評估資訊安全風險管理計畫與能力時的重要考慮因素

Key Consideration When Evaluating ISRM Programs and Capabilities

作者: John P. Pironti, CISA,CISM, CGEIT, CRISC,CISSP, ISSAP, ISSMP,

is president of IP Architects LLC. He has designed and implemented enterprisewide electronic business solutions, information security and risk management strategy and programs, enterprise resiliency capabilities, and threat and vulnerability management solutions for key global customers in a range of industries, including financial services, insurance, energy, government, hospitality, aerospace, health care, pharmaceuticals, media and entertainment, and IT. Pironti frequently provides briefings and acts as a trusted advisor to senior leaders of numerous organizations on information security and risk management and compliance topics and is also a member of a number of technical advisory boards for technology and services firms.

譯者: 張碩毅, 中正大學會計與資訊科技學系教授

資訊安全和風險管理(Information Security and Risk Management, ISRM)在傳統上對於組織和企業領導來而言常被認為是一種成功的屏障以及不利的力量，而不是一種有利益和有利的能力。首先在使用時會考量到安全，在使用時會感到恐懼，同時不確定和懷疑等因素引起組織對於安全的需求，這些都是典型對於科技的傳統觀念。然而一個成熟的 ISRM 計畫和能力，在組織中是可以扮演一個推動者的角色，許多情況下也被視為在企業營運中的一種策略優勢。

近來 ISRM 計畫和能力已經被許多組織視為一種不可或缺的元素，因為他們發現到他們的資料以及資訊基礎建設的價值。這些能力近來已快速的成熟並且遠遠超過基本的需求，因此這些能力需要被管理和發展，以確保可以與商業上的期望與活動彼此相符合。審核員對於這些計畫與能力的準確和持續評鑑對於組織的成功、組織的員工還有了解組織的利益與挑戰是相當重要的。

評估方法

一般來說有許多的方法和做法可以用來評估組織 ISRM 的計畫與能力，包括：問卷、訪談、歷史紀錄與證據的審查、績效評鑑、能力成熟度模型或是在能力上是否有符合業界公認業界領導的功能庫。這些方法都分別提供一個指標給評估者與企業，但並沒有提供一個概括的看法給相關的單位。通常最好的方式是結合並同時使用這些能力，以確保組織擁有完整且準確的看法。

通常最有效、最全面且廣泛被認可的方法是使用客製化的能力成熟度模型(CMM)(表1)來評估ISRM的計畫和能力。雖然原先CMM是為了軟體產業而開發，但CMM也可以非常容易的應用於評估ISRM的計畫和能力。藉由增加一個遞增量表於傳統的CMM獨立層級中，對於管理階層與利益相關者常提出要求的，評估人員便可以提供相關的細節供他們參考。遞增量表應代表三個不同的部分：1~3代表在初始狀態下能力的成熟度，4~6代表已穩定的成熟度，7~9代表進展至下一個層級的成熟度。

表1：ISRM 能力成熟度模型

成熟等級	一般描述
5	理想、最佳化、已與企業相校準
4	已管理、已控制、可預測
3	主動預防、已定義、已實施
2	可再生、對事故之反應、盡最大努力
1	初始、未定義、現有狀態
0	未辨識、有意願

增加範圍	增加之描述
.7-.9	進展
.4-.6	已穩定
.1-.3	初始

目前主要評估ISRM計畫和能力的方法是利用功能庫並以組織功能評估和治理模型審查為基礎。對於

ISRM 的來說，適用的功能目錄有兩種：資訊安全計畫(表 2)和資訊風險管理計畫(表 3)假設組織有實施全面的計畫和能力，那該功能庫應清楚的包含組織該有的服務和能力。

表 2：資訊安全計畫功能目錄

首席資訊安全長	威脅與脆弱性評鑑	脆弱性管理與事件通報	適法性與法規	策略
政策、程序、原則與標準	企業永續性	教育與溝通	治理	結構與設計
技術與能力評估與認證	關鍵績效分析與有效性	資訊安全督導委員會		

表 3：資訊風險管理計畫功能目錄

首席風險長	資訊安全	實體安全	遵循性	隱私
財務風險	市場與策略風險	企業營運風險	風險方法、實作與標準	關鍵績效分析與有效性
文化意識、訓練和溝通	策略與治理	風險督導委員會		

