國際資訊稽核實務準則(ITAF™)

專業實踐框架

(第4版)

ISACA®

ISACA簡介

五十多年來，ISACA® (www.isaca.org) 紮根技術，培養出了最優秀的人才，積累了深厚的專業知識和極高的學習能力。ISACA為個人提供知識、認證、指導並建立社群網路，推動人員的職業發展及其所在組織的轉型，說明企業培訓和打造高素質團隊。ISACA是一家全球性的專業協會和學習組織，擁有145,000名具備資訊安全、治理、確保、風險與隱私方面專業知識的成員，致力於通過技術推動創新。ISACA成員遍佈188個國家和地區，在全球設有超過220個分會。

免責聲明

ISACA設計並編制了《國際資訊稽核實務準則 (ITAFTM)：專業實踐框架（第4版）》（下稱「準則」），主要用作從事確保工作人員的參考資料。ISACA不保證使用本準則就一定能取得成功。本準則不應被視為包含所有適用的資訊、程序和測試，不排除在其它資訊、程序和測試的合理指導下獲得同樣結果的可能性。在確定具體資訊、程序或測試的適宜性時，從事確保工作從業人員應就具體的情況對特定的系統或資訊技術環境做出自己的專業判斷。

ISACA
1700 E. Golf Road, Suite 400
Schaumburg, IL 60173, USA
電話：+1.847.660.5505
傳真：+1.847.253.1755
聯繫我們：https://support.isaca.org
網站：www.isaca.org

提供回饋：https://support.isaca.org
參加ISACA線上論壇：https://engage.isaca.org/onlineforums

Twitter: http://twitter.com/ISACANews
LinkedIn: www.linkedin.com/company/isaca
Facebook: www.facebook.com/ISACAGlobal
Instagram: www.instagram.com/isacanews/

ISACA Taiwan Chapter

11070 台北市信義區
基隆路一段143號7樓之4, Taiwan
電話：+886 225288875
傳真：+886 225288876
Email：isaca.caa@gmail.com
網址：www.isaca.org.tw

