附錄一、國內對巴塞爾電子銀行業務風險管理原則解釋比較

電子銀行業務風險管理原則比較表

Basel 政策指導原則	銀行公會電子銀行風險管理自律規範	銀行業監理會審查分組第二階段研究工作報告
原則一：董事會及高階管理階層應對電子銀行業務所帶來的風險，建立有效的監督管理制度，包括各類風險的說明、風險管理政策及風險控管程序，以有效管理電子銀行業務風險。 一、在進入新的電子銀行業務之前，董事會及高階管理階層應針對該新開業務對銀行現階段之風險架構、經營策略的影響及成本/效益進行分析，並確定銀行具備充分的專業能力以管理此新開業務所帶來之風險。 二、高階管理階層應持續監督可能發生的電子銀行系統問題或是安全漏洞。 三、建立電子銀行業務風險管理之主要授權及通報機制，定期或於必要時將風險管理系統之執行狀況及任何會影響銀行經營及聲譽之緊急突發事件（例如駭客入侵、客戶資料外洩）向董事會及高階管理階層報告。 四、在辦理跨國界	**一、董事會（或常務董事會，下同）及高階管理階層應成立專責單位或指定專人，建立有效風險管理制度，包括風險管理政策及風險控管程序，以有效管理電子銀行業務風險。** 一、對於擬提供新的電子銀行業務或產品，董事會及高階管理階層應確信已對銀行風險概況、經營策略、成本、效益進行分析，並能勝任管理此新開業務所帶來之風險。 二、高階管理階層應持續監督電子銀行系統可能問題或是安全漏洞。 三、應建立電子銀行業務風險管理授權及通報機制（影響銀行經營及聲譽之緊急突發事件，例如駭客入侵、客戶資料外洩），定期或於必要時將風險管理執行狀況及風險承擔情形向董事會及	**原則一：董事會及管理階層須對電子銀行業務所衍生的風險，設立有效管理及監測的機制，包括訂定明確責任歸屬、政策及控管等，以管理相關風險** 一、董事會及高階人員應針對下列電子銀行業務的特性，檢視新種業務對銀行可能的衝擊： 1. 銀行無法掌控電子銀行業務的資料傳輸管道技術（包括網路及資訊科技）的發展。 2. 網路服務，除可能跨越數國的法律管轄範圍，其內容亦包括許多目前實體作業所無法提供的業務。 3. 電子銀行業務涉及大量科技語言及觀念，這與董事會及高階管理者傳統的經驗是有所出入。 二、董事會及管理階層應確認：銀行在引進新

(cross-border)電子銀行業務之前，應先對該相關國之金融相關法規及國家風險，進行嚴謹的分析，並確實的遵守法規及有效的控管風險。	高階管理階層報告。 四、對於有辦理國際性之電子銀行業務，應確信已進行嚴謹的風險分析，並遵守相關國之金融相關法規及規範。	種業務或技術前，已聘有合格的專家，可從事相關風險管理作業。 三、配合電子銀行業務發展，銀行應重新檢視其風險控管流程，並將本項業務之風險控管流程與全行風控機制整合為一。 四、<u>管理階層在從事管理監測時應注意事項：</u> 1. 銀行的風險偏好應與電子銀行業務相契合。 2. 應建立關鍵時刻的人員配置及通報機制，以因應突發事件對銀行可能的影響。 3. 找出與電子銀行業務安全性、整體性及效益等攸關的風險因子，並要求合作的第三者廠商亦應採取同一標準來衡量風險。 4. 確認在進行跨國電子銀行業務前，銀行已完成相關之實地調查及風險分析作業。

原則二：銀行的關鍵性安全控管機制須經董事會及高階管理階層的檢視及認可。 一、建立適當之授權管理、簽入和實體存取安全控制及合適之安全控管設備，以提供內、外部使用者適當之安全介面及限制。 二、有效之安全控管機制應包含： 1. 設置專責人員負責監督銀行安全控管政策的建立及維持。 2. 確實執行簽入及實體安全管制措施，以防止未經授權者對銀行資訊安全所造成的威脅。 3. 定期檢測安全管制措施，包含：持續注意現階段金融業安控機制的最新發展、安控軟體的安裝與升級等。	**二、銀行之關鍵性安全控管機制應經董事會及高階管理階層認可。** 一、建立適當之授權管理、實體存取安全控制及合適之安全控管設備，以提供內、外部使用者適當之安全介面及限制。 二、有效之安全控管機制應包含設置負責監督安控機制之專責人員、落實執行銀行資訊安全政策及定期檢測安全管制措施。	**原則二：董事會及管理階層須審議並核准銀行安全控管措施** 1. 電子銀行業務之安全控管機制包括： 1. 適當的授權機制 2. 邏輯層及實體層的存取控管機制 3. 妥善的安全架構，可有效的區隔銀行內、外部的使用者 2. 管理階層應確認銀行之安控作業已包含下述事項： 1. 指派專人負責審視有關建立/維持銀行的安控政策 2. 有足夠的控管設備，以避免未經授權的實際存取行為發生 3. 有完善的邏輯層面控管及偵測機制，以避免未經授權者擅自入侵應用程式或資料庫 4. 定期檢測安控作業

原則三：董事會及高階管理階層應建立完善且持續嚴謹之監督程序，以管理委外作業廠商及其他第三者所提供之支援電子銀行業務服務。 一、銀行對於其電子銀行系統、運用程式之委外處理者及其他合夥處理者，應該完全瞭解其所帶來之風險。並就其對於銀行的風險結構與風險控管能力所造成的影響，進行持續且完整的評估。 二、在委外及合夥契約簽定之前應詳細審核評估委外作業廠商之專業、信譽及財務能力。 三、合約上應詳細載明委外廠商、合夥廠商、提供服務之第三者之委外或合夥權利義務。 四、對於電子銀行業務委外事項之風險管理、安控機制及資料保密機制，均須符合銀行本身的標準。 五、對於電子銀行業務委外事項要定期實施內部及外部稽核 六、對於電子銀行業務委外事項應建立一套適當之緊急應變計畫。	**三、董事會及高階管理階層應建立全面持續嚴謹之監督程序，以管理委外作業廠商所提供支援電子銀行業務之服務。** 一、銀行對於電子銀行系統及應用程式之委外處理者，應完全瞭解其所帶來之風險。 二、在訂約之前應詳細審核評估委外作業廠商之專業、信譽及財務能力。 三、合約至少應載明下列事項，以確保委外服務品質。 1. 具體之委外事項及內容。 2. 委外作業廠商應建立內部控制機制，定期與不定期進行內部考核，委外事項如有不能履行、履行困難或履行困難之虞者，對於銀行負有立即通知之義務。 3. 銀行於必要時，得於事前通知委外作業廠商後終止契約。 4. 委外作業廠商同意主管機關得依銀行法第四十五條規定辦理。	**原則三：董事會及管理階層須對委外廠商及其他支援電子銀行業務之機構設立完善的監測及管理流程。** 一、對廠商之管控監測範圍，應涵蓋所有的轉包單位。 二、處理委外作業時，僅可能分散委託對象，以免產生風險集中的問題。 三、<u>管理階層監測委外廠商時，應注意下述事項：</u> 1. 銀行已充分了解委外所可能產生的風險 2. 與委外廠商訂約前，銀行應實地了解該公司之作業能力與財務情況 3. 合約內容應明確規範雙方權利義務 4. 要求委外廠商之風險控管作業應與本行採一致 5. 標準定期稽核，且稽核標準應採與銀行自辦該項業務時相同的標準 6. 訂定「緊急事件應變計畫」

