以可讀性做為使員工遵循資訊安全政策的工具

Readability as Lever for Employees' Compliance With Information Security Policies

作者: **Franz-Ernst Ammann,** Ph.D., is employed by Deutsche Telekom AG. Ammann previously worked in IT strategy and conducted related assessments on the German Act to Modernize Accounting Law (BilMoG).

Aleksandra Sowa, Ph.D., ITCM, is employed by Deutsche Telekom AG. Sowa initiated the Horst Görtz Institute for Security in Information Technology, a European university-based institution for interdisciplinary research in the field of IT security, and worked as an auditor in the financial services industry.

譯者: 陳禮炫, ISACA Taiwan Chapter Supervisor, 中華民國電腦稽核協會 監事

資訊安全政策是資訊安全內部正式管理架構的一部分，也是組織機構資訊安全治理的一部分。資訊安全政策（政策涉及指引及要求）是在組織機構內指引政策及行動，以達成預定成果。這些政策被理解為告知、授權及強制執行的原則或規定。因此，人(不是政策)能確保系統、組織及資料適當及充分的安全水準。

員工要經常確認企業資訊安全主要弱點及無數安全意外原因。無論如何，員工能按照他們所了解的政策執行。可讀性是了解政策的關鍵，它依賴目標讀者的教育—在這個案例，所有員工應用到科技方法。

安全政策的影響

少數有關的努力被投入這個政策的估計及評價，無論是安全政策在稽核資訊安全遵循及設計資訊系統運作的重要角色。比起依據資訊安全政策設計的資訊系統、程序及控制，這些政策較少聚焦在內部稽核的查核。

安全政策在 IT 結構、系統及程序的設計決策是重要的。安全政策描述內部控制目的，並定義標準安全衡量。資訊安全政策說明人員行為及程序的約束。作為資訊系統設計及運作的管理工具及內部標準，安全資訊政策應落實扎根在組織治理架構。內部及外部稽核人員以外部基準、標準及通用(政府及國際)的正式管理架構，使用安全政策評估內部架構的遵循。當查核安全基準有效性時，稽核人員通常考慮其執行基準是否與安全政策一致。資訊安全稽核人員是高度專業並經良好訓練人員。他們熟練閱讀及解說安全政策。它們的理解力遠超過一般人員。在首次侃侃談論這些政策後，即使事情順利進行，還是有風險。第一波執行政策的人們經常與創作者溝通政策，更勝與涉及建立程序的人溝通。關於資訊安全效果及遵循的政策，可能證明對決定政策資訊交付給讀者是有用的。當安全意外發生時，根本原因可能是安全政策本身，例如，事實是員工無法了解政策。

資訊安全政策的品質

甚麼造成有效的資訊安全政策? 很明顯的，就是品質。名詞「品質」涵蓋多方面，包括關聯、完全及適用。例如，在「難以掌握」的政策由有經驗和有技術的執行，當結果(以實現的安全等級)可能有效，這不能提供本政策品質的證據。反而，因為有經驗及技術的人執行結果，最後，因為「難以掌握」政策的品質缺陷而賠償。

實際上，已實現的安全等級結果是在政策及人員之間相互影響的評價。

假如資訊安全稽核確認內部控制及資訊及安全是被評估遵循資訊安全政策有效運作，這應被理解為安全政策及當時主辦者工作互相影響的間接證明。在相反的案例裡，無效率或不充分的內部控制及安全評估可能直接確定一個不太好的資訊安全政策。

資訊安全政策的本質在此無須爭論。評估不精確執行的原因，可能是安全政策的不正確說明，或者甚至是完全不懂安全政策。安全政策的評價本身能夠確信安全政策是否傳達其責任，以及安全政策給稽核人員與經理人確定那項評估必須改善〝現狀〞的洞察力。

任何人必須專注在資訊安全政策的可讀性及可理解性。安全政策編寫者及在有效狀況下評價安全政策的稽核人員，如何決定安全政策是否適合那些必須執行並處理安全政策的員工?為目標讀者整修安全政策原文是可能嗎?是否為資訊安全政策的目的衡量?

