致理技術學院

資 訊 管 理 系

專題期末報告書

資安監控告警整合平台

組長：連偉丞(19810123)
組員：陳弘億(19810120)
楊丞勛(19810125)
吳欣樺(19810139)
蔡依庭(19810142)

指導老師：林裕淇

中華民國 101 年 9 月

摘要

隨著時代的變遷、資訊的發達，，不論是在哪一個國家，攸關社會治安的問題都層出不窮，犯罪率都在不斷的上揚，因此必須提高自我防護的能力，以免危害到自己的權益與自身的安全。

在現今，人們非常重視資訊安全這個議題，因為這並不是單靠人力資源就能防範的，光是靠警衛或是保全的巡邏勘查是根本不夠的，因此人們就會藉由建置資訊安全監控系統，監視是否有發生異常的現象，讓人們可以迅速找出解決的方式來排除危害資訊安全的事件，以保障資產與人員安全。

資安監控系統能保障資產與人員的安全、有效降低企業資訊安全的風險，也能為企業節省對於在處理各種的資訊安全事件所要付出的人力資源，因此對人們來說，『如何建置出一個整合又有效的資安監控系統』是現今人們一直在研究的問題。

就因為如此，現在的資訊安全監控技術才會越來越發達，在生活週遭資訊安全監控技術的應用幾乎隨處可見。

關鍵詞：資訊安全、資安監控

目　錄

摘要 I

目　錄 II

表　目　錄 IV

圖　目　錄 V

第一章 序論 1

第一節　研究背景 1
第二節　研究動機 2
第三節　研究目的 2
第四節　研究範圍 2
第五節　操作性定義 3

第二章 文獻探討 4

第一節　資訊安全風險 4
一、　*資訊安全* *4*
二、　*資訊安全風險評鑑* *4*
三、　*定量與定性風險評鑑* *5*
第二節　風險評估方式 7
一、　*資訊風險評估* *7*
二、　*資訊風險評鑑方式* *8*
第三節　告警 14
一、　*告警系統* *14*

第三章 系統研究方法 15

第一節　研究流程 15
第二節　研究方法 16
第二節　SWOT 分析 17

第四章 預期研究成果 18

第一節　系統功能 18
第二節　系統特色 18
第三節　使用對象 19
第四節　使用環境 19
第五節　開發工具 19
第六節　系統平台架構 19

第五章研究結論與建議 21
第一節 結論 21
第二節 後續研究建議 21
第六章 分工執掌與進度表 22
第一節 分工職掌 22
第二節 進度表 23
文獻探討 24

表　目　錄

表 1、各個風險管理方法的優點與缺點.....7

表 2、資訊安全風險管理與 ISMS 過程對應.....11

表 3、風險識別級風險估計項目.....12

表 4、風險評鑑方法比較表.....13

表 5、資安監控告警整合平台 SWOT 分析 17

圖　目　錄

圖 1、資訊安全風險管理流程 11

第一章 序論

第一節 研究背景

在現今這個資訊發達的時代，隨著資訊科技的發展，改變了人們以往的生活模式，然而也因此出現了許多令人擔憂的資訊安全問題，網路威脅以驚人的速度成長，需要不同設備來監控與防堵，提高網路管理的複雜性。尤其伴隨著駭客攻擊途徑的多樣化，企業無不加強購置網路與資訊安全設備，以規避遭受攻擊的風險。

就因為現在出現了許多危害到資訊安全的問題，人們的隱私權已經不再受到完整的保護，雖然已有訂定出許多防護資訊流出、保護資訊安全的機制，但是防不勝防還是會有漏洞的發生，進而危害到整個資訊的安全。

現今不論是在哪一個國家，社會治安的問題都層出不窮，犯罪率都在不斷的爬升、上揚，所以如今只能人人自危，提高警備的能力，才能維護自身的權益、使自身的安全不受到危害。因此藉由建置資訊安全監控系統，辨識是否有外來的入侵、監視畫面是否有發生異常現象，那些會使自身的權益受損或是會危害到企業公司的資訊安全…等的事件，讓人們可以迅速找出解決的方式來排除危害資訊安全的事件，以保障資產與人員安全。

上述同樣的道理套用在公司、校園、居住的環境，這些地方都動輒就是上百、上千人到幾萬人，建地面積有的更是高達幾百坪、幾千坪甚至是到幾十萬坪...等都有，範圍是如此的廣闊，試問這是單單靠人力資源就能顧及到所有範圍的安全嗎？因此光靠警衛或是保全的巡邏勘查是根本不夠的，總是會有一些漏洞是用人力所無法顧及到的監控範圍，另外再加上因為警衛或是保全不太可能二十四小時一直盯著所有的監視畫面，所以這會導致警衛或是保全遺漏掉一些可能危害資訊安全的畫面，進而危害到人員的安全、造成資產的遺失與損毀。

因此為了要保障資產與人員的安全，就是必須要利用現在越來越進步的科技，來建置出一個可以保障資產與人員安全的資訊安全監控系統(簡稱：資安監控系統)，利用智能畫面辨識的科技，使系統能自動辨識出監視畫面中發生異常的現象，進而通知或是發出巨大聲響的警報聲來提醒資訊安全人員、警衛或是保全，另外可以針對必需要設置讀卡才能進入的特殊設備場合，而當讀卡發生異常時，進而通知資訊安全人員、警衛或是保全前往查看，提供即時有效的監控及因應措施。

除了上述功能外，並能加以統計每個月/季定期的中文事件報表，依照發生異常訊號的來源、地點、發生的事件…等，進行長期性資訊安全事件的統計與分析，並於每月統計資訊安全事件，產生通報及處理記錄的報表。來提升資訊安全人員的資訊安全知識及處理問題的能力，進而改善系統漏洞，或需要加以補強資訊安全的地點。

資安監控系統既能保障資產與人員的安全、有效降低企業資安風險，也能為企業節省資訊人員在處理繁雜、詭譎多變的資訊安全事件所要付出的人力資源，進而降低整體企業營運成本，協助企業達成永續經營之目標。資安監控系統，不僅是公司為防止安全漏洞、系統安全設備而進行的；對員工而言，更有保護員工本身的作用。

所以對人們來說，『如何建置出一個整合又有效的資安監控系統』就是現今社會上很重要的問題，也是大家非常關切的議題，也因為人們如此重視資訊安全，現在的資訊安全監控技術跟應用才會越來越普及。

