摘譯文章

ISACA®
Trust in, and value from, information systems

電腦稽核

VOLUME 2, 2008
摘譯文章第4期

Information Systems Control Journal

目　　錄

(以上文章皆摘譯自 Information Systems Control Journal, Volume 2, 2008)

資訊技術治理與業務/資訊技術配合之研究
(Practices in IT Governance and Business/IT Alignment)

作者：Steven De Haes, Ph.D., and Wim Van Grembergen, Ph.D.
譯者：楊期荔, CISA, BS7799LA,ISACA Taiwan Chapter CISA Coodinator

現在很多的組織中，資訊技術(IT)已經在支援、維運和開發業務的過程中，具有決定性的影響。因資訊技術的普遍使用，故資訊技術治理也受到日益重視，希望經由領導、組織架構及程序與資訊技術治理的配合一致，最終可以保證組織策略與目標的達成。

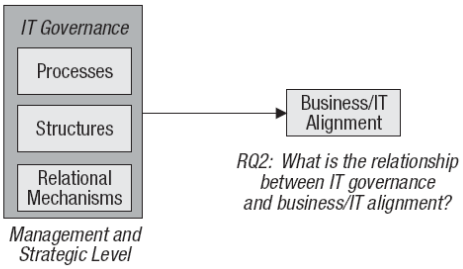
今天，資訊技術治理在很多組織的陳議是高的，因而，高階的資訊技術治理模型也持續在發展中。但是，組織發展一個高階的資訊技術治理模型，並不暗示該治理模型已實際上運作在組織中。治理模型的發展是第一步，其次才是實施，以及維持在運作的水準。一旦選擇並且實施一個具體的資訊技術治理模型，它應該使資訊技術能夠支援並且延續業務目標，換句話說，就是確保資訊技術要能配合業務上的需要。這篇文章內容的核心，就是資訊技術治理的實施與其後影響的挑戰，以及資訊技術與業務目標的配合。

以比利時為例，安特衛普大學管理學院的研究人員曾研究：中型與大型的金融服務組織怎樣實施資訊技術治理以達到業務目標和資訊技術之間的更好配合?這問題可以更進一步分解為(見**圖 1**)：

- **組織如何實施資訊技術治理? (How are organizations implementing IT governance?)**一個高階資訊技術治理模型的開發不暗示該治理實際上已運作在組織中。治理可以使用多種架構、程序和機制。架構包括結構的(正式的)、程序和機制，但它能連結或橫向連繫生意和資訊技術管理(決策)功能嗎?

圖1 – 研究問題(Research Questions)

RQ1: 組織如何導入 IT 治理?



*比利時中型企業至大型金融服務組織

- **何為資訊技術治理和業務/資訊技術配合間的關係?(What is the relationship between IT governance and business/IT alignment?)**如前所言，資訊技術治理的目標是取得業務和資訊技術之間更好的配合。最終的議題是，導入程序、架構和相關的機制，使業務/資訊技術配合成為可能。辨識出每個提供特別或複雜的多重目標的應用程序、架構和相關機制是一項具挑戰但卻又是重要的事。不過，把資訊技術治理架構分成更小的成份，並且分別解決每個問題，這卻與解決整體問題常常不竟相同。整體的處理方法，能讓我們瞭解資訊技術治理，其複雜和動態的本質，係因由互相依存的子系統(程序、架構和相關機制)的一堆元件組成強而有力的整體。

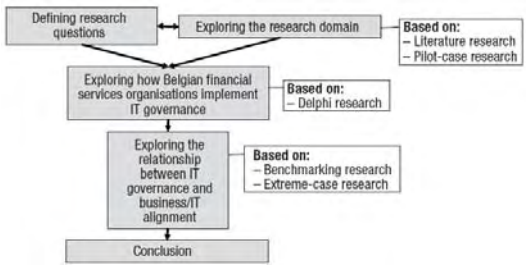
我們知道研究如果只聚焦在一個部門和地理地區可能限制研究結論的應用；另一方面，我們相信很多結論很可能可以適用於其他環境。

研究方法學和方式
(Research Methodology and Approach)

研究策略應是基於多種研究方法的彙整：文獻研究，試行案例研究，德而非法研究，標竿研究和極端案例研究等。這樣的多角度的方式能獲得更豐富及對現實有更多了解。如**圖 2** 中所示，可以並行或依序使用不同的研究方法。

研究過程應係從探索研究範疇及確定問題開始，透過一些詳細的文獻探討，了解業務/資訊技術配合的方面開始。聚焦點應在定義且精煉待研究的問題，並且發現初始的架構、程序和相關機制，組織能調控對資訊技術治理的導入。為了補充資訊技術治理實務的初始表，本研究的試行案例使用在 KBC, Vanbreda, Sidmar-Arcelor ,CM, AGF 和 Huntsman。

圖2 – 研究流程(Research Process)



在探索比利時金融服務組織正怎樣實現資訊技術治理的過程中，一組專家採用德爾非研究方法學，以獲得共識。透過不同回合的審視，由一個 22 位顧問和資深資訊技術和業務專業人員組成的專家小組，提供關於資訊技術治理實務有效性的判斷 (0 為無效，5 為非常有效)，並評斷該實務是否易於實施(0 為不易，5 為非常容易)。回答者也被問到，前 10 名重要的資訊技術治理實務，哪個是，在他們看來，具決定性的要素或者是最佳的資訊技術治理所需的最小底線。

下列研究步驟有助探索資訊技術治理實施時和業務/資訊技術配合之間的關係。此階段從建立一個源於 10 個比利時金融服務組織的樣本的比利時金融服務業業務/資訊技術配合的基準開始，在每個組織中，5 到 10 個資深業務和資訊技術經理，要求他們完成一張量測業務/資訊技術配合成熟度(從 0 到 5)的問卷，依據這些基準，挑選出 4 個極端分數的組織來(由業務/資訊技術配合度上，取兩個高績效和兩個低績效者)，通過會議討論(極端案例研究會)，來決定一般使用的資訊技術治理實務的成熟規模(測量值基於來自 0(不存在)與 5(樂觀)的排序)，透過對收集到的數據進行交叉分析，可有助於解釋一些組織能得到較高的業務/資訊技術配合分數，而其他組織卻不行的原因。

研究的結果
(Results of the Research)

從試行案例研究中，我們找出採用資訊技術治理的不同的驅動因素。最重要的一項係為符合美國沙賓法案的要求，該法案相當程度的影響現行資訊技術的控制環境。另外的重要驅動因素，來自於規模經濟的追求、企業合併和預算壓力，上述原因導致專案預算較過去更少，如何把剩下的預算指派到能為業務增加價值的專案和活動上，形成新的挑戰。最後，一些試行案例公司提及資訊技術治理專案是最能將已有的機制，加以正式化或架構化的方法。

組織怎樣實現資訊技術治理?
(How Are Organizations Implementing IT Governance?) 德爾非研究顯示，根據一組 22 位各業別的專家意見，比利時金融服務組織能調控大部份的架構、程序和機制，以實現資訊技術治理支持業務/資訊技術配合的議題。這研究揭示包含 33 項資訊技術治理實務的名單，皆是由策略性和執行/資深

業務和資訊技術管理層所認定的事項。應當注意的是，這研究內，名單中已剔除操作面上不能徹底做到的狀況。這些實務列示在**圖 3** 的前兩個欄位， 其中 Sx 為架構，Px 是過程和 Rx 為相關的機制。

研究發現，根據專家意見，某些指明的實務較另一些有效且容易實現(見**圖 3** 右方欄位)。5 項比利時金融服務業較有效運用的實務為：資訊技術監督委員會、資訊長向執行長/運營長報告、資訊長位列執行委員會一員、資訊技術預算控制及報告以及(專案)組合管理。所有這些實務也都被視為相對容易實現。而最沒有效運作的實務為資訊技術治理保證和自評、工作輪調和 COSO 企業風險管理事項等。某一些實務被視為有效，但不是容易實現，最好的例子就是利潤管理、報導及移轉定價。

這裡作者要提到的另一個有趣的現象是，有關的(CobiT)的控制目標的項目。這框架在文獻和此領域內得到許多注意，然而關於是否易於實施，其得分僅高於一般平均。在這研究過程中多數實務為 CobiT 框架是不可缺少的。這些的包括於難以實現的實務項目?在 CobiT 裡的實務，其內容的高水準且具抽象理念，明顯影響 P6 中的易於實施項目的結果，如同**圖 3** 中表明的。

圖 3 - IT 治理架構、程序與相關機制的驗證名單

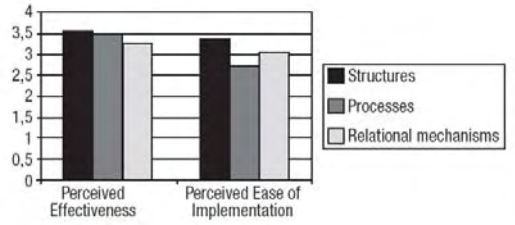
		有效性 (1-5 分)	易於實施 (1-5 分)
S1	資訊策略委員會在董事會的層級	3,67	3,40
S2	資訊專業度在董事會的層級	3,14	2,18
S3	(電腦)稽核委員會在董事會的層級	3,22	3,40
S4	CIO 在執行委員會	4,38	3,56
S5	資訊長向執行長/運營長報告	4,50	4,21
S6	IT 監督委員會(由高階管理層級做 IT 投資評估/優先權)	4,69	3,35
S7	IT 治理職務/主管	2,93	3,11
S8	安全/遵循/風險 官	3,28	4,06
S9	IT 專案指導委員會	4,03	4,01
S10	IT 安全指導委員會	2,82	3,61
S11	架構指導委員會	3,04	3,14
S12	治理整合/結合角色與責任中的任務	3,18	2,63
P1	策略資訊系統規畫	3,82	2,82
P2	IT 績效量測(如:IT 平衡計分卡)	3,97	2,76
P3	(專案)組合管理[包含企業案例、資訊經濟、投資報酬率及投資回收率	4,13	2,67
P4	收費安排-總擁有成本(如:活動成本)	3,28	2,40
P5	服務等級協定	3,47	3,13
P6	COBIT IT 治理	3,36	2,42
P7	IT 治理保證和自評	2,79	2,54
P8	專案治理/管理 方法論	4,10	2,94
P9	IT 預算控制和報告	4,13	4,00
P10	效益管理和報告	2,85	2,36
P11	COSO 企業風險管理事項	2,39	2,04
R1	工作輪調	2,35	2,36
R2	主機代管	2,79	3,01
R3	交叉訓練	2,76	2,82
R4	知識管理(如:IT 治理)	3,24	2,68
R5	企業/IT 帳號管理	3,79	3,36
R6	高階主管人員提供好的例子	3,88	2,81
R7	在業務與 IT 高階管理中非正式會議	3,79	3,88
R8	IT 領導力	3,89	2,82

