第二章　文獻探討

第一節　線上拍賣風險

一、Martin（2000）

此研究探討電子商務之利益、風險，及內部稽核人員評估企業電子商務活動時需考量之風險。作者系透過觀念性架構之論述，說明電子商務風險之評估。作者認為成功的電子商務可以帶來以下之效益：

1、降低交易成本，提高生產力：企業間利用電子商務可以在供應商管理、庫存管理、配送管理、網路管理及付款管理上獲得利益。

2、全年無休的服務：電子商務消除企業與消費者間時間障礙，企業可以每週七天每天二十四小時提供消費者服務。

3、企業與其供應鏈間溝通之全面改革：電子商務使企業與其供應鏈間可藉由電子化文件的方式迅速地溝通及交易。

4、提供本土企業轉型為全球化企業的機會：由於電子商務消除企業與消費者間空間障礙，可使服務無遠弗屆。

不過，電子商務亦為企業帶來許多風險。企業評估其因電子商務所面臨的風險時，主要要從兩方面來考量：一為電子商務牽涉之人數，二為交易價值。當牽涉人數越多、交易價值越高，風險越大。電子商務代表透過網際網路，世界所有人皆可至此交易。當進入系統的人漸多、範圍漸廣，無形中對企業形成挑戰，不但得保障所有交易，也要保護企業重要資料、資源不受破壞。作者認為在電子商務環境下，企業往往會面臨以下風險：

1、詐欺：企業內部的員工或網路匿名使用者，透過做虛假交易的資料或竄改企業資料，影響企業的紀錄。

2、隱私及保密性的威脅：企業機密資料外洩。

3、缺乏授權：未授權的第三者與企業交易，造成責任歸屬問題。

4、拒絕交易的迫害：系統顯示曾發生交易，但是另一方卻否認曾執行此交易。

5、資料錯誤：未授權的修改資料，造成資料的不完整。

6、企業中斷經營：在災害之後，企業無法繼續經營。

7、不適當的投資：電子商務企業必須重新規劃企業流程，並且建立一些安全機制，但是錯誤的評估往往使得企業接受了較高的風險。

總結作者論述，線上拍賣之風險有詐欺、隱私及保密性的威脅、缺乏授權、拒絕交易的迫害、資料錯誤、企業中斷經營、不適當的投資。於考量電子商務下之內部控制時，必須確定此些風險皆被適當控制。故本論文評估方法建立時需考量上述之風險。

二、Coy（2000）

作者透過觀念性架構論述線上拍賣常見之詐欺情況，認為線上拍賣常見的詐欺情況有二：

（一）得標者的詛咒

買方通常以高於物品實質價值的價格標到物品，使得得標的買家事實上吃虧。這種情況只在物品無客觀價值時，買方以心目中價值競價，才可能不發生。但此情形發生機率較小。另一避免得標者詛咒之方式則為蒐集有關物品的資訊，包括賣方的評價資訊。但在許多情況之中，買方通常跟隨其他競標者動作，使得競標過程行為瘋狂。

（二）串謀

一般的英式拍賣多是採增額出價的方式，因此可能發生傷害賣方之串謀，而此可藉由秘密競標之方式避免，並且進而可顯現產品真實價值。

綜上論述，避免得標者之詛咒方式之一為建立有效評價制度，使買方

於交易前瞭解賣家過去交易行為，以推測其物品品質及價格合理性，幫助買家決定出價金額，避免溢付價金風險。此與拍賣中之串謀風險皆於本論文評估拍賣網站風險架構中探討之。

第二節　內部控制

一、COSO Report

根據 Committee of Sponsoring Organizations of Treadway Commission (COSO) 所發佈的 Internal Control---Integrated Framework，內部控制的設計是為了合理確保達成下列之目標：

（一）營業的效率與效果，

（二）財務報表的可靠性，及

（三）法令的遵循。

企業經營係透過規劃、執行、及監督等過程進行，而內部控制（internal control）正是此過程之一部份，其目的在幫助企業達成其目標。企業為永續經營，須在紀律環境下審慎評估其所面臨之風險，設計適當控制活動以降低風險，並且即時取得適切資訊與企業上下溝通，並且加以監督以確保內部控制品質。因此不論在何種情況下，適當的控制可合理確保其達成績效及營利目標，預防資源損失，幫助企業達成其財務報表可靠、遵循既定法律，避免企業的名聲受損及其他後果。

在 COSO 的架構之下，內部控制包含以下五種要素：

（一）控制環境：此為企業之核心，包含企業內部的人及企業所處的環境，亦是塑造組織文化影響員工控制意識之綜合因素。

（二）風險評估：企業瞭解其面臨的風險，並加以評估的過程。

（三）控制活動：企業為了控制其風險，確保其達成企業目標，於是訂定控制之政策及程序，並予執行並有效落實。

（四）資訊與溝通：使企業內部人於執行、管理和控制營運時，能取得所需資訊並交換此些資訊。

（五）監督：內部控制整體過程須被監督，並適時予以修正。

該五要素並不因企業開始經營電子商務而不同，但在此環境下

經營風險發生變動，企業必須重新評估風險所在，並設計相對應之控制。

內部控制必須保持其有效性。所謂內部控制之有效係董事會和管理階層能合理確保其悉知企業營運目標達成程度、對外報告可靠度且已遵循相關之法律。決定某一類的內部控制是否有效，係基於五組成要素是否存在及其運作是否有效。若內部控制任一組成要素未能合理確保其目標之達成，則代表內部控制有缺失。

根據 COSO Report，內部控制須在內部控制五要素皆有效時才真正產生效用，故當企業進入電子商務時，為達有效內部控制須具備下列之特色：

（一）在控制環境方面：管理階層須建立一合適環境，企業內部人應具有適當能力，並高度正直且具高尚的道德觀。

（二）在風險評估方面：企業必須辨視電子商務下之風險，並判斷何風險須藉由內部控制使其降低於可接受範圍內。

（三）在控制活動方面：辨認風險後，企業須採取行動---控制活動降低此些風險。企業須確定運作系統及企業流程皆已加入控制活動。Hollander 認為在電子商務下，主要控制活動通常包括職能分工、實體控制、資訊處理控制以及回饋機制。

（四）在資訊與溝通方面：電子商務下，系統所提供資訊必須完整且正確以正確報導企業經營結果。而在溝通方面，所有人須瞭解其於系統內部控制中所扮演之角色及責任。

（五）監督：企業必須監督其有關於電子商務之內部控制，以確保其有效運作，並且於必要時適當修改。

二、Sunder（2002）

為解決如何在變動的企業環境下維持適當之控制，Sunder 提出契約模型。其認為企業是與許多經濟體簽訂契約以及盟約之集合體。藉由合約訂

定，個體承諾提供資源，另一方則提供資源作為回報。依據各個體不同目的，與特定他人簽訂不同契約。因此企業的契約可視為資源流動的期望（Expectation）。企業及與其訂約者皆於契約中表達其對未來資源流動的期望。根據 Lin 及 Sunder（2002）的研究，一個個體的行為將會影響他人之期望，而他人將會改變其自身之行為以滿足其已改變的期望。個體皆會管理他人對其之期望。他們會做出適當的期望並且滿足該期望。對於企業而言，若是無法達到期望，將會使企業面臨無法繼續經營之窘境。

而期望的產生往往建立在雙方的共同認知（Common Knowledge）上。所謂的共同認知就是大家所有之知識、知悉他人所有的知識。共同認知是控制的基本要素。由於個體的行為是建立於他人的期望上，所以為達成他人期望的先決條件就是了解他人的信念，而這些信念就是以共同認知來推估。除了共同認知，另一個影響推估他人信念的因素即是文化（Culture）。文化就是在一團體中，對於他人行為期望的共同認知。

組織的控制即是建立在此四個觀念上：契約之集合體：組織、期望、共同認知及文化。控制包含規則、激勵、監督及強制以促使組織的所有參與者之行為與其他參與者之期望一致。控制是實際行為與組織參與者相互期望的平衡。為了使組織順利運作，所有參與者的行為都必須加以控制。尤其是在電子商務之下，顛覆交易的傳統社會關係，電子商務的範圍僅限於連接網際網路及終端共享系統。在此情況下，共同的規範即於交易過程中扮演相當重要的角色。由於網路交易的不透明限制了共同認知，故在電子商務下做好控制較為困難。電子商務往往牽涉了許多直接互相訂約的外部參與者，在所有參與者中建立期望的控制即成了電子商務成功的先決條件。

但是環境的持續變遷往往造成企業控制中斷的威脅。在環境變化的情況下，個體往往會因而改變期望，而原先所訂定之契約極可能無法滿足其期望。於此情況之下，組織若無適當的重新訂約，則可能因缺失或缺乏協

調而倒閉或破產。因此持續對潛在即現有風險加以監控即成為一個重要的管理功能。當環境有所改變時，必須依據環境的變化重新設計契約並將控制調整至最佳狀態。

綜上論述，該篇文獻提供了在電子商務下必須對企業外在參與者加以控制之依據。根據該篇研究可知在電子商務環境下建立一共同依循規範之重要性。而此兩個論點及提供本研究對於拍賣網站使用者需加以控制論點之基礎。

第三節　電子商務及線上拍賣下之內部控制

一、電子商務及線上拍賣下之內部控制

（一）夏安齡（1999）

其以個案研究法探討企業內部控制有效性對導入電子商務成效之影響程度及企業導入電子商務後對原有內部控制有效性之影響。

其認為比較完整的電子商務控制架構包括網路安全控管及網路系統控制，但多偏重於控制活動面。實施電子商務往往會導致組織因整體控制環境及流程之改革，對於控制活動、資訊與溝通及監督等均會產生影響。而網路安全控管包括：

1、 安全政策，

2、 安全意識，

3、 加密，

4、 認證，及

5、 授權。

網路系統控制則包括：

1、 處理程序之整合性，

2、 應用系統之安全控管，

3、 資訊基礎架構存取安全，及

4、 資料轉換。

企業在導入電子商務過程中會受其內部控制有效度影響。由於內部控制有效度對導入電子商務之效益有正面影響，若缺乏有效度的內部控制，導入之電子商務將無法發揮其成效，因而無法成功導入電子商務。企業在導入電子商務後，對於原有之內部控制各要素之有效度會有不同程度的影響。對組織結構、作業目標之制定、資訊之取得與使用、內部與外部之溝通及個別評估會有較強之影響度。透過該篇研究可知電子商務與內部控制

有相當強的互動性，於導入電子商務前、後都必須注意內部控制之有效性。另外，其提出之電子商務控制架構亦有被本研究參考引用。

（二）Pathak（2003）

作者透過過去的文獻，提出電子商務成功因素及其控制架構。其認為電子商務策略之成功因素包括：

1、降低入侵者及其探測之技術，

2、採用電子商務最佳實務，

3、內部稽核人員的參與，

4、顧客的信任其交易過程之適法性，

5、個人資料的隱私保全，及

6、交易安全。

於建立電子商務系統時，必須使內部稽核人員參與以確保有足夠有效的控制。

（三）Yu, Yu, and Chou（2000）

在電子商務的環境之下必須注意以下之控制要素：

1、電子文件傳輸之安全控制：確保資訊於傳輸時的完整性、機密性、隱私性，並且具適當的授權，以避免資料遭竊。

2、保留交易軌跡之控制：企業必須注重內部職能分工及授權，並且盡可能保存交易記錄，以便以後稽查。

3、電子簽章之安全控制：電子簽章不但可以做為確定交易記錄真實性的方法，並且可以證明買賣雙方的交易。由於企業交易的重要性，私密金鑰（private key）和公開金鑰（public key）必須妥善的保管及控制。