	5. 委外作業廠商對外不得以銀行名義辦理受託處理事項。 四、對於電子銀行業務委外事項其風險管理、安控機制及資料保密機制應符合銀行本身的標準。 五、對於電子銀行業務委外事項要定期實施內部及外部稽核。 六、對於電子銀行業務委外事項應建立一套適當之緊急應變計畫。	
原則四:銀行應針對透過網際網路進行業務交易的客戶，建立適當的認證措施、身份辨識及授權機制。 一、顧客原始帳戶之確認是重要的步驟，若未能有適當的認證措施，可能導致非法個人存取電子銀行帳戶，最後導致銀行財物損失及信譽受損。 二、銀行可以採用下列認證措施：PINs、passwords、smart cards、biometrics、digital certificates。同時採用多	**四、銀行應採行適當的認證措施，建立客戶辨識及授權機制，以確保客戶在網際網路上進行該銀行業務交易的安全性。** 一、確認客戶電子銀行帳戶為重要的步驟，若無適當的認證措施，可能導致非法個人存取電子銀行帳戶，進而導致銀行財物及信譽之損失。 二、銀行可以採用下列認證措施：PINs、	**原則四：對於透過網際網路進行交易的客戶，銀行應採取適當措施驗證客戶的身分及交易權限。** 一、在客戶申請帳戶時，應即對其身分進行確認，以降低發生偽冒申請及洗錢等事件。 二、建議銀行採取多重驗證方式來強化網路交易安全性。 三、銀行在決定驗證方式時應考量下列事項： 1. 業務性質 2. 資料儲存的敏感性及價值

種的認證措施，通常能提供較佳的效果。 三、銀行宜採行相關認證及安控措施，以確保下列事項： 1. 運用於存取電子銀行客戶帳號或敏感性系統之認證資料庫，應確保避免被竄改或破壞；而對於企圖竄改或破壞資料之行為，系統應能偵測及留存稽核追蹤紀錄。 2. 凡是新增、刪除或變更個人、代理者、系統之認證資料，均需經過認證辨識及授權。 3. 銀行應有適當措施，保護電子銀行系統之連結，以防不明或不法之第三者取代正常客戶，而使客戶權益受損。 4. 經認證之電子銀行系統連線應全程保持安全性，當發生安全事件時，此類連線應重新認證客戶身份及權限。 四、銀行在決定驗證方式時應考量下列事項： 1. 業務性質 2. 資料儲存的敏感性及價值 3. 客戶操作的難	passwords、smart cards、biometrics、digital certificates 及 OTP(One Time Password)動態密碼。 三、銀行宜採行相關認證及安控措施，以確保下列事項： 1. 運用於存取電子銀行客戶帳號或敏感性系統之認證資料庫，應確保避 免被竄改或破壞；而對於企圖竄改或破壞資料之行為，系統應能偵測及留存稽核追蹤紀錄。 2. 凡是新增、刪除或變更個人、代理者、系統之認證資料，均需經過認證辨識及授權，才可修改認證系統資料庫。 3. 銀行應有適當措施，保護電子銀行系統之連結，以防不明或不法之第三者取代正常客戶，而使客戶權益受損。 4. 經認證之電子銀行系統連線應全程保持安全性，當發生安全事件	3. 客戶操作的難易度 四、跨國交易的客戶身份確認工作，困難度較高。 五、<u>由於驗證技術不斷演進，建議銀行應：</u> 1. 防止儲存驗證資料的資料庫遭竄改或破壞，同時系統應有能力偵測這些異常交易，並將這些紀錄以書面化方式存檔備查。 2. 任何增刪資料庫的動作，須事先取得許可。 3. 銀行應建立適切的評估標準，以控管系統的連續性。 4. 客戶通過驗證後，則交易全程都受保障；惟如逾安全時限，應要求客戶重新取得驗證許可，才得以再進行交易。

易度 五、跨國交易的客戶身份確認工作，困難度較高。	時，此類連線應重新認證客戶身份及權限。	
原則五:銀行應採行交易認證方法，以加強電子銀行交易的不可否認性及建立電子銀行交易的可信度。 一、不可否認性，係為證實原始資訊的傳送者/接收者確曾傳送/接收該訊息,以避免另一 方否認。業者或可採用 PKI（公開金鑰架構);或數位認證、數位簽章等技術來確保電子銀行交易之不可否認性。 二、銀行應依交易類別及交易風險高低建立交易面安全設計，以確保下列事項： 1. 降低有權使用者進行無意的交易之可能性，並讓客戶充分了解交易所伴隨的可能風險。 2. 所有的交易攸關者均應透過認證系統被確認無誤。 3. 財務交易資料應確保無法被更改，且任何更改動作均可被偵測到。	**五、銀行應採行交易認證法，加強電子銀行交易的不可否認性，釐清客我之責任與義務，進而建立客戶與銀行間的互信機制。** 一、銀行應依交易類別及交易風險高低建立交易面安全設計，例如可使用數位簽章、PKI 等機制。 二、電子銀行系統應設計能夠降低有權使用者發出無意的交易，及讓客戶充分了解他們所發出交易所可能帶來的風險；全部交易攸關者應透過認證系統被確認無誤；財務交易資料應確保無法被更改，及任何更改動作是會被偵測到。	**原則五：銀行須使用交易認證方式，以確保電子銀行交易之不可否認性及明確權責。** 一、不可否認性，係為證實原始資訊的傳送者/接收者確曾傳送/接收該訊息，以避免另一 方否認。 二、業者或可採用 PKI（公開金鑰架構);或數位認證、數位簽章等技術來確保電子銀行交易之不可否認性。 三、銀行可採取下述方式，以避免因客戶否認電子交易存在所招致的風險： 1. 電子銀行交易系統的設計，應能有效降低發生客戶進行無意識（unintended）交易之機率；而且充分告知客戶進行該交易所可能的風險。 2. 交易雙方均取得授權認證，且銀行

		可經由認證管道來管控交易者行為。 3. 對屬於財務性質的交易紀錄，應確保其資料內容是不可更動的，同時，系統應可以偵測到任何意圖異動該等資料的行為。
原則六：對於電子銀行系統、資料庫及運用程式，銀行應確信已採行適當的分工牽制機制。 一、職務分工，不只可減少作業流程或系統發生詐欺的機會，亦可減少發生個人詐欺的機會。網路交易，發生交易者身分被偽冒的機會較一般情形大，此時，職務分工尤其重要。如果疏於防範，有心者將利用網路安全的漏洞竊取資料，因此，經營電子銀行業務應強調：嚴格的授權及身分識別機制、安全的一貫化交易流程處理（straight-through process）架構、及適當的稽核追蹤。 二、實務上對於分工牽制機制之建立與維持，有以	**六、銀行對於電子銀行系統、資料庫及應用程式，應採行適當的分工牽制機制。** 一、於交易處理程序及系統，任一員工或委外作業廠商不能單獨輸入、授權及完成任何交易。 二、對於原始靜態資料（包含網頁內容）及負責檢核資料完整性要符合分工牽制原則。 三、必須經過測試確信電子銀行系統符合且無法規避分工牽制機制。 四、開發電子銀行系統及管理使用電子銀行系統皆應符合分工牽制原則。	**原則六：銀行須將電子銀行系統、資料庫及應用等領域的各個職責明確劃分。** 一、職務分工，不只可減少作業流程或系統發生詐欺的機會，亦可減少發生個人詐欺的機會。 二、網路交易，發生交易者身分被偽冒的機會較一般情形大，此時，職務分工尤其重要。 三、如果疏於防範，有心者將利用網路安全的漏洞竊取資料，因此，經營電子銀行業務應強調：嚴格的授權及身分識別機制、安全的一貫化交易流程處理（straight-through

下的做法： 1. 對於交易處理程序及系統，單一員工或委外作業廠商無法單獨輸入、授權及完成任何交易。 2. 原始靜態資料（包含網頁內容）的建立及後續資料完整性檢核之間，必須符合分工牽制原則。 3. 電子銀行必須經過反覆的測試，以確保系統符合且無法規避分工牽制機制。 4. 電子銀行系統的開發及使用管理之間，必須符合分工牽制原則。		process）架構、及適當的稽核追蹤。 四、<u>電子銀行業務職務分工應注意事項：</u> 1. 銀行在設計交易流程及資訊系統時，應注意職務上的相互牽制。 2. 對於負責建立靜態資料者（包括網頁內容）、及負責驗證資料完整性者間，應明確劃分職責。 3. 進行職務劃分時，不應有模糊的空間存在。 4. 系統管理及研發者間，職責應明確劃分。
原則七：銀行對於電子銀行系統、資料庫及應用程式，應採行適當的授權控管及存取管理機制。 一、分工牽制機制的維持，有賴於銀行嚴格控管授權及存取的權限。 二、電子銀行系統對於授權和存取權限之管理可採集中管理或分散管理方式。	**七、銀行對於電子銀行系統、資料庫及應用程式，應採行適當的授權控管及存取管理機制。** 一、為了維持分工牽制，銀行必須嚴謹控制授權和存取之權限，在電子銀行系統對於授權和存取權之管理可採集中管理或分散管理方式。	**原則七：銀行對電子銀行系統、資料庫及應用等領域的授權控管及進入特權須嚴格規範。** 一、嚴格的規範授權控管及進入特權，可用以確保職責的劃分；並可避免有心者藉由竄改使用者權限，違規進出資料庫。 二、銀行應確保用來「儲存授權控管及進出特許權限」資料庫之安全性。