R9	企業內部溝通來解決問題	3,43	3,69
R10	IT 治理意識活動	2,83	3,14
*由 0-5 評分,0 表示無效;5 表示非常有效			

一項有趣的發現是,很多資訊技術治理定義上都強調資訊技術治理是董事會方面的首要責任,而當這些結果顯示能證明的機制(如：有資訊技術背景專家位列董事會和資訊技術策略委員會),相對言，就評量有效性而言,看來並不如想像的明顯。這事實可能解釋為,如要使董事會成員具更多資訊技術素養,是不容易達成的目標,這可以由問卷中將此一項目列在最不易達成的第 2 位得到確認。這研究的結果引出的深一曾的問題是,金融服務組織董事會介入此一實務上到底有多少。

如果計算有效與易於實施得分的平均數，包括架構、程序和相關機制(見**圖 4**),，看起來架構和程序通常是同樣有效，不過，看起來 IT 治理架構較 IT 治理程序容易實施些，雖然在許多狀況下，他們具相當關聯性。

圖4 – 有效性與易於實施的平均分數



*由0-5評分,0表示無效;5表示非常有效

一個好例子是 IT 監督委員會，它是建立組合管理程序的一項決定性的要素,但是也被認定為比整個組合管理程序容易實施得多。相關機制也顯示出較 IT 治理程序容易實施，或許，一些相關機制能有非正式屬性(例如 R7 業務與 IT 執行/資深管理者的非正式會議)。

德爾非研究也導出一個可以被認為是實現 IT 治理最基本實務的名單，這建議表明在實施資訊技術治理時,如在一個具體的金融服務組織內的治理方面,這些最基本實務可以起重要作用。這些實務指的是資訊技術監督委員會、資訊長為執行委員會一員、資訊技術組合管理、資訊技術預算控制與報告、資訊技術策略委員會，策略型資訊系統規劃、資訊技術領導、資訊長向執行長或運營長報告、資訊技術專案監督委員會及專案管理方法學。

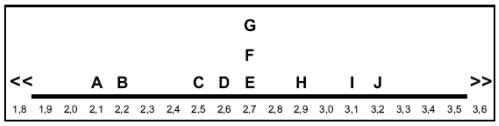
只有一個相關的機制被列在這些最基本實務(指資訊技術領導)方面的報告是令人詫異的,因許多作者都強調此項目是資訊技術治理的決定性相關機制,一個可能的解釋是，正如文獻所顯示，較少詳細的知識體系和專家能提供相關的機制,此也是經常發生難以捉摸和非正式屬性機制項目的原因。

另一方面，應當指出其他的相關機制，例如在業務/資訊技術帳戶管理上，資深管理者就是一個好例子,以及在業務和資訊技術的執行/資深管理者間的非正式會議，都有助於有效性上與容易實施上,取得非常正向的得分,故這些在考慮配合的最基本實務時，應該加以考慮。

同時本文必須指出的是,前面提到的最基本實務項目,應該被認為是一套最重要的整體的實務，整體上，其能為更好的業務/資訊技術配合作出貢獻。這可以清楚的解釋一些個別的實務，例如資訊技術策略委員會，得到有效性方面較低的分數。它的價值,就是成為最基本實務項目的一部分,使其它實務能夠有效運作。

何為資訊技術治理在業務/資訊技術配合的影響?(What is the impact of IT Goverance on business/IT Alignment?)在測量 10 個比利時金融服務組織配合度之後，如果成熟度最高得到五分法下，比利時金融服務業的平均分數為 2.69 分(**圖 5**)

圖5 –業務/資訊技術整合成熟度基準

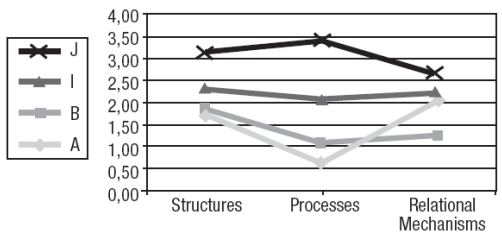


*由0-5評分,0表示無效;5表示非常有效

成熟度比較的標竿包含二個組織(高績效者，I 和 J)，與總平均比，具有比較高的業務/資訊技術配合成熟度，與兩個具較低的得分組織(低績效者，A 和 B)，其它 6 個組織則落在平均數的周遭。這裡有一個有趣的狀況是，什麼是金融服務業的目標或者未來的情勢將如何。這塊領域可得到的文獻不多，但是考慮對於資訊技術的高依存度，我們可以提出的結論至少要達水準 3，表示應有標準化與文件化的程序與過程。

在這些極端的情況中，每個組織都採用前述 33 項資訊技術治理實務，評估其成熟水準。當比較成熟的資訊技術治理實務(架構、程序和相關機制)的平均數與那些極端的情況時，通常而言，高績效者有較成熟的資訊技術治理架構與程序，如**圖 6** 中所示。這個數字也顯示一般而言，當程序不如架構成熟時，實施過程會較實施架構困難，這也是之前討論過的。

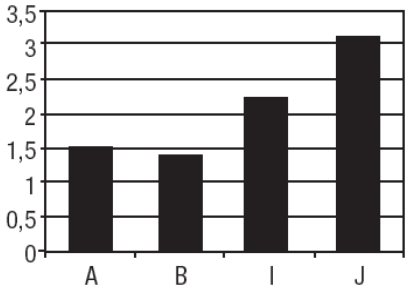
圖6 –較極端的案例1



*由0-5評分,0表示無效;5表示非常有效

我們也注意到業務/資訊技術配合成熟度較低的組織，會有許多的實務，但這些實務的平均位置，多低於水準 2 的成熟度，如**圖 7** 中所示。這可能表明，影響業務/資訊技術配合的資訊技術治理實務的成熟度，成熟水準 2 應是限制門檻。

圖7 –較極端的案例2



*由0-5評分,0表示無效;5表示非常有效

本研究並未能證明，相關機制的影響在業務/資訊技術配合成熟度的關係(**圖 6**)；但是，研究確實發現兩個高績效組織，許多年前已經開始他們的資訊技術治理導入工作，而且重點是很多資訊技術治理的架構和程序，已嵌入在日常的作業中了。而此時，相關機制的重要性就變得不那麼重要了。而由兩個低績效者分數落點可以知道，相關機制在資訊技術治理起始階段較為重要。

更詳細分析高績效者，顯示他們自己所運用的一套資訊技術治理實務，也正是被在德爾非研究裡所推薦為最基本實務的資訊技術治理實務項目。由以前確定的 10 項最基本實務中，有 7 項出現在高績效者的內容中，且成熟度亦高(高於成熟度 2)。這些限縮後的實務被叫為關鍵最基本底線，內容為下列實務項目：資訊技術監督委員會、資訊技術專案監督委員會、組合管理、資訊技術預算控制與報告、資訊長向執行長/運營長官報告、專案治理/管理方法學及資訊技術領導。

任何組織都沒採用的一個有趣的資訊技術治理實務，雖然專家並意見領袖，都認為它非常重要，就是資訊技術策略委員會應該具有董事會的地位。鼓吹這一實務架構是為了，確保資訊技術治理議題，為董事會成員重視。當審視此一項目時，4 間組織中有 3 間表示董事會介入資訊技術治理，是不可行且可能是不需要的。研究發現股東的代表更重視核心金融服務活動，較少涉及(操作)資訊技術議題。另一顯示與資訊技術配合無關的資訊技術治理實務，就是 COSO 企業風險管理，一般認為這是對內部控制、治理價值或影響，有利配合度的因素，卻未出現在任何一個組織中。

結論 (Conclusions)

這研究顯示出，與某些組織相比，資訊技術治理在架構、程序及相關機制較成熟的組織，的確與業務/資訊技術配合成熟度，有很高的關聯。一些詳細的結論是，關於資訊技術治理架構，程序和相關的機制，研究證明導入資訊技術治理架構較資訊技術治理程序容易。相關的機制也似乎看起來，是一項在資訊技術治理實施專案開始階段非常重要，但是日後已將資訊技術治理架構嵌入日常的作業時，就變得不那麼重要了。

這研究也提供各個組織必需有的相關 7 個資訊技術治理實務與其補充的關鍵最基本實務，這些都被視為是非常有效並且容易實現的項目。當一個組織想要實現這些實務時，它必須保證至少，成熟度能達到 2 的水準，以保證對業務/資訊技術配合有正面影響。

要實現資訊技術治理的最好的方法，是開始建立這 7 項關鍵最基本實務的資訊技術治理實務。這核心的實務應該靠非常有效並且相對容易實現的其他關鍵實務支持。在這樣的資訊技術治理專案的創始時期，相關機制應該受到充分的注意，以確保過程中，全部介入人員的承諾。一旦治理文化嵌入在架構與程序裡，相關的機制就不需太多的注意。

參考文獻(References)

De Haes S.; W. Van Grembergen; 'IT Governance Best Practices in Belgian Organisations' , proceedings of the Hawaii International Conference on System Sciences, USA, 2006

Nolan, R.; F.W. McFarlan; 'Information Technology and the Board of Directors' , *Harvard Business Review*, 83(10), 2005, p. 96-106

Sledgianowski D.; J. Luftman; R.R. Reilly; 'Development and Validation of an Instrument to Measure Maturity of IT Business Strategic Alignment Mechanisms', *Information Resources Management Journal*, 19(3), 2006, p. 18-33

Van Grembergen, W.; S. De Haes; *Information Technology Governance: Models, Practices, and Cases*, IGI Publishing, 2008

Van Grembergen, W.; S. De Haes; E. Guldentops; 'Structures, Processes and Relational Mechanisms for IT Governance', in Van Grembergen, W. (Ed.), *Strategies for Information Technology Governance*, Idea Group Publishing, 2003

Weill, P.; J. Ross; *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*, Harvard Business School Press, USA, 2004

【註】

[1] Peterson, R. R.; Information Strategies and Tactics for Information Technology Governance? in *Strategies for Information Technology Governance*, Idea Group Publishing, 2003

[2] *Ibid.*

[3] *Ibid.*

[4] IT Governance Institute, *Board Briefing on IT Governance, 2nd Edition, 2003, www.itgi.org*. Monnoyer, Willmott P.; What IT Leaders Do: Companies That Rely on IT Governance Systems Alone Will Come Up Short', McKinsey Quarterly, 2005

作者簡介

The results reported in this article are based on Ph.D. research executed by Steven De Haes under the direction of Professor Wim Van Grembergen at the University of Antwerp Management School (*www.uams.be/itag*).

