IT 安全確保的基本概念
Fundamental Concepts of IT Security Assurance

作者：Haris Hamidovic, CIA, ISMS IA, IT Project+,

is chief information security officer at Microcredit Foundation EKI Sarajevo, Bosnia and Herzegovina. Prior to his current assignment, Hamidovic served as IT specialist in the North American Treaty Organizationled Stabilization Force in Bosnia and Herzegovina. He is the author of five books and more than 70 articles for business and IT-related publications. Hamidovic is a certified IT expert appointed by the Federal Ministry of Justice of Bosnia and Herzegovina and the Federal Ministry of Physical Planning of Bosnia and Herzegovina. He is a doctoral candidate in critical information infrastructure protection at the Dzemal Bijedic University, in Mostar, Bosnia and Herzegovina.

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

政府及商業組織高度依賴資訊的運用，進行他們的經營活動。資訊及執行業務缺少保密、正直、有效、責任及真實可以產生對組織不利影響。因此，在組織內部有保護資訊及處理IT系統安全的重要需求。為了追求重大利益，每種新科技產生保護這類資訊的新挑戰。保護資訊的需求在當今環境是很重要，因為許多組織以IT系統網路連接內外部資訊[1]。

由於錯誤及弱點容易造成IT系統失敗及安全失效。這些錯誤及弱點可以歸究於許多原因，例如技術快速變化、人為錯誤、缺少所需求的規格設計、缺少發展程序或低估預期威脅。此外，經常被提到的系統變更、新缺點及新威脅，也會透過IT系統生命週期增加弱點、失敗及安全失效[2]。

因為干擾的安全結構、人為錯誤或疏漏、以及系統結構或設備失效[3]，企業瞭解到不可能保證沒有錯誤、沒有風險。

只有那些系統所有者能改變對滿足系統安全需求的信心程度，才可完全確保IT系統不發生前列的問題[4]。

此外，許多資訊系統未曾設計安全功能。資訊系統透過技術工具能夠確保安全是有限的，並且需要適當的管理及程序支援資訊安全[5]。

「資訊安全(ITS)」工作的指導及管理，是以技術及組織的安全標準，降低弱點及威脅，達到IT系統可接受的確保，來處理資訊安全風險。ITS管理有個附加的任務：建立可接受的保證及風險目標。依此作法，IT系統持有者在IT系統可接受風險及相關預算下，完成特定或必要的目標，獲得合理的信心[6]。

ISO/IEC TR 15443 資訊科技–安全技術-IT安全確保的架構是多項技術報告，當我們要詳述、選擇或展開一種安全的服務、產品或環境要素(通常視為“可表達者”)[7]時，這報告會指導ITS(資訊安全)各項專業作法，以選擇一種適當的資訊安全方法。ISO/IEC TR 15443 的目的是表達多種安全確保方法，並且引導ITS專業作法，選擇適當的安全確保方法(或綜合多種方法)，達到IT系統滿足需求的信心。分析安全確保方法也許不是唯一針對ITS；無論如何，這標準所提供的指導僅限於ITS的需求。這個主題以ISO/IEC TR 15443 為基礎，介紹ITS(資訊安全)確保的基本

確保及信心

強調確保及信心不是相等的，而且不能相互取代，這是很重要的。因為確保及信心是接近且有關連，這兩個名詞常常被不正確使用[8]。

ISO/IEC TR 15443定義這些名詞如下：「從個人觀點，信心是被企業的安全確保證明，然而安全確保是證明企業達成安全目的的能力。安全確保是從企業評價程序產生的證據所決定。」[9]

關於資訊安全技術處理，「安全確保」被定義為資訊系統安全需求滿足的信心程度。[10]

安全確保不增加對安全相關反擊風險的任何額外控制，但安全確保對曾已執行減少預期風險的控制提供信心。安全確保也能判斷安全設備是否如預期發揮功能的信心[11]。我們瞭解到「安全確保不會自動帶來好的安全」。安全確保只能讓企業符合他的安全目標。換句話說，安全確保提供表達堅持安全目標的信心，而不能檢查安全目標是否適當顯示風險及威脅。[12]

