圖資中心 104 學年度第 2 學期			
主 題	BS 10012:2009 標準條文介紹		
時 間	105 年 04 月 14 日（星期四 ）下午 2：00～4：00		
地 點	G603 電腦教室	人 數	教職員：60 人
講 者	漢昕科技-王吉祥 講師		
主辦單位	圖資中心		

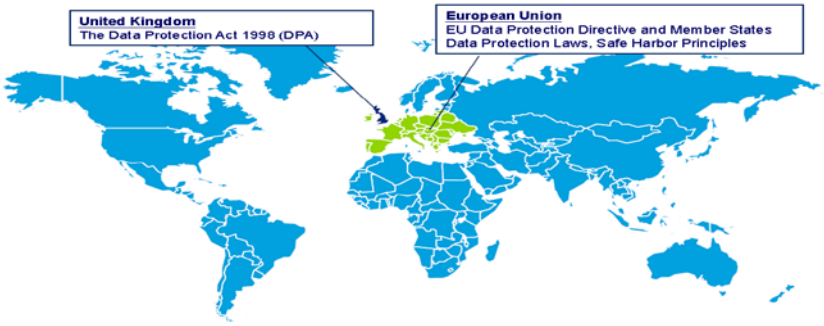
簡報大綱

1. BS 10012介紹
2. 執行規劃PIMS
3. 實作與運作PIMS
4. 監視與審查PIMS
5. 維持與改進PIMS
6. 問題與討論

1

BS 10012簡介

- BS 10012係由英國國家標準局(BSI)所發展的個人資料保護架構，於2009年6月2日公布，該標準的目的在建立個人資料保護的最佳實務與協助組織符合個人資料保護法的規範。
- 該標準所遵循之法律為英國資料保護法(The Data Protection Act 1998)，其包括8大保護原則，就持有、取得、使用或揭露有關個人資料處理過程等方面，提供遵循之規範。



2

3.1 建立與管理PIMS

控制目標	無。
控制措施	無。
說明	◆ 組織應依據3.2~3.7之要求建立、實作、維護及持續改進PIMS。

3

3.2 界定PIMS適用範圍及設定目標

控制目標	無。
控制措施	無。
說明	◆ 組織應依據下列項目界定PIMS的範圍並設定個人資料管理目標 a) 個人資料管理的需求； b) 組織的目標與義務； c) 組織可承受的風險等級； d) 適用之法令、規章、契約（合約）與專業職責； e) 個人和其他利害關係之利益。

4

3.3 個人資料管理政策

控制目標	無。
控制措施	無。
說明	◆ 組織應確保高階管理階層被賦予發行及維護個人資料管理政策之責，而其政策中應明訂政策的框架，並展示對於遵循資料保護法令與最佳實務的支持與承諾。 ◆ 其所謂高階管理階層包含董事會、總經理與資深主管、公司合夥人或公司負責人。 ◆ 個人資料管理政策所陳述之內容應包含： a) 整個組織，或 b) 特定的組織範圍。 ◆ 個人資料管理政策應公告予所有同仁。

5

3.4 政策內容

控制目標	無。
控制措施	無。
說明	◆ 個人資料管理政策中應陳述組織對於遵循資料保護法令與最佳實務的承諾，包含： a) 僅於合法的組織需求下，始得進行個人資料之處理； b) 僅針對特定目的蒐集必要的個人資料，且不過度的處理個人資料； c) 明確告知當事人其個人資料將如何被使用及被誰使用； d) 僅處理相關且適當的個人資訊； e) 公平與合法地處理個人資訊（參考4.7）； f) 組織應維護一份個人資料清冊（參考4.2）； g) 確保個人資料的正確性，並於必要時進行更新； h) 僅依法或合法的組織目的下保存個人資料； i) 尊重當事人對其個人資料所能行使之權利，包含其申請閱覽權； j) 確保所有個人資料的安全； k) 當組織將個人資料傳輸至非歐洲經濟區成員之國家時，應確保其具良善保護之機制； l) 個人資料保護法令所允許之例外情形的應用； m)建立與實施PIMS，以確認個人資料保護政策的實行； n) 鑑別內外部利害關係者及其參與PIMS治理與運作的程度； o) 於PIMS運行中，明確界定員工之責任與義務（參考3.5）；

