致理技術學院

商務科技管理系

實 務 專 題 報 告

企業資訊安全政策施行架構
—以電信業為例

指導老師：郭正華 教授

學生：蔡嘉容 19533106

李育玫 19533108

陳璟瑩 19533114

劉蕙慈 19533140

謝佩勳 19533143

中華民國 98 年 12 月

致理技術學院

商務科技管理系

實 務 專 題 報 告

企業資訊安全政策施行架構
—以電信業為例

學生：蔡嘉容 19533106

李育玫 19533108

陳璟瑩 19533114

劉蕙慈 19533140

謝佩勳 19533143

本成果報告書經審查及口試合格特此證明。

指導老師：_____

中華民國　98 年　12 月

CTM 實務專題研究授權書

本授權書所授權之實務專題研究為 蔡嘉容、李育玫、陳璟瑩、劉蕙慈、謝佩勳 共 5 人，在致理技術學院商務科技管理系 98 學年度第 1 學期完成商管實務專題。

商管實務專題名稱： 企業資訊安全政策施行架構－以電信業為例

■同意 □不同意

本組同學共 5 人，皆同意著作財產權之論文全文資料，授予教育部指定送繳之圖書館及本人畢業學校圖書館，為學術研究之目的以各種方法重製，或為上述目的再授權他人以各種方法重製，不限地域與時間，惟每人以一份為限。

上述授權內容均無須訂立讓與及授權契約書。依本授權之發行權為非專屬性發行權利。依本授權所為之收錄、重製、發行及學術研發利用均為無償。上述同意與不同意之欄位若未勾選，該組同學皆同意視同授權。

指導教授姓名:

專題生簽名: 學號:

專題生簽名: 學號:

專題生簽名: 學號:

專題生簽名: 學號:

專題生簽名: 學號:

中華民國 98 年 12 月

誌　　謝

回顧在致理漫長的求學歲月，在即將落幕的時刻除了豐收的雀躍心情之外，還有許多的感謝與不捨，大學生涯過程中的點點滴滴，絕非這短短言語所能表達，在專題寫作的過程，只能用“倍感艱辛”來形容。

首先要感謝系主任陳明郁教授以及系上每一位師長的熱心指導下，給予我們足夠的空間揮灑自己的想法，面對困境時，從旁協助指導與鼓勵，使我們更有信心完成。特別感謝**專題指導教授郭正華博士**的細心帶領與指導下，給予我們許多建議與分析的方向，使我們得以進入企業資訊安全的研究領域，讓我們能就學理面、管理制度、及能給予我們無限的鼓勵，在他的諄諄教誨下皆能迎刃而解，使我們能深入瞭解資訊安全管理範疇，對於研究的方向、觀念的啓迪、架構的匡正、資料的提供與求學的態度逐一斧正與細細關懷，於此獻上最深的敬意與謝意，師恩浩瀚，銘感於心。

其次感謝**國立臺北科技大學資訊工程系陳英一主任**的專業知識領域下，提供我們不少關於系統內容的精闢建議，適時的解答各種疑惑，使我們在企業資訊安全知識、解決問題上與專題寫作過程中提供我們莫大的幫助，讓我們受益良多，獲益匪淺，謹在此致上最高的謝意。

藉由這次專題團隊合作的經驗，讓我們學習到互相幫助與包容，以及合理的溝通協商方式，爲我們留下許多珍貴回憶。

最後，再次感謝專題製作期間所有幫助過我們的師長與同學，謝謝你們，在此我們致上最誠摯的謝意。

摘　　要

資訊安全是企業的一項重要議題，而其管理已漸漸成爲企業要強化投資者信心，降低營運風險與快速達成符規(Compliance)時的首要策略。在許多的案例中，資訊安全施行的驅動力是來自於外部法案(如沙氏法案與HIPAA)、資安規範(如 ISO 17999，COBIT，與 ITIL)，或者是內部商業行爲與倫理準則。對於任何支援符規(Compliance)的協同流程而言，其資訊安全施行的最大考量在於是否能夠將無結構的資安政策轉換爲結構化且可施行與稽核的規則。本研究提出一個多層次的政策趨動式資訊安全施行架構(PDSE)來協助導引企業建置資訊安全的機制，流程，與管理。這個架構不但使用了持續監視與審計的機制，並且將 ITIL 的變革管理也一併考量。這個架構目前已實際建置於中華電信，成功地展現其持續改善流程、降低符規成本、提升符規彈性與資安施行效率的多項效益。

關鍵詞：資訊安全政策、符規、連續性審計、變革管理、沙氏法案、聯邦健康保險法案

Abstract

Information security enforcement is an issue of paramount importance for organizations, with its management increasingly becoming a strategic imperative as organization seeks to boost investor confidence while reducing operational risks and decreasing time-to-compliance. In many cases, the driver for proper information security enforcement derives either from external regulations (such as Sarbanes-Oxley and HIPAA), security management standards (such as ISO 17999, COBIT and ITIL), or internal stipulations like codes of ethics or business conducts. For any process that support cooperative work geared toward compliance, the primary concern of security management is actually the enforcement of structured and auditable rules, which are the descendents of the unstructured policies derived from regulations, standards, or codes. A multi-level policy driven security enforcement (PDSE) framework that incorporated the concepts and mechanisms of continual auditing and monitoring, and change management is proposed and discussed in this paper to address the issue. This PDSE framework has been implemented in a telecom company, demonstrating its usefulness of continual process improvement, reduced compliance cost, increased compliance flexibility and improved security enforcement efficiency.

Keywords: security policy, compliance, continuous auditing, change management, Sarbanes-Oxley, HIPAA

目　　錄

圖　目　錄

表 目 錄

第一章　緒論

1.1　研究背景

自從 1990 年代出現在網際網路上的全球資訊網(World Wide Web, WWW)，與幾項創新的資料整理及搜尋技術，諸如Directory、Indexing、Search services 等，以及多媒體技術的進步，使網際網路的資料傳播及表現更加有效率與多元化[1]，也爲人類帶來無限的美好遠景，而網路也已成爲全世界各國產官學界不可或缺的資訊基礎建設。然而，不可諱言，衍生而來的高科技、高智慧的犯罪型態與案件也就層出不窮。由於網路乃開放性架構，稍有不慎，均可能造成各企業、組織無可挽回的有形或無形的財產損失。像是未經授權者（如駭客）侵入電腦系統，竊取或更改資料甚至更動原系統設定；合法電腦使用人員有意或無心，造成資料的毀損、竊取或系統破壞；資料在傳輸中途被截取、窺竊或變更；電腦感染病毒與傳遞病毒等等。

在實例上，曾有傳聞某國家中學生可透過電腦網路窺得該國國防機密、電腦駭客傳送病毒破壞我駐美機構網站、國內某銀行遭駭客侵入內部網路篡盜客戶存款、徵信社業者勾結不肖警員及電信人員竊取個人電腦資料、電腦維修商透過網路進入機關資料庫窺得限閱資料等。一般來說，許多企業並不瞭解何時應該用什麼方式來解決，故根本的方式就是讓企業充分瞭解現今電子商務環境下充斥著何種威脅，以及現有技術對此威脅防護之道，若沒有適當地系統輔助工具，企業在面對資訊安全方面將會是一項繁雜且費時的工作[1]。

[1] 張偉斌，網路資訊安全諮詢服務系統之研究，國立臺北科技大學商業自動化與管理研究所，2001。

資訊雖然帶來人們的便利，卻也在另一方面帶來令人擔憂的資訊安全問題，因此我們必須做好資訊安全防護措施，唯有在確保資訊安全之前提下享受資訊便利，才是面對資訊世紀來臨的正確態度，進而迎接未來更大的挑戰與衝擊。

有鑑於此，我們在享受便利快捷的資訊服務的同時，亦應隨時提高警覺，防範電腦洩密及影響單位安全事件發生。

1.2 研究動機與目的

隨著資訊科技的普及應用，企業大量的使用資訊系統用來增進企業內部、企業與客戶、供應商之間的資訊流通，然而在網際網路這種開放式架構上容易造成資訊安全的漏洞，我們究竟該如何運用資訊安全政策來保護企業資訊的機密性、完整性及可用性等資訊安全？

資訊安全首重在事前的規劃工作，也就是政策的制定與風險管理，當企業持續透過電子化方式在與許多擁有不同資訊安全機制的廠商進行聯絡時，企業之間的商業模式漸趨於分散且虛擬化，企業資訊安全的界線也越來越模糊，這使得企業資訊可以在任何時間、地點進行存取，資訊安全風險也相對越來越高，所以企業必須建立一個整體資訊安全系統架構，以確保企業資訊安全[2]。

資訊安全的主要特色是政策(Policy)，也就是所謂企業的政策，這個政策是跟資訊安全相關的。資訊安全乃是利用各種政策或程式系統，透過命令或法規的執行，來確保未授權開放性的資料得到授權過後的控制或保護之結果，此保護是爲了避免一些未經允許的資訊被公開、操作、損毀與修改[3]。

資訊安全政策是一種整合，因爲資訊安全牽涉到的範圍相當廣泛，像是資料庫及網路。在企業裡資料庫的運用就非常繁多，網路則包含路由器、網路設備、軟體等應用。若要在使用上能控管資訊安全，則需要使用軟體來防範，包含軟體登入，須有帳號跟密碼、要自己設定使用者名稱及密碼，如此才有獨立的資訊安全控制。過去大部分的系統架構把重心集中

[2] 張詠翔，銘傳大學資訊管理學系碩士在職專班，結合 BS7799 與資訊安全藍圖建構－資訊安全評估機制之研究，2005。

[3] 蔡思達，國立台灣科技大學資訊管理系研究所，以適應性結構化理論探討資訊安全管理系統導入之徵用過程與成效，2007。

在技術上的建構而沒有處理程式和資料參與安全執行，他們的架構在安全政策和執行程式上少把重心集中並且疏忽了技術的落實細節。以往並沒有企業整合，包含執行資訊安全的政策及使用權限的分別，這裡面包含有許多的重要性議題，而資料安全執行正是組織最重要的一個議題，藉由資料安全執行的管理逐漸地成爲策略性的命令。因爲組織在減少操作風險與執行時間的同時，也企圖尋求提升投資者信心，故該如何更有效的確保企業資訊資料、系統、設備及網路通訊安全，有效降低因人爲疏失、蓄意或天然災害等導致之資訊資產遭竊、不當使用、洩漏、竄改或破壞等風險，並建立資訊安全管理方向[4]，是此研究的重點。

企業資訊安全如果不完善，導致客戶的重要資料外洩，可能會造成很嚴重的問題，如此一來會造成企業與客戶、合作廠商間的不愉快，甚至可能衍生官司問題；另外，財務資料的管理也是相當重要，當初的安隆案就是因爲該企業的高階主管，不當的修改企業的財務資料，讓投資人從表面上看起來以爲公司的財務狀況良好，誘使許多投資人加以投資，最後造成企業倒閉，影響層面相當廣泛。

擁有一個完善的資訊安全系統，不僅可以維護企業的資料，更可以形成一道強而有力的後循，做爲企業的一大競爭優勢。

所以基於上述的研究背景與動機中所提及之仍有缺失或不足需改善的地方，本研究系統就是用來改善這些缺失或不足的地方，主要有下列幾項：

一、保護中華電信網路資訊，避免未經授權的存取與修改。

二、建立資訊業務永續運作計畫，確保中華電信業務永續經營。

三、面對龐大的用戶數及業務量，能有效率的處理用戶的帳務資

[4] 考試院，資訊安全政策，http://www.exam.gov.tw/。

料。

本研究對象爲電信業者，是目前擁有 2,300 萬用戶，全球第十四大電信公司－中華電信，該公司爲在台灣電信服務業的領導廠商，亦是國內營運經驗最豐富、規模最大之綜合電信業者。所屬之資訊資產機密性、完整性及可用性，保障使用者資料隱私並符合相關法規之要求，使其免於遭受內、外部的蓄意或意外之威脅。處理客戶的帳務資料，一般傳統的做法是資料中心會應用大型磁帶館的架構來做備份，透過本研究希望能完成帳務整合系統，改善相關企業作業人工處理之效率，確保企業資訊資料、系統、設備及網路通訊安全，有效降低因人爲疏失、蓄意或天然災害等導致之資訊資產遭竊、不當使用、洩漏、竄改或破壞等風險，並建立資訊安全管理方向[4]。

本研究目的在於確保企業業務資訊及帳務系統之整合性、機密性、完整性與可用性。

整合性：簡化企業流程且有效率之整合用戶的帳務資料 。

機密性：確保已獲授權之人員才可使用資訊。

完整性：確保使用之資訊正確無誤、未遭竄改。

可用性：確保被授權之人員能取得所需資訊[4]。

1.3 研究流程

本研究流程如下圖 1.3.1 所示：

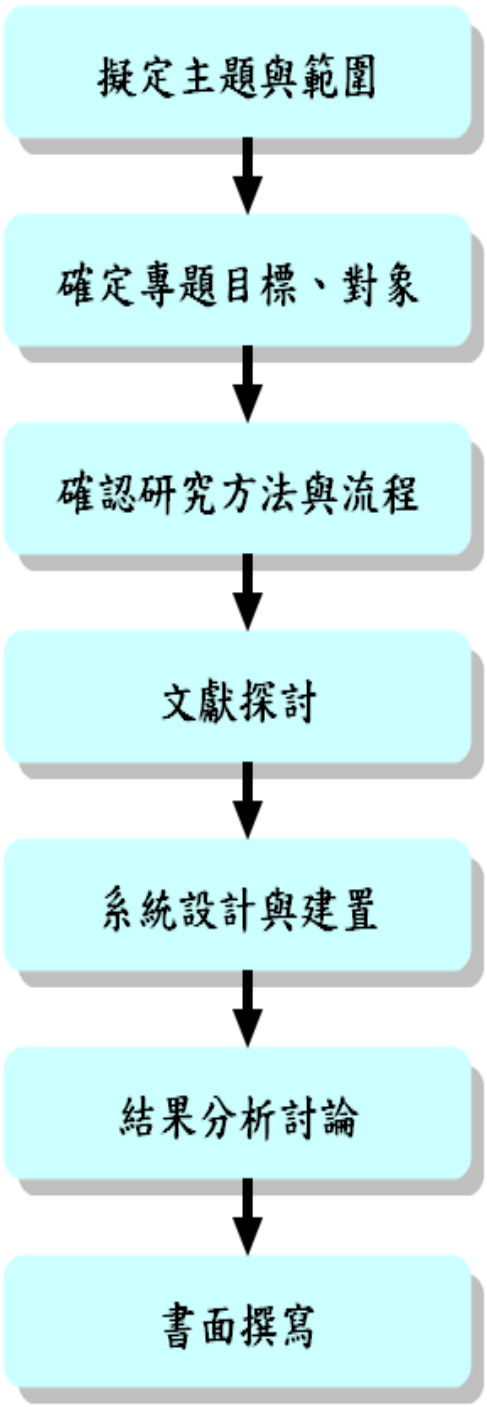


圖 1.3.1　研究流程圖

第二章　文獻探討

包括本研究所提及的各式各樣的安全管理框架，在過去已經有許多研究發現有不足的地方，這些已經被建議處理的問題討論如下說明，比較整理則如表 2.1 所示。

(1) Bradley 和 Josang 提議將其命名爲企業安全管理。支援其組織架構的主要有 3 個部分：資料容器、經理規劃和結構代理人。資料容器在中心儲存政策資料，與處理計畫、結構代理人合作執行政策。他們的重心集中在技術上的架構，而且非處理程式和參與資料安全執行。

(2) Sengupta 等人提出了一個統一企業資訊系統安全的資訊模型，並且開發一套網路服務安全管理架構。該架構集中於落實技術執行的詳細資料與細節，而略過了一些策略安全和執行程式。

(3) Coyle 等人提出一種多層次架構，包含定義、功能、結構和安全管理的構成要素。他們特別地指出資訊保護的重要性，而不是系統。雖然此架構使用的相當廣泛，但是在執行程式、支援架構、工作組成要素方面仍不見整體意見。

在比較過後，政策驅動安全執行(PDSE)在本文中提出的架構在幾個方面有所區分。

第一，提供多層意見，企業內不同專長的職員能夠全部瞭解工作、資訊、技術上的架構和來自不同觀點的安全執行程式。第二，與幾個其他研究人員不同，PDSE 架構指定有關任務和情報交流。 在 PDSE 架構裡，安全執行程式中的工作因爲情報交流互相連結形成一個完整的生命週期。 第三，連續的審計機制和監控被嵌入在 PDSE 裡。第四，變動管理被帶入其過程和技術架構中，作爲它的驅動因子，如此一來 政策將使安

全執行成爲一個連續的改進過程。第五，PDSE 基本上是架構的一個機制，它根據在組織中可能影響政策組織中的可審計規章的政策規章轉變問題，做出明確的處理。若沒有這樣的轉變，政策就不能被有效實施，符規的水準不能被有效地測量與追蹤。

表 2.1.1　其他架構之比較表

架構	Chen, Kuo	Bradley, Josang	Sengupta et al	Coyle et al
出版年份	2009	2004	2005	2007
流程驅動力	政策	無	無	無
流程或控制資訊	流程和控制資訊	只有流程	只有控制資訊	只有流程
實際應用案例	中華電信	無	有	無
變革管理	嵌入	無	嵌入	無
連續監控/稽核機制	嵌入	無	無	無
政策規則轉換機制	提供	無	無	無

第三章　系統建構與設計

3.1　系統特色

近年來企業資訊安全問題屢見不鮮，也因此企業針對資訊安全問題也日漸重視，然而企業所希望的政策卻難以與系統連結。資訊安全可能發生在很多地方，如應用、資料庫，甚至是流程都有可能是資訊安全漏洞產生的區塊。

