Feature

COBIT 為基礎的法規遵循及預防性處置

A COBIT Approach to Regulatory Compliance and Defensible Disposal Understanding the Core Concepts in COBIT

作者: Lorrie Luellig, J.D., of Ryley Carlock & Applewhite, is the founding member and practice leader of Information Governance (RCA-IG) PC, faculty member of the Compliance, Governance and Oversight Council (CGOC), and leader of the Electronic Discovery Reference Model (EDRM) IGRM Corporations Subgroup and CGOC RIM WorkGroup. Luellig advises global clients from Fortune 100 to small privately held companies headquartered in

Jake Frazier, J.D., is the information life cycle governance expert for IBM and is the program director, legal and e-discovery for the CGOC. Frazier provides assistance to corporate legal departments and law firms in identifying, evaluating and implementing in-house e-discovery and information governance solutions.

譯者: 張碩毅,電腦稽核協會編譯出版委員會主委,國立中正大學會計與資訊科學系,教授兼系主任

成功的 IT 治理計劃需要以一個現代且透明的方式進行資料保存和例行的處置。現今的資訊長（CIO）面對著前所未有的挑戰：

- **巨量資料**：由 IT 所收集和管理的資訊不斷膨脹，不斷測試著收集、分析、存儲、處理和資料歸檔的流程和工具。
- **全球化**：現在你幾乎不可能找到所有部門都集中在同一區域的大型企業。企業的總部、研發和製造部門可能分隔上千里，而客戶、合作夥伴、供應商和衛星辦公室可能散佈在世界各地。因此，資訊科技必須支援存儲在各地及各種基礎架構上的資訊，例如:網路、伺服器、桌上型電腦、筆記型電腦和行動裝置。
- **複雜、不斷演進的規範**：超過 10 萬條的國際法規和規章與富比士全球 1000 大企業所蒐集的資訊有直接或間接的關聯。這些資訊包括財務資訊，市調資料，電子郵件，文件，社群媒體文章，Twitter 訊息，通話記錄，log 紀錄等。許多規章，包括對財務資訊揭露、資料保存和隱私規範的要求，一直不斷地在變化，甚至因為跨越國界和司法管轄權造成許多規定相互矛盾。這使得企業在面對這些規章時更具挑戰性。
- **緊縮的預算**：儘管面對眼前這些挑戰-如果無法遵守全球性的規範並且成功的管理資料的話，這將會導致一場災難性的後果-面對這些持續性壓力 IT 的預算還是被限縮了。IT 能夠面對這些挑戰提供全面、全球化的資訊治理方案，減少資料量，集中管理分散在各司法管轄區的資料，並確保法規遵循—同時降低成本。許多 CIO 們已經在使用 COBIT® 架構，用以支援業務目標、降低企業風險、將資源做最佳化利用。但是當涉及到監管問題、法律遵循，記錄保留和處置策略相關的資訊管理規範，COBIT 的原則往往無法盡可能地被有效和廣泛利用。然而 COBIT 可能是成功的關鍵治理方案。

無價值的企業資料

無法洞察哪些資訊需要保存，導致企業積累許多資料碎片，需要額外申請伺服器，存儲空間和備份磁帶去保存那些不再具有任何效用的資訊。

治理和監督委員會（CGOC）[1]近期一項對企業資訊長和法律總顧問的法規遵循調查發現，通常企業儲存的資訊中，只有1%是為訴訟保留，5%是記錄保留類別和其中的25%目前具

有商業價值[2]。這意味著，大約有69%組織所收集和保存的資料都不具商業、法律或控管價值可言。

為了依合乎法律規定的預防性處置處理任何事，創造一個成功資訊治理方案的關鍵步驟就是建構出一對任何具有商業、法律或控管價值資訊的識別和保護的能力。有效的預防性處理—將定期自動刪除，沒有控管、法律或商業價值的資訊—這對資訊的經濟效應產生了重大的影響。更少的IT預算用於存儲、伺服器和備份，意味著有更多的資源可以進行策略性投資。需要篩選的資訊更少意味著，法律和監控得以更精簡、以更高的效率進行處理，同時可以減少儲存過多或過少的資料所帶來的風險，還有對資訊保存要求不斷變化的隱私法規，法規要求我們刪除的資料我們就必須予以刪除，以免被對方的律師發現我們所擁有的資料比規定的還多。減少資訊管理的浪費，最終能使企業將更多的利潤回饋給股東。