Steven De Haes, Ph.D.
is responsible for the information systems management executive programmes and research at the University of Antwerp Management School. He is managing director of the Information Technology Alignment and Governance (ITAG) Research Institute and recently finalised a Ph.D. on IT governance and business/IT alignment. He has been involved in research and development activities of several COBIT products. He can be contacted at steven.dehaes@ua.ac.be.

Wim Van Grembergen, Ph.D.
is a professor at the Information Systems Management Department of the University of Antwerp and an executive professor at the University of Antwerp Management School. He is academic director of the ITAG Research Institute and has conducted research in the areas of IT governance, value management and performance management. Over the past years, he has been involved in research and development activities of several COBIT products. He can be contacted at wim.vangrembergen@ua.ac.be.

每一位電腦審計人員應該了解的網路犯罪
(What Every IT Auditor Should Know About Cybercrimes)

作者：Tommie W. Singleton, Ph.D., CISA, CMA, CPA, CITP
譯者：張騰龍, CISA

因為多種因素，在過去 10 年內網路犯罪有逐步增加的趨勢。因此，電腦審計人員需要瞭解網路犯罪對於其查核對象所帶來的風險(例如，針對查核對象的系統環境所犯下的網路犯罪或使用查核對象系統環境所犯下的網路犯罪)。本文將介紹一些常見的網路犯罪類型，應能協助電腦審計人員在執行查核時針對相關類型的網路犯罪執行風險評估。

在 2005 年，電腦安全協會（Computer Security Institute, CSI）和美國聯邦調查局（Federal Bureau of Investigation, FBI）所執行的"電腦犯罪和安全問卷調查"顯示，百分之 56 的受訪者發現在過去 12 個月內有發生至少一次的資訊安全事件，同時這 693 名的受訪者也在同一期間提報了 1.3 億美元的相關損失（見**圖 1**，部分於 2005 年問卷調查中所辨識出來的損失清單）。

圖 1 –2005 年網路犯罪損失

犯罪類型	損失金額
病毒	US $43 百萬
未經授權存取	US $31 百萬
資訊盜竊	US $31 百萬
金融詐騙	US $3 百萬

為了達到本文的目的，我們需要一個較明確的網路犯罪定義來描述網路犯罪到底涵蓋了哪些類型的活動：使用電腦犯罪，非法儲存的資訊或數據，或針對關鍵資訊基礎設施執行非授權活動。這個定義包括以下行為: 非法取得數據，機密資訊或其他資訊；非法使用任何非公用電腦；以及非法使用一個受保護的電腦系統，例如政府或金融機構的電腦系統。

網路犯罪分類

第二個議題是要提供一些網路犯罪的分類以便電腦審計人員履行其職責。**圖 2** 提供了對於電腦審計有所影響的網路犯罪分類(不包括較屬於法律問題的犯罪行為)。電腦審計人員需要分析每個類別以辨識相關的風險。

圖 2 –網路犯罪分類

- 資訊系統入侵
- 智慧財產權
- 信用卡舞弊
- 網路勒索與詐騙
- 身份盜用
- 洗錢

資訊系統入侵

資訊系統入侵包含因非法或不道德的行為而造成對營運各體可量化的損失。

一個日益嚴重的領域是工業間諜活動。有一些國家似乎支持其公民針對其他國家的營運各體從事這種類型的活動，而有一些政府甚至直接從事間諜活動。營運各體面對這方面的風險包括：航空、航天系統、軍事裝備、化學系統、生物系統、動能系統、電子、制導控制系統、資訊系統、資訊戰爭、材料加工、海洋系統、核能系統、傳感器和激光器、簽名控制系統和武器對策系統。

其他資訊系統入侵的領域包括未經授權而從一個營運各體的資訊系統獲取資訊或數據，使營運各體的資訊系統感染上病毒或蠕蟲，以及資訊基礎設施的攻擊，如阻斷服務攻擊 (Denial of Service Attack, DOS)。

智慧財產權

智慧產權有時是可以通過電子方式取得/使用，如有版權的書籍或數位化的商品(音樂，電影，軟體等)。非法使用或複製軟件就是一個很好的網路犯罪例子。但國際法規和慣例複雜化了此問題。例如，許多著作權法只有效於某一個國家，但不一定在另一個國家能生效。因此，被攻擊的公司或政府機構難以起訴來自國外的網路攻擊，除非有關國家有類似的法律。

信用卡舞弊

有數據表示，有一些犯罪分子，以前可能不會罪犯或只會執行一些較不起眼的街頭犯罪(例如，從事毒品銷售，勒索或放高利貸)，正在轉向以盜取信用卡號作為一種犯罪或"謀生"工具。有組織性的犯罪集團也已轉向網路犯罪，包括信用卡盜竊，網上賭博，網上敲詐勒索，網上毒品銷售，甚至網路恐怖行動，而不是大家以往印象中在街頭上大火拼的幫派活動。

網路勒索與詐騙

跟盜竊信用卡一樣，網上敲詐勒索已成為一個與幫派組織相關的犯罪領域。但同時，即使是十幾歲的駭客，尤其是那些居住在離被攻擊對象較遠國家的駭客，也正嘗試在獨立作業並進行勒索。例如幾年前一位住在歐洲的十來歲的小夥子企圖勒索總部設在美國的 CD 宇宙公司(CD Universe)。

網路詐騙包括電訊詐欺和電子郵件勒索威脅。

身份盜用

身份盜竊應該是大家最熟悉的網路犯罪類別。它包括網路釣魚及相關活動，其最終目的是要偷取他人的身份以便非授權的取得信貸或金融資產。大多數的讀者很有可能在這過去一星期中已經收到了詐騙電子郵件的經驗。銀行與出名的網路企業經常是此犯罪類別的受害者。

在某種意義上，網站劫持也是一種對於企業的身份盜用。也就是說，網路惡徒建立了一個企業的偽裝官網，並利用電子郵件或其他手段，引導客戶到此假網站來獲取個人資訊。這就是為什麼有一些銀行和其他金融機構使用 passmark 控制來驗證自己的官網。Passmarks 是結合客戶選擇的圖件與客戶定制的詞組以協助客戶確保該網站是官網，而不是偽裝的。

洗錢

金融機構對於這方面的風險有很大的興趣。因為最近的恐怖襲擊事件，如在美國紐約發生的 911 事件，以及隨後的法規，為查明可疑的活動，銀行和其他金融機構已須提交可疑活動報告(Suspicious Activity Report, SAR)。許多可疑活動都與洗錢有關。事實上，美國聯邦政府機構認為，恐怖分子使用各種洗錢模式資助恐怖活動。美國聯邦政府機構希望藉由可疑活動報告來查明這些人。

洗錢不一定涉及電腦，但電子匯款在近幾年常常被用於洗錢活動。由於此類活動的增長和大眾對於此議題的高度興趣，這方面也被列為一種網路犯罪。

攻擊的來源

當在分析網路犯罪的風險時，電腦審計人員通常不必四處尋就可以找到罪魁禍首。CSI 和聯邦調查局的 "電腦犯罪和安全

問卷調查”顯示，最可能的攻擊來源是對公司心懷不滿的員工。依攻擊可能性排列，獨立駭客和競爭對手皆排列於心懷不滿的員工之後。

結論

電腦審計人員需要了解與受查單位有關的網路犯罪才能執行有效的風險評估－現代審計方式的基礎。即使不同受查單位可能面臨的網路犯罪風險可能會不同，擁有對於網路犯罪的基本了解，或相關的網路犯罪分類，應能協助電腦審計人員執行他/她的職責。

參考資料

The US federal government has established a web site, the Internet Fraud Complaint Center,[1] that allows the public to report Internet frauds, identity theft and other crimes. It is also an education site that teaches individuals about Internet fraud.

Another web site is the Internet Crime Complaint Center (IC3),[2] cosponsored by the FBI and National White Collar Crime Center (NW3C). Its mission is to serve as a vehicle to receive, develop and refer criminal complaints regarding cybercrimes.

【註】

[1] Internet Fraud Complaint Center, *www.usa.gov/Citizen/Topics/Internet_Fraud.shtml*

[2] Internet Crime Complaint Center, *www.ic3.gov*

作者簡介

The author would like to thank former FBI agent Alton Sizemore for his contributions to this article.

Tommie W. Singleton, Ph.D., CISA, CMA, CPA, CITP
is an associate professor of information systems at the University of Alabama at Birmingham (USA), a Marshall IS Scholar and a director of the Forensic Accounting Program. Prior to obtaining his doctorate in accountancy from the University of Mississippi (USA) in 1995, Singleton was president of a small, value-added dealer of accounting information systems (IS) using microcomputers. In 1999, the Alabama Society of CPAs awarded Singleton the 1998-1999 Innovative User of Technology Award. Singleton is the ISACA academic advocate at the University of Alabama at Birmingham. His publications on fraud, IT/IS, IT auditing and IT governance have appeared in numerous journals, including the *Information Systems Control Journal*.