有別於傳統以個別資訊爲單位的作法，在與中華電信合作的系統中，採取將所有東西整合成爲一個更爲完善的系統。該系統可直接檢視企業有哪些地方產生了可疑的問題、資訊安全是否產生漏洞、有無人員違反資訊安全規則。

美國零售業者 TJX 在 2007 年所創下的 4570 萬筆客戶資料外洩紀錄。但驚人的數據有可能被突破！每月處理逾 1 億筆的交易、爲美國飯店、酒店及零售業提供信用卡、借貸卡、薪水支付及相關付款處理服務的 Heartland Payment Systems 於 1/20 宣布，旗下付款處理系統被植入惡意程式。以 Heartland 在全美擁有 25 萬家客戶及每月超過 1 億筆的交易次數來看，可能創下有史以來最大宗的客戶資料外洩事件。據悉駭客是在去年底連續數星期入侵該公司的電腦系統，直到一月中才發現遭入侵。台灣發生的「史上最大」個資外洩案例，是發生在去年底由刑事局破獲的 5000 萬筆個人資料外洩事件。外洩的原因之一是委外廠商將客戶資料外洩，更嚴重的單位甚至還有被廠商，用硬碟直接 Copy 資料帶走的！資料外洩防護產品所需要的成本還抵不上一次成本高昂的侵權事件，而且個資外洩也損害了公司信譽與競爭力。企業策略集團(Enterprise Strategy Group) 調查報

告指出，三分之一的組織在近 12 個月內曾發生資料外洩，且有 30% 的調查對象表示他們組織的資料外洩導致了直接的收益損失。英國史上最嚴重資料外洩－官員寄丟光碟，導致 2500 萬筆資料遺失，分析公司 Gartner 預計，該事件引發的帳戶關閉及重建，以防止可能的詐騙行爲，大約需要花費 5 億美元。一家位於瑞典的音樂下載網站資料遭竊，兩個多月後收到駭客通知信才知道系統遭到入侵，一百萬以上的註冊使用者資料因而外洩。由以上案例可以看出，個資外洩所產生的問題，與對企業在營運上的威脅。

根據美國資料竊盜資源中心(The Identity Theft Resource Center，ITRC)指出 2008 年資料外洩案件總計有 656 件，比 2007 增加了 47%；而且企業資料外洩有愈來愈嚴重的傾向，自 2006 年佔 21%增加到去年的 36.6%。ITRC 所列出的身份資料外洩管道包含筆電或電腦等儲存裝置的遺失、備份磁帶的遺失、駭客入侵、內部員工偷竊或受到木馬、病毒程式的入侵等。

一般企業、健康醫療產業及金融產業的資料外洩比例皆呈現成長趨勢。資料外洩的途徑以人爲疏忽居冠，佔 35.2%，其他依序是旅行中資料遺失的 20.7%、內部竊賊的 15.7%、意外揭露的 14.4%，駭客入侵則以 13.9%位居第五。企業遭竊取的研發資料、會員資料，很快就會在駭客圈流傳。2006 年底台灣某高科技公司遭入侵竊取資料後，經過刑事局鑑識比對後發現，光是內部研發資料外洩起碼損失 2,000 萬元以上，甚至可能導致企業難以繼續維運。

去年開始各種個人資料外洩事件頻傳，各界也紛紛期盼新版個資法「電腦處理個人資料保護法」可盡速通過，預估近期內就可通過。一待新法實施，企業也必須對使用者個人資料付出更多責任，一旦新版個資法通過後個資損害賠償上限爲五千萬元。若實際損害金額超過五千萬，以實際

受害金額爲主。違法取得並利用個資圖利者，處 20 萬到 100 萬罰款，並從告訴乃論罪轉爲公訴罪。個人資料防護就像是保險的觀念。若沒有事前防範得宜，若因資料外洩而上頭條，可就得不償失了[5]。

本研究系統的特色爲整合，係將原本分散於各處的資訊，集中在一個資料庫中，以方便檢視，並結合企業政策。企業的政策在制定時，通常會以高階政策爲主，在實際執行中則是以許多的規則加以規範，對應至資訊系統後則爲規則，規則在系統中就像是一道又一道的關卡，在進入系統前必須通過嚴格的檢視，如：誰能在什麼時候用、誰能夠用什麼、誰能看什麼資料、哪些資料是只有特定人員才可瀏覽…等。

然而，企業在制定政策時並不會如此詳細的載明，只是制定出執行大綱，如高階政策必須經過主管的簽核之類的。因此，政策與資訊系統兩者之間，在實際執行時產生了間隙，即政策無法對應至系統的規則，原因在於政策與規則是不一樣的，通常政策是屬於非常高階的，因此造成高階的政策無法對應至較低階的系統規則。當企業的高階主管訂定出政策時，必須交由資訊人員將其政策轉換成系統規則，但資訊人員往往不瞭解該項政策是根據何種要素與原因而制定，甚至可能連帶造成資訊人員對於系統規則違反哪些政策都不瞭解。

再者，企業在制定政策時又必須與外部因素配合，如政府法規、國際法案等。外部因素對企業在制定政策時將造成影響，而政策受到影響後也將連帶影響資訊人員設定系統規則方與系統實際執行情形。多數的企業資料外洩，遭攻擊者通常是無法補救後才知道，如果能有一套統一且簡單明瞭的系統供企業作爲資訊安全維護的後盾，如此一來將可使企業建立更加完善的資安防護網以減少企業、顧客的損失！

[5] 趨勢科技 http://www.trendmicro.com.tw/micro/TMLP/TMLP_microsite_index.html

3.2 使用對象

隨著資訊科技、個人電腦的普及以及網際網路的蓬勃發展，資訊資產早已成爲企業在獲取競爭優勢上最重要的因素，也就是說資訊是有價值的，是一種資源也是一種資產。在現今的社會中，每天都有數以百萬計的人，透過網際網路以搜尋各類所需資訊，企業組織把本身營運相關的資訊、系統，視爲是自己核心的資產，愈是倚賴資訊、系統，愈覺得「資訊安全」很重要。

相對的，許多企業利用網際網路來進行資料交易及聯繫，以傳遞內外資訊與溝通聯繫，卻也造成資訊安全事件層出不窮。雖然網際網路成功的扮演了增加資訊、降低成本的橋樑。同時也產生弊端，遭有心人士利用非法入侵的方式進入企業內部竊取、讀取、更改、破壞電腦重要資料，或企業內部離職人員蓄意破壞，不當取得資料等違反安全的事件。再者，企業組織在制定資訊安全政策時，也可能因考慮不周或疏忽而導致資訊安全政策出現了弱點，使得內部使用者或外部的入侵者利用這些弱點進行攻擊、滲透、資訊竊取等行爲，或因爲措施上的弱點而導致危害企業組織資訊安全事件的發生，這些往往造成企業巨大的損失[6]。

因此，更看的出來資訊安全是企業不可或缺的一部分，至於要由誰來推動資訊安全呢？我們將使用對象鎖定爲企業資訊安全主管。讓企業資訊安全主管，透過資訊安全的推動與執行，可以從整體性的安全對策著手，思考如何達到保護企業內之資訊的「機密性」：防止未經授權的人取得訊息，以免資料外漏；「完整性」：確保傳送者的訊息跟接收者的訊息是一樣的；「可用性」：確保合法使用人可以順利使用系統資源，而達到安全控管稽核、有效降低資訊安全事件發生的頻率及衝擊，提升企業的競爭力，達

[6] 張詠翔，銘傳大學資訊管理學系碩士在職專班，結合 BS7799 與資訊安全藍圖建構資訊安全評估機制之研究，2005。

成維持企業活動運作之目標[7]。

[7] 方仁威，國立交通大學資訊管理研究所，資訊安全管理系統驗證作業之研究，2004。

3.3 使用環境

中華電信股份有限公司成立於 1996 年 7 月 1 日，由當時的臺灣交通部電信總局營運部門改制而成，成立時資本額爲新臺幣 964.77 億元。主要業務涵蓋固網通信、行動通信以及資料通信三大領域，提供語音服務、專線電路、網際網路、寬頻上網、智慧型網路、虛擬網路、電子商務、企業整合服務以及各類加值服務，是臺灣營運經驗最豐富、規模最大的綜合電信公司，也是國際電信合作重要的夥伴。在促進全球化即時訊息溝通、全面提高社會大眾生活品質以及增進經濟社會運作效率等方面成就卓著。在自由競爭的市場上，消費者選擇電信業者時，除了申裝成本、費率、通訊可靠度等方面的基本的考量之外，業者是否能夠提供符合客戶需求的客戶服務，是一項十分重要的因素。而對大多數的消費者而言，客戶服務中最重要的一環正是帳務服務。由於在電信業界，不同的公司所使用的技術、通訊設施、以及所能提供的業務種類等方面通常並沒有太大的差別，帳務系統及其相關的客戶服務反而成爲最關鍵的差異化因素，在客戶選擇電信業者的決策上扮演不可或缺的重要角色。

再者，從作業面、經營管理面及策略面等各種角度來看，帳務系統更是電信企業營運上最關鍵的後盾。因此建置符合企業需求的帳務系統，並配合提供符合顧客需求的客戶服務，便成了大型電信公司創造競爭優勢的一項重要課題。

本研究採用新一代營運系統及軟體(New Generation Operations Systems and Software, NGOSS)的應用軟體開發方法論，如圖 3.3.1 NGOSS 發展生命周期所示，從商業流程分析與設計(Business Process Analysis and Design)可以看到商業觀點，從系統分析與設計(System Analysis and Design)可以看到系統觀點，從解決方案設計與整合(Solution

Design and Integration)可以看到建置觀點，從測試與開發(Testing and Development)可以看到佈署觀點，從此流程可以看出不同層次的觀點。隨著國內電信業開放民營化後，競爭已日益激烈，中華電信也陸續推出了許多新業務與新服務，如 ADSL、寬頻到家、MOD 等業務與服務；此外，還對企業客戶及合作夥伴推出了許多客戶優惠及業內合作方案，這些新興的電信加值業務使得中華電信的帳務系統面對更新與更高的需求。

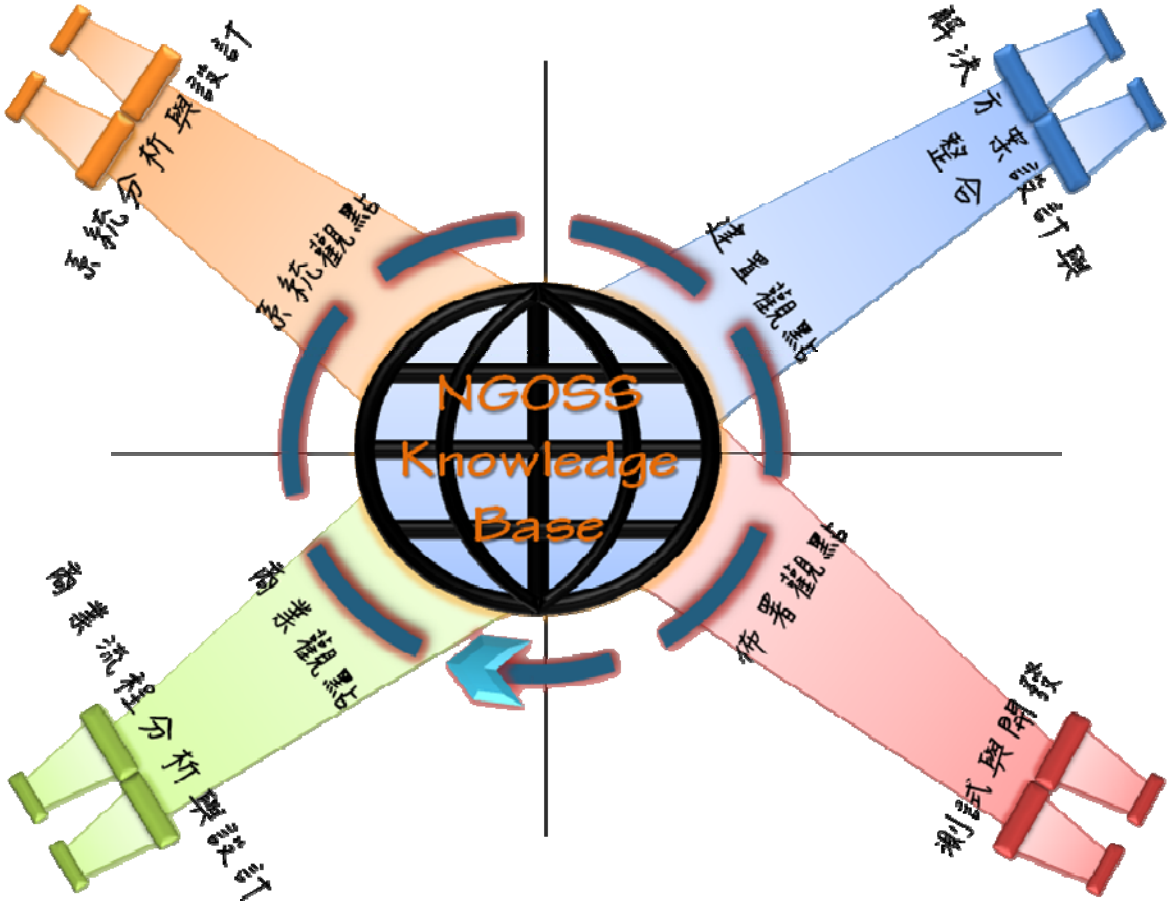


圖 3.3.1　NGOSS 發展生命周期

中華電信目前擁有 2,300 萬用戶，爲全球第十四大電信公司，帳務系統採用 IBM 的大型主機，負責處理用戶的帳務資料，包括每月客戶電話費的批價、出帳、合併帳單、帳單遞送，查詢，繳費後的銷帳、催收，停話、復話，拆機、退費、訴追以及呆帳管理等，帳務系統涵蓋了約 1,400

台伺服器。一年處理的出帳金額約 1,800 億元。龐大的用戶數及業務量使得中華電信的帳務系統成爲臺灣電信行業最大的帳務系統，它對於支撐中華電信組織和管理業務的正常營運有著相當重要的地位，所以經由此系統將可以使業務流程縮減，中華電信的帳務主管極需優良的軟體工具以提升大型主機上的軟體開發與維護效率，以提供客戶更卓越的服務品質。

第四章　系統結果

4.1　系統架構

企業資訊安全政策施行系統主要爲一系列擁有一致性且能重複地改進管理的程式。安全執行架構裡的四大功能是一個不斷重複的過程，也是一個可以持續改進的一個系統。本研究系統特色爲整合，把原本分散在各處的資料藉由入口網站把資訊集中在一個地方，再經由子系統的監控，將每個事件與資訊安全政策管理子系統政策規則資料庫結合。經由事件資料庫與高階主管所發布的政策作稽核與比對，辨識是否符合規則。如需修改更完善的規則，此系統將會產生問題經由問題資料庫作更正或補救，再經由評估及修訂以持續政策的改善，而後將再回到第一階段，如此週而復始，形成一個循環。反之，若無需修正則回到原流程繼續循環。本系統架構圖如圖 4.1.1，PDSE 架構圖之流程圖如圖 4.1.2。