原則八：銀行應採取適當的措施，以確保電子銀行交易、紀錄與資訊的資料完整性。 一、資料完整性係指保證資訊於傳輸或儲存時，非經正常授權不能被更動。資料完整性若未能被確實維持，將導致銀行的財物損失及信譽受損。 二、一貫化交易流程處理有其本質上的缺失，銀行如採用該法，應特別重視資料的安全性、有效性及完整性，俾能即時修正程式設計上的缺失。 三、銀行應採取適當之措施，以保護電子銀行業務交易、紀錄及資訊的正確性、完整性與可靠性，不論資料是在網際網路傳輸或是存在銀行內部資料庫或者傳輸/儲存於第三服務提供者處。 四、確保資料完整性的策略： 1. 用確保交易過程中資料不會被竄改的方式。 2. 嚴格規範資料存取及修改的原則。 3. 設計資料存取流程，應嚴格防範未經授權者入侵。 4. 確保原始資料的可靠	**八、銀行對於電子銀行交易、紀錄及資訊，應採行適當的措施，以維護資料之完整性。** 一、資料完整性係指保證資訊於傳輸或儲存時，非經正常授權不能被更動。 二、當電子銀行透過開放式網路進行交易，銀行應採取適當之措施，以保護電子銀行業務交易、紀錄、資訊的正確性、完整性及可靠性，不論資料是在網際網路傳輸或是存在銀行內部資料庫或者傳輸、儲存在第三服務提供者。	**原則八：銀行須確保電子銀行交易、紀錄及相關資訊的完整性。** 一、銀行疏於維護交易資料的完整性，除可能產生財務損失外，亦可能招致法律或聲譽風險。 二、一貫化交易流程處理有其本質上的缺失，銀行如採用該法，應特別重視資料的安全性、有效性及完整性，俾能即時修正程式設計上的缺失。 三、無論是針對傳送中的資料、儲存於資料庫的檔案、或資料係委由第三人處理，銀行均應採行適當的方式來評估資料的正確性、完整性及可靠性。 四、<u>確保資料完整性的策略：</u> 1. 採用確保交易過程中資料不會被竄改的方式。 2. 嚴格規範資料存取及修改的原則。 3. 設計資料存取流程，應嚴格防範未經授權者入侵。 4. 確保原始資料的可靠性，不會因系統控管政策（含監測流程）改變而受破壞。

性，不會因系統控管政策（含監測流程）改變而受破壞。 5. 採用具有可偵測資料遭破壞的機制。		5. 採用具有可偵測資料遭破壞的機制。
原則九：銀行應對所有的電子銀行交易，留有詳細的稽查追蹤紀錄。 一、下列型態的電子銀行交易，必須要有清楚的稽核追蹤紀錄： 1. 客戶帳戶之開戶、變更及結清資料。 2. 任何與帳務有關之交易。 3. 客戶超出授權限額的交易。 4. 系統存取權之異動。	**九、銀行對於電子銀行全部交易，應留有清楚的稽核追蹤紀錄。** **下列電子銀行交易型態，必須要有清楚的稽核追蹤紀錄：** 一、客戶帳戶之開戶、變更及結清帳戶資料。 1. 任何與帳務有關之交易。 2. 任何超出客戶原有限額之交易。 3. 系統存取權之異動。	**原則九：銀行須確保所有電子銀行交易均可清楚稽核追蹤。** 一、稽核追蹤之重點項目： 1. 客戶資料檔之啟閉或修改。 2. 與財務有關係之交易。 3. 需經特殊授權才完成之交易。 4. 系統存取權限之交易。
原則十：針對傳輸中或儲存於資料庫中之電子銀行關鍵資訊，銀行應依資訊的敏感性採取適當的措施，以維持資料的機密性。 一、只有被適當授權及經過認證之後的個人、代理者或系統管理者才可存	**十、銀行對於電子銀行資料，應依其敏感性及傳送、儲存方式，採行適當的措施，以維護資料之機密性。** 一、經由適當授權及認證過的個人、代理者或系統，才可存	**原則十：銀行應採取適當的措施，以維護重要電子銀行業務資訊的機密；且須視其所傳送之資訊及（或）儲存於資料庫資訊之機密程度，採取相對稱的機密維護措施。** 一、維護電子銀行業務資

取銀行機密性資料及紀錄。 二、所有銀行機密性資料在透過網際網路或內部網路傳輸時必須要有加密的安控機制，以防止被未經授權者瀏覽及修改。 三、委外廠商及提供服務的第三者對銀行機密性資料所進行的存取、運用及保護，必須符合銀行所定的標準。 四、存取限閱資料必須留存紀錄，且確保該紀錄不會受到損害。	取銀行機密資料及紀錄。 二、電子銀行機密性資料在透過網際網路或內部網路傳輸時必須要有安全保護措施，以防止未經授權之瀏覽及修改。 三、對限閱資料之存取都要留存紀錄，且能確信該紀錄無法被竄改。	料機密性之方式： 1. 存取機密性檔案資料，須先取得授權許可。 2. 應嚴密的規範機密資料的維護作業，並防止機密資料於傳輸中遭窺視或竄改。 3. 對委外廠商存取資料庫行為，應有一致的管理標準。 4. 違規存取資料庫者應予建檔，並妥善保存。
原則十一：銀行應於其電子網頁中，就銀行本身提供之服務內容及相關規章制度，提供充分的資訊，以供客戶進行交易前之參考。 一、爲降低電子銀行業務所可能產生的適法性及信譽風險，銀行應在電子銀行網頁上提供足夠的資訊，例如: 銀行名稱、營業據點及總行所在地；客戶申訴管道及電話；顧客服務中心；客戶存款保險理賠; 針對特定法律管轄區，客戶所應知悉之訊息 等資訊，以供客戶進行交	**十一、銀行對於本身之特性及狀態，應於電子銀行網頁提供足夠資訊，以供客戶在進行電子銀行交易時之參考。** 一、為降低法律及信譽風險，銀行應在電子銀行網站上提供足夠資訊，讓客戶了解銀行網站所提供之服務內容及其影響。 二、銀行網站提供之資訊包括： 1. 銀行名稱、總行地址、營業據點等。	**原則十一：銀行應確保在其網站提供充分的資訊，使潛在客戶在進行電子銀行業務交易之前，即可對該銀行的身分及法律地位有判斷依據。** 一、建議銀行網站應揭露訊息如下： 1. 銀行名稱及總行地址 2. 總行所屬監理機關 3. 客戶服務專線 4. 申訴專線 5. 存款保險及其他保障相關事項 6. 針對特定法律管

