Feature

資訊治理的七個迷思
Seven Myths of Information Governance

作者: **Vasant Raval, DBA, CISA,**

is a professor of accountancy at Creighton University (Omaha, Nebraska, USA). The coauthor of two books on information systems and security, his areas of teaching and research interests include information security and corporate governance.

Greg Dyche.

is IT director of Nebraska Methodist Health System and an adjunct professor at the University of Nebraska at Omaha (USA).

譯者:周濟群,台北商業技術學院會計資訊系 副教授

”治理”一詞隨著使用者的角度而有不同詮釋。在機械工程領域中，”governor”是指機械（系統）的回饋裝置，可用於速度、壓力或溫度的自動控制（譯按：如調速器）。而依ISACA 的定義，治理可確保”在決定平衡、共同協議的企業目標時，利害關係人的需求、情況與選擇能被納入考量；藉由優先權與決策制訂來設定方向；以及監督協議方向與目標的達成績效和遵循。[1]”從本質上來說，治理的角色即在於授予主理人（principal）監督與控制代理人（agent）行為的權力。以公司治理為例，主理人－通常指股東－的代表為董事會，其被授予的責任即為監管管理當局。公司治理的目的為說服、促使、強制或激勵企業管理者遵守其對投資人之承諾。[2] 除了上述這些高階定義以外，在討論治理觀念時也必須考量不同的企業特性（如：公開或私有公司、大型、小型公司或合夥）、行業（如：醫院、政府、合作社、非營利機構）與利害關係人（如：股東、客戶、員工、社會大眾）。[3]

有趣的是，治理同時也用於表達某機構組織內部的監督與控制。用於此時（譯按：狹義），治理乃成為企業整體治理的子集合。例如，企業整體治理包含了資訊治理－資料擷取、資料儲存與建立、以及資訊分派與使用的監督和控制。資訊治理也包括資料治理。[4] 當某個主要科技革新成為經濟的關鍵動因時，革新就可能帶來自己的治理問題，例如：雲端運算治理。如此多元化的治理觀點可能導致討論上的混淆與適得其反，必須清楚界定。在本文中，”治理”乃指資訊治理而言，將探討若干與治理有關的迷思與誤解。

治理的兩大焦點：資源與流程、企業價值

COSO 委員會定義”企業風險管理”（ERM）如下：[5]

> *企業風險管理是一個流程，乃是由一個機構的董事會、管理當局與人員所決定，可應用於策略制訂且範圍及於整個機構，主要是設計用於確認有那些會影響機構的潛在事件，並在風險胃納內管理其風險，以提供機構目標能達成的合理保證。*

治理的概念伴隨著 ERM 的監督，因此其本質上即為策略性的，且可藉由流程驅動以達成預計目標。因此，治理即為如何確保流程的控制無虞，且能持續地達到企業價值（BV）攸關的目標。”控制無虞”和”能達到預期結果”即為治理流程的兩大相關、但卻不同的焦點目標。資源與流程焦點是指控制資源與流程的風險；企業價值焦點則是指監督與創造 BV 有關的決策。雖然在概念上是分離的，但兩者彼此相互影響，主要是因為任何

可達成 BV 的流程都可能伴隨著額外的風險與控制。例如，企業購併或可增加 BV，但也會由於機構變大，而增加了控制資源和流程的需求。

在資訊治理領域中，資源和流程焦點是指控制資訊相關的資源和流程，以減輕風險暴露並達到系統的績效目標。此項焦點用以確保 IT 資源與流程的績效與風險管理。通常透過檢視成本預算來達成。同時，BV 焦點則針對系統行為的控制，以確保使用者能取得預期的產出資訊。資源和流程焦點著重於產出資訊的流程，而 BV 焦點則著重於如何使用資訊以產生企業價值。