價值管理的動因
(The Drive for Value Management)

作者：John Thorp, CMC, I.S.P.
譯者：許林舜，資誠會計師事務所 系統與流程管理部 主持會計師

不論組織規模之大小、公開發行或非公開發行、營利或非營利組織，所有企業之存在係為私人企業之所有人或股東、非營利組織受益人或納稅人等利害關係人提供其價值；近幾年，企業價值及其如何達成這個議題，已廣被討論，企業價值備受關注，主要因素如下：

- 企業價值難以捉摸。
- 價值具有變動性的本質，且絕大成份並非是有形的。
- 因普遍使用資訊科技及全球化，使價值之創造日益複雜。
- 因 Clinger-Cohen 法案(有關資訊技術管理改革的法案)及美國沙賓(Sarbanes-Oxley)法案等之規範，使企業價值日益透明。

過去五年來，已有超過七十本著作探討此議題，另經濟學人智庫(Economist Intelligence Unit)在 2006 年與 Deloitte[1] 合作，針對全球 150 位資深主管的調查發現，藉由企業變革的投資，以創造及保存企業價值的作法，常僅為隱含的概念，尚未普遍被採用，無法成為標準的規範。

企業變革可創造企業價值的想法，在 IT 相關的投資方案上尤其明顯，IT 投資不僅是科技方面的投資而已，其已逐漸著重於組織變革，不了解創造企業價值的 IT 投資所引起的組織變革，只不過是隱憂的前兆而已，這樣的隱憂也帶給管理階層全新且重大的挑戰，對於成功導入重大變革的過程紀錄是難以言喻的，以企業流程改造及併購二個重大變革的例子，其成功的比例，不見得比涉及 IT 投資的成功比例多。

無法利用 IT 投資創造企業價值的根本原因包含：

- 不了解今日的領導階層受到的挑戰，是劇烈的文化變遷之一環。
- 無法針對變革訂出目標明確的方案，包含明確且共享的產出結果。
- 無法體會，甚至是常忽略策略實行的複雜性。
- 只會衡量價值，而非真正將創造價值與實際達成目標之行動方案連結，就如同在一場比賽裡，只專注於計分版，而非注重比賽本身的精神。
- 欠缺資深管理階層的注意及承諾，卸責予較低的組織層級，且常無明確的作業標的。
- 在多數的個案裡，治理過程令人遺憾地不足以管理整個達成目標的不確定過程，其導致於：
  - 無法衡量達成目標的過程。
  - 無法呈現及追蹤相關假設。
  - 無法針對變動的環境，及時作適當的察覺及回應。

企業價值的概念在於每個利害關係人的期望以及所需動用的資源中求平衡，每個利害關係人對於企業價值可能有不同想法，價值管理的目的係為協調這當中的差異，藉由選擇及執行投資，使企業獲得最大的進步，以及在可接受的風險下，合理動用資源[2]以達到企業價值最大效益。[3]

價值管理已發展了幾十年，並非全新的概念，但仍有許多值得發掘的議題，麥肯錫季刊報導，充分運用價值管理通常能增加起

碼 5%至 15%的效益[4]，在前述提及 2006 年針對全球 150 位資深管理者的調查發現[5]：

- 31%的受訪者表示流程及系統常與策略無法呼應配合。
- 47%的受訪者表示流程及系統常與員工行為無法呼應配合。
- 僅 14%的受訪者表示在自己的計畫管理中擁有創造重要價值的必要流程。
- 僅 39%的受訪者將過去的專案進度追蹤納入持續績效管理的過程。
- 僅 16%的受訪者完全同意他們的公司能快速地因應經濟、金融及商業的變化。

資訊治理協會(IT Governance Institute，簡稱 ITGI)出版的 Val IT™[6]，提出有效的實務，以幫助企業解決上述的問題，根據研究機構 Forrester 最近的一份報告裡，Craig Symons 寫道：「企業若嘗試要執行 IT 策略以達成商業價值，以及將商業價值傳達給利害關係人，應評估採用 Val IT 為工具以改善價值的提供。[7]」雖然這些實務常主要涉及與 IT 有關的投資，但不管有無涉及 IT 投資，其多數可全面應用於企業變革之投資。

要完成上述所提的價值管理，一開始可能覺得難以下手，不過已有公司成功地適應商業上的文化變遷，付出心力並得到成果，Deloitte 的研究顯示，例如達美樂比薩、芝加哥商品交易所及羅技等均已採用價值管理，並成功地將此概念融入其企業中。[8]

【註】

[1] Economic Intelligence Unit, *Adopting the Value Habit*, survey produced in cooperation with Deloitte, 2006

[2] In this context, "asset" refers to anything that can be used by an enterprise to advance its objectives.

[3] Adapted from work done by the Institute of Value Management, *www.ivm.org.uk*

[4] Benson-Armer, R.J.; R.F., Dobbs; P. Todd; "Putting Value Back in Value-based Management," McKinsey Quarterly, Spring 2004

[5] *Op cit*, Economic Intelligence Unit

[6] For more information about Val IT, refer to *Enterprise Value: Governance of IT Investments, The Val IT Framework*, which can be downloaded from *www.itgi.org* and is also available from the ISACA Bookstore at *www.isaca.org/bookstore*.

[7] Symons, Craig; "From IT Governance to Value Delivery," Forrester Research, 22 June 2007

[8] *Op cit*, Economic Intelligence Unit

作者簡介

John Thorp, CMC, I.S.P.
is president of The Thorp Network Inc. and a consulting fellow with Fujitsu Consulting. He is an internationally sought-after management consultant with close to 45 years of experience in the information management field. Author of *The Information Paradox*, Thorp's focus is on helping organizations realize the benefits of IT-enabled change. Over the last five years, his work has extended beyond IT to the broader issues of enterprise value management and strategic governance. He is currently working with ITGI to research, develop and promote Val IT.

資訊風險管理計畫之要素：將資訊安全轉換為資訊風險管理 (Key Elements of an Information Risk Management Program: Transforming Information Security Into Information Risk Management)

作者：By John P. Pironti, CISA, CISM, CGEIT, CISSP, ISSAP, ISSMP
譯者：許林舜，資誠會計師事務所 系統與流程管理部 主持會計師

資訊安全與保護對組織有絕對的重要性，但並無法確保組織營運的成功，從風險管理的角度出發，不但可在資訊安全與組織營運的需求中取得平衡，更可加強資訊保護，並進一步促使組織達到營運活動的效率與成功，資訊在企業營運中一向有著其可觀的價值，然而，資訊的價值卻是一直到了最近，才被有能力與企圖心的企業競爭對手真正瞭解及運用。

目前全球企業的趨勢，是針對法令遵循、資訊與實體安全、隱私權、以及作業及財務風險等，個別建立獨立的部門以達到上述各面向的公司治理。這些個別的組織個體皆能有效的達到其組織目標，然而，由於這些部門各自獨立作業，並隸屬於不同管理階層，它們可能無法達到企業整體的有效資訊風險管理目標，透過這些獨立部門組織的結合，有效的資訊風險管理是可行的。

為何資訊安全如此具挑戰性?

資訊安全因有著持續變更與演化的特性，成為資訊作業流程中，最具挑戰性的一環。簡單來說，資訊安全之所以困難，是因為敵人只需要猜對一次就成功了，而防守的一方則需要每次都對，才得以保住資訊安全，然而，資訊安全負責人員卻往往被缺乏資金、資源、時間、以及知識而困擾著。企業往往期望資訊安全負責人能夠在有限的資源與能力下，避免任何可能造成資訊架構損壞之風險，每當資訊安全負責人創造或導入了一套防止敵人攻擊之控制機制，對手往往會發展出一套更新更有效的攻擊手法，迫使資訊安全負責人再發展出更多的其他控制。

職場倫理、法令規範、組織士氣、資金的匱乏、以及資源的缺口，皆無法限制敵人的惡性行為。網際網路的廣泛使用與發展，使得資訊安全不良份子有了更方便的平台，不需要面對面討論，就可集結各方知識，開發出更新的攻擊手法，他們共同產生的研究分享、知識、以及開發能力，遠遠超過了任何企業組織可以單獨達到的境界，而資訊安全負責人剩下最有可能遏止敵手的方法，便是運用風險管理的方法以保護資訊，以有限的資源與能力，協助企業有效的保護必要與重要的資訊。

資訊安全現況

目前企業主要的資訊安全仍是著重在透過科技的使用，以降低其威脅，過去的經驗證實，政策、流程及程序，再輔以科技的應用，比起單獨依靠科技的使用，更能夠提供有效的防護效果，然而，大部分企業並未慣常的建置這些要素，其主要原因在於政策、流程及程序的建置及運作，比起直接採購與安裝一科技性的控制措施，困難度較高，且無法像科技性的控制措施一樣可以立即見到效果，企業普遍缺乏耐心，導致威脅

的範圍擴張，並顯著的提升了敵人接近與利用企業資訊架構之能力。

「僅為法令遵循的安全」是一個非常危險的全球化趨勢，其意思是指，企業將全部的資訊保護重點，放在達到政府與產業制定之各項規範上，例如支付卡產業標準(Payment Card Industry (PCI) Standards)、沙賓法案(Sarbanes-Oxley Act)、歐洲資料保護與隱私權法案(European Data Protection and Privacy Act)、以及資訊揭露相關法令等，提供了某些程度上的資訊保護引導方針，部分上述標準，例如 PCI 標準，提供了企業必須建置特定科技與控制的相關規範，即使這些控制對於該企業沒有實際效用，甚至其與企業本身根本沒有重大關聯，此概念因此有著極高的風險，它將重點放在組織達到法令遵循上，而非了解與降低實際企業在資訊架構上面臨的風險與威脅。

企業面臨的威脅版圖在過去的幾年中已大幅的改變了，資訊攻擊社群已將其重點從概念性的驗證及地位追求為目標之攻擊，轉換至高目標導向、高效果、與不醒目的攻擊為主，這代表著過去用來保護資訊與資訊架構之智慧、科技控制框架、以及手法與實務操作，已經無法有效的保護資訊安全，企業因此必須以風險為導向的決策流程與架構，以因應新的挑戰。

資訊風險管理 vs. 資訊安全

資訊風險管理定義組織資訊架構的範圍，辨識需要保護之資訊內容，並依照組織的風險容忍值擬訂資訊保護之程度，其辨識企業之價值、商業衝擊、法令遵循需求、以及組織整體商業策略之一致性，一旦辨識出上述相關資訊，資訊風險管理單位可將此資訊呈報給企業領導者，供其在評估為達到適當的資訊保護與風險管理時，應作多少財務及資源投資的決策參考依據。

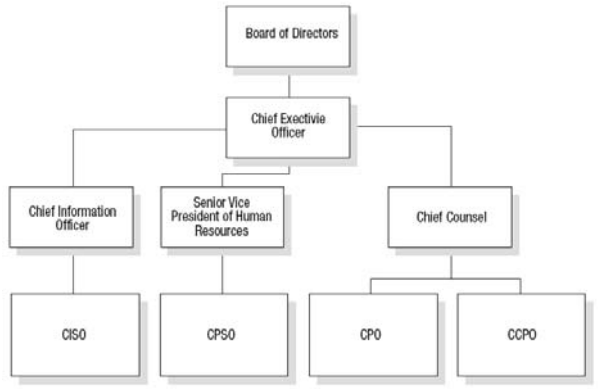
在完成資訊安全相關投資決策後，資訊安全小組可依照企業領導者之決策，著手進行適當功能與機制的建置，資訊安全小組協助辨識威脅、研擬及建置控制措施、以及定期監控相關控制之有效性，以確保控制與目標之一致性。此風險管理模型與目前的資訊安全狀況的主要差異，在於資訊安全小組的決策權，在風險管理模型中，資訊安全小組在整體企業中，不再擁有定義資訊安全及資訊架構相關與否的決策權，取而代之的，該小組負責提供企業領導者有價值的參考資訊，由企業領導者依照獲得的資訊作出適當的商業決策，這項重大的變化，顯著的提升了資訊安全小組的有效性，組織不再將這些小組成員視為阻礙企業營運的糾察隊，而是協助企業營運的專門顧問。

