會計師專案查核銀行
個人資料保護之執行程序
及確信報告範例

財團法人
會計研究發展基金會
ACCOUNTING RESEARCH AND DEVELOPMENT FOUNDATION

前言

1. 為配合金融監督管理委員會頒布之「金融控股公司及銀行業內部控制及稽核制度實施辦法」第二十八條第二項之規定：「主管機關得請銀行業委託會計師依主管機關規定辦理個人資料保護與防制洗錢及打擊資恐機制專案查核」，財團法人中華民國會計研究發展基金會組成專案小組，負責研擬會計師專案查核銀行個人資料保護之執行程序及確信報告範例，以供各會計師在執行專案查核及出具確信報告時參考。

2. 會計師辦理前項所述之專案查核時，係依確信準則公報第一號「非屬歷史性財務資訊查核或核閱之確信案件」之規定執行合理確信案件。會計師應對標的及案件情況取得足夠瞭解，俾能辨認及評估標的資訊之重大不實表達風險並針對前述重大不實表達風險設計及執行程序，以取得合理確信並作出結論。

3. 會計師專案查核銀行個人資料保護之執行程序及確信報告範例之編寫內容係供各會計師參考。各會計師應考量受查銀行之實際作業及風險後，依其專業判斷，擬訂執行程序並出具合宜之確信報告。

4. 本範例係由財團法人中華民國會計研究發展基金會邀集中華民國銀行商業同業公會全國聯合會、安永聯合會計師事務所、安侯建業聯合會計師事務所、資誠聯合會計師事務所、勤業眾信聯合會計師事務所組成工作小組擬訂初稿後，邀集產官學界代表組成初審及覆審委員會召開審查會議，並彙集外界意見且充分討論後定稿。

5. 本專案小組成員如下：

召集人	財團法人中華民國會計研究發展基金會董事長	王怡心
覆審委員	國立政治大學會計學系教授	周玲臺
覆審委員	財團法人中華民國會計研究發展基金會企業會計準則委員會主任委員	盧聯生
覆審委員	財團法人中華民國會計研究發展基金會審計準則委員會主任委員	張銘政
覆審委員	華南金控暨華南銀行董事長	吳當傑
覆審委員	滙豐（台灣）商業銀行總經理	李鐘培
覆審委員	中華民國會計師公會全國聯合會理事長	陳富煒
覆審委員	中華民國銀行商業同業公會全國聯合會內部稽核委員會主任委員	胡其相
覆審委員	中華民國會計師公會全國聯合會會計審計委員會主	劉克宜

	任委員	
覆審委員	安永聯合會計師事務所會計師	王金來
覆審委員	安侯建業聯合會計師事務所會計師	于紀隆
覆審委員	資誠聯合會計師事務所會計師	張明輝
覆審委員	勤業眾信聯合會計師事務所會計師	郭政弘
初審委員	國立臺灣大學會計學系教授	吳琮璠
初審委員	國立政治大學會計學系教授	林美花
初審委員	中華民國銀行商業同業公會全國聯合會內部稽核委員會主任委員	胡其相
初審委員	安永聯合會計師事務所會計師	張正道
初審委員	安永聯合會計師事務所會計師	謝勝安
初審委員	安永聯合會計師事務所執行副總經理	張騰龍
初審委員	安永聯合會計師事務所協理	高旭弘
初審委員	安侯建業聯合會計師事務所會計師	吳麟
初審委員	安侯建業聯合會計師事務所會計師	王勇勝
初審委員	安侯建業聯合會計師事務所會計師	尹元聖
初審委員	安侯建業聯合會計師事務所協理	林其侯
初審委員	安侯建業聯合會計師事務所協理	黃鈺珺
初審委員	安侯建業聯合會計師事務所協理	郭宇帆
初審委員	資誠聯合會計師事務所會計師	黃金澤
初審委員	資誠聯合會計師事務所會計師	紀淑梅
初審委員	資誠聯合會計師事務所副總經理	羅蕉森
初審委員	資誠聯合會計師事務所協理	蔡旻霓
初審委員	資誠聯合會計師事務所經理	林郁文
初審委員	勤業眾信聯合會計師事務所會計師	陳盈州
初審委員	勤業眾信聯合會計師事務所執行副總經理	陳嘉祥
初審委員	勤業眾信聯合會計師事務所副總經理	侯玉燁
初審委員	勤業眾信聯合會計師事務所協理	黃菽芳
初審委員	勤業眾信聯合會計師事務所協理	潘麗如
初審委員	勤業眾信聯合會計師事務所協理	江榮倫
初審委員	勤業眾信聯合會計師事務所協理	劉曉軒
初審委員	勤業眾信聯合會計師事務所經理	陳鴻棋