IT 資源和流程的課責較 BV 的創造更易確認與衡量。BV 是透過組織而產生的，IT 可以協助其促成，但可能並非唯一或主要的角色。由 IT 投資所產生的 BV 並非由 IT 實現的，而是由企業面創造的 [6]，有時則以科技為配角。BV 焦點則與行動者（actor）有關，而非資訊的創造者（creator），行動者會應用資訊以提供商品、服務以及制訂、輔助決策等價值創造活動，可能也會產出更深入的資訊或智慧。[7]

有了 IT 資源和流程焦點，系統開發、實作、維護和控制監督才可以減輕產出資訊的系統與流程的風險。另一方面，BV 焦點則以財務數字的方式影響著組織的價值績效。這些產出（如：財務報表中的彙總）也必須適當地加以衡量、監督與揭露。因此，資訊資源管理主要乃是由 IT 資源和流程焦點的創造者所驅動，而 BV 的產出則是由 BV 焦點的使用者所驅動。

由於資訊創造者的課責（如：強調成本控制）與行動者的課責（如：成本節省、額外利益、投資報酬）在本質上就不同，故通常將產出資訊的資源、流程和 BV 的增加這兩者分開討論較為方便。以外部查核會計師為例，他們會提供給受查者關於控制架構（資源和流程焦點）的意見，而隨之而來的則是對於財務報表（BV 焦點）表達意見。

這兩個焦點彼此有重疊且交互影響。以是否要將 IT 服務外包至雲端運算環境的決策為例。這個決策可能導致成本降低而改善了營業利益－BV 衡量。但此決策也會帶來必須加以評估與減輕的新風險，同時亦會影響用以創造資訊的資源和流程之風險。雖然決策通常與兩者皆相關，但了解兩者之不同，並提供必要的異質性控制，對於有效掌握資訊治理是很關鍵的。

若由廣義的角度使用”資訊治理”一詞，通常會引發讀者隱含的假設性焦點。到底焦點是置於創造資訊或是使用資訊產出的資源與流程控制？雖然兩者分別處理是最好的方式，但仍必須清楚如何達成各自目標以及兩者分別影響之區域。本文將探討關於資訊治理的若干觀念誤解、提出關鍵觀點並建議如何克服錯誤觀念。因此，前四個迷思主要皆針對兩大焦點在觀念區辨上的錯誤來加以釐清。

”組織某部份的每個行動皆同時伴隨著風險與機會，且兩者皆需加以管理。”

迷思 1：風險與機會是分離的

組織的每個行動都會涉及風險與機會 [8]，而且這兩者皆須妥善管理。當受到機會誘惑時，不應忽略了企業決策所改變的風險情況。因此，風險與機會不能分離，只考慮其一都是不能接受的。若某企業只看機會而忽略風險，則風險主管（CRO）可說是失職的，因為風險管理並未如機會追求般同等地被評價。[9]

通常問題發生於以為與資源、流程有關的風險治理，是與 BV（BV 焦點）無關的。風險管理相關決策應該與利用機會改善實質績效的決策相連結。以外包雲端服務為例，其風險衡量應視為流程評估，而利用機會則可以成本節省的現值來衡量。由課責面來看，風險可能在某一區域（如：資訊長）而財務績效管理則在另一個區域（如：財務長）。因此，一個新機會所產生的負擔可能完全由一個區域承擔，但潛在效益卻歸於另一個區域。即使一般都了解風險與報酬應該對

等，但在現實中，風險與效益課責仍可能分開而且永遠難以整合。

”監督風險與機會...不是一次性行動，而是一個旅程。”

可為資訊治理提供完整結構的理論架構為 COBIT 和 Val IT [10]。大致上來說，COBIT 傾向於資源和流程焦點，而 Val IT 傾向於 BV 焦點。雖然兩種架構支援各自獨特的治理需求，但彼此間必須存在有效且持續的對應。某些衡量指標或可用於此。例如，企業關鍵績效指標（KPIs）即可與 IT KPIs 對應，而適當的平衡計分卡（BSCs）亦可用於連結企業與 IT KPIs。[11, 12] 雖然這些步驟有助於兩者間的對應，但發展出一個介於 COBIT 4.1 和 Val IT 之間、系統性且全面性的”橋樑”，方能達到最大效益，正如同 COBIT 5 所做的。這樣的橋樑可同時提供給資訊創造者和行動者溝通的基礎，以便釐清兩者間的課責。

