範例十三：風險情境表

風險大分類	風險子分類	個資潛在風險事件
1.紙本類	1.1 處理	1.1.1 紙本文件於內部處理過程中，是否在長時間不使用或於下班時收存於辦公室上鎖之資料櫃。
	1.2 保存	1.2.1 紙本文件之保存(含暫存區)地點是否具備進出管控措施。
		1.2.2 紙本文件歸檔、入倉(庫)或集中保管前，是否確實清點數量及內容。
		1.2.3 紙本文件存放地點是否已有消防、滅火、溫度控制等設施。
	1.3 傳遞	1.3.1 紙本文件於內部傳遞過程中，是否具有簽收/點收等控管措施。
		1.3.2 紙本文件提供外部利用是否均有公文往返等使用紀錄。
	1.4 銷毀	1.4.1 包含個資之紙本文件是否禁止回收使用。
		1.4.2 紙本文件於內部進行銷毀時，是否均銷毀致無法辨識。
		1.4.3 紙本文件交由受委託廠商銷毀前，是否已簽訂包含雙方權利義務及賠償條款之契約或保密協議。
		1.4.4 紙本文件交由受委託廠商進行銷毀時，是否已妥善進行監銷並留存紀錄。
2.電子類	2.1 傳輸	2.1.1 同仁透過對外寄發、傳輸個資檔案是否均進行加密。
		2.1.2 同仁對外傳輸個資檔案是否均有傳輸記錄，如 Email 寄件備份、FTP 傳輸記錄、網路硬碟等。
	2.2 保存	2.2.1 存於本機電腦之個資檔案，是否均有加密或存放於專用且安全之資料夾。
	2.3 銷毀	2.3.1 電子檔案保存期限屆滿後是否均進行刪除。

3.電子檔-可攜式媒體	3.1 傳遞	3.1.1 將個人資料檔案使用可攜式媒體傳遞時，是否均進行加密。
	3.2 銷毀	3.2.1儲存個人資料之可攜式媒體不再使用或損毀時，是否均進行刪除資料或實體破壞。
4.系統資料庫	4.1 存取權限	4.1.1 資訊系統之使用者帳號是否均定期審查。
		4.1.2 系統是否具備職務區隔機制，並給予適當之存取權限。
	4.2 使用紀錄	4.2.1資訊系統是否已具有記錄使用者活動日誌功能。
		4.2.2單位主管或其授權人員是否定期審查資訊系統使用者之活動日誌。
5.委外作業類	5.1 選商	5.1.1委外案件是否均會評估及選擇可提供符合組織對個人資料保護需求之受委託廠商(如一年內未曾發生個資外洩事件、重大資安事件或有無通過 ISO 27001、BS10012、TPIPAS、ISO29100、ISO 27701 等驗證)。
	5.2 簽約	5.2.1在委託外部單位處理個人資料是否有簽訂契約，並包含適當安控措施是否足夠。
		5.2.2組織與受委託廠商所簽訂之契約中是否已包含是否得將個人資料處理作業進行轉包/分包之規定。
		5.2.3 若允許轉包/分包，受委託廠商與其複委託廠商(下包商)所簽訂之契約是否已要求複委託廠商實行與受委託廠商相同等級之安控措施。
		5.2.4組織與受委託廠商所簽訂之契約中是否已明確規範，當資料逾保存期限或契約終止時，有關個人資料之銷毀、交還原組織或其他處理方式。
	5.3 履約	5.3.1於委託外部單位處理個人資料契約期間內，是否定期監督或實地審查受委託廠商之安控措施是否落實執行。
		5.3.2組織是否定期依據與受委託廠商所簽訂之契約進行監督，當資料逾保存期限或契約終

		止時確認有關個人資料之銷毀、交還原組織或其他處理之方式。
	5.4 小額採購	5.4.1 如以小額採購方式委託外部單位蒐集、處理、利用或銷毀個人資料時，是否均簽訂書面協議並落實監督作業。