6

3.5 職責與當責性

控制目標	無。
控制措施	無。
說明	◆ 高階管理團隊之成員應負起組織管理個人資料之責，以展示組織遵循資料保護法令及最佳實務之決心（亦可參考4.1.1）。其職責應包含： a) 核准個人資料管理政策； b) 依個人資料管理政策建立與實行PIMS； c) 遵循個人資料管理政策執行安全與風險管理（亦可參考4.13.1）。 ◆ 應指派一位或多位合適或具經驗的同仁負責日常個人資料管理政策的遵循（亦可參考4.1.2）。 ◆ 藉由流程與程序的實行、適當的員工發展或對於不符合事項制訂控管程序，以確保所有同仁皆能遵循個人資料管理政策之要求。

7

3.6 資源提供

控制目標	無。
控制措施	無。
說明	◆ 組織應決定並提供建立、實行及維運PIMS所需的資源。

8

3.7 將PIMS嵌入組織文化

控制目標	無。
控制措施	無。
說明	◆ 為確保個人資料管理可成為公司核心價值的一部分並可有效管理，組織應該： a) 透過持續的教育訓練與認知課程，以提高、強化與維持所有員工對PIMS的認知； b) 建立衡量PIMS認知宣導有效性的程序； c) 對所有員工傳達下列項目的重要性： 1) 達成PIMS的目標： 2) 遵循個人資料管理政策： 3) 個人資料管理政策的持續改善： d) 確保每個員工都瞭解他們如何影響組織PIMS目標的達成度與未遵循目標的後果。

9

4.1 責任的配置

控制目標	為確保組織能依個人資料管理政策委派適當之權責予同仁。
控制措施	4.1.1 高階管理階層；4.12日常遵循政策之責任；4.1.3資料保護代表
說明	◆ 高階管理階層 ● 高階管理團隊之成員應負起組織管理個人資料之責，以展示組織遵循資料保護法令及最佳實務之決心。 ◆ 日常遵循政策之責任 ● 應指派一位或多位合適或具經驗的同仁負責日常個人資料管理政策的遵循，並依組織的大小與個人資料的處理性質，將該責任指派予全職或兼職的人員。受指派的人員應承擔下列責任： a) 遵循個人資料管理政策之責； b) 發展與審核個人資料管理政策； c) 確保個人資料管理政策的實行； d) 個人資料管理政策的管理審查作業（參照5.2）； e) 依個人資料管理政策之需求進行教育訓練與持續的認知宣導（參照4.3）； f) 個人資料處理程序之核准作業，例如： 1) 隱私權公告的管理與溝通（參照4.7.1）； 2) 處理來自當事人之需求（參照4.12.1）； 3) 個人資料的蒐集與處理（參照4.7.1）；

4.1 責任的配置

說明	4) 抱怨事件的處理（參照4.12.2）； 5) 資安事故的管理（參照4.13.6）； 6) 委外與岸外生產（off-shoring）（參照4.14）； g) 與組織內負責風險管理與安全議題的單位/人聯繫（參照4.13）； h) 提供有關資料保護法令相關事項的專家意見與指引文件； i) 說明與應用個人資料處理的各種例外狀況（參見簡介或4.8.1）； j) 提供資料分享方案之建議（包含資料處於異地之資安議題）（參照4.8.3）； k) 確保組織可接收與資料保護法令相關之法例修訂及合適的指導綱要（參照4.5）； l) 持續確認法律、實務與科技的變化對PIMS帶來的改變（參照4.5）； m) 在資料保護法令的要求下，填寫、提交及管理隱私權通告予資料保護長（Information Commissioner）（參照4.6）； n) 考量任何具強制或諮詢性單位針對個人資料處理所制定之法規，經評估其適用性後於組織內實行。 ◆ 資料保護代表 ● 當組織由多個執行個人資料處理作業的部門或系統組成時，組織應決定是否設立個人資料保護代表，以： a) 代表於管理個資具高風險之部門或系統（參見4.2.2）；及 b) 協助員工日常的政策遵循。