易前之參考。	2. 客戶申訴管道或客戶服務中心。 3. 客戶存款保障等資訊。	轄區，客戶所應知悉之訊息
原則十二：銀行在提供電子銀行產品及服務時，應採取適當措施以保護客戶資料的隱私權。 一、保護客戶資料隱私權是銀行之基本責任。為避免因誤用或揭露未經客戶授權之機密資料所導致的適法性及信譽風險，銀行應採取下列措施: 1. 電子銀行服務對保護客戶資料隱私權之政策及標準，應遵守相關法令規定。 2. 明確告知客戶，銀行在提供的電子銀行產品及服務時，所採取的客戶資料隱私權政策及標準。 3. 銀行使用客戶資料不得超越客戶授權的範圍。 4. 委外作業廠商對客戶資料的使用，應符合銀行的客戶資料隱私權政策及標準。	**十二、銀行對於所提供之電子銀行產品及服務，應採取適當措施以保護客戶資料隱私權。** 一、保護客戶資料隱私權是銀行之基本責任，為避免因誤用或揭露未經客戶授權之機密資料，造成侵犯客戶資料隱私權而導致銀行在法律及信譽上之風險，銀行應採取下列措施: 1. 電子銀行服務對保護客戶資料隱私權之政策及標準，應遵守相關法令規定。 2. 明確公告電子銀行所提供的產品及服務之客戶資料隱私權政策及標準。 3. 讓客戶知道允許銀行將客戶相關資料提供給第三者可能會導致其隱私權下降。	**原則十二：銀行應採行適當措施，以確保其於提供電子銀行業務商品或服務時，遵守該司法管轄區適用之客戶機密維護規定。** 一、<u>建議銀行應採行下列措施：</u> 1. 所提供之維護客戶機密措施，應符合該交易所在地法令規範標準。 2. 將銀行有關的維護機密措施，充分告知客戶。 3. 客戶有權拒絕銀行將其資料與其他第三者分享。 4. 客戶資料的運用範圍應事先與客戶約定。 5. 委外廠商亦應遵守銀行與客戶間有關機密維護之規範。

	4. 使用客戶資料不能超越客戶授權的範圍。 5. 委外作業廠商對保護客戶資料隱私權之政策及標準，應符合銀行的標準。	
原則十三：銀行應建立一套有效的業務復原及災變應變計畫，以維持電子銀行系統服務的持續性。 一、為避免營運、法律或聲譽風險，銀行經營電子銀行業務應在一致的、即時的基礎上提供客戶所期待的服務項目。為達成前述目標，銀行應確保有能力將服務順利送達終端使用者；同時有能力處理駭客入侵的問題。如何在尖峰/離峰期間提供一致的服務品質，對銀行而言是一項考驗。 二、應依電子商務市場動態及客戶對電子銀行產品及服務的接受程度，來分析規劃電子銀行系統所需容量及將來規模。 三、經由壓力測試及定期的檢核，估計電子銀行交	**十三、銀行應建立一套有效之災變備援及業務復原計畫，以維護電子銀行服務之持續性。** 一、銀行應建立一套業務持續營運計畫，減少及避免緊急事件所造成之衝擊，以維持電子銀行系統及服務之可用性。 1. 應依電子商務市場動態及客戶可接受程度，來分析規劃電子銀行系統所需容量及將來規模。 2. 經由壓力測試及定期的檢核，估計電子銀行交易處理之容量。 3. 重要之電子銀行業務處理程序及	**原則十三：為使電子銀行系統與服務能持續有效運作，銀行須具有足夠處理能力及備有緊急應變計畫。** 一、為避免營運、法律或聲譽風險，銀行經營電子銀行業務應在一致的、即時的基礎上提供客戶所期待的服務項目。 二、為達成前述目標，銀行應確保有能力將服務順利送達終端使用者；同時有能力處理駭客入侵的問題。 三、如何在尖峰/離峰期間提供一致的服務品質，對銀行而言是一項考驗。 四、為提供客戶持續性且為其所期望的服務，銀行應確保履行下列事項：

易處理之容量。 四、對於重要之電子銀行業務處理程序及傳輸系統，建立災變備援及業務復原計畫並定期測試。	傳輸系統已建立災變備援及業務復原計畫並定期測試。	1. 應預估市場發展潛力，建置作業系統。 2. 對交易的處理能力應執行壓力測試，並作定期檢視。 3. 訂定緊急應變計畫，並作測試。
原則十四：銀行應建立適當的緊急應變計畫，處理突發及未預期事件(包含內部及外部攻擊)，以維持電子銀行系統及服務的正常運作。 一、電子銀行系統及服務之緊急應變計畫，須因應在不同緊急情境下，對不同業務、地理位置等，皆能適時恢復正常運作。且應評估風險發生時對銀行之衝擊，評估範圍亦應包含委外作業廠商所提供之服務。 二、緊急事件一旦發生，應有明確之評估及認定機制(包括事件之重要性及事件發生所帶來之危機)，進而控制因任何服務中斷所導致的信譽風險。 三、對於市場及大眾傳播媒體所關心之安控漏洞、線上攻擊及網路銀行系統失敗之情事，要建立適當之溝通及聯絡策	**十四、銀行應建立適當的緊急應變計畫，以維持電子銀行系統及服務之正常運作。** 一、電子銀行系統及服務之緊急應變計畫，須因應在不同緊急情境下，對不同業務、地理位置等，皆能適時恢復正常運作，且應評估風險發生時對銀行之衝擊，計劃範圍亦應包含委外作業廠商所提供之服務。 二、緊急事件之發生應有明確之評估及認定機制，包括事件發生所帶來之危機、事件之重要性及服務中斷之信譽風險；另外監控連線支援作業和定期分析客戶抱怨事項，可幫助確認現	**原則十四：銀行須訂定意外事故應變計畫，以管理及降低不可預期事件（包括內部及外部攻擊）對電子銀行系統及服務所帶來之衝擊。** 一、對突發事故回應機制應包括： 1. 意外事故應變計畫內容，需涵蓋各種不同情境下之復原作業標準。前述情境分析，探討範圍包括：風險發生的可能性，以及對銀行可能產生的影響。同時應將委外情事納入作整體考量。 2. 建立可即時辨識突發事故的機制。 3. 事件發生時，應有制式化的聯繫管道，可將訊息告知外界。 4. 訂定明確的、標準

略。 四、重要的安控缺失或服務中斷事件應建立緊急通報程序，通報主管機關。 五、要設置緊急事件處理小組，小組人員須經過充分專業訓練，以分析、解釋、處理相關結果的意義及重要性。 六、要有明確之指揮體系，處理內部或委外業務之緊急事件，並適時通報董事會。 七、對於重要電子銀行業務中斷及業務復原，應即時對外公告。 八、應蒐集及保留法律證據紀錄，以協助電子銀行緊急事件之追蹤檢討及提供法律訴訟之佐證。	有安控機制之漏洞。 三、對於市場及大眾傳播媒體所關心之安控漏洞、線上攻擊及網路銀行系統失敗之情事，要建立適當之溝通及聯絡策略。 四、重要的安控缺失或服務中斷事件應建立緊急通報程序，通報主管機關。 五、要設置緊急事件處理小組，小組人員須經過充分專業訓練，以分析、解釋、處理相關結果的意義及重要性。 六、要有明確之指揮體系，處理內部或委外業務之緊急事件，並適時通報董事會。 七、對於重要電子銀行業務中斷及業務復原，應即時對外公告。 八、應蒐集及保留法律證據紀錄，以協助電子銀行緊急事件之追蹤檢討及提供法律訴訟之佐證。	的作業流程。 5. 設立緊急應變小組，並加強對突發事件之偵測及反應能力。 6. 建立與外部相關團體的聯絡網，事件發生時可即時聯繫。 7. 應適時通知銀行管理階層。 8. 確認已即時通知所有外部相關團體（含消費者）。 9.為利事後檢討或法院起訴之用，銀行應建立完善的事件資料蒐集及保存流程。

附錄二、工作期間及研究報告之簡報

附錄三、座談會會議記錄

一、第一次專案座談會

座談議題	電子銀行業務發展及相關法規
座談日期	94 年 12 月 20 日(星期二)下午 2 時至 5 時
座談地點	金融研訓院 6 樓會議室
出席人員	主持人：謝明華 出席者：方鏘傑、潘維忠、林孟津、陳嘉鍾、盧建志、黃惠卿 列席者：陳章正

會議記錄：何習詮

金財通陳章正總經理：本計畫背景及電子銀行發展概述之簡報

台灣銀行盧科長建志：

電子銀行可以區分為 B2C 與 B2B 業務。B2C 業務以台灣銀行的經驗，在 5、6 年前推行網路銀行是很不容易的，必須教育分行的行員，因對於新技術的陌生，以致推廣的成效有限；然而，目前的業務推廣反而較容易，客戶會自行主動的來申請這項服務，因此減少了現場櫃檯的工作壓力，網路銀行的成效開始可以看到了，而目前的網路業務只提供存放款作業，應可再朝授信與外匯等服務發展。