4、應用程式及軟體之安全控制：避免不適當的執行程式或是破壞應

用程式或軟體。

5、網際網路服務提供者之控制（Internet Service Providers，ISPs）：ISPs 所採行的控制程序亦必須仔細考量，以確保足夠且有效的交易安全及完整性存在。

6、較早的預防控制點：在電子商務的環境之下，預防控制的控制點較以往要提前，故預防控制必須在開發電子商務應用系統的分析及設計階段即要考慮。

為了完成在奠子商務下之稽核，其提出定期稽核程序模型（Periodical auditing process model，PAPM）以及持續稽核程序模型（Continuous auditing process model，CAPM）。

1、PAPM：利用安全電子技術蒐證及驗證之方式。

2、CAPM：運用及時監控交易系統連結企業的會計資訊系統，以幫助稽核人員偵測異常活動並且產生例外報告。

透過本文可知電子商務下之控制有電子文件傳輸之安全控制、保留交易軌跡之控制、電子簽章之安全控制、應用程式及軟體之安全控制、網際網路服務提供者之控制以及較早的預防控制點，而於本研究發展控制評估方式時皆有加以考慮。

（四）Jarvenpaa and Tiller（2001）

其透過個案研究探討電子商務下個人隱私權之保護。

新技術可以允許電腦使用者保留控制私人資料的權利。公司不可以對於顧客的資料在沒有他們的允許之下擅自作資料採礦、描寫、分析或是任何利用。而線上隱私的主要重點在於降低蒐集及使用資料。

使用者特別關心網站會在他們不知情及未充分揭露資料蒐集的目的的情況下，蒐集他們的資料。大多數的使用者不能辨別他們的機器何時會被追蹤，何時又會禁止追蹤。

隱私主張者辯稱公開隱私政策並遵守政策並不足以保護隱私。他們宣稱，必須為隱私增進技術如：匿名、加密、防火牆、暫時性身份，並且限制揭露以及蒐集個人資料。

總結上述，保護隱私權之方式有公開隱私權政策並遵守政策、增加如匿名、加密、防火牆、暫時性身份以及限制揭露及蒐集個人資料之技術。於本研究中，由於係探討線上拍賣，為辨別使用者之身分以防止交易缺乏完整性，因此除暫時性身份不適用外，其他皆為拍賣網站應採取之相關保護隱私權之控制。

（五）Wurman（2003）

此研究論述線上拍賣之歷史、拍賣之概念，並且建構拍賣之核心架構以及相關補充元素。於建立拍賣系統時，企業須加強用以儲存關於拍賣、競價、使用者及交易資訊之資料庫。使用資料庫可確保資料可靠性及溝通不同系統資料，但為了確保資料庫正確運作，及避免溝通上之瓶頸，須建立妥善的控制。除此之外，拍賣系統須確保所有事件皆依正確發生次序處理，並且是一致的（consistent）、可稽核的（auditable），使使用者能夠透過電子郵件或是藉瀏覽網站以檢視資訊，並妥善考量瀏覽網頁及拍賣規則人數對網站負荷量之影響，以決定其規模。

除了建立良好的拍賣系統外，另須考量下列六項因素：

1、個人化：

授權式個人化視窗。

2、分類及搜尋：

方便使用者尋找物品及相關資訊。

3、付款及保管暨代付服務

4、聲譽管理：

聲譽機制是普遍用以對抗匿名自由之方式。但為避免電子商務下聲

譽欺騙地膨脹，使用者通常於相互交易後才允許使用此機制。為避免具負面評價使用者另外開闢新帳號掩蔽過去不佳行為，eBay 要求使用者提供信用卡號來區辯使用者，但新卡號即可規避此規範。另外，交易者相互利益或懼怕報復等皆可影響聲譽機制可靠性。

5、 審查：

對於拍賣的物品必須審查其不可為：

（1）政治敏感性物品，

（2）非法物品，及

（3）情色、暴力物品。

6、詐欺：

（1）不送貨，

（2）賣家故意哄抬價格，

（3）串謀：買家聯合他人串謀，他人先以極高價競標，買方以合理價競標，他人得標後棄標，使賣家必須將貨賣給買家。

（4）評價勒索（feedback extortion）：買家以給予負面評價要脅賣家降低售價。

（5）誤陷他人詐欺行為。

7、 系統整合：

拍賣系統必須與企業之其他系統整合，以促其經營上之效率。

二、電子商務及線上拍賣內部控制之評估

（一）eSAC

內部稽核人員必須瞭解企業因科技改變所帶來之風險，以及提供管理者系統性的風險管理並且確認系統之可取得性、產能、功能性、具保護性、責任性及可稽核性。eSAC Model 建立在 COSO 的架構之上，主要的目的著重於如何管理由於快速的科技以及電子商務變動所帶來的風險。為了反

應整體環境及科技對於企業所需控制的影響，eSAC 提供一架構模型（如圖 2-1）。

該模型描述企業透過建立策略及目標、依循其本身的價值達成其使命。經過努力運作達成既定的結果，建立企業聲譽並且學習如何於未來改善其績效。一套完整的控制系統，可以幫助企業達成其使命。根據 COSO Report，控制之範圍包括達成營運的效率與效果、提供完整的財務及管理報表，並且依循法律及法令之規範。在電子商務活動之下，控制必須達到可取得性（Availability）、具適當的能力（Capability）、功能性（Functionality）、保護性（Protectability）以及責任性（Accountability）之特性。這些特性也被稱為企業確認目標（Business assurance objective）。以下將詳述各目標。

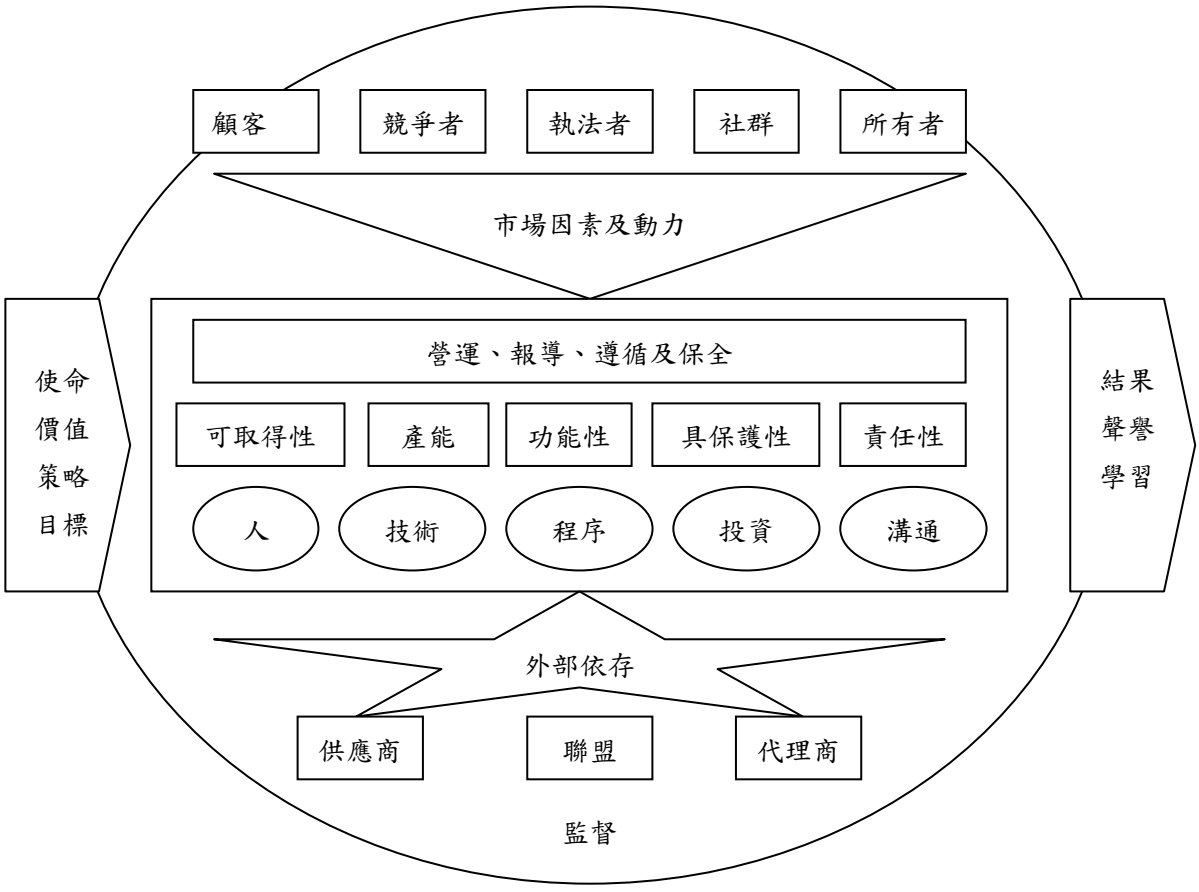

圖 2-1　eSAC Model

1、可取得性

可取得性係指在需要當需要資訊、流程及服務時，必須能夠取得。尤其企業必須以客戶能接受的方式接收、處理及支援交易。為評估可取得性，通常以處理企業經營中斷之控制來衡量。其包括：

（1） 系統資源的實體與邏輯安全，

（2） 檔案儲存裝置的機械壞損，

（3） 軟體故障或是未預期的不相容，及

（4） 不適當的容量規劃。

2、具適當之能力

具適當之能力係指線上的每個節點之互信並能及時的完成交易。系統必須有適當的產能、溝通以及滿足其他的需求，即使是已達最大的需求。為了使系統能夠提供如此的服務，使用的監控，與 ISP（service providers）、ASP（application service providers）服務協定都是重要的控制。而且系統以及流程的瓶頸必須辨識出來並且加以消除或管理，最重要的是要維持跨企業的效率與效果的平衡。

系統的效率是具適當之能力的另一重要組成項目，此將導致資源使用的有效性。為達系統之效率，最有效之作法是管控系統的發展及取得的方法以避免過高的成本及系統不符預期。為了確保資訊系統之效率，必須定期評估對可能造成超支成本、浪費或不效率之風險所做的控制。此項評估可包含：

（1） 預防控制是否不足導致過度的更正錯誤，及

（2） 控制較其所帶來的效益花費更多的成本。

在適當的控制環境下，企業還是必須接受適度的風險。系統發展控制主要在避免系統之不效率而花費過多的成本及於正式的系統之下衍生非正式的系統運作。因此，系統於建置時必須確定有適當之控制並且維持系統

之可稽核性與安全性。

一個不能保持有效的資訊系統將十分不可靠。關於維持系統可靠性的控制為變更控制（Change Control），其控制硬體或軟體變更的時候提供持續性，並且確保所有的變更都經過書面化、核准及確認。而維持控制（Maintenance Control）則包括於程式變更時，讓適當的使用者參與要求、測試及核准、留下適當的審計軌跡、核准資訊科技（IT）及使用者並且將程式變更做足夠書面化。適當的控制可以降低未核准測試程式上線之風險。

3、功能性

功能性係指系統提供容易、具回應且便於使用的特性，以達到使用者的需求。使用者不但包括已熟悉企業系統介面之使用者，而且包括未經訓練的不知名線上使用者。良好的功能性不但包括降低交易處理程序，還包括提供控制資訊及其他管理議題之記錄。為了增進功能性，企業必須評估有關監督及提供回饋之控制，以確保管理者知悉系統功能性之相關問題。