4.2 辨識及記錄個人資料的使用情況

控制目標	確保組織瞭解個人資料之類別，及不同類別資料的處理過程及其風險。
控制措施	4.2.1概述；4.2.2具高風險的個人資料
說明	◆ 概述 ● 組織應維護一份個人資料分類清冊。此清冊亦應記錄各類個人資料之使用目的。 ● 個人資料清冊需能明確的通告Information Commissioner's Office組織處理資料的方式。 ● 組織應記錄個人資料在組織中之流向。 ◆ 具高風險的個人資料 ● 個人資料清冊（參見4.2.1）中應明確的鑑別與描述組織中具高處理風險之個人資料類別。 ● 具高風險之個人資料類別可能包含： a) 敏感的個人資訊（定義於DPA之Section2）； b) 個人銀行帳戶與其他財務資訊； c) 身分識別號碼； d) 弱勢成人與兒童之個人資訊； e) 個人特徵的詳細說明； f) 對個人將產生負面影響的資訊。 ● 當大量處理個人資料時，將會提升風險程度。

12

4.3 認知與教育訓練

控制目標	確保所有員工皆明白在處理個人資料時應負之責任。
控制措施	無。
說明	◆ 組織應確保負責日常個人資料管理政策遵循之同仁（參見4.1.2）皆能展現其瞭解資料保護法令與最佳實務及如何具體實現之能力。 ◆ 組織應與外部相關團體維持適當的溝通管道，以持續提供負責日常個人資料管理政策遵循之同仁關於個人資料處理之相關議題。 ◆ 組織應證明所有員工皆瞭解其本身在個人資料保護上的責任，以確保其皆能依適當之程序以保護及處理個人資料，並考量到相關的安全需求。 ◆ 所有員工皆應接受教育訓練，以確保其皆能依適當之程序處理個人資料。另外，教育訓練應依組織內不同之角色而分別舉辦。

13

4.4 風險評鑑

控制目標	確保組織能瞭解在處理各種特定類型之個人資料所可能產生的風險。
控制措施	無。
說明	◆ 組織應評估在處理個人資料的過程中，對當事人可能產生的風險等級。本評估亦應包含處理該個人資料之其它組織。組織應管理在風險評鑑過程中所識別的各項風險，以減輕違反政策要求的各種可能性。 ◆ 風險評鑑之程序應包含經由負責管理個人資料之責的人員（參見3.5）檢視任何可能造成當事人困擾或損失的個人資料處理過程後，所做出提升其個人資料處理風險等級之過程。 ◆ 組織可使用本身的風險評鑑方法論。另外，亦可以參考ICO所公告的隱私衝擊評估評估指引（http://www.ico.gov.uk/tools_and_resources/document_library/data_protection.aspx）。

14

4.5 PIMS的持續更新

控制目標	為評估組織之PIMS能持續提供一架構，以維持及改善資料保護法令與最佳實務之遵循。
控制措施	無。
說明	◆ 負責日常政策遵循之員工應持續評估組織遵循資料保護法令與最佳實務之狀況，並適時加以調整。 ◆ 此評估應包含當組織需求或科技環境改變時，重新審視PIMS。

15

4.6 通告

控制目標	確保組織依據DPA的要求，將處理個人資料過程之細節通報資訊保護安全官（the Information Commissioner）。
控制措施	無。
說明	◆ PIMS中應包含觸發通報之程序（除非該組織被DPA排除在通報的對象之外），並確保所通報之訊息能保持其真確性且處於最新狀態。