資訊風險管理的演進

在現今之大多數企業中，資訊保護與確保能力等相關專案以不同的型態，存在於不同的流程階段中，相關能力通常可依照功能別來區分，其領導者可能命名為資訊安全長(Chief Information Security Officer, CISO)、隱私長(Chief Privacy Officer, CPO)、實體安全長(Chief Physical Security Officer, CPSO)、以及法令遵循長(Chief Compliance Officer, CCPO)等，不幸地，這些職務雖然皆有「長」的頭銜，實質上他們卻沒有領導階層權限，與參與重大策略活動擬定之權限，並且各自分別隸屬於不同的領導階層類別，他們亦通常獨自運作，僅在必要時有部分交流，與企業策略無關。

這些資訊保護機制必須依照現今資訊與資訊架構所面臨的挑戰而演進。這些機制的演進(**圖 1**)，需要透過這些各自獨立的單位之整合，進而產生一個整體性的企業單位，也就是所謂的資訊風險管理計畫。

圖 1–資訊風險管理的演進



資訊風險管理計畫

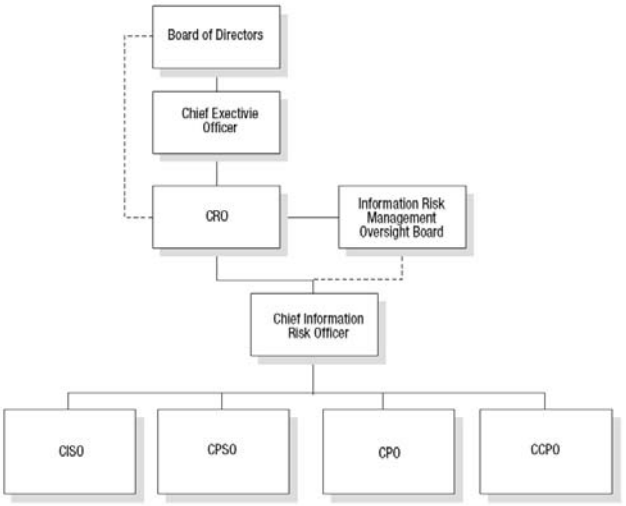
資訊風險管理計畫可提供企業一個360 度的全面性資訊資產與其所有相關資訊架構之風險觀點，此計畫為公司治理模式之演化，主導資訊風險管理相關之概念與商業活動，它並將既有負責提供資訊保護之獨立領導單位與計畫元素，整合為一個單一的功能組織，由一個統一的領導者帶領，該領導者並擁有參與企業之商業活動與策略決策之權限。

資訊風險管理計畫若能有效的導入及運作，可促使組織在風險導向的模式下營運，帶來相對應的企業價值。與其限制企業的運作，資訊風險管理計畫提供了更有效果的營運規範，使企業能夠在正常營運的同時，達到資訊資產及架構的有效保護。此計畫之概念徹底改變了企業營運的典範，其透過找出方法以促進企業的活動及能力，而非因著察覺到的風險，而限制了企業的商業活動，舉例來說，資訊風險管理並不會阻止企業存取系統與資訊，相對的，它會評估出適當的存取權限，以及適當的存取時點。過多的資訊安全控管機制可能阻礙到企業的營運，而此計畫之目標為在使資訊資產風險最小化的同時，促使企業之商業活動能達到其營運目標。

組織架構設計之進化

欲有效的達到組織風險管理需求，企業之組織架構需要導入一個整合且有效率的管理方法(**圖 2**)。此方法之概念係使企業中之所有風險管理活動皆回報給單一主管 - 風險長(Chief Risk Officer, CRO)，此風險長為所有風險辨識、風險降低、與風險控管等相關活動之統一溝通資訊匯集中心，風險長亦與高階管理階層有定期的互動，提供管理階層所有與資訊風險有關的企業決定、策略、與活動之相關資訊、引導、及方向。

圖 2–組織架構設計之進化



關鍵績效指標

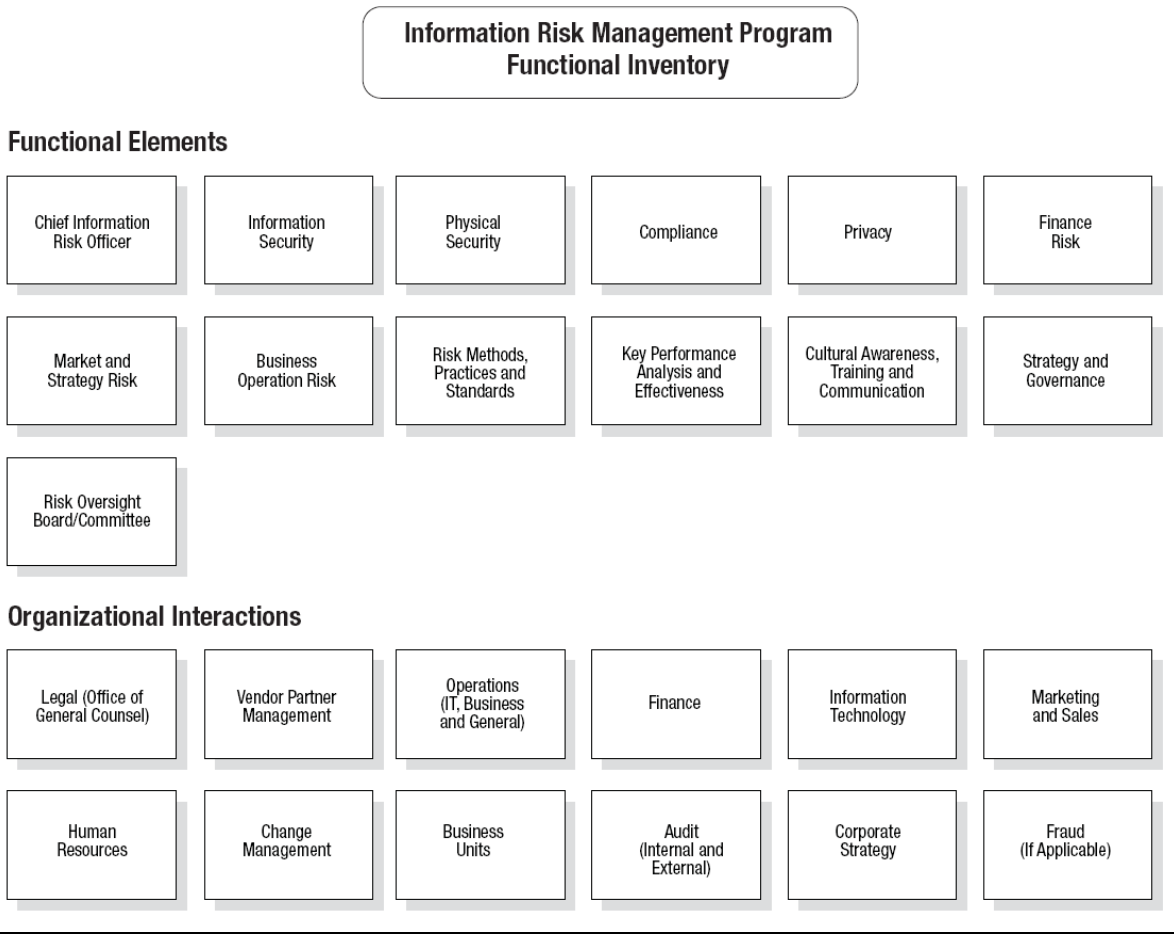
關鍵績效指標(KPIs)是用來評量商業功能、流程及能力之重要商業智慧工具，若要有效果的治理企業之資訊風險管理，各功能單位與流程皆需要配有可衡量的關鍵績效指標，這些指標需要設有對應的上、下限門檻值，使企業能及時的知道企業內部的各單位組織是否正常營運，亦或是需要特別關注，關鍵績效指標亦提高了資訊風險管理計畫的價值，並對於該計畫的成熟發展有絕對的貢獻。

唯有從商業功能與流程的角度出發，才能設計出有效的關鍵績效指標，有效的績效指標需要與企業的營運活動說著相同的語言，並且與組織內部經過適當與有效的溝通，未能符合這些條件的關鍵績效指標，通常都是無效的，並可能造成企業內部的困惑及負面效應，因此，關鍵績效指標在企業內需有經過共同認可的價值，才能產生其效果，欲促成有效績效指標之建置，與衡量指標相關之衡量者與被衡量者，皆須參與其設計、運作、與推廣之活動，如此一來，這些指標才可實際協助企業的營運，而非只是成為另一個被組織遺忘或誤解的資料數據，在企業中，無效或是不準確的關鍵績效指標，可能造成與沒有使用關鍵績效指標相同或是更多的傷害。

資訊風險管理計畫之要素

資訊風險管理計畫(**圖 3**)替企業資訊風險管理議題提供了一個結構性的方法，它在企業既有的元素中，建置相關流程與功能，提供了企業更有效果的溝通及資訊分享管道，透過企業內部既有功能的合併，以及擬訂一致的方法論、流程及程序，資訊風險管理計畫可有效的提升企業資訊風險管理功能的效率。

圖 3－資訊風險管理計畫



風險管理計畫在企業中，扮演著擁有最小營運責任的顧問參謀腳色，與其負責作資訊保護相關之決策，風險管理計畫提供企業決策者有價值及可靠的資料，作為商業決策之參考依據。

資訊風險長

資訊風險長(Chief Information Risk Officer , CIRO)是安全長(Chief Security Officer, CSO)一職自然演化而成的，負責整體資訊風險管理計畫之相關活動，其係負責與企業領導階層及組織整體溝通所有風險相關議題的主要人員，且應為組織高階領導階級，並有參與企業重要領導活動，資訊風險長負責建立與溝通組織中各商業元素、流程、及企業整體之資訊風險層級，其關鍵績效指標包括：

- 辨識、評估、分類及降低的資訊風險數量。
- 資訊風險管理計畫(含內部及外部)的瞭解程度。
- 與競爭對手及同業相較之下，資訊相關事件或意外之衝擊度。

資訊安全

資訊安全是可以提供企業關於威脅與弱點相關資訊的有效機制，但它卻不是一個可有效辨識風險的管理機制，資訊安全組織通常需要負責辨識與企業資訊及其相關資訊架構有關之潛在風險，然而大部分的資訊安全組織卻無法適當的完成此任務，因為他們缺乏了組織策略、稽核、法令遵循、財務及行銷等相關所需知識，以提供上述之風險辨識服務。

