郵件歸檔方案大直擊（下）

個資法總動員 從郵件歸檔做起

作/曹乙帆

經過上期的介紹，讀者對於郵件歸檔因應個資法之最佳化細節，乃至郵件歸檔與郵件備份之間的差異想必了然於胸。本期將為讀者再接再厲，進一步對繁雜的產品類型，乃至錯綜的採購注意環節抽絲剝繭，以助企業在尋得最佳方案上一臂之力。

隨著新版個資法全面施行的腳步愈來愈近，企業必須緊鑼密鼓地做好相關的因應措施。在所有個資容易外洩的管道中，電子郵件一直扮演著十分重要的角色。同時企業莫不透過防火牆、IPS、垃圾郵件過濾、郵件安全及災難復原等一道又一道的安全機制來確保郵件服務的安全無虞及運作順暢，由此再再說明了電子郵件在企業營運上扮演了極其重要的角色。也因為電子郵件的重要，電子郵件的歸檔備存，絕對是因應個資法等法規遵循上的一大捷徑，也是邁向更完備法規遵循建置的一大基礎。

郵件歸檔的重要性勿庸置疑，如何選擇良好適用的郵件歸檔方案更加重要。所以本期重點會放在郵件歸檔在產品上的類型、不同部署方式，乃至採購上應該注意的地方。

郵件歸檔設備產品類型

目前郵件歸檔的類型不外軟體式、硬體式及雲端三大類方案，以下且讓我們看看這些方案之間的差異所在：

1. 軟體式歸檔伺服器

所謂軟體式郵件歸檔方案，亦即透過設置內建該軟體之專屬郵件歸檔伺服器的方式，來進行內對外、外對內及內對內之郵件歸檔作業。該類型方案多半會採用直接複製(Replication)至郵件伺服器的方式，進行郵件歸檔、查詢及調閱之管理。

台灣賽門鐵克資深技術顧問陳力維表示，不論Exchange或Domino，除了在企業內部會有成千上萬個郵件信箱外，同時會在伺服器上特別建立所謂的Journal MailBox，用來存放所有郵件的備份檔。但隨著時間的增加，該信箱容量會愈來愈大，同時該信箱與其它信箱多半皆共用伺服器的內建硬碟，所以對伺服器效能影響不小。

一般而言，大部分歸檔方案（尤其是軟體式的）會不斷從Journal MailBox中將備份郵件搬離至與歸檔方案相連接的儲存設備中，以便讓Journal信箱空間得以清空，進而降低伺服器效能的影響。以賽門鐵克Enterprise Vault(EV)而言，並不需要在郵件伺服器上安裝任何代理程式，只需在所架設的EV Server上建立一個可以存取郵件伺服器系統的帳號，如此便可自動進行搬信及清空信件的作業。

目前軟體式郵件歸檔方案，基於日後搜尋及查詢之用，而會在郵件儲存上採取不同的方式。一種是完全將郵件伺服器的整份原始信件備出來，另一種則會針對郵件內容依欄位進行拆解儲存至資料庫之中。

後者，一旦需調閱時，會在查詢之後自動將郵件加以拼湊以供使用者瀏覽。同樣有提供軟體式郵件歸檔方案的Openfind採取的是直接複製並搜尋的機制，並質疑資料庫查詢式軟體方案，會有破壞原始格式，進而無法符合法規遵循要求的風險及疑慮。

比起硬體設備，安裝在專屬伺服器的軟體式方案，其硬體規格不會被定死，所以可以隨時進行處理器升級或記憶體添加的升級作業。不過在安裝及設定上，會比一整台硬體設備稍嫌麻煩。

2. 硬體式設備

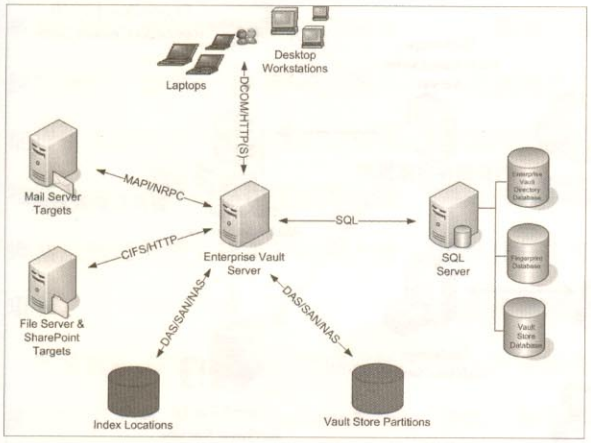
亦指設備型的郵件歸檔方案，目前歸檔設備會依照使用戶需求分別提供閘道、複製及監聽等不同部署模式，對此會在稍後的段落中做進一步介紹。歸檔設備的好處在於安裝方便，而且不需像軟體方案需要每年簽MA。但硬體設備不像伺服器可以針對特定零組件說換就換，所以企業購買時必須精準計算出未來幾年內可能成長的郵件量，如此才能買到可以因應好幾年郵件歸檔需求量的適當設備，否則，一旦發生不敷使用的情形，有可能必須完全放棄而改買全新夠用的設備。