有效性的資訊（Effective information）是由具功能性之系統提供之攸關企業流程之資訊。而攸關的資訊（Relevance information）必須基於要求使用者及管理者的參與以達成功能性之系統的設計而得。系統所產生的資訊必須符合管理者及使用者需求，故於系統發展過程中，使用者必須參與其設計，以確保其可產生有效且攸關之資訊。為了確保有效性，企業必須評估對資訊及時性、正確性、一致性及有用性之控制。

4、保護性

保護性係指保護硬體、軟體及資料免於未授權的入侵、使用或是破壞。由於透過網路，資訊被接近的可能信大大增加，故要維持其安全性相當的困難，因此保護 IT 資源免於損失及當損失發生時能夠辨識出來的控制是必須的。許多目前的控制著眼於減低災難損失、內部舞弊或侵吞的風險。為

了確保保護性，稽核人員必須評估 IT 的一般控制有下列三項：

（1） 資料安全及保密

a、存取資料必須限於已授權之處理及維持資料或記錄。

b、保護組織資料室資訊安全功能及其管理者之責任。

c、安全性功能包括限制透過邏輯的途徑存取資料及程式庫。

（2） 程式安全

a、接近程式檔案或是程式館必須採用進入控制或其他安全軟體將其限於授權人員。

b、程式的更新也必須以圖書管理軟體（library management software）監控。

c、適當的分工亦可確保限制程式撰寫功能進入程式館。

（3） 實體安全：

a、進入處理及儲存裝置必須限於要求進入以執行職務功能者。

b、進入伺服器電腦室亦必須加以監控。含有機密資料的報表之實體控制亦必須執行。

c、實體保護包括免於天災、預防的維修，資料檔案的備份以及資產保險。

保護性之目標在確保資料完整性，也就是資料是完整、正確與及時的，並且不可經未授權的更改。為了確保資料的完整性，稽核人員必須衡量錯誤資料發生的原因，及所有上述的接近控制。更進一步之完整性控制包括：

（1） 授權交易都在最初即完整的紀錄，

（2） 所有的交易都完整且正確的輸入系統以供處理，

（3） 輸入的授權交易皆被系統接受並且完全處理，

（4） 所有的交易僅被處理一次，沒有重複的情況，及

（5） 所有的交易都正確的處理，並且正確的更新檔案以及記錄。

保密及隱私是遵循責任性及實踐可保護性之議題。保密通常指的是智

慧資產、商業機密、競爭性計畫或國際安全。隱私則有關於私人資料。企業需要維護個人必要資料以達使命，但僅止如此略嫌不足。

5、責任性

責任性指的是個體角色、行動及責任。包括資料所有權、認證及授權及所有能夠辨識何者以及什麼啟動交易。所以審計或交易記錄必須提供足夠的資訊證明交易的發生。責任性亦包括不可賴帳的觀念。這代表著一旦確認，使用者不可以放棄這個交易。另外，亦包括准許可追溯接近被限制之資訊及軟體功能的議題。

企業需要確認更改資料檔案或軟體的人。同樣的，握有隱私資訊的企業有義務在揭露資訊時認證要求者身份。在某些情況下，責任性及隱私性是相抵觸的。責任性代表著辨識交易來源，而隱私性則否定此種辨識。這是企業必須謹慎協調的問題。

為了達成責任性，資訊必須適切、正確、及時與可用以管理並達成其責任。為了確認資訊的可靠性，稽核人員需評估不被接受的處理流程及報告，包括：

（1） 資訊不可反駁的被支持：具有交易或審計軌跡。

（2） 資訊及時的提供：在做決策時即可取得資訊。

（3） 依據適用的政策，資訊是一致的：程式或人工不當處理或處理錯誤，通常是造成資訊不一致的原因。管理階層的逾越則是另一個原因。

為了達成上述五項目標，企業必須有適當的基礎、資源及組織承諾。故，企業必須擁有適當的人、技術、程序、投資及溝通以達程目標。複雜的環境促成企業對外的互動及連結增加，並且與外在力量（顧客、競爭者、執法者、社群及所有者）共享、快速變動，並且互相依賴（供應商、聯盟、代理商）。

在模型中動態環境也就是控制環境。為了使環境保持穩定控制，整個環境必須被審慎的監督，以確保企業內、外部之風險已被持續的控制。

綜上所述，eSAC Model 描述了在電子商務的環境下，企業為了達成其目標及使命並且實現其價值，必須以適切的控制來降低其風險。環視企業所面臨的整個環境，eSAC 認為企業必須控制其內、外環境所帶來的風險，以達成可取得性、具適當能力、功能性、保護性以責任性之目標。而為了達成這些目標，企業必須要有適當的人、技術、程序、投資以溝通，並且時時監控整體環境變動及其帶來之風險變動。

（二）Trust Services Principles＆Criteria v1.0

Trust Services Principles＆Criteria v1.0（以下簡稱 Trust Service）之原則主要是論述企業系統必須達成之目標，而準則則是用以達成這些目標的方法，也是用以衡量的標竿。適當的準則應該是客觀的（Objective）、可衡量的（Measurable）、完整的（Complete）而且是攸關的（Relevant）。

Trust Service 之原則及準則主要由四部分構成：

1、政策（Policies）：企業對一相關原則所訂定且書面化之政策。

2、溝通（Communications）：企業必須將其制定之政策與授權之使用者溝通。

3、程序（Procedures）：企業必須使用特定程序以達成其政策之目標。

4、監督（Monitoring）：為了符合企業政策，其必須監控其系統並做出相關因應。

Trust Service 之原則共有下列五項：

1、安全性（Security）：企業需確保其系統免於未授權人實體或邏輯上的接近。

2、可取得性（Availability）：企業確保其系統可依承諾或約定運作及使用。

3、處理之完整性（Processing Integrity）：系統處理必須是完整的、正確的、及時的並且是經授權的。

4、線上隱私性（Online Privacy Program）：經由電子商務蒐集而得的個人資料皆是依承諾或約定蒐集、使用、揭露及保存。

5、機密性（Confidential）：機密資料皆依承諾或約定保護。

在某些電子商務環境之下，政策（terms）及條約（condition）包含雙方之權利、義務及承諾，此對於網站交易顧客有絕對的影響。為了滿足溝通原則，該政策及條約必須揭露於企業網站上供使用者瞭解。

1、安全性原則

安全性原則指的是不論是在實體上或是在邏輯上，保護系統免於未授權之第三者接近。在電子商務及其他系統之下，每個交易者都希望其所提供的資料只有參與交易者或解決後續問題者可取得。透過這些系統傳輸的資訊，都有於傳輸途中或存於該系統時遭未授權人士接近之可能。故，對於系統妥善之接近控制可以避免濫用系統元件、資料遭竊、誤用軟體或不當的接近、使用、更改、毀損、揭露資訊的可能性。

2、可取得性原則

可取得性原則指的是顧客可以如廣告或是與企業訂定之契約、服務條款或其他約定所述接近系統、取得產品及服務。本準則並未設定企業可取得性之最低限度。企業可取得性將限於其與顧客所訂定之合約中。

3、處理之完整性原則

處理之完整性原則係指系統處理之正確性（accuracy）、完整性（completeness）、及時性（timeliness）及授權（authorization）。「正確性」係指確保用以交易之資料於處理過程中保持正確。「完整性」係指所

有的交易皆被處理且無重複處理之情形。「及時性」係指依照合約及時的提供服務或是配送商品。授權則指的是交易的處理依循交易處理政策核准。

處理完整性之風險在於交易無法完整的處理或是服務無法正確的提供。若缺乏妥善的控制，顧客可能無法獲得正確的商品或服務。因此，為了使顧客能夠合理確保其能如預期取得正確的商品或服務，適當的控制是不可缺的。

當資料輸入源自於企業之外，因企業之控制無法加諸企業外部，則可能發生資訊錯誤之情況。故，處理完整性不同於資料完整性，處理完整性並不代表儲存於系統之資訊之完整、正確、及時及已授權。由於資訊是處理系統重要一環，企業對系統之正確、完整、及時及授權控制亦必須將其囊括，在此情況之下，企業必須述明其系統並未包含外部輸入之部分。

4、線上隱私性原則

線上隱私性著重於保護企業可能透過電子商務系統從其客戶蒐集之個人資訊。儘管企業有執行保護這些資訊之控制，這些控制的範圍不僅限於網路為基礎的系統，更應包括其服務提供者。電子商務能夠從個人蒐集其個人及後續與他人交易資訊。有些消費者因為可獲得他們所需之行銷素材而喜歡這些蒐集資訊的動作，但是有另一些人確認為蒐集這些資料是侵害他們的隱私權。所以企業必須告知其的使用者，其會蒐集何項資訊、如何運用這些資訊，並且提供使用者選擇其所提供之資訊。

電子商務具有全球化的性質。為了經營全球化的事業，企業必須依循法令及相關準則對隱私權之規定。除了法令的限制外，顧客通常也會擔心他們所提供的私人資訊是否有受到妥善的保護。若缺乏妥善的控制及揭露相關之保護政策，顧客通常無法安心於此交易。除此之外，就如同與一般的交易，顧客通常會擔心他們抱怨是否會被妥善的處理。當網站不願意或是無法處理顧客抱怨的時候，顧客是否有其他的途徑可尋求？顧客的權利是否有保障？在許多國家已有要求以消費者請求權程序（Consumer

recourse procedure）保障消費者的權利。但是靠傳統法庭來處理是相當費時且昂貴的。所以可透過第三者爭議機制（Third-party dispute mechanism）替消費者提供有效的解決方法。當企業屬於頒佈此等法律的國家時，必須依循此法並且需將其揭露於電子商務網站上。

線上隱私性的標準要求企業必須做到下列兩點：

（1） 承諾採用第三者爭議機制。

（2） 揭露企業無法解決顧客問題時，其所能採行之請求權程序。

在 AICPA/CICA 隱私架構包含九個隱私策略：

（1） 警告（Notice）：企業在其蒐集資訊之前、中、後必須提供與使用者有關其隱私性政策或策略之警告。該警告說明私人資訊之蒐集及其運用。

（2） 選擇及同意（Choice and consent）：企業必須說明使用者有選擇並且同意個人資料之提供、使用、揭露及保存之權利。

（3） 收集（Collection）：企業蒐集之個人資料必須限於其警告中所述之目的。

（4） 使用及保存（Use and retention）：企業對於私人資料的使用必須限於其警告中所述；對於私人資料的保存也僅限於達成其所述之目的，或是滿足法律、法規之要求。

（5） 接近（Access）：企業提供個人可檢視、更新、禁止未來使用及刪除其私人資料。

（6） 移轉及揭露（Onward transfer and disclosure）：企業將私人資料提供於第三人之情況僅限於其警告中所述。除此之外，也僅可將資料揭露於與企業有實質上相當之隱私保護之第三者。

（7） 安全（Security）：企業必須基於資訊之敏感性及價值對保護私人資訊免於遺失、誤用、未授權接近、揭露、更改以及破壞提供合理的預防。

（8） 完整（Integrity）：企業必須維持私人資訊之正確、完整、攸關及可靠。

（9） 管理及強制（Management and enforcement）：企業必須指派一至兩人對企業是否遵循其隱私政策負責並且定期評估其是否遵循其隱私政策。另外，亦必須訂定處理隱私相關疑問及爭議之程序。