資訊安全政策的一般衡量

在稽核或自行評估的過程中，那一種衡量可以協助評價資訊安全政策品質?一般衡量是用在有關下列主題的資訊安全政策評估及評價，詳圖1:

- 企業資訊安全政策的宣導
- 不同部門在資訊安全政策的應用
- 資訊安全政策的認知
- 資訊安全政策的異常
- 適時使用及更新模式

圖 1 資訊安全政策的衡量

衡量類型	績效指標
安全政策宣導	1. 編制單位安全政策及程序書關於安全特色管理標準化定義、施行及完成的百分比 2. 編制單位依照組織風險、資產危機及資訊敏感度，使用安全政策及程序書的百分比。 3. 員工證實全安政策、作業程序書及標準與他們有關聯的百分比。
應用	4. 本期測試並證明在正常及不正常狀況下適當完成工作的安全衡量比率。 5. 在正常及不正常狀況下，使用安全政策、作業程序書及標準的比例。
認知	6. 那些曾收到對他們工作通用且有關安全政策、程序及標準的員工，通常按比率區分組織單位為內部員工、內部外來員工(例如:在本公司工作的顧問)及外派內部員工(通常稱為假冒外來者，例如:本公司員工在外擔任顧問者)。 7. 有關安全政策、程序及標準的員工訓練頻率，依據組織單位可分為: ・上次訓練日期 ・最近六個月內，收到必要訓練的員工比率 ・最近六個月內，在訓練課程曾經提出評論或修正建議的次數
適當及適時	8. 安全政策、程序及標準的貢獻:

	・最新者 ・足夠明細用來執行 ・定義角色及責任 ・定義特別選定的功能 ・適合特定風險及精確對象 ・依據組織單位連結到特定的資產
執行程度	9. 安全政策需求比例、程序及標準依據下列要項執行並納入營運: ・技術控制 ・制度或管理控制 ・前列二項併用 10. 與在公司內部工作的外來員工、外部聘用的本公司員工、委外代工夥伴及待離夥伴約定遵循安全政策的第三者比例。
資料來源:Adapted from Herrmann, D.S.; Complete Guide to security and Privacy Metrics: Measuring Regulatory Compliance, Operational Resilience, and ROI, Auerbach Publications, USA, 2007; and Brooks, P.; Metrics for IT Service Management, ITSMF International, 2006	

從圖一可以找出適當的衡量類型，依據特定的稽核目標，內部稽核人員評估內部控制是否充分及有效的評價(不是為了資訊政策)。這些衡量經常來自使用「目標問題範例」(GDP)，這是一種將企業目標與績效指標(例如衡量)可能連結在一起的方法論。無論如何，這是一些衡量的評論者。企業應努力對安全政策充分認識，以保證他們的有效執行。因此，標準的處理方法是將安全通告一年一次(例如:在員工簽名表上正式書面化安全指示)，有時附帶一個複選的理解力測驗。這個方法有缺點。這個作法只對職員、主管及稽核等

一般讀者提出很基本的知識需求。無論如何，它不能反應內部管理架構的複雜程度。

人們需要接受哪些更複雜內容的安全政策?安全政策的構成要素就是簡單理解安全政策本身內容。只有一個方法顯著改善嗎?

可讀性衡量

資訊安全政策必須修正去改善其效果的細節，來自於衡量其原有的本質:資訊安全政策本文，它的可讀性極容易閱讀。這假設是如果資訊安全政策無法瞭解，或是它的內容難以閱讀，資訊安全政策將無法適用，或是將適用的很少。可讀性及易讀的衡量，使資訊安全政策可能被評估如何容易瞭解這些文件。

可讀性衡量能夠用來評估(詞彙的)容易讀資訊安全政策。可讀性指標(或得分) 是依據資訊安全政策本文統計分析的幾種測定方法來衡量，例如句子的長度、音節數量及文字帶三個或更多音節的文字。這種衡量說明本文更長，則句子更長，或是更多的文字帶著三個以上的音節，理解資訊安全政策本文就更難。這就是更高的易讀指標，要瞭解資訊安全政策更容易。

最廣泛使用易讀指標是「Flesch 易讀指標」，它能依據下列公式計算：

FI=206.835-(1.015xASL)-(84.6xASW)
在此公式:
FI=Flesch 易讀的可讀性得分
ASL=文字中平均句子長度(在一個句子裡的文字平均數量，用一個句子的文字數量除以句子數量)
ASW=每個文字的平均音節(音節數量除以文字數量)

計算得到的分數—依據資訊安全政策統計分析取得的 Flesch 指標—是詳細表列作為表示可讀性水準。

這 Flesch 指標的特色是每個數字在 0 和 100 之間，但數據也會發生在限度以外(參考圖 2)。

圖 2 根據易讀指標評估可讀性

Flesch 指標	可讀性水準
0-29	很困難
30-49	困難
50-59	一般困難
60-69	標準
70-79	一般易讀
80-89	易讀
90-100	非常易讀
資料來源:Adapted from Flesch, R.; The Art of Readable Writing, Harper Row Publishers, USA, 1974	