此外，晶片卡的應用例如網路 ATM 或其創新應用，目前各家銀行均積極投入，可預期此市場可日漸成長。

B2B 的部份，事實上推廣時的難度較高，但是一旦成功的簽下約後，就可很容易的綁住客戶，進而提供深化的服務，例如台灣銀行對

中華電信所提供的統收、統付的整合服務，為中華電信帶來更有效率的管理，也為台灣銀行帶來更大的業績。欲整合式的服務例如外匯、授信及更多的服務，則需要電腦ｅ 化的整合。

玉山證券陳總經理嘉鍾：

ATM、Internet Banking 與 Call Center 的通路是值得開發的。而就個人通路的ｅ 化、M 化，若加上行銷的手法，則可化被動為主動的接近顧客。對於企業金融部份可分為中小企業與大型企業。企業規模會影響到服務方式的不同。中小企業的服務方式可思考為介於個人與大型企業的方式。而大型企業的方式則可用 EDI 與PKI 的方式進行。

第二代晶片卡的推行，台灣的進度是領先世界的，而網路ATM 只要使用者有讀卡機就能在家裡或辦公室等地方作金融操作，因此很有發展潛力。若能整合商店端的付款與結算業務，則可提供一氣呵成的服務。

儲值卡受限於目前法規，因此開發業務有些限制。而ETC、悠遊卡或是i-cash 等多家齊鳴未能整合，此部份需要政府主管機關的領導與協助。

再者，網路銀行對使用者來說首要的考量是安全性，第二是快速與便利，第三是自主性高，可不受時間與空間的限制。

而網路銀行在實務上遇到的問題是使用者電腦所用的瀏覽器(IE)的技術問題，IE 改版或是使用者自行安裝其他的plug-in 軟體崁於IE 上通常會發生無法交易的情形，使得實務上很難管理。

而銀行與使用者均期盼能夠有定型化契約來使雙方能夠有互信的依據，並建立業界統一的規範。

業務推廣方面，M 化的技術以備妥，如手機的 3G 服務、手機下載憑證而進行交易等。

合作金庫銀行林經理孟津：

銀行的業務目前以多通路來服務客戶，由實體轉為虛擬通路， 在這個變動的過程中，銀行這個產業的排名將會因此而重新洗牌。 此外，誠如前 2 位的觀點，我再補充一點，B2B 的業務範疇亦會向政府的業務延伸，例如政府採購業務等。

CRM 通常是根據歷史資料來挖掘潛在客戶群,但是如果以網路銀行的通路來看，輸入的資料不再僅僅是歷史資料了，銀行可透過網路得知客戶的反應，了解市場與客戶的需求，進而根據這些資料可推出新的產品與服務。

E 化的目的在於降低成本、提高效益，但是效益通常是未能立竿見影，因此經營價值的轉移是很重要的，我們必須讓決策者了解 E 化的潛力，E 化是鞏固長期的競爭力，必須視為基礎建設，才可在市場重新洗牌時佔有一席之地。

銀行局方稽核鏘傑：

電子銀行目前的定義與業務範疇相當的零散,因此希望本研究能夠提供一個對電子銀行一個較為明確的業務範疇與定義。而政府主管機關的法規是越少越好，避免因法規的限制而影響此領域的發展。而我

國銀行目前需培養全球化的能力，而銀行內部的管理需有成本的觀念，運用管理技術與資訊技術來控制成本使成本降低。則有助於提升本身的競爭力，有二個成本模型希望銀行能夠導入到企業中，一個是人力成本計價模型，另一個是投資效益模型，銀行可利用此類模型來作為成本控管的基本工具。

從客戶的觀點，提供安全的交易環境是必須的，有了安全才有信賴，有了信賴客戶才願意使用更多的服務甚至要求更多更便利的服務，銀行也因此樂於提供更完善的服務，如此正向循環會使此產業更為蓬勃。銀行對於企業用戶的深化服務，例如 Korea Airline 的例子，值得我國銀行借鏡。

政治大學謝教授明華：

Basel II 對於電子銀行亦是僅提供大方向的指導原則，因此與方稽核的觀點「政府主管機關的法規是越少越好，避免因法規的限制而影響此領域的發展」不謀而合。

第一銀行黃專門委員惠卿：

目前每個銀行都在進行組織改造，希望達到降低成本提高收益，也各有所謂商品開發處，負責研究開發新的金融商品；這些金融商品希望能藉由電子銀行的方式來提供顧客服務，能夠節省櫃檯人員之人力資源來改從事行銷之工作。

考慮到客戶的方便性而言，客戶的反應是目前個人網路銀行之服務非常不便。例如申請金融卡與領取卡片都需要親自到分行一趟；另外網路上使用 SSL 轉帳需要非約定帳號，為了申請帳號又需跑銀行一次；若是以 SET 方式，固然安全上有較多考量，但也更多限制與不便，

仍有許多使用者甚至行員並不知如何使用 CA（憑證），這是需要再加強教育與訓練的部分。

在企業網路銀行的部分，許多銀行投資了很多資金在建置 C 計畫，如能好好推展，其實 C 計畫會是一個企業 e 化很好的契機，例如在招攬中心廠時，下游許多供應商自然會跟進，即能達到推展的成效；另一方面，除非如預約付款是由銀行包攬的，在融資這部分企業建置 AP-to-AP 的成本很高。

另外，使客戶能在網站上一次查詢其帳戶下之所有轉帳、消費、及繳款等交易的資訊，或跨行歸戶查詢等，提供更安全便利的服務，是我們未來可努力的一個方向。

財金公司潘協理維忠：

從需求導向或是客戶導向來談電子銀行，首先先對電子銀行下一個定義，基本上是從銀行櫃臺往外延伸的服務才算，如果是屬於銀行內的業務則只是電子化而已，所以電子銀行等於把銀行的櫃檯向外延伸到客戶端與企業端。談到國內電子銀行發展的完整性，是否能夠符合需求，應具備有下列幾點：

從服務對象來看，應能服務到企業與一般消費者。在企業支付方面，如 EDI、XML 等屬於企業金融的部分，與企業的關聯性相當密切，並牽涉到企業端的 ERP 與 SCM 等；另一方面則是由消費性支付部分的服務來看。

再依支付工具來區分，與帳戶有關的部分是如金融卡、信用卡；與帳戶無關的如儲值卡。

依支付金額區分，有大額、小額及介於二者之間的。目前大額支付金額暫定是在二千萬元以上，企業支付的部分；小額的定義是在一萬元以下偏向個人支付的部分，介於二者間的中等金額，是在一萬至二百萬元間。在支付金額方面，可以來檢視看看國內的電子銀行是否都具備了這些部分或者欠缺了哪些部分。

依功能面區分，不論是 B2B 或 B2C 都提供了轉帳、繳稅、繳費等功能。在強調 B2C 之消費性金融方面就是與購貨、提款、查詢有關；在 B2B 方面，如國內銀行業走向金控的趨勢，功能如基金下單等；基本上功能是蠻齊備的。

依設備或通路面來看，透過行動銀行、Internet、手機、PDA、ATM、網路 ATM 等，看看網路銀行是否能夠透過這些通路來提供服務。

依標準面來看，是否有共通性，有共通性走的路線是共通標準，沒有共通性走的是差異化；大部分的業務走共通標準約佔 80%，小部分走差異化約佔 20%。

現階段國內電子銀行的服務可以由以上這些分類來切入探討。大致上國內電子銀行多已具備上述之功能，較欠缺的是 micro-payment（小額付款）的機制，它有共通性也有差異性，目前各銀行所做的部分是屬於差異性的部分，實際上從需求的角度來看，消費者還是希望能夠有共通性，個人認為 micro-payment 未來仍有相當大的成長空間。

以上是從大架構的完整性來討論，若再切入看較細節機制面的部分，銀行由過去的實體走到現在的虛擬，在建置電子銀行時，提供的是偏向直線性的服務，行動銀行是一條線、網際網路是一條線、電子

銀行是一條線，比較少去做整合的動作；不論從銀行角度或由共通的角度來看，以後的發展走向會是專業分工。專業分工的意義在於，資訊流的部分由事業體的部分負責，金流的部分在銀行內，去做一個整合、專業分工的切割，也是C計畫正在進行的工作，由於成本的限制目前尚未做到很好的切割，這是需要好好努力的部分。