一旦組織確定要使用功能庫時，評估組織為 ISRM 計畫與能力所開發的策略是相當重要的，以確保這些策略是與企業的期望與要求相符合的。

評估 ISRM 策略

考核組織是否有針對 ISRM 的計畫與相關的能力，開發與實施一個正式的策略，並且將其文件化以及得到組織的批准是相當重要的。一個全面性的策略至少會包含以下的要素：

- 對於企業環境的理解與認知
- 將使用治理的模型
- 將組織風險的概況和風險胃納相互校準
- 預算的考慮和資源的計畫
- 機制與測量
- 溝通與認知的計畫

策略是評估中一個重要的元件。在與企業的要求與期望相互校準時需要小心去考慮和執行。

企業校準與認可

對於 ISRM 計畫的成功，ISRM 能力與企業要求和活動的相互校準是不可或缺的。對於企業的利害關係者與領導階層分別作詢問和訪談，了解他們對於 ISRM 組織與其功能的看法和互動是目前在業界中對於考核企業校準的主要做法。企業以及其他有關的各方，如：外部的利益相關者和控制督導小組(如果適用的話)，不僅要了解他們所提供的能力，同時也要能獲得提供知識與服務的價值。企業或是有關的各方對於他們所提供或是可用的能力與服務無法察覺甚至感到不悅時，便可透過上述類似的指標得知 ISRM 缺乏與企業間相互校準。

在評估 ISRM 與企業相互校準時也可以考量 ISRM 計畫與能力對於協助提升企業營運與財務狀況的能力。當現有或是潛在的顧客與夥伴決定開始或增加與組織之間的業務關係時，ISRM 可以做為一個有價值的資產用以增加他們的信心。一個對於這個能力已存在的關鍵指標，可以在組織的銷售與行銷的方法中找到。包括對於 ISRM 概念和能力的訊息傳遞或是活動交流，都可以顯現對這些能力的信心並了解他們潛在的策略價值。

企業接受 ISRM 的一個關鍵指標是 ISRM 計畫與能力是被包含在產品與服務開發的週期裡面。有些組織經常在發展活動的初期就利用 ISRM 能力，他們發現 ISRM 能力可以有效的協助組織降低成本(一般是 30%)並提升效率。這是因為組織在設計的階段就整合 ISRM 的概念與要求，而不是在發展活動的末期，當組織發現需要時才進行整合，導致再造與調整上需要花費更多的成本。

另外一個企業接受 ISRM 的關鍵指標是例外措施要求申請的數量以及被 ISRM 組織

核准的數量。當新政策提出時，經常可以看到例外要求突然增加或是高於平常的數量。這些例外的要求若是基於需要更多時間來遵循政策的話，便不會像其他的要求是因為企業嘗試逃避或避免遵循這些政策來的重要。比起請求的數量而言，更重要的是這些請求被核准的數量。從大量的要求與核准可以看出組織目前的措施未與企業的能力或需求相符合。

治理

在功能上欲達到最好的效率和能力，ISRM 計畫和能力需要建置一項)治理的計畫和治理的架構並且發揮它們的功能。治理的模型必須包含功能庫中組織目前有涵蓋的功能以及每一個功能的作業計畫。這個治理計畫應包含對於人員與資源的需求、預算追蹤、成熟與穩定計畫、和企業策略的目標與需求相對應並能佐證與企業營運上的一致。這個治理模型也必須對每一個功能明確的定義出最小和最佳的營運需求，同時顯示了追蹤活動的證據來說明 ISRM 計劃與企業經營的領導力對計畫和服務的健康與績效以及計畫所展現的效能具備了準確且有意義的洞察力。

ISRM 計畫的報告結構是 ISRM 計畫能否在組織中有效率且成功運作的關鍵。在過去，許多 ISRM 計畫被建立在技術組織的一部分且向首席資訊長報告。對初始效能的發揮，這可以是一種有效的架構，但常常對一個成熟的組織而言並不是一種理想或適當的架構。ISRM 應以保護資訊和資訊基礎建設為目標，當然這其中包含著技術但也不應該僅限於關注在技術層面上。當檢視 ISRM 能力時，應注重的地方是他們可能會有利益上的衝突，這些衝突可能來自於 ISRM 的管理階層與技術層面的人員的互動，因為這些技術管理階層可能無法了解或支持這些能力和需求的全貌。

一旦企業治理架構被評估完成後，下一個重要的評估範疇將是 ISRM 計畫用以辨識、評估和報告主要的風險和企業隨時都應該要關注的事項時所使用的"威脅、脆弱性和風險評鑑方法與實務"。