資訊安全組織在風險管理模式中，扮演著辨識與評估企業內資訊資產及其相關資訊架構有關風險及弱點的角色，此單位定義、建置、監控及善用控制措施及控制架構，以降低辨識出之威脅與弱點，此單位於得知企業對於威脅與弱點之可容忍風險水準後，便可著手擬定符合企業營運需求之適當控制。

資訊安全功能對資訊風險管理組織最主要的利益之一，即是提供資訊及其相關資訊架構有關之威脅與弱點資訊，透過威脅與弱點分析，資訊安全組織可以提供給資訊風險管理組織可靠的潛在威脅與弱點之商業衝擊及可行性等相關資訊，這些數據對於用來開發提供給企業的風險相關資訊，有著極高的價值，其可使企業及時處理最有可能發生及有最高商業衝擊之威脅，並對其他威脅與弱點作有效的追蹤。

資訊安全的主要績效衡量指標包括：

- 威脅與弱點分析活動與資訊之準確度。
- 弱點管理計畫及控制之有效性。
- 政策、程序、方法及標準之有效性。

實體安全

實體安全組織係負責提供關於企業實體架構元素相關之威脅與弱點等資訊，其負責定義、建置、監控及善用實體控制措施及控制架構，以降低辨識出之威脅與弱點，此單位於得知企業對於威脅與弱點之可容忍風險水準後，便可著手擬定符合企業營運需求之適當控制。

實體安全的關鍵績效指標包括：

- 衝擊商業活動之實體安全事件及意外之發生次數。
- 辨識出之實體威脅及其矯正計畫之數量。
- 實體安全控制之有效性。

法令遵行

法令遵循功能辨識企業需要符合之政策、標準及法令，確保企業有足夠的控制可以因應上述需求，並同時監控組織之運作，此單位亦負責確保相關資訊有效及確實地與企業內部相關單位，以及外部主管機關適當溝通。

法令遵循功能須建置一個衡量架構，確保企業之合規評量及管理機制能持續進行，此架構可使組織了解哪些區塊尚未與政策及法令規範相符，以及發現哪些區塊在法令遵行上已注入過多的投資。

法令遵循的關鍵績效指標包括：

- 內、外部稽核發現的數量。
- 法令遵循相關需求的成本。
- 內部政策與規範需求的例外數量。

隱私權

隱私權功能負責建置隱私相關需求，及其他與隱私權有關的企業政策與程序，此單位定義及辨識企業內非公開個人資訊之使用，辨認與該資訊使用相關之商業及個人風險，並定義該資訊在企業商業流程中之適當與可接受的使用方式，此單位亦負責編撰及管理企業之正式隱私權聲明，以及企業與內部利害關係人、客戶、廠商及合夥人間溝通之相關控制。其關鍵績效指標包括：

- 隱私相關之暴露及意外事件之數量。
- 內、外部利害關係人對於企業隱私權政策及程序之瞭解程度。
- 隱私權政策之例外數量。

財務風險

財務風險功能負責評估企業之財務風險，包括信用、資本、投資及財務風險、以及商業流程活動及資訊資產相關企業活動之舞弊等，此單位提供商業決策的潛在財務衝擊及衝擊商業活動之事件等，此單位亦提供與風險單位之各單獨活動及功能相關的財務衝擊分析資訊。其關鍵績效指標包括：

- 資訊風險管理控制之成本。
- 處理資訊風險管理事件及意外之成本。
- 針對以辨識之信用威脅與弱點所開發之財務風險模型之數量。

市場與策略風險

市場與策略風險功能提供與資訊資產有關之市場導向活動及公司策略而產生之商業活動的潛在衝擊，此單位與企業相關之市場最新狀況，並辨識可能阻礙企業在整體活動或特定商業流程中成功之相關風險，此單位分析企業整體及個別商業流程及活動之商業策略，並辨識出可能影響成功之資訊風險，並會檢視新商業動機及概念，用以評估其相關之資訊風險。其關鍵績效指標包括：

- 與資訊事件相關之負面媒體報導之數量。
- 資訊保護活動及需求對於進攻市場最佳策略之衝擊。
- 風險分析與實際策略活動結果之比較準確度。

商業營運風險

商業營運風險即為阻礙企業正常運作之風險。此功能負責分析特定商業流程之風險，以適當地對資訊資產相關活動中可能影響商業運作之風險作有效的辨認、歸類及管理，此單位亦負責建置衡量機制，監督用來降低商業營運相關威脅與風險之控制的能力及有效性。其關鍵績效指標包括：

- 降低風險之控制對於商業流程的衝擊。
- 商業營運中可靠辨識出之風險的數量。
- 用來監控風險控制能力及有效性之衡量指標的準確度。

風險方法論、實務作業及標準

若要適當的辨識、分析及管理企業中之資訊相關風險，企業必須發展、採用及維護一套一致性的方法論、實務作業及程序，這些包括了用以產出可靠並可執行的風險情報，提供組織作適當決策之人工流程及系統自動流程，此單位負責建立上述功能機制，並確保該機制可穩定進化與成長，該些功能應可被獨立審查單位定期稽核，以確保功能

是否準確運作，以及該些功能機制產生之資訊是否是可靠的風險相關資訊，其關鍵績效指標包括：

- 使用者對於方法論、實務作業、程序及標準之接受比例。
- 與功能成熟度模型標準比較之方法論、實務作業、程序及標準之成熟度。
- 企業中用來強化風險管理機制之新功能的數量。

關鍵績效分析及有效性

資訊風險管理計畫中之各功能元素皆包含了一系列的關鍵績效指標，以確保其能如預期的作用，並創造企業價值。關鍵績效指標之監控、分析及成熟度，對於確保其在各功能區塊之設計是否適當，及衡量其表現是否符合預期，亦是非常重要的，此單位負責針對各功能區塊設計對應的關鍵績效指標，並蒐集其所有相關之數據資料，資料取得與分析後，針對企業中之風險狀態產生有意義與可執行的報告，提供管理階層對風險管理計畫作有效性評估。

此功能亦負責辨識及研擬關鍵績效指標，並規劃其成熟度與生命週期，部分關鍵績效指標在風險管理計畫中，僅對某些商業流程之特定週期有效，而其他的關鍵績效指標則可能是整個計畫生命週期中的持續性指標，一旦辨識出新的功能區塊，此功能即研擬及監控對應該功能區塊的關鍵績效指標，並針對這些指標產出成熟度報告，以確保組織能持續進步，並能達到關鍵績效指標之完整性與準確度。

欲取得計畫中功能及關鍵績效指標成熟度之相關資訊，其中一種方法是透過使用功能成熟度模型標準(Capability Maturity Model Standard)來衡量，透過此標準，企業可取得與企業功能風險管理相關之成熟度資料，並了解所提供的資訊及指引之預期可靠度與完整度。

關鍵績效分析及有效性的關鍵績效衡量指標包括：

- 分析過之數據及擬定出的衡量機制之數量。
- 與產業標準或同業數據之功能比較結果。
- 產生之報表對於使用者之可用性。

文化認知、訓練及溝通

資訊風險管理之主要挑戰之一，是對於風險的認知的缺乏，以及企業內辨識及降低風險的能力，在大多數情況中，「人」是企業可用來降低風險之最有效控制，此功能即是負責企業間的風險相關資訊、能力、與資訊風險管理對企業價值之有效溝通，溝通對象包括供應商、合作夥伴、客戶，及其他企業認為可從風險管理教育與知識中獲益之對象。

企業欲擁有此能力，此功能必須研擬出相關之能力及工具，協助瞭解、教育及溝通企業文化，文化考量例如語言、學習模式、地理政治考量及人員之個性與背景等，皆可透過此功能來辨認出，取得上述資訊後，可將教育訓練及認知宣導活動搭配學習與處理資訊的各個需求，融入有益的商業活動中。

文化認知、訓練及溝通的關鍵績效衡量指標包括：

- 資訊相關事件或意外之數量。
- 企業中資訊風險管理實務作業與能力之採納度。
- 針對特定對象之訓練及認知教材的有效性。

策略及治理

資訊風險管理組織是一個企業中負責提供諮詢服務及有價值之營運作業的商業單位，其策略與治理功能提供了資訊風險管理計畫一個有架構的管理及策略思維，以確保計畫能夠持續地替組織帶來效益，此單位

的管理功能，創造了用以分析因計畫及營運流程而產生的相關商業流程之能力模型、組織架構及衡量機制等營運需求。

此專案的策略元素，辨識了資訊風險管理組織的未來方向，確保其與企業中之商業需求、作業、標準及方法，以及全球資訊風險管理社群之一致性，此單位可確保各功能區塊中皆有適當的商業流程，以有效支援該流程之功能，亦同時辨認及整合新的活動及功能，以提高有效性並替企業整體帶來更大的效益。

策略及治理的關鍵績效衡量指標包括：

- 資訊風險管理活動的成本。
- 能力模型的成熟度，以及其符合商業需求的準確度。
- 企業內對於資訊風險管理計畫有效性的回饋。

風險監督委員會

資訊風險監督委員會可確保資訊風險管理組織的活動皆與商業活動及企業整體需求一致，此委員會由負責企業內部所有重要商業功能的利害關係人組成，他們提供了資訊風險管理組織中之戰略性及策略性指引，風險監督委員會的關鍵績效衡量指標包括：

- 委員會成員中主要商業利害關係人的人數。
- 委員會提供之指引的有效性。

組織內部交流

企業內之資訊風險管理計畫若要有效，須取得其他主要商業單位的意見及該些單位的活動結果，以確保與計畫進行方向是否一致，以協助作出更好的風險管理決策，上述這些組織中的交流活動，不限於經由企業功能單位的日常溝通方法及管道，或一般的訓練與認知活動。其關鍵績效評估指標包括：

- 資訊相關之事件的數量。
- 組織間各單位溝通方法及能力之有效性。
- 資訊風險管理計畫及與其功能之有效性與價值之回饋。

結語

資訊風險管理是企業資訊安全的成熟及演化的結果，資訊風險管理計畫的 導入，可協助企業完整的檢視所有可能影響企業生產力及成功的潛在風險，此外，資訊風險管理更可提供企業縝密分析後之企業營運相關資料，作為風險管理決策之參考依據，資訊風險管理組織在實務上，是負責提供資訊供決策者參考之諮詢單位，而非一個決策單位，透過對於其實務功能之瞭解，風險管理單位可替組織帶來更高的效益，並更可受到各營運企業組織之歡迎，大幅降低企業風險的發生。

作者簡介

John P. Pironti, CISA, CISM, CGEIT, CISSP, ISSAP, ISSMP
is the chief information risk strategist for Getronics. He designs and implements enterprisewide electronic business solutions, information risk and security programs, and threat and vulnerability management solutions for key customers in a range of industries, including financial services, government, hospitality, aerospace and information technology, on a global scale. He is a published author and writer, and a frequent speaker on electronic business and security topics at international industry conferences.