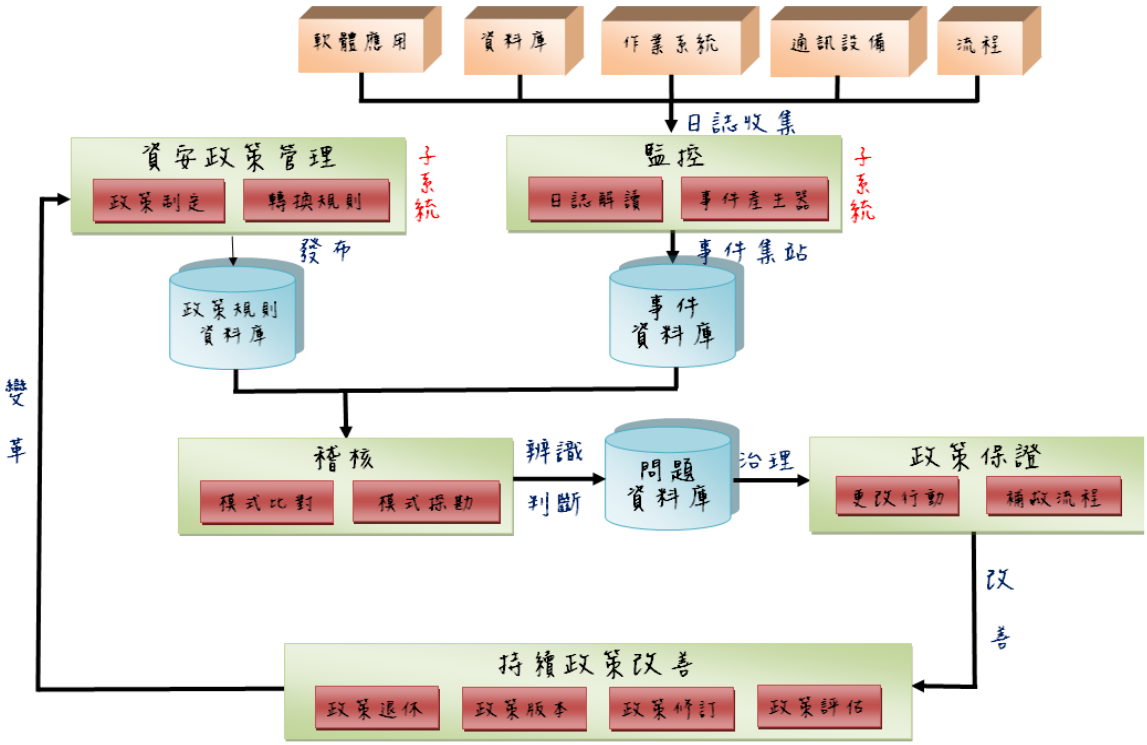


圖 4.1.1　資訊安全系統架構圖

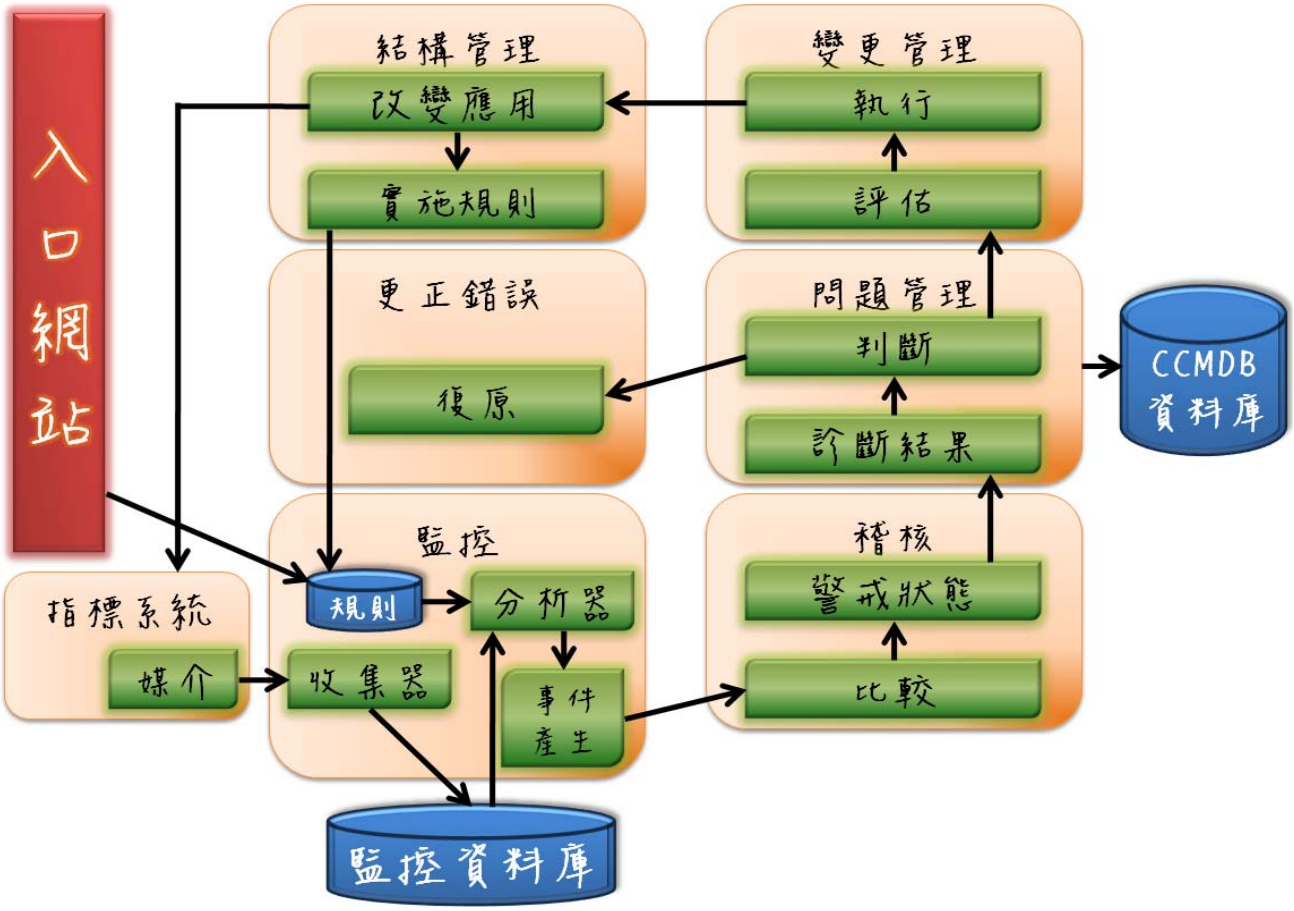


圖 4.1.2　PDSE 架構流程圖

4.2 系統建構方法與流程

爲了幫助電信公司有效率地處理安全執行管理，將所有的資訊安全執行整合在一起，故此架構分爲四個程式，作爲未來整體資訊系統管理過程的導引，此四階段爲規則－監視－稽核－補救（或稱爲 SMAC），持續循環改進程式，形成爲 SMAC 方法論，如下圖 4.2.1（SMAC 流程圖）所示。

圖 4.2.1 SMAC 方法論－PDSE 框架的第一層

簡言之，此系統是一系列能一致且重複改進管理的程式。安全執行架構裡的四大功能是一個不斷重複的過程，也是一個可以持續改進的一個系統，又稱爲安全執行架構之生命週期。當管理者訂了政策，就必須也訂定規則來執行監控，系統會稽核企業各活動的進行與規則是否一致、是否能夠達成目標。若稽核出來結果不符合，就必須找出其差異之處並立即提出修正或補救方案。即使一切符合規則，無需修正，仍須回到第一階段，

如此週而復始，形成一個循環。

一個組織根據先前已決定的預期來操作發展事物被稱爲符規。通常預期已決定的事物大多來自於闡述政策規則或需求，或是擷取外部的規章，例如沙氏法案(Sarbanes-Oxley)和HIPAA或來自企業條文中的商業指導方針。爲了達成其要求條件並維持其狀態，首先企業應在基於外部或內部規章的需要去規定政策並說清楚可或不可。然後企業必須建立一個機制來監督與稽核政策以實行評估或確認遵從狀態。任何非符規的事物應該在監控期間被發現，企業必須矯正或更正錯誤去遵守政策規定。最後，如果對現今的政策認爲是必要的，有任何需要改變，那麼企業必須重新執行一開始規定的步驟。

SMAC 方法論盡可能有系統地將流程縮短至只剩八件工作（政策規則，政策轉換、規則執行、管理監控，符規分析，補救錯誤，控制評估和政策更新），爲了使要求條件的管理程式變得容易，會將這八件工作連接在一起作爲促進安全的執行程式。以程式的觀點來看，描述特定的工作參與安全執行程式，並且以小組爲單位或者以方法歸類，即稱爲系統管理整合，和安全執行程式可以作爲一套被探討的構成要素或工具，如圖 4.2.2 所示。

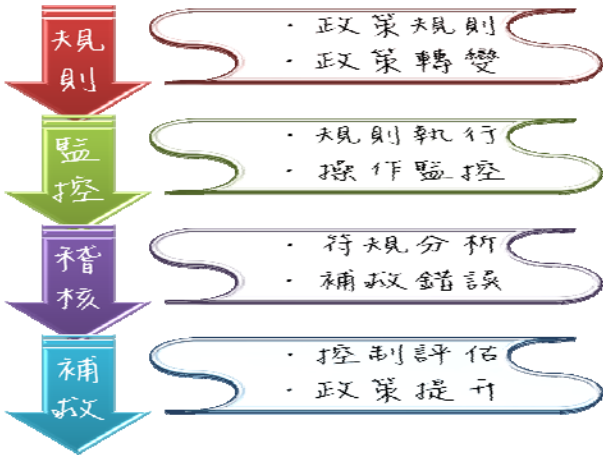


圖 4.2.2　資訊安全控管流程－PDSE 框架的第二層

爲了要達成政策而且維持符合狀態，企業首先需要訂定規則，清楚地說出是基於何種政策或優先考量的外部或內在條例的不能違反的規則。然後，企業一定要建立一個機制來監控政策和稽核所實行的事件。在監視期間若發現任何不符合的事件，企業一定要加以改善或者採取變更行動，制訂出符合該規定的政策。最後，如果目前的政策不適合，那就要變更政策，產生新的政策。如此一來，企業一定要再從第一個環節－規定這個步驟開始重複循環。

在SMAC 方法論中所是出的第一件工作－規定，是指依照政策規定外部與內在的條例。舉例來說，西元 2001 年美國爆發金融史上重大醜聞「安隆案」，一夕之間使這間美國第二大企業瓦解，並波及美國第一大會計事務所－安得森事務所也連帶瓦解。因茲事體大，故美國國會自西元 2002 年頒布沙氏法案，對會計審計界造成莫大影響[8]。

沙氏法案(Sarbanes-Oxley)的執行需要公司提供範本，公司必須提供財務申請的證據來證明或支持系統和服務能夠確認財務報告是安全的，如此政策的規定可以從一些事情來說明對於關鍵的財務報告數據必須被稽核的。然後，企業需要設法解釋某種不知轉變的原因，通常是無確實根據的、無系統性的政策，對應到之後的監控稽核是可實施和稽核規則。換句話說，這是一個政策轉變的工作或以團隊技術的角度來設計規則或控制。如此設計一個規則可能需要任何不是屬於財務應用的用戶組織的使用者，去執行稽核任何在財務資料庫內反對財務報告表的操作行爲。在這個例子中，是根據那些規則去強調在技術裡的物件項目。這項工作基本上是把企業的預期轉變成可推行的要求，且若不能正確執行這工作將使企業很難評估要求條件的狀態，因爲在描述兩者之間的控制實現和政策規定、規章可能會是不全或者錯誤的。

[8] 美國現行審計雙軌制　http://my.so-net.net.tw/joe21799/l/l3.htm

事件在政策轉變之後是規則執行，是指實際上執行先前被設計的規則，被執行的規則可以被分成兩種類型。 第一個是預防，而另一個是偵測。在先前的例子中，預防的措施可以藉由存取控制被瞭解，在預防措施中屬於被授權的用戶將不被允許連接資料庫的通路或者對資料庫連接的應用。另一方面，偵測的控制能藉由登錄對應到資料的應用資料庫或探訪資料的應用存取去執行。在現今可用的技術上，無論是基於可提供的技術或物理上應合乎邏輯等原因，對資料庫的存取、應用、程式、伺服器和設備都能全部被記錄而沒有任何問題。在規則或者控制已經被執行之後，企業必須管理操作監控，盡可能利用連續模式來監控每日營運的工作。當一名人員在準備先前的工作步驟時，企業應該藉由詳查的記錄來收集所產生的事件，掃描先前的工作措施所產生的事件，事件產生應該包含有一個統一的格式記錄先前誰要做什麼的資訊（資料、應用、程式、伺服器和裝置），和從哪裡來。

藉由事件收集，企業必須執行順從分析，確定事件是順從的還是非順從的，每當不符合的事件發生，企業一定要先做補救或矯正行動，因此企業中的高階政策是在建立一個合適地管理結構與機制。我們可以明顯地的看出每當企業反覆循環改進週期，以期改善安全執行程式的時候，在過程中採用新政策取代原政策，使企業政策變的更穩定發展，將使企業政策能提高價值，如圖 4.2.3（資訊安全流程圖－安全防護執行工作與控制訊息之間的關係）所示。

就長期考量方面而言，企業必須實行評估控制工作以判斷在適當的有效控制下，是否需要更嚴謹的預防措施或需要偵測控制。這樣的特性問題通常會要求管理部門需特別著重於重新探討當前的政策。最後一個工作－政策更新，在這個工作項目中，企業必須建立一個變革和結構管理辦法，使任何適當的政策調整變得更協調。

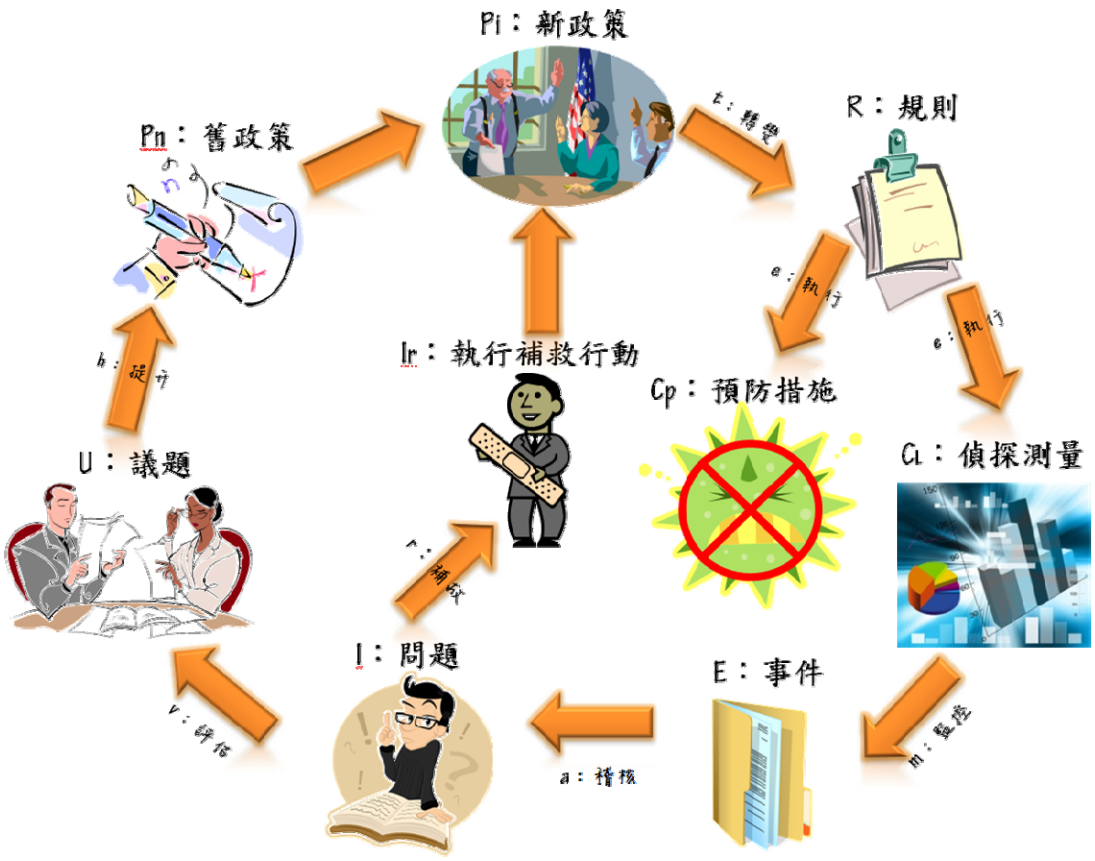


圖 4.2.3　PDSE 框架的第二層與第三層

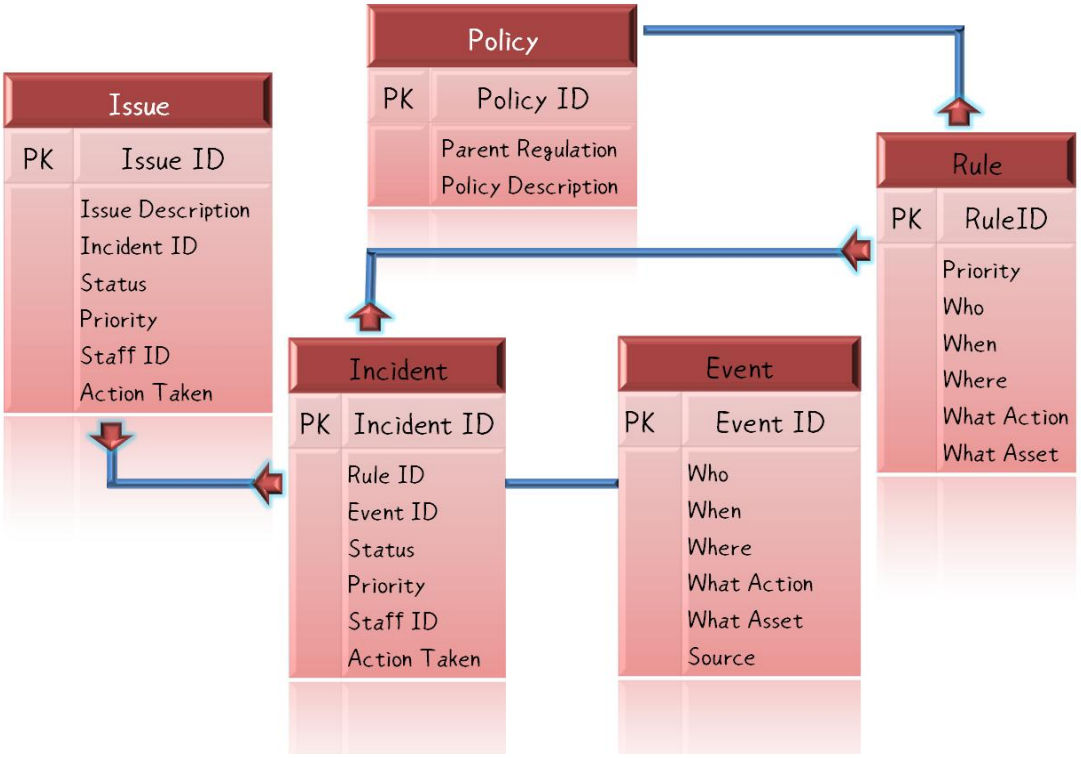


圖 4.2.4　PDSE 框架的第三層

最後，PDSE 架構的技術建構是由一套協調部分所組成，如圖 4.2.5（PDSE 框架的最終層級－技術結構）中所示，這種架構有助於自動化處理和在第二、三層級裡所指定的情報交流。它主要的功能是將內定中無特定結構政策結構化轉換成可執行、可稽查的規則，以取得相關安全紀錄資料，並轉換成符合的格式，儲存於資源庫中。並且執行多種的監控、分析、提醒調查或討論分析目的的任務，以促進持續安全執行進步的自動化，增加效率和連續過程的改進是該結構之主要特性。自動化監控則用於嵌入在機制和收支檢查中當作整合原始單獨儲倉審計機制訊息安全之管理元件。該元件相關的技術結構包含：四個原始（基礎）管理伺服器、一組紀錄集合物件軟體的代理程式、三個中央資源庫和控制台。