目錄

會計師專案查核銀行個人資料保護之執行程序

銀行個人資料保護之確信報告範例

會計師專案查核銀行個人資料保護之執行程序

控制重點	相關規定	執行程序
1. 個人資料保護之規劃		
1.1 銀行應依其業務規模及特性，衡酌經營資源之合理分配，配置管理之人員及相當資源，以： 1.1.1 規劃、訂定、修正與執行其個人資料檔案安全維護計畫，及業務終止後個人資料處理方法。 1.1.2 上述計畫及處理方法應經銀行常務董（理）事會決議或經其授權之經理部門核定。	【個人資料保護法】(以下簡稱【個資法】)第 27 條 【個人資料保護法施行細則】(以下簡稱【個資法施行細則】）第 12 條 【金融監督管理委員會指定非公務機關個人資料檔案安全維護辦法】（以下簡稱【檔案安全維護辦法】）第 3 條	1. 取得銀行之個人資料檔案安全維護計畫及業務終止後個人資料處理方法，檢查其是否符合法令規定。 2. 詢問銀行相關權責人員，瞭解銀行個人資料保護相關組織、責任分配及人員配置，並評估是否有明顯不足情形。 3. 檢查上述計畫及處理方法是否經適當層級授權，如有修正亦經其核准。
1.2 銀行應依個人資料保護相關法令，定期查核確認所保有之個人資料現況，界定其納入個人資料檔案安全維護計畫及業務終止後個人資料處理方法之範圍。	【個資法】第 27 條 【個資法施行細則】第 12 條 【檔案安全維護辦法】第 4 條	1. 取得銀行個人資料蒐集之相關政策、程序及個人資料清冊。 2. 詢問相關權責人員並檢查上述資料及銀行執行定期查核之相關紀錄，以確認： (1) 銀行是否定期確認所保有個人資料之現況。 (2) 銀行是否依據所確認之個人資料現況，界定其

控制重點	相關規定	執行程序
		納入個人資料檔案安全維護計畫及業務終止後個人資料處理方法之範圍。
1.3 銀行應依【檔案安全維護辦法】第4條界定之個人資料範圍及其業務涉及個人資料蒐集、處理、利用之流程，評估可能產生之個人資料風險，並根據風險評估之結果訂定適當之管理機制。	【個資法】第 27 條 【個資法施行細則】第 12 條 【檔案安全維護辦法】第 5 條	1. 檢查銀行是否對個人資料進行風險評估並適時更新。 2. 檢查銀行是否根據風險評估結果訂定相關管理機制，並評估該等機制是否適當。
1.4 銀行為因應個人資料之竊取、竄改、毀損、滅失或洩漏等安全事故（以下簡稱事故），應訂定下列應變、通報及預防機制： 1.4.1 事故發生後應採取之各類措施，包括： 1.4.1.1 控制當事人損害之方式。 1.4.1.2 查明事故後通知當事人之適當方式。 1.4.1.3 應通知當事人事故事實、所為因應措施及諮詢服務專線等內容。 1.4.2 事故發生後應受通報之對象及其通報方式。 1.4.3 事故發生後，其矯正預防措施之	【個資法】第 12 條及第 27 條 【個資法施行細則】第 12 條及第 22 條 【檔案安全維護辦法】第 6 條	1. 取得銀行訂定之個人資料事故應變、通報及預防機制及相關政策程序。 2. 檢查前述程序之內容是否包含控制重點所列之各項目。 3. 詢問銀行相關權責人員以瞭解查核年度是否有相關事故發生，如有相關事故發生，則抽核檢查其是否依據相關規範執行通報及處置，矯正預防措施之研議是否符合規定。 4. 檢查銀行是否定期執行個資事件通報演練並留存相關紀錄。

控制重點	相關規定	執行程序
研議機制。 銀行遇有重大個人資料事故者，應即通報主管機關；其所研議之矯正預防措施，並應經公正、獨立且取得相關公認認證資格之專家，進行整體診斷及檢視。		
1.5 銀行應定期對所屬人員，施以個人資料保護認知宣導及教育訓練，使其明瞭相關法令之要求、所屬人員之責任範圍與各種個人資料保護事項之機制、程序及措施。	【個資法】第 27 條 【個資法施行細則】第 12 條 【檔案安全維護辦法】第 7 條	1. 取得銀行對個人資料保護進行之宣導及教育訓練計畫並評估該計畫是否包括可確認銀行所屬人員瞭解相關法令之要求、其責任範圍與各種個人資料保護事項之機制、程序及措施之方法（例如訓練後測驗）。 2. 取得年度教育訓練及宣導紀錄並抽核檢查銀行是否依據教育訓練及宣導計畫執行。
2. 個人資料之管理程序及措施		
2.1 銀行應訂定個人資料之管理程序，針對蒐集、處理或利用之個人資料包含特種個人資料者（病歷、醫療、基因、性生活、健康檢查及犯罪前科），確保其特定目的符合相關法令之要件；其經當事人書面同意者，並應確保符合【個資法】第6條第二項準用第7條第一項、第二項及第四項之規定。	【檔案安全維護辦法】第 8 條第一項第一款 【個資法】第 6 條、第 7 條、第 19 條及第 20 條 【個資法施行細則】第 4 條	1. 取得銀行訂定有關特種個人資料蒐集、處理或利用之管理程序，並評估其是否適當。 2. 抽核檢查個人資料清冊中包含有特種個人資料之檔案，確認其特定目的是否符合相關法令之要件。 3. 針對上述抽核之樣本，其經當事人書面同意者，並應檢查是否符合【個資法】第 6 條第二項準用第 7 條第一項、第二項及第四項之規定。
2.2 銀行應訂定個人資料之管理程序，針對	【檔案安全維護辦法】	1. 取得銀行所訂定有關個人資料蒐集、處理之告知

