
回應

- 尚未對電子商務服務系統之外部網路入侵及非法或異常使用行為所致之個資外洩情境，研擬演練計畫進行演練及檢討改善。

Source: https://www.cybersaint.io/blog/what-the-nist-privacy-framework-draft-means-for-privacy-and-cybersecurity

KPMG

5G 時代的個資稽核應提出的問題



5G的豐富應用場景

- **擴增實境 AR**

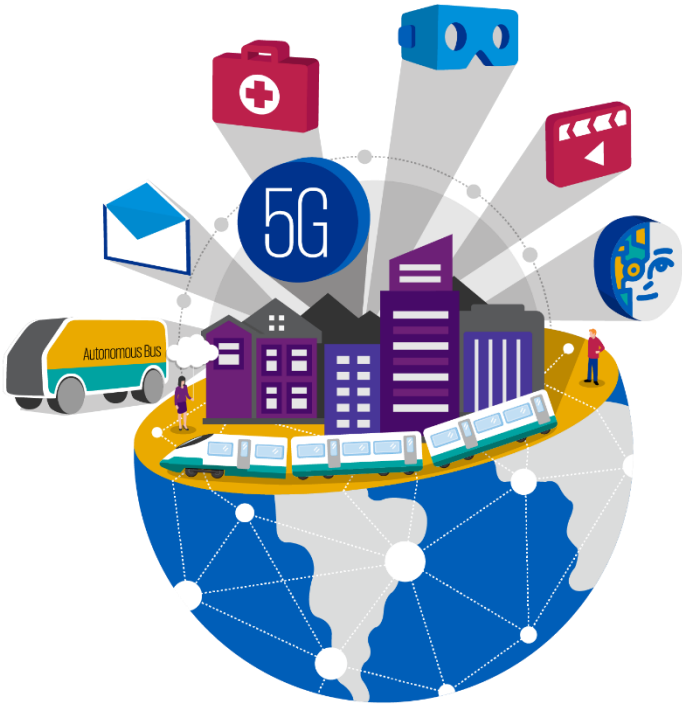
  如用擴增實境的方式，在眼鏡中告知飛機維修人員目前所處理的螺絲，該施以多大的扭力，旋至多深的深度等，讓這些複雜的工程更容易進行，也能大幅減少人為的失誤。

- **其他應用、自駕車、AIoT 等**

  前端設備採集量超過雲服務可處理的即時傳輸、即時回傳的效能要求，系統對低延遲與高頻要求極高，若無邊緣運算整合，系統反應時間可能會高於數百毫秒反饋延遲表現，直接影響服務品質。