第二節　研究動機

1. 動機一

   致理技術學院(簡稱：致理)的校園幅員不大，但是卻受限於保全人力有限，所以在校園裡面還是可能出現安全管理死角。

2. 動機二

   因保全人員不可能二十四小時盯著監視器畫面，會導致遺漏掉危害資訊安全的關鍵畫面。

3. 動機三

   像重要的機房庫房以及電梯等場所，雖然都有裝置監控系統，但都沒有發揮到最大的效果。

第三節　研究目的

1. 目的一

   運用大量的監控系統，輔助保全人員的巡查來消弭危害安全的因素。

2. 目的二

   提供一個整合的監控管理畫面及告警系統。

3. 目的三

   亟須提升安全監控的地方，並提供即時的處理

第四節　研究範圍

針對致理校園所有的人員，讓他們能在一套更完善的資安監控系統下放心的處在安全的校園裡快樂的學習。

第五節 操作性定義

資安非常重要，如何做好資訊安全防護措施是企業首要的任務。然而資安的系統很難監控，需要專業的能力。因此，我們提出一套很簡易的監控平台，可以有效的監控，並且以低成本、低技術門檻，當發現問題再轉給專業人員及時處理，有效控管資安問題發生後的空窗期，可以大大降低企業可能遭遇之資安風險。

本組專題已經完成系統的設計、關鍵技術測試、系統分析以及資料庫設計；後續將持續開發上述報告的系統功能，預期本系統可在暑假前完成，並逐步加強各項細部的功能測試。

第六節 章節結構

本論文的主要架構雨流程如下所示：

第一章 序論

本章敘述研究背景、目的、動機及範圍

第二章 文獻探討

本章文獻主要研究二部份，一是關於資訊安全風險第二部份是針對風險評估方式

第三章 系統研究方法

主要說明本系統的研究流程及方法，包括 SWOT 分析本系統，系統特色、系統功能、使用對象、使用環境。

第四章 預期研究成果

主要針對本系統功能、特色及使用對象、使用環境的詳細說明，及使用哪些開發工具及整體系統平台架構和雛型畫面的呈現

第五章 研究結論

本章是將本系統作個完整的結論，並討論預期研究效益及研究之限制

第六章 分工執掌及進度表

本章主要說明本組的詳細分工情形及完成進度的時間表。

第二章 文獻探討

第一節 資訊安全風險

一、 資訊安全

隨著電腦運用的普及與網際網路的蓬勃發展，已帶給人類急速而巨大的衝擊，也改變了人類生活模式。然而隨著資訊便利而來的則是令人擔憂的資訊安全問題，因此，我們必頇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。

資訊安全防護的種類：

一、 實體安全：包含硬體環境控制、火災、地震、風災、水災及盜竊人為破壞管理控制等。

二、 軟體安全：包含程式及系統安全防護防止駭客、入侵、病毒及人為破壞管理控制等。

三、 資料安全防護：包含防止重要資料受損遺失或外洩，讓資料安全防護做到滴水不漏。

影響資訊安全的因素：

一、 未經授權者(駭客)侵入電腦系統，竊取或更改資料甚至更動原系統設定。

二、 合法使用電腦人員有意或無心，造成資料的毀損、竊取或系統破壞。

三、 資料在傳輸中途被截取、竊窺或變更。

四、 電腦感染病毒與傳遞病毒。

二、 資訊安全風險評鑑

在資訊安全風險管理(樊國楨，2002)中對風險評鑑過程的定義為「透過資訊安全政策及資訊安全裝置之選擇，以保護資訊資產免於遭受經由人、設施、硬軟體、通訊網路、作業系統等之脆弱性而產生安全威脅的傷害」，本節簡單介紹評估風險階段中的三個步驟：規劃、資料收集和確定風險優先順序。

(1)規劃

正確的風險評估規劃是整個風險管理計畫成功的關鍵。未能適當地執行評估風險、確定評估風險階段的範圍或獲得對評估風險階段結果的確認，這會降低其他階段的有效性。

(2)資料收集

規劃後的下一步是從整個企業內的風險承擔者收集與風險有關的資訊。在實施政策支援階段中也將使用這些資訊。在資料收集步驟中收集的主要資料要素為

1、組織資產：對公司有價值的任何東西。

2、資產說明：各個資產、資產的價值以及所有權的簡短說明，有助於理解整個評估風險階段。

3、安全威脅：可能對資產造成負面影響的原因或事件，用資產的機密性、完整性或可用性的損失來表示。

4、漏洞：可用來影響資產的控制之弱點或缺陷。

5、當前控制環境：整個組織內的當前控制措施及其有效性的說明。

6、提議的控制措施：降低風險的初始策略。

(3)決定風險優先順序

在資料收集階段，收集的資訊將決定風險優先順序。決定優先順序本質上即具備主觀特性，畢竟流程本身是針對未來進行預測。評估風險的輸出結果將影響未來的資訊安全投資。風險評估者與風險承擔者的角色相當微妙。如果定義明確的角色和職責的定義與流程的透明化，對風險評估結果的接受與推動風險處理措施非常重要。評估風險在整個流程中也要求不同的風險承擔者負責相應的任務。

三、 定量與定性風險評鑑

在 CNS 17800 資訊技術-資訊安全管理系統規範（經濟部標準檢驗局，2002）中對風險評鑑的定義為「對資訊及資訊處理設施的威脅、衝擊及弱點及其發生可能性的評鑑」。風險分析可以是定性或定量的，在風險評估中，通常使用定性化的描述，比如高、中或者低。這是由於風險得不可預測性以及難以定量化的原因。定性化的方法可以區分風險的種類與發生頻率，但是這些呈現是敘述性質的，而不是可測量的。定性描述是風險測量的基礎，若是用數據可以表現資訊資產風險的發生率和重要性。因此本研究以定量評估資訊資產的風險，並以此做為建立風險評鑑的基本要素。

3-1、定量風險評鑑

微軟 The Security Risk Management Guide（Shon Harris，2003）的定量風險評估中，在風險評估與成本效益分析期間收集各個組成部分，以計算客觀數字值。例如復原成本、生產率損失成本、品牌名譽成本以及其他直接和間接商業價值來估計資產的真實價值。在計算資產暴露係數、控制成本以及在風險管理流程中鑑別出的其他價值時，應儘量有相同的客觀性，從財務方面分析或是參考顧問公司的統計報告是較客觀的資料。以下逐一說明資訊安全風險管理（樊國楨，2002）定量風險評鑑主要組成要素：

(1)賦予資產價值：資產的價值是安全風險管理的一個重要組成部分。企業通常會根據資產的價值來決定應該花多少成本來保護資產的安全。許多企業都維護一份資產價值（AV，Asset Value）清單。

(2) 評估每個風險潛在損失：定量分析過程參考兩個基本指標，事件發生的機率以及事件造成的損失

(3)執行威脅分析：執行威脅分析主要工作為計算出威脅發生的頻率，以合理方式預估威脅每年發生機率，做出這些估計相當困難，只有極少的實際資料可供使用。

(4)分析威脅整體潛在的損失：我們可以年度損失預期（ALE，Annualized Loss Expectancy）較完整評估威脅造成的潛在損失。

(5)風險處理：企業有兩種處理風險的基本策略，可以接受風險，也可以實施降低風險的控制措施。如果企業無法有效地降低風險符合成本效益的措施。也就是控制措施對營運持續的影響大於需要保護的資產價值，企業應該選擇接受該風險。風險接受的另一個方式是將風險轉移給第三方承擔，企業可與其他專業從事管理安全服務的公司簽訂委外合約，由承包廠商負責承擔對企業委外資產的部份或全部責任。