控制重點		相關規定	執行程序
	個人資料之蒐集及處理，進行告知並確保告知之內容、方式合法妥適。若有免為告知之事由，應符合【個資法】第8條第二項之規範。	第 8 條第一項第二款【個資法】第 8 條、第 9 條	或免告知之管理程序，並評估其是否適當。 2. 詢問銀行相關權責人員，以瞭解前述管理程序之實施情形。 3. 抽核檢查個人資料清冊之個人資料檔案及其相關紀錄，確認銀行是否進行告知，以及告知之內容、方式是否合法妥適。 4. 抽核後如發現有未告知而進行蒐集、處理個人資料之情形，檢查其是否符合【個資法】第 8 條第二項規範免為告知之事由。
2.3	銀行應訂定個人資料之管理程序，針對一般個人資料之蒐集、處理，確保符合【個資法】第19條之規定，具有特定目的並符合【個資法】第19條規定之情形；其經當事人同意者，並應確保符合【個資法】第7條之規定。	【檔案安全維護辦法】第 8 條第一項第三款【個資法】第 7 條、第 19 條	1. 取得銀行所訂定有關一般個人資料蒐集及處理之管理程序，並評估其是否適當。 2. 抽核個人資料清冊之個人資料檔案及其相關紀錄： (1) 針對一般個人資料之蒐集及處理，檢查其是否符合【個資法】第 19 條規定具有特定目的及法定情形。 (2) 如經當事人同意者，檢查其是否符合【個資法】第 7 條之規定。
2.4	銀行應訂定個人資料之管理程序，針對一般個人資料之利用，確保符合【個資法】第20條之規定於蒐集之特定目的必要範圍內為之；若其為特定目的外之利用者，應符合【個資法】第20條規定之	【檔案安全維護辦法】第 8 條第一項第四款【個資法】第 7 條、第 20 條	1. 取得銀行所訂定有關一般個人資料利用之管理程序，並評估其是否適當。 2. 抽核個人資料清冊之個人資料檔案及其相關紀錄： (1) 針對一般個人資料之利用，檢查其是否符合

控制重點	相關規定	執行程序
情形，若經當事人同意者，並應確保符合【個資法】第7條之規定。		【個資法】第 20 條規定蒐集之特定目的必要範圍。 (2) 其為特定目的外之利用者，檢查是否符合【個資法】第 20 條規定之情形，或經當事人同意。 (3) 如經當事人同意者，檢查是否符合【個資法】第 7 條之規定。
2.5 銀行應訂定個人資料之管理程序，針對利用個人資料為行銷，當事人表示拒絕行銷者，立即停止利用其個人資料行銷，並至少於首次行銷時，提供當事人免費表示拒絕接受行銷之方式。	【檔案安全維護辦法】第 8 條第一項第五款	1. 取得銀行所訂定有關利用個人資料為行銷之管理程序，並評估其是否適當。 2. 取得銀行當年度利用個人資料為行銷之紀錄，並抽核檢查： (1) 是否至少於首次行銷時，提供當事人免費表示拒絕接受行銷之方式。 (2) 如當事人表示拒絕行銷者，是否立即停止利用其個人資料行銷。
2.6 銀行應訂定個人資料之管理程序，針對委託他人蒐集、處理或利用個人資料之全部或一部時，對受託人依【個資法施行細則】第8條規定為適當之監督，並於委託契約或相關文件中，明確約定其內容。委託機關應對受託者為適當之監督，其至少應包含下列事項： 2.6.1 預定蒐集、處理或利用個人資料之範圍、類別、特定目的及其期	【檔案安全維護辦法】第 8 條第一項第六款 【個資法施行細則】第 8 條	1. 取得銀行所訂定有關委託他人蒐集、處理或利用個人資料之管理程序，並評估其是否適當。 2. 取得當年度委託他人蒐集、處理或利用個人資料之委託契約或相關文件，並抽核檢查是否包含下列相關內容： (1) 預定蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。 (2) 受託者就【個資法施行細則】第 12 條第二項採取之措施。