國際資訊稽核實務準則(ITAFTM)：專業實踐框架(第4版)
印刷地點：美國

致謝

ISACA向以下人員表示感謝：

校審專家

Manoj Agarwal，CISA，CIA，CRMA，CA，DISA，Metro Brands Limited，印度
G.M.Faruk Ahmed，CISA，Rupali Bank Limited，孟加拉
Winnie Ang，CISA，CISM，新加坡
Anagha Apte，CISA，CRISC，CISM，Birlasoft Ltd.，美國
Kenia Arias，CISA，A-FE Consulting LLC，美國
Bode Bary Aro，CISA，CRISC，Enugu Electricity Distribution Company，奈及利亞
Mais Barouqa，CISA，CRISC，CGEIT，ISO27K，ITIL，COBIT FL，GRCP，Deloitte，約旦
Marquita Bass，CISA，PMP，Rausch Advisory，美國
Cindy Baxter，CISA，ITIL，State Street Corporation，美國
Zsolt Bederna，CISA，CRISC，CISM，CGEIT，CISSP，CEH，ITIL-F，Cyex OÜ ，匈牙利
Vijay Bhalerao，CISA，COBIT-F，ISO 27001 LA，MCSA，ITIL-F，Unisoft Computrade Pvt. Ltd.，印度
Parmeet Bhatiya，CISA，PricewaterhouseCoopers，阿聯酋
Bakan Borupile，CISA，MCSE，MCSA，Btech，Mascom Wireless，波札那
Ricardo Jimenez Caicedo，CISA，Ernst & Young，哥倫比亞
Jules Chachine，CISA，CISM，PMP，Jconseil，黎巴嫩
Elastos Chimwanda，CISA，CIA，ZWMB Bank Limited，辛巴威
Joyce Chua，CISA，CISM，CDPSE，CIPP(E)，© CISO，CIPM，CIPP(A)，CFE，CIA，PMP，CITPM，ITIL，MCP，IRCA ISMS 協理稽核員，Sony Electronics，新加坡
Ari Ecrument，CISA，CRISC，CDPSE，FIP，CIPP/E，CIPM，CRMA，CEH，ISO 27001/22301/20000
Bhaskar Ghosh，CISA，Wintrust Financial Corporation，美國
Miguel A. Gonzalez，CISA，ITESM，墨西哥
J. Winston Hayden，CISA，CRISC，CISM，CGEIT，南非
Andrew Hinder，CISA，CMIIA，QIAL，CRMA，CIA，BAE Systems，英國
Marko Jagodic，CISA，CRISC，VRIS, LLC，斯洛維尼亞
Ashane J.W. Jayasekara，CISA，BDO，斯里蘭卡
Daniel Jones，CISA，CRISC，CISM，Devon Energy，美國
Abbie Anne Julien，CISA，CDPSE，Life Extension Foundation Buyers Club Inc.，美國
Mladen Kandic，CISA，CIA，Eurobank，塞爾維亞
Joanna Karczewska，CISA，波蘭
Glenn Kirke，CISA，Integrated Audit and Compliance，美國
Matthias Kraft，CISA，CRISC，CISM，CGEIT，CAC，DPO，Fidelity International，盧森堡
Abhishek Kumar，CISA，ISO 27001 LA，ISO 22301 LA，Deloitte，印度
Hiu Sing Lam，CISA，FRM，PMP，中國香港
James Lam，CISA，CRISC，CISM，TOGAF，Aon Cybersecurity Advisory，美國
Larry L. Lliran，CISA，CISM，Precelsus Consulting，波多黎各
Angel Giovanni Vasquez Lopez，CISA，Banco GYT Continental，瓜地馬拉
Michael Malcolm，CISA，CIA，CRMA，CFSA，CGAP，CFE，Opentext Corporation，加拿大
A.T. Manjunath，CISA，CCSK，CSA STAR AUDITOR，Applied Materials，印度
Rafael Pérez Marín，CISA，委內瑞拉
Larry Marks，CISA，CRISC，CISM，CGEIT，CDPSE，CISSP, ITIL，PMP，美國
Vivek Mathivanan，CISA，CRISC，CGEIT，Worley，澳大利亞
Benedicta Mlingi，CISA，NMB Bank Plc.，坦尚尼亞
Juan Carlos Morales，CISA，CRISC，CISM，CGEIT，COBIT 2019，瓜地馬拉
Donald Morgan，CISA，Farm Credit Canada，加拿大
Syed Aun Muhammad，CISA，加拿大

致謝（續）

Christine Lilian Mukhongo，CISA，CRISC，CISM，Kenya Universities & Colleges Central Placement Service，肯亞
Sitambaram Ainslei Naidu，CISA，CIA，Edcon，南非
Tushar Nerurkar，CISA，CISSP，PMP，PricewaterhouseCoopers，美國
Daisha Ngo，CISA，CPA，CRMA，Spectrum Health，美國
Geoffrey Nkuutu，CISA，特許公認會計師 (FCCA)，Wazalendo Savings & Credit Cooperative Society Limited，烏干達
Alexander Obraztsov，CISA，CISSP，PMP，Societe Generale (New York)，美國
Darren O'Brien，CISA，CRISC，Vitality，英國
Iroko Oluwatosin，CISA，CRISC，CISM，ITIL，CEH，ISO 27001，Alberta Blue Cross，加拿大
Anas Olateju Oyewole，CISA，CRISC，CISM，CDPSE，CISO，CISSP，CCSP，PMP，Indigo Books and Music，加拿大
Chirag Ali Peerzada，CISA，CEH，ISO 27001 LA，ISO 22301 LI，Mahindra Special Service Group，印度
John Pouey，CISA，CRISC，CISM，CIA，Entergy，美國
Shahid Qureshi，CISA，CPA，CGA (Canada)，FCCA (UK)，CIA (USA)，FCMA，FCIS，FCSM，Leverage Global Inc.，加拿大
Sreechith Radhakrishnan，CISA，CRISC，CISM，CGEIT，CDPSE，COBIT評估員，ISO 27001 LA，ISO 20000 LA，ISO 37001 LA，ISO 22301 LA，Global Success Systems FZ LLC，阿聯酋
Allan Rono，CISA，CISM，ITIL，Liberty Group，肯亞
Sampa David Sampa，CISA，World Vision International，尚比亞
Megah Santio，CISA，CISM，COBIT評估員，CIA，澳大利亞
Garimella Chandrasekhar Sarma，CISA，CRISC，CDPSE，CFE，CtrlS Datacenters，印度
S. Phani Krishna Sunkaranam，CISA，CRISC，CISM，CISSP，ITIL，Trianz，印度
Luong Trung Thanh，CISA，CISM，CGEIT，越南
Catalin Tiganila，CISA，CRISC，CISM，CISSP，CBCP，CIPM，Deloitte，盧森堡
Marisela Parra Valencia，CISA，ITIL，哥斯大黎加
Kaysi Veatch，CISA，CSX-F，CIA，Maxar，美國
Ionnis Vittas，CISA，CISM，Quest Holdings SA，希臘
Ross Wescott，CISA，CUERME，CCP，CIA（退休），Wescott & Associates，美國
Surendra Yakkali，CISA，CSM，ITIL，SAFe 5，CMMI Associate，OptumServe Technology Services, Inc.，美國