威脅、脆弱性和風險評鑑方法

在 ISRM 計畫和效能中被用於評估威脅、脆弱性和風險的方法與實務必須具備一致性、重複性以及使參與人員容易了解等特性。這些方法與實作應包含下列的要素:

- 與企業流程相對應
- 資產盤點與分類
- 威脅與脆弱性分析方法
- 風險評估方法
- 情報的蒐集、處理與報告的能力

組織內，威脅與脆弱性分析和分險管理活動兩者之間務必加以明顯的區隔。資訊安全專業人員經常因為在認定技術層面影響的過程中，沒有對企業營運層面的影響去做適當的了解或結合，而誤將威脅與脆弱性之特徵視為風險之特徵。在大部分的案例中，資訊安全計畫和執行計畫的相關專業人員對與企業經營策略、企業流程與效能的重要性排名，以及對商業情報做適當的辨識和風險排序等方面有關的企業經營領導力並不具備完整的洞察力。然而，他們在威脅方面，包括：機率和經營衝擊洞察所提供的資訊，對風險評鑑和排名的準確性和價值是很重要的。

當評估 ISRM 能力時，向組織和重要的利益相關者確認與表達風險的流程是一項必須關注的重要領域。風險評鑑、排序和報告的效能必須運用且遵循一種結構性的，一致性的和可重複性的方法。一個組織的 ISRM 能力可對該組織在企業風險管理(Enterprise Risk Management, ERM)效能方面提供有價值的見解，而且通常更能促進企業在資訊風險

評鑑和排序方面的執行績效。ERM 通常缺乏相關的成熟度與知識來將資訊風險適當地納入到組織的評鑑、排序和報告。總體的來說，ISRM 計畫和其能力必須與 ERM 組織和組織的利益相關者緊密的一起運作，藉此以了解他們的需求並配合他們的活動來協助他們。

營運模式

在組織內 ISRM 的計畫與能力是獨特的，因為他對於組織有預防事件發生與對發生之事故作適當反應的責任。評估這些能力在這兩種模式下是否有效率的運作是非常重要的。一般來說成熟的計畫通常會比較專注在預防事件發生的能力上，如：威脅與脆弱性的分析、脆弱性管理、訓練與認知、訊息活動以及控制活動的成熟與提升。針對事故做反應的計畫則偏向於執行遵循性活動以及對發生的威脅與事件做反應。若組織是專注在針對事故做出反應的能力時，那就表示組織是不成熟的同時也沒有專注於 ISRM 的計畫與能力上。

在評估組織的 ISRM 計畫與能力時，找出外部的規範以及組織希望 ISRM 去保護的事物或需要去解決的問題是非常重要的。通常我們可以利用兩種不同的操作模式。第一種是主要反應和以技術為導向的方法。第一種模式經常發現於當組織對於 IRSM 的能力比較不成熟以及/或組織無法藉由 ISRM 獲得商業價值。在這種情況下，組織通常對 ISRM 的計畫並沒有適當的投入資金，組織也只有在資安事件對組織產生負面的衝擊時才會利用 ISRM 作為組織因應資安事件的能力。

第二種作業模式是以資料和企業流程為導向的方法，這種方法通常是較為成熟的組織的做法。在這個模式下，組織認為 ISRM 是可以提供企業價值的，同時將充分利用這些能力為企業的活動創造收入，組織也會將這個指導綱要和功能視為組織成功的助力，而不是阻擋企業成功的絆腳石。在這個模式下，科技仍然與 ISRM 能力相關的活動作結合，但是在這些活動中可能比較專注在企業的流程和企業的資料。在大多數的情況中，科技成為一個支援的角色並使控制的機制得以被執行，而不是 ISRM 活動中的焦點。

這兩種作業模式都可以協助組織達成他們所需要遵循的目標(內部與外部的目標，如果適用的話)。而這兩種模式的遵循度都應基於組織的遵循性方法進行評估和檢查。

遵循的方法

遵循性已快速的成為任何一個組織 ISRM 計畫或能力不可缺少的一塊。許多外部的規範，是組織必須去遵循並使其符合組織的遵循目標，如：法律、業界標準和內部政策等。因此必須針對組織在遵循上的方法做出相關的考量。在理想的狀況下，遵循性應被視為 ISRM 能力的起點而不是 ISRM 能力的終點。但很不幸的，許多組織採取了一項稱作"安全性遵循"的方法，這個方法不僅代表著不成熟更使組織在面臨到大量企業衝擊的威脅時反而變得脆弱，同時也可能使組織面臨各種無法應付的風險。