16

4.7 公正與合法的處理

控制目標	確保組織公正且合法的處理個人資料，並於處理個人資料前，清楚識別法令上之各項要求。
控制措施	4.7.1個人資料的蒐集與處理；4.7.2隱私公告與聲明之紀錄； 4.7.3隱私公告與聲明之取得；4.7.4隱私公告與聲明之可用性；4.7.5第三方
說明	◆ 個人資料的蒐集與處理 ● PIMS應制訂相關程序以確保下列要求： a) 組織應公正且合法的處理個人資料； b) 組織應依據DPA Schedule 2的要求，僅在合理的情形下處理個人資料； c) 組織應僅在符合組織目標及DPA Schedule2及3的要求下，處理敏感性個人資料。 d) 組織應針對提供個人資料之當事人提供（線上）隱私權聲明（privacy notice, privacy statement），不論該通知或聲明為完整、抽取片段加超連結或僅為超連結，其皆應明確陳述下列訊息： 1) 組織之身份資訊； 2) 處理個人資料之目的； 3) 將個人資料揭漏予第三方之相關資訊； 4) 當事人對於其個人資料可行使之權利； 5) 個人資料是否被傳輸至非歐洲經濟區成員之國家； 6) 對組織處理個人資料之過程有任何疑問時，詳細的組織聯繫方式； 7) 於網站上蒐集當事人個人資料之任何技術之描述，如cookies ； 8) 說明組織可公正地處理個人資料之其它資訊。 ● 為目前或未來之行銷目的的所蒐集之個人資訊，PIMS應制訂提供當事人表示拒絕接受行銷之方式，並能明確告知當事人。

17

4.7 公正與合法的處理

說明

- PIMS中應制訂曾經當事人同意之個人資料處理作業被撤銷後，相關作業將被終止之程序。
- 當其他利害關係團體或法令要求清楚說明行銷目的時，PIMS應包含蒐集當事人同意處理權之程序。
- 當組織為特定目的而蒐集敏感性個人資料時，其PIMS中應制訂一確保隱私權聲明得以明確陳述該敏感性個人資料之使用目的程序。
- PIMS中應制訂相關程序，其可確保新設立的個人資料蒐集方法由合適且具經驗之人員（參見4.1.2）加以檢視，並留下簽署紀錄，進而確保該方法得以遵循資料保護法令與最佳實務。

◆ 隱私公告與聲明之紀錄

- PIMS中應制訂一維護（線上）隱私權聲明紀錄之程序。該紀錄之保存時限應至少等同於其個人資料。

◆ 隱私公告與聲明之取得

- PIMS中應制訂當組織直接從當事人端取得其個人資料時，於取得其個人資料前，組織得以提供當事人取得（線上）隱私權聲明或其取得方式之程序。

◆ 隱私公告與聲明之可用性

- PIMS中應制訂一確保任何的（線上）隱私權聲明內容易於當事人瞭解且取得之程序。
- 對弱勢人士、閱讀困難之人或孩童，隱私權聲明之設計必需以他們所能理解之形式或語言呈現，並需便於取得。

18

4.7 公正與合法的處理

說明

◆ 第三方

- PIMS中應制訂一確保第三方得公正且合法取得個人資料之程序。
- PIMS中應制訂一確保組織得以提供（線上）隱私權聲明（參見4.7.1）之程序，除非該作業會造成不相稱之投入（disproportionate effort），即該作業已超出組織所評估之相對成本。
- 不相稱之投入（disproportionate effort）在此不僅指"大量的成本投入"，也可以指當資料處理流程可能對當事人產生不好的影響時，要提供相當長度的說明。

19

4.8 個人資料處理的目的

控制目標	為確保個人資料僅為某些特定目的所取得，而不用於任何違反原目的之處。
控制措施	4.8.1處理準則；4.8.2新目的的同意 4.8.3資料分享；4.8.4資料配對
說明	◆ 處理準則 ● PIMS中應制訂相關程序，以確保於處理個人資料的過程中，不會產生違反或潛在可能違反任何法定義務之情況，包含法令條文、一般法律或契約條款等。 ● PIMS中應制訂相關程序，以確保為特定目的所蒐集之個人資料不會用於其他目的，除非： a) 有相關法令免責之規定；或 b) 當事人已同意其個人資料可被使用於新設立之目的上。 ● PIMS中應制訂相關程序，以確保當敏感性之個人資料被使用於其他新設立的目的時，應於其資料處理前取得當事人的同意，除非有其他免責之情況。 ◆ 新目的的同意 ● PIMS中應制訂相關程序，以確保對新目的之任何同意承諾是出於自由意識且充分明確的表達。 ● PIMS中應制訂相關程序，以確保： a) 為新處理目的，已明確取得當事人之同意。 b) 為新處理目的所得之當事人同意紀錄的保存。