董事會

Tracey Dedrick，主席，Hudson City Bancorp前首席風險官，美國
Rolf von Roessing，副主席，CISA，CISM，CGEIT，CDPSE，CISSP，FBCI，FORFA Consulting AG合夥人，瑞士
Gabriela Hernandez-Cardoso，獨立董事，墨西哥
Pam Nigro，CISA，CRISC，CGEIT，CRMA，Home Access Health資訊技術副總裁/安全官，美國
Maureen O'Connell，Acacia Research (NASDAQ) 董事會主席，Scholastic, Inc. 前首席財務官兼首席行政官，美國
David Samuelson，首席執行官，ISACA，美國
Gerrard Schmid，Diebold Nixdorf總裁兼首席執行官，美國
Gregory Touhill，CISM，CISSP，AppGate Federal Group總裁，美國
Asaf Weisberg，CISA，CRISC，CISM，CGEIT，introSight Ltd.首席執行官，以色列
Anna Yip，SmarTone Telecommunications Limited首席執行官，中國香港
Brennan P. Baybeck，CISA，CRISC，CISM，CISSP，2019-2020年ISACA董事會主席，Oracle Corporation客戶服務副總裁兼首席資訊安全官，美國
Rob Clyde，CISM，2018-2019年ISACA董事會主席，Titus獨立董事，White Cloud Security執行主席，美國
Chris K. Dimitriadis，博士，CISA，CRISC，CISM，2015-2017年ISACA董事會主席，INTRALOT集團首席執行官，希臘

目錄

簡介

ISACA的國際資訊稽核實務準則 (ITAF) 是一個全面的資訊稽核框架，用於：

- 制定相應標準，確立資訊稽核和從事確保工作人員的角色和職責、道德、預期的職業行為，以及必要的知識和技能；
- 定義資訊稽核和確保的特定術語和概念；
- 為資訊稽核和確保業務的計畫、執行和報告提供指引和技術支援。

ITAF以ISACA資料為基礎，為資訊稽核和從事確保工作人員提供，獲取有關稽核執行和有效稽核報告編製方面的單一資訊來源指引。ITAF第3版涵蓋2013年11月生效的資訊稽核和確保標準及指南。在發佈ITAF第4版之前，ISACA公佈了一份徵求意見稿，並收到了超過65位複核人員的回饋。ITAF第4版於2020年10月生效。