對此，Openfind提供所謂分散式架構的硬體設備，即使企業一開始所買設備不敷使用，也可以藉由分散式架構，不斷添加新設備串連起來，算是極具擴展性的不錯解決方案。此外，中華數位也與Openfind在設備上提供多種可供選購的模組，例如內部信模組、Replication模組等，透過這些模組便可增加許多新的部署或安全功能。

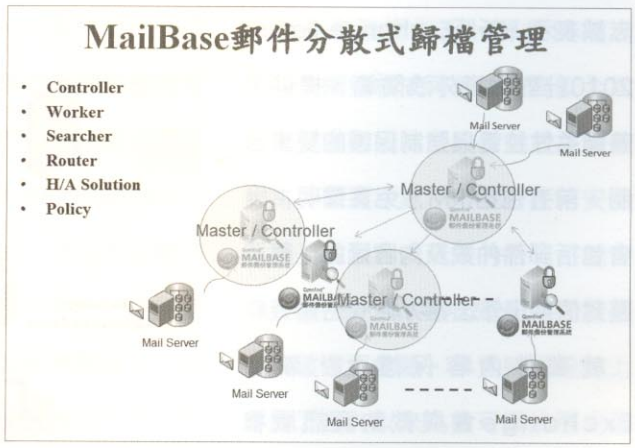
3. 雲端郵件歸檔服務

亦即將所有進出企業郵件伺服器的郵件，完整歸檔至雲端上的解決方案。透過該方案，企業完全不需麻煩地自行架設歸檔伺服器或部署歸檔設備，也不用不斷地為備份郵件添加儲存裝置及設備，如此可為企業每年省下可觀的採購、設定、維護管理等成本及費用。

這類方案並且會為企業提供方便的郵件搜尋、查詢及調閱的介面及機制。在法規遵循上，企業並可透過服務層級協議(SLA)的簽署，將郵件快速調閱及法規遵循的風險轉移至服務供應商身上。畢竟雲端歸檔服務商所提供的服務應該比企業自建機制，不論在專業度上及效能



▶ Symantec Enterprise Vault郵件歸檔各元件架構圖。（圖片來源：Symantec）



▶ Opendfind MailBase郵件分散式歸檔管理。（圖片來源：Openfind）

上會來得更好，而且還有SLA的保證，實不失為降低法規遵循風險的最划算方案。

目前提供雲端郵件歸檔服務的方案不少，例如Openfind Mail ASP、Symantec MessageLabs Email Archiving.cloud、McAfee SaaS Email Archiving等。

郵件伺服器內建歸檔機制

除了前面3種歸檔方案外，事實上，Exchange等郵件伺服器軟體也支援歸檔乃至個資外洩防護功能。對於企業來說，透過郵件伺服器軟體便能搞定郵件歸檔，乃至法規遵循上的種種需求，當然是最簡便又符合成本效益的不錯方案。