所謂控制措施，也稱為風險處理對策，是有系統、有規則控制風險的方法或技術。首先企業所以必須找出所有可能的控制措施，計算實施控制措施所需的成本，f 確定控制措施有關的其他成本，例如對使用者造成不便以及控制措施的持續維護成本，並評估各個控制措施降低風險的程度。這些資訊使企業可以提供對各個控制措施進行成本效益分析，以合理的成本最有效地降低企業的關鍵資產面臨的風險。

3-2、定義化風險評鑑

定性風險評鑑與定量風險評鑑的差別在於定性風險評鑑不用對資產鑑別出財務價值、預期損失和控制成本，而是以層級的概念取代。通常透過群體決策方式進行風險分析，成員可會能來自企業重要商業流程內各個部門人員，例如資訊安全專家、資訊技術經理、員工、資產負責人和使用者以及高階經理。在風險分析會議中，參與者確認資產並評估資產價值，接下來參與者嘗試指出各個資產可能面臨的威脅，然後描述這些威脅在將來可能利用的弱點。資訊安全專家和系統管理員通常會準備降低風險的控制措施，以便提供管理階層考慮並估計各個控制措施的成本，分析成本效益。

定性評估的流程類似於定量方法，差別在參與者不會用大量的時間來嘗試位資產評估計算精確的財務數字，而是討論出現實的風險的可能影響以及實施控制所需的成本。定性方法的優點是克服了精確計算的挑戰，並且通常在實施後幾週內即可顯示重要的結果，然而選擇定量方法必須依靠長時間的資料蒐集。定性方法的缺點是得出的數據可能是模糊的，由其對具財務或會計背景的企業管理者，可能會對在定性風險評鑑中確定的相對值感到不信任。

3-3、定性與定量風險評鑑比較

安全風險管理的定性方法和定量方法都具有各自的優臉與缺點。財務主導的情形下，企業會要求採用定量方法。小型組織或資源有限的組織可能會發現定性方法比較適合他們的需求。表 1 概括敘述定量與定性方法的優點缺點。

表 1、各個風險管理方法的優點與缺點

	定量風險評鑑	定性風險評鑑
優點	1. 依財務影響確定風險控管優先順序。 2. 依財務價值決定資產重要性。 3. 透過安全投資效益推動風險管理。 4. 隨著企業建立資料的歷史紀錄並獲得數據資料，時間越長其精確度越高。	1. 容易達成意見一致。 2. 毋須量化威脅頻率。 3. 無需確定資產的財務價值。 4. 便於不是安全或電腦專家的人員參與。
缺點	1. 風險的影響值以參與者的主觀意見為基礎。 2. 計算可能會非常複雜且耗時。 3. 流程要求財務專業。	1. 沒有成本效益分析，難以證明投資控制實施是否正確。 2. 主觀意識。

第二節　風險評估方式

一、　資訊風險評估

隨著資訊技術的蓬勃發展，資訊安全的重要性日趨重要，為了避免組織曝露於潛在的威脅而造成重大的損失,如何選擇適當的風險評鑑方法以完整的評估組織範圍內可能遭遇到的威脅及弱點就成為關鍵的議題之一。綜觀現行運作的風險評鑑方法，一般皆由下述四個步驟所組成：威脅的識別、脆弱性的識別、決定風險值及控制項目的建議（Syalim, Hori, & Sakurai, 2009），但由於風險評鑑的作法並沒有一定的標準流程可循，即便是標準 ISO/IEC 27001（2005）和 27002（2005）也沒有詳細的風險評鑑作業程序。因此，若是希望能夠遵循著這些標準進行風險的評估,則必須自行定義或是透過其他組織已經施行過的評估方法加以修正，以滿足組織內對於資訊安全風險評鑑的需求。目前已有許多組織各自發展不同的風險評鑑方法，這些風險評鑑方法中大致可分為定量和定性兩種，在定量評估方法中使用統計和數學相關工具表示風險;而定性的評估方式則是假設損失是無法以貨幣價值衡量，因此將衡量指標轉換成描述性的變數，然而，由於現在的資訊系統的架構較為複雜且涵蓋的領域較廣，相較於定性的評估方式，定量的風險計算方式較不適合目前的環境且使得評估的過程更為困難與複雜（Karabacak & Sogukpinar, 2005）。定量與定性的風險評鑑方式各有優缺點，因此也有學者提出兩者融合的風險評鑑方法，希望能降低執行過程中的複雜度並達到較精確公正的結果。本研究將比較五種現行的風險評鑑方法，並且透過方法步驟的說明分析各種評估方法的差異及其特性和優缺點,使組織在執行風險評鑑活動時，能依據組織的規模、架構及運作模式等特性，選擇合適的風險評鑑方法，期以用最小的成本對組織產生最大的貢獻。本研究組成架構如下：第二章將進行相關文獻的探討，詳細介紹目前現行的五種風險評鑑方法；第三章為此五個方法的比較；第四章為結論。

二、 資訊風險評鑑方式

各節中將針對 CORAS、OCTAVE、IS risk analysis based on a business model、ISRAM 及 ISO 27005 此五種目前現行風險評鑑方法進行詳細的介紹。

2-1、CORAS

CORAS 為 IST（Information SocietyTechnologies）下的開發項目之一，並於 2002 年由 Stolen et al.所提出，其公會是由 3 個商業公司 Intracom（Greece）, Solinet（Germany）and Telenor（Norway）；7 個研究機構 CTI （Greece），FORTH（Greece），IFE（Norway），NCT（Norway），NR（Norway），RAL（UK） and Sintef 及 1 個大學：QMUL（UK）所組成，其中 Telenor and Sintef 分別負責行政管理及科學方面的協調（denBraber, Dimitrakos, Gran, Stolen, & Aagedal,2002）。CORAS 是一個整合風險評鑑方法的平台，可支援危險可用的程序分析（Redmill,Chudleigh, & Catmur, 1999）、錯誤樹分析（Bertsche, 2008）、失敗模式和影響與關鍵性分析（Bouti & Ait Kadi, 1994）、馬爾可夫分析（Littlewood, 1975）以及 CRAMM（Atkinson, 2002） 5 種風險評鑑方法。主要是希望改善傳統風險評鑑的方法，將過程系統化，並達成三個目標：在適當的階層描述評估的目的、作為參與風險評鑑的利益相關者間溝通互動的媒介，及文件化風險評鑑的結果與這些結果所依據的假設（Stolenet al., 2002）。在 CORAS 中使用 UML 的方式來訂定不同風險評鑑方法之間的指標，並以 XML 作為工具發展的平台，同時基於 AS/NZS 4360 標準作為風險管理的程序及 RM-ODP 作為系統風險說明文件的架構。下面將介紹 CORAS 的七個實作步驟（DenBraber, Hogganvik, Lund, Stolen, & Vraalsen,2007）：