5、機密性原則

在溝通及進行商業交易時，通常需提供必須保密之資料。資料於傳輸及儲存於第三者電腦系統時，往往面臨著未授權者接近之風險。在大多數的情況之下，我們都希望我們所提供之資料僅提供予與交易有關或是需解決與交易相關問題的人。為了增進交易者的信心，企業必須提供其機密性政策予其交易者。企業需要揭露其規定授權接近、使用及分享機密資訊之相關政策。而哪些資料會被認定為機密資料，各公司可能大相逕庭，在大多數的情況之下，是明訂於契約之中。所以在與企業訂約時，必須瞭解何資料將以機密方式保存，以及為確保資料之正確及完整之接近更新權利。另外，相關控制，如加密，能於資料傳輸時保護資料的機密性；而防火牆及嚴密的接近控制則能保護存於電腦系統之資訊。

（三）Duh, Jamal, and Sunder（2002）

因為線上拍賣涉及許多不相關的團體，平台操作員必須建立控制內部以及外部人的控制機制。任何未受控制的行為都可能損及拍賣網站的名聲以及影響拍賣網站的成長。這是一個新的控制問題，因為拍賣網站在他們開始使用平台時並不知道任何有關這些交易者的資料。在電子商務下，這些參與交易者可能數以百萬計。另外可能威脅電子商務的是平台操作員在沒有參與交易者的同意之下，蒐集他們私人及交易資訊的能力。這些大量

的電子資料可能因操作員或是其他可以進入擷取資料的外人的誤用帶來新的風險。在線上拍賣下，規則通常用於規範使用者之註冊、認證、列示拍賣物拍賣、評價、付款以及運送。

上述評估架構能夠分析及評估規範：

1、 規範可由其對四個層面的使用者之影響來評估：買家、賣家、員工及操作員。

2、 線上拍賣可由其對拍賣參與者之三貢獻來評估：

（1）資訊的隱私性，

（2）拍賣的完整性，及

（3）交易的安全性。

資訊的隱私性為透過市場上的參與者，尤其是操作者，蒐集而得的資訊僅可用於拍賣參與者提供資訊之目的。根據 Etzioni（1999）所提出之理論，隱私性是否有得到適當的保障可由下列五點來評估：

1、警告及提醒（Notice/Awareness）：在使用者於提供任何私人資料時，必須告知提供者組織對於該資訊之處理策略。

2、選擇及同意（Choice/Consent）：資料提供者應可以選擇他的資料可用於何時，特別是非為該交易之用途。

3、存取及參與（Access/Participation）：資料提供者應可以存取有關於他的資訊，並於資料錯誤或不完整的時候作更改。

4、完整及安全（Integrity/Security）：蒐集資訊者必須採取適當的步驟，以確保資料的完整。若要將該資料作為他用時，必須將不合時宜的資料刪除或是將資料變更為匿名。

5、執行及糾正（Enforcement/Redress）：必須要有強化隱私政策之機制存在。

拍賣的完整性係指確保買家欲意、能夠且真正依其承諾適當且及時支付賣家；相對的，亦確保賣家依約定時程於收到付款後運送正確的貨品給

買家。其主要目的即在交易詐欺及虛假交易。相關於完整性之常見詐欺行為包含：

1、誘標（shill bidding）：賣方充當買方向自己下標以抬高物品的價格。

2、偷標（bid-siphoning）：買方藉由觀察對自己出售之商品有興趣的買家，私下透過電子郵件聯絡、買賣，以規避服務費用。

3、圍標及假出價（bid-shielding）：兩個或者是更多的買家（也可能是擁有多重帳號者）串謀，故意將買價抬高，使其他人卻步，但在結標之前高價者抽單，使其共謀者能夠以較低的價格買到。

4、得標者不付款，惡意棄標。

5、賣家可能誤刊貨品之品質或特性，拍賣贋品，非法或是盜版商品，或是提供與得標者錯誤的物品。

6、拍賣違法或違規物品。

7、缺乏員工交易限制之規定。

8、評價方面的詐欺行為：

（1） 假信用評價（shill feedback）：串謀或是使用兩個帳號互相給予良好的評價

（2） 信用評價轟炸：串謀陷害競爭者，給予其不良評價

（3） 強索信用評價（feedback extortion）

（4） 吸引信用評價（feedback solicitation）

而為了不使交易之完整性受到侵害，企業必須採行適當的控制，以降低詐欺行為的發生。

交易之安全性係指交易之程序及記錄免於參與者或第三者不當的侵入。一個安全的市場必須有適當的控制程序辨識使用者、控制接近資料並且避免未授權之資料揭露，並且避免第三者竄改拍賣參與者之回饋記錄。在安全性下，線上拍賣的主要風險為：

1、不適當的終端讀取公司的資料：駭客竊取帳號、密碼以及信用卡號，或假造評價。

2、外部攻擊引起服務中斷：病毒及中斷服務攻擊，導致訴訟的危機。

針對上述二項風險，主要可採行的控制有：

1、針對不適當的終端存取公司的資料有關的控制：

（1） 加密，

（2） 防火牆，

（3） 防毒軟體，

（4） 授權程序，

（5） 內部資料傳輸及存取政策，

（6） 伺服器及硬體的擺置與接近控制，

（7） 以加密的形式儲存資料，

（8） 備份以及回復系統，

（9） 定期內部稽核，及

（10）網路監控。

2、針對外部攻擊引起服務中斷有關的控制：

（1） 防毒軟體，

（2） 網路監控，

（3） 災害回復，

（4） 緊急回應小組，及

（5） 快取技術。

依據該評估架構，其可以高階層（High Level）來評估線上拍賣網站之控制（如表 2-1）亦可以微觀（Micro Level）的方式方式來評估（如表 2-2）。高階層評估方式係採線上拍賣控制對其四使用者之三目標。每個格子內所代表的即是相關的控制方式。低階層的評估方式，主要用以衡量控制對於各使用者控制目標之影響，以確保風險已被適當的控制。

本研究根據該篇文獻，將線上拍賣之控制分為隱私性、完整性以及安全性三方面來探討。除此之外，本篇文獻所提及線上拍賣之風險及控制亦於本研究建立控制評估方式時加以評估。

表 2-1　高階層控制流程

	使用者			
目標	買家	賣家	員工	操作者
隱私性	（1）檢視賣家所給的評價，並且給予回應。 （2）編輯檔案中的資料。	（1）檢視買家所給的評價，並且給予回應。 （2）編輯檔案中的資料。	（1）簽署保密協定。	（1）沒有參與者的同意之下，不使用拍賣資料作其他的用途。
完整性	（1）要求買家提供信用卡號，並且使用他們的真名交易。	（1）要求賣家提供信用卡號，並且使用他們的真名交易。	（1）禁止員工參與拍賣交易。	（1）不允許交易者在最後一分鐘放棄競標。
安全性	（1）給每一個買家唯一的會員編號以及密碼。	（1）給每一個賣家唯一的會員編號以及密碼。	（1）限制察看保留價格。	（1）資料加密、病毒防護軟體以及防火牆的設置。

資料來源：Rong-Ruey, Karim, Shyam（2002），p32

表 2-2　低階層控制控制流程

	使用者			
目標	買家	賣家	員工	操作員
隱私性	—	—		
完整性	—	＋		
安全性				

資料來源：Rong-Ruey, Karim, Shyam（2002），p32

第四節　使用者之信賴

一、Suh and Han（2003）

Suh and Han 藉由網站調查 502 個網路銀行使用者對於安全控制之認知，再以實證分析哪些安全控制項目會影響顧客對於電子商務之信任，並驗證信任對於電子商務之接受程度有重要的影響。

其認為許多人都不願意在網站上提供敏感的私人資訊，因為他們不信任電子商務的安全性。這些感覺是因為他們不止覺得網路及電子商務安全性的缺乏，而且也不相信那些衡量標準。而顧客的疑慮是電子商務發展的障礙。另外，資訊、服務遭竊及資料錯誤的風險是安全性的一大挑戰。匿名使得網路詐欺的可能性大幅上升，因為對於追蹤服務的使用相當的困難。除此之外，竊聽者也可能在資料的傳輸過程中竊取資訊。如果安全性發生問題，很可能回影響企業的形象，甚至遭到法律上的刑罰。

Suh and Han 認為安全控制主要有下列五項，而顧客對於此五項安全控制之認知則會影響其對電子商務之信任：

1、 辨識性（Authentication）：在電子交易及溝通的過程中，與我們互動的人，就是其宣稱者。

2、 不可否認性（Nonrepudiation）：交易者不可在事後否認參與過交易。

3、 保密性（Confidentiality）：在交易者間的溝通事項只限於與交易有關的人知道。

4、 隱私保護（Privacy protection）：在電子交易過程中所蒐集的私人資訊都被保護免於同意外之揭露。

5、 資料完整性（Data integrity）：交易中的資料不被非法的創造、攔截、竄改、或刪除。

信任（Trust）係指在事先不知的情況之下，信賴他人承諾的信念是加

諸善意之人。而信任有下列三個特徵：

1、 能力（Competence）：信任者相信被信任者有能力為自己作所需作的事情。

2、 慈愛（Benevolence）：信任者相信被信任者會作對信任者好的事，排除任何自利的動機。

3、 完整（Integrity）：被信任者訂立良好信賴合約，誠信的言行，並且達成承諾。

相較於其他情況，電子商務環境存有固有之不確定性與風險，並缺乏合約與保障，因此，「信任」更顯得重要。

Suh and Hane 根據科技接受模型（Technology acceptance model，TAM）提出了下述之五個假說：

1、 確認性、不可否認性、保密性、隱私保護以及資料完整性對於顧客在電子商務環境下的信任性有正面的影響。

2、 信任性對於顧客對於使用電子商務交易之態度有正面的影響。

3、 信任性對於顧客使用電子商務交易之意圖有正面的影響。

4、 使用電子商務的態度對於顧客使用電子商務之意圖有正面的影響。

5、 使用電子商務的意圖對於顧客實際上是否使用電子商務交易有正面的影響。

根據實證結果，其研究結果為：

1、 不可否認性、隱私保護及資料完整對於顧客在電子商務環境下的信任性有正面的影響。

2、 信任性對於顧客使用電子商務交易之態度及意圖有正面的影響。

3、 使用電子商務的態度對於顧客使用電子商務之意圖有正面的影響。

4、 使用電子商務的意圖對於顧客實際上是否使用電子商務交易的確

有正面之影響。

二、Patton and Josang（2004）

Patton 及 Josang 認為增進顧客對電子商務信任之因素包括：

1、藉由網頁介面溝通信任性

網站上必須提供足夠的資訊並且讓使用者便於使用。

2、隱私性

必須提供足夠的隱私權保護，降低顧客之風險。

3、自我規範以及信任標章

適當的規範以及網站上貼有信任標章者可增進顧客的信任度。

4、安全性

顧客只願意相信有足夠安全保護並且致力發展及部署安全服務之電子商務企業。

5、付款中介者及保險提供者

付款中介者以及保險提供者以第三者的角度監督電子商務，故可使顧客感到較高的信任感。

6、聲譽系統

聲譽系統提供了一個在電子商務環境下，增強陌生人間相互信任的方法。此機制提供給使用者決定該相信誰並且提供其表現良好的誘因。

7、爭議解決機制（Alternative dispute resolution，ADR）

ADR 是另一個可增進信任之機制。當爭議情況發生且企業無法順利解決時，如果顧客獲得一個公平、可靠且有效的解決方式，則其將會更有信任感。

由本文獻可知良好的介面、隱私權、自我規範及標章、安全性、付款中介者及保險者、聲譽系統以及爭議解決機制皆是可增進顧客信任之因

素。於本研究探討顧客對拍賣網站交易安全控制之滿意度時，皆加以考量。

三、Herzberg and Mass（2004）

其結合科技接受模型（Technology acceptance model，TAM）及信任與風險的觀念，驗證：

1、 顧客交易意願將正向影響其交易行為。

2、 顧客於線上交易之意願與其對電子商務之信任有正向關係。

3、 顧客交易意願與其對網路介面有用性之認知有正向之關係。

4、 顧客交易意願與其對網路介面易於使用性之認知有正向之關係。

5、 網路介面之有用性及易使用性有正向之關係。

6、 顧客線上交易意願與風險認知有負向之關係。

7、 顧客信任與網路介面之有用性有正向之關係。

8、 顧客信任與網路介面易於使用性有正向之關係。

9、 顧客之風險認知與電子商務之信任有負向之關係。

檢驗後，皆為顯著之結果支持其假說。根據研究結果，信任及風險認知皆直接影響顧客之交易意願，此代表者降低不確定性是使得顧客接受電子商務之重要因素。另外，由於顧客對於網路介面有用性及易於使用性之認知對其信任有正向之影響，以及顧客對風險之認知亦對信任有反像支影響，可知概念化以及顧客認知對於信任有相當大的影像。此外，認知的介面有用性及易於使用性對於交易意願之正面影響，代表者 TAM 可以延伸至電子商務解釋顧客之接受行為。