控制重點	相關規定	執行程序
間。 2.6.2 受託者就【個資法施行細則】第12條第二項採取之措施。 2.6.3 有複委託者，其約定之受託者。 2.6.4 受託者或其受僱人違反【個資法】、其他個人資料保護法律或其法規命令時，應向委託機關通知之事項及採行之補救措施。 2.6.5 委託機關如對受託者有保留指示者，其保留指示之事項。 2.6.6 委託關係終止或解除時，個人資料載體之返還，及受託者履行委託契約以儲存方式而持有之個人資料之刪除。 銀行應定期確認受託者執行之狀況，並將確認結果記錄之。 受託者僅得於委託機關指示之範圍內，蒐集、處理或利用個人資料。 受託者認委託機關之指示有違反【個資法】、其他個人資料保護法律或其法規命令者，應立即通知委託機關。		(3) 有複委託者，其約定之受託者。 (4) 受託者或其受僱人違反【個資法】、其他個人資料保護法律或其法規命令時，向委託機關通知之事項及採行之補救措施。 (5) 委託機關如對受託者有保留指示者，其保留指示之事項。 (6) 委託關係終止或解除時，個人資料載體之返還，及受託者履行委託契約以儲存方式而持有之個人資料之刪除。 3. 查詢銀行是否定期確認受託者執行狀況並抽核檢查相關紀錄，以確認： (1) 銀行是否定期確認受託者執行之狀況，並將確認結果記錄之。 (2) 受託者是否僅於委託機關指示之範圍內，蒐集、處理或利用個人資料。 (3) 受託者認委託機關之指示有違反【個資法】、其他個人資料保護法律或其法規命令者，是否立即通知委託機關。
2.7 銀行應訂定個人資料之管理程序，確保銀行於進行個人資料國際傳輸前，檢視	【檔案安全維護辦法】第 8 條第一項第七款	1. 取得銀行所訂定有關進行個人資料國際傳輸之管理程序，並評估其是否適當。

控制重點	相關規定	執行程序
是否受主管機關限制並遵循之。	【個資法】第 21 條	2. 抽核檢查銀行於進行個人資料國際傳輸前，有無依程序檢視是否受主管機關限制並遵循之。
2.8 銀行應針對當事人行使【個資法】第3條所定權利之下列相關事項訂定管理程序： 2.8.1 當事人身分之確認。 2.8.2 提供當事人行使權利之方式，並告知所需支付之費用，及應釋明之事項。 2.8.3 對當事人請求之審查方式，並遵守【個資法】有關處理期限之規定。 2.8.4 有【個資法】所定得拒絕當事人行使權利之事由者，其理由記載及通知當事人之方式。	【個資法】第 3 條、第 10 條、第 14 條 【檔案安全維護辦法】第 8 條第一項第八款	1. 取得銀行所訂定有關當事人行使【個資法】第 3 條所定權利之管理程序，並評估其是否適當。 2. 取得當事人行使【個資法】第 3 條所定權利之申請紀錄，並抽核檢查： (1) 是否確認當事人身分。 (2) 是否提供當事人行使權利之方式，並告知所需支付之費用，及應釋明之事項。 (3) 對當事人請求之審查方式，是否遵守【個資法】有關處理期限之規定。 (4) 有【個資法】所定得拒絕當事人行使權利之事由者，是否依程序記載其理由並通知當事人。
2.9 銀行受理當事人依【個資法】第10條規定之請求，應於十五日內，為准駁之決定；必要時，得予延長，延長之期間不得逾十五日，並應將其原因以書面通知請求人。	【個資法】第 10 條、第 13 條第一項	1. 取得銀行個人資料之管理程序，並檢查其內容是否包含銀行受理當事人依【個資法】第 10 條規定之請求之相關程序與其遵法性。 2. 取得當年度受理當事人請求之相關紀錄並抽核檢查其是否依據管理程序辦理相關作業。
2.10 銀行受理當事人依【個資法】第11條規定之請求，應於三十日內，為准駁之決定；必要時，得予延長，延長之期間不	【個資法】第 11 條、第 13 條第二項	1. 取得銀行個人資料之管理程序，並檢查其內容是否包含銀行受理當事人依【個資法】第 11 條規定之請求之相關程序與其遵法性。

控制重點	相關規定	執行程序
得逾三十日，並應將其原因以書面通知請求人。		2. 取得當年度受理當事人請求之相關紀錄並抽核檢查其是否依據管理程序辦理相關作業。
2.11 銀行應訂定個人資料之管理程序，確保個人資料於蒐集、處理或利用過程中之正確性；其有不正確或正確性有爭議者，應依【個資法】第11條第一項、第二項及第五項規定辦理。	【檔案安全維護辦法】第 8 條第一項第九款 【個資法】第 11 條	1. 取得銀行個人資料之管理程序，並檢查其內容是否包含個人資料於蒐集、處理或利用過程中是否正確之檢查程序，以及個人資料有不正確或正確性有爭議者之相關處理程序與其遵法性。 2. 取得當年度受理當事人請求之相關紀錄並抽核檢查其是否依據管理程序辦理相關作業。
2.12 銀行應訂定個人資料之管理程序，包括檢視所保有個人資料之特定目的是否消失，或期限是否屆滿；其特定目的消失或期限屆滿者，應依【個資法】第11條第三項規定刪除、停止處理或利用。	【檔案安全維護辦法】第 8 條第一項第十款 【個資法】第 11 條	1. 取得銀行個人資料之管理程序，並檢查其內容是否包含檢視所保有個人資料之特定目的是否消失或期限是否屆滿之程序，以及其特定目的消失或期限屆滿者，相關刪除、停止處理或利用之程序與其遵法性。 2. 取得當年度刪除、停止處理或利用之相關紀錄並抽核檢查銀行是否依管理程序辦理相關作業。
2.13 銀行為維護所保有個人資料之安全，應採取下列資料安全管理措施： 2.13.1 訂定各類設備或儲存媒體之使用規範，及報廢或轉作他用時，應採取防範資料洩漏之適當措施。 2.13.2 針對所保有之個人資料內容，有加密之需要者，於蒐集、處理或	【檔案安全維護辦法】第 9 條	1. 取得銀行個人資料之管理程序，並檢查該程序是否訂定下列之適當資料安全管理措施： (1) 各類設備或儲存媒體之使用規範、報廢或轉作他用之規範。 (2) 針對所保有之個人資料內容，如有加密之需要者，於蒐集、處理或利用時，應採取之適當加密措施。 (3) 作業過程有備份個人資料之需要時，對備份資料