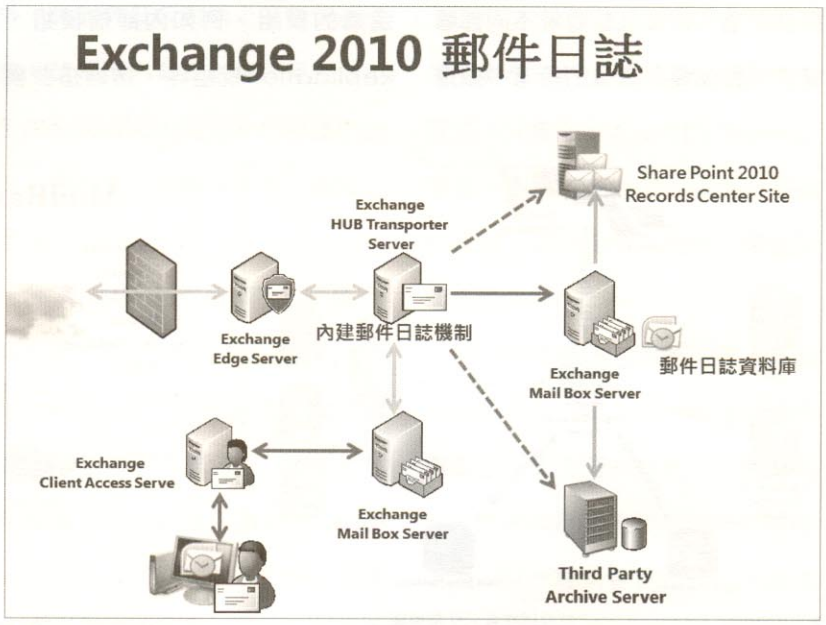
台灣微軟大型企業業務暨經銷事業群專案技術部專案技術經理常志誠表示，新版Exchange Server 2010針對個資外洩防範，提供了兼顧柔性控管與強制保護的雙重機制，前者包括IRM、免責聲明；後者包括郵件仲裁及內容過濾，甚至整封信禁止外送等功能。

就郵件內容保護上，新版Exchange會與微軟資訊版權管理(IRM；Information Rights Management)整合。郵件系統可藉此方便快速地為每封信做好加密保護，這一切只要透過傳輸規則的制定便可搞定，因此可免除過去用手動設定或忘了保護的麻煩。再者，Exchange並支援動態簽名，亦即會自動加上免責聲名，不失為因應個資法規遵循的方便貼心功能。

Exchange Server 2011另外並提供郵件仲裁的預設機制，該功能要求信件在傳輸過程中，可先送交主管核可才能發出。管理人員只需針對特定信件或部門需求，透過設定規則的方式展開郵件仲裁。不僅如此，Exchange另外並針對郵件附件檔提供內容過濾機制，凡不符合安全規則或政策者，便自動將附件剔除掉以策安全。

在日常郵件往來過程中，使用者常常會順手對所收信件按下「全部回覆」，但此舉可能會將信一併寄給不相干的收件者，抑或副本連絡人，進而造成資料外洩的可能。對此，新版Exchange會在回覆信件時，針對可能不合理的收件者發出提示訊息，例如明明是內部信，卻不慎CC 給外部使用者。

在郵件生命週期上，針對個人用戶，早期之際，微軟提供PST檔的封存，新版Exchange則支援線上封存，如此便可透過任何行動裝置上的瀏覽器存取郵件。該軟體並支援保存政策(Retention Policy)的制定，針對不同郵件可透過右鍵



▶ 微軟Exchange 2010郵件日誌架構圖。（圖片來源：台灣微軟）

設定的方式，方便地設定郵件保存年限。除此之外，尚有合法保存機制，該機制會將原始使用者郵件保存在伺服器一段時間，如此可以確保使用者刪除或修改該郵件後，可以迅速回復，以避免誤刪的可能性，進而減輕IT人員的負擔。

台灣微軟營運暨行銷事業群資訊工作者事業部資深產品行銷經理賴柏蓉指出，新版Exchange特別強調郵件搜尋功能，尤其是多重信箱的搜尋機制。管理人員可以方便地授權並提供使用者親和的操作介面，透過方便的關鍵字，快速搜尋到重要的郵件。同時搜尋結果會以清楚來龍去脈的方式排列，方便使用者清楚瀏覽並做更進一步的精準篩選，這對因應法規遵循之郵件調閱有很大幫助。

陳力維表示，當前郵件伺服器軟體的確具備郵件日誌儲存及郵件歸檔機制。但專門性的歸檔方案，能提供更好的儲存管理機制與郵件稽核介面，而這兩點也是因應法規遵循及個資外洩上最重要的兩大要項。

網擎資訊(Openfind)研發協理葉慶章指出，Exchange Server本身的確具備歸檔功能，但相對專門性的歸檔方案並不齊全。原則上僅將信件備份下來，然後進行簡單的管理。尤其是其所提供的Google-like郵件搜尋介面，並無法因應個資防護郵件探勘、快速搜尋及調閱的需求，至於報表功能上也有所差別。