如需這些標準的譯文，請參考：

https://www.isaca.org/bookstore/audit-control-and-security-essentials/witaf4。

常見問題解答

- **ITAF適用於誰？**ITAF適用於以資訊稽核和從事確保工作身份致力於確保資訊流程及資訊應用程式、系統及基礎設施元件工作人員。不過這些標準、準則和稽核技術經過了謹慎的設計，可能對更廣泛的受眾也有幫助，包括資訊稽核和確保報告的使用者。
- **在什麼情況下應使用ITAF？**使用該準則是執行資訊稽核和確保工作的前提。標準是強制性的。準則、工具和技術旨在為執行確保工作人員提供非強制性的協助。
- **在什麼情況下應使用ITAF資訊稽核和確保標準以及相關指南？** ITAF的設計考慮到，從帶領以 資訊為重點的稽核到參與財務、合規或營運稽核，資訊稽核和從事確保工作人員面臨不同的要求和不同類型的任務。ITAF適用於任何資訊稽核或評估專案。
- **ITAF是否涉及顧問和諮詢工作的要求？**除了執行稽核工作，資訊稽核和從事確保工作人員還可以為雇主或代表客戶承接非稽核業務。顧問和諮詢業務通常涉及特定領域的審查。出於多種原因，包括工作的性質（尤其是測試的程度和參與業務範圍），資訊稽核和從事確保工作人員通常不會發布正式的稽核報告。因此，顧問和諮詢工作成果通常是對當前執行情況的意見（可能採用備忘錄的形式）和改進建議。
- **ITAF第4版何時可用？**修訂後的資訊稽核實務準則於2020年10月可用。

組織

ITAF標準分為三類：

- **通用標準（1000系列）**— 詳述資訊確保產業的指導原則。這些原則適用於所有業務，包括但不限於資訊稽核和從事確保工作人員的道德、獨立性、客觀性和應有的審慎性，以及知識、專業能力和技能。

- **執行標準（1200系列）**— 涉及到業務的執行，例如規劃與監督、業務範圍界定、風險評估、資源調動、業務管理、稽核與確保證據，以及專業判斷和應有的審慎性的實踐。
- **報告標準（1400系列）**— 涉及到報告類型、溝通方式及所溝通的資訊。

ITAF準則為資訊稽核和從事確保工作人員提供有關資訊稽核或確保業務的資訊和指導。與上述三類標準一樣，準則重點關注各種稽核方法、方法論和相關資料，以協助執行資訊流程、控制和相關資訊稽核或確保措施的規劃、執行、評估、測試和報告。準則還有助於闡明企業承擔的活動和舉措與資訊承擔的活動和措施之間的關係。適用準則遵循相關標準。
ISACA網站提供有關各種方法論、工具和範本的具體資訊，包括它們的應用和使用指導，以使指南中提供的資訊得以落實到實踐中。例如ISACA編製的《資訊稽核抽樣：執行準則2208》便是ITAF框架的一本配套手冊。這些準則幫助資訊稽核和從事確保工作人員在稽核程序的樣本不是全母體的情況下，通過抽樣得出關於全母體的結論。有關其他工具和技術，也包括白皮書、稽核程序和書籍，請參考：
www.isaca.org/resources/insights-and-expertise/audit-program-and-tools。

使用ITAF

資訊稽核或確保過程涉及特定程序的執行，以提供關於查核事項合理的保證。從審核到證明或檢查，資訊稽核和從事確保工作人員承擔了不同層級的確保任務。

每個資訊稽核或確保任務都必須遵守規定的標準，包括個人是否具備執行工作的資質、如何執行工作、執行哪些工作，以及如何根據不同任務的特徵和所得結果的性質報告稽核結果。

如果只有一個人執行工作，則此人必須具備完成業務所需的技能和知識。如果由多個人執行工作，則整體團隊必須具備執行業務所需的技能和知識。
資訊稽核或確保任務都有幾項固有的關鍵假設，包括：

- 事項是可被識別的，而且可被稽核。
- 成功完成專案的可能性很高。
- 方法和方法論不存在偏差。
- 專案範圍足以滿足資訊稽核或確保目標。
- 專案將得出客觀而且不會誤導讀者的報告。

標準在所有情況下都是強制性的。術語「應」表示「必須 」。在完成資訊稽核或確保業務之前，應解決任何偏離標準的情況。
本準則可能不適用於所有情況，但在任何情況下都應予以考慮。準則賦予資訊稽核和從事確保工作人員一定程度的靈活性。因此，在審查準則以確定適用性時，從業人員應運用專業判斷，並做好辯護的準備，證明與準則發生重大偏離或忽略準則相關部分的正當性，必要時尋求更多指導。

