# 部隊導入 ISMS 對幕僚成效的架構研究
# The Study on the Architecture of Staff Effectiveness after Introducing the ISMS to the Troops

盧瑞山
德明財經科技大學
資訊科技系
助理教授

黃佐元
德明財經科技大學
資訊管理系
研究生

rslu2000@gmail.coma0927576249@gmail.com

**摘　要**

本研究使用「企業架構塑模語言 ArchiMate」，規劃一個讓幕僚能遵循的 ISMS (Information Security Management System)導向。現今幕僚對於 ISMS 的導入，尚有完全不懂其概念的。然而隨著網路的快速發展，以及智慧型手機的普及，使得 ISMS 的重要性日趨嚴重，走向網路雲端應用的道路，已是時勢所趨；尤其是在無線網路的環境下，相關資訊的取得，更為容易。

本研究之貢獻乃是以「企業架構塑模語言 ArchiMate」建構 ISMS 利用電腦及網路通信技術，顯示出 ISMS 的重要性，來驗證企業架構建構的正確性。藉由企業架構對 ISMS 之策略規劃(Strategic Planning)，使得目標不失焦；同時，提升了資訊安全的重要性。

關鍵詞：企業架構方法、企業架構塑模語言、ISMS、資訊安全。

## 一、緒論

現今網際網路的發展一日千里，資訊充斥著日常生活之中無所不在，生活上、工作時、甚至於睡覺時也受到資訊的洗腦。本研究借用了企業架構方法(Enterprise Architecture Method)，配合資訊安全管理系統(Information Security Management System, ISMS)，研究幕僚們的資訊安全(Information Security)觀念成效，可準確推導出幕僚層級架構中受資訊安全的影響深淺。然而在傳統的觀念中，進行分析研究時，僅只局限於個人工作的內容及涉及的資訊安全層級，往往無法做到幕僚對於資訊安全的基本觀念，也無法取得幕僚當前面對工作的情緒及壓力。透過本研究的問卷調查及口頭訪問，從事資訊業務方面的幕僚，能於網路的作業環境下，注意到資訊安全的防護，使 ISMS 的導入，能達到一定的層級影響，但對非資訊業務人員，能提升相對的資訊安全觀念，仍是本研究之目的。

本研究規劃以企業架構(Enterprise Architecture)為基礎，可以清楚地了解幕僚對於資訊安全的不同認知及面向，因此能夠配合 ISMS 之實際需求，適當地做出問題解決(Problem Solving)的對應方案。

本研究使用「企業架構塑模語言 ArchiMate」，規劃一個讓幕僚能遵循的 ISMS (Information Security Management System)導向。現今幕僚對於 ISMS 的導入，尚有完全不懂其概念的。然而隨著網路的快速發展，以及智慧型手機的普及，使得 ISMS 的重要性日趨嚴重，走向網路雲端應用的道路，已是時勢所趨；尤其是在無線網路的環境下，相關資訊的取得，更為容易。

本研究之貢獻乃是以「企業架構塑模語言 ArchiMate」建構 ISMS，利用電腦及網路通信技術，顯示出 ISMS 的重要性，來驗證企業架構建構的正確性。藉由企業架構對 ISMS 之策略規劃(Strategic Planning)，使得目標不失焦；同時，提升了資訊安全的重要性。在塑模過程中，定義轉換機制，並以 ArchiMate 完成之；同時，實際以專案本文為例，加以闡述與驗證。

## 二、文獻探討與相關技術

### (一) ISO 27001 資訊安全管理系統(Information Security Management System, ISMS)

ISO 27001 國際標準提供規範以建立、實施、監控、操作、審查、維護及改善資訊安全管理系統而準備，然而 ISMS 被採用必須是組織的策略性決策[1]。部隊中導入 ISMS 的過程，往往也因為些政策及法令稍有不同，而做些許修改及遵循方向。

[2]所謂「資訊安全管理系統(Information Security Management System)」，是整體管理系統的一部分，繼而根據企業風險管理的辦法制定，用來建立、操作、執行、監控、審查、充新檢討、維護及改進資訊安全。顯而易見的，[1] ISO 27001 是「資訊安全管理系統(Information Security Management System)」標準，且遵循 PDCA 模式(Plan 規劃-Do 執行-Check 檢查-Act 行動)循環進行有效的風險管理。

ISO 27001 涵蓋了 11 個管理領域，分別為安全政策、資訊安全的組織、資產管理、人力資源安全、實體與環境安全、通訊與作業管理、存取控制、資訊系統獲取(開發)及維護、資訊安全事故管理、營運持續管理、遵循性。其 11 個管理領域下又可細分為 39 個控制目標暨 133 個控制要點。此一數據顯示了 ISO27001 分工細項如此的完整，各項領域、目標及要點，均能使其更有效率的遵循