確保需求

從ITS(資訊安全)的角度來看，充份的安全確保預示：特定的、預設的資訊安全各項需求，可以經由提供適當確保程序及活動獲得滿足。[13]

安全確保需求由下列因素決定：

1. 分析安全需要的IT系統、影響者、決策者、企業經營管理者及IT系統目標環境。

2. 影響者要提出會影響IT系統確保需求的任何應考慮事項。

3. 影響項目有任何來源，並包括政治、文化、本地法規及委託需求等無形項目。

安全與資產保護有關。資產是由人認定價值的實體。[14]許多資產以資訊形式由IT產品儲存、處理、傳送，以符合資訊所有者訂定的需求。保護資產利益是認定資產價值所有者的職責。實際或假設威脅者也可以認定資產價值，並設法用資產所有者利益對立的做法，誤用資產。[16]

執行並完成「風險評估」，係針對資產的敏感性、弱點及威脅，提供深度檢討，並對現有及預計資產保護提供建議。執行風險評估建議，係解析原有的安全需求，進而修正安全確保需求。

以下的註記也很重要：

為了無數的企業以及每個企業環境的安全需求，安全需求對每個企業環境的影響是獨一無二的。同樣的IT系統可能不適合其他企業環境，除非修正，因為不同的安全需求將需要個別滿足。[17]

確保方法應用到ITS

適當確保活動的應用，可以建立IT系統滿足安全目標的信心。信心實現來自在企業發展、展開及營運過程中，透過覆核由評估程序及活動所獲得的安全確保證據，並透過使用IT系統所獲得的經驗。任何活動可以產生證明歸因於IT系統更正、效果及品質的證據，以減少不確定性，對決定安全確保是有幫助的。[18]

有許多既有的安全確保方法，但只有少數特定歸歸ITS(資訊安全)。無論如何，非歸ITS確保方法可能包含與ITS確保特性。[19]因為少數可用的確保方法特定歸屬ITS，而且許多非安全確保方法在IT產業遍及使用，辨識所有所有確保方法的價值是很重要的。任何事物皆可以用在設計確保論點，因此，減少結合特定可陳述的不確定性是不可忽視的重要性。[20]

選定安全確保

選定一種安全確保方法及適量的確保，必須以組織安全確保政策、企業經營管理需求及可達

的樣式(例：產品、程序、環境、系統、服務或人員等)舉例說明：有些確保方法只能應用在程序(例：ISO/IEC 21827)，其他應用在產品(例：ISO/IEC 15408資訊科技-安全技術-IT安全評價標準)，及其他應用在安全管理(例：ISO/IEC 27001資訊科技－安全技術－資訊安全管理系統－需求)。

以下三個常用模式的簡介

- 現代統計程序控制提出：較高品質的產品能夠產生更多有效成本，經由著重過程品質，以產生這些產品，並且完成在這些過程固有的組織實效。為了發展正常系統及可信賴產品，更多有效率的過程產生增加的成本及時間是正常的。正常系統的營運及維持，依賴著連結人員及科技的程序。這些相互依賴的人員、科技及程序能夠處理更多有效成本，經由著重過程品質實際執行，以產生這些產品，並且完成在這些過程固有的組織實效。ISO/IEC 21827提供一種程序參考模式，聚焦在ITS(資訊安全)領域內，執行一個系統或相關系統系列的安全需要。在ITS領域裏，ISO/IEC 21827 聚焦在達成ITS的各種程序，多數明確地聚焦在這些程序的達成。[21]