根據本篇文獻可知顧客認知之良好的網路介面以及較低的風險皆可增進顧客的信任，並進而影響其交易之意願。因此根據此一論點，本研究認為企業必須設計符合顧客滿意之介面，並且提供足夠之控制降低風險至顧客可接受之範圍內，才可促進顧客於拍賣網站交易之意願。

四、Klein and O'Keefe（1999）

本文獻以 TeleTrade 為例，論述品質以及信任於線上拍賣之重要性。

TeleTrade 之事先註冊要求即為一監控潛在拍賣者的方法，而且信賴對於吸收潛在客戶來說相當重要。信賴可以藉由嚴格設立的制度以及交易平台提供者（auctioneer）建立的信任制度來達成。當考量品質時，第三者，也就是交易平台提供者，必須提供保護及控制機制來確保交易品質並且減少執行交易的危機。在選擇交易平台提供者以及拍賣的管理架構時，信任往往扮演一個很重要的角色。對於一個與 TeleTrade 相似的拍賣地來說，信任以及品質控制在面對許多新競爭者時即為一競爭優勢。

所以，以下兩種關係必須仔細探討：

1、 直接交易關係（買、賣雙方的關係）

2、 服務提供關係（交易平台提供者以及交易者之間的關係）

由於拍賣之良好聲譽以及對有效設立的規範以及交易系統之信任能夠替代由人與人間的信任，因此交易者間的鬆散關係可就由交易者與交易平台提供者間的信任關係來彌補。

根據本篇文獻可知成功的拍賣交易平台必須有良好的品質並取得顧客的信任，而交易平台本身也扮演了一個增進交易者間信任感的中介。因此其不但必須提供安全保護機制以減少交易危機，而且還必須建立良好的聲譽並設立值得信任之規範以及系統。

五、Noll（2001）

由於在電子商務的環境下不確定的問題相當嚴重，但信任是社會行為上必要的要求，故企業必須提升自身的可信度。而提升可信度之方式有二：

1、提高顧客的熟悉度

熟悉度是信任的前提，而在電子商務的環境下，主要是來自於電子商務網頁的設計。其必須滿足的條件有：

（1） 商店環境：包括提供完整的商品資訊、良好的瀏覽功能以及整個網頁的便性。

（2） 顧客：包含顧客之認知、決策及行動。良好的網站可以幫助顧客快速建立認知、做出決策並採取行動。越複雜的搜尋及交易步驟越會使顧客改變心意。

（3） 良好的網路技術，使企業運可有效率地達到既定目標。

2、聲譽機制的採用

確保行為值得信任之管理機制，使企業於銷售、配送及付款皆非企業本身經營的情況下，依然能夠取得顧客的信任。

第五節　研究延伸

本節根據本章前述之文獻對於電子商務下內部控制及其評量方式以及使用者對於電子商務之信任接受相關文獻，說明本研究參酌過去文獻，並補充其不足之處，以作為研究設計之依據。本節共分兩部分：（一）線上拍賣環境下，內部控制評估方式之彙整及延伸，以及（二）線上拍賣環境下，內部控制對使用者信任度影響之彙整。

一、線上拍賣環境下，內部控制評估方式之彙整及延伸

（一）線上拍賣環境下，內部控制評估方式之彙整

控制係為了避免企業無法達成營業之目標而設置，故於討論線上拍賣之適當控制前，必須對企業經營線上拍賣時所面臨之風險有相當程度的瞭解。由上述之文獻回顧可以彙整出線上拍賣企業會面臨之風險，如表 2-3 所示。這些風險有些源自於企業本身資訊系統安全性之疑慮，另一些則來自於線上拍賣業務所引發之風險。前者涉及企業內實體、軟體及資料之安全；後者則牽涉使用者隱私權及交易過程之保障。然而，顧客隱私權及交易過程之保障，必須仰賴可靠的系統運作才可達成，因此企業資訊系統之風險亦會影響資訊隱私及交易完整（如圖 2-2）。因此，本研究將線上拍賣所涉及之風險以及其相關控制皆分為如 Duh, Jamal, and Sunder（2002）所建議之資訊的隱私性、拍賣的完整性以及交易的安全性三方面來探討。

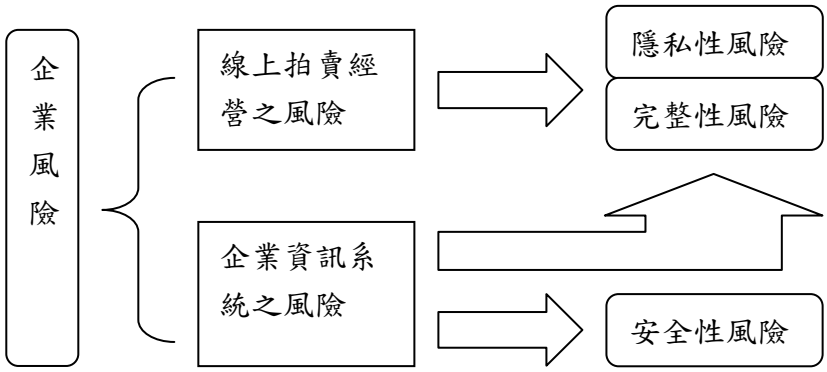

圖 2-2　線上拍賣風險分析

1、隱私性風險

隱私性風險在於市場上參與者所蒐集之私人或機密資料，未經資訊所有者之同意，被擅自用於交易以外之用途。當顧客之隱私性要求無法被滿足時，即會發生隱私性之風險。根據 Etzioni（1999）所提出之理論，當使用者之資料被蒐集前，未提出適當的警告及提醒、無法自行選擇同意提供何資料、無法對其所提供之資料進行存取及做適當之變更，或是資料蒐集者無法對資料提供完整之保護，或訂定必要之隱私權政策並定期檢視時，即可能產生隱私性之風險。

2、完整性風險

完整性風險在於拍賣過程無法公平且完整的完成（如圖 2-3）。此類風險涉及

（1） 未對拍賣物品做好適當監督，使得不合規定之物品亦於網站上拍賣；

（2） 能夠接近拍賣資料的員工（如知曉拍賣底價），因缺乏適當的政策規範，亦可如一般人般參與拍賣；

（3） 網頁介面管理不當，無法使使用者易於找尋所需物品；

（4） 評價機制缺乏適當管理，使得使用者錯誤評估買家、賣家

之過去交易誠信；以及

（5） 交易詐欺，包含買家無意願購買其所承諾的購貨，或無能力及時付款，或是賣家無法在約定期間之內提供允諾販售的商品。

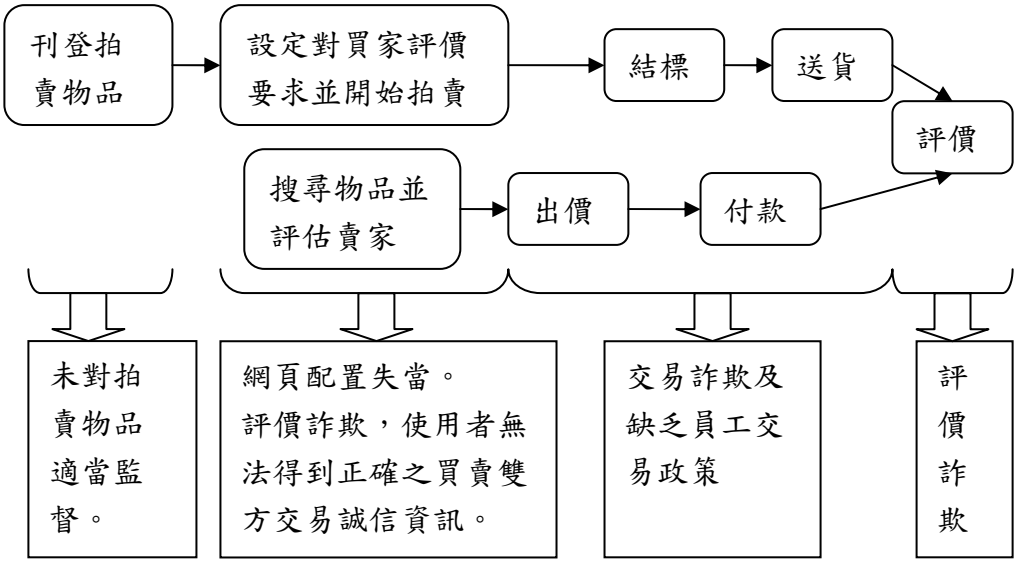

圖 2-3　　完整性風險

3、安全性風險

安全性風險在於企業系統無法順利運作，以及交易流程與紀錄遭受參與者或其他闖入系統者之不當使用或竄改。此類之風險因子包括；

（1） 系統缺乏可取得性，讓使用者無法順利取得資訊及進行交易：

a、使用錯誤的軟、硬體，

b、系統缺乏效率、效果，

c、系統容量不足，以及

d、不適當的投資。

（2） 企業資料缺乏妥善保護：

a、未授權的更改、竊取資料以及竄改交易資料，

b、機密資料外洩，及

c、系統缺乏審計、交易軌跡。

（3） 外部攻擊引起服務中斷

茲將上述之各類風險及其組成要素，彙整如表 2-3。

表 2-3　線上拍賣風險彙總

分類	風險	風險因子	相關文獻
隱私性	市場上參與者所蒐集之私人或機密資料除了用於交易之外，在未經資訊擁有者之同意，被擅自用於該資訊做交易以外之用途。	在未告知使用者的情況下蒐集資訊。	Etzioni（1999） Jarvenpaa and Tiller（2001）
		無法自行選擇同意提供何資料。	
		無法對其所提供之資料進行存取及做適當之變更。	
		資料蒐集者無法對資料提供完整之保護。	
		資料蒐集者無法訂定必要之隱私權政策並定期檢視之。	
完整性	完整性之風險在於拍賣過程無法公平並且完整的完成。	付款以及貨品交易無法提供完整的保障。	Martin（2001） Pathak（2003） Duh, Jamal and Sunder（2002）
		缺乏對拍賣物品之審核。	
		網頁介面管理不當。	
		使用者之交易詐欺行為： 誘標 偷標 圍標 拒絕付款 誤刊商品特性 販賣違法物品或贓物 虛假交易 拒絕交易的迫害 使用者缺乏授權 逃避必要費用	
		缺乏規範員工之政策，危害顧客權益或企業名聲。	