其他指導資源包括：

- 企業內部或外部的同事（例如通過專業協會或專業網路團體）
- 管理階層
- 企業的治理機構（例如：審計委員會）
- 專業指導材料（例如：書籍、論文和其他準則）

工具和技術是指為準則提供支援的補充材料和資訊。在某些情況下，它們代表替代方案甚至一系列技術（其中許多方案或技術可能適用）。資訊稽核和從事確保工作人員應該僅選擇能夠輸出相關、客觀且無偏差資訊的適合技術。

章節編號故意留出了空格，以便根據ITAF的發展情況插入未來的指引。

其他標準制定機構發佈的標準

ITAF標準為資訊稽核和從事確保工作人員提供了全面的指導和方向，但在某些情況下，從業人員可能還需要使用其他組織發佈的標準。

如果資訊稽核和從事確保工作人員遵循ITAF標準，但ITAF標準與另一組織的適用標準發生衝突時，則資訊稽核和從事確保工作人員應將ITAF標準作為執行複核和報告結果的主導標準。

如果出於監管目的或營運期望，資訊稽核和從事確保工作人員必須遵守ITAF以外的其他標準，則資訊稽核和從事確保工作人員可以：

- 將其他權威機構要求的專業標準與ITAF標準結合使用，
- 在報告中引用其他要求的標準。

術語和定義

在本文件中，常用詞彙有特定的含義，適用於資訊稽核和從事確保工作人員執行的最常見業務類型。ITAF的 附錄C中提供了這些詞彙的定義。這樣可確保這些詞彙及其在本文件的上下文含義中得到一致的理解和應用。

在可行的情況下，ITAF的術語和定義通常與專業稽核實踐以及資訊技術和安全中常用的術語保持一致；但是，從業人員應參考與執行特定業務類型有關的最新來源標準，以確保使用最新和最適當的術語和定義。

對於ITAF中未包含的其他術語和定義，請參閱ISACA網站提供的完整詞彙表：*www.isaca.org/glossary*。

ISACA職業道德規範

ISACA制定了職業道德規範，以指導協會會員和證書持有人的職業行為與個人行為。

協會會員和ISACA證照持有人應：

1. 支持實施並鼓勵遵守適當的標準和程序，以有效治理和管理企業資訊系統及科技，包括稽核、控制、安全和風險管理。
2. 依照專業標準，客觀、盡職、專業上的注意執行職務。
3. 以合法誠信的方式，維護利害關係人之權益，並保持高標準的行為和品行，且不損害其專業或協會的形象。
4. 維護活動過程中所取得資訊的機密與隱私，除司法機關要求予以揭露的情況外。不應將此類資訊用於圖利個人，或發布予不適當的團體。
5. 維護其專業領域內的能力，並同意在合理範圍內，從事預期能以必要的技術、知識所完成的活動。
6. 向適當團體告知所執行工作的結果，並揭露他們需要知道的所有重要事實；如不揭露時，可能導致報告結果失真。
7. 提升利害關係人對治理和管理企業資訊系統和科技的瞭解，包括稽核、控制、安全和風險管理，以支持其專業教育訓練。

未遵守職業道德規範，將導致對協會會員或證照持有人的行為進行調查，最終可能遭受到紀律懲戒處分。

資訊稽核和確保標準公告

ITAF中的標準包含旨在協助資訊稽核和從事確保工作人員的關鍵內容。ITAF標準定期進行複核以實現持續改善，並在必要時進行修訂，與資訊稽核和確保業務的發展保持同步。

標準公告

通用標準

1001稽核組織章程

1001.1資訊稽核和確保工作應在稽核組織章程中訂定明確之稽核部門職能，指出目的、職責、職權和當責。

1001.2資訊稽核和確保工作應將稽核組織章程提請負責治理和監督稽核部門的機構（例如：董事會或審計委員會）同意和正式核准。

1001.3資訊稽核和確保工作應向執行階層與高階管理階層傳達稽核組織章程。此外，應在啟動會議或稽核專案委任書中與受查單位分享稽核組織章程的相關要素。

1001.4透過定期複核稽核組織章程，確保稽核組織章程中反應的稽核和確保工作的職責與企業的使命和策略保持一致。如果企業的使命或策略發生變化，或稽核部門的職責發生變化，必須立即重新檢視稽核組織章程。