硬體式郵件歸檔設備之部署類型

當前郵件歸檔設備在安裝上會有多種不同方式，而不同的部署模式，會為企業郵件歸檔管理帶來不同的效益及優缺點影響，企業必須針對自身環境與需求，慎選部署模式。不過，當前產品並非所有模式盡皆支援，所以在部署模式的支援性上，也不妨可以納入考量，以做為增加企業導入彈性之依據。目前常見的郵件歸檔部署模式大致分成以下幾種：

1. 閘道(Gateway)模式

閘道模式可說是當前郵件歸檔方案最常見的部署形式，該模式又稱為轉送或中繼模式(Relay Mode)。透過此一安裝方式，所有內送郵件會先經過歸檔設備，先行分類歸檔後，才會轉發至郵件伺服器上。同樣的，所有從郵件伺服器外送的郵件，會在歸檔設備中進行郵件備份後才會發送到外面去。

中華數位(Softnext)產品暨市場營運中心產品經理王智衛表示，該模式的最大好處在於能同時兼顧事前預防及事後稽核的要求，由於所有進出信件都會經過郵件歸檔設備，管理人員便可以設定一些內容過濾的規則，針對內容進行安全篩選，或轉寄給相關主管做進一步的確認後才可內發或外送，如此便可防止不必要的惡意攻擊或資料外洩。

不過，該模式必須變更網路DNS等設定才行。除此之外，閘道模式的最大缺點，莫過於無法對內部信（亦即內對內的信件）進行歸檔備份。對此，另有折衷解決之道，也就是在郵件伺服器上安裝代理程式，讓所有內部信先導到歸檔設備上進行備份後，然後再導回到郵件伺服器上進行正常發送。

葉慶章強調指出，郵件歸檔設備採用閘道模式可能會有高安全風險之疑慮。因為該設備就放在整個網路外圍邊緣處，一旦有任何安全防護上的漏洞或疏失的話，可能會導致機密外洩。這比起郵件伺服器被攻破還要危險，畢竟歸檔設備上存放了長久以來為數可觀的歷史信件，其中難免會有許多機密因而外

洩。如此一來，原本為了個資外洩防護而建置郵件歸檔方案的初衷及本意便蕩然無存了。

除此之外，針對內對內的閘道模式權宜之計，可能會引發同一封信會有兩筆以上日誌的情形。如此會形成郵件管理及查詢上的困擾，尤其在是郵件量非常大的環境或狀況下最嚴重。

2. 郵件複製(Replication)模式

Replication模式亦稱之為Mail Copy模式或Journaling模式，亦即所有進出信件會先進入到郵件伺服器上，在分送到各郵件信箱之前，郵件伺服器本身便會先複製一份到Journal Mailbox之中。然後郵件歸檔設備或歸檔伺服器再從該信箱中自我複製一份，以進行歸檔作業。當然，為了讓郵件伺服器上的郵件能自動複製一份到歸檔機器上，必須先在郵件伺服器進行相關設定才行，但這些設定多半是郵件伺服器軟體預設內建好的，所以比起閘道模式的網路設定會容易得多。

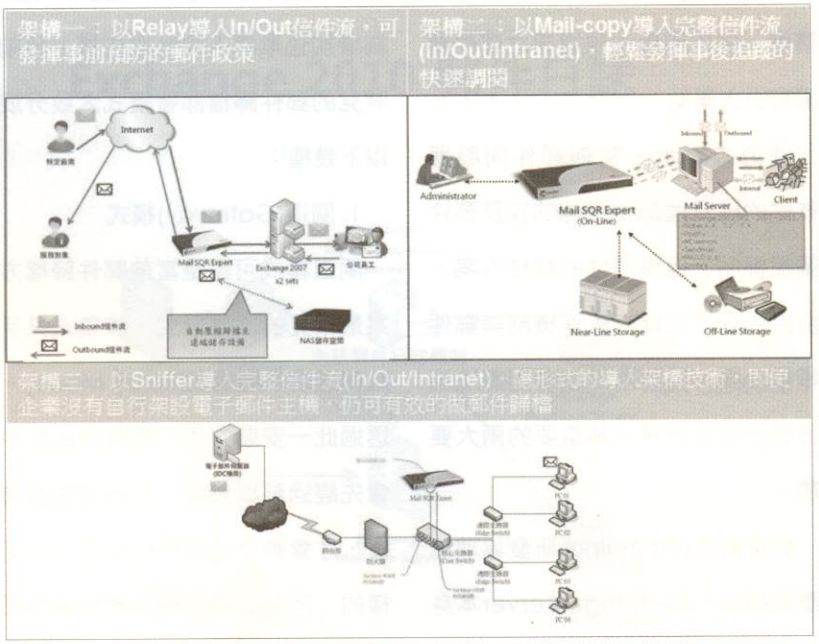
Replication模式的最大好處，在於不論內對外、外對內或內對內的所有信件全都可以備份下來，如此在個資外洩防護或其它法規遵循上才比較完備。另外，在安全上，由於郵件歸檔設備或伺服器位於企業內部，所以會比閘道模式來得安全。