I. 介紹會議

風險評鑑的初期，客戶與分析人員雙方必須要能夠認同評估的目標與範圍、需要保護的資產等事項，因此在評估的初始需將所有相關人員集合，召開簡單的介紹會議，由客戶代表說明此次風險評鑑的目的和目標，而專業的分析人員來介紹 CORAS 分析方法並藉由會議討論設定整個風險評鑑的焦點目標和範圍，同時訂定後續會議的日期以及參與的人員。

II. 高階分析

本階段中將會對評估的目標做初步的分析，由分析人員說明於前次會議及組織所提供的文件中所獲得的資訊並進行資產辨識。在識別的過程中，組織內的相關人員提供資訊系統的 UML 圖，從圖中找出關鍵的部分，接著再依照關鍵部分的描述進行資產識別，同時也必須針對這些資產，初步找出最為重要的威脅和弱點並列出高階風險表，將有助於分析人員知道哪個部分最為緊急並予以更深入的分析，可更明確的定義整個評估的範圍。

III. 認可

認可是 CORAS 前置活動中的最後一個步驟，可藉由多次的會議甚至是電子郵件中進行，其主要的目標在於取得客戶對於目標的敍述、識別後的資產等的同意，並且需要定義出不希望發生的意外事件其發生的可能性及可能造成的衝擊程度，藉由此分析結果評估出每個資產風險的嚴重性及可接受的風險程度，並用風險矩陣表示。

IV. 風險辨識

在風險識別的部分 CORAS 使用結構化的腦力激盪，也就是針對分析的目標採用沙盤推演（Walk-through）的方式進行模擬每個可能發生的風險，結構化的腦力激盪用意在於採納多方背景的人員所提供的意見，使得分析結果更為深入與完整。經由此步驟將會產製出威脅場景圖。其中 CORAS 對於分析結果的文件化提供一個模組語言，以不同的符號作為代表。

V. 風險估計

當明確的在威脅場景圖中描述每個威脅的場景、不希望發生的意外事件、威脅和弱點後，必須要開始估計其發生的可能性和衝擊程度，這些估計值可作為未來該風險可否接受的依據。其中可能有多個威脅情境導致同一個不希望發生的意外事件發生，那麼此意外事件發生機率的計算就必須整合兩個威脅發生機率的範圍。

此步驟包含兩個部分，第一個是根據評估出來的機率和衝擊程度計算出風險值，並且經由其風險值的對應填入至風險矩陣中，評判出是否為可接受的風險，同時也識別出哪些風險是必須要進行處理，第二部分是將此矩陣展示給顧客端進行檢查，以確認是否符合現實的作業情形。

VI. 風險處理

風險評鑑的最後一個步驟即為風險處理，對於無法接受的風險擬訂風險處理辦法以降低降風險發生的機率或是減少衝擊的程度，並使用 CORAS 的模組圖形表示，然而風險處理辦法有時是耗費成本的，因此在風險處理計畫擬定之前必須考慮其實施的成本效益，以達到最大貢獻。

2-2、OCTAVE

OCTAVE 方法於 2003 年由 CERT 協調中心（CCERT/CC）提出（Alberts , Dorofee,Stevens & Woody, 2003; Alberts, Dorofee &INST, C. U. P. P. S. E., 2001），有別於傳統風險評鑑方法專就技術相關的資產為主的評估，OCTAVE 針對組織性的風險及專注於策略和實作相關的議題，並且考量組織面及技術面提供了一個有效的資訊安全風險評鑑方法，圖 5 為 OCTAVE 與其他風險評鑑方法的比較。OCTAVE 具有自我導向（Selfdirection）的特色，也就是說在組織中的成員對於安全策略的訂定都應負有責任，當組織應用 OCTAVE 風險評鑑方法，必須成立一個跨單位的分析團隊，無論是作業業務相關的人或是資訊技術部門的人員將會一起投入於組織安全議題的討論，提供更為完整的視角評估組織性的資訊安全風險，並結合作業風險、安全實作及技術層面這三個重要的構面。

I. 建立資產為基礎的威脅輪廓

在此階段中有兩個主要的功能,從組織中的各單位蒐集資訊及針對關鍵資產建置出威脅輪廓。其中又包含了四個子流程,在前三個子流程中分析團隊藉由高層管理部門、業務區域管理部門及員工收集組織中重要資產的資訊、安全需求、威脅及目前組織的優勢和弱點,第 4 個子流程則是選出 3~5 個關鍵資產相關的資產,並且針對這些關鍵資產製作威脅輪廓。

II. 識別基礎設施的弱點

在本階段中,分析團隊將會評估支援關鍵資產的系統重要元件所產生的技術弱點,此階段包含了兩個子流程。

1. 辨識關鍵元件——辨識出支援或是處理關鍵資產的系統重要元件,並且訂定出評估這些重要元件的方法。
2. 評估選定的組件——透過工具評估選定的元件,並且分析結果以完善關鍵資產的威脅輪廓。

III. 制定安全性策略和計畫

此階段最主要的目的即在於評估關鍵資產的風險並且制定出組織性的保護策略和風險降低計畫。在此階段中又包含了兩個子流程。

1. 執行風險分析——確立一套影響評估的標準以決定日後威脅對於關鍵資產所造成的影響程度(例如:高、中、低),所有活動的風險都應該評估影響的程度,而威脅發生的機率也可以加入 OCTAVE 方法中成為另一個評估的指標。
2. 開發保護策略——分析團隊制定組織性的保護策略及風險減低計畫,其著重於提升組織的安全實作並降低關鍵資產所產生的重大風險。OCTAVE 方法的執行是組織營運持續的一環,並且提供組織一個當下資訊安全風險的資訊,但若組織無法確實執行風險處理的計畫,那麼依舊會面臨同樣的威脅,組織可依據實際的情況或是有其他重大的事件時,定期的修正上次執行的結果,再一次識別新的風險及新風險與現行風險之間的關係。

2-3、ISO/IEC 27005

ISO 27005 標準(2008)是 ISO/IEC27000 系列標準的一部分,它提供了組織對於資訊安全風險管理的指導綱要,並且支援了 ISO/IEC 27001 在 ISMS 的特殊需求,以 PDCA 的模式不斷的修正改進,然而,在此標準中並沒有提供任何具體資訊安全風險管理的方法,組織可依據 ISMS 的範圍、風險管理的全景或是產業別定義風險管理的方法。下面將詳細介紹各個活動:

I. 建立全景

在建立全景的過程中,必須要建立起組織中所有與資訊安全風險管理相關的資訊,包含設定資訊安全風險管理的基本準則、定義範圍與邊界及建立運作資訊安全風險管理適切的組織,並且為營運持續計畫及事故回應計畫做準備。其中基本準則又包括風險評鑑準則、衝擊準則及風險接受準則。