在過去保存計畫只包含檔案—無論是紙本還是電子檔—但這與組織中其餘的資訊是截然不同的。為了達成預防性處置，IT利害關係人必須能緊密且無保留的和檔案與資訊管理（RIM）、法律、業務單位合作，建立現代化且可執行的計畫—制定資料需要保存超過保留期限的標準。“檔案”被認為應包括組織中的所有資訊，並納入法律和商業價值有關的資訊作為保留標準。

數位世界中的保存計畫

一個保留計劃提供了檔案管理的規範，法律部門必須視公司規定和業務的需要制定這些檔案需要保留多少時間。問題是許多組織在制定現行的保留計劃時，使用紙本檔案還是普遍的現象。

然而，他們根本不清楚現今的企業，因為電子化所產生大量需要保存或刪除資料，包括在過去沒有被定義必須視為一個檔案，例如，社群媒體的文章和Twitter訊息。這將造成一個關鍵的疏離，因為資訊是包含在IT的構面中，公司中包含成千上萬的應用程序、資料庫和其他IT管理都須遵循義務。同時，法律和RIM專家們擁有專業知識，他們根據相關法律、法規制定的保留計劃和處置政策，但他們可能無法綜觀所有的IT基礎架構或理解現有資訊所擁有的商業價值。應該訂定一套判別相關資料是否應該進行處理的機制。

- 有一種不恰當的現象是CGOC所特別強調的，調查顯示：[3] 77%的受訪者表示，他們保存計劃是不可以透漏給業務和IT人員
- 50%的人表示他們的IT部門沒有使用保存計畫
- 75%的受訪者沒有能力對資料進行預防性的處理是他們最大的挑戰之一，他們進一步強調巨量的舊資料造成了財政上的負擔，也造成了法規遵從的困難和業務的風險。

建立一個現代化、透明並且可執行的保存計劃的目的，是為了能透過一個容易判斷無價值資訊的方法並自動以合法的方式處理以克服這些挑戰。

以COBIT架構建置一個更好的保留計畫

因為現代的、可執行的保留計劃深明電子資料的動態性，並且需同時對資訊的管理和處理負責，COBIT的原則為此提供一個堅實的基礎。對於企業IT的治理和管理，COBIT® 5是基於以下五個關鍵原則：

1. 滿足利益相關者的需求。
2. 覆蓋企業的端到端。
3. 採用單一且整合的架構。
4. 使用全面性的方法。
5. 區分治理和管理。

這些原則適用於建立一個現代化的、可執行的保留計畫，透過此架構對不再需要的資料進行預防性的處理，並考慮到法律、檔案與資訊管理(RIM)、業務需求和IT利害關係人：

- 了解企業資訊的流程-從資料的建立到處置-並採用一個全面性的方法來管理資訊。
- 了解資料保存和處置的多面性，並可讓個別關鍵的利害關係人之間相互依存和合作的關係，以滿足所有法律、規範和業務需求

- 擁有整合的治理政策和流程，以滿足各利害關係人多樣化的的需求、實現全球化，並定期更新以跟上法律和企業的變化
- 透過明確的治理政策和流程，使日常的資訊管理更加有效率以及更加的遵循性。

在這樣的環境中，使用者將擁有進行資訊分類的知識和工具，IT將合乎法律的規範，對於檔案的管理我們需要導入一個可行的計畫，並在適當的時機處置沒有價值的資訊。以下是在現今資訊化的時代保存計畫所必須包含的要素：