值得注意的，該模式有可能對郵件伺服器的負荷造成一定程度的影響。對此，Openfind產品經理廖享進建議，如果處理郵件的量及負荷過大時，不妨另建一台負責信件轉發備份的專責郵件伺服器，便可讓這個問題獲得抒解。王智衛補充表示，相對於閘道模式， Replication模式會有只能進行事後稽核，而無法兼顧事前預防的缺點。

3. 監聽(Sniffer)模式

所謂監聽模式是專門針對沒有自身郵件主機，而採取郵件主機代管或郵件雲端服務的企業，所專門量身打造的郵件歸檔方案。雖然當前郵件代管或雲端服務供應商有提供額外的郵件備份功能，但該功能僅止於備份而已，與具備檢索功能的郵件歸檔相去甚遠。有鑑於此，市面上遂出現了提供監聽模式的郵件歸檔方案。

該方案可透過對交換器封包映射監聽的方式，進行郵件檢索及歸檔作業，前提是企業內部交換器必須支援網路埠映射(Port Mirror)功能才行。目前市面上提供這類型服務的廠商有中華數位，該公司原本預設支援Relay模式的郵件歸檔設備，允許透過Relication模式及Sniffer模式模組的添購，便能讓使用者享受



▶ 中華數位三大郵件部署架構圖。（圖片來源：中華數位）

到郵件複製，以及對雲端郵件加以歸檔的好處。

採購要訣大剖析

當前郵件歸檔的方案類型繁多，部署模式多元，其中尤以因應法規搜尋的快速調閱能力最為重要。若再加上郵件備份方案的魚目混珠，益使得企業面對郵件歸檔方案的採購變得更加模糊不清。在此特別綜合整理了幾個在採購上務必注意的要點，以做為郵件歸檔方案導入時的參考。

1. 支援監控郵件伺服器功能

郵件歸檔產品是否兼具監控郵件伺服器的功能是很重要的，畢竟郵件伺服器發生問題的話，歸檔機制也會隨之停擺。若有監控機制，便可提早發現郵件伺服器的異常狀況，便可以確保歸檔過程是持續穩定而安全的，而不會發生備份流失的情形。

2. 儲存裝置的支援及管理能力

在儲存方案的搭配上，必須檢視歸檔方案是否支援具備單寫多讀(WORM；Write Once Read Many)機制的儲存方案，這點對於稽核人員而言特別重要，因為可藉此確保所歸檔儲存的郵件內容不致遭到篡改。

以賽門鐵克EV為例，其會將儲存裝置分成不同層級(Tier)，會按時間放在不同層級的儲存裝置之中，並且支援WORM機制。該方案會在儲存中分成供郵件備存的開放儲存區，一旦某儲存區滿了，便會予以關閉並變成唯讀。接下來的待歸檔的郵件會存在另外開放的儲存區中直至存滿為止。如此亦可確保歸檔郵件不致遭到惡意篡改，進而影響日後法規上的種種要求。除此之外，若郵件歸檔能與支援重複資料刪除功能的儲存裝置相搭配，相信能夠有效節省許多儲存空間，並讓儲存空間管理變得更有效率，同時為企業省下可觀的儲存購置成本。

3. 支援歸檔郵件的加密

除了前述WORM儲存裝置的支援及採用之外，另外也可透過加密方式來保障原始郵件內容不會被篡改。廖享進建議，最好是WORM儲存與儲存加密兩種機制都並行支援，如此才可達到IT管理人員與稽核人員分權管理的精神。

4. 支援郵件日誌的備存

除了郵件本身的歸檔外，郵件歸檔方案最好能同時支援郵件日誌的備存功能。畢竟郵件伺服器在進行數量龐大郵件之收發業務時，若要再同時進行郵件日誌作業，難免會使原本郵件處理的效能大受影響。就以賽門鐵克的EV為例，會主動協助郵件伺服器將郵件日誌另外備存出來，進而節省出更多空間，以供其它方面的使用，同時提供方便的介面供使用者搜尋。