控制重點	相關規定	執行程序
利用時，採取適當之加密措施。 2.13.3 作業過程有備份個人資料之需要時，對備份資料予以適當保護。		予以適當保護之控管措施。 2. 取得當年度各控管措施之相關紀錄並抽核檢查銀行是否依管理程序辦理相關作業。
2.14 銀行若提供電子商務服務系統(指透過網際網路進行有關商品或服務之廣告、行銷、供應、訂購或遞送等各項商業交易活動)，應採取下列資訊安全措施： 2.14.1 使用者身分確認及保護機制。 2.14.2 個人資料顯示之隱碼機制。 2.14.3 網際網路傳輸之安全加密機制。 2.14.4 應用系統於開發、上線、維護等各階段軟體驗證與確認程序。 2.14.5 個人資料檔案及資料庫之存取控制與保護監控措施。 2.14.6 防止外部網路入侵對策。 2.14.7 非法或異常使用行為之監控與因應機制。	【檔案安全維護辦法】第 10 條第一項	1. 查詢銀行權責人員，瞭解銀行是否提供電子商務服務系統。 2. 如銀行有提供電子商務服務系統，取得銀行有關電子商務系統之相關資訊安全措施程序文件規範，並檢查其內容是否包含下列各項： (1) 使用者身分確認及保護機制。 (2) 個人資料顯示之隱碼機制。 (3) 網際網路傳輸之安全加密機制。 (4) 應用系統於開發、上線、維護等各階段軟體驗證與確認程序。 (5) 個人資料檔案及資料庫之存取控制與保護監控措施。 (6) 防止外部網路入侵對策。 (7) 非法或異常使用行為之監控與因應機制。 3. 取得當年度資訊安全措施之相關紀錄並抽核檢查銀行是否依管理程序辦理相關作業。
2.15 銀行針對電子商務服務系統所採取之下列安全措施，應定期演練及檢討改善：	【檔案安全維護辦法】第 10 條第三項	1. 查詢銀行權責人員，瞭解銀行是否提供電子商務服務系統。 2. 如銀行有提供電子商務服務系統，取得銀行電子

控制重點	相關規定	執行程序
2.15.1 防止外部網路入侵對策。 2.15.2 非法或異常使用行為之監控與因應機制。		商務系統之相關資訊安全措施程序文件規範，並檢查其內容是否包含防止外部網路入侵對策及非法或異常使用行為之監控與因應機制。 3. 取得當年度演練之紀錄，檢查是否依所訂定之程序進行演練；對於需改進事項，檢查是否有相關檢討改善狀況之紀錄。
2.16 銀行保有之個人資料存在於紙本、磁碟、磁帶、光碟片、微縮片、積體電路晶片、電腦、自動化機器設備或其他媒介物者，應採取下列設備安全管理措施： 2.16.1 實施適宜之存取管制。 2.16.2 訂定妥善保管媒介物之方式。 2.16.3 依媒介物之特性及其環境，建置適當之保護設備或技術。	【檔案安全維護辦法】第 11 條	1. 取得銀行保有個人資料之設備安全管理措施，並檢查其內容是否包含存取管制、妥善保管媒介物及建置適當之保護設備或技術等機制。 2. 取得當年度設備安全管理相關紀錄並抽核檢查銀行是否依管理程序辦理相關作業。
2.17 銀行應依執行業務之必要，設定相關人員接觸個人資料之權限及控管其接觸情形，並與所屬人員約定保密義務。	【檔案安全維護辦法】第 12 條	1. 取得銀行管理其人員接觸個人資料之相關程序及其與所屬人員約定保密個人資料義務之相關文件。 2. 檢查銀行是否依業務需要設定相關人員接觸個人資料之權限及控管其接觸情形。 3. 取得銀行當年度接觸個人資料之人員清單。 4. 抽核檢查當年度人員確認或簽署其瞭解保密義務之相關紀錄以確認是否依相關規定辦理。