不管是消費者或是企業或是共通平臺，都需有一個共識是專業、整合、分工；未來電子銀行的發展將會走向多通路設備之整合，前端如行動銀行網路銀行等新資訊科技的加入，這些部分將由專業的單位去做資訊的處理，再將資訊轉成銀行的訊息，讓銀行去處理金流的訊息，若是屬於共通性的訊息則使用共通性的標準。

安全也是一個很重要的考量層面；現階段國內的發展，有一部分是正在進行中，例如晶片卡金融卡對於電子銀行是一個革命性的改變，讓交易能在網路上進行並且也解決了安全的問題。再看國外在安全上的發展，例如亞洲國家如韓國，是由政府積極推動使用憑證方式來解決安控及身份認證問題；國內目前仍然沒有共識及共通的解決方法，在規模和經營上仍有困難，未來將會是一個影響電子銀行發展的因素。

再探討到與共通性相關平臺的成本，其實是不可能藉由手續費之中收取，換言之金融業務沒有十年的虧損是不可能達到如今日的ATM、通匯等服務的普及，通常是銀行認為有商機且與其他銀行之平臺合作發展可能，願意藉由其他交易收入補助。事實上電子銀行走的是策略主導，只要能夠考量到未來發展趨勢就會願意投入資金或以其他業務來補貼目前的機制發展。

國內目前仍欠缺的是退場機制；可以看到的是安控對業務的影

響，應該考慮到隨著不同技術的發展，該退場的安控技術應有退場的機制，而不影響到業務的發展與消費者的權利，而銀行與消費者也應有共識了解不可能有某一種安控技術永遠提供服務，時間到了就會汰換成其他技術。

開放討論－

合作金庫銀行林經理：

由於機制面技術面時代潮流或客戶需求的改變，會有不同需求，因此技術會有淘汰退場的時候，此時就需要周全的轉換機制，要如何讓客戶不會感到困擾不便，例如推動 SET 後憑證機構改推行 XML 憑證而必須中止舊有的 SET；例如台塑網及中鋼已有共通平臺，而企業早期配合建置 AP-to-AP 成本也相當高昂，若現今憑證機構一改變制度就要配合，造成企業對於參與政府推動之計畫會感到遲疑，要如何解決這樣的問題？

銀行局方稽核：

我的觀點是支付系統的營運其實上需要去揭露其成本，是一個 cost-based 的問題，意即它的服務是隨著交易量而成長，它的收費機制也應該隨著改變，而不是固定成本的，這個概念在世界各國都是如此；在初期系統建置有多少固定成本、變動成本在其中，而變動成本應該隨著交易量的增加去攤提，固定成本也隨著交易量的增加而攤提而降低，事實上都應該去揭露成本，使營運正常化，但目前我們不是在這樣的制度下去發展。

在銀行配合支付系統時會有二種情況，大銀行會想要去 occupy 支付系統，小銀行則是依賴系統。銀行對於服務收費的重點是以能 cover

其成本為要務；能否成功推動一個系統，應該考慮到其試驗期成熟期有多長；而銀行在將面臨成熟期之工具上應有替代工具（一個工具原本就有成熟退出之生命週期），而使客戶沒有受到影響的感覺。

臺灣在這方面的問題往往只看到 revenue 而未看到 cost；如借鏡國外時應考慮結構性問題，有些問題之解決可能要等到時點到達才能解決。

黃專門委員：

有些公司在 C 計畫中並不願配合共通標準(例如台塑自訂其標準)並以更換銀行為要脅，如何因應？

銀行局方稽核：

這個問題的產生是來自客戶沒有被教育或者教育不夠;事實上 EDI 已經 face out，而許多觀念是平常就須溝通教育建立的。銀行可以配合客戶要求提供非共通性的服務，但必須讓 user charged 的觀念被落實，達到成本揭露；其實與國外相較，國內提供 ATM 的服務是虧損的，但為何銀行仍繼續進行？是因為沒有去仔細計算成本，造成了浪費與虧損的漏洞；cost down 是 top-down 都要做而不只是 down 做起而已，包含內部組織結構生產力的設算模型都應該考量去發展

補充－

台灣銀行盧科長：

就臺銀立場提供一些本身的經驗做為參考。當初臺銀在推廣網路銀行時因安全性之考量並未採用 SET，但有配合政策使用 SET 做繳稅；本身的網路銀行用 SSL（約定、非約定帳戶）：2004 年三月網銀事件造

成非約定帳戶之中止，約在七八月時配合晶片卡之推行使得非約定之帳戶的服務恢復，移轉成功，交易量上昇。因此在考量若對於安全性未來發展性有疑慮的技術時，應該有策略性的考量。

在 B2B 方面，臺銀非 C 計畫內的組織，亦建了類似的 infrastructure，雖然 AP-to-AP 量很少，但把 C 計畫的精神建置在後端的業務模式；而前端可能會遇到客戶的需求格式不同，因此若希望能夠儘量配合不同客戶需求，建議後端是一統整的系統，前端發展比較靈活性的介面，前端 by 客戶的部份做少部份調整是必然的。

財金公司潘協理：

電子銀行的瓶頸在於科技進步遠大於市場進步速度，例如 EDI 好不容易推廣至目前規模又變成 XML 的崛起；其實市場的大小是固定的，當某個新技術標準成熟舊有技術標準自然會萎縮汰換，但是必須提早發展替代的工具和解決方案。國內應該有專責單位去觀察國際脈動與新技術標準的發展，並研發配合的技術與策略，推廣共通平臺，若各個銀行自行去做 R&D 的工作其實是資源的浪費也無法達到時效性的應用。

銀行局方稽核：

其實剛才的概念是很重要的觀念，如財金公司R&D是一直仰賴其他業務扶持；我國的晶片卡正在起步，但英法挪威芬蘭等國之晶片卡使用成熟度高（例如配合biometrics生物辨認之技術）。臺灣一直很支持全球化，而在支付系統營運方面可能須考量，國內與國外之系統是否有interoperability之問題？例如香港有自己的外幣清算中心；畢竟新臺幣不是國際性的貨幣，很多國際性的交易還是仰賴使用國際性貨幣，應該去研究我國每年有多少外幣之交易，不能因為有問題，而就

一直抱持觀望的態度。

(二)第二次專案座談會

座談議題	電子銀行之風險控管
座談日期	95 年 1 月 20 日(星期五)下午 2 時至 5 時
座談地點	金融研訓院 6 樓會議室
出席人員	主持人：季延平 出席者：方鏘傑、林孟津、羅安昌、曾淑峰 列席者：陳章正、謝明華

會議記錄：何習詮

政治大學謝明華教授：

針對電子銀行業務風險控管十四項原則與跨界電子銀行業務風險管理原則介紹，簡報。

上海商銀羅安昌協理：

銀行公會電子銀行風險管理自律規範的內容不是只有翻譯 BASEL II 的文件而已，而是經過討論與實務工作者的經驗所擬定的。實務工作者的安全控管利用 CHECK LIST 來實施，可有效的審視銀行目前對於規範所實施的程度。該指導原則，包含了 IT 面的細部實施內容，可供銀行界來參考，但由於 IT 的變化速度較快，原則性的內容較不需包含實務上技術面的技術，以免日後 IT 技術更新後的修法困擾。例如，PASSWORD 不是很好的認證方式(萬年密碼)。此外，安全的等級加強，若能區分個人戶與企業戶的層級區分，那會更好。

政治大學季延平教授：

原則性的條款很容易被過度簡單的解讀,若是能以實務面的且細化的舉例說明，則能夠夠清楚的說明與規範。

銀行局方銷傑稽核：

安全的要求與其解決方案是無止盡的不歸路。因此只能提規範性的指導原則來對業者提出最低的安全要求。參考美國的電子資金轉移法，以保護消費者為概念，而我國因立法的程序複雜，因此以定型化契約來取代類似美國的電子資金轉移法的條款。基於安全的考量，便利與平衡是相對的，是必需在這兩邊做取捨的。

金融業者的信譽風險是很重要的，稍微的服務中斷與缺失，可能早成大量的客戶損失。

此外，安全的規範準則，可以說是依國情不同而產生不同的看法，例如，花旗銀行對於本國的規範覺得嚴厲，這是因為美國政府覺得業者應該自由競爭，無法取得客戶信任的銀行自然會被市場淘汰。