ISO27001 規範標準，實行資訊安全管理。

本研究規劃以企業架構(Enterprise Architecture)為基礎，可以清楚地了解幕僚對於資訊安全的不同認知及面向，因此能夠配合 ISMS 之實際需求，適當地做出問題解決(Problem Solving)的對應方案。

(二)分析層級法(Analytic Hierarchy Process, AHP)

[3] 分析層級法主要應用於決策問題上，根據 Saaty 經驗，認知於下列 13 類問題中也可以代入應用：規劃(Planning)、替代方案的產生(Generating a Set of Alternatives)、決定優先順序(Setting Priorities)、選擇最佳方案或政策(Chooseing a Best Policy Alternative)、資源分配(Allocating Resources)、決定需求(Determining Requirements)、預測結果(Predicting Outcomes)、系統設計(Designing System)、績效評量(Measuring Performance)、確保系統穩定(Ensuring System Stability)、最佳化(Optimization)、衝突的解決(Resolving Conflict)、風險評估(Risk Assessment)。

本研究將利用 AHP 的分析方法，找出幕僚對於資訊安全的不同認知及面向，配合 ISMS 之實際需求，適當地做出問題解決的對應方案。

**三、ISMS 導入對其幕僚成效塑模**

本研究之貢獻乃是以「企業架構塑模語言 ArchiMate」建構 ISMS 利用電腦及網路通信技術，顯示出 ISMS 的重要性，來驗證企業架構建構的正確性。藉由企業架構對 ISMS 之策略規劃(Strategic Planning)，使得目標不失焦；同時，提升了資訊安全的重要性。

動機架構(Motivation Architecture)

利害關係人(Stakeholder)

- 利害關係人視圖(Stakeholder View)係由「部隊導入 ISMS 對幕僚成效的架構研究」的利害關係人觀點，建構出相對的主要利害關係人(Key Stakeholder)視圖，如圖 1 所示動機架構(Motivation Architecture)

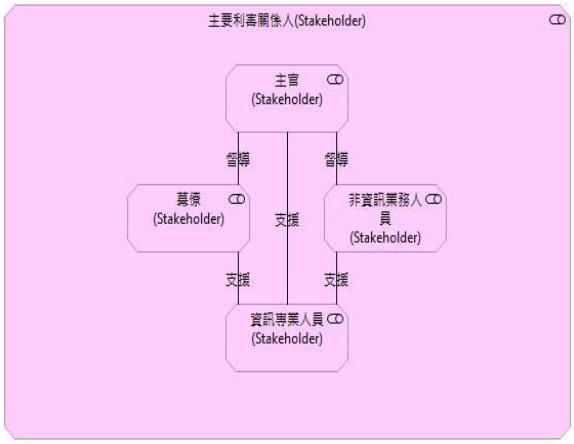


圖 1.主要利害關係人視圖

- 利害關係人關注視圖(Stakeholder Concern View)係由「部隊導入 ISMS 對幕僚成效的架構研究」的利害關係人關注觀點，建構所有主要利害關係人之主要關注視圖(Key Concern of Key Stakeholder View)，如圖 2-1、2-2、2-3、2-4 所示。