在以伺服器爲主的協同管理下執行下列八個任務：規定(S)、轉換(T)、執行(E)、監視(M)、稽查(A)、補救(R)、評估(V)與改進(H)，在此架構的第二個層級的觀點中已概略說明程序的每個步驟所匯集的安全控制訊息明細。

管理伺服器把相關的訊息傳送到客戶端的控制台，訊息安全專家以政策爲基礎配置可實施的規章的有關訊息、監視事件、事件調查的進行、補救或矯正行動、管理變更和整體安全配置。

日誌彙集軟體代理程式在不同的企業資產上，意圖要保護網路裝置、資料庫伺服器、收集安全設定或配置的應用程式伺服器、存取和改變紀錄，和其他的相關安全訊息。而之後收集到的訊息將會傳遞到更進一步分析的一個中央紀錄集合資料庫。資料收集後將會被傳遞至更進一步分析的中央日誌集合儲存處。

日誌彙集資料庫儲存事件資訊並與其他兩個資料庫共存，這兩個資料庫的其中一個被用於儲存調整(L)、政策(P)和規則(R)，另一個則是用來儲

存事件(I)和議題(U)資訊的資料庫。

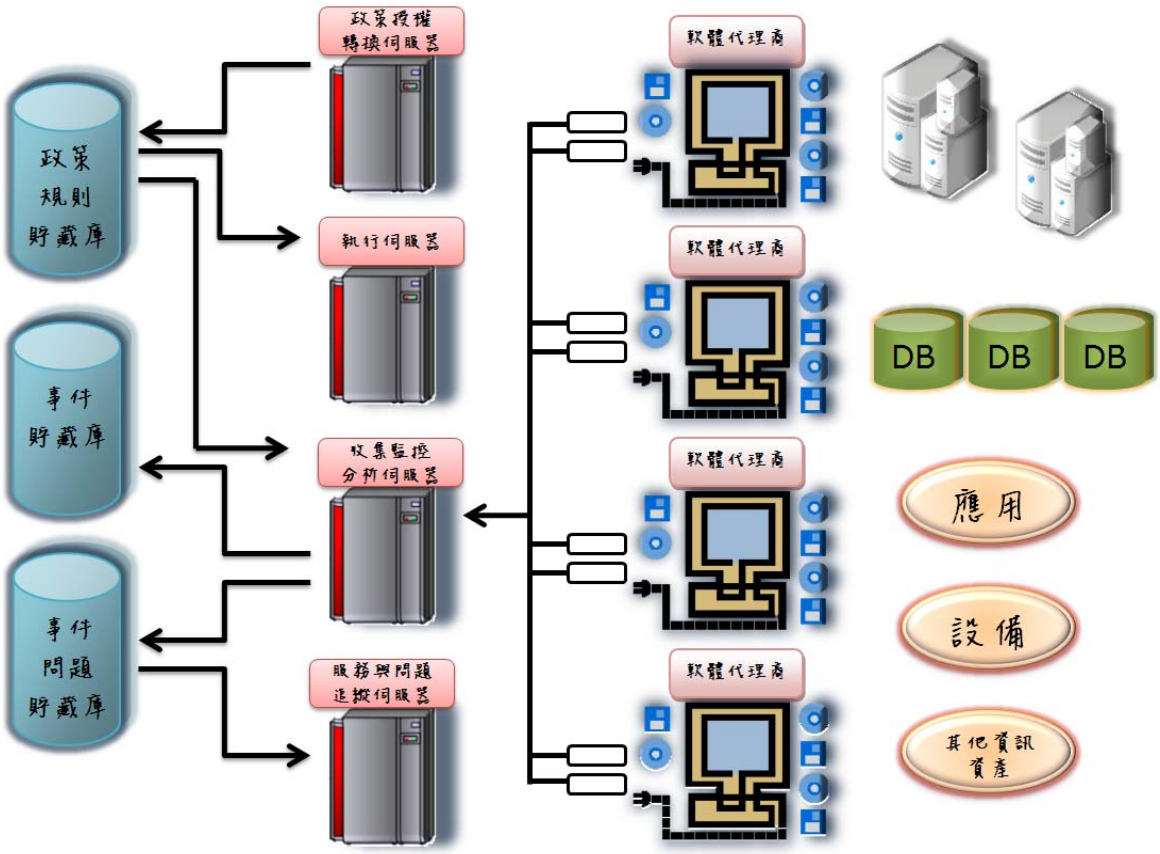


圖 4.2.5　PDSE 架構圖之最終層級－技術結構

4.3 開發工具

表 4.3.1　開發工具、功能伺服器及資料庫系統表

開發工具	Websphere Business Modeler Advanced 6.0.2 Websphere Integration Developer 6.0.2 Rational Software Architect 6.1 Rational TestManager 6
功能伺服器	Websphere Portal Server 5.1 Websphere Process Server 6.0.2 Websphere Message Queue 6 Websphere Application Server 6.0.2
資料庫系統	Oracle 11g

本研究開發工具如表 4.3.1 可以看出開發工具爲 Websphere Business Modeler Advanced 6.0.2、Websphere Integration Developer 6.0.2、Rational Software Architect 6.1、Rational TestManager 6。

其中 Websphere Business Modeler Advanced 6.0.2 提供了企業進行分析的工具，以便實現企業決策的功能和可用性。它提供程式模型、模擬和分析功能，幫助企業使用者瞭解決策並持續進步。企業的內部決策是允許企業使用者設計、仿製，而且讓使用者在處理企業內部重要的決策之前，先經由我們的所開發的工具，以先進的模擬、分析能力爲基礎和實際資料作出明智的決定，提供整合的內容幫助企業使用者解決方案，以加快決策的流暢度。Websphere Integration Developer 6.0.2 可幫助企業設計架構，將消息對應到由不同目的地傳送至需要處理的事件（消息）、調整和記錄內容。

而配合本研究所使用的功能伺服器爲 Websphere Portal Server 5.1、Websphere Process Server 6.0.2、Websphere Message Queue 6、Websphere Application Server 6.0.2。其中 Websphere Portal Server 5.1，它透過網路把電子商務應用的程式傳送到各個客戶端。主要提供了多種類型的訊息和應用程式，不管這些訊息停留在哪裡，也不管它們是什麼格式，最終都會以最適合的方式聚集所有的訊息。Websphere Portal Server 5.1 爲解決企業方案並方便使用者完成他們所需的每一個工作，它允許使用者與企業、人員、可用內容及流程的交流，管理他們的文件、共用的檔案。Websphere Process Server 6.0.2 用於對企業流程進行轉換，對決策和服務進行整合，這種具有整合服務、流程自動化服務使用的基本技術，包含人員、工作流程、應用程式、系統、平臺等來整合企業的流程。

另外，本研究的資料庫系統是使用美商甲骨文公司的 Oracle 11g 資料庫，可以幫助企業管理、企業資訊並迅速自動地做出調整以適應不斷變化的競爭環境。使用 Oracle 11g 資料庫，客戶可以在安全、高可用度和可擴展的需求下，由低成本伺服器和儲存設備組成的網路上，滿足最嚴謹的交易處理、資料倉儲和內容管理應用。

4.4 系統畫面

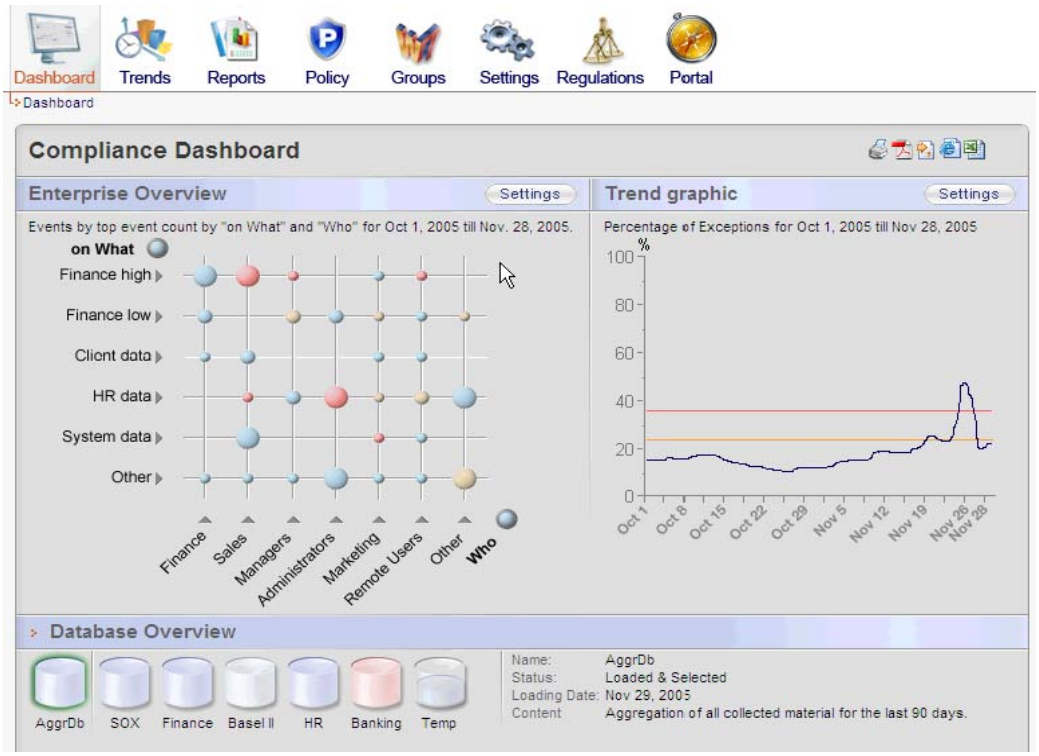


圖 4.4.1 符規儀表板(一)

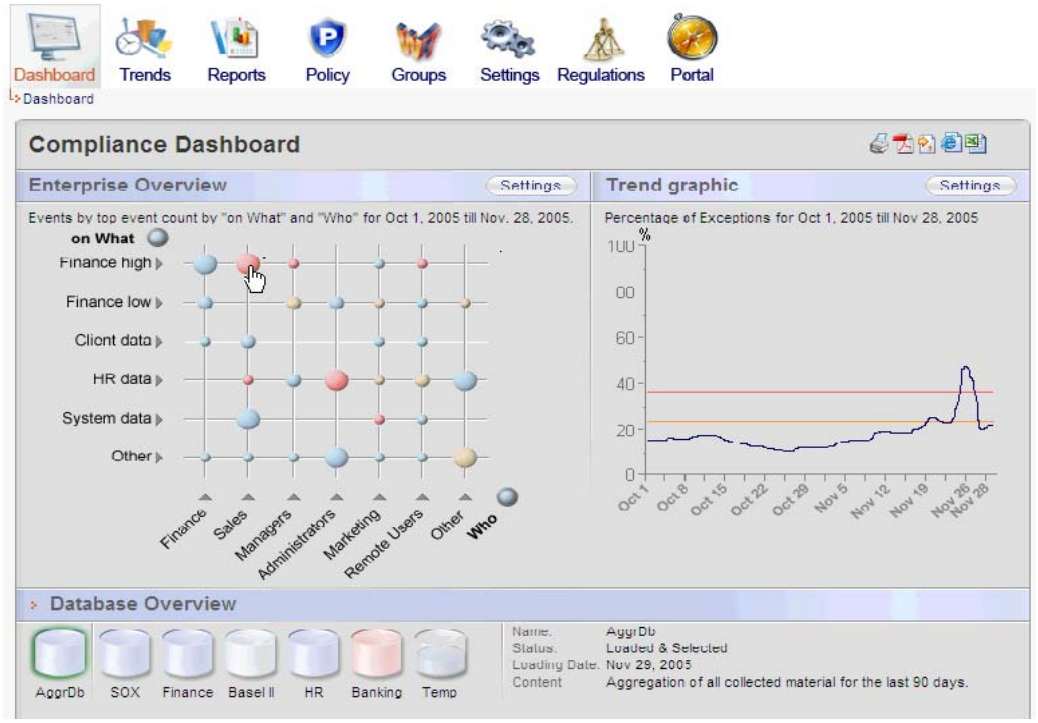


圖 4.4.2 符規儀表板(二)

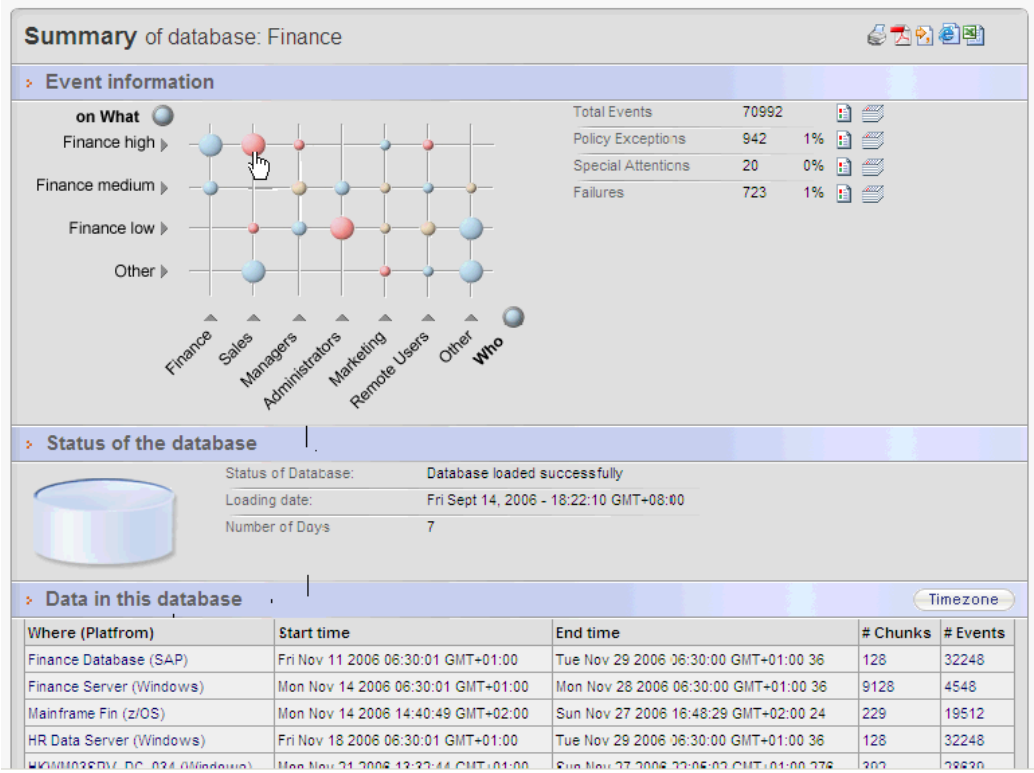


圖 4.4.3　資料庫監控結果之摘要內容

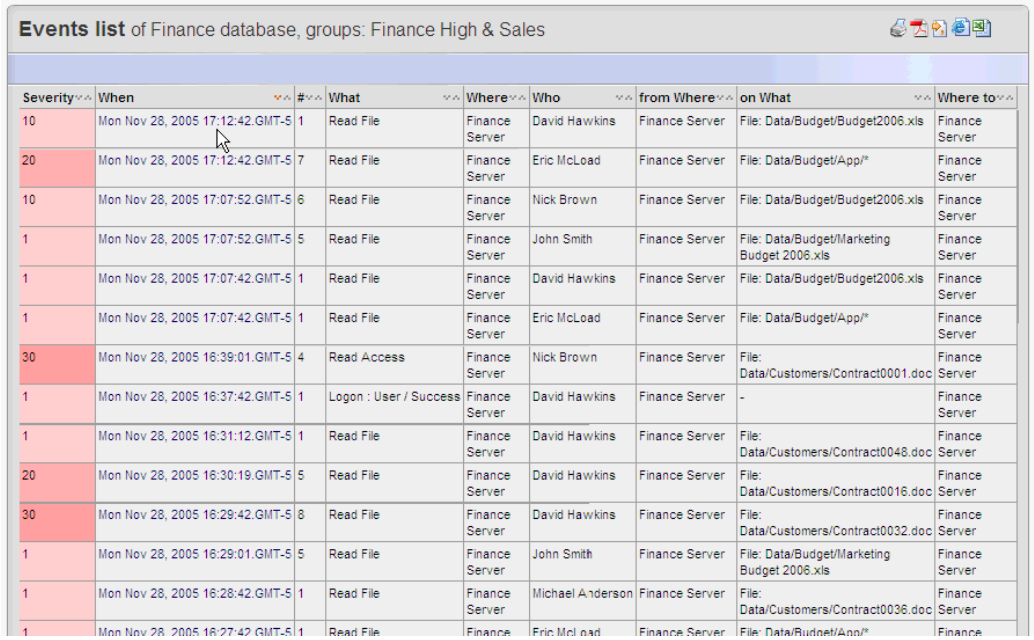
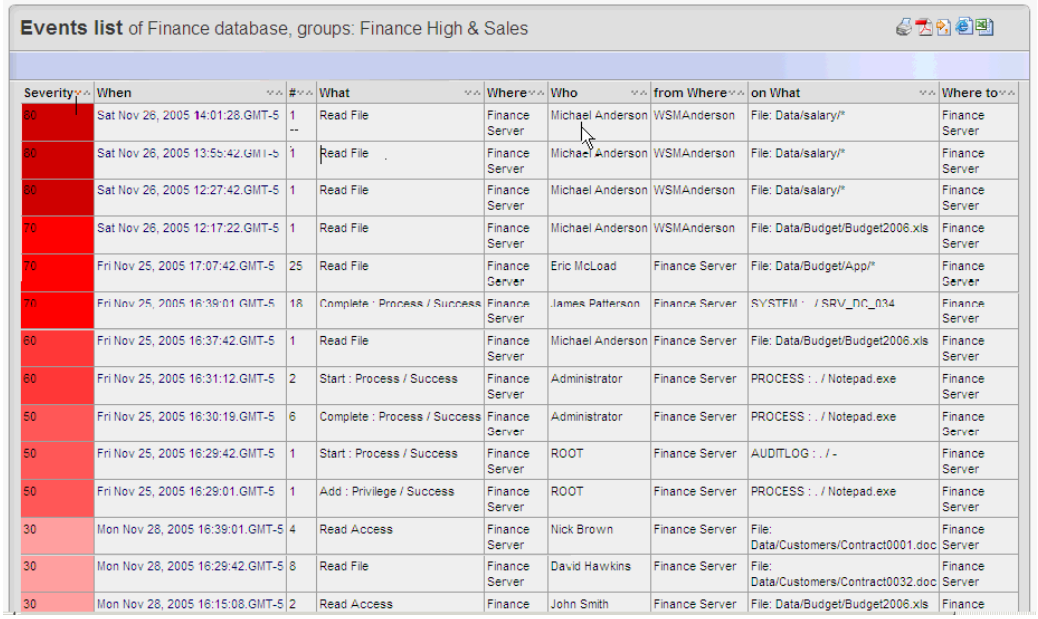