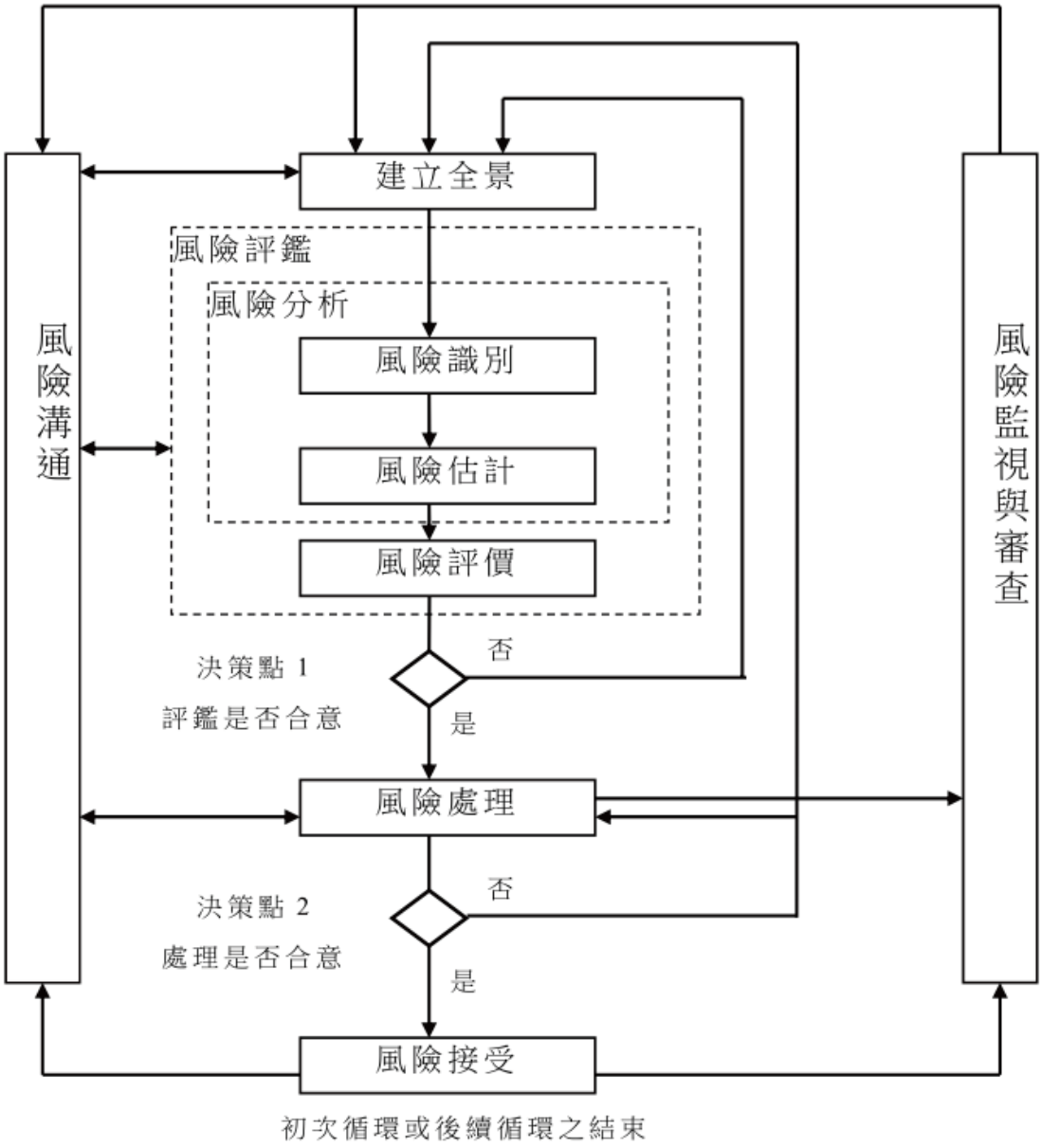


圖 1、資訊安全風險管理流程

表 2、資訊安全風險管理與 ISMS 過程對應

ISMS 過程	資訊安全風險管理過程
規劃（Plan）	建立全景 風險評鑑 發展風險處理計畫 風險接受
執行（Do）	風險處理計畫之實作
檢查（Check）	持續監視與審查風險
行動（Act）	維持與改善資訊安全風險管理過程

II. 風險評鑑

風險評鑑通常需要決定資訊資產的價值、識別出資產所面臨的威脅及潛在的弱點及目前既有的控制措施等，並且通常於兩個（或是更多）循環中進行，藉由每個循環針對潛在高風險做更深度考量，因此在此風險評鑑步驟中應包括風險分析及風險評價，而在風險分析中又可分細分為風險識別及風險估計兩部分，風險識別及風險估計所包含的項目整理如表。

III. 資訊安全風險處理

風險處理可有 4 種可行的方式，風險降低，透過適當的控制措施將風險降低，使重新評鑑後的剩餘風險為可接受的等級；風險保留，假設風險等級已符合風險接受準則，則可不需做額外的控制措施；風險避免，若所評鑑的風險過高或是風險處理的實作其成本超過利益時，可從既有活動中退出或是變更運作的環境；風險轉移，可藉由投保等涉及外部團體的決策將風險轉移分擔，但通常此做法可能會帶來新的風險或改變既有的風險，因此尚需做額外的風險處理。組織可基於風險評鑑的結果、實作的預期成本或是預期利益進行選擇適當風險處理。

IV. 資訊安全風險接受

在風險處理計畫中應明確的描述如何處理所評鑑出的風險及處理過後的殘餘風險，在某些情況中，即便是處理過後的殘餘風險仍可能無法滿足風險接受準則，例如伴隨著風險所帶來的利益是非常具有吸引力，或是降低風險的成本太高，而必須接受風險，此種情況下可能需要修改不合宜的風險接受水準，或是接受不符合風險接受水準的風險並且註解所衡量的理由。

V. 資訊安全風險溝通

為避免相關者對風險的認知的不同導致資訊安全危害的發生，必須透過決策者與其他相關者之間的雙向溝通，瞭解決策的基礎及特定活動需求的理由。

VI. 資訊安全風險監視與審查

風險並非是靜態，因此必須持續的監視威脅、脆弱性、風險發生的可能性或後果的變化，另外也需持續監看風險管理範圍內的新資產或是價值修改的資產所產生的威脅、脆弱性和可能性等，確保組織內的資訊安全風險管理過程及相關活動於現今環境中保持為適切的。

表 3、風險識別級風險估計項目

風險識別	識別資產	在風險評鑑的範圍與邊界內識別出對組織有價值的資產，並以適當的等級劃分資產的重要性及識別資產擁有者。
	識別威脅	由事故審查、資產擁有者、使用者與其他來源，包括外部威脅目錄所取得之資訊進行威脅的識別。
	既有控制措施之識別	控制措施若運作不如預期，可能導致脆弱性，因此必須檢查以確保控制措施的正確運行。