20

4.8 個人資料處理的目的

說明	◆ 資料分享 ● PIMS中應制訂相關程序，以確保組織分享個人資料予其他組織時，雙方的權責皆可以正式協議書或契約等方式記錄之。 ● PIMS中應制訂相關程序，以確保其他組織得依據其所設定之目的使用個人資料： a) 於書面協議或契約中說明雙方使用資料的目的，以及若為其它目的的使用該資料時，其相關限制為何；及 b) 其他組織應提供其處理個人資料時，並不會違反DPA要求之保證或其他承諾之證據。 ● PIMS中應制訂相關程序，以確保任何涉及將資料提供給第三方之新處理程序，皆需視情況調整組織之隱私通告（參見4.6）及組織所提供之（線上）隱私權聲明（參見4.7.1d）。 ● 不管有沒有可能，組織都應確保： 1) 資料分享的法令依據；及 2) 若需要，資料分享前應取得當事人的同意。 ● 當資料分享可不需取得當事人同意時，PIMS應制訂相關程序，以確保此資料分享所使用的協定或控制措施，皆能被記錄並稽核之。 ● 當資料必需分享給第三方時，如法令要求，PIMS應制訂相關程序，以確保資料分享所使用之協定與控制措施，皆能被記錄之。 ◆ 資料配對 ● 當個人資料可與其他資料配對，造成組織可提升其識別特定當事人之能力時，PIMS應制訂相關程序，以確保經配對的資料僅被使用於適宜的目的下，即在法令獲許或取得當事人同意的情況下。

21

4.9 適當、相關及不過度

控制目標	為確保個人資料為適當、相關及不過度之處置。
控制措施	4.9.1適當性；4.9.2相關且不過度
說明	◆ 適當性 ● PIMS應制訂相關程序，以確保組織所蒐集的個人資料皆符合組織之目的。 ● PIMS應制訂相關程序，以定期檢視處理個人資料之科技與程序，確保資訊得以持續符合其使用目的。 ◆ 相關且不過度 ● PIMS應制訂相關程序，以確保： a) 組織所處理之個人資料數量，在符合其法令目的下，使其最小化。 b) 組織不處理無關或超過原來所陳述之使用目的的額外個人資料，除非使用此資料並無特定規範或僅於取得當事人同意後方才使用。 c) 處理個人資料之新系統或程序得以定期檢視，以確保個人資料處理之適當性及不過度使用。 ● 當個人資料的處理程序與組織的目的無關或不必要，PIMS應確保個人資料不被處理。

22

4.10 正確性

控制目標	確保個人資料的正確性，並適需求持續更新。
控制措施	無。
說明	◆ PIMS應制訂相關程序，以確保個人資料之完整性與正確性得以維護。 ◆ PIMS應制訂相關程序，以確保當事人可質疑其個人資料之正確性，並視需要修改之。當個人資料發生錯誤且無法被更正時，如歷史資料，PIMS亦應制訂一程序，以記錄該錯誤資訊，並視情況記錄正確之個人資料。 ◆ PIMS應制訂相關程序，以檢視所宣稱之錯誤資訊是否為真。 ◆ PIMS應制訂相關程序，以確保所有員工皆瞭解保持正確個人資料之重要性，及當進行重要決策時，必需使用正確之個人資料。 ◆ PIMS應制訂相關程序，以 a) 通知第三方過去曾提供錯誤或非最新之個人資訊，不可使用在會影響客戶權益的決策上；及 b) 必要時傳遞正確之個人資料予第三方。 ◆ PIMS應制訂相關程序，以檢視與處理個人資料有關之新系統與流程，以便： a) 確保這些系統或流程盡可能避免記錄任何錯誤或過時的個人資訊，及 b) 允許修正錯誤或過時的個人資訊。