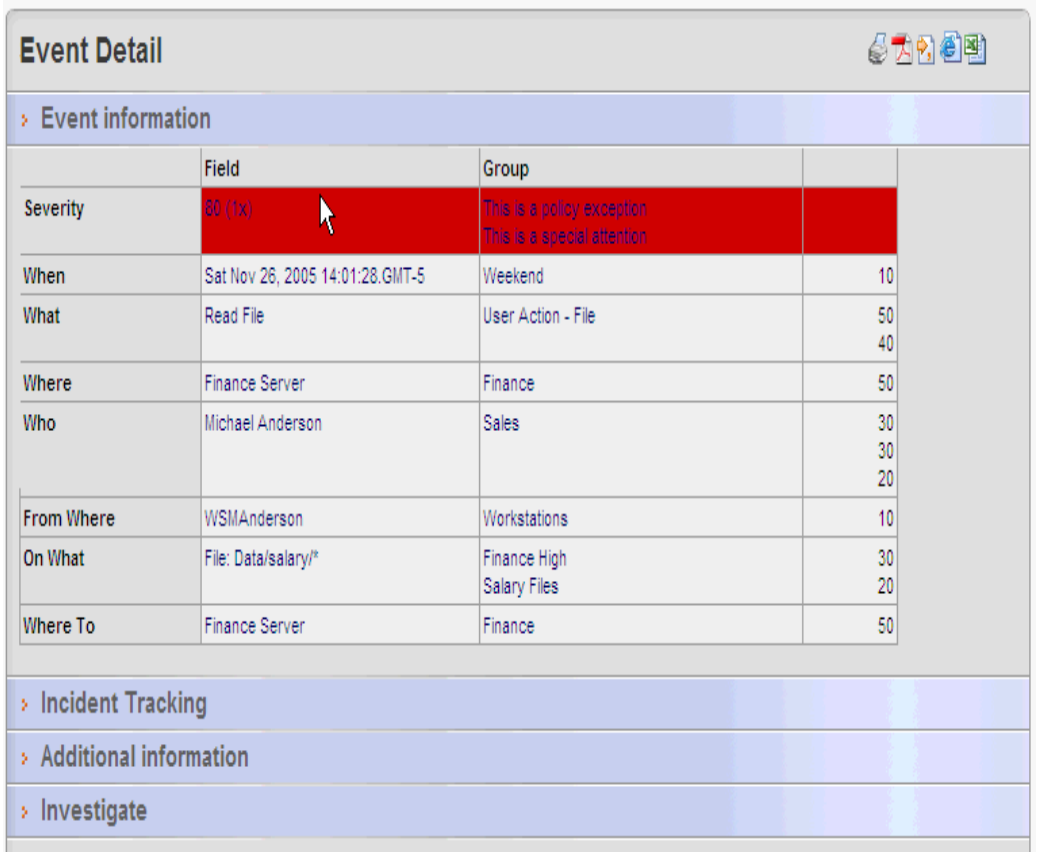
圖 4.4.4　事件清單畫面



Events list of Finance database, groups: Finance High & Sales

Severity	When	#	What	Where	Who	from Where	on What	Where to
80	Sat Nov 26, 2005 14:01:28.GMT-5	1	Read File	Finance Server	Michael Anderson	WSMAnderson	File: Data/salary/*	Finance Server
80	Sat Nov 26, 2005 13:55:42.GMT-5	1	Read File	Finance Server	Michael Anderson	WSMAnderson	File: Data/salary/*	Finance Server
80	Sat Nov 26, 2005 12:27:42.GMT-5	1	Read File	Finance Server	Michael Anderson	WSMAnderson	File: Data/salary/*	Finance Server
70	Sat Nov 26, 2005 12:17:22.GMT-5	1	Read File	Finance Server	Michael Anderson	WSMAnderson	File: Data/Budget/Budget2006.xls	Finance Server
70	Fri Nov 25, 2005 17:07:42.GMT-5	25	Read File	Finance Server	Eric McLoad	Finance Server	File: Data/Budget/App/*	Finance Server
70	Fri Nov 25, 2005 16:39:01.GMT-5	18	Complete : Process / Success	Finance Server	James Patterson	Finance Server	SYSTEM : / SRV_DC_034	Finance Server
60	Fri Nov 25, 2005 16:37:42.GMT-5	1	Read File	Finance Server	Michael Anderson	Finance Server	File: Data/Budget/Budget2006.xls	Finance Server
60	Fri Nov 25, 2005 16:31:12.GMT-5	2	Start : Process / Success	Finance Server	Administrator	Finance Server	PROCESS : . / Notepad.exe	Finance Server
50	Fri Nov 25, 2005 16:30:19.GMT-5	6	Complete : Process / Success	Finance Server	Administrator	Finance Server	PROCESS : . / Notepad.exe	Finance Server
50	Fri Nov 25, 2005 16:29:42.GMT-5	1	Start : Process / Success	Finance Server	ROOT	Finance Server	AUDITLOG : . / -	Finance Server
50	Fri Nov 25, 2005 16:29:01.GMT-5	1	Add : Privilege / Success	Finance Server	ROOT	Finance Server	PROCESS : . / Notepad.exe	Finance Server
30	Mon Nov 28, 2005 16:39:01.GMT-5	4	Read Access	Finance Server	Nick Brown	Finance Server	File: Data/Customers/Contract0001.doc	Finance Server
30	Mon Nov 28, 2005 16:29:42.GMT-5	8	Read File	Finance Server	David Hawkins	Finance Server	File: Data/Customers/Contract0032.doc	Finance Server
30	Mon Nov 28, 2005 16:15:08.GMT-5	2	Read Access	Finance	John Smith	Finance Server	File: Data/Budget/Budget2006.xls	Finance

圖 4.4.5　依嚴重程度排序後之事件清單



Event Detail

Event information

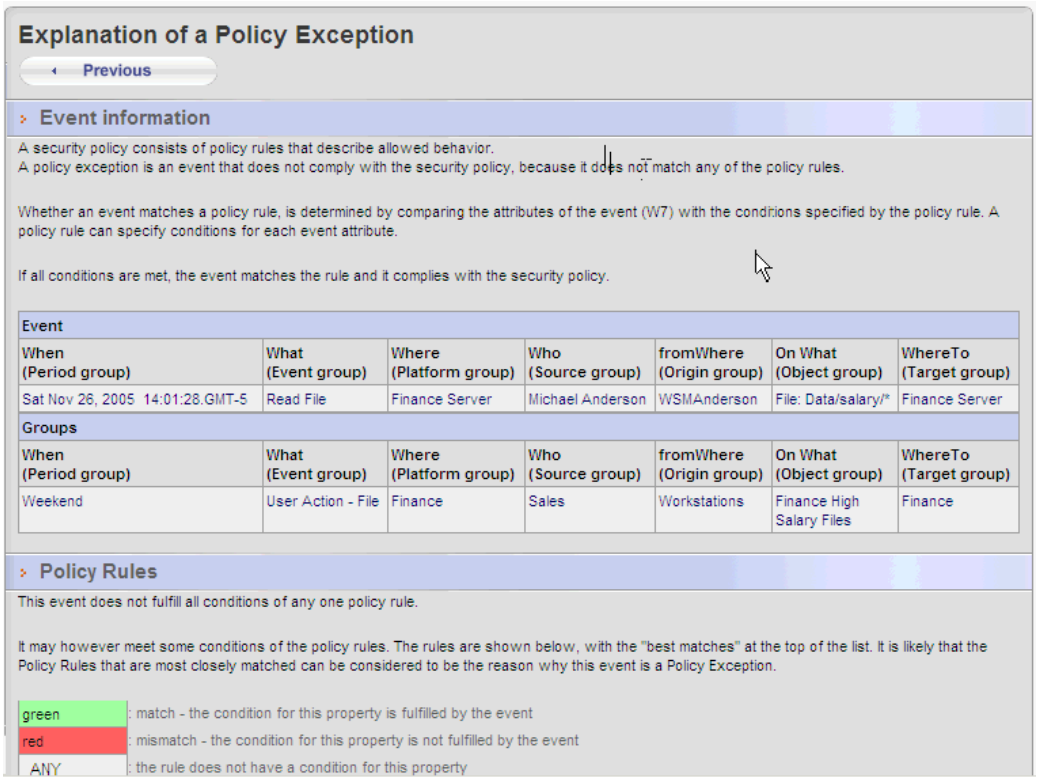
	Field	Group	
Severity	60 (1x)	This is a policy exception This is a special attention	
When	Sat Nov 26, 2005 14:01:28.GMT-5	Weekend	10
What	Read File	User Action - File	50 40
Where	Finance Server	Finance	50
Who	Michael Anderson	Sales	30 30 20
From Where	WSMAnderson	Workstations	10
On What	File: Data/salary/*	Finance High Salary Files	30 20
Where To	Finance Server	Finance	50

Incident Tracking

Additional information

Investigate

圖 4.4.6　事件詳細內容



Explanation of a Policy Exception

Previous

Event information

A security policy consists of policy rules that describe allowed behavior.
A policy exception is an event that does not comply with the security policy, because it does not match any of the policy rules.

Whether an event matches a policy rule, is determined by comparing the attributes of the event (W7) with the conditions specified by the policy rule. A policy rule can specify conditions for each event attribute.

If all conditions are met, the event matches the rule and it complies with the security policy.

Event						
When (Period group)	What (Event group)	Where (Platform group)	Who (Source group)	fromWhere (Origin group)	On What (Object group)	WhereTo (Target group)
Sat Nov 26, 2005 14:01:28.GMT-5	Read File	Finance Server	Michael Anderson	WSMAnderson	File: Data/salary/*	Finance Server
Groups						
When (Period group)	What (Event group)	Where (Platform group)	Who (Source group)	fromWhere (Origin group)	On What (Object group)	WhereTo (Target group)
Weekend	User Action - File	Finance	Sales	Workstations	Finance High Salary Files	Finance

Policy Rules

This event does not fulfill all conditions of any one policy rule.

It may however meet some conditions of the policy rules. The rules are shown below, with the "best matches" at the top of the list. It is likely that the Policy Rules that are most closely matched can be considered to be the reason why this event is a Policy Exception.

green	: match - the condition for this property is fulfilled by the event
red	: mismatch - the condition for this property is not fulfilled by the event
ANY	: the rule does not have a condition for this property

圖 4.4.7　政策違反情況說明

Policy Rules

This event does not fulfill all conditions of any one policy rule.

It may however meet some conditions of the policy rules. The rules are shown below, with the "best matches" at the top of the list. It is likely that the Policy Rules that are most closely matched can be considered to be the reason why this event is a Policy Exception.

green	: match - the condition for this property is fulfilled by the event
red	: mismatch - the condition for this property is not fulfilled by the event
ANY	: the rule does not have a condition for this property

When (Period group)	What (Event group)	Where (Platform group)	Who (Source group)	fromWhere (Origin group)	On What (Object group)	WhereTo (Target group)	Description
Weekend	User Actions - File	_ANY_	Administrators	_ANY_	_ANY_	_ANY_	
Office Hours	User Actions - File	_ANY_	Salary Administration	_ANY_	Salary Files	_ANY_	
Office Hours	User Actions - File	_ANY_	Sales	_ANY_	Client Maintenance	_ANY_	
Office Hours	User Actions - File	_ANY_	Sales	_ANY_	Client Objects	_ANY_	
ANY	User Actions - File	_ANY_	Financial Management	_ANY_	Finance High	_ANY_	
Office Hours	User Actions - File	_ANY_	Financial Staff	_ANY_	Finance High	_ANY_	
ANY	System Operations	_ANY_	_ANY_	_ANY_	_ANY_	_ANY_	
ANY	System Processes	_ANY_	_ANY_	_ANY_	_ANY_	_ANY_	
ANY	System Actions	_ANY_	_ANY_	_ANY_	_ANY_	_ANY_	
ANY	Password Changes	_ANY_	_ANY_	_ANY_	_ANY_	_ANY_	
ANY	Logon and logoff	_ANY_	_ANY_	_ANY_	_ANY_	_ANY_	

圖 4.4.8　政策規則

Sarbanes Oxley Regulation Reports

Title	Description
Sarbanes Oxley (FFIEC 1.1.1.4) Security Policy report	No description given
Sarbanes Oxley (FFIEC 1.3.1.1) Classification report	No description supplied
Sarbanes Oxley (6.3, 8.1.3) Security alert	Alerts sent in response to policy exceptions or special attention exceptions.
Sarbanes Oxley (8.1.2) Operational change control	Changes to the operating environment such as system updates, DBA activity etc.
Sarbanes Oxley (8.1.5) External contractors	Exceptions and failures caused by External Contractors.
Sarbanes Oxley (8.3) Malicious attacks	Exceptions and failures due to Malicious attacks.
Sarbanes Oxley (8.4.2) Operator log	Actions performed by the IT Admin staff.
Sarbanes Oxley (8.5) Network management	Actions and everts caused by users on Network Services.
Sarbanes Oxley (8.7.4.1) Mail server	Exceptions and failures for the Mail Server assets.
Sarbanes Oxley (8.7.6) Publicly available systems	Actions and exceptions on Publicly Published Data.
Sarbanes Oxley (9.2.4, 9.7) Review of user access rights	Actions performed by administrators on users.
Sarbanes Oxley (9.2.4.c, 9.7) System access and use	Successes and failures against key assets
Sarbanes Oxley (9.3) User responsibilities and password use	Logon failures and successes either locally or remotely.
Sarbanes Oxley (9.4) Network access control	Actions performed on and events and exceptions generated by Network or Router.
Sarbanes Oxley (9.4.4) Node authentication	Authentication of connections to remote computer systems
Sarbanes Oxley (9.4.5) Remote diagnostic port access	Detection of accesses to the diagnostic ports on servers.
Sarbanes Oxley (9.5.3) User identification and authentication	Logon/Logoff successes and failures.
Sarbanes Oxley (9.5.5) System utilities	Usage of system utilities
Sarbanes Oxley (9.6) Application access control	Actions, Exceptions and events on HR Data, Sensitive Data, User Sensitive Data, System, Financial Data, Proprietary Data and General Data.
Sarbanes Oxley (9.6.1) Information access restrictions	Who accessed sensitive or private data successfully or unsuccessfully

圖 4.4.9　沙氏法案報告

Data access of Finance database

Time period setup

Summary report

Who group	What group	On What group	Where to group	#Events	#Pol.Excp.	#Spec.Att	#Fail.
Administrators	User Actions - File	Financial Data	Finance Server	7	7	7	0
Administrators	User Actions - File	HR Data	HR Server	5	5	0	0
Administrators	User Actions - File	Sensitive Data	Finance Server	7	7	7	0
System	User Actions - File	Financial Data	Finance Server	42	0	0	0
System	User Actions - File	Salary Data	Finance Server	306	0	0	0
System	User Actions - File	Sensitive Data	Finance Server	42	0	0	0
NY Management	User Actions - File	Financial Data	Finance Server	494	0	0	0
Wealth Management	User Actions - File	Financial Data	Finance Server	178	0	0	0
Stock Holders	User Actions - File	Financial Data	Finance Server	10	0	0	0
Client Maintenance	User Actions - File	Financial Data	Finance Server	1	0	0	0
Banking Reservations	User Actions - File	Financial Data	Finance Server	4	0	0	0
FinAdmin Management	User Actions - File	Financial Data	Finance Server	166	0	0	0
FinAdmin Management	User Actions - File	HR Data	HR Server	203	0	0	0
FinAdmin Management	User Actions - File	Sensitive Data	Finance Server	166	0	0	0
FinAdmin Management	User Actions - File	Financial Data	Mainframe FIN	294	7	7	0
FinAdmin Management	User Actions - File	General Data	Mainframe FIN	150	5	0	0
FinAdmin Management	User Actions - File	Sensitive Data	Mainframe FIN	334	7	7	0
FinAdmin Staff	User Actions - File	Financial Data	Finance Server	121	0	0	0
FinAdmin Staff	User Actions - File	HR Data	HR Server	121	0	0	0