5. 良好的分權管理機制

一般企業內各種IT應用與設施的最大權限，多半都掌握在IT人員手中，但在因應郵件歸檔乃至法規遵循時，這個既定的做法勢必需要重新加以審視。換言之，企業必須確實展開IT人員與稽核人員權限分離的分權管理機制，同時最高稽核調閱權應歸稽核或法務人員所有，IT人員只有協助性的安全歸檔政策等制定權限。不僅如此，同為稽核團隊也得實施分權制，亦即將部分權限下放給一般稽核人員，以協助主管進行龐大郵件的審閱工作，對於郵件審閱效率的提升，以及主管工作負荷的分擔會有很大助益。賽門鐵克EV甚至支援郵件審核過程的記錄機制，同時允許稽核人員可在所審郵件中添加註解等功能，這些都可以有效防止郵件審閱過程中不致發生

遺漏或判斷錯誤的情形，並使整個稽核機制及流程更加嚴謹完善。

6. 線上或離線調閱權限的一致性

葉慶章特別強調調閱權限一致性的重要，亦即不論線上或離線郵件的調閱，其權限與功能都必須一致。換言之，即使在離線狀能也能提供與在線時一致的全文檢索及調閱能力，如此才能讓管理更加方便有效率。

7. 快速調閱能力

郵件歸檔除了一般的查詢(Query)之外，並能支援個資監控追蹤、關鍵字過濾等能力。更重要的莫過於快速調閱能力，畢竟新版個資法會要求企業必須因應法律訴訟要求，而能在30天內完成舉證的動作。所以攸關訴訟的郵件必須能及時調閱出來才行。

8. 大規模郵件之歸檔與調閱能力

許多郵件歸檔方案莫不擁有漂亮的規格，但在面對實際郵件流量，甚至一段時間之後累積成堆的郵件量或堆積如山的歷史歸檔郵件時，其歸檔處理能力與調閱能力是否經得起真實考驗，絕對是非常重要的事。這是企業在採購上最需考量的重點，企業不應以現有郵件量的思維面對郵件歸檔方案的採購，而必須精準計算出若干年後成長的可能狀況來採購最適合的產品。

9. 支援災難復原能力

雖然郵件災難復原會是郵件備份方案的最重要強項，但事實上歸檔方案除了符合法規稽核需求之外，因應災難復原的能力也會是採購上的重要考量。唯有如此，才能在個人電腦或郵件伺服器停擺時，快速將之前的郵件乃至正常收發服務復原。不過，仍要看歸檔方案所提供的災難復原的便利性，以及所支援復原格式的數量。

10. 清楚完備的統計報表

透過清楚完整的強力報表統計功能，才能讓企業主管、稽核人員乃至IT人員，清楚掌握郵件歸檔、安全政策實施、郵件調閱等狀況，進而隨時對異常狀況做調整或最佳化處理。雖然郵件伺服器本身即提供許多報表，但歸檔方案若有強大報表能力，也可補足郵件伺服器不足之處，進而讓相關管理人員掌握更精準的訊息，並進而讓郵件歸檔及調閱能力最佳化。

11. 郵件查詢與調閱權的分離

歸檔機制必須提供方便調閱及檢視的機制，並可以查詢到信件內容是否會有任何安全外洩疑慮之處。除此之外，就郵件內容而言，郵件查詢與調閱權必須截然分開。例如特定人員可以進行郵件的查詢搜尋，但卻沒有瀏覽所搜尋郵件內容的權力，如此可避免不必要的個資外洩風險。目前不少郵件歸檔方案並引進類似銀行的雙重認證機制，亦即必須同時會同法務稽核人員才能進行郵件內容的調閱及檢視。

12. 廠商能力及背景

雖然台灣個資法尚未上路，但郵件相關的法規遵循要求事實在國外許多國家行之久年，若廠商能有豐富的海外郵件歸檔部署及導入經驗，相信在因應國內法規需求的方案提供、經驗傳承乃至種種注意要點，都能為企業提供許多實質的助益，所以企業在採購時不妨也將此點納入考量。

13. 支援歷史郵件的滙入方案

對於企業來說，在導入歸檔方案之前，必然會有很大量已經備份好的歷史郵件資料，如何將這些歷史郵件備份資料，悉數納入全新郵件歸檔管理範疇內是很重要的事。