迷思 2：以治理為目標

如前所述，治理可依據預期目標，保障性地監控每個正在發生或將發生事件的風險與機會面。它並不是一次性的事件，而是一個旅程。以資源與流程焦點來說，若不能持續地評估控制架構且無法進行必要適當的更正行動，則可能造成新風險無法減緩，卻仍一直進行對組織已不重要的風險控制。從 BV 焦點來說，企業策略與價值創造的持續革新是不可避免的，因此也不是一次性事件。

某種程度上來說，以治理為目標的這種印象，可能是來自於大家認為一旦控制設計好後，它就會持續有效地減輕風險，因此唯一需要持續關心的事只有如何創造 BV，而非風險減緩。也有可能是因為負責資訊治理者並不認為資源與流程焦點控制架構的持續評估和對應符合成本效益原則。一旦控制架構到位，他們可能因已存在的控制而感到滿意。但必須要摒除這種不再重新審視既存控制的心態，尤其是當公司經營面臨重大營運、戰略或策略改變等對未來產出有重大衝擊的事件時。例如，若某公司決定要裁減數百名員工，此決策可能會改善財務績效，然而也可能因為關鍵員工離職而形成流程控制中的潛在缺口。

事實上，遵循行動不會停頓下來。為了確保持續地遵循，像是 Deming 的 PDCA（Plan-Do-Check-Action）循環應該是值得參考的模型。[13]

迷思 3：法規遵循是主要產出

遵循和法律在社會和商業活動中佔有一席之地。缺少了法令規範則很難要求企業做到該做的事。也因此我們可能給予美國法氏法案或歐洲 Basel II 協定等強制企業達到的治理門檻過高的評價。

因此，訂定了治理標準的法規遵循乃形成了壓倒性的力量。最近，某些美國國會議員鼓勵美國證管會（SEC）強制企業揭露資訊系統的資料外洩等相關事件。額外的監督和揭露負擔可能導致董事會等治理權威單位感覺只要符合法令規範即足夠。”[14] 一個常被提及的迷思或誤解是認為好的治理...可能會花費很多時間和成本。這種論調通常是由某些認為治理只是沈重的遵循的人所提出的。”[15] 這種認知進一步地強化了做再多的遵循也只會多花成本、不會帶來有形效益。因此組織就不會把額外的治理衡量為有附加價值的行動。

然而，最首要的是，治理通常被認為有利於所有權人。因此，僅止於遵循之門口卻不再多做些什麼是令人失望的。例如，SEC 近來強制公開發行公司必須採用以 XML 為基礎的 XBRL 標籤來滿足主管機關的報告需求。企業有兩種方法來完成：使用”固接”方式將最終報告標籤化或將標籤嵌入企業的總帳系統中。後者對於企業來說較有潛在效益，因為標籤化的資料可用於進行有效率和效果的管理決策。通常來說，大部份企業傾向於使用固接式的捷徑，而不會考慮到採用後者最終所能帶來的效益。結果則是能夠使用標籤來追踪交易（例如：編製以預計和實際績效比較的內部報表）的效益不會被選上，唯有法規遵循

需求被滿足。

”經營和資訊科技領導者應該強調客製化方法。”

與風險管理和揭露有關的法令規範僅設定了全面性、一般化的最小需求。如果存在好的治理，則滿足法規需求可能只是最低水準。在這種情況下，遵循可能只是附帶的效果，而非主要產出。