23

4.11 保留及處置

控制目標	確保個人資料僅保留於其所需之時間內。
控制措施	無。
說明	◆ PIMS應參照個人資料之保存計畫，其應： a) 包含組織與法令所規定之最低資料保存期限； b) 明確設定個人資料保存期限的判斷標準與依據；及 c) 記錄任何當個人資料超過其所陳述之最低資料保存期限的說明，例如其為歷程記錄或因研究使用。 ◆ PIMS應制訂相關程序，以實施個人資料之保存計畫，並與所有相關之同仁確認該計畫。 ◆ PIMS應制訂相關程序，以確保不需要之個人資料皆被銷毀。 ◆ PIMS應制訂或參考相關程序，以控管： a) 其為被核准之程序； b) 其安全等級符合個人資料之敏感程度；及 c) 其與公司資訊安全風險評鑑之要求一致。 ◆ 在某些情況下，個人資料的處置可能是將其傳送至永久保存的儲存設施中。

24

4.12 個人權利

控制目標	為確保組織制訂實現個人權利之適當程序。
控制措施	4.12.1個人權利；4.12.2抱怨與申訴
說明	◆ 個人權利 ● PIMS應制訂相關程序，以確保個人權利的實現及實現該權利之法定時間限制。 ● 此權利包含存取個人資料、拒絕個人資料的處理及檢視自動處理個人資料的機制。 ◆ 抱怨與申訴 ● PIMS應制訂當事人抱怨受理之程序，以確保當事人對於組織處理其個人資料的不滿能得體地被受理。該程序亦應包含組織於處理當事人抱怨事件後，當事人可再申訴之程序。

25

4.13 安全議題

控制目標	為確保個人資料免於遺失或損毀及未經授權或非法的處理，組織得以實施適當的管理與技術層面之安全控管機制。
控制措施	4.13.1安全控管；4.13.2儲存與管理；4.13.3傳輸；4.13.4存取控制 4.13.5安全評估；4.13.6資安事故管理
說明	◆ 安全控管 ● PIMS應實施具體之控管措施： a) 於不同之個人資料類別；及 b) 於當個人資料外洩時，造成當事人損失或困擾之風險（參見4.4）。 ● 風險評鑑（參見4.4）為組織設定其合適的控管水準，而過度的安全控管所帶來的損害可能會和過鬆的安全控管一樣。 ● 於處理具高風險的個人資料時，PIMS應制訂相關程序，以確保其安全控管措施的採用與實施皆能符合其所評估之風險等級，並維持此控管。 ● 組織可考量遵循BSISO/IEC27001。由公正第三方所認證之BSISO/IEC27001可以證實組織安全控管之遵循程度。 ◆ 儲存與管理 ● PIMS應制訂相關程序，以確保個人資料可根據其機敏性得以安全的儲存與處置。 ● 組織應特別注意儲存於可攜式儲存設備之個人資料，如備份磁帶、移除式USB裝置、移除式硬碟、筆記型電腦及手提式設備。

26

4.13 安全議題

說明	◆ 傳輸 ● PIMS應制訂相關程序，以確保當個人資料以電子或人工方式在組織內外傳輸的過程中，皆施予合適之控管措施，進而提供資料傳遞之安全防護。 ◆ 存取控制 ● PIMS應制訂相關程序，以確保人員僅於其職掌角色所需，始得取得個人資料存取權限。 ● PIMS應制訂相關程序，以確保組織能明確告知所有人員經合法授予之個人資料存取權僅可使用於工作目的，而個人資料的存取作業亦應在合法目的下方可執行。 ● 於處理具高風險的個人資料（參見4.2.2）時，PIMS應制訂相關程序，以確保組織所實行之存取控制措施符合該個人資料之敏感等級。 ● PIMS應制訂相關程序，以確保所有個人資料的存取作業皆被監視，且經資訊安全風險評估。

27

4.13 安全議題

說明	◆ 安全評估 ● PIMS應制訂相關程序，以確保資訊安全評估可被定期執行。 ● 此安全評估應確認現存之安全控制措施是否合適，並給予相關的改善建議。 ● 此安全評估應考量當資安事故發生時，當事人所受到之傷害、損失及困擾等風險。 ◆ 資安事故的管理 ● PIMS應制訂相關程序： a) 以評估及管理涉及個人資料之資安事故，包含降低損害之程序； b) 以記錄每筆資安事故，包含評估該事故的發生原因、採用什麼矯正措施以及可以從資安事故中學習到什麼； c) 以決定是否需通報主管機關（如Information Commissioner或FSA）或通知當事人；及 d) 以留存任何通報及報知紀錄。