控制重點	相關規定	執行程序
2.18 銀行若違反【個資法】之規定，致個人資料被竊取、洩漏、竄改或其他侵害者，應查明後以適當方式通知當事人。	【個資法】第 12 條	1. 取得銀行通知當事人個人資料被竊取、洩漏或竄改之相關程序。 2. 抽核檢查當年度通知當事人之相關紀錄，並確認其妥適性。
2.19 銀行之國外分支機構有對個人資料蒐集、處理或利用者，其應要求建立適當之治理機制，以確保其國外分支機構依據【個資法】第51條第2項建立適當之內部控制制度，以遵循國內【個資法】之要求。	【個資法】第 51 條第 2 項 【金融控股公司及銀行業內部控制及稽核制度實施辦法】第 8 條第 9 項	1. 詢問相關權責人員並檢查對個人資料保護之內部控制之相關文件，瞭解銀行之國外分支機構蒐集個人資料之情形及範圍。 2. 檢查及瞭解銀行是否針對國外分支機構之個人資料管理建立治理機制，包括： (1) 銀行是否要求國外分支機構依據國內【個資法】建立相關政策及程序，並有相對應之組織、責任分配與人員。 (2) 上述政策程序是否包含要求國外分支機構定期與銀行溝通及報告個人資料之管理情形。 (3) 國外分支機構是否定期自行評估個人資料相關內部控制制度設計及執行之有效性，並將其結果及改善情形回報。 (4) 內部稽核單位是否定期查核國外分支機構之個人資料保護內部控制制度實施情形，並追蹤其改善結果。 3. 抽核檢查上述相關治理機制之執行紀錄，以確認銀行對國外分支機構個人資料管理之治理機制是否適當執行。

控制重點	相關規定	執行程序
3. 個人資料之安全稽核、紀錄保存及持續改善機制		
3.1 銀行應依業務規模及特性，衡酌經營資源之合理分配，訂定適當之個人資料安全稽核機制，並將相關機制列入內部控制及稽核項目。	【檔案安全維護辦法】第 13 條	1. 取得銀行有關個人資料安全稽核之相關程序規範，並檢查個人資料安全稽核項目之妥適性。 2. 抽核檢查當年度稽核紀錄以確認其落實性及相關稽核發現改善狀況。
3.2 銀行依法令規定執行各種個人資料保護機制、程序及措施，應記錄其個人資料使用情況，留存軌跡資料或相關證據。	【檔案安全維護辦法】第 14 條第一項	1. 取得當年度執行各種個人資料保護機制、程序及措施之相關紀錄，抽核檢查銀行是否依據其機制、程序及措施辦理相關作業。
3.3 銀行依【個資法】第11條第三項規定刪除、停止處理或利用所保有之個人資料後，應留存下列紀錄： 3.3.1 刪除、停止處理或利用之方法、時間。 3.3.2 將刪除、停止處理或利用之個人資料移轉其他對象者，其移轉之原因、對象、方法、時間，及該對象蒐集、處理或利用之合法依據。 3.3.3 前述之軌跡資料、相關證據及紀錄，應至少留存五年。若法令另有規定或契約另有約定者，不在	【個資法】第 11 條 【檔案安全維護辦法】第 14 條第二項	1. 取得銀行所訂定其依法令規定刪除、停止處理或利用所保有之個人資料後留存證據及紀錄之機制，並檢查其內容是否符合個人資料保護相關法令之要求及其遵法性。 2. 取得當年度相關證據及紀錄，抽核檢查銀行是否依據上述機制辦理。 3. 抽核檢查相關之證據及紀錄是否保留至少五年。

控制重點	相關規定	執行程序
此限。		
3.4 銀行應針對個人資料安全維護定期提出相關自我評估報告，並訂定下列機制： 3.4.1 檢視、修訂個人資料檔案安全維護計畫及業務終止後個人資料處理方法等相關個人資料保護事項。 3.4.2 針對評估報告中有違反法令之虞者，規劃、執行改善及預防措施。 自我評估報告應經銀行董（理）事會、常務董（理）事會決議或經其授權之經理部門核定。若銀行為外國在臺分行、分公司，或未設董（理）事會者，應經其負責人簽署。	【檔案安全維護辦法】第 15 條	1. 取得銀行當年度個人資料安全維護自我評估報告，並檢查其內容是否包含檢視、修訂個人資料檔案安全維護計畫及業務終止後個人資料處理方法等相關個人資料保護事項。如有違反法令之虞者，是否規劃、執行改善及預防措施。 2. 檢查自我評估報告是否經由銀行董（理）事會、常務董（理）事會決議或經其授權之經理部門核定。

銀行個人資料保護之確信報告範例

注意事項：

執業人員可選擇以「短式」或「長式」報告與預期使用者溝通。「短式」報告通常僅包含基本要素，「長式」報告則包含其他不影響執業人員結論之資訊及說明。除基本要素外，長式報告尚可能包含對案件條款與適用基準之詳細說明、與案件特定層面有關之發現、參與案件之執業人員及其他人員之資格及經歷、重大性之揭露及建議（如適用時）。執業人員於編製報告時，宜考量該等資訊之提供就預期使用者之資訊需求而言是否重要。額外資訊應與執業人員之結論明確區分，且其用語應能使預期使用者瞭解該等資訊不影響執業人員之結論。

情況一　對銀行個人資料保護內部控制制度之設計及執行有效性之聲明書所出具無保留結論之確信報告

於此範例中，假設：

1. 會計師係執行合理確信案件。
2. 管理階層對個人資料保護內部控制制度之設計及執行係為有效出具聲明書。
3. 會計師已將海外分（子）行納入執行程序之範圍。
4. 會計師依據所取得之證據，作成無保留結論。