1. **將保留計劃應用於所有資訊，而不僅是檔案。**保存計畫應視檔案管理和資料管理的需求持續調整，並應用於組織中所有的資產。將所有資訊分類-包括結構化和非結構化的資料來源-無論是否具有法律、法規或商業價值抑或是資料碎片。
2. **將具體的法律、隱私和管理保留義務與相關資訊直接連結。**保留計畫必須輔以一個公開的全球性架構，此架構須明確定義所有類型的資訊和商業用戶的法律及監管責任，所涵蓋的範圍包括，誰有遵守的義務，以及何時保存和處置的機制將啟動。該架構還必須包括持續發展中與隱私相關的義務。技術解決方案，例如:對索引或本文進行資料分析和分類，因導入了最新的法律、隱私和管理規範，現在可以自動處理資料的保存和處置。
3. **考慮資訊的商業價值。**該價值必須由業務利害相關人明確的定義，並讓法律、RIM和IT了解。再來，技術解決方案已經存在，對於這一企業資料管理人員長期關注的議題，即幫助使用者處理相關資訊（例如，採購訂單或員工協議）與特定資料來源（例如，企業內容管理系統和人力資源系統或應用程式如微軟的SharePoint）和包括該資訊為什麼含有商業價值和具有多長時間的價值等詳細資訊。
4. **確認資訊的所在位置。**保存計畫應包含儲存資訊儲存所在位置的清單、用甚麼檔案類別進行儲存、誰必須對其內容負責、誰該管理它。在可靠的資料索引圖幫助下，資料管理員可以更輕鬆地識別資料，了解相關資訊的價值及其所需遵守的義務，例如，業務規範和部門規範。
5. **用利益利害關係人能夠理解的語言與其溝通保留和處置的義務。**這涉及兩個要素。首先，資料使用者必須知道當他們建立和識別資訊時須要注意甚麼。其次，資料管理員必須了解他們對於相關資訊的處置責任。例如:IT人員不清楚“符合HUM100的檔案”的處置規範，一個較為適合的翻譯是：“由人力資源（HR）所建立工作的應用程序，使用者資訊和其儲存在人力資源部共享的存儲裝置上的資料，必須在終止聘雇該員工10年後永久刪除。“讓人能清楚的遵循該規範。
6. **保留彈性，以符合當地的法律、義務和限制。**各專業領域和司法管轄區的企業用戶是最了解他們所創建的資訊及其所包含的價值與目的。保存計畫必須保有彈性，以適用於各地的規範。另外，保存計畫的技術解決方案，必須涵蓋所有適用地區和司法管轄區中具體的法律規範，使各種例外和變化可以被納入保留計畫，並傳達資訊給相關的利害關係人，以確保能合乎全球各地規範。
7. **在執行和終止法定保留時應包括一個可讓法律和IT能合作的機制。**若對法定保留資訊和何時法規已被鬆綁沒有清楚地了解，那麼沒有任何一個保留計劃有可能達成預防性處理的這個目標。知道的資訊存放的實體位置是非常重要的，特別是對於嚴格的協議，如在銷毀硬碟時必須全程錄影。建立資訊價值和IT間明確的關聯，法律部門會擁有來自世界各地的法定保留，並個別的檢視相關檔案和資訊確保與當地計劃一致。
8. **識別並刪除重複資訊。**不清楚到底該保存多少和保留多久所以我們傾向，“保存所有的東西，以防萬一”。除了與越來越多的隱私保護法（例如，美國健康保險流通與責任法案、歐盟的個人資料保護法），要求在一段時間後必須刪除某些類型的資訊，保存所有

的東西意味著數十甚至數百個相同的文件的備份都被保留。通過透明的治理和管理架構，企業可以確信他們已經保留了所需資料，並處置所有不必要的備份。

9. **即時更新以符合法律對業務和技術的規範。**隨著全球性的法律、法規和隱私要求不斷的發展，保持主導地位並因應新的要求立刻調整保留計畫是非常重要的。技術解決方案可以自動更新系統和提醒資料管理員相關變化。幾個主要法律資料庫的供應商，也提供工具讓用戶能夠隨著法律的變化做計畫的調整。
10. **在資料來源就自動應用保留計畫和判斷法定保留，所以現在能自動從政策工具接收指令，以及所有保留和處理流程的自動化。**這確保了不需要的資料，將有一致性的處置，使法律和RIM可以驗證保存請求和法規遵從的工作，讓資訊治理的管理者，能夠監控和改善預防性處置計畫。

橫跨所有資訊生命週期的良好治理

前所未有的資料成長、全球商業運營、成本議題以及一個複雜且不斷變化環境，為所有的資訊長帶來了一個艱鉅的資訊治理之挑戰。然而，COBIT架構使得資訊長們可以藉此有效率且符合成本效益的治理原則來克服這些挑戰，控管企業的資訊流。當資料歷經所有生命週期，將自動刪除不再具任何法律、法規或商業價值的資訊。藉由法律、RIM和公司利害相關人的合作，IT也可以幫助建立一個現代化、公開的及可執行的保留計劃，可以確保在提高業務靈活性的同時，還是能遵循計畫，降低風險、並通過預防性處理無價值的資料已降低成本。

ENDNOTES

1. The Compliance, Governance and Oversight Council (CGOC), founded by Deidre Paknad, director of information life cycle governance at IBM Corporation, is a forum of more than 1,900 legal, IT, records and information management professionals from corporations and government agencies.
2. Compliance, Governance and Oversight Council (CGOC), “Benchmark Report on Information Governance in Global 1000 Companies,” www.cgoc.com/register/benchmarksurvey-information-governance-fortune-1000-companies
3. Ibid.

Quality Statement:

This Work is translated into Chinese Traditional from the English language version of Volume 5, 2013 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 2013,Volume 5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。