- **虛擬實境 VR**

  如頭戴裝置搭配邊緣運算及高速網路，可將運算需求轉移，可解決現行頭戴裝置的重量、耗電、發熱、價格高昂等問題。



雲端與邊緣運算服務個資稽核問題

1 5G 雲端平台隱私稽核問題：

① 若雲端服務提供商服務出現問題，雲端業者有挑選優先回復之權利，此時如何確保使用者體驗？

② 雲端平台業者將配合不同的司法管轄區，在特殊情況下將資料提供外部，適法性應如何確認？

③ 雲端平台資料應將不同租戶的資料個別區隔，如何證明？

④ 若雲端平台發生資料外洩事件，雲端業者是否會誠實通知？法令要求的通報期限如何落實？如何釐清當事人賠償責任？

2 5G 邊緣運算伺服器隱私稽核問題：

① 伺服器負擔部分運算功能，亦為處理資料之一部分，如何確認資料保存期限？

② 承上，當事人權利是否包含該伺服器？

③ 該裝置可能為遠端伺服器，維護時之安全標準為何？

④ 邊緣運算伺服器亦可能為使用者終端裝置，安全性責任應如何劃分，且讓使用者知悉？

3 5G 大數據、AI 應用伺服器運算平台隱私稽核問題：

① 將已蒐集之個資進行 AI 分析後，提供的客製化虛擬體驗，是否可簡單返回預設值，並刪除已分析之資料？

② 已蒐集的個資，是否能將心跳、呼吸、動作資料、週邊環境資料分離，使其無法直接辨識當事人後，進行後續利用？

③ 提供之虛擬環境體驗，是否考量未成年人使用之情況？

④ 蒐集大量週邊資料後，可描繪當事人週邊環境，是否算是個資？如是，隱私條款內容適切性應如何確認 (應避免模糊描述)？

⑤ 承上，若屬於個資，一旦納入大數據、AI 分析的個資，能否單獨行使刪除權？

5G通訊線路

- 峰值速率快10倍以上
- 點到點零時延遲體驗
- 高鐵使用亦無問題

AR、VR、AIoT 裝置個資稽核問題

- 於虛擬影像中看到的置入性廣告，如三星 logo、NIKE、APPLE 等，是否算對當事人行銷？可否拒絕？
- 應用服務、遊戲等，提供多人之家庭使用之月租方案，需識別是否為家人，故原不屬於個資的裝置識別代號，結合後為個資的一部分。
- 裝置可能大量蒐集資料，如人體的動作、呼吸、心跳等，週邊環境、週邊的人體身形 (含容貌) 並納入虛擬環境體驗，相關資料是否算是個資？如是，如何行使同意權？
- 為落實預設隱私保護，歐盟指導文件指出，資料蒐集與撤回同意應盡可能便利行使，如何實現於大量蒐集個資之裝置或虛擬環境內？其他當事人權利如何實現？裝置開啟時是否有提示訊號？
- 設備或裝置亦有作業系統 (如 Android) 及應用程式 (如 APP)，安全性 / 弱點更新應如何確保？

AR、VR、AIoT 裝置個資稽核問題

- 於虛擬影像中看到的置入性廣告，如三星 logo、NIKE、APPLE 等，是否算對當事人行銷？可否拒絕？
- 應用服務、遊戲等，提供多人之家庭使用之月租方案，需識別是否為家人，故原不屬於個資的裝置識別代號，結合後為個資的一部分。
- 裝置可能大量蒐集資料，如人體的動作、呼吸、心跳等，週邊環境、週邊的人體身形 (含容貌) 並納入虛擬環境體驗，相關資料是否算是個資？如是，如何行使同意權？
- 為落實預設隱私保護，歐盟指導文件指出，資料蒐集與撤回同意應盡可能便利行使，如何實現於大量蒐集個資之裝置或虛擬環境內？其他當事人權利如何實現？裝置開啟時是否有提示訊號？
- 設備或裝置亦有作業系統 (如 Android) 及應用程式 (如 APP)，安全性 / 弱點更新應如何確保？

- **擴增實境 AR**

  如用擴增實境的方式，在眼鏡中告知飛機維修人員目前所處理的螺絲，該施以多大的扭力，旋至多深的深度等，讓這些複雜的工程更容易進行，也能大幅減少人為的失誤。

- **虛擬實境 VR**

  如頭戴裝置搭配邊緣運算及高速網路，可將運算需求轉移，可解決現行頭戴裝置的重量、耗電、發熱、價格高昂等問題。

- **其他應用、自駕車、AIoT 等**

  前端設備採集量超過雲服務可處理的即時傳輸、即時回傳的效能要求，系統對低延遲與高頻要求極高，若無邊緣運算整合，系統反應時間可能會高於數百毫秒反饋延遲表現，直接影響服務品質。

KPMG

Thank You

kpmg.com/socialmedia

kpmg.com/app

Contact Us

KPMG TAIWAN
IT Advisory in Management & Risk Consulting

謝 昀 澤 Jason Hsieh
執行副總經理 Partner
+886-2-8101-6666 ext.07989
jasonhsieh@kpmg.com.tw

KPMG Advisory Services Co., Ltd.
68F, Taipei 101 Tower, No. 7, Sec. 5, Xin-Yi Road,
Taipei, 11049, Taiwan, R.O.C.