分類	風險	風險因子	相關文獻
		缺乏有效的評價制度，因而出現評價詐欺： 信用評價轟炸 假信用評價 強索信用評價 吸引信用評價	
安全性	企業系統無法順利運作，以及交易流程及紀錄遭受參與者或其他闖入系統者的不正當行為。	系統缺乏可取得性： 使用錯誤的軟、硬體 系統缺乏效率、效果 系統容量不足 不適當的投資	Pathak（2003） Denys（2000） Duh, Jamal and Sunder（2002）
		企業資料缺乏妥善保護及保全： 未授權的更改、竊取資料以及竄改交易資料 機密資料外洩 系統缺乏審計、交易軌跡	
		外部攻擊引起服務中斷	

為了降低上述風險，企業必須採行相關的控制。根據過去的文獻以及eSAC、Trust Services Principles＆Criteria v1.0 提出之控制之目標及準則，茲將線上拍賣所需做到之相關控制目標及其準則彙整如下。

1、資訊隱私性之相關控制目標及準則

根據過去文獻，有關保護個人資料隱私之控制目標包括：

（1） 揭露及蒐集個人資料之限制，

（2） 個人辨識及授權傳輸及變更資料，

（3） 資料傳輸之隱私性，

（4） 隱私資料保護，以及

（5） 建立適當之隱私權政策，並定期評估政策及其執行之有效性。

此外，Trust Service 之隱私性以及機密性亦與本研究之隱私性有關，其所述之控制目標則有：

（1） 政策：企業必須制定其保護由電子商務所蒐集之個人資訊及保護資訊機密性之政策。

（2） 溝通：企業必須向內部或外部使用者溝通其所訂定之保護個人資料及機密資訊之政策。

（3） 程序：企業為依循其政策達成其隱私及機密性目標之程序。

（4） 監督：企業監督系統並且採取適當之行動，以維持其符合保護個人資訊以及機密性政策。

上述之，「政策」即在於建立適當之隱私權政策，並定期評估其有效性；「溝通」就是必須揭露其蒐集、使用個人及機密資料之方式及限制；「程序」則是用來保護資料傳輸及儲存時的隱私與安全性，包含授權適當的人員可存取隱私性資料；而「監督」則是必須持續的檢視隱私及機密政策是否適當的執行。因此，Trust Service 中之政策、溝通、程序及監督之目標已包含於前述文獻提及之目標。本研究將採用文獻中所述之五控制目標，作為線上拍賣隱私性所應達成之控制目標。

再者，Etzioni（1999）指出，隱私性是否得到適當的保障，可由下列五點來評估：

（1） 警告及提醒，

（2） 選擇及同意，

（3） 存取及參與，

（4） 完整及安全，以及

（5） 執行及糾正。

而在 TRUSTe 中，企業隱私性係依據下列各準則來評估：

（1） 採行考量網站以及顧客擔心之線上個人資訊為目的所制訂的隱私權政策。

（2） 透過隱私權政策,揭露對於使用者個人資訊之蒐集及使用方式。

（3） 給予使用者選擇及同意如何使用及分享其個人資訊之權利。

（4） 制訂資料安全、品質及存取之衡量，用以保護、更新及更正個人辨識性資料。

至於 AICPA/CICA 隱私架構則包含九項隱私策略：警告、選擇及同意、收集、使用及保存、存取、移轉及揭露、安全、完整與管理及強制，並延伸出 Trust Service 中有關線上隱私及機密性兩項與隱私性相關之控制目標與準則。

綜上所述，與隱私性相關之控制目標可彙整比較如表 2-4。

表 2-4　隱私性控制目標彙總比較

Etzioni（1999）	**TRUSTe**	**AICPA/CICA 隱私架構**	**相關文獻**
警告及提醒	透過隱私權政策,揭露對於使用者個人資訊之蒐集及使用。	警告、收集、使用及保存、移轉及揭露	揭露及蒐集個人資料之限制
選擇及同意	給予使用者選擇及同意如何使用及分享其個人資訊之權利。	選擇同意	
存取及參與	制定資料安全、品質及接近之衡量，用以保護、更新及更正個人辨識性資料。	接近	個人辨識及授權傳輸及變更資料
完整及安全	制定資料安全、品質及接近之衡量，用以保護、更新及更正個人辨識性資料。	安全、完整	資料傳輸之隱私性、隱私資料保護
執行及糾正	採行考量網站以及顧客擔心之線上個人資訊為目的所制定的隱私權政策。	管理及強制	建立適當之隱私權政策並定期評估政策及其執行有效性

為了達成上述之控制目標，企業必須採行適當之步驟及方法。根據 Trust Service，控制準則是用以達成控制目標之方法，其隱私性及機密性中之控制準則，符合本研究所定義之隱私性目標。

2、拍賣完整性之相關控制目標及準則

根據過去的文獻，有關保護拍賣完整性之控制目標包括：

（1） 完善的網頁：使用者可便利的尋找所需之物品。

（2） 身份具辨識性：使用者不可冒充他人，以他人名義交易。

（3） 交易不可否認性：一旦承諾交易，買賣雙方皆有義務完成交易。

（4） 良好的聲譽系統：交易前可評估交易者之誠信，並於交易後留下對此次交易之意見，以供未來交易者之參考。

（5） 良好的爭議解決機制：當企業無法解決顧客問題時，有其他之方式可用以解決顧客與企業間之爭議。

在 eSAC 中，關於責任性以及功能性兩項目標，亦是在交易完整性中需達成者。責任性代表著交易者之身份必須是可辨識，必須對其所做的交易負責到底；功能性則指企業網站的便於使用性，以及對使用者使用困擾做出回應，以達到使用者的需求。因此，本研究將採過去文獻中彙整出之五項控制目標作為線上拍賣交易完整性之控制目標。

在 Duh, Jamal, and Sunder（2002）以及 Patton and Josang（2004）之研究指出，關於完整性之控制準則包括：

（1） 辨識使用者（如提供信用卡號）並且要求其以真名交易，

（2） 禁止知悉拍賣資訊之員工參與拍賣交易，

（3） 不允許交易者在最後一分鐘放棄競標，

（4） 採用並管理評價機制，

（5） 採用付款中介人機制，以及

（6） 採用保險機制。

此外，根據 Trust Serice 中處理完整性的部分可知，達成交易完整性之相關準則有：

A、溝通

企業備有對其系統及範圍之客觀描述，並將其與授權使用者溝通。如果是電子商務系統，則需另於網站上揭露其他的資訊。該資訊包括但不限於下列各項：

（1） 商品或服務之描述，

（2） 經營電子商務之政策及條約，

（3） 企業於其網站上揭露顧客可從何處取得售後服務保障、維修服務以及其他於網站上購買之貨物或服務之相關支援，以及

（4） 有關解決處理完整性議題之程序。此處理程序可包含顧客交易之任何一環節，包含對商品或服務品質、正確、完整、以及無法適當處理抱怨之抱怨。

B、程序

（1） 關於完整、正確、及時及授權輸入之程序與訂定之系統處理完整性政策相符。若是電子商務系統，企業需在交易處理前取得顧客正面確認。

（2） 關於完整、正確、及時及授權系統處理之程序，包括錯誤更正及資料庫管理，需與企業所訂定之系統處理完整性政策相符。若是電子商務系統，企業之程序還需包括但不限於下列各項：

a、正確的貨品及數量在要求的時限內送達，服務及資訊亦如顧客之要求提供，以及

b、例外情況需立即與顧客溝通。

（3） 關於完整、正確、及時及授權輸出之程序，需與企業所訂定之

系統處理完整性政策相符。若是電子商務系統，企業之程序還需包括但不限於下列各項：

a、企業於處理交易前向顧客列示售價及其他相關之成本、費用，

b、發出交易帳單，以及

c、立即更正帳單或付款錯誤。

線上拍賣不同於一般的電子商務之處在於賣方並非企業本身，因此，部分交易的處理過程需要由賣方來執行。但企業為了保障買方之權益，必須對賣方處理交易之行為加以控制，對於買方亦同。然而，就如同 Trust Service 當中所規定者，該準則皆是規範在電子商務下之賣方---企業所需達到的控制，對於一個交易平台提供者應該如何規範其賣家及買家，目前之理論及實務皆缺乏完整的控制準則及控制評估方式。因此，本研究就企業應控制其風險為由，推論企業為降低其所面臨之風險此採取之作為即為其控制，而企業是否能夠規避前述之完整性風險，則可用來評估交易完整性是否完善。

3、交易安全性之相關控制目標及準則

根據過去的文獻，有關保護交易安全性之控制目標包括：

（1） 安全政策及安全意識，

（2） 應用系統、程式及軟體之安全控管，

（3） 處理程序的完整性，

（4） 資料傳輸之完整性，

（5） 資料保密性及完整性，以及

（6） 系統之可取得性。

前述之 eSAC 可取得性、具適當之能力、功能性、保護性以及責任性，以及 Trust Service 中之安全性、可取得性以及處理之完整性，皆與本研究所定義之安全性有關。所謂「可取得性」係指在需要資訊、流程以及服務

時，必須能夠取得，因此，可取得性之目的，可包含文獻中之應用系統之安全控制系統之可取得性。「具適當之能力」係指線上的每個節點之互信並能及時的完成交易，也就是必須對 ISP 以及應用系統以及程式軟體做適當的控制。「功能性」係指系統提供容易、具回應且便於使用的特性，以達到使用者的需求，包括必須提供及時且攸關的資訊給予管理者以及使用者，也就是必須適時的產生例外報告，此項目標必須仰賴企業足夠的安全意識以及資料保存的完整性。「保護性」以及「安全性」係指保護硬體、軟體以及資料免於未授權的入侵、使用或是破壞，因此必須保護系統、程式以及資料的安全及完整。「責任性」指的是個體角色、行動以及責任，在責任性之下必須區別出交易執行以及系統、程式與資料存取之職能，故必須保存完整的資料以證明交易及存取的發生。此外，藉由職能分工，可確保系統、程式以及資料的完整及安全性。「處理之完整性」則指系統處理必須是完整、正確、及時並經過授權，以保證存於系統內之資料的正確性。因此，本研究據以彙整出之六項線上拍賣安全性之控制目標。

茲將上述三類風險及相關控制目標彙整於表 2-5。

表 2-5　線上拍賣風險及控制目標彙整

分類	風險	控制目標	相關文獻
隱私性	（1）在未告知使用者的情況下蒐集資訊 （2）無法自行選擇同意提供何資料 （3）無法對其所提供之資料進行存取及做適當之變更 （4）資料蒐集者無法對資料提供完整之保護 （5）資料蒐集者無法訂定必要之隱私權政策並定期檢視之	（1）警告及提醒 （2）選擇及同意 （3）存取及參與 （4）完整及安全 （5）執行及糾正	Yu, Yu and Chou（2000） Jarvenpaa and Tiller（2001） Patton and Josang（2004） Suh and Han（2000） Etzioni（1999）
完整性	（1）付款以及貨品交易無法提供完整的保障 （2）缺乏對拍賣物品之審核 （3）網頁管理不當 （4）使用者之交易詐欺行為 （5）缺乏規範員工之政策以致於危害顧客權益或企業名聲 （6）缺乏有效的評價制度，使得出現評價詐欺	（1）完善的網頁 （2）身份辨識性 （3）交易不可否認性 （4）良好的聲譽系統 （5）爭議解決機制	Patton and Josang（2004） Yu, Yu and Chou（2000） Suh and Han（2003） Noll（2001）
安全性	（1）系統缺乏可取得性 （2）系統缺乏審計、交易軌跡 （3）企業資料缺乏妥善保護 （4）外部攻擊引起服務中斷	(1)安全政策及安全意識 （2）應用系統、程式及軟體之安全控管 （3）處理程序之完整性 （4）資料傳輸之完整性 (5)資料保密性及完整性 （6）系統之可取得性	夏安齡（1999） Yu, Yu and Chou（2000） Jarvenpaa and Tiller（2001） Suh and Han（2003） Patton and Josang（2004）