- 保護利益的資產是那些將價值寄託在資產所有者的職責。資產所有者要(擁有)負責這些資產，因此，必須能夠抗拒接受資產暴露在威脅中的風險。許多資產所者缺少對判斷足夠及正確對策的知識、專門技術或資源，他們不希望孤單地依賴對策開發者的斷言。因此，這些使用者（相對開發者）只有安排這些對策的評價，來選擇加強部份或全部對策足夠及正確的信心。ISO/IEC 15408為IT產品安全實用功能，並且為在安全評價期間適用那些產品的確保評估，提供一套通用型式工具。IT產品將在硬體、固定實體或軟體內使用。評價程序為這些IT產品的安全實用功能，以及適用這些IT產品以符合這些需求，建立信心程度。評價結果可能協助使用者決定這些IT產品是否符合他們安全需求。[22]

- 「資訊安全」是保護資訊遠離廣大範圍的威脅，以確保企業永續、企業最小風險、最大投資報酬及企業發展機會。資訊安全是靠執行一套適當的控制達成目的，包括政策、程序、過程、組織結構、軟體功能及硬體功能。這些控制必須建立、執行、監督、覆核及改進等必要過程，以確保組織特定的安全及企業目標達成。這些過程必須配合企業其他經營管理過程共同完成。[24]在組織所有企業風險的背景下，ISO/IEC 27001詳加敘述「資訊安全管理系統（Information Security Management System,ISMS）」建立、執行、營運、監督、覆核、維護及改進的書面化需化。ISMS的設計是確保選定足夠及適當的安全控制，以保護資訊資產，並給有關係者信心。ISO/IEC 27001能夠被有關係的內、外部人員一致評價。[25]選定的安全確保方法必須和組織環境並存，並且必須有能力審查可陳述的期望特質及生命週期階段。確保方法選定必須被視為可使用的資源（例：時間、人員、預算等）以確保這些資源的使用對所得到的確保類型及數量是合理的。

確保處理方法

安全確保方法可以分為三種高階處理方法：[26]

1.可陳述的確保，例：透過評價及測試。

2.過程用在發展或產生可陳述的確保。

3.環境的確保，例如人力資源及設施。

ISO/IEC TR 15443定義這三種高階處理方法於後。可陳述的確保引起可陳述的檢查（例：產品、系統及服務）。以這個案例，這些確保方法評核可陳述者，以及獨立於發展過程相關安全規劃的文件。

過程確保引起在可陳述的生產及營運整個生命週期裏，檢查使用過的組織過程（例：發展、

配置、輸送、測試、維護、處分）。

透過推論，確保可以獲利：由人員執行過程，會影響可陳述者發展及執行的品質，因此，當確保符合ITS(資訊安全)可陳述時，會產生安全確保。

環境確保引起環境因素的檢查，環境因素對過程及生產的可能陳述者是有貢獻（這些因素並不直接檢查可陳述者或過程）。這些因素包括人員及實際使用的設備（例：發展、生產、輸送、營運）。

確保方法依據技術及生命週期的焦點，產生特定型式的安全確保。為了特定的焦點，有些或更廣為人知的確保方法包括：[27]

- ISO/IEC 21827-確保的焦點在品質及發展過程
- 開發者血統－確保的焦點在給予深刻印象；認識企業所產生的可陳述品質（依據歷史關係或資料）
- 保證－確保焦點在保險，由製造者支持承諾修正可陳述者的缺陷
- 供應廠商的宣告－確保的焦點在自我宣告
- 專業檢定及認可－確保的焦點在個人的專業及知識
- ISO/ICE 14589-資訊科技－軟體產品評價－第一部份：總論－確保的焦點在可陳述的評價
- ISO/ICE 27001-確保的焦點在安全管理

正確及有效財產

當資訊安全如期完成，安全確保就能被視為信心。這信心來自於財產的正確及有效。[28]

「正確確保」依據可陳述的評價，以證明按照原有設計正確執行。對比之下，「有效確保」依據可陳述的安全功能適當反擊已察覺或已證實的威脅。[29]

這個觀念可以用ISO/IEC TR 15443的二個例子說明：[30]