1 2 3

圖 4.4.10　財務資料庫存取紀錄

Sarbanes Oxley (9.2.4.c, 9.7) System access and use	Successes and failures against key assets
Sarbanes Oxley (9.3) User responsibilities and password use	Logon failures and successes either locally or remotely.
Sarbanes Oxley (9.4) Network access control	Actions performed on and events and exceptions generated by Network or Router.
Sarbanes Oxley (9.4.4) Node authentication	Authentication of connections to remote computer systems
Sarbanes Oxley (9.4.5) Remote diagnostic port access	Detection of accesses to the diagnostic ports on servers.
Sarbanes Oxley (9.5.3) User identification and authentication	Logon/Logoff successes and failures.
Sarbanes Oxley (9.5.5) System utilities	Usage of system utilities
Sarbanes Oxley (9.6) Application access control	Actions, Exceptions and events on HR Data, Sensitive Data, User Sensitive Data, System, Financial Data, Proprietary Data and General Data.
Sarbanes Oxley (9.6.1) Information access restrictions	Who accessed sensitive or private data successfully or unsuccessfully.
Sarbanes Oxley (9.6.2) Sensitive system isolation	Exceptions and failures against sensitive systems data in asset groups User, HR Data, Source Code, and Financial Data
Sarbanes Oxley (9.7.2.3) Logging and reviewing events	Exceptions and failures recorded by the InSight system.
Sarbanes Oxley (9.8.1) Mobile worker	Exceptions and failures for mobile workers.
Sarbanes Oxley (9.8.2) Teleworker	Exceptions and failures for teleworkers.
Sarbanes Oxley (10.4.1) Control of operational software	Exceptions and failures caused by updating or changing of critical system components.
Sarbanes Oxley (10.4.2) System test data	Controlled access to System test data
Sarbanes Oxley (10.4.3) Source code access	Exceptions and failures caused by accessing Source Code.
Sarbanes Oxley (10.5.4) Covert channels and trojan code	Exceptions found from anti virus software
Sarbanes Oxley (12.1.3) Human Resource data access	Exceptions and failures against Human Resources data
Sarbanes Oxley (12.1.4) Data access	Exceptions and failures against HR, Sensitive and Proprietary data.
Sarbanes Oxley (12.1.5) Prevention of misuse of information processing facilities	Misuse of information processing facilities for non-business purposes
Sarbanes Oxley (12.1.7.1) Rules for evidence	InSight self audit report. Evidence collected conforms to the rules laid down in the relevant law
Sarbanes Oxley (12.2.1) Compliance with security policy	InSight self audit report. Monitors changes to InSight settings.
Sarbanes Oxley (12.2.2) Technical compliance checking	Show that the systems have been checked for compliance with security implementation standards

圖 4.4.11　沙氏法案法規政策清單

Data access of Finance database

Time period setup

Summary report

Who group	What group	On What group	Where to group	#Events	#Pol.Excp.	#Spec.Att	#Fail.
Administrators	User Actions - File	Financial Data	Finance Server	7	7	7	0
Administrators	User Actions - File	HR Data	HR Server	5	5	0	0
Administrators	User Actions - File	Sensitive Data	Finance Server	7	7	7	0
System	User Actions - File	Financial Data	Finance Server	42	0	0	0
System	User Actions - File	Salary Data	Finance Server	306	0	0	0
System	User Actions - File	Sensitive Data	Finance Server	42	0	0	0
NY Management	User Actions - File	F				0	0
Wealth Management	User Actions - File	F	Finance Server	178	0	0	0
Stock Holders	User Actions - File	F		18	0	0	0
Client Maintenance	User Actions - File	F	Finance Server	11	0	0	0
Banking Reservations	User Actions - File	F	Finance Server	1	0	0	0
FinAdmin Management	User Actions - File	F	Finance Server	153	0	0	0
FinAdmin Management	User Actions - File	H	HR Server	203	0	0	0
FinAdmin Management	User Actions - File	S	Finance Server	1386	0	0	0
FinAdmin Management	User Actions - File	F	Mainframe FIN	1294	7	7	0
FinAdmin Management	User Actions - File	C	Mainframe FIN	5	0	0	0
FinAdmin Management	User Actions - File	S	Mainframe FIN	334	7	7	0
FinAdmin Staff	User Actions - File	Financial Data	Finance Server	121	0	0	0
FinAdmin Staff	User Actions - File	HR Data	HR Server	121	0	0	0

Filter settings

Column Filter

Who Group

What Group

On What Group

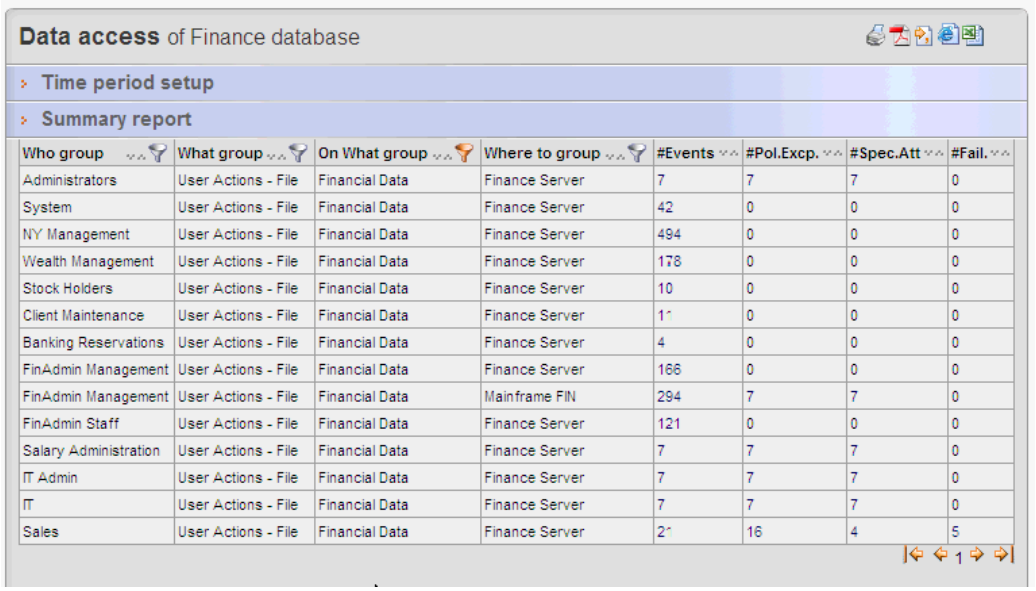
Where To Group

Use ? and * as wildcards and ^ as escape character.

Apply　Clear　Cancel

1 2 3

圖 4.4.12　篩選財務資料庫存取事件



Data access of Finance database

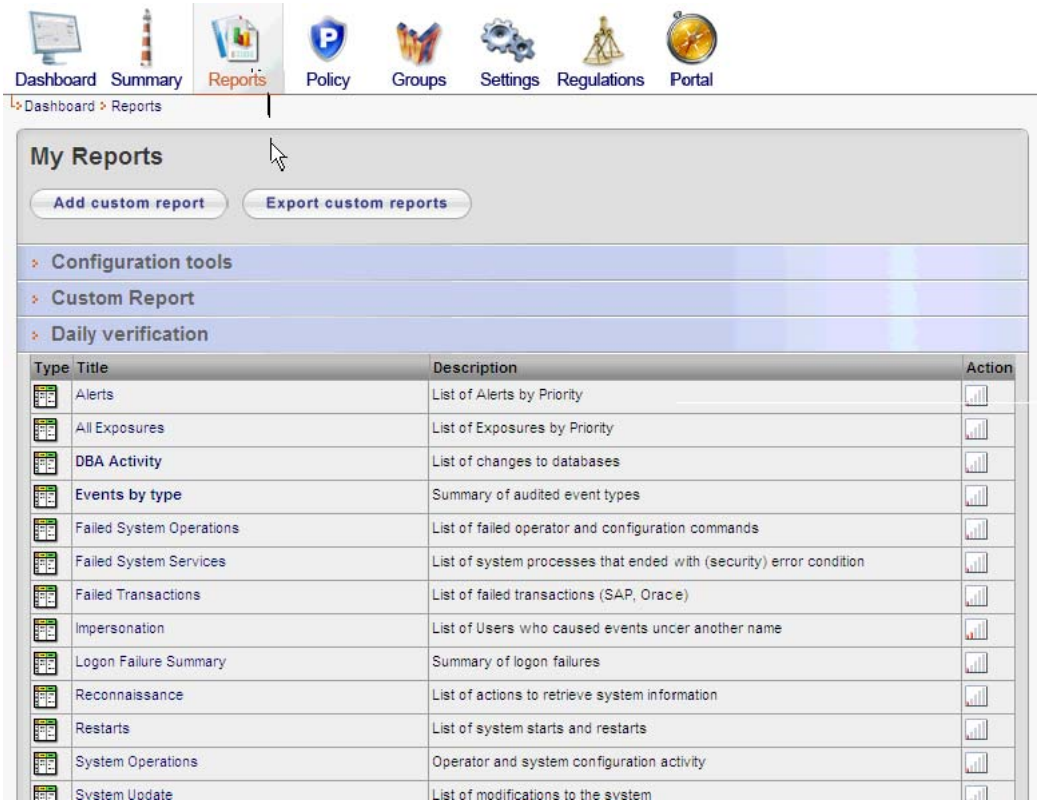
Time period setup

Summary report

Who group	What group	On What group	Where to group	#Events	#Pol.Excp.	#Spec.Att	#Fail.
Administrators	User Actions - File	Financial Data	Finance Server	7	7	7	0
System	User Actions - File	Financial Data	Finance Server	42	0	0	0
NY Management	User Actions - File	Financial Data	Finance Server	494	0	0	0
Wealth Management	User Actions - File	Financial Data	Finance Server	178	0	0	0
Stock Holders	User Actions - File	Financial Data	Finance Server	10	0	0	0
Client Maintenance	User Actions - File	Financial Data	Finance Server	1	0	0	0
Banking Reservations	User Actions - File	Financial Data	Finance Server	4	0	0	0
FinAdmin Management	User Actions - File	Financial Data	Finance Server	166	0	0	0
FinAdmin Management	User Actions - File	Financial Data	Mainframe FIN	294	7	7	0
FinAdmin Staff	User Actions - File	Financial Data	Finance Server	121	0	0	0
Salary Administration	User Actions - File	Financial Data	Finance Server	7	7	7	0
IT Admin	User Actions - File	Financial Data	Finance Server	7	7	7	0
IT	User Actions - File	Financial Data	Finance Server	7	7	7	0
Sales	User Actions - File	Financial Data	Finance Server	2	16	4	5

1

圖 4.4.13　財務資料庫存取篩選結果



Dashboard　Summary　Reports　Policy　Groups　Settings　Regulations　Portal

Dashboard › Reports

My Reports

Add custom report　Export custom reports

Configuration tools

Custom Report

Daily verification

Type	Title	Description	Action
	Alerts	List of Alerts by Priority	
	All Exposures	List of Exposures by Priority	
	DBA Activity	List of changes to databases	
	Events by type	Summary of audited event types	
	Failed System Operations	List of failed operator and configuration commands	
	Failed System Services	List of system processes that ended with (security) error condition	
	Failed Transactions	List of failed transactions (SAP, Orace)	
	Impersonation	List of Users who caused events uncer another name	
	Logon Failure Summary	Summary of logon failures	
	Reconnaissance	List of actions to retrieve system information	
	Restarts	List of system starts and restarts	
	System Operations	Operator and system configuration activity	
	System Update	List of modifications to the system	

圖 4.4.14　客製化報告(一)

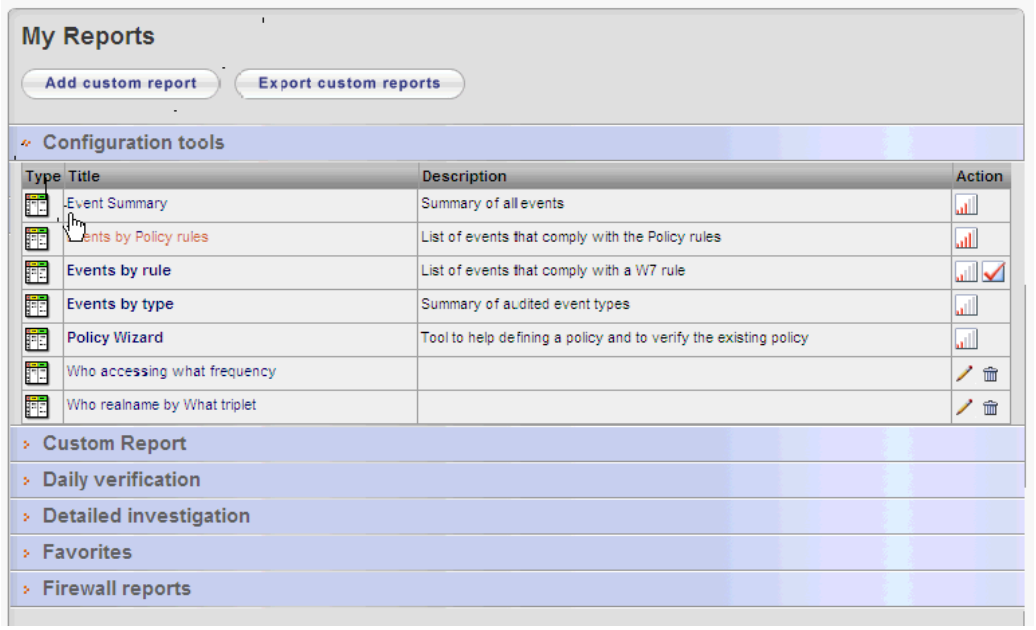
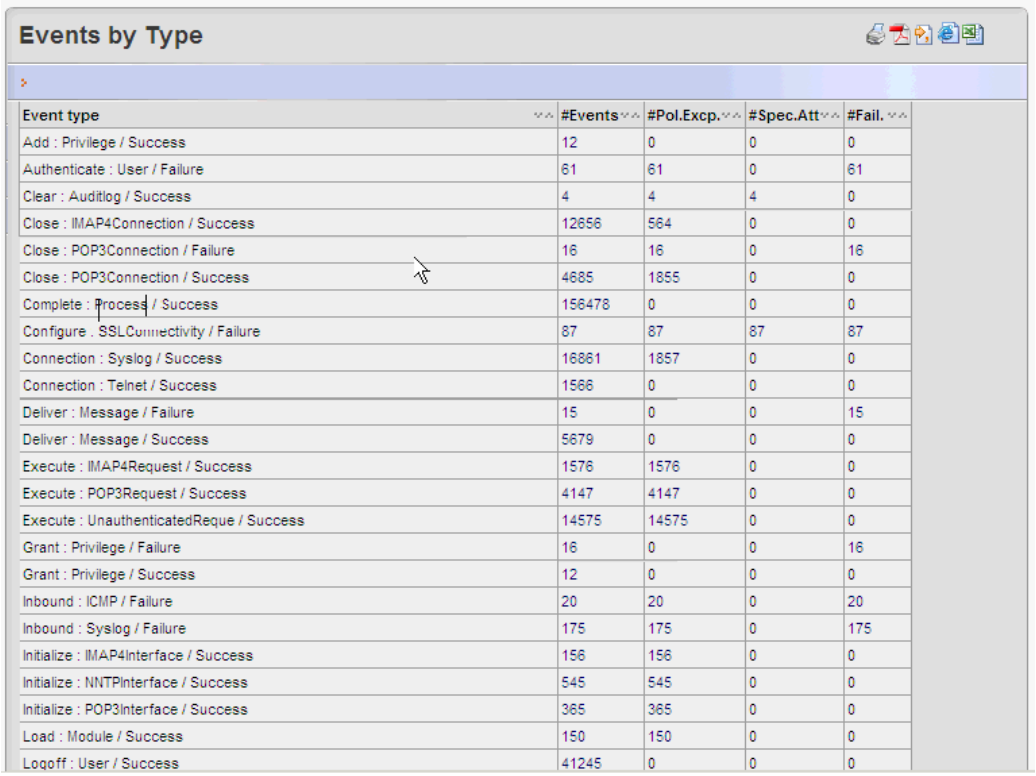
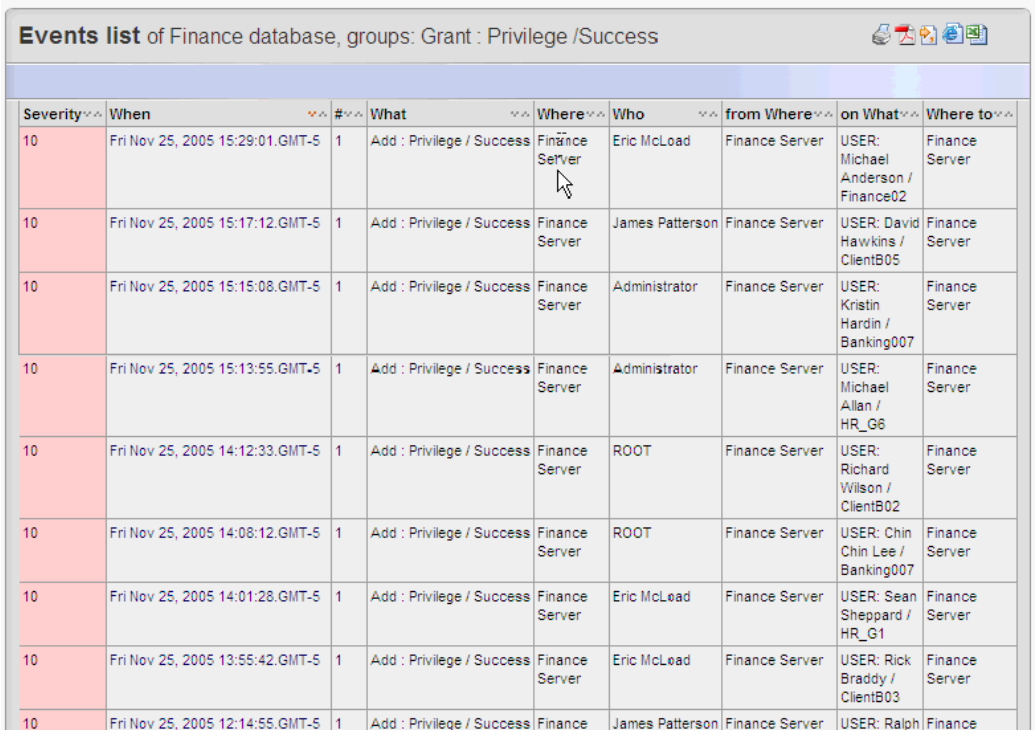


圖 4.4.15　客製化報告(二)