合作金庫銀行林孟津經理：

網路上的應用，在安全控管方式上存在著矛盾，使用者希望方便，又擔心交易不安全，而銀行端注重安全，但又怕複雜的安控程序引起使用者不願意使用。因此常常對於安全上作出使客戶滿意的讓步，也因此常常背負著龐大的壓力。電子銀行業務風險控管十四項原則看似簡單，但事實上實施卻是很困難的。

美國世貿大樓的門禁安控十分嚴謹，但還是遭到 911 恐怖攻擊，但卻能在 3 天後將資料復原回覆交易。客戶端的駭客是無時不在，令銀行防不甚防。

國內較偏向保護消費者，88 年開放 SET 實施，但是客戶感覺不方便，因為要安裝憑證，因此 SET 將於今年底淘汰。而英國的外匯交易

也僅僅用 SSL 來交易。因此基於方便與安全週延，銀行端要做策略性選擇所提供的業務範疇，例如：約定戶交易與分約定戶交易、SET 與 Non-SET 交易等。

政治大學季延平教授：

感謝方稽核與林經理的寶貴意見，由這些意見中我們可以了解要遵守這十四項原則其實不是非常容易，其中牽涉到許多資料的稽核和分析，這些工作成本非常高但是電子銀行的收益卻非常低，銀行本身要承擔很高的風險而收入又有限，但若不發展這些功能則會有聲譽的問題，所以很多銀行目前只發展簡單的（功能）而沒有積極地推動。在國內也可以看到這方面較高級如資料倉儲的技術人才，其實是不全的，所以很多銀行採用套裝軟體，但事實上功能沒有那麼適用，也很難對資料做深入分析，這些是目前遭遇到的一些問題；而這些問題還沒有談到跨國界（電子銀行），目前的交易也尚未發展到跨國界的程度；接下來我們再聽聽看其他專家的意見。

政治大學曾淑峰教授：

個人觀點來說，不管有沒有 Basel II 的存在，本來風險控管就是要做的工作，也有許多參考準則已經提出；許多管理顧問公司也已提出了一些作法可以參考，例如 BS7799 等，所以個人認為其實在作業基準原則標準的討論上其實沒有太多可以再努力的空間，因為已經存在許多國際標準；反而重點是在於風險如何衡量，知道風險大小才能知道如何去規避。在過去通常是教銀行如何去規避風險，但沒有去教主管機關如何去根據衡量出來的風險去制訂規範，如果在原來的架構下去增加一些衡量的基準，再參考 Basel II 的大原則，這樣似乎就足夠了，再增加可能也難以超越目前現存的標準；因為管理顧問公司提供的東西其實已經非常完整，背後擁有雄厚的 knowledge base，例如

BS7799 或是軟體產業的 CMMI 等一些 operation 的參考準則，其實我們在短期內可能無法發展出更完整的準則，也不能將準則完全鎖定下來否則會無法因應環境的變化而沒有彈性；倒不如因應 Basel II 去將一些原則量化、去做預測。

在信用風險的部分，我們去做這些預測，可以提供一些決策支援的參考；但回到電子銀行方面，似乎沒有決策參考的需要，因為電子銀行的服務是全面性的，比較類似消費金融，不是針對每個客戶去做決策而是做 group 的分群管理，看是屬於哪一類作業原則、風險評估，會比較適宜。在 Basel II 裡面作業風險本來就是很難去衡量的，但基本上還是需要去找一些風險因子，可能牽涉到銀行的作業營運面需要改善的部分，是作業準則裡面需要規範處置的。

政治大學季延平教授：

感謝曾教授的分享；從過去的經驗我們可以了解到有時完整的機制不一定是最好的，適用的機制才是最重要的；準則也不一定適用於不同公司的作業流程。先前提到過的風險通報機制，其實可以提供案例給各家銀行做為參考以及讓一些資訊安全能力較不足的銀行獲得警示的機會以做好防範風險的工作。

上海商銀羅安昌協理：

舉一個例子來看，在金融機構作業委外處理辦法中，就我們金融機構的看法，無論是作業政策或準則，其實裡面提到的無形之中已經對我們（業務行為）有相當的約束了，而稽核人員來稽查時也相當容易進行，例如有哪些制度是否落實、客戶識別程序、風險效益分析等，都相當清楚。而最重要的是必須請董事長總經理等高階主管，對全公司發一份聲明強調資訊安全的重要、是全體人員的責任，再來就是資

安小組的責任，去針對每個業務每個流程訂定依循的辦法準則，而不止是概念式的東西，我想每個行庫都會去遵循。目前我們比較希望可以看到的可能是國內和國外的銀行比較之下是否有一個參考準則的summary，來了解哪些事項是必備、一定要進行的。

政治大學季延平教授：

謝謝羅處長的意見；由剛才的討論我有一些想法，在目前美國的企業開始發覺他們的資訊化其實成效不佳，大約只有三成的企業資訊化是成功的，而大部分的企業資訊化只能滿足基本的需求，例如報表產生的自動化，而成本降低、生產力提高等這些需求是沒有達到的。因此產生了「IT Governance」IT 治理的概念，強調的是如同剛才羅協理提到的董事會的職權，許多高階經理只是提出資訊化很重要的觀念後就將工作丟給資訊部門去推展，最後產生問題卻沒有人承擔責任；另外是重視資訊稽核的概念，因為很多工作只是陽奉陰違做到最基本的程度，到最後造成了資訊化的失敗；如何去加強董事會的權責，而不是只是資訊部門的工作，如果能夠協同其他業務部門一起分擔，也能夠爭取較多經費來增加資訊安全工作的落實，這是與 IT Governance 觀念不謀而合的。

銀行局方鏘傑稽核：

其實今天花旗銀行代表不能與會是很可惜的，除了無法了解外商銀行對於此方面的需求與意見，也沒有機會藉由之前花旗銀行的資安事件經驗來得到一些分享。其實從風險管理的角度來看，金融業本身就是存在了許多風險，談到了所謂的交易風險、信用風險、資訊上的作業風險，尤其資訊本身是沒有信用風險的因此著重在作業性風險，因為資訊作業的服務而產生的損失是銀行必須去賠償顧客的，如前面教授所提到很重要的是如何去衡量風險。

在風險的評估裡有三點是很重要的：首先是 Identify risk，去找到風險是歸於哪一類，例如 IT 的風險在 BaselII 的作業風險，找到哪些點是存在風險的;再來是如何衡量風險的 weight,如何影響損失，再來評估有多少資本是需要計提的。既然知道 IT 上有哪些點是可能有風險存在的，就應該儘量用 IT 的方法用安全的措施去解決它防範風險的產生。國內目前用 IRB 的方法似乎還未見到，模型和財務工程的設計是需要資料庫有足夠大量的歷史資料來支援，才能讓模型是 reliable 是可用的；因此大多仍採用標準法，也是最簡單的權數的概念。

回到電子銀行來看，側重於電子金融，也就是資訊這一塊，它不會有信用風險、交易風險的問題，因為這些是原本銀行的交易之中就會產生的（信用風險、交易風險)；因此為什麼在電子金融是以 guideline 為規範的道理也在於此。談到 IT 作業上的風險，剛才羅協理講得非常好，就是要回歸到作業程序和作業方法上來看，以及手冊的設計，也就是一點一滴地攤在陽光下，照著標準作業流程(SOP)的程序來進行;而如何落實這樣的程序，就需要 audit 的工作來看手冊 SOP 的訂定是否嚴謹、是否有遵照 SOP 進行。當然就算依照 BS7799 的規範來進行，也通過了認證，但問題仍然可能發生，原因在於「人」是最難掌控的；其實以目前來看 IT 本身被攻破的機率不高，主要的問題還出在「人」;安控機制本身必須要有彈性，一旦問題發生要能很快修正去因應。第二個是談到所謂的通報制度，這是目前有在進行的，當案例發生時要通報到主管機關去產生因應動作。總結來說安全與風險控管這個領域要做到非常好，有賴於聘用的人以及制度的完整，才能確保做到不能說是絕對安全但至少是有效的安全機制運作。

