使用開源工具協助科技治理

Using Open Source Tools to Support Technology Governance

作者: Ed Moyle,

Is director of thought leadership and research at ISACA. Prior to joining ISACA, Moyle was senior security strategist with Savvis and a founding partner of the analyst firm Security Curve. In his nearly 20 years in information security, he has held numerous positions including senior manager with CTG's global security practice, vice president and information security officer for Merrill Lynch Investment Managers and senior security analyst with Trintech. Moyle is coauthor of Cryptographic Libraries for Developers and a frequent contributor to the information security industry as an author, public speaker and analyst.

譯者: 李興漢, 國立臺北商業大學會計資訊系教授, 中華民國電腦稽核協會編譯出版委員會委員

當涉及到企業環境中資訊安全與確保議題時，大多數從業人員已經非常習慣使用技術工具來協助進行處置。這些技術或工具可能是開源軟體或商業軟體，舉例來說：使用者可能採用開源軟體例如：Clam、Wireshark 或 OpenVAS 去完成特定任務（病毒防範、網絡分析和漏洞評估），或者，他們可能會採用商業產品提供從入侵檢測系統（IDS）到防火牆，數據丟失防護（DLP）到雲端訪問安全代理（CASB）（以及其他）的任何功能。簡而言之，精心挑選和明智使用這些工具是從業人員的一項重要課題。

然而，當涉及到科技治理（企業IT治理 [GEIT]）時，通常很難找到可以幫助從業者的特定工具。原因不難理解。首先，根據定義，治理是一種對於不同組織需要進行客製化擬定的工作；因此，組織A如何實施治理可能與組織B有很大不同。這部分是由於不同的目標（包括企業的目標以及從各層級利益相關者需求出發的技術目標），以及用於確保持續改進的不同指標和關鍵績效指標（KPI），和不同文化和風險胃納以及其他組織相關特定因素所造成。換句話說，這也讓從業者很難找到一個萬能工具能夠同時支援不同的組織。

儘管如此，還是有一些工具可以協助從業人員朝向整體性與系統化的治理邁進。

在本專欄中，這些工具以及它們如何適用於廣泛的治理實施將被加以標示出來。此外，也會對許多的工具進行大略的概述，針對其對於組織進行科技治理時的效益。

此外，在考量預算的狀況下（特別是在預算緊縮且審查嚴謹的情況下），使用開源工具將被更為重視。但是，這並不意味著沒有商業工具可以做類似的事情或以不同的方式提供幫助；事實上，市面上有成百上千種的商業產品可以協助GEIT實施。 然而，並非每個組織都具有相同的預算支持水平（更不用說經營環境是善變的），因此，本專欄將聚焦於開源軟體。

對於實施GEIT的組織來說，考慮接受使用開源軟體可能會很困難。因為預算考量通常只算是一個小小的考慮因素，但若真的是考量到預算問題，那開源軟體將會被毫不遲疑的使用。

1 資產清單

正如每位從業人員都知道的那樣，資產管理很難做好。 因此，利用支持資產管理的工具可以在多個領域獲得廣泛的收益。 但是，在 GEIT 的背景下，支持資產管理的工具可能特別有價值。

為什麼呢？ 因為在 GEIT 部署的實施階段，組織開展了一些關鍵活動（即風險評估和評價，KPI 和績效指標的確定，適當範圍的設置）。在宏觀層面上，這些任務不會（非必要）需要知曉每個系統、應用程序或資訊環境所配置的節點的組成元件。 但是，當一個組織開始探索問題並超越宏觀層面進入更為細節的活動規劃時，就需要考慮到環境的獨特細微差別（假設人們知道其中的差異）這將可能導致稽核專案的成功和失敗。

考慮到這一點，支持資產清查和發現的工具，如 GLPI（www.ubuntugeek.com/glpi-it-and-asset-managemet-software.html）和 OCS Inventory NG（www.ocsinventory-ng.org/en/）就可能是有助益的。組織可以利用這些工具來發現他們現有的資產來協助進行風險管理工作。他們還可以用記錄中已部署的資產，比較工具所收集的資產內容，以協助建立持續的效能改進指標。更進一步，組織可以將該系統中包含的訊息與支持 GEIT 規劃實施階段涉及的所有內容聯繫起來。

2 風險管理

ISACA“GEIT 入門指南：實施企業 IT 治理入門”強調了在 GEIT 實施階段進行風險評估的必要性：具體來說，指南概述了：“執行風險評估和監測為實施 GEIT 的第一步，以確保專案風險（無論是資源承諾、預算編制還是時程規劃）得到關注，以保持計劃正常進行。“1 這表明風險評估- 並據此作出反應 - 是 GEIT 本身實施的一部分。 在這方面，也有免費和開源工具可以幫助實施。

確切來說，這方面的軟體確實不多，首先，像 SimpleRisk（https://www.simplerisk.it）這樣的工具可以協助記錄風險發生的區域並追蹤哪些部分屬於高風險，更進一步可以達到及時追蹤的功能，另外，提供將風險減輕策略與風險區域相連結的功能，並可記錄補救進展。

同樣，也有免費工具可以幫助組織了解風險因素，並識別/描述它們。例如，實用威脅分析（PTA）（www.ptatechnologies.com）工具可以幫助開發系統化的風險威脅模型，以確保組織可以系統化的查看風險。

取決於利害關係人在此過程中想要達到的級別，他們可能會利用 OpenVAS 或 Vega 等工具幫助識別應用程序和基礎架構表層上的漏洞，以便告知他們該做的風險評估取向。當然，並不是每個 GEIT 實施都會將風險評估的部分納入到執行細部選項中，但是如果組織選擇要做這件事，那工具是現成的。

3 監控

GEIT 實施的目標是為了獲得反覆的持續改進。 這意味著，透過持續監控組織—藉由將利害關係者的需求綁定其相關聯衡量指標和關鍵績效指標並提供預警功能—組織可以一目了然看到需要改進的地方，並持續在這些方面做改善。 這部分有很多可以提供幫助的選項。

首先，有很多工具可以支持持續性效能監控。 這包括諸如 Icinga 2（https://www.icinga.com/products/icinga-2/）、Nagios（https://www.nagios.org）、OpenNMS（https://www.opennms.org/en）和 Zabbix（www.zabbix.com）等工具。對於組織在進行科技治理時有興趣的效能監控相關資訊，都可以透過對話方式輕易與可靠的進行溝通。然而，從更廣泛的角度來看，Observium（https://www.observium.org）或 Cacti（www.cacti.net）等工具，可以提供更多層次的細節，具體取決於組織打算走多深。 當然，一些組織可能已經有了提供類似訊息的工具，但對於還沒有使用工具的組織而言，這些工具或許可以提供他們所需的資訊。

雖然說，進行監控對組織非常重要，但是，能夠將監控訊息呈現為組織能夠採取行動的格式也很重要。 從治理的角度來看，有助於數據可視化的工具，例如 Datawrapper（https://www.datawrapper.de/gallery）等，也可能對組織很有助益。

Endnotes

1 ISACA®, *Getting Started with GEIT: A Primer for Implementing Governance of Enterprise IT*, USA, 2016, *www.isaca.org/getting-started-with-GEIT*

Quality Statement:

This Work is translated into Chinese Traditional from the English language version of Volume 1, 2017of 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 2017,Volume 1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。

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。