28

4.14 將個人資料傳輸於EEA外

控制目標	為確保當個人資料傳輸至非歐洲經濟區（EEA, European Economic Area）成員之國家時，該個人資料將獲得適當等級之保護。
控制措施	無。
說明	◆ 當組織將個人資料傳輸至非歐洲經濟區成員之國家時，PIMS應制訂相關程序以確保當事人之權力仍受到保護，例如： a) 藉由契約條款以確保資料的保護及處理方式，如使用標準契約（model contracts）或受到共同約束條款（BCR, binding corporate rule）的管理； b) 若將資料傳輸至美國境內，即必須遵循美國隱私權豁免原則（Safe Harbor）； c) 經歐洲委員會（European Commission）評估過，該國家或地區已具備完善的資料保護機制；及 d) 由其它組織處理其個人資料時，可於該組織中實施實質審查（Due Diligence）。 ◆ PIMS應制訂相關程序，以確保負遵循資料保護法令與最佳實務之責的同仁（參見4.1.2），於個人資料初次傳輸至非歐洲經濟區成員之國家時，執行審核作業。此審核作業則為確保該傳輸行為已受到良善的保護。 ◆ PIMS應制訂相關程序，以確保當由承包商代表該組織執行個人資料處理作業時，且該承包商非為歐洲經濟區成員，其皆應遵循由歐洲委員會（European Commission）為個人資料保護所要求的標準契約，除非另有其他適當的程序可保護。

29

4.15 揭露予第三方

控制目標	為確保揭露個人資料予第三方之相關作業皆可遵循資料保護法令及最佳實務之要求。
控制措施	無。
說明	◆ PIMS應制訂相關程序以確保第三方可提出下列之證據： a) 其存取個人資料之權利；及 b) 必要時提出其第三方身分識別資料。 ◆ PIMS應制訂相關程序，以確保組織已檢核其揭露個人資料予第三方之作業是依法有據，並僅揭露最少數量之個人資料予第三方。 ◆ PIMS應制訂相關程序，以維護揭露個人資料予第三方之作業紀錄。該紀錄中應證實其揭露作業為合法行為，且應使組織掌握其個人資料之揭露動態。 ◆ 若第三方已經法令核准且授權可存取個人資料，如資訊公開法（Freedom of Information Act 2000），那麼對於第三方之身份識別或確認最少化數量之揭露程序即可免除。

30

4.16 轉包處理

控制目標	為確保揭露個人資料予第三方之相關作業皆可遵循資料保護法令及最佳實務之要求。
控制措施	無。
說明	◆ PIMS應制訂相關程序，以確保當個人資料交由其它組織處理時： a) 該組織僅選擇在技術面、實體面及組織面皆可提供符合組織對個人資料保護需求之第三方廠商； b) 於其它組織處理個人資料前，評估其實行之安控措施，以做為實質審查（Due Diligence）的一部分。此外，組織也可視情況於簽定契約前對該組織之安控措施實行稽核作業，其情況可考量欲處理之個人資料的特性或於特殊情況下處理個人資料； c) 一旦選定第三方廠商後，組織應與其簽訂正式之書面協議，以確保履行契約的過程中，第三方廠商在處理個人資料時，可供適當之控管措施； d) 於第三方廠商獲得存取個人資料權限之期間，組織與第三方廠商所簽訂之契約中，應保留對其安控措施之稽核權； e) 若該第三方廠商欲進一步將個人資料處理作業再進行轉包，其得依據契約的條款取得組織之許可。 f) 若該第三方廠商將個人資料處理作業進行轉包，則其所簽訂之契約亦應要求承接方至少實行與該第三方廠商一樣的安控措施，以及該第三方廠商所要求之條款；及 g) 與第三方廠商所簽訂之契約應明確陳述，當契約終止時，相關之個人資料應被銷毀、交還原組織或其指定之單位。