誰瞭解安全政策

評估資訊安全政策的 Flesch 指標可以幫助評估閱讀及瞭解相關文件有多困難。這是必然的，如果資訊安全政策本文難以閱讀，稽核人員會建議用一種較少複雜的方法(用較短句子，較少長文字)明確表達這些本文，因此大致上容易閱讀。

無論如何，容易閱讀只是安全政策可讀性的一種狀況。另外的狀況是政策易讀是否符合目標讀者所提易需求的問題。可讀性水準衡量可能用來答覆這個問題。

流行的 Flesch-Kin caid Grade Level Index 做為可讀性水準的一種衡量作法使用。這個測試是依據 Rudolf Flesch 產生的得分，以及日後的 John P. Kin caid 發揚光大。這個測試將 Flesch Index 變成美國等級水準。這個測試也表示教育年數通常需要去瞭解資訊安全政策本文。美國國防部把這個測試當做一個標準測試，需要所有各種內部需求及指令。

在美國中小學各年級水準的得分分析及評估本主題，係依據每個文字的音節及每個字句的文字(類似 Flesch Index)的平均數量。例如，得分 60.0 的人，表是一個在 8 年級的學生會瞭解資訊安全政策本主題(參考圖 3)。

圖 3 資訊安全政策的衡量

Flesch Index	教育
90.0-100.0	一個平均 11 歲的學生容易瞭解
60.0-70.0	13-15 歲的學生們容易瞭解
0.0-30.0	大學畢業生最瞭解

各國對教育需要瞭解一個特定的 Flesch Index 是不同的。

結論

例如，如果經過計算的資訊安全政策 Flesch Index 是在 20 以下，其易讀程度將與一個專業評論或博士論文相當符合。假如特定的政策是針對一般沒有資訊安全專業的員工，那是很明顯的不適當。

而且，許多經理人及專家沒有時間對管理事務有完整的學習，例如資訊安全政策。這群人也從易讀及高的 Flesch Index 獲得利益。在瞭解資訊安全政策個案，“時間是金錢”也是正確的。閱讀及瞭解易讀文件(例如:較高易讀指標)，比學習用以評論性質的易讀指標文件還花費較少時間。

利用資訊安全政策適當語言修訂版，這些政策的易讀能夠依次輪流改善，組織的安全水準也能改善。

資訊安全政策的衡量，能夠用來評估文件的品質及效果，例如:如何容易瞭解，並且各種要求必然被遵守。另外，當資訊安全政策正在執行時，為了監控安全政策的例外及組織目標遵循程度。關於分類、執行、適時或認知的衡量能夠使用。

ENDNOTES

1. *Independent Oracle Users Group (IOUG), Closing the Security Gap: 2012 IOUG Enterprise Data Security Survey, https://blogs.oracle.com/securityinsideout/*
2. *For examples of typical security metrics and maturity models, see: Chapin, A.; S Akridge; "How Can*
3. *Security Be Measured?," Information Systems Control Journal, vol. 2, 2005, www.isaca.org/archives*
4. *Sowa, A.; S. Fedtke; Metriken—der Schlüssel zum erfolgreichen Security und Compliance Monitoring: Design, Implementierung und Validierung in der Praxis, Vieweg Springer, 2011*
5. *The test is based on a score created in the 1940s by Austrian-born American author Rudolf Flesch. The formula to compute the Flesch Index is one of the best known and most popular for readability indicators. However, the formulas differ for different languages. The formula provided here is true only for English documents.*
6. *Hayden, L.: IT Security Metrics: A Practical Framework for Measuring Security & Protecting Data, McGraw-Hill Professional, USA, 2010*

Quality Statement:
This Work is translated into Chinese Traditional from the English language version of Volume 4, 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 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。

若為非商業用途之課堂教學，則允許教師免費複印單篇文章。若為其他用途之複製，重印或再版，則必須獲得ISACA的書面許可。如有需要，欲複印ISACA Journal 者需向Copyright Clearance Center(版權批准中心，地址：27 Congress St., Salem, MA 01970) 付費，每篇文章收取2.50元美金固定費用，每頁收取0.25美金。欲複印文章者則需支付CCC上述費用，並說明ISACA Journal 之ISSN 編碼(1526-7407)、文章之出版日期、卷號、起訖頁碼。除了個人使用或內部參考之外，其他未經ISACA或版權所有者許可之複製行為則嚴明禁止。