Event type	#Events	#Pol.Excp.	#Spec.Att	#Fail.
Add : Privilege / Success	12	0	0	0
Authenticate : User / Failure	61	61	0	61
Clear : Auditlog / Success	4	4	4	0
Close : IMAP4Connection / Success	12656	564	0	0
Close : POP3Connection / Failure	16	16	0	16
Close : POP3Connection / Success	4685	1855	0	0
Complete : Process / Success	156478	0	0	0
Configure : SSLConnectivity / Failure	87	87	87	87
Connection : Syslog / Success	16861	1857	0	0
Connection : Telnet / Success	1566	0	0	0
Deliver : Message / Failure	15	0	0	15
Deliver : Message / Success	5679	0	0	0
Execute : IMAP4Request / Success	1576	1576	0	0
Execute : POP3Request / Success	4147	4147	0	0
Execute : UnauthenticatedReque / Success	14575	14575	0	0
Grant : Privilege / Failure	16	0	0	16
Grant : Privilege / Success	12	0	0	0
Inbound : ICMP / Failure	20	20	0	20
Inbound : Syslog / Failure	175	175	0	175
Initialize : IMAP4Interface / Success	156	156	0	0
Initialize : NNTPInterface / Success	545	545	0	0
Initialize : POP3Interface / Success	365	365	0	0
Load : Module / Success	150	150	0	0
Logoff : User / Success	41245	0	0	0

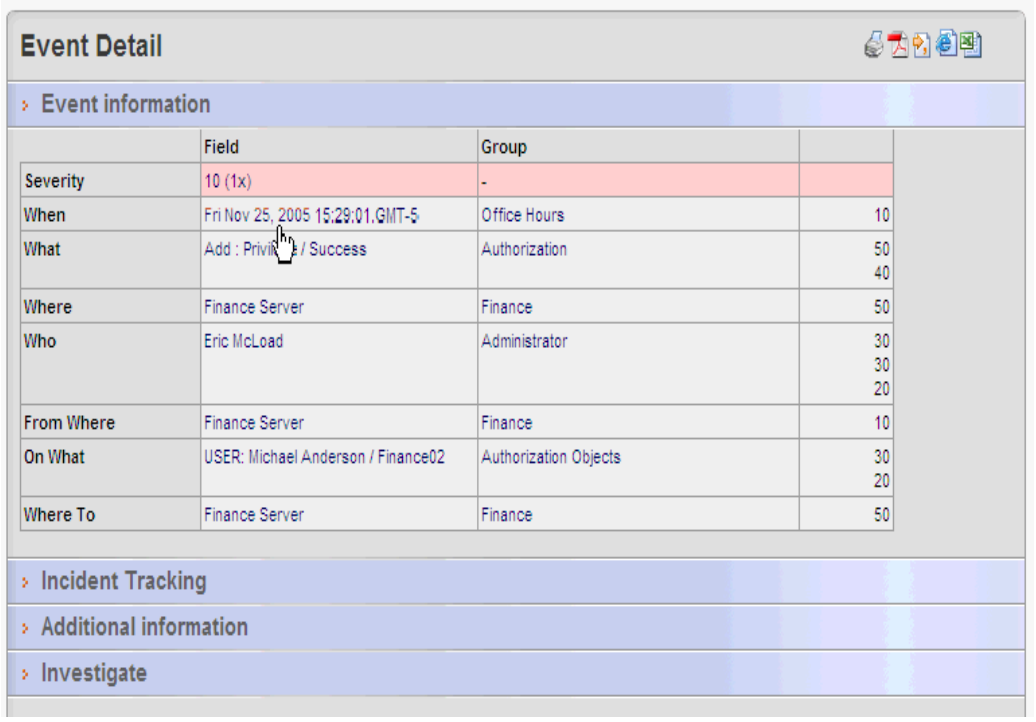
圖 4.4.16　依類別排序之事件清單



Events list of Finance database, groups: Grant : Privilege /Success

Severity	When	#	What	Where	Who	from Where	on What	Where to
10	Fri Nov 25, 2005 15:29:01.GMT-5	1	Add : Privilege / Success	Finance Server	Eric McLoad	Finance Server	USER: Michael Anderson / Finance02	Finance Server
10	Fri Nov 25, 2005 15:17:12.GMT-5	1	Add : Privilege / Success	Finance Server	James Patterson	Finance Server	USER: David Hawkins / ClientB05	Finance Server
10	Fri Nov 25, 2005 15:15:08.GMT-5	1	Add : Privilege / Success	Finance Server	Administrator	Finance Server	USER: Kristin Hardin / Banking007	Finance Server
10	Fri Nov 25, 2005 15:13:55.GMT-5	1	Add : Privilege / Success	Finance Server	Administrator	Finance Server	USER: Michael Allan / HR_G6	Finance Server
10	Fri Nov 25, 2005 14:12:33.GMT-5	1	Add : Privilege / Success	Finance Server	ROOT	Finance Server	USER: Richard Wilson / ClientB02	Finance Server
10	Fri Nov 25, 2005 14:08:12.GMT-5	1	Add : Privilege / Success	Finance Server	ROOT	Finance Server	USER: Chin Chin Lee / Banking007	Finance Server
10	Fri Nov 25, 2005 14:01:28.GMT-5	1	Add : Privilege / Success	Finance Server	Eric McLoad	Finance Server	USER: Sean Sheppard / HR_G1	Finance Server
10	Fri Nov 25, 2005 13:55:42.GMT-5	1	Add : Privilege / Success	Finance Server	Eric McLoad	Finance Server	USER: Rick Braddy / ClientB03	Finance Server
10	Fri Nov 25, 2005 12:14:55.GMT-5	1	Add : Privilege / Success	Finance	James Patterson	Finance Server	USER: Ralph	Finance

圖 4.4.17　篩選後之事件清單



Event Detail

Event information

	Field	Group	
Severity	10 (1x)	-	
When	Fri Nov 25, 2005 15:29:01.GMT-5	Office Hours	10
What	Add : Privilege / Success	Authorization	50 40
Where	Finance Server	Finance	50
Who	Eric McLoad	Administrator	30 30 20
From Where	Finance Server	Finance	10
On What	USER: Michael Anderson / Finance02	Authorization Objects	30 20
Where To	Finance Server	Finance	50

Incident Tracking

Additional information

Investigate

圖 4.4.18　事件詳細內容(一)

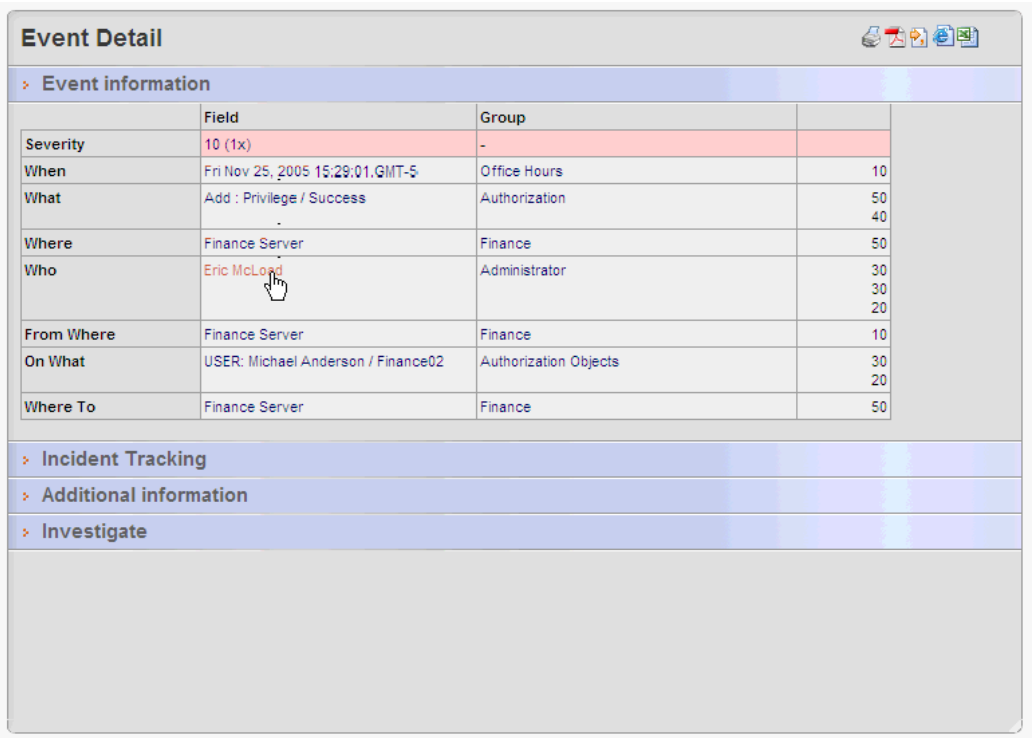


圖 4.4.19　事件詳細內容(二)

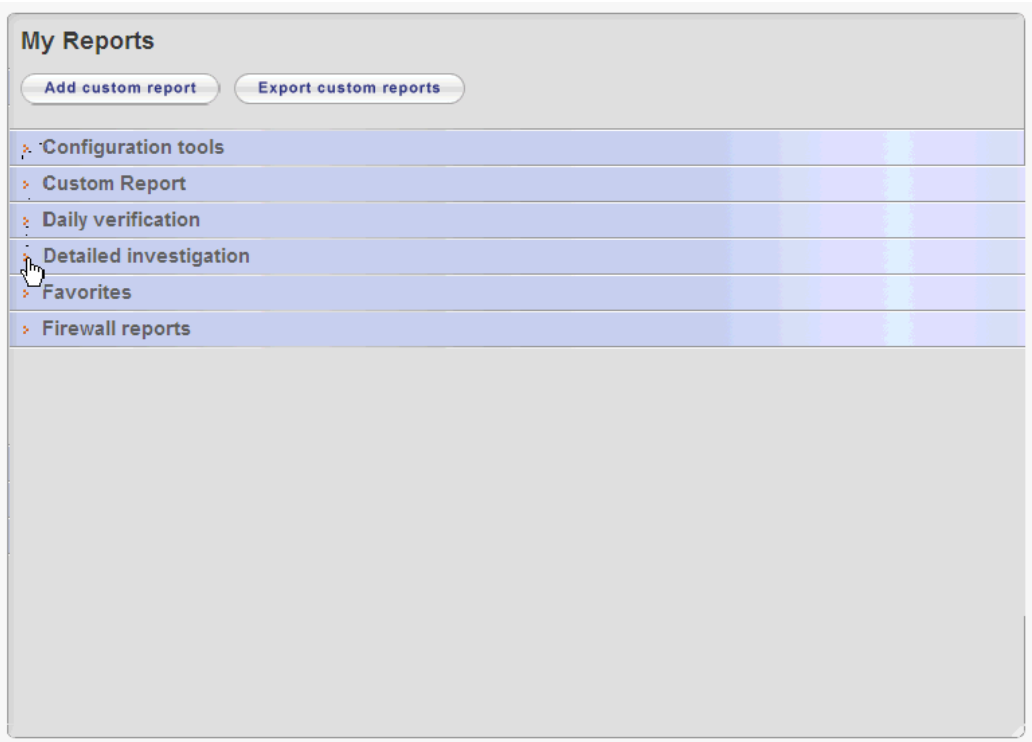


圖 4.4.20　客製化報告入口畫面

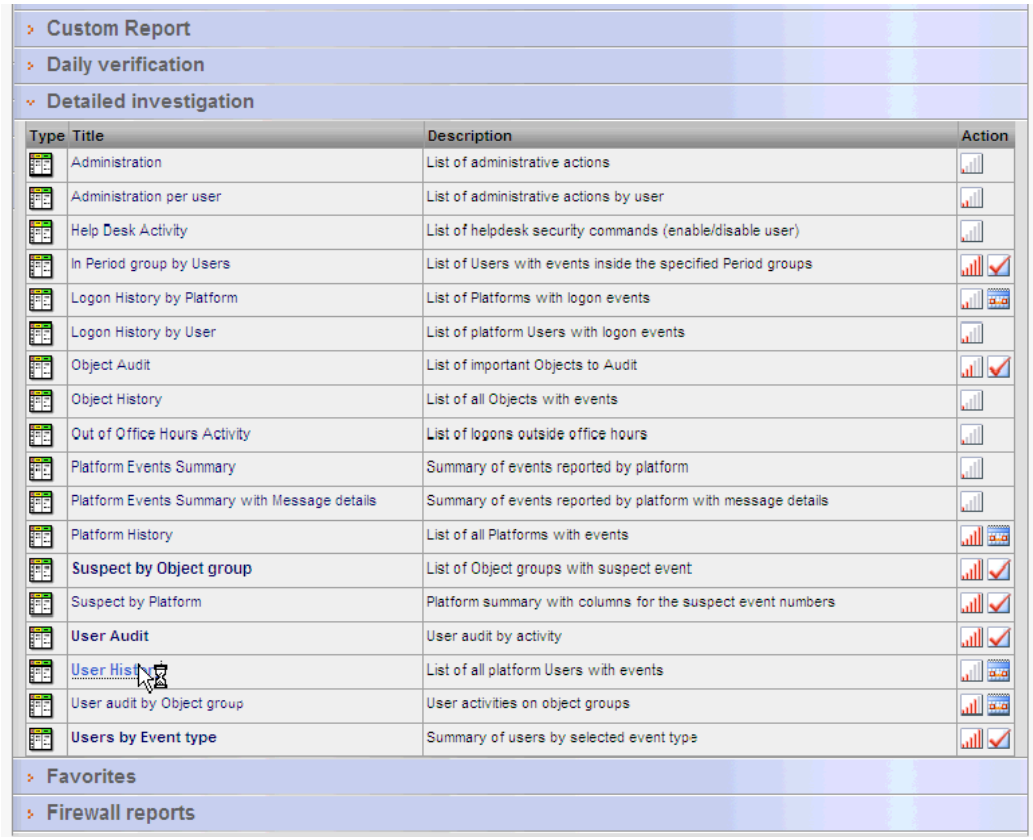


圖 4.4.21　事件調查畫面

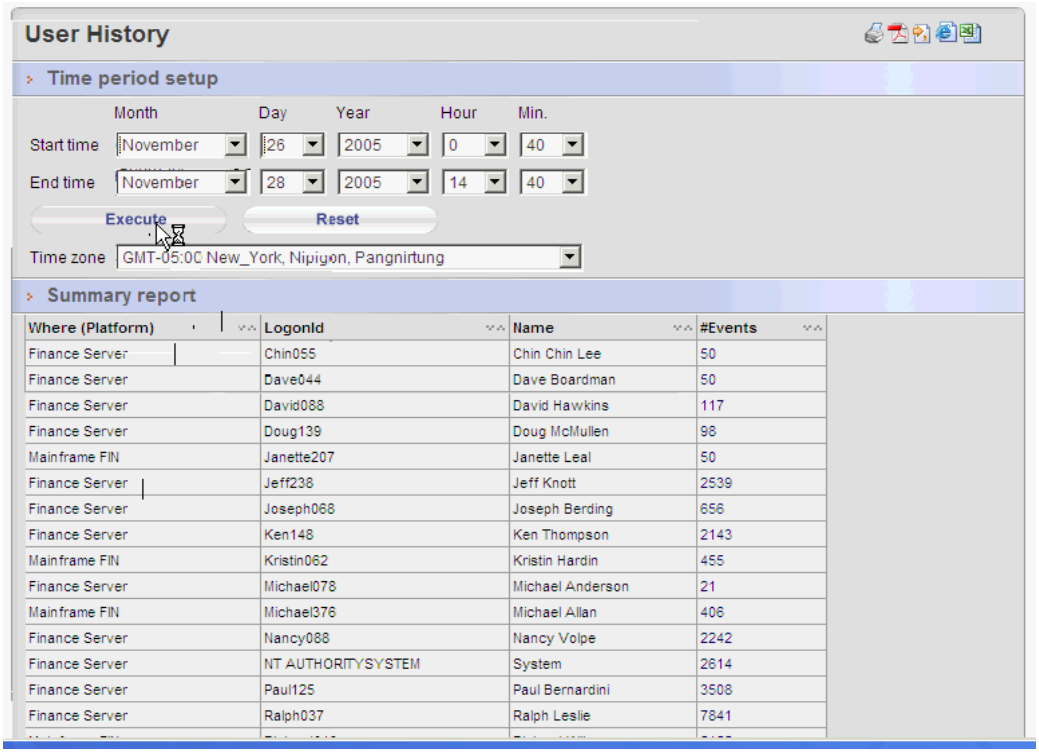


圖 4.4.22　使用者存取歷史紀錄(一)