最後，法規遵循本身可能只投射出資源與流程焦點，不足以執行企業的經營策略。而 BV 焦點則是與資訊治理不可分離的。

解除這個迷思，經營和資訊科技領導者應該強調使用客製化方法來滿足企業內的各項需求，以便產生超越法規門檻的綜效。這也就是為何高階管理者的聲音－包括陳述、聲明、管理當局的解釋和行動等的一致性－對於有效治理是如此重要。[16]

迷思 4：治理與經營績效是分離的

本迷思乃是第一個迷思的推論結果。在組織中，我們或許認為減輕風險主要是與資源與流程有關。但藉由管理行動而產生 BV 的 BV 焦點，也是治理中不可分離的一部份。是否有可能管理當局配置了不成比例的權重於資源與流程焦點，而犧牲了 BV 焦點。由於貨幣性收益通常並非資訊系統管理的焦點，因此風險治理通常以成本為課責目標，而非收益或利益。此外，機會的治理則通常被視為是一種收益、利益或投資中心。這些觀點會通常引發不同的反應，因為成本控制主要是預算考量，而非策略計畫。[17]

這樣的二分法－資源與流程相對於 BV－可能導致我們邏輯上認定風險治理領域與機會治理是分離的。兩者間的不相容可能更增加了彼此融合對應的難度。例如，將某些交易處理系統委外給國外廠商每年可能節省大量成本。當管理者認定這是一個可降低成本和改善利益的吸引人方案時，也應該要解決相關的治理風險議題。例如，誰擁有客戶資料、這些資料安全性如何，且若未來打算與委外廠商解約時會如何？[18] 很明顯地，即使某些案例中，與資源和流程有關的風險管理（資訊創造者）似乎與善用機會（資訊行動者）互斥，但風險與機會的治理其實是無法分離的。

不論治理型態的衝擊為何，皆應由負責風險與機會兩個領域的管理者，審慎地評估這兩者。在第一個迷思中所建議的指引亦可應用於此。而且在 COBIT 架構中所推薦和解說的責任、課責、諮詢與／或知會（RACI）圖也是一個能克服本迷思的有效整合機制。[19] COBIT 5 闡明了如何將代表企業價值聯結的企業目標轉化為能減輕資源與流程風險的 IT 相關目標。[20]

迷思 5：治理是一種全有或全無的

在觀察如 COBIT 這類縝密的架構時，我們可能同時會感到深刻和困惑。COBIT 是一個很強大的架構，但卻無法在短時間內達到其潛在利益。它需要長期時間才能將架構調整至正確。這樣的挑戰使得某些人全盤放棄，因為建置架構的工作看來十分可觀。另一方面，任何控制皆有可能在缺乏嚴密的控制架構下到位，但卻可能只是隨機的、設計或作業上有瑕疵和不夠整齊劃一。為了確認和填滿這些缺口，必須應用控制架構。放棄不用控制架構長期可能適得其反。即使對控制架構的效益仍有疑慮，美國公開發行公司仍受到法律規範，必須建置與財務系統相關的適當內部控制。

即使控制架構對於紀律化的風險管理是必要的，但卻不必然要在每個領域目標同時生效。只要藍圖和綜覽十分清楚地揭示，可以先處理那些控制效果有嚴重缺失的目標。一旦風險暴露已經過評等和優先權化，即可排定行動的優先權。這就是採取允許按步就班、分頭克服的方法來建置整體的控制架構。適地性的行動方案可以強化風險管理是所有人的事情，而非只是風險長的責任。雖然由上而下來規劃控制架構建置幾乎是必要的，但個別控制建置的順序則未必一定如此。只要拼

圖中的每項工作都已確認，則依優先順序來建置即適當且有效。

為了避免資訊治理架構的負面偏誤，可以進行先導計畫專案。在小團隊、小系統或小區域中執行一項可達成遵循的先導專案，可提供方法論的再度保證，並可在未來整個組織導入時，作為能協助閃避相關陷阱的範例。[21]