31

4.17 維護

控制目標	無。
控制措施	無。
說明	◆ PIMS應制訂定相關程序，以確保組織得以持續維護其所制訂的程序及運用的技術之正確性及功能適切性。

32

5.1 內部稽核

控制目標	無。
控制措施	5.1.1內部稽核計畫；5.1.2稽核員的挑選；5.1.3內部稽核需求
說明	◆ 內部稽核計畫 ● 組織應制訂內部稽核程序，以監控及審查處理個人資料過程之有效性，且該程序應被規劃、建立及維護，亦可將個人資料管理政策之考量納入。 ● 內部稽核程序之範圍應涵蓋所有具高風險之個人資料處理流程（參見4.2.2）及所有由其它組織所執行之個人資料處理流程（參見4.16） ◆ 稽核員的挑選 ● 為確保內部稽核之客觀及公平性，組織應選擇適當之稽核員並審慎的執行稽核作業。 ● 大型組織或處理具高風險之個人資料流程（參見4.2.2）可考量定期執行外部稽核。 ◆ 內部稽核需求 ● 內部稽核應依所規劃之時間執行，以確認PIMS是否： a) 依個人資料管理政策及既有之程序執行；及 b) 依技術需求執行及維護之。 ● 稽核報告應詳實說明任何違背政策及程序之事項，並應將之提供予管理階層。 ● 稽核報告亦應識別所有可能會影響政策遵循之技術或程序的議題。

33

5.2 管理審查

控制目標	無。
控制措施	無。
說明	◆ 組織應執行PIMS之管理審查，其執行頻率可為定期、於預先安排的期間或發生重大變更時，以確保該體制得以持續維持其適當及有效性。 ◆ PIMS之管理審查應依據： a) 來自PIMS使用者之回饋； b) 由組織人於所辨識及提升之風險； c) 稽核結果； d) 程序審查之紀錄； e) 資訊技術提升及替換之結果； f) 來自主管機關評估後之正式要求； g) 抱怨事件的處理；及 h) 已發生之資安事故及資料外洩事件。 ◆ 管理審查應提供所有可能造成PIMS變更之詳細資訊，其資料來源可為政策的調整、可能影響作業遵循之程序與技術。 ◆ 當PIMS發生重大變更後，應立即執行稽核作業。

34

6.1 矯正與預防措施

控制目標	無。
控制措施	6.1.1概述；6.1.2預防措施；6.1.3矯正措施
說明	◆ 概述 ● 組織應藉由實行適當之矯正及預防措施，以持續改進PIMS。 ● 所有被提出之變更及改善建議皆應於執行前進行評估，以確保其符合政策之需求。 ● 應審查所有可能影響資料保護法令或最佳實務之遵循的變更，例如將個人資料轉換為新的儲存格式，以確認法令遵循的影響程度。 ● 由矯正與預防措施所引發之變更應加以記錄，並依其保存期限保留相關之紀錄。 ◆ 預防措施 ● 組織應採取措施以消除潛在不符合之原因，並防止其發生，故組織應制訂相關程序，以： a) 識別潛在不符合事項及其原因； b) 決定與實作所需之預防措施； c) 記錄及審查所採取措施之結果； d) 識別已變更之風險；及 e) 確保所有應瞭解該潛在不符合原因及預防措施之人員皆瞭解。

35

6.1 矯正與預防措施

說明	◆ 矯正措施 ● 組織應制訂相關程序，於發生不符合事項時，組織得檢視各項不符合事項，並依風險評鑑作業，以： a) 消除不符合事項之原因； b) 降低不符合事項之風險等級；或 c) 經風險評鑑後，評估其不符合事項之風險調降並不適當，則需將該情況加以詳細記錄之。 ● 風險評鑑作業應定期執行確認風險是否改變且不符合事項需要予以矯正（參見4.4）。 ● 組織應確保所有新辨識風險到個人資料(無論是從組織內部或在更廣泛的國家觀點)使用主動評估程序如個人隱私衝擊分析。

36

6.2 持續改善

控制目標	無。
控制措施	無。
說明	◆ 組織應藉由稽核結果、矯正與預防措施及管理階層審查，以持續改進PIMS之有效性。 ◆ 抱怨事件、資安事故、本人申請閱覽（subject access request）及其它相關議題皆可促使PIMS有效性之改善。

37

問題與解答