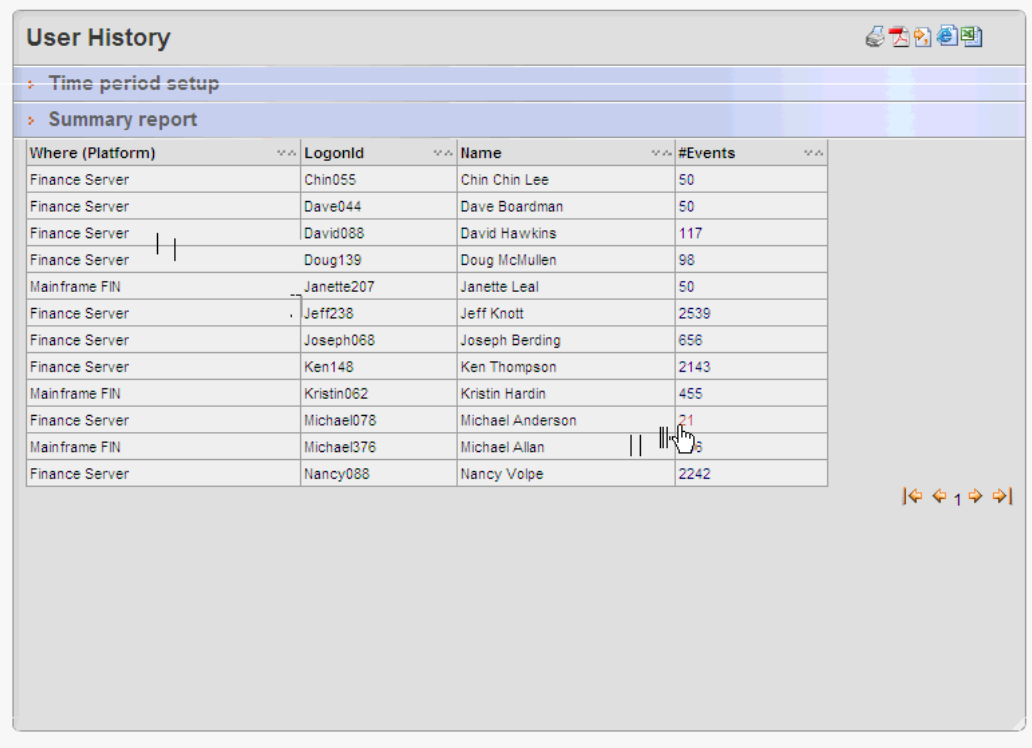


圖 4.4.23　使用者存取歷史紀錄(二)

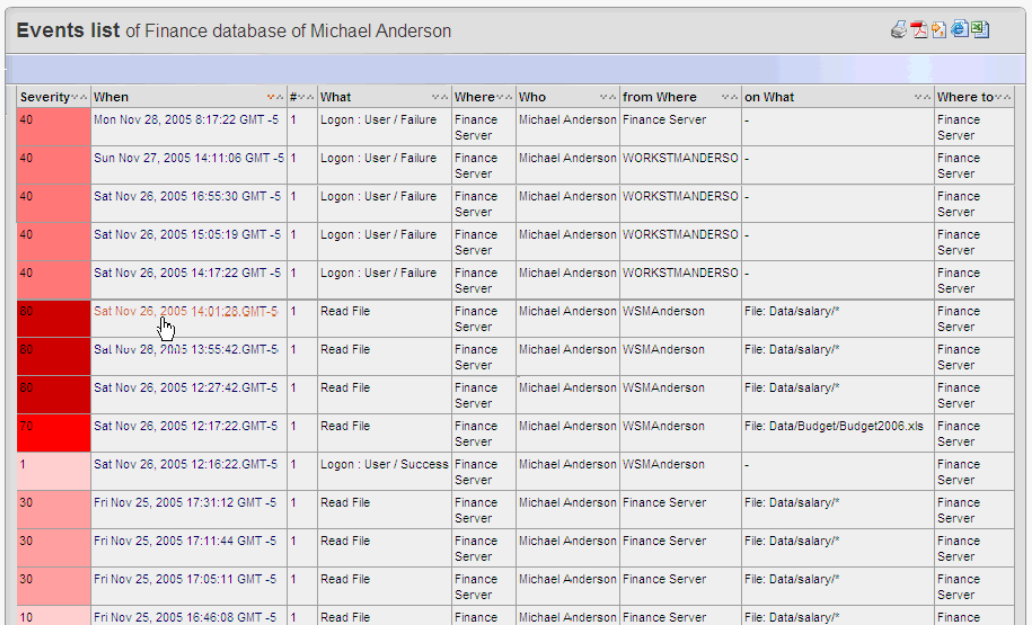


圖 4.4.24　針對特定使用者篩選之事件清單

4.3 系統實例操作說明

面臨當今日益新增的法規和稽核要求，企業必須遵守眾多的法規，例如沙氏法案、金融服務法案、醫療保險可攜性與責任法案(HIPAA)，以及新巴塞爾資本協議等等。近期的研究報告發現，賦予權限的使用者最有可能是風險的來源，這更加重了處理此問題的複雜度。若因不當授權而產生錯誤或蓄意的行動，內部風險可能會讓企業蒙受極大的損失。

如圖 4.4.1 符規儀表板(一)所示，在與現有政策規定比較之後，符規儀表板會顯示企業組織目前的法規符合狀況。左側的節點格線可讓管理者一覽可能有問題的地方。格線上的紅色泡泡指出需要研究的事件，且泡泡的大小代表特定類形的事件總數。因此，讓我們檢視「財務」資料庫的摘要資訊，以研究財務資料所顯示的使用者活動。

如圖 4.4.2 符規儀表板(二)所示，我們再一次在「銷售」與「高度敏感性財務資料」兩個區塊的交叉處看到一項警告。 按一下該泡泡，我們可取得事件清單。

如圖 4.4.3 資料庫監控結果之摘要內容所示，於「事件」資訊格線中，在「高敏感性財務」與「銷售」交叉處按一下紅色大泡泡。

如圖 4.4.4 事件清單畫面所示，系統提供以許多不同方式檢視事件的功能。讓我們依嚴重的高低程度整理該清單，並研究其中幾個嚴重警示。在「事件」清單中，按一下「嚴重度」標題右側的向下箭頭。

如圖 4.4.5 依嚴重程度排序後之事件清單所示，在此我們可以看見初級客戶銷售經理邁可曾經觀看「薪資」資料。按一下該事件，我們可以向下切入細節部分。在該表的第一列，按一下「時間」欄位的日期。

如圖 4.4.6 事件詳細內容所示，請注意，經過按下幾次的滑鼠，我們

可已從財務資料狀態的圖形綜覽，進入特定事件的詳細檢視表。在這些詳細資料中，我們可清楚看到邁可隸屬於銷售群組，而他曾在週末檢視「高度敏感性財務資料」。邁可應該無法檢視該類資料，這也就是爲何被標上例外狀況註記的原因。

所有事件均依照一組定義授權活動的規則來進行評估，這是系統的一項功能。此外，系統藉由提供規則產生器，可以更容易判定組織與現有的安全政策規則，讓我們瞧瞧爲何該事件會被歸類爲例外狀況。

如圖 4.4.7 政策違反情況說明所示，在該表的「嚴重度」列中，按一下「此爲例外狀況」的文字。當某事件與適用的規則相比較時，若判定該事件是不被允許的，則會產生例外狀況。藉由檢視相關解釋，您可以完全瞭解爲何該事件被判定爲例外狀況。這些規則說明「高度敏感性財務資料」應當只提供給財務管理團隊成員、財務人員與系統管理員。然而，我們在任何地方均未看到允許銷售群組成員存取該資訊的相關規則。

如圖 4.4.8 政策規則所示，系統提供了一個介面，可以讓管理者定義要產生的符規報告。

如圖 4.4.9 沙氏法案報告所示，我們剛剛調查邁可曾經檢視過具存取限制的特定檔案。現在我們看看整體的狀況，以判定財務資料是否出現其他狀況。「資料存取」報告是一份符合此用途的有用報告。往下捲動並按一下「沙氏法案 (12.1.4) 資料」存取。

如圖 4.4.11 沙氏法案法規政策清單所示，此報告提供所有發生於 SOX 相關資料的彙總，即「人力資源資料」、「敏感性資料」與「財務資料」，讓我們篩選「財務資料」。在「群組」欄位標題按一下篩選圖示，在「群組」文字欄位元中輸入「財務」，然後按一下「套用」。

如圖 4.4.12 篩選財務資料庫存取事件、圖 4.4.13 財務資料庫存取篩選

結果所示，該清單的項目會減少，而我們在這裡可看見「銷售」與 21 個事件相關。我們可以透過檢視標準報告，以瞭解爲何屬於「銷售」群組的邁可能夠存取該類資料。在頁面的上方，按一下「報告」圖示。

如圖 4.4.14 客製化報告(一)所示，會出現一份項目眾多的清單，內含事先定義好的標準報告，如設定、驗證與研究報告。此外圖 4.2.15 客製化報告(二)，系統提供自訂報告的撰寫程式。按一下「每日」驗證左邊的紅色箭頭，以摺疊該區塊。按一下「設定」工具左邊的紅色箭頭，以展開該區塊。

如圖 4.4.16 依類別排序之事件清單所示，在「設定」工具區塊內，我們依「類型」報告尋找「事件」。此報告提供所有已經發生的不同事件的彙總。依類型按一下「事件」。

如圖 4.4.17 篩選後之事件清單所示，在該表第一列的「事件編號」直欄中，按一下「12」。

如圖 4.4.17 篩選後之事件清單所示，在先前的報告中，我們看見邁可曾檢視財務資料，並因此而產生一些例外狀況。我們看到政策規則不允許銷售群組內的成員存取該類資料。但邁可能夠存取該資料，代表有人賦予他存取的權限。系統可簡易判定是誰賦予邁可權限。 讓我們向下切入並一窺究竟。在該表的第一列，按一下「時間」欄位的日期。

如圖 4.4.19 事件詳細內容(二)所示，如我們所看到的，一位系統管理員艾力克將邁可新增至 Finance02 群組。

經過簡單的調查，我們知道該組成員有權限存取薪資資料。現在我們知道邁可所做的事，以及誰賦予他存取權限。但爲何艾力克要給他這些權限呢？關於此問題，我們需檢視「使用者紀錄」報告。

如圖 4.4.21 事件調查畫面所示，在網頁上方，按一下「報告」圖示。展開詳細研究區塊，並選取「使用者紀錄」。

如圖 4.4.22 使用者存取歷史紀錄(一)所示，此報告彙總了在特定期間內所觸發的事件。在「使用者紀錄」頁面上，「時間設定」下方，將「起始」時間變更至 11 月 26 日，然後按一下「執行」鈕。

這裡我們看見邁可在財務伺服器上有 21 個事件。在「事件編號」直欄中，按一下「21」。(由下往上數的第 3 列)

往下切入邁可的事件，我們看見他首先檢視美國客戶的銷售合約。這可能是他爲何能取得該資料授權的首要原因。

如圖 4.4.24 針對特定使用者篩選之事件清單所示，但之後，他也檢視了薪資資料。 邁可首先存取該資料 5 次，產生了嚴重度較低的例外狀況。但如您所看到的，再存取 3 次產生的嚴重度則較高。此資訊可協助安全人員快速辨識可疑的行爲，並使他們能夠準確判斷違反公司規則的行爲是如何被啓動的。 經由此系統，管理者可持續擁有不被侵入的保障與相關的檔案證據，使您的資料與系統可依公司與法規原則進行管理。

第五章　研究結論、效益與建議

5.1　研究結論

中華電信的業務支撐系統，是以業務別爲分類項目進行縱向開發，系統的橫向整合能力並不足夠。也就是說，中華電信在部署業務支撐系統時，並沒有依循一致的資訊策略，因此，不僅各個系統是獨立運作的，也常有功能模組重疊的現象發生。其次，由於系統運作模式不一致，命名也不同，很難相互比對及稽核，相對的新系統開發及舊系統更新的效率也不高，最後，由於各系統的軟硬體平台不同，不僅得花費更多的資金及資源維護系統，對使用者來說，亦需熟悉不同的畫面及指令才能執行相關業務。傳統的資訊系統架構，已無法讓電信服務供應商在最短時間內視市場狀況彈性調配系統功能模組提供相對應的服務。

本研究爲企業資訊安全政策施行架構系統，除了連續的監控和帳務收支檢查之外，政策驅動性質、變動管理和政策規章轉變機制結合後，已使政策趨動安全執行(PDSE)成爲一種架構，使連續的過程改進變得更完善。資訊安全執行是企業最重要的一個議題，而多層次的政策趨動安全執行(PDSE)架構建議與詳述能幫助組織統整，有效地實現並且監控執行。

PDSE 的四層式架構，提供不同資訊安全控管人員不同的觀點，並提供了一個將政策轉換成規則的機制，且保持讓資訊安全控管流程由政策驅動，形成一個持續改善的資訊安全控管流程。

這個架構已實際建置於中華電信，成功地展現其持續改善流程、降低符規成本、提升符規彈性與資安施行效率的多項效益。雖然帳務系統是中華電信核心操作支援系統(OSS，operation support system)之一，下一階段

工作有可能是在其他領域，例如履行在電信業裡的保證實施政策趨動安全執行(PDSE)。另一個研究的潛在領域，在於爲公司安全執行過程的衡量標準，更深入地進行有系統的分析。

本研究透過與 IBM 及北科大合作，中華電信完成依循 SOA 所部署的帳務系統及聯單系統 POC 專案，成效極佳，不僅可讓中華電信使用，也可將該系統外銷給其他單位，本研究最終做出帳務整合系統，改善相關企業作業人工處理之效率，確保企業資訊資料、系統、設備及網路通訊安全，有效降低因人爲疏失、蓄意等風險，並建立資訊安全管理方向。

5.2 研究效益

電信公司正面臨著必須降低費率且提高效率的挑戰，以改善消費者的滿意度、適應消費者偏好的演變，並且還得遵從各種不同的外部、內在的條例。相對重要的是要有效且有效率地強制執行無特定結構的政策，而最被注意的是資訊安全執行的問題。

本研究提出了一個多層次的政策趨動式資訊安全施行架構(PDSE)，藉此引導電信公司的設備能完整且有效率地處理資訊安全執行。這四個層級（方法學、程序、資料和結構）可以在一張完整的圖片中一起呈現，並且也提供足夠的細節幫助不同專長的職員可以初步理解安全執行程序的完整資料。

除了連續監視和收支檢查之外，政策驅動性質、改變管理和政策規則的轉換機制在結合過後，已經使 PDSE 成爲一個可以促進連續過程進步的完整架構，它可以幫助組織不斷地藉由提高發現間隙爲基礎鞏固執行過程，以形成一個可以改善 PDSE 自動化、聯合過程與結構之連續過程的一個架構。

本研究系統已成功使用於中華電信公司，中華電信公司是世界上第 14 大的電信公司，該公司規定在以 SOA 爲基礎的 NGOSS 裡所允許的帳務系統中須檢驗降底遵從成本的有效性、提高符規彈性、改良安全執行效率。

中華電信在使用此系統後宣稱獲得的實際效益如下：

(1) 資安事件反應時間縮短 61%

(2) 符規成本降低 18%

(3) 新政策或修改政策的生效時間從兩天縮短爲四小時

5.3 研究建議方向與未來發展

雖然本研究已經導入中華電信，但往後若想要再進一步深入研究的話，因其帳務系統也是中華電信公司的核心 OSS(操作支援系統)之一，故首要目標是把其工作擴大到中華電信其他部分(Assurance、Fulfillment)，至於下一階段的工作項目的可能性將會是在其他的區域中介紹 PDSE，使本研究的系統能夠廣泛的被使用，例如 PDSE 架構在中華電信雲端計算服務的應用。

其次則是要如何有效地在通訊業裡執行實現和保證系統的功能。此外，在中華電信的履行和保證方面，可以在另一研究的潛在領域針對安全執行程式再更進一步的分析，該工作內容乃是分析本系統架構的內部如何執行符規的結合，且更深入地進行有系統的分析。

參考文獻

中文文獻

張偉斌(2001)。**網路資訊安全諮詢服務系統之研究**。國立臺北科技大學商業自動化與管理研究所碩士論文。

張詠翔(2005)。**結合 BS7799 與資訊安全藍圖建構－資訊安全評估機制之研究**。銘傳大學資訊管理學系碩士在職專班論文。

蔡思達(2007)。**以適應性結構化理論探討資訊安全管理系統導入之徵用過程與成效**。國立台灣科技大學資訊管理系研究所碩士論文。

方仁威(2004)。**資訊安全管理系統驗證作業之研究**。國立交通大學資訊管理研究所碩士論文。

藍雅雯(2009)。**架構導向 WiMAX 帳務管理研究**。國立中山大學資訊管理學系研究所碩士論文。

英文文獻

A. Zuccato, “Holistic Security Management Framework Applied in Electronic Commerce”, Computers & Security, Vol 26 (3), p256-265, 2007.

J. C. Sipior, B. T. Ward, “A Framework for Information Security Management based on Guid Standards: A United States Perspective”, Issues in Informing Science and Information Technology Vol 5, p52-60, 2008

Policy Enforcement Framework for Web Services and Grid Operational

Anton Chuvakin, Gunnar Peterson, "Logging in the Age of Web Services," IEEE Security & Privacy, Vol. 7 (3) , pp. 82-85, May/June, 2009.

K.J. Knapp, R.F. Morris Jr., T.E. Marshall, T. Anthony, “Information Security Policy: An Organizational-Level Process Model”, Computer & Security, Volume 28 (7), p493-508, 2009.

S.C. Shih, H.J. Wen, “E-enterprise Security Management Life Cycle”, Information Management & Computer Security, Vol 13 (2), p121-134, 2005.

D. Bradley, A. Josang, “Mesmerize – An Open Framework for Enterprise Security Management”, ACM International Conference Proceeding Series; Vol. 54, Proceedings of the second workshop on Australasian information security, Data Mining and Web Intelligence, and Software Internationalisation - Volume 32, Dunedin, New Zealand, p37-42, 2004

A. Sengupta, A. Mukhopadhyay, K. Ray, A.G. Roy, D. Aich, M.S. Barik, C. Mazumdar, “A Web Enabled Enterprise Security Management Framework based on a Unified Model of Enterprise Information System Security”, Lecture Notes in Computer Science, Vol 3803, p328-331, 2005.

J. Colye, J. Demerest, R. McAllister, “A Proposed Security Management Framework for the Global Information Security”, 6th Workshop on Enabling Technologies Infrastructure for Collaborative Enterprises (WET-ICE ’97), p200-206, 1997.

網路文獻

考試院 http://www.exam.gov.tw/

美國現行審計雙軌制 http://my.so-net.net.tw/joe21799/l/l3.htm

趨勢科技 http://tw.trendmicro.com/tw/home/enterprise/

經營決策論壇 http://www.gss.com.tw/tw/eispage/vol56/eispage5606.htm