使用"安全性遵循"的方法，常是組織對於現在的 ISRM 能力感到不信任或是挫折的指標。遵循性的要求提供組織一個衡量的方式，使他們相信他們可以判斷出組織對於 ISRM 能力的需求。再次的強調，遵循性應視為 ISRM 計畫、能力和要求的起點而不是終點。

另外一個有效和成熟的 ISRM 計畫與能力的關鍵屬性是組織是否有能力在日常企業活動中用最小的努力達到內部與外部在遵循性上的要求與目標。遵循性不應被視為一個獨立的計劃或行動，應視為組織在企業活動整合上的要素。在許多情況下，組織為證明

他們有在進行遵循性的活動，組織會開始執行一些零星的動作來達到遵循性的要求或製作出可能不是組織日常企業營運中所需要的報告，使得遵循性活動淪為組織僅僅在製作或是報導這些資料而已。

遵循性的策略同時也是該遵循性相關活動的一部分。對組織當下的企業情況或活動，完全的達到遵循性可能是不理想且無法實現的。在這種情況下，組織有對應的策略與路線圖可以先強調並集中於最關鍵的遵循性要求是相當重要的，進而再解決其他與企業衝擊有關的要求以及在合理的時間內組織欲達成這些要求時所需要努力的程度。

隨著組織欲達到遵循性的要求所制訂出策略，訓練與認知的活動有效性也需要被加以評估和考量。訓練和認知對於文化變革的概念是相當重要的，同時對於組織成功的達成日常營運的目標也是相當重要的。

訓練和認知

訓練與認知的活動對於任何一個 ISRM 計畫或是 ISRM 能力的成功都是相當重要的。訓練與認知不應侷限在定期的去舉辦相關的教育訓練活動或是將教育訓練的平台僅侷限在一種平台上(電子化、講課、廣播等)。在評估訓練與認知的活動時，決定組織是否有找出利益相關者和組織成員的學習型態以及是否有開發出符合的訓練教材是非常重要的。

訓練與認知活動應該要讓參與者在學習與溝通上可以有互動和對等的機會。可能的參與者擁有表達問題、表示關注或是/以及提出意見的能力是非常重要的。電子化平台如：組織的內部網站可以提供一些常見的問題(FAQs)供參考，部落格文章、社群媒體功能並有直接和 ISRM 的管理階層與執行人員聯繫的選項，藉此展示組織與組織成員一同努力的承諾而不是用權威或是獨斷的方式。

一種評估 ISRM 計畫的訓練與認知能力的方法是隨機的從組織中挑選員工並詢問他們對於該計畫的了解和印象。這些被選中的個別的員工應要可以代表組織的眾多部門，包括個別的參與者、經理和組織領導人，同時他們需要被詢問同樣的問題。藉由從詢問不同組別所蒐集而來的資料做關聯分析，我們可以從可能的組織成員和文件中了解到他們對 ISRM 計畫與能力的認知情形。

資料的關連分析以及向企業的領導者和利益相關人報導等相關的活動通常和機制與測量有關。組織的領導階層通常以機制與測量來判斷商業價值與 ISRM 計畫和能力的有效性。

機制與測量

機制與測量協助專業人員評估企業單位與功能的能力。ISRM 計畫與能力近來已經如同獨立的企業部門單位和企業的功能並且根深蒂固於組織當中，不再僅僅是一種計畫方案中的一個元素。這些計畫和能力必須要對組織成員以及它們所在的組織展現出在商業上的價值。有關於 ISRM 能力的機制與測量應要顯示出他們個別所提供的功能和服務所能帶給組織的價值，以及這些功能在能力上的效率和成熟度。

對於一個組織在機制與測量能力上的關鍵績效指標是他們利用那些方法與實作來進行開發和運作。在建立資料收集、分析、報導和”門檻規範”等元素的機制與測量方法時，此方法須具備連續和可重複的性質。如果機制與測量的方法一直變動(非典型大概在一年以下)，可能會使這些被蒐集的資料以及使用這些資料相關報告的準確性下降與代表性下降。

每一個重要的機制與測量(那就是多元機制與測量的組合或是對組織成功很重要的機制與測量)同時應包含相關行動或活動的門檻。

機制與測量中若沒有一個進入的門檻便無法針對正面或負面的含意義提供相關的見解。這個門檻可以像一個通知一樣的簡單或者複雜的一旦觸動便會引起一連串行動與活動的觸發器。我們預期的讀者會被要求採取行動或是被行動所影響，達到這些門檻的讀者應可以容易的了解企業的需求或是這些行動的正當性，同時這些讀者便可認同組織被賦予的價值。