會計師確信報告

XX 商業銀行股份有限公司　公鑒：

XX 商業銀行股份有限公司對民國 XX 年度個人資料保護內部控制制度之設計及執行情形所出具之聲明書，業經本會計師執行必要程序竣事。

確信標的資訊與適用基準

本確信案件之標的資訊係貴公司對民國 XX 年度個人資料保護內部控制制度之設計及執行係為有效所出具之聲明書（以下稱「標的資訊」），詳附件。

用以衡量或評估上開標的資訊之適用基準係「個人資料保護法」、「個人資料保護法施行細則」，以及「金融監督管理委員會指定非公務機關個人資料檔案安全維護辦法」。

先天限制

由於任何個人資料保護內部控制制度均有其先天上之限制，故貴公司上述內部控制制度仍可能未能預防或偵測出業已發生之錯誤或舞弊。此外，未來之環境可能變遷，遵循內部控制制度之程度亦可能降低，故在本期有效之內部控制制度，並不表示在未來亦必有效。

管理階層之責任

管理階層之責任係依據個人資料保護相關法令與指引，訂定相關政策及程序，建立內部控制制度，並由超然獨立之稽核部門執行查核，定期呈報董事會，確認有關個人資料保護之內部控制均能確實有效執行。

會計師之責任

本會計師係依照確信準則公報第一號「非屬歷史性財務資訊查核或核閱之確信案件」對標的資訊執行必要程序以取得合理確信，並對標的資訊在所有重大方面是否允當表達表示意見。

獨立性及品質管制規範

本會計師及所隸屬會計師事務所已遵循會計師職業道德規範中有關獨立性及其他道德規範之規定，該規範之基本原則為正直、公正客觀、專業能力及盡專業上應有之注意、保密及專業態度。此外，本會計師所隸屬會計師事務所遵循審計準則公報第四十六號「會計師事務所之品質管制」，維持完備之品質管制制度，包含與遵循職業道德規範、專業準則及所適用法令相關之書面政策及程序。

所執行程序之彙總說明

本會計師係基於專業判斷規劃及執行必要程序，以獲取相關標的資訊之證據。所執行之程序包括評估貴公司個人資料保護之控制環境及風險，並針對相關紀錄執行測試、檢查、觀察或查詢。

確信結論

依本會計師之意見，貴公司對民國 XX 年度個人資料保護內部控制制度之設計及執行情形所出具之聲明書，在所有重大方面係允當表達。

其他事項

本確信報告出具後，本會計師不負更新本確信報告之責任。

使用限制

本確信報告僅供貴公司依「金融控股公司及銀行業內部控制及稽核制度實施辦法」之規定申報主管機關使用，不得作為其他用途或分送其他人士。

××會計師事務所
會計師：（簽名及蓋章）
××會計師事務所地址：
中華民國××年×月×日

註：若海外分（子）行未納入執行程序之範圍，會計師應考量是否出具保留結論或無法表示結論之確信報告。

情況二　對銀行遵循個人資料保護相關法令之情形，出具無保留結論之確信報告

於此範例中，假設：

1. 會計師係執行合理確信案件。
2. 管理階層未對個人資料保護內部控制制度之設計及執行出具聲明書。
3. 會計師已將海外分（子）行納入執行程序之範圍。
4. 依據所取得之證據，會計師就銀行個人資料保護內部控制制度之設計及執行是否遵循相關法令，作成無保留結論。

會計師確信報告

XX 商業銀行股份有限公司　公鑒：

XX 商業銀行股份有限公司民國 XX 年度個人資料保護內部控制制度之設計及執行，業經本會計師執行必要程序竣事。

確信標的與適用基準

本確信案件之標的係貴公司民國 XX 年度個人資料保護內部控制制度之設計及執行。

用以衡量或評估上開標的之適用基準係「個人資料保護法」、「個人資料保護法施行細則」，以及「金融監督管理委員會指定非公務機關個人資料檔案安全維護辦法」。

先天限制

由於任何個人資料保護內部控制制度均有其先天上之限制，故貴公司上述內部控制制度仍可能未能預防或偵測出業已發生之錯誤或舞弊。此外，未來之環境可能變遷，遵循內部控制制度之程度亦可能降低，故在本期有效之內部控制制度，並不表示在未來亦必有效。

管理階層之責任

管理階層之責任係依據個人資料保護相關法令與指引，訂定相關政策及程序，建立內部控制制度，並由超然獨立之稽核部門執行查核，定期呈報董事會，確認有關個人資料保護之內部控制均能確實有效執行。

會計師之責任

本會計師係依照確信準則公報第一號「非屬歷史性財務資訊查核或核閱之確信案件」對標的執行必要程序以取得合理確信，並對個人資料保護內部控制制度之設計及執行在所有重大方面是否遵循適用基準表示意見。

獨立性及品質管制規範

本會計師及所隸屬會計師事務所已遵循會計師職業道德規範中有關獨立性及其他道德規範之規定，該規範之基本原則為正直、公正客觀、專業能力及盡專業上應有之注意、保密及專業態度。此外，本會計師所隸屬會計師事務所遵循審計準則公報第四十六號「會計師事務所之品質管制」，維持完備之品質管制制度，包含與遵循職業道德規範、專業準則及所適用法令相關之書面政策及程序。

所執行程序之彙總說明

本會計師係基於專業判斷規劃及執行必要程序，以獲取相關標的之證據。所執行之程序包括評估貴公司個人資料保護之控制環境及風險，並針對相關紀錄執行測試、檢查、觀察或查詢。