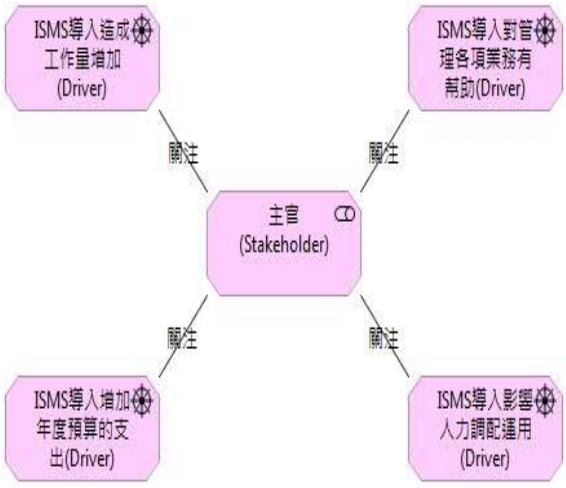


圖 2-1 主要利害關係人(主官)之主要關注視圖

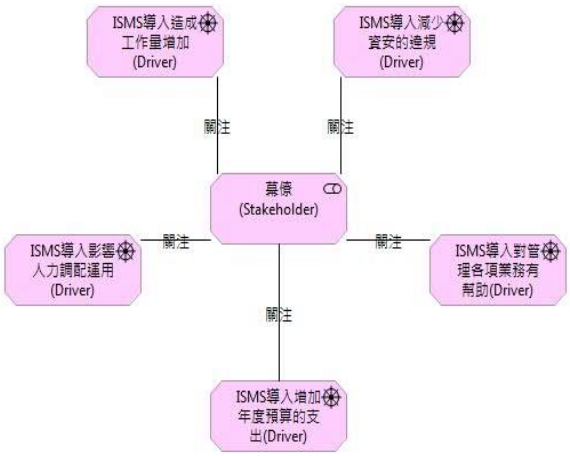


圖 2-2 主要利害關係人(幕僚)之主要關注視圖

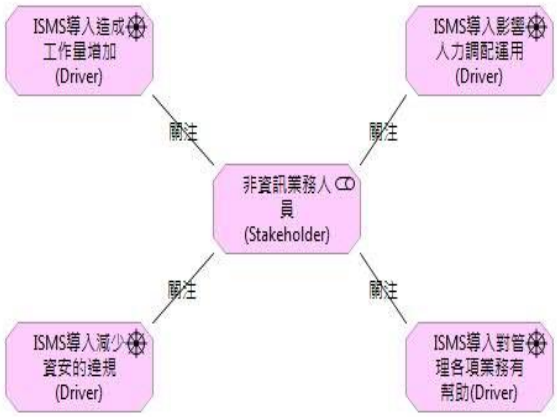


圖 2-3 主要利害關係人(非資訊業務人員)之主要關注視圖

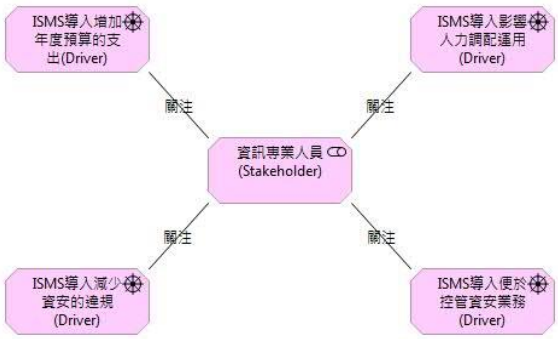


圖 2-4 主要利害關係人(資訊專業人員)之主要關注視圖

- 組織視圖(Organization View)係由「部隊導入 ISMS 對幕僚成效的架構研究」的組織觀點，建構達成子目標(Sub-goal)與總目標(Super-goal)的主要組織視圖(Key Organization View)，如圖 3 所示。

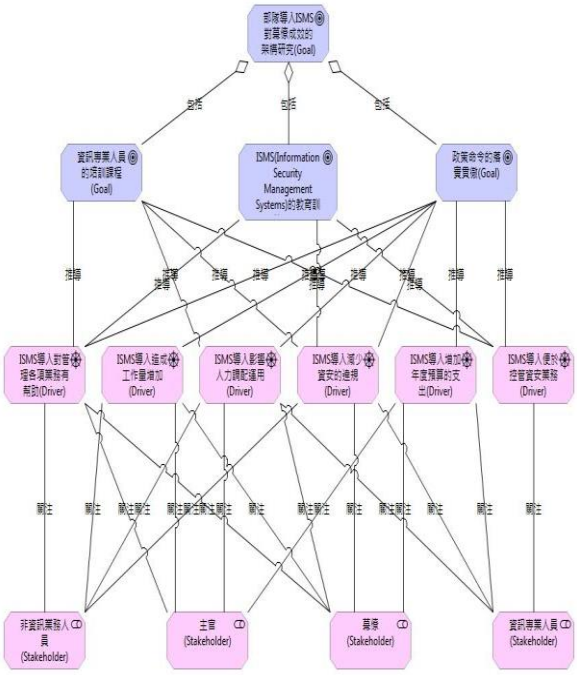


圖 3.主要組織視圖

## 四、研究心得

本研究之貢獻乃是以「企業架構塑模語言ArchiMate」建構ISMS利用電腦及網路通信技術，顯示出ISMS的重要性，並加以了解幕僚對於資訊安全的不同認知及面向，期待能夠配合ISMS之實際需求，適當地做出問題解決(Problem Solving)的對應方案。

現今網際網路的發展一日千里，資訊充斥著日常生活之中無所不在，生活上、工作時、甚至於睡覺時也受到資訊的洗腦。本研究借用了企業架構方法(Enterprise Architecture Method)，配合資訊安全管理系統(Information Security Management System, ISMS)，研究幕僚們的資訊安全(Information Security)觀念成效，適時適地的找出協尋相關資訊安全的觀念並且深植於人心。

研究中利用了「企業架構塑模語言ArchiMate」繪製相關的利害關係人及其關注點，使其後續研究者對其架構一目了然，以及後續研究方向更加明確暨有系統的步驟化。

## 參考文獻


[1] 劉魯青，「國軍電腦鑑識中心導入資訊安全管理系統之關鍵成功因素」，世新大學資訊管理研究所碩士論文，2014年。

[2] 郭建麟，探討組織如何落實ISO27001-以網路入侵衍生危安事件為例，教育部TANet2008研討會，台北市，2000年。

[3] Saaty, T.L., “The Analytic Hierarchy Process”, New York: McGrew-Hill. 1980.