（二）線上拍賣環境下，內部控制評估方式之延伸

本研究針對前數之內部控制目標及其評估，進行下列之研究延伸。

1、 安全性方面

本研究對於安全性風險之定義為企業系統無法順利運作，以及交易流

程及紀錄遭受參與者或其他闖入系統者的不正當行為。然而，當企業系統無法順利運作時，也包含企業之線上拍賣網站無法順利運作、當機或是拍賣功能的不健全，皆會影響拍賣之完整性。而交易流程及記錄遭受參與者或其他闖入系統者之不當行為，除了資料、紀錄可能遭到竄改之外，企業所蒐集之顧客個人資料亦可能遭竊，隱私性也會遭受影響。因此，本研究認為，隱私性及完整性之目標必須仰賴安全性才可達成。

另一方面，本研究對於控制準則之評估係以 Trust Service 中所列示之準則為基礎。根據上述之風險分析可知，企業資訊系統之風險亦會影響線上隱私性及交易完整性目標之達成。然而，Trust Service 係將營業及系統之風險混於各主題中論述，造成各原則中出現重複的準則。因此，本研究基於隱私性、完整性以及安全性三大主題，另依照風險來源區分為拍賣經營風險及企業資訊系統風險，將企業資訊系統風險之隱私性及完整性部分，併入安全性之範疇，而將相關之控制目的及準則分為三大項（如表 2-6）：

表 2-6　控制準則分類

	隱私性	完整性	安全性
針對企業拍賣經營風險之控制			
針對企業資訊系統風險之控制			

2、 隱私性方面

過去的文獻所討論的大多是如何保護使用者之隱私權免於受到迫害，較少論及在顧客隱私權遭受侵害時該如何處理。然而，在 Trust Service 所列示之控制準則中，確有述及應於隱私權政策內點明，並與使用者溝通當企業對於未遵循其隱私權政策時，其應採取之解決方式。因此，本研究將「申訴及保障」增列為隱私性控制目標之一。

3、**完整性方面**

由文獻整理出之完整性風險及控制目標整理如下表。

表 2-7　完整性風險及控制目標對應

完整性之風險	**完整性之控制目標**	
付款以及貨品交易無法提供完整的保障		爭議解決機制
缺乏對拍賣物品之審核		
網頁管理失當	完善的網頁	
使用者之交易詐欺行為	身份具辨識性、交易不可否認性	
缺乏規範員工之政策		
缺乏有效的評價制度	身份具辨識性、良好的聲譽系統	

由上表可知，文獻中之控制目標並無法因應完整性風險，因此，本研究針對付款以及貨品交易無法提供完整的保障以及缺乏對拍賣物品之審核兩類風險，增列「適當的交易保障」以及「適當審核拍賣物品」兩項完整性控制目標。此外，有關使用者之交易詐欺行為所帶來的風險，不能僅藉由身份具辨識性及交易不可否認性加以消除，因此，本研究加入「交易公平性」以彌補其不足。至於缺乏規範員工之政策之風險，即指在缺乏規範之下，員工有進行交易詐欺之風險，因此本研究將其併入交易公平性此控制目標下。再者，本研究認為完整性控制之基礎在於企業必須制訂其完整性政策，並定期檢視其達成程度，因此增列「政策之執行與糾正」做為所有控制目標之基礎。

根據上述控制準則分類表，本研究先將所有控制目標加以分類，以利以下控制評估準則之產生。

表 2-8　控制目標分類

	隱私性	完整性	安全性
針對企業拍賣經營風險之控制	警告及提醒 選擇及同意 存取及參與 執行及糾正 申訴及保障	完善的網頁 身份辨識性 交易不可否認性 良好的聲譽系統 爭議解決機制 適當的交易保障 適當審核拍賣物品 政策之執行與糾正	
針對企業資訊系統之風險之控制	安全政策及安全意識 應用系統、程式及軟體之安全控管 處理程序之完整性 資料傳輸之完整性 資料保密性及完整性 系統之可取得性		

此外，由於 Trust Service 並未對隱私性、完整性列出完整之控制準則，本研究增加下列之控制準則：

1、隱私性之控制準則

針對存取及參與之控制目的，本研究增加下列之控制準則：

（1） 存有使用者對其所提供之資訊可隨時存取之程序。

（2） 存有使用者對其所提供之資訊，可隨時就已改變或是錯誤的部分提出變更及修正之程序。

2、完整性之控制準則

過去的研究以及實務上之評估準則多缺乏對於完整性控制準則之論述，因此，本研究根據完整性風險，研擬出如表 2-9 之控制準則。

表 2-9　完整性風險及控制準則之對照

完整性風險	完整性控制準則	
付款以及貨品交易無法提供完整的保障	【政策、溝通】 1、限制使用者需以真名交易 2、制定保護交易雙方收款及收貨之政策，包含但不限於： （1）採用付款中介者； （2）施行保險政策。 【程序】 1、交易之程序規定交易人必須以註冊之真名交易。 2、企業有關於保護交易雙方收款及收貨之執行程序。	【政策】 1、制定交易完整性之相關政策，並定期審閱之。 2、必須於完整性政策內述明當發生企業無法解決之完整性議題時，使用者可尋求之其他解決爭議之方式。
缺乏對拍賣物品之審核	【政策、溝通】 1、定義禁止拍賣之物品，並且加以審核。 2、禁止刊登不合規定之物品。 【程序】 1、企業具有審核拍賣物品之程序。 2、企業具有移除不合規定拍賣品刊登之程序。	【溝通】 1、與使用者溝通完整性之相關政策，以及發現完整性遭破壞時，像企業溝通以及抱怨之方式。 2、企業備有對其系統及範圍之客觀描述，並將其與授權使用者溝通。如果是電子商務系統，則需另於網站上揭露其他的資訊。該資訊包括但不限於下列各項： 商品或服務之描述： （1）其經營電子商務之政策及條約； （2）企業於其網站上揭露顧客可從何處取得售後
使用者之交易詐欺行為	【政策、溝通】 1、禁止使用雙重帳號。 2、禁止偷標、誘標、圍標之行為。 3、禁止惡意棄標行為。 4、訂定適當之刊登規則，避免錯誤之刊登方式及內容。 【程序】 1、有避免及發現使用雙重帳號之程序。 2、有避免或發現偷標、誘標、圍標之行為之程序。 3、具有正當之棄標程序。 4、具有惡意棄標之申訴程序。 5、有使用者可依循之刊登方式之程序。 6、有發現及移除錯誤刊登之程序。	
缺乏規範員工之政策以	【政策、溝通】 制定關於企業內部員工交易之相關政	

完整性風險	完整性控制準則	
致於危害顧客權益或企業名聲	策。 【程序】 1、有員工交易時須依循之額外程序。	服務保障、維修服務以及其他於網站上購買之貨物或服務之相關支援。 （3）有關解決處理完整性議題之程序。 【監督】 1、企業必須定期檢視其保障交易完整性之執行結果，並且與完整性政策相比對。 2、辨識並指出對企業目前以及未來環境對達成其完整性政策目標之潛在危害。
缺乏有效的評價制度，使得出現評價詐欺	【政策、溝通】 1、禁止使用雙重帳號。 2、禁止信用評價轟炸。 3、禁止販售信用評價。 4、禁止強索及吸引信用評價。 【程序】 1、有避免及發現使用雙重帳號之程序。 2、有避免及發現販售信用評價之程序。 3、有供以申訴並解決評價詐欺之程序。	

根據相關文獻彙整出之控制目標，以及 Trust Service 中所提及之控制準則，本研究彙整出下列之控制準則。

1、隱私性控制評估準則

隱私性針對企業拍賣經營風險之控制目標有：

（1） 警告及提醒，

（2） 選擇及同意，

（3） 存取及參與，以及

（4） 執行及糾正。

針對以上控制目標，茲彙整 Trust Service 之控制準則以及本研究增列之控制準則列於下表，以作為本研究之隱私性控制評估標準，如表 2-10。

表 2-10　隱私性控制評估標準

隱私性控制目標	Trust Service Criteria
警告及提醒	【溝通】 1、企業備有對其系統及範圍之客觀描述，並將其與授權使用者溝通。 2、線上隱私及相關安全之義務及承諾必須與授權使用者溝通，並揭露於網站上。 （1）特定類型之資訊之蒐集、保存、使用以及分配與第三者之可能性。 （2）顧客拒絕提供資訊或是選擇不使用特定資訊之後果。 3、如果企業網站使用 Cookies 或是其他追蹤方式，企業必須揭露其使用方式。如果顧客拒絕使用 Cookies，必須揭露其拒絕之後果。 4、向授權使用者溝通取得支援及通知企業有關線上隱私、機密性及系統安全之破壞情形之程序。 5、當企業之隱私權及機密性政策有變更或廢止之情事時，必須提供顧客清楚且明顯的政策變更警告。 6、當顧客離開企業隱私權政策所涵蓋之網頁時，必須有適當警告。 7、企業之線上隱私及相關安全政策必須包含述明： （1）資料保存及銷毀之政策。 （2）提供顧客有關於資訊收集之警告。 8、機密性及相關安全之義務及承諾於機密性資料提供時，必須與授權使用者溝通。這些溝通包含但不限於下列各項： （1）資訊如何分類為機密資訊。 （2）授權如何接近機密資訊。 （3）如何使用機密資訊。 （4）如果資訊提供予第三者，需揭露第三者機密性策略及控制之限制，否則則代表企業信賴第三者之機密性策略予其相當或更勝之。 （5）機密性政策需符合相關法律與法規。 【程序】 1、企業之程序規定個人資訊僅提供予與交易相關之個體，除非顧客再提供資訊之前有接收到明顯的警告。 2、企業程序規定機密資訊僅揭露與規定於機密性及相關安全政策內者。

隱私性控制目標	Trust Service Criteria
選擇及同意	【溝通】 1、線上隱私及相關安全之義務及承諾必須與授權使用者溝通，並揭露於網站上。 （1）顧客有權選擇其提供何資訊以及該資訊之使用及分配方式，而這些選擇並不可影響其交易。 （2）在收集及傳送電子商務交易所需之敏感性資料時，顧客必須有權選擇是否繼續。 2、企業之線上隱私及相關安全政策必須包含提供顧客選擇收集資料的種類。 【程序】 1、若於提供資訊實無清楚之警告，在提供資訊予第三者前亦必須取得顧客之同意。 2、下載之檔案及資訊於使用者電腦上儲存、變更或複製前，必須取得顧客之同意。 （1）如果顧客指出其不希望使用 Cookies，則企業必須控制確保 Cookies 並未存於顧客之電腦。 （2）企業要求顧客允許其於顧客電腦上儲存、變更或複製資訊。 3、揭露之隱私政策廢止或變更時，企業必須有適當的程序依循其提供資訊當時之政策保護個人資訊，或是取得顧客依循新政策之同意。
存取及參與	【政策】 企業之線上隱私及相關安全政策必須包含允許顧客更新、更正其資訊。 【補充】 1、存有使用者對其所提供之資訊，可隨時存取之程序。 2、存有使用者對其所提供之資訊，可隨時針對以改變或是錯誤的部分提出變更及修正之程序。
執行及糾正	【政策】 1、企業需建立並且由指派之個人或小組定期審閱及核准企業之隱私、系統機密性及相關之安全政策。 2、企業線上隱私及相關安全政策及其之變更、更新之責任必須妥善劃分。 3、企業之線上隱私、機密性及相關安全政策必須包含辨識並且遵循相關法律、法規及服務層級之約定或其他契約之規定。