確信結論

依本會計師之意見，貴公司民國 XX 年度個人資料保護內部控制制度之設計及執行在所有重大方面已遵循「個人資料保護法」、「個人資料保護法施行細則」，以及「金融監督管理委員會指定非公務機關個人資料檔案安全維護辦法」。

其他事項

本確信報告出具後，本會計師不負更新本確信報告之責任。

使用限制

本確信報告僅供貴公司依「金融控股公司及銀行業內部控制及稽核制度實施辦法」之規定申報主管機關使用，不得作為其他用途或分送其他人士。

××會計師事務所
會計師：（簽名及蓋章）
××會計師事務所地址：
中華民國××年×月×日

註：若海外分（子）行未納入執行程序之範圍，會計師應考量是否出具保留結論或無法表示結論之確信報告。

情況三　對銀行所出具整體內部控制制度聲明書中，有關個人資料保護內部控制制度之設計及執行係為有效之聲明，出具保留結論之確信報告

於此範例中，假設：

1. 會計師係執行合理確信案件。
2. 管理階層係出具整體內部控制制度聲明書，而未對個人資料保護內部控制制度之設計及執行出具聲明書。
3. 會計師已將海外分（子）行納入執行程序之範圍。
4. 會計師所發現個人資料保護內部控制制度之設計及執行之顯著缺失，其影響重大但非屬廣泛。
5. 依據所取得之證據，會計師就上述聲明書中有關個人資料保護內部控制制度之設計及執行係為有效之聲明，作成保留結論。

會計師確信報告

XX 商業銀行股份有限公司　公鑒：

XX 商業銀行股份有限公司民國 XX 年度之整體內部控制制度聲明書中，有關個人資料保護內部控制制度之設計及執行係為有效之聲明，業經本會計師執行必要程序竣事。

確信標的資訊與適用基準

本確信案件之標的資訊係貴公司民國 XX 年度之整體內部控制制度聲明書（詳附件）中，有關個人資料保護內部控制制度之設計及執行係為有效之聲明（以下稱「標的資訊」）。

用以衡量或評估上開標的資訊之適用基準係「個人資料保護法」、「個人資料保護法施行細則」，以及「金融監督管理委員會指定非公務機關個人資料檔案安全維護辦法」。

先天限制

由於任何個人資料保護內部控制制度均有其先天上之限制，故貴公司上述內部控制制度仍可能未能預防或偵測出業已發生之錯誤或舞弊。此外，未來之環境可能變遷，遵循內部控制制度之程度亦可能降低，故在本期有效之內部控制制度，並不表示在未來亦必有效。

管理階層之責任

管理階層之責任係依據個人資料保護相關法令與指引，訂定相關政策及程序，建立內部控制制度，並由超然獨立之稽核部門執行查核，定期呈報董事會，確認有關個人資料保護之內部控制制度均能確實有效執行。

會計師之責任

本會計師係依照確信準則公報第一號「非屬歷史性財務資訊查核或核閱之確信案件」對標的資訊執行必要程序以取得合理確信，並對標的資訊在所有重大方面是否允當表達表示意見。

獨立性及品質管制規範

本會計師及所隸屬會計師事務所已遵循會計師職業道德規範中有關獨立性及其他道德規範之規定，該規範之基本原則為正直、公正客觀、專業能力及盡專業上應有之注意、保密及專業態度。此外，本會計師所隸屬會計師事務所遵循審計準則公報第四十六號「會計師事務所之品質管制」，維持完備之品質管制制度，包含與遵循職業道德規範、專業準則及所適用法令相關之書面政策及程序。

所執行程序之彙總說明

本會計師係基於專業判斷規劃及執行必要程序，以獲取相關標的資訊之證據。所執行之程序包括評估貴公司個人資料保護之控制環境及風險，並針對相關紀錄執行測試、檢查、觀察或查詢。

保留結論之基礎

貴公司個人資料保護內部控制制度之設計及執行於民國 XX 年 XX 月 XX 日仍存有下列顯著缺失：〔敘明顯著缺失內容〕。

前揭顯著缺失未揭示於貴公司民國 XX 年度之整體內部控制制度聲明書。

保留結論

依本會計師之意見，除保留結論之基礎段所述顯著缺失之影響外，貴公司民國 XX 年度之整體內部控制制度聲明書中，有關個人資料保護內部控制制度之設計及執行係為有效之聲明，在所有重大方面係允當表達。

其他事項

本確信報告出具後，本會計師不負更新本確信報告之責任。

使用限制

本確信報告僅供貴公司依「金融控股公司及銀行業內部控制及稽核制度實施辦法」之規定申報主管機關使用，不得作為其他用途或分送其他人士。

××會計師事務所
會計師：（簽名及蓋章）
××會計師事務所地址：
中華民國××年×月×日

註：

1. 若海外分（子）行未納入執行程序之範圍，會計師應考量是否出具保留結論或無法表示結論之確信報告。
2. 若會計師所發現個人資料保護內部控制制度之設計及執行之顯著缺失其影響重大且廣泛，則會計師應出具否定結論之確信報告。