人員、投資組合和流程：資訊治理之 3P 模型 (People, Portfolios and Processes: The 3P Model of IT Governance)

作者：Bop Sandrino-Arndt, CISA, PMP
譯者：謝持恒,CISA,CISM, CGEIT

十年前，資訊技術只是位於支援的功能，是組織眾多功能中分散開來的一支。今天，資訊技術是很多公司的關鍵差異的因素之一，同時在二十一世紀已經成為組織的核心。

資訊技術的管理功能，在許多組織內被視為一項挑戰和複雜的任務之一。資訊技術的功能總是要求迅速的改變，並且又有多樣化的需求。組織的需求經常在改變，同時系統一但上線以後，還要維持適當的運作。資訊技術的建置包括現有設備及未來技術的投資，這也就是資訊技術不能被明確地預測結果的原因。

因此，今天的企業不能再把資訊技術當作是基礎設施而已，而需要用系統化的方式專門管理資訊技術，並且持續的訂定決策以確保資訊功能是符合需求的。另一方面，資訊功能是獨立於組織內其他的功能(如財務、會計)，必須加以管理以便產生企業最佳的價值。

除了這些來自內部的驅動，近期的一些立法行動，例如美國健康保險以及沙賓法案等，都增加了企業內部法令遵循和風險管理的需求。尤其是在資訊部門，這無疑是增加了資訊部門主管的壓力，需要訂定作業規範以及管理機制，以便擁有較好的資訊管理功能，然而該如何做呢?

當資訊治理被視為資訊作業能夠有效的達成企業目標的關鍵成功因素的同時，但對於很多企業而言，如何介紹並且建置資訊治理仍然是一個很大的挑戰。

本篇文章將定義資訊治理並解釋資訊治理與其他公司治理的關係，這個關聯性將會影響資訊治理的建置。我們將會利用 3P 的模型做為建置資訊治理的參考。

資訊治理的定義

資訊治理最簡單的定義，就是管理資訊的功能，利用一套正式的規則及非正式的慣例來治理資訊。這些規則和慣例決定資訊投資是如何決定的、決策如何被執行以及監控、決策的結果是如何被衡量的，決策的能力如何被運用，以及做決策的人如何負起應負的責任。

對於資訊治理比較正式的定義，以下是一些參考：

- 資訊治理是董事會及高階主管的一種責任，包括了領導能力、組織架構和流程，以確保整個資訊作業有符合組織的策略及目標。[1]
- 資訊治理是董事會、高階主管用以控制資訊策略，以確保企業和資訊相結合的一種能力。[2]
- 資訊治理是組織有系統的指導並控制資訊。資訊治理描述在不同利害關係人間，資訊決策的過程及責任。這些規則和程序協助制訂及監控資訊策略。[3]

雖然這些定義在某些方面不同，但是他們都強調將驅動建置模型的發展，以達到有效的資訊治理實施的兩個中心概念：誰能

做出決定(決策權)和如何形成決策(流程/程序)。

資訊治理是整個企業治理的一部分

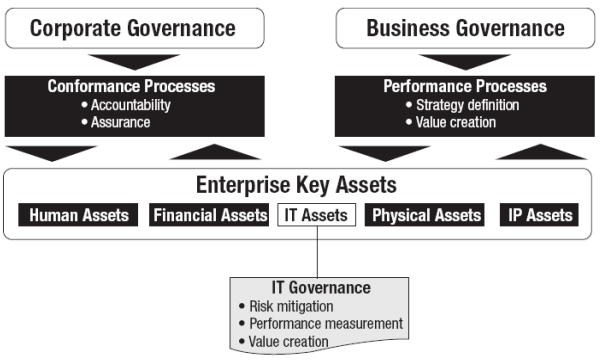
資訊治理的功能，就像企業其他的治理一樣(如財務或人力資源)，是直接且強而有力的連結整個企業的治理。因此，定義治理並且了解彼此間的關聯性及依賴性，會是建置資訊治理時重要的一環。

Chartered Institute of Management Accountants(CIMA)參照 ISACF(Information Systems Audit and Control Foundation)(如今稱為資訊治理協會)，[4] 定義企業治理為：

董事會和高階管理階層用來提供策略決定、確保目標達成以及風險管理之一系列責任與實務運作，以確保企業的資源被合理使用。[5]

企業治理包含了整個組織的管理框架，主要有兩個面向，分別是一致性及效能，這兩者需要彼此間的平衡，如**圖 1** 中所示：

圖 1－業務治理架構(依 CIMA)[6]



- **一致性(也稱為公司治理)** - 包括的議題有治理架構和責任的分派，關注於確保法律和責任義務的一致性和控制。
- **效能性(也稱為業務治理)** - 包括策略定義和價值創造，關注於協助董事會制定策略，並且瞭解組織承擔風險的意願及主要關鍵效能的驅動者。

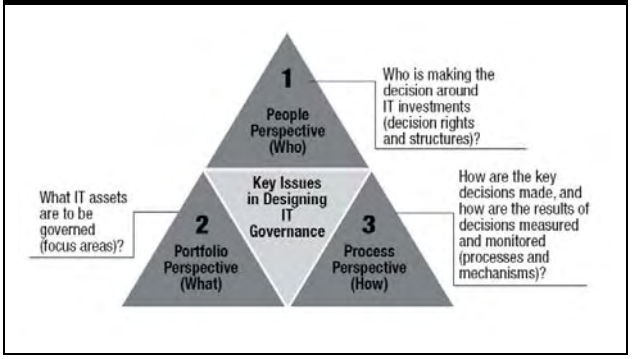
公司治理和業務治理包含了不同的功能(包括 IT)，資訊的功能既然也是整體公司治理的一部分，也就不能獨立於企業的功能(如財務、人力資源、會計及市場)之外，因此資訊治理在管理面和使用資訊科技以達到組織的目標方面，必須反映出董事會企業治理的原則。

設計資訊治理的關鍵問題

資訊治理可以被視為架構、流程和機制的混合使用。當為組織設計資訊治理時，很重要的一件事必須要注意的，那就是資訊治理必須要考量內部及外部等多種有時會衝突的因素，因此要達到資訊治理的有效性，在整合前後關係和組織特性時，應該要平衡整個企業的治理。三個有關資訊治理的問題必須要設計在資訊治理的模型中。

- **誰**應該決定資訊技術有關的投資(決策權和架構)?
- **如何**決定主要的決策，決策過程如何執行監控並且衡量決策的結果(流程和機制)。
- **什麼**樣的資訊資產需要被治理(資訊投資組合)？

圖2－資訊治理的**Who, How, What**



從資訊功能的觀點來看企業治理，當前面兩個問題包含責任及價值創造時，第三個問題

所強調的內容就和資訊治理有關，包含了辨識資訊資產(如 架構、應用系統、專案)，如此一來便會將焦點放在資訊治理上面。

3P 模型：資訊治理設計為導向的內容

如同前面所描述，決定架構、流程和機制的正確組合是複雜的。在這方面，資訊治理的參考模型能提供極大的幫助，以便在建置組織內部資訊治理相關作業時，能設定一個框架。

參考模型的主要目的，在於提供一個一般性的方法，來處理建置資訊治理時的主要問題，如**圖 2** 所示。更進一步，則提供了選擇及定義組織全面性治理的基礎及要素。如圖三所示的 3P 模型，就是這樣一個參考模型。

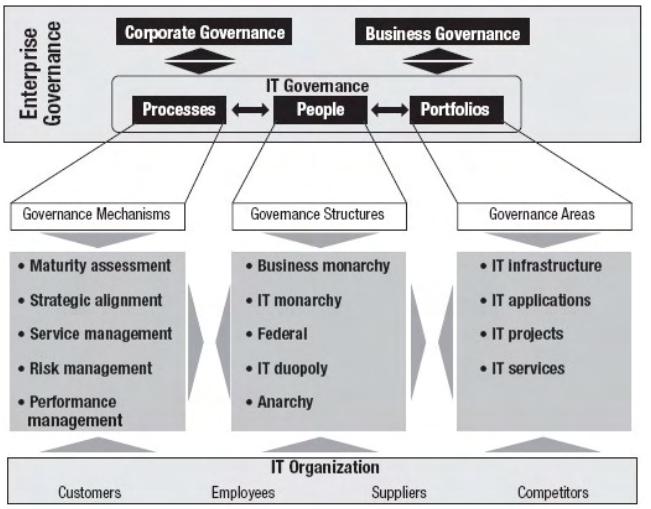
對於前面所提到影響資訊治理建置的 3 個問題(誰、如何、什麼)來說，這個模型提供了特定內容的要素。依賴從三個不同的面向(人員、投資組合和流程)，模型提供了核心元件(流程、架構、關注領域)設定的一般性治理框架。

人員觀點

在試圖設計一套治理框架中，第一步就要確定誰做了決定以及誰應該對這些決定加以負責。從這方面，就必須要去探討資訊組織的架構，[7] 目的在於定義資訊治理的主體時，必須要平衡現有的資訊架構。進一步而言，是要確保與主要的利害關係人及參與的團體持續有效的溝通。因此從人員的觀點，必須要整合現有的溝通機制，以及決策制定的程序。

關鍵的成功因素在於透過資訊的功能，明瞭並且整合現有決策制定的過程。一但資訊組織被定義了，接下來就是參考**圖 3** 所標示的，選取其中的一種方式，以便決定資訊投資的決策過程。[8]

圖3 –設計IT治理時以3P模型為參考



企業決策-這一類的決策過程，是將決策過程集中在一個資訊組織，資深的高階管理階層或是一組的高階管理人員，包括資訊技術長，都是委員會或資訊投資委員會的成員，它們決定所有與企業中和資訊有關的各項決策。