- 如果IT系統安全功能提供出潛在的威脅，但是安全功能無法分析並正確設計及執行，沒有人能相信這系統經得起攻擊。在這個案例，「有效確保」已確立，但「正確確保」因為缺少安全功能而未確立。
- 同樣狀況下，如果分析已經發現IT系統安全功能的設計及執行是正確的，但是，規劃未能包括提出可能威脅的適當功能，沒有任何人對經得起那些威脅的信心。在這個案例，雖然「正確確保」存在，因為無效果的安全功能對付可能的威脅而缺少「有效確保」。為達成廣泛的確保，IT系統必須評價能保證正確的設計、執行及營運（「正確確保」的因素），以及可陳述者應提供適當的安全功能，以反擊已確定的威脅（「有效確保」的因素）

結論

傳統上，安全確保只和由硬體及軟體組成的IT產品與系統有關聯，並被認為屬於「產品確保」或「系統確保」。現在，安全確保被認知為一種範圍廣泛的風險，必須有安全目的（例如：安全服務、過程、人員、組織或其他環境因素的確保。

有IT系統風險資產的IT系統所有者尋求安全確保。因此，所有者應決定可接受的確保方法及確保程度可能需要及（或）影響。

安全確保不能增加任何保護或服務給可陳述者。不安全的人員有時難以知道他們從投資資源收到何種利益。

安全確保貢獻的直接品質或評價，或增加組織的安全確保是不易達成的。無論如何，安全控制的確保增加，會減少相關不確定的風險，特別是風險弱點因素的控制是被提供去執行。

我們必須知道每一種安全確保方法如何建立安全確保，才能決定那一種特定的安全確保方法

能滿足組織需求。

ENDNOTES

1 International Organization for Standardization (ISO),
ISO/IEC 13335-1:2004 Information technology—
Security techniques—Management of information and
communications technology security—Part 1: Concepts and
models for information and communications technology
security management, Switzerland, 2004
2 ISO, ISO/IEC TR 15443-1:2005 Information technology—
Security techniques—A framework for IT security assurance—
Part 1: Overview and framework, Switzerland, 2005
3 Ibid.
4 Dražen, Dragicevic; Computer Crime and Information
Systems, Informator Zagreb (in Croatian), 1999
5 ISO, ISO/IEC 27002:2005 Information technology—
Security techniques—Code of practice for information
security management, Switzerland, 2005
6 Op cit, ISO/IEC TR 15443-1:2005
7 Ibid.
8 Ibid.
9 Ibid.
10 US National Institute of Standards and Technology
(NIST), NIST Internal Report (NISTIR) 5472 A Head Start on Assurance: Proceedings of an Invitational Workshop on Information Technology (IT) Assurance and
Trustworthiness, USA, 1994
11 ISO, ISO/IEC 21827:2002 Information technology—
Systems Security Engineering—Capability Maturity Model®
(SSE-CMM®), Switzerland, 2002
12 Op cit,, ISO/IEC TR 15443-1:2005
13 Ibid.
14 Ibid.
15 ISO, ISO/IEC 15408-1:2009 Information technology—
Security techniques—Evaluation criteria for IT security—
Part 1: Introduction and general model, Switzerland, 2009
16 Ibid.
17 Op cit, ISO/IEC TR 15443-1:2005
18 Ibid.
19 For example, while ISO 9000 Quality management
systems is a quality assurance standard originally intended
for manufacturing organizations, it also contains process
assurance properties applicable to software and, as such, to
ITS software products and systems.
20 Op cit, ISO/IEC TR 15443-1:2005
21 Op cit, ISO 2002
22 Op cit, ISO 2009
23 Op cit, ISO/IEC 27002:2005
24 Ibid.
25 ISO, ISO/IEC 27001:2005 Information technology—
Security techniques—Information security management
systems—Requirements, Switzerland, 2005
26 Op cit, ISO/IEC TR 15443-1:2005
27 Ibid.
28 Op cit, ISO 2002
29 Op cit, ISO/IEC TR 15443-1:2005
30 Ibid.

Quality Statement:

This Work is translated into Chinese Traditional from the English language version of Volume 2, 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 2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。