當評估這些機制的能力時，報導會因具備較高的價值和重要性所以需要密切的去重複檢視。相關的報導是機制與測量活動的進行所累積而成的，同時也將會是最後呈現給組織的訊息。報導需考慮的是讀者對此事的認知和相關性。在大多數的情況下，ISRM 計畫可以提供相關的數據給有關的各方人員，包括：領導高層、企業流程的擁有者以及技術和操作的人員。機制與測量的報導在呈現和格式以及包含的資料應適合所有的讀者。我們可以藉由訪談不同類型的資料接受利益關係人，衡量他們對於這份報導所能感受到的價值，並且找出如何在商業的活動使用這一份報告。如果這些報告是用於企業的活動或是單純因為報告的接受者認為必須執行這個動作以達到領導者的期望而去檢視這個報表，那麼這些報告需要重新的審查以確保可以提供一致的商業價值給接受方。

操作方法 V.S. 諮詢方法

ISRM 執行計畫可以含括操作方面的項目做為它們的核心效能，或者他們可以在建議的和諮商的能力範圍內來操作。如果含括操作方面的項目，那麼對在這組織內所預設的操作責任歸屬和它們與操作效能間之差異必須加以清楚的定義。除了上述之定義以外，同時也必須對有關操作的有效性、需求、情報和偶發事件之反應等資訊分享方面的文件必須建立相關處理和流程。

如果相關的諮詢方法僅僅屬於建議性的和諮商性的，那麼對組織所提供之服務必須建立清楚的文件，就像服務要能成功，努力的程度和與業務上的互動是必要的一樣。如果一項 ISRM 執行計畫只有指導綱要和建議而不包含操作責任歸屬，那麼對組織而言，此項執行計畫只是看起來具有正面意義而已，因為這將使防止組織在執行操作效能和 ISRM 執行計畫兩者間之不協調的能力受到限制。

符合業界標準

有很多的方法可以展現 ISRM 計畫的能力讓有關的各方或第三方的檢驗者了解，但是一般來說最有效的方法是展現 ISRM 計畫在能力上符合業界的標準以及/或法規。業界目前的做法傾向於採用業界的標準，或者業界的標準至少被接受為組織在基本能力與競爭力的展現。當評估 ISRM 能力時，重要的是要找出組織欲遵循的標準以及組織為什麼要去遵循這套標準。如果組織在遵循的目的純粹只是要滿足遵循性指導綱要，那組織可能不了解或無法感受到標準背後隱含的優點。如果組織將標準視為指導綱要進而塑造出標準所要求的服務和能力，那麼這可能是不成熟組織的一個跡象，因為組織只在乎外在的觀點而不是要為組織自己的需求發展出一套最佳的實作方法。

對於 ISRM 的計畫或者能力而言符合業界標準是有很多益處的。欲了解組織在標準的遵循上是否有效率，其中一個指標是組織現有的能力是否有對應到標準中所敘述的條款，同時組織也認為這些條款對於企業而言是有利且有用的。這個方法可以展現出組織對於其遵循的標準有深入的了解，並且感受到自行發展這些能力的需要。ISRM 的組織和能力可能藉由某些業界中重要的標準來展示其對於標準遵循的程度，包括：

- ISO 27001-27008 and 31000
- US National Institute for Science and

Technology (NIST) 800 series of standards
- Payment Card Industry Data Security Standard (PCI DSS)
- COBIT

結論

近來許多組織在快速的找出 ISRM 計畫和能力的商業價值與衝擊。ISRM 計畫已經不再僅次於組織的其他能力，而且 ISRM 計畫是需要定期的被評估與評價以確保 ISRM 計畫持續的符合組織的需要和需求。ISRM 的有效性評估可以使組織及其領導階層了解 ISRM 的能力如何與他們的期望以及業界公認的做法相符合，並讓他們了解到需要進行那些投資以符合他們的需要和需求。

References and Further Reading

1 *Nolan, Richard L.; "Stages of Growth Model for IT Organizations," Harvard Business Review, 1973*
2 *Humphrey, Watts; Managing the Software Process, Addison Wesley, USA, 1989*
3 *Pironti, John; "Developing an Information Security and Risk Management Strategy," ISACA Journal, vol. 2, 2010*
4 *Pironti, John; "Key Elements of an Information Risk Management Program," Information Systems Control Journal, vol. 2, 2008*
5 *Pironti, John; "Key Elements of an Information Security Program," Information Systems Control Journal, vol. 1, 2005*