迷思 6：好的治理一定得依賴新科技

科技的進步如此令人印象深刻，因而導入新科技對於組織而言是勢在必行。新科技同時也會創造出如綠色行動、能源節省、生產力改善和較佳安全等顯著相對效益。而科技廠商在過了一段時間後，可能不再支援舊版、且與最近購入科技不相容，而現有系統可能也開始令系統與管理專業心灰意冷。基於上述原因，導入新科技似乎很吸引人。總而言之，如同常被規範的，導入科技是營運用途，而非為導入而導入。導入新科技的理由必須來自於它能為企業帶來 BV。若導入新科技的著眼點在於資源與流程焦點，而非 BV 焦點，則可能較不易成功。

為了達成有效治理，可能會導入新科技，但並非勢在必行。一般來說，若使用一項可與現有技術相容的新科技，能在符合成本效益原則下達成某個風險暴露的減輕，則是可以支持的。很明顯地，雖然新科技能使治理變容易或改善它，但有效治理並非新科技的產物。若某項新科技與現存科技大不相同，則風險治理可能帶來更大的挑戰。

迷思 7：好的治理需要獨立分離的資金

好的治理無法缺乏資源配置，然而若假定每個治理衡量皆必須由分離的預算來支持則是一種誤導。事實上，應用 BV 焦點的管理者，通常在思考善用機會所需要件時，如何減輕相關風險也是其整體行動的一部份，並非分離的行動。因此，每次在組織善用機會時，其風險治理的支出預算並不會有重大改變。

但這種管理行為可能導致由管理決策所引發的新風險未能被察覺，因此也無法處理。這種情況無論新風險是否需要額外資金都可能會發生。一種強制發現風險和如何處理它的方法，是將風險相關資源與流程決策的潛在衝擊納入 BV 的評量流程中。

結論

清楚地理解這兩項治理焦點－產生資訊的資源與流程和 BV－乃是企業各階層在處理資訊治理的關鍵前提。若無法明確區分兩者，則爭論會隨之而來且可能因為每個人所認定風險的假設不同，有的是看資源與流程相關風險，有的則是看 BV，而導致採行了不同的方法。ISACA 近來出版的 COBIT 5 則將此兩種觀點整合為一，因此可以將企業 IT 治理（GEIT）簡化為統一的方法。

某些迷思或錯誤觀念是導因於這種治理二分法的疏忽或其它類似的概念。本文舉出七個此類迷思，並盡可能地建議解決之道。企業的風險管理計畫有可能因為此種誤解或偏見而不效率，應該經由系統化的溝通來加以排除，才能把它們對於組織治理的影響降到最低，甚至消弭。

ENDNOTES

1 ISACA, COBIT® 5, USA, 2012, www.isaca.org/cobit
2 Macey, Jonathan R.; Corporate Governance: Promises Kept, Promises Broken, Princeton University Press, USA, 2008
3 Hilb, Martin; New Corporate Governance: Successful Board Management Tools, Springer, Germany, 2005
4 Khatri, Vijay; Carol V. Brown; "Designing Data Governance," Communications of the ACM, vol. 53, issue 1, January 2010
5 Committee of Sponsoring Organizations of the Treadway Commission, Enterprise Risk Management—Integrated Framework, USA, 2004