政治大學曾淑峰教授：

我在這邊提出一些看法，如相關規範或處理原則已經現存的，可把他落實，因為這些是正在執行的，當初在制訂時也已大費周章，可以看看執行面上有什麼需要再修訂再往前推動，而不必再費時訂定新的規範。

上海商銀羅安昌協理：

我想如果參考 Basel II 目前是只存在一些準則，至於詳細作業要遵從進行的部分，可參考銀行委外作業處理原則這樣比較有明確的參考細則，分段來進行，在作業和稽核時會比較清楚，也能達到我們計畫的目的。

銀行局方錡傑稽核：

重點是這樣的工作可能會讓一些小銀行發現他們有做到不足的部分去加強，這也是一個貢獻並且提供一些參考資料。

政治大學謝明華教授：

當初 Basel II 將這些準則列在健全實務準則的部分，是因為認為其實每個銀行從事 e-banking 的比例是不一定的，是屬於銀行各自的 business strategy 的部分，如果把規則訂得很死，對一些不從事這些業務的銀行來說會太嚴格，因此把它放在 appendix 的部分，屬於 guideline 的角色，預留了彈性空間。

政治大學季延平教授：

美國有的（銀行）採取的是悲觀主義，也就是事前成本的概念，發生問題時其實都不難處理；有的採取的是樂觀主義，認為問題不會發生，一旦發生事件要處理的成本是很可觀的；臺灣其實沒有樂觀主

義的本錢，（銀行）發生問題會造成連鎖效應，對金融的影響很大。再來談論到境外交易的風險，其實也是相當高的。

銀行局方稽核：

因為我國對外匯的管制是相當嚴格的，所以談到 cross-border 交易的部分，像香港成立了美元部位的清算中心，臺灣來說是滿遺憾的也許是基於外匯管制的考量，尚未成立像這樣的清算中心，對於想要成為亞太金融中心的目標是較不利的。

林孟津經理：

我認為臺灣其實可以說是法規中心，世界上現行的法規臺灣幾乎都不會落於其後，但是實用面來說，太多或者太完整的法規也會造成一些應用的障礙，讓執行者不願去執行以避免牴觸法規，使得一些政策還未執行當事者已經下臺，也浪費資源；如何去取得平衡，是值得專家學者來思考，怎麼樣在有限度的風險之內，讓業務可以去執行，在國外其實是容許有一些風險存在的，從事業務是不可能零風險；因此在網路應用上臺灣不見得比較發展比較快，甚至可能落後於大陸，因為我們已經被教育到了解也認為風險是可怕的，而造成業務推廣上的困難。

金財通陳章正總經理：

依據數據顯示，我國電子銀行的使用比率相對於國外銀行偏低，當然造成影響因素不少。因此，所引伸的相關議題，是值得大家繼續去研究探討及改進。

附錄四、參考文獻

項次	資料名稱	來源/出版處	著者
1	電子錢包通路打不開 全球踢鐵板	聯合報新聞網	記者孫中英
2	電子錢包 全台剩5千張	聯合報新聞網	記者孫中英
3	電子發票推動整體規劃及監督審驗	資策會	王存致
4	電子銀行業務及IC卡業務介紹	金融研訓院 財金資訊	潘維忠
5	資訊系統與電子銀行之風險管理		
6	電子商務之現況與展望	玉山銀行電子金融部	陳嘉鐘
7	電子商務經營模式之策略分析	玉山銀行電子金融部	陳嘉鐘
8	電子銀行犯罪案例說明與防制		
9	電子銀行犯罪案例研究		
10	電子銀行（e-banking）十四項風險管理原則	金融研訓院	
11	電子銀行風險管理自律規範	金融研訓院 銀行公會	金融業務電子化委員會
12	BASEL- Risk Management Principles for Electronic Banking	Bank For International Settlements	
13	英國當地網路銀行最新相關規定(Electronic Commerce Directive)	ECO	
14	新加坡當地網路銀行相關規定(Internet Banking Technology Risk Management Guidelines)	MAS(Money Authority of Singapore)	
15	香港當地網路銀行相關規定(電子銀行的監管、科技風險管理的一般原則)	香港金融管理局	
16	協助小型金融機構做好風險管理	工商時報	李三榮
17	IC儲值卡在我國零售業消費支付應	金財通	陳章正

	用之研究		
18	美國金融業電子銀行業務之網路架構安全控管及稽核方式之研究	中央存款保險公司	紀慧敏
19	企業網路銀行安全控管作業要點	第一銀行	
20	金融機構辦理電子銀行業務安全控管作業基準	銀行公會	
21	Internet Banking : Developments and Prospects— Program on Information Resources Policy	Harvard University	
22	Technological Innovation in Retail Payments: Key Developments and Implications for Banks	Office of the Comptroller of the Currency	Karen Frust and Daniel E.Nolle*
23	Beyond the Field of Dreams: How Citibank Drives Account Opening Online	Tower Group	George Tubin
24	Distribution strategies in US retail banking	DATAMONITOR	
25	Expedited Bill Payments:The Basics of Convenience	Tower Group	Elizabehe Robertson
26	New Payment Options: E-Commerce Looks Beyond the Credit Card	Tower Group	Elizabehe Robertson
27	European eBanking technology strategies	DATAMONITOR	
28	The Future of Banking	Prentice Hall	Henry Engler, James Essinger
29	Electronic Commerce and the Revolution in Financial Markets	South-Western College Pub	Ming Fan, Jan Stallaert, Sayee Srinivasan, Andrew Whinston

30	Retail Financial Services in 1998: Travelers	Harvard Business School Press	Stephen P. Bradley, Takia Mahmood
31	Merrill Lynch: Integrated Choice	Harvard Business School Press	V. Kasturi Rangan, Marie Bell
32	DLJdirect: "Putting Our Reputation Online"	Harvard Business School Press	Thomas Eisenmann, Gillian Morris
33	Wit Capital: Evolution of the Online Investment Bank	Harvard Business School Press	Roger Hallowell, Charles G. Ruberto
34	WingspanBank.com (A)	Harvard Business School Press	Sandra J. Sucher, Daniel Galvin
35	QuickenInsurance: The Race to Click and Close	Harvard Business School Press	Lynda M. Applegate
36	E-Loan: The CarFinance.com Acquisition	Harvard Business School Press	Morten T. Hansen, Jeffrey A. Berger
37	Wells Fargo Online Financial Services	Harvard Business School Press	Robert S. Kaplan, Nicole Tempest
38	Innovations in Retail Banking	UNISYS	
39	Information Systems Control Journal		
40	金融業資訊委外方興未艾	新聞	
41	網路銀行安全嗎?	各大報章雜誌	
42	電子銀行業務管理辦法及安全評估指引出爐	新華網	

43	資訊系統外包的隱憂	財團法人國家政策研究基金會	黃朝盟
44	網路銀行的安全如何做	資安人科技網	
45	銀行業分享資安經驗	資安人科技網	
46	亞太地區新巴塞爾資本協定實施情況調查報告	資安人科技網	
47	安全政策指引讓台灣資訊環境更健全	資安人科技網	
48	電子簽章法通過後對網路交易相關應用的影響	資安人科技網	
49	為什麼需要資訊安全委外	資安人科技網	
50	網路銀行的風險管理(上)		
51	電子銀行安全評估指引	中國銀行業監督管理委員會	
52	電子銀行業務管理辦法	中國銀行業監督管理委員會	
53	銀監會審議通過《電子銀行業務管理辦法》	中證網	
54	監理審查分組第二階段報告		
55	Hype Cycle for the Banking Industry,2005	Gartner	
56	Management Update:Predicts 2005: Microcommerce Will Transform Payments	Gartner	
57	Microcommerce Will Transform the Commercial Landscape	Gartner	
58	Predicts 2005:Emerging Trends Drive Business Opportunities	Gartner	
59	Checks in Decline:The Tipping Point in Electronic Payments and Its Impact on US Cash Management	Tower Group	
60	金融機構資訊系統安全基準使用說明--設備基準	KPMG	
61	金融機構資訊系統安全基準使用說明--營運基準	KPMG	

62	金融機構資訊系統安全基準使用說明--技術基準	KPMG	
63	Work Program--Internet Banking	KPMG	
64	金融檢查	OCC	
65	電子銀行之安全查核	KPMG	