資訊決策-在資訊決策中，[9] 與資訊有關的決策是獨立出來的，有一個專門的資訊高階主管或是有資訊決策委員會(沒有業務代表)。資訊決策大部分是考量資訊架構或基礎建設的決定，最常使用建置資訊決策做為治理架構的，就是資訊決策小組或是架構覆核委員會。

聯邦制-所謂聯邦制就是把資訊架構包含在執行階層及業務代表內，並且運作資訊部門有關的決策。

資訊壟斷 [10]-這是由資訊的高階主管，以及業務代表為成員，進而決定與資訊有關的議題，通常是由資訊治理委員會及資訊策略委員會所組成。

無政府狀態-這種是最分散的架構，每一個別的使用者，或是小單位各自依照需求來做成決議。這種模式是當個別的客戶有快速變動時才會需要。

投資組合觀點

一旦有適當的組織架構以便與資訊投資有關決策能被制定，一家公司就必須關注於資訊資產的治理。因為這個目的，所以從投資組合的觀點，參考的模型將會有以下的步驟：

1. **鑑別資訊治理的內容**-第一步要做的，就是清楚的定義並且明瞭會影響資訊治理組合管理的元素(包括應用系統、架構、服務以及專案)。因此所有資訊資產可以逐步的開始進入資訊治理的範圍內。有些資產會比以往更加重視，端賴進入到資訊治理的內容。舉例而言，改進資訊技術對企業價值的貢獻，如此將會關注在專案的有效性。當專案開始有成效之後，將會減少現有應用系統操作的成本。
2. **架構資訊資產投資組合**-實務作業上，訂立資訊治理所關注的目標是最具有挑戰性的，這是導因於資訊資產分類的成熟度很低[11]。從這樣的角度，組合是要平衡現有資訊資產的財務內容，這將使資訊資產更佳關注於資訊治理上。

流程觀點

從人員和投資組合的觀點，設定誰有權能做出決策，以及哪些領域是需要治理的。從流程的觀點，則是如何設計治理的流程，以便能讓資訊技術的使用，可以達到理想狀態，同時確保能將結果持續在組織內溝通。

雖然從人員和投資組合的觀點，參考使用的模型是強烈的依賴組織內部的文化上，但是從流程的角度，仍然有六個關鍵步驟，藉此用來設計資訊治理的流程：

- **成熟度評估**-在設計資訊治理流程時的第一步，就是衡量現行組織實際現況，和作業流程的成熟度，也就是利用成熟度模型[12]。無論是使用資訊治理協會或是Luftmann的資訊成熟度模型，都可以來探究現行組織成熟度的狀態，發現目前狀態與理想狀態間的差異，就可以往理想狀態邁進。這些是後續設計資訊治理模型的基礎。

- **策略結合**- 基本上來說，資訊治理的目的就是要將資訊的功能與企業相連接，所以就必須要結合企業策略。最佳實務就是利用平衡計分卡，藉以設計資訊治理的作業流程[13]，另外也可以使用投資核准流程或是COBIT對應目標來執行。[14]

- **服務管理**-服務管理的機制強調資訊技術與客戶之間的關係，主要包括資訊服務提供和資訊需求管理。資訊服務管理包括定義服務水準協議(Service Level Management)，或是服務水準協議(Service Level Agreement)的制訂，目的是要將資訊服務定義出雙方都可以接受，同時可以追蹤的量化指標，ITIL(Information Technology Infrastructure Library)是一個設計框架[15]很好的工具。

- **風險管理**-如果沒有適當的風險管理，策略就不能有效的結合，策略結合的機制強調價值的建立，而風險管理則是強調保護現有價值。由於越來越多的組織，是把價值建構在資訊技術上，因此風險與資訊技術必須要成功的整合，相對組織而言也較越加的成功，依據風險等級定義出風險管理框架[16]，以及作業風險管理框架。

- **績效管理**- 在談績效管理之前，一定要談到量測。在這方面，持續的衡量資訊治理的決策和執行是一件很重要的事。透過績效管理的機制，就可以明瞭所參考的模型中，所強調的流程遠景結果，以便在整個組織交流的過程中，進行監控與測量的

重要性，最經常使用到的就是 Val IT 的架構[17]。

●溝通/ 關係機制-在大型企業中，造成資訊治理最大的絆腳石，就是缺乏明瞭決策制定的過程是如何制訂的?那些流程需要被定義?又有那些是想要達到的狀態。進一步來說，企業內有些小的資訊需求，但這卻和利害關係人間有著巨大的關係，這時就必須要透過資訊治理才可以得到效益。企業與資訊人員之間，藉由雙向的溝通以及良好的觀察，以便能發揮更大的效果。要注意這不是一步就可以達成的，需要透過前面三個觀點所參考的模型做為基礎。溝通和關係的機制是為了平衡需求管理、人員輪調、交叉訓練，以及 CIO 及資訊治理辦公室間定期的溝通。

當大型組織中，已經不再強調哪些人和如何去做資訊治理時，那麼流程就已經變成關鍵的項目之一。尤其是對流程成熟度較低的企業，同時 3P 模型也提供了一個替代性的綱要。因此 3P 模式藉由 3 種不同的觀點，很容易被選為資訊治理建置時的核心元件。

結論

資訊治理在企業治理中如果要能成為主要的成功因素，端視資訊治理能否有效的建置，並且瞭解資訊治理和企業治理間的關聯性是有必要的。同時，在設計資訊治理的框架時，須將關鍵問題在建置時一併考量。

有越來越多建置資訊治理框架的最佳實務經驗被提出來供大家參考，如何針對企業所需要特定的資訊治理而加以建置，這樣的經驗還是相對較為缺乏。3P 模型可以藉由四個主要步驟來縮短之間的差異：

- 針對現有治理的架構，辨別資訊治理主要驅動的項目，並且辨別成熟度。
- 當建置資訊治理有關的委員會時，需要平衡一下現行其他的委員會。
- 將資訊治理的驅動因素，放在資訊治理主要關注的區域。
- 在關鍵的地方選擇適當的機制。

參考資料

Van Grembergen, Wim; *Strategies for Information Technology Governance*, Idea Group Publishing, USA, 2004

Weill, Peter; Jeanne W. Ross; *IT Governance—How Top Performers Manage IT Decision Rights for Superior Results*, Harvard Business School Press, USA, 2004

White, Terry; *What Business Really Wants From IT—A Collaborative Guide for Business Directors and CIOs*, Elsevier Ltd., UK, July 2004

【註】

[1] IT Governance Institute, COBIT ® *Quickstart, 2nd Edition*, USA, 2007, *www.itgi.org*

[2] Peterson, R.; “Integration Strategies and Tactics for Information Technology Governance,” Strategies for Information Technology Governance, Idea Group Publishing, USA, 2004

[3] Van Grembergen, Wim; “Introduction to the Minitrack IT Governance and Its Mechanisms,” Proceedings of the 35th Hawaii International Conference on System Sciences, 2002

[4] IT Governance Institute, *www.itgi.org*

[5] CIMA, “Enterprise Governance—A CIMA discussion paper,” 2004, www.cimaglobal.com/cps/rde/xbcr/SID-0AAAC544-0F6A361A/live/tech_dispap_enterprise_governance_2004.pdf

[6] The Chartered Institute of Management Accountants (CIMA), “The CIMA Strategic Scorecard,” *www.cimaglobal.com/cps/rde/xbcr/SID-0AAAC544-0F6A361A/live/tech_dispap_CIMA_strategic_scorecard_0305.pdf*

[7] Symons, Craig; "IT Governance Framework," white paper, Forrester Wave, 2005

[8] Weill, P.; Jeanne Ross; "A Matrixed Approach to Designing IT Governance," *MITSloan Management Review*, vol. 46, no. 2, 2005

[9] An IT monarchy differs from a business monarchy in that the decisions in an IT monarchy are always made strictly by IT representatives. No business representatives take part in the decision-making process.

[10] A duopoly differs from a federal model in that a federal arrangement always has both corporate and local business representation, while a duopoly has one or the other but not both and always includes IT professionals.

[11] IT Governance Institute, *Enterprise Value: Governance of IT Investments*, The Val ITTM Framework, USA, 2006, *www.itgi.org*

[12] Luftman, Jerry; "Assessing Business—IT Alignment Maturity," *Strategies for Information Technology Governance*, Idea Group Publishing, USA, 2004

[13] Van Grembergen, Wim; "Linking the IT Balanced Scorecard to Business Objectives at a Major Canadian Financial Group," *Strategies for Information Technology Governance*, Idea Group Publishing, USA, 2004

[14] IT Governance Institute, COBIT 4.1, 2007, *www.itgi.org*

[15] Central Computer and Telecommunication Agency (UK), ITIL, *www.itil-officialsite.com*

[16] Office of Government Commerce, *Management of Risk: Guidance for Practitioners (M_o_R)*, *www.ogc.gov.uk*

[17] IT Governance Institute, Val IT, *www.isaca.org/valit*

作者簡介

Bop Sandrino-Arndt, CISA, PMP
is manager of the IT strategy and governance practice at Maxence (*www.maxence.de*), a Dusseldorf, Germany-based business consulting firm specializing in the pharmaceutical industry. He is an internationally operating management consultant with more than 10 years' extensive experience in the field of IT strategy consulting, especially in the areas of large project and program management, IT governance and effectiveness, and IT support in mergers and acquisitions. He can be reached at bop.sandrino-arndt@maxence.de.

Information Systems Control Journal is published by ISACA. Membership in the association, a voluntary organization serving IT governance professionals, entitles one to receive an annual subscription to the *Information Systems Control Journal*.

中華民國電腦稽核協會

Information Systems Control Journal

摘譯文章第 4 期　民國 99 年發行

發 行 人：黃明達

總 編 輯：張碩毅

編輯委員：李順保、林宜隆、花俊傑、高進光、陳立群、陳禮炫、黃士銘、劉其昌、歐進士

發 行 所：中華民國電腦稽核協會

Information Systems Audit and Control Association Taiwan Chapter

授 權 者：Information Systems Audit and Control Association

寄 件 處：11070 台北市信義區基隆路一段 143 號 2 樓之 2

電子信箱：isaca@caa.org.tw

電　　話：(02) 2528-8875

傳　　真：(02) 2528-8876

網　　址：www.isaca.org.tw

信賴資訊系統，獲取珍貴價值

Taiwan Chapter

會 址：台北市信義區11070基隆路一段143號2樓之2

2F.-2, No.143, Sec. 1, Keelung Rd., Xinyi Dist.,Taipei, Taiwan, R.O.C

Tel：886-2-2528-8875 Fax：886-2-2528-8876

Website : www.isaca.org.tw