	識別脆弱性	脆弱性的存在並不會導致風險，需有相對應的威脅利用之，因此若為此類脆弱性，可不需實作控制措施，但仍應識別並且監視其變化。
	識別後果	某一威脅利用某項或多項脆弱性所造成暫時性或是永久性的損害或後果。
風險評估	風險估計方法	組織可依據需求選擇定量、定性或是兩者混合的風險評估方式。
	後果評鑑	評鑑來自可能或是確實存在的資訊安全事故所導致的營運衝擊及資訊安全遭破壞的後果。
	事故可能性評鑑	考量威脅發生的頻率及弱點可能被利用的容易程度，以定性或是定量的估計方法評估每一個情境和衝擊發生的可能性。
	風險估計等級	透過定性或是定量的方法計算對風險發生的可能性及衝擊後果。

2-4、評鑑方法比較

承上節所介紹的三種現行的風險評鑑方法，於本節中將針對此三種方法進行比較，並且彙整於表。

由比較可知，各個評估方法皆由 5 個以上不等的步驟或是子流程組成，然而在整個風險評鑑的過程中，必須要完成某些前置作業才能進行真正風險分析的部分。

表 4、風險評鑑方法比較表

方法 / 項目	CORAS	OCTAVE	ISO 27005
方法步驟數	5 個步驟	3 個步驟 8 個子流程	6 個步驟
定量／定性方法	定量／定性	定性	定量／定性
評估出法點	資產	資產	資產
風險分析針對單一／群組資產	單一	單一	單一
計算容易程度	簡單	簡單	N/A
風險計算精確度	較不精確	較不精確	N/A
發生機率及衝擊結果	相對	相對	N/A

第三節　告警

一、　告警系統

告警系統（early warning system）是指所有在自然界中部署的生物性或技術性系統，透過個體或群體發布一場未來可能發生危險的消息。其目的是為了讓接收消息者可預備即將發生的危險，並作出相應的行動，以減輕或避開其帶來的傷害。

主要分為生物告警系統與人工告警系統這二種。

1-1 生物告警系統

- ✓ 警戒態 （例如：警戒色）
- ✓ 敬畏
- ✓ 疼痛

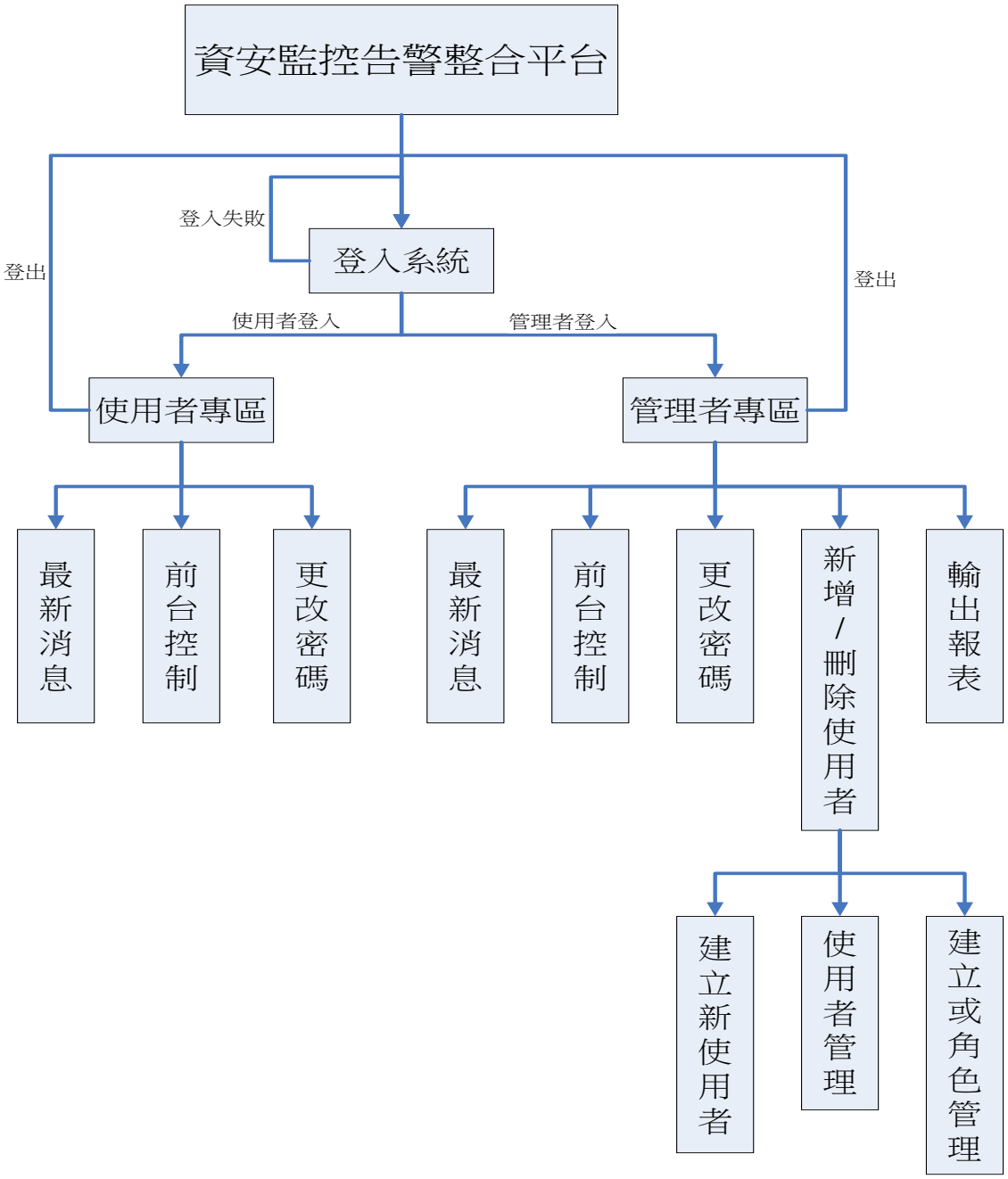
1-2 人工告警系統

- ✓ Alberta Emergency Public Warning System
- ✓ 自動列車警報裝置
- ✓ 兒童綁票預警系統
- ✓ 水壩安全系統
- ✓ 地震預警系統
- ✓ 緊急警報系統 (美國)
- ✓ 火警系統
- ✓ 強風預警
- ✓ 地面迫近警告系統
- ✓ 印度洋海嘯預警系統
- ✓ 國際預警計劃
- ✓ 全國瞬時警報系統
- ✓ 車道偏離警示
- ✓ 北方預警系統
- ✓ 空中防撞系統
- ✓ 海嘯預警系統

第三章 系統研究方法

第一節 研究流程

針對我們所作的系統做需求分析並規劃架構，進而蒐集所需要的資料與系統的環境建置，經由系統分析討論資料庫所需要欄位並建置，與進行資料轉檔的動作，即可設計系統功能與版面，建置完成後進行系統整合與測詴維護，上線後即可使用，如圖所示。