隱私性控制目標	Trust Service Criteria
	【監督】 1、企業之隱私、機密性及安全表現必須定期的檢視並與其所訂定之線上隱私與安全政策相比對。 2、可辨識並指出對企業目前達成其隱私、機密及安全政策目標之潛在危害。 3、監控環境及科技之變更並評估其對企業線上隱私、機密性及安全之影響。 4、企業揭露其他需符合之法律、法規或任何企業參與之自我約束計畫之其他隱私策略。
申訴及保障	【政策】 1、企業之機密及安全保護必須包含聲明如何處理與機密性及相關安全有關之抱怨。 2、企業之線上隱私及相關安全政策必須包含聲明如何處理與線上隱私及相關安全有關之抱怨，以及使用第三者爭議處理機制之程序。 【程序】 企業需揭露當企業無法解決隱私議題時，顧客可採取之請求權程序。這些議題包括收集、使用及分配個人資訊以及企業無法解決這些議題之後果。此解決程序可包含下列特徵。 （1）管理者顧客不滿企業解決方式時，對於採用特定第三者爭議排解服務或其他法令規定之方式之承諾。 （2）解決爭議之程序。 （3）當爭議解決之後，需對個人資訊做何使用及採行哪些步驟。

2、完整性控制評估準則

完整性之控制目標有：

（1） 完善的網頁，

（2） 身份辨識性，

（3） 交易不可否認性，

（4） 良好的聲譽系統，

（5） 適當審核拍賣物品，

（6） 適當的交易保障，

（7） 交易公平性，

（8） 政策之執行與糾正，以及

（9） 爭議解決機制。

針對上述之控制目標，茲將前述依風險延伸出之控制準則，彙整為本研究評估完整性控制評估標準。

表 2-11　完整性控制評估標準

完整性控制目標	控制準則
完善的網頁	【政策、溝通】 訂定適當之刊登規則，避免錯誤之刊登方式及內容。 【程序】 1、有使用者可依循之刊登方式之程序。 2、有發現及移除錯誤刊登之程序。
身份辨識性	【政策、溝通】 禁止使用雙重帳號。 【程序】 有避免及發現使用雙重帳號之程序。
交易不可否認性	【政策、溝通】 1、禁止惡意棄標行為。 2、限制使用者需以真名交易。 【程序】 1、交易之程序規定交易人必須以註冊之真名交易。 2、具有正當之棄標程序。 3、具有惡意棄標之申訴程序。
良好的聲譽系統	【政策、溝通】 1、禁止使用雙重帳號。 2、禁止信用評價轟炸。 3、禁止販售信用評價。 4、禁止強索及吸引信用評價。 【程序】 1、有避免及發現使用雙重帳號之程序。 2、有避免及發現販售信用評價之程序。

完整性控制目標	控制準則
	3、有供以申訴並解決評價詐欺之程序。
適當審核拍賣物品	【政策、溝通】 1、定義禁止拍賣之物品，並且加以審核。 2、禁止刊登不合規定之物品。 【程序】 1、企業具有審核拍賣物品之程序。 2、企業具有移除不合規定拍賣品刊登之程序。
適當審核拍賣物品	【政策、溝通】 制定保護交易雙方收款及收貨之政策，包含但不限於： （1）採用付款中介者； （2）施行保險政策。 【程序】 企業有關於保護交易雙方收款及收貨之執行程序。
交易公平性	【政策、溝通】 1、制定關於企業內部員工交易之相關政策。 2、禁止偷標、誘標、圍標之行為。 【程序】 1、有避免或發現偷標、誘標、圍標之行為之程序。 2、有員工交易時須依循之額外程序。
政策之執行與糾正	【政策】 制定交易完整性之相關政策，並定期審閱之。 【監督】 1、企業必須定期檢視其保障交易完整性之執行結果，並且與完整性政策相比對。 2、辨識並指出對企業目前以及未來環境對達成完整性政策之風險。
爭議解決機制	【政策】 必須於完整性政策內述明當發生企業無法解決之完整性議題時，使用者可尋求之其他解決爭議之方式。 【溝通】 與使用者溝通完整性之相關政策，以及發現完整性遭破壞時，像企業溝通以及抱怨之方式。

3、安全性控制評估準則

安全性之控制目標有：

1、 安全政策及安全意識，

2、 應用系統、程式及軟體之安全控管，

3、 處理程序的完整性，

4、 資料傳輸之完整性，

5、 資料保密性及完整性，以及

6、 系統之可取得性。

針對上述之安全性控制目標，茲彙整如表 2-12 之安全性控制評估準則。

表 2-12　安全性控制評估準則

安全性控制目標	Trust Service Criteria
安全政策及安全意識	【政策】 1、企業需建立並且由指派之個人或小組定期審閱及核准企業之安全性、可取得性以及處理完整性政策。 2、企業之安全性政策必須包含，但不限於下列之項目： （1）辨識並且將政策與對授權使用者之相關要求書面化。 （2）允許接近並定義接近的本質及誰被授權接近。 （3）避免未授權的接近。 （4）增加新使用者、變更現有使用者的接近程度，以及移除不存在使用者之程序。 （5）劃分線上隱私及相關安全之責任。 （6）劃分系統變更及維護之責任。 （7）系統元件在使用前必須先行測試、評估及授權。 （8）聲明如何處理之抱怨，以及使用第三者爭議處理機制之程序。 （9）處理破壞事件之程序。 （10）處理未於政策中提及之例外情況之條款。 （11）提供支援政策之訓練及其他資源。 （12）辨識並且遵循相關法律、法規及服務層級之約定或其他契約之規定。 （13)依據與顧客之承諾或其他協定之復原及繼續服務計畫。 （14）監控系統產能以滿足與顧客承諾及約定之系統可取得

	性。 3、企業政策及其之變更、更新之責任必須妥善劃分。 【監督】 1、企業之安全性、可取得性以及處理完整性表現必須定期的檢視並與其所訂定之安全性以及處理完整性政策相比對。 2、可辨識並指出對企業目前達成其安全性、可取得性以及處理完整性政策目標之潛在危害。 3、監控環境及科技之變更並評估其對企業安全性、可取得性以及處理完整性之影響。
應用系統、程式及軟體之安全控管	【溝通】 1、企業備有對其系統及範圍之客觀描述，並將其與授權使用者溝通。 2、使用者之義務及企業對使用者之承諾必須與授權使用者溝通。 3、企業政策及其變更、更新之責任必須溝通與企業內對其有責並執行該政策者。 4、影響系統隱私性、機密性、安全性、可取得性及之變更必須向會受其影響之管理者及使用者溝通。 【程序】 1、存在限制邏輯性存取系統 2、存在限制實體存取系統 3、存在保護系統免於未授權者邏輯存取之程序。 4、存在保護免於電腦病毒、惡意程式以及未授權軟體破壞之程序。 5、存在對破壞安全性、可取得性事件之辨識、報導及回應程序。 6、當發生不符安全性、可取得性政策時必須迅速的辨識並且及時的採取應變措施之程序。 7、設計、取得、執行、配置、修改及管理與安全性有關之架構及軟體必須與訂定之政策一致，以確保授權之存取以及避免未授權之存取。 8、存有程序規定個人對影響安全性之系統之設計、發展、建置及操作之責任。 9、存有保護系統元件，包括與訂定之政策一致之架構之程序。 10、存有程序規定系統僅可接受授權、經測試且書面化之變更。 11、存有要求緊急變更需書面化及授權之程序。
處理程序	【程序】

的完整性	1、關於完整、正確、及時及授權輸入之程序與訂定之系統處理完整性政策相符。若是電子商務系統，企業之程序還需包括但不限於下列各項。 （1）檢查每個要求及交易之正確性及完整性。 （2）在交易處理前取得顧客正面確認。 2、關於完整、正確、及時及授權系統處理之程序，包括錯誤更正及資料庫管理，需與企業所訂定之系統處理完整性政策相符。若是電子商務系統，企業之程序還需包括但不限於下列各項。 （1）正確的貨品及數量在要求的時限內送達，服務及資訊亦如顧客要求之提供。 （2）例外情況需立即與顧客溝通。 （3）傳入之訊息皆正確及完整的處理並發送至正確的 IP 位址。 （4）輸出之訊息皆正確及完整的處理並發送至網際網路服務提供者之存取點。 （5）當訊息於服務提供者之網路傳輸時，必須確保其密封完整。 3、關於完整、正確、及時及授權輸出之程序，需與企業所訂定之系統處理完整性政策相符。若是電子商務系統，企業之程序還需包括但不限於下列各項。 （1）企業於處理交易前向顧客列示售價及其他相關之成本、費用。 （2）發出交易帳單。 （3）立即更正帳單或付款錯誤。 4、有追蹤資料從來源輸入至最後處置之程序。
資料傳輸之完整性	【程序】 1、使用者之辨識及相當之資料於網際網路上傳輸時，使用加密或是相當之安全技術保護之。
資料保密性及完整性	【程序】 1、企業之程序規定經電子商務收集之資料僅由員工使用於企業經營。 2、存在限制透過電子商務之邏輯性接近個人資料之程序，包括但不限於下列各項： （1）新使用者之註冊及授權。 （2）辨識所有使用者。 （3）變更及更新使用者資訊之程序。 （4）准許接近系統特權及允許之程序。

	（5）限制接近系統架構、超級使用者功能、主密碼以及安全機制。 3、存在限制實體接近存有保護透過電子商務所收集之個人資訊之企業系統。
系統之可取得性	【溝通】 向授權使用者溝通通知企業有關系統安全、可取得性遭受破壞之情形以及提出抱怨之程序。 【程序】 1、保護系統免於遭受中斷運作或是損害系統可取得性風險之程序。 2、備份、離線儲存、復原及災害回復需符合系統可取得性及相關安全政策之程序。 3、維持資料備份及系統的完整性以遵循系統可取得性及相關安全政策之程序。

但由於在本研究無法取得個案公司完整的安全性政策，因此僅就其餘網站上公布之政策加以評估，故評估準則之部分僅就與使用者溝通之部分評估之。

二、線上拍賣內部控制對使用者信任度之影響

根據過去的文獻，影響使用者信任之因素有：

（1） 辨識性，

（2） 交易不可否認性，

（3） 保密性，

（4） 隱私保護，

（5） 資料完整性，

（6） 網頁介面溝通，

（7） 自我規範以及信任標章，

（8） 安全性，

（9） 付款中介者及保險提供者，

（10）聲譽系統，以及

（11）爭議解決機制。

本研究對於風險以及相關之控制皆以隱私性、完整性以及安全性加以分類，故將上述影響使用者信任之因素分類於表 2-13。

表 2-13　影響使用者信任因素之分類

	影響使用者信任之因素	
隱私性	保密性	自我規範以及信任標章、爭議解決機制
完整性	辨識性、交易不可否認性、網頁介面溝通、付款中介者及保險提供者、聲譽系統	
安全性	隱私保護、資料完整性、安全性	

本研究根據上述之信任因素，設計「拍賣網站交易安全機制問卷」，作為蒐集使用者對相關事項看法之工具。