6 De Haes, Steven; Wim Van Grembergen; "Moving From IT Governance to Enterprise Governance of IT," ISACA Journal, vol. 3, 2009, www.isaca.org/journal
7 Kooper, M.N.; R. Maes, E.E.O. Roos Lindgreen; "On the Governance of Information: Introducing a New Concept of Governance to Support the Management of Information," International Journal of Information Management, vol. 31, no. 3, 2011
8 Raval, Vasant; Ashok Fichadia; Risks, Controls and Security: Concepts and Applications, Wiley, USA, 2007
9 Protivity Inc., "Positioning the CRO for Success," Board Perspectives: Risk Oversight, USA, 2010
10 The scope of governance and management of enterprise IT (GEIT) practices addressed in Val IT and Risk IT are now an integral part of COBIT 5 (www.isaca.org/cobit), such that COBIT 5 can act as the framework by which enterprises can identify the GEIT needs of all stakeholders and balance short- and long-term enterprise goals effectively.
11 Robinson, Nick; "The Many Faces of IT Governance: Crafting an IT Governance Structure," Information Systems Control Journal, vol. 1, 2007, www.isaca.org/archives
12 Rouyet, Juan Ignacio; Willem Joep Spauwen; Luis Joyanes Aguilar; "Using COBIT 4.1 to Achieve Business-IT Alignment: A Practical Approach," JournalOnline, ISACA Journal, vol. 1, 2010, www.isaca.org/jonline
13 Annaswamy, Subramanian; "A Road Map for Regulatory Compliance," ISACA Journal, vol. 4, 2009, www.isaca.org/archives
14 Kelley, Diana; "Risk of Breaches: Congress Asks SEC to Intervene," SecurityCurve, 13 May 2011, www.securitycurve.com/wordpress/archives/4125
15 Barnier, Brian; "Driving Value From Nonrevenue-generating Activities: Myths and Misunderstandings of Governance and Risk Management," ISACA Journal, vol. 2, 2009, www.isaca.org/archives
16 Bruinsam, Christine; Peter Wemmenhove; "Tone at the Top Is Vital!—A Delphi Study," ISACA Journal, vol. 3, 2009, www.isaca.org/archives
17 IT Governance Institute, "Excerpt: IT Governance Roundtable: Brisbane September 2008," ISACA Journal, vol. 3, 2009, www.isaca.org/archives
18 Raval, Vasant; "Risk Landscape of Cloud Computing," ISACA Journal, vo1. 1, 2010, www.isaca.org/archives
19 ISACA, "COBIT: Transforming Enterprise IT," USA, 2009, www.isaca.org/knowledge-center/cobit/documents/cobitoverview.ppt
20 For some examples, see ch. 2, p. 21 of COBIT 5, ISACA, 2012.
21 Op cit, Annaswamy

Quality Statement:
This Work is translated into Chinese Traditional from the English language version of Volume 4, 2012 of the ISACA Journal articles by the Taiwan Chapter of the Information Systems Audit and Control Association (ISACA) with the permission of the ISACA. The Taiwan Chapter assumes sole responsibility for the accuracy and faithfulness of the translation.

品質聲明：
ISACA臺灣分會在ISACA總會的授權之下，摘錄ISACA Journal 2012,Volume 4中的文章進行翻譯。譯文的準確度及與原文的差異性則由臺灣分會獨立負責。

Copyright

版權聲明：

Disclaimer:
The ISACA 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 ISACA Journal.

Opinions expressed in the ISACA Journal represent the views of the authors and advertisers. They may differ from policies and official statements of ISACA and/or the IT Governance Institute and their committees, and from opinions endorsed by authors' employers, or the editors of this Journal. ISACA Journal does not attest to the originality of authors' content.

Instructors are permitted to photocopy isolated articles for noncommercial classroom use without fee. For other copying, reprint or republication, permission must be obtained in writing from the association. Where necessary, permission is granted by the copyright owners for those registered with the Copyright Clearance Center (CCC), 27 Congress St., Salem, MA 01970, to photocopy articles owned by ISACA, for a flat fee of US $2.50 per article plus 25¢ per page. Send payment to the CCC stating the ISSN (1526-7407), date, volume, and first and last page number of each article. Copying for other than personal use or internal reference, or of articles or columns not owned by the association without express permission of the association or the copyright owner is expressly prohibited.

免責聲明：
ISACA Journal係由ISACA出版。ISACA 為一服務資訊科技專業人士的自願性組織，其會員則有權獲得每年出版的ISACA Journal。

ISACA Journal收錄的文章及刊物僅代表作者與廣告商的意見，其意見可能與ISACA以及資訊科技治理機構與相關委員會之政策和官方聲明相左，也可能與作者的雇主或本刊編輯有所不同。ISACA Journal 則無法保證內容的原創性。