第二節　研究方法

本研究針對校園安全與使用者期望系統達到何種效能二大方面，所設計出來的問卷，如下：

一、校園安全

1、您對於目前學校對其及周邊環境管理是否滿意？
2、您對於目前校園中的保全機制是否滿意？
3、您對於目前發生校園安全事件時的通報速度是否滿意？
4、您對於目前發生校園安全事件時的處理方式是否滿意？
5、您對於目前發生校園安全事件時解決事件的速度是否滿意？
6、您對於目前校內外人員進出校園的管制是否滿意？
7、您認為校園中的治安死角是否有受到適當的監控？
8、您認為目前校園中的防災措施或設備是否完善？
9、您對於目前校園中的防災機制是否滿意？
10、您對於目前學校中的宿舍門禁(人員進出)管制是否滿意？
11、您對於目前校園夜晚的燈光明亮程度是否滿意？
12、您對於目前校園夜晚保全的巡邏機制是否滿意？

二、期望校園安全程度

1、您是否期望學校在校園內的各個角落設置監視設備？
2、您是否期望學校在校園內較陰暗的角落設置照明設備？
3、您是否期望學校多舉辦校園安全宣導？
4、您是否期望學校在校園內多設置道路燈？
5、您是否期望學校對於校內外人員進出校園的人員管制更嚴謹？
6、您是否期望校園夜晚保全的巡邏機制更完善？
7、您是否期望校園安全事件發生時的通報速度更迅速？
8、您是否期望學校在校園內多設置防災措施或設備？
9、您是否期望校園安全事件發生時的處理方式或機制更完善？

第一節 SWOT 分析

表 5 資安監控告警整合平台 SWOT 分析

● 改善校園安全 ● 提供更完善的系統功能 ● 節省人力資源 **S** 優勢	● 卡片的系統無法支援多種作業系統 **W** 劣勢
O 機會 ● 不用 24 小時盯著監視畫面 ● 讓校園成為最安全的地方 ● 可以省下請保全的費用	**T** 威脅 ● 會造成其他的系統無法使用

第四章 預期研究成果

第一節　系統功能

系統功能有五項，其說明如下：

1. 消滅死角：

能消除校園中的死角，讓每個角落都能在保護範圍內。

2. 節約經費：

節省人力資源的花費。

3. 查詢紀錄：

可查詢先前的系統影像紀錄。

4. 告警機制：

加入告警功能當有狀況發生時可以立即通知，使保全有效率的處理危機。

5. 提高成效：

單靠警衛巡邏校園成效不彰、效率低，人力有限的情況下形同浪費時間，無法照顧周全，使用監控系統可節省時間，更有效的監視校園每個角落。

第二節　系統特色

系統特色有二項，其說明如下：

1. 加入告警系統：

如有發生會危害資訊安全的因數出現時,將會以告警系統告知警衛要查看監視畫面，以免錯過重要的過程。

2. 突顯出關鍵時刻：

監視系統平時會維持一般狀態，如有危害因數出現時，會將特別顯示出監視畫面，並將此段時間的影片另存起來，也方便以後的找尋。

3. 不必擔心警衛漏掉事件的發生：

因為本系統不用讓警衛２４小時一直盯著螢幕,如果有危害到資訊安全的事件發生，本系統的告警設備就會通知警衛。

4. 可以讓學校師生在安全的校園中學習：

雖然致理校園不大,但要讓學校師生有個安全的環境,所以本系統能讓學校的師生有個安全的地方學習與教學。

5. 連接告警設備：

本系統連接告警設備，如有事件發生，告警設備會亮紅燈並響起聲響，告知警衛有事件發生，讓警衛做緊急處理。

第三節　使用對象

系統的使用對象主要是以圖資中心為主軸

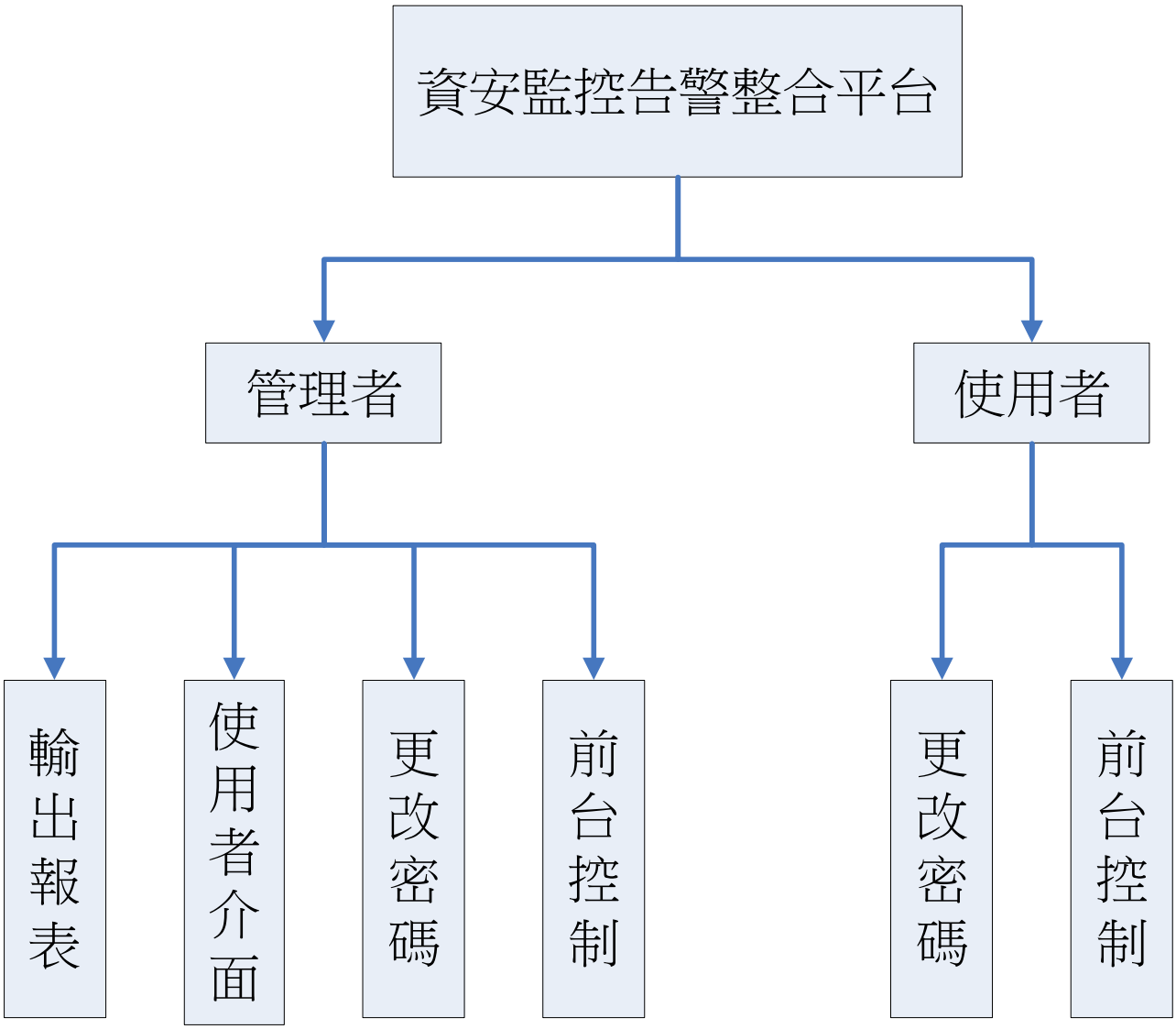
第四節　使用環境

可以在Windows XP、Windows Vista、Windows 7的環境中使用此系統功能。

第五節　開發工具

1. Microsoft Office 2003
   －製作書面文件的工作
2. Microsoft Office 2007
   －製作書面文件的工作
3. Microsoft Office Visio 2003
   －製作系統各種結構圖
4. Microsoft SQL Server 2008
   －建置系統資料庫
5. Microsoft Visual Studio 2008
   －製作系統程式
6. Adobe Illustrator CS3
   －系統美工設計
7. Adobe Photoshop CS3
   －系統美工設計
8. Adobe Dreamweaver CS3
   －網站排版、動態網頁製作、編輯網頁原始碼、網享管理
9. Adobe Flash CS3 Professional
   －製作系統動畫
10. Java Script、Ajax、 ASP.NET 3.5、LINQ、C#
    －使用以上技術進行系統設計與程式編碼
11. CSS
    －利用此技術進行系統文字與樣式設計
12. Internet Information Services(IIS) 、.net framework
    －利用此軟體架設伺服器環境
13. Microsoft Windows XP Professional Version2002 Service Pack3
    －使用此軟體進行系統建置。

第六節　系統平台架構


資安監控告警整合平台
管理者
使用者
輸出報表
使用者介面
更改密碼
前台控制
更改密碼
前台控制

第五章研究結論與建議

第一節 結論

對於學校而言，建設資訊安全監控管理系統暨告警管理系統不只可以減少人力資源的付出、還可以改善校園的治安死角問題，防範事件的發生，讓全校的師生可以在安全的環境下學習、教學，另外再配合告警設備，發生事件時，能使警衛適時做出緊急的危機處理，有效率的解決事件。

對學生而言，建設資訊安全監控管理系統暨告警管理系統不只可以使學生們在校園走動時，不必擔心走到校園的死角、在校園學習時，不必擔心自身的安全、財產的損毀，能放心的在校園學習，使學生能更有效率的學習。

對家長而言，建設資訊安全監控管理系統暨告警管理系統可以使家長們放心讓自己的孩子在校園裡學習，不必擔心事件的發生，就算事件發生時，學校也會馬上做出緊急的處理。

第二節 後續研究建議

本系統相關研究範圍只限學校，希望後續能研究較大的範圍，例如社區、政府、國家。

因為現在是個學生，個人經費非常稀少，又加上專業知識沒有非常的豐富，所以只能以學校作為基礎，如果學校的資訊安全監控管理系統暨告警管理系統能獲取獎金時，就會持續的向外延續發展。

第六章 分工執掌與進度表

第一節　分工職掌

本研究的組員有陳弘億、連偉丞、楊丞勛、吳欣樺、蔡依庭，本研究的分工執掌表，如下表所示：

工作主題	負責人員
初步規劃	
擬定專案主題	陳弘億、連偉丞、楊丞勛、吳欣樺、蔡依庭
資料搜集	連偉丞、楊丞勛、吳欣樺、蔡依庭
初步規劃系統架構	陳弘億、連偉丞、楊丞勛、吳欣樺、蔡依庭
系統分析	
系統需求分析	陳弘億、連偉丞、楊丞勛、吳欣樺、蔡依庭
系統應用分析	陳弘億、連偉丞、楊丞勛、吳欣樺、蔡依庭
系統架構分析	陳弘億、連偉丞、楊丞勛、吳欣樺、蔡依庭
系統功能分析	陳弘億、連偉丞、楊丞勛、吳欣樺、蔡依庭
資料庫分析	陳弘億、連偉丞、楊丞勛、吳欣樺、蔡依庭
設計與建置	
伺服器架設	楊丞勛、吳欣樺
資料庫架設	楊丞勛、吳欣樺
資料庫匯入	陳弘億、連偉丞、楊丞勛、吳欣樺、蔡依庭
資料表統整	陳弘億、連偉丞、楊丞勛、吳欣樺、蔡依庭
網頁版面設計	連偉丞、蔡依庭
網頁版面配置	連偉丞、蔡依庭
網頁程式設計	陳弘億
系統程式設計	陳弘億
維護	
系統測試、檢查	陳弘億、連偉丞、楊丞勛、吳欣樺、蔡依庭
PowerPoint 製作	連偉丞、蔡依庭
撰寫文件	楊丞勛、吳欣樺

第二節　進度表

本研究的工作進度時間從 2012 年 3 月初至 2012 年 11 月底，本研究詳細工作進度表，如下圖所示：

識別碼	工作名稱	開始	完成	期間	2012 三月 四月 五月 六月 七月 八月 九月 十月 十一月
1	系統規劃	2012/3/5	2012/4/4	4.6w	
2	系統分析	2012/4/5	2012/5/1	3.8w	
3	系統設計	2012/4/20	2012/8/20	17.4w	
4	系統實作	2012/5/25	2012/10/24	21.8w	
5	測試維護	2012/10/10	2012/11/29	7.4w	

文獻探討

Joel Snyder 李慶發譯(2004) “利用安全資訊管理工具整治資安洪流”(資安人雜誌} 14 38-48
路克(2004) “資安人的救星 SEM ” (資安人雜誌) 13 94-97
陳俊彥(2004) “以量化軟體度量指標支援 CMMI 模式的導入與評鑑” 碩博士論文 國立台灣科技大學資訊管理系
曾宇瑞(2000)”網路安全縱深防禦體制之研究” 碩博士論文 國立中央大學資訊管理學系
劉永禮(2001)”以 BS7799 資訊安全管理規範建構組織資訊安全風險管理模式之研究” 碩士論文 元智大學工業工程與管理學系
經濟部標準檢驗局(2002) “CNS 17800 資訊技術-資訊安全系統管理規範”
樊國楨(2002) “資通安全專輯之五:資訊安全風險管理引導” 行政院國家科學委員會科學技術資料中心
Microsoft Corporation (2004) The Security Risk Management Guide, from http://www.microsoft..com/technet/security/guidance/secrisk/default.mspx.
Nessus(2004)”Nessus Open Source Vulnerability Scanner Project” from http://www.nes-sus.org.
OpenNMS(2004)” OpenNMS Home” from http://wiki.opennms.org/tiki-index.php
OSSIM(2004)”Open Source Security Information Management ” from http://www.ossim.net
Snort(2004)”The Open Source Network Intrusion Detection System”” from http://www.snort.org
Shon Harris(2003)”Security Management Practices” CISSP All-in-One Exam Guide,ch3,Mcgraw-Hill