1002組織獨立性

1002.1對資訊稽核和確保工作對於專案所有相關的問題，應避免利益衝突和不當影響。如果發現獨立性受到（實質上或形式上的）損害，應向有關單位揭露。

1002.2資訊稽核和確保工作應有業務報告關係（例如：向董事會報告），以支持該職能能夠免於不當影響。

1002.3資訊稽核和確保工作應有行政報告關係，以支持該職能能夠不受阻礙的履行其職責（例如：專案範圍、現場工作或報告）。

1003稽核的客觀性

1003.1資訊稽核和從事確保工作人員，對於所有與稽核和確保專案相關的問題都應保持客觀性。

1004合理預期

1004.1資訊稽核和從事確保工作人員應合理預期能夠按照適用的資訊稽核和確保標準（必要時還包括其它可得出專業性意見或結論的產業標準或適用的法律法規）來完成稽核和確保專案。

1004.2資訊稽核和從事確保工作人員應合理預期稽核和確保業務的範圍，使他們能夠就查核事項得出結論並解決範圍限制的問題。
1004.3資訊稽核和從事確保工作人員應合理預期管理階層瞭解其在提供執行業務所需的適當、相關和及時資訊方面的義務和責任。

1005應盡專業上的注意

1005.1根據ISACA的《職業道德規範》，稽核員將執行盡職調查並保持專業上的注意。他們將保持高標準的行為和品格，避免從事可能有損自身或專業信譽的行為。稽核員應維護其在履行職責過程中所獲得資訊的隱私性和機密性。此外，不得將這些資訊用於個人利益，另除法律要求外，皆不得揭露這些資訊。

1006業務熟練

1006.1資訊稽核和從事確保工作人員以及協助執行稽核和確保業務的其他人員應具備執行所需工作的專業能力。
1006.2資訊稽核和從事確保工作人員應對查核事項具備充分的知識，以履行其在資訊稽核和確保業務中的職責。
1006.3資訊稽核和從事確保工作人員應通過適當的持續專業進修和訓練來保持專業能力。

1007聲明

1007.1資訊稽核和從事確保工作人員應審查評估查核事項所參照的聲明，以確定此等聲明能夠被稽核且聲明是充分、有效和相關的。

1008衡量標準

1008.1資訊稽核和從事確保工作人員對查核事項所選擇參照的衡量標準應客觀、完整、攸關、可靠、可衡量、易於理解、被廣泛認可、具權威性，並為所有讀者和用戶所理解或掌握的標準。
1008.2資訊稽核和從事確保工作人員應考慮衡量標準的可接受性，並關注那些公認、權威和公開的衡量標準。

執行標準

1201規劃中的風險評估

1201.1資訊稽核和確保工作應使用恰當的風險評估方法（即兼顧定量和定性因素的資料驅動方法）和佐證方法來制定總體的資訊稽核計畫，並確定有效分配資訊稽核資源的優先順序。
1201.2資訊稽核和從事確保工作人員在規劃各別專案時應辨別並評估與所稽核領域相關的風險。

1201.3資訊稽核和從事確保工作人員在規劃稽核業務時應考量查核事項風險、稽核風險以及企業所面臨的相關風險。

1202 稽核安排

1202.1資訊稽核和確保工作應制定總體策略計畫，形成短期和長期的稽核規劃。短期規劃包含將在一年內執行的稽核工作，而長期規劃則包含基於企業資訊和科技（I&T）環境中與風險有關事項的稽核，且這些稽核可能將在未來進行。

1202.2應與負責治理和監督職責的機構(例如：審計委員會)就短期和長期稽核規劃達成共識，並在企業內部進行傳達。

1202.3資訊稽核和確保工作應根據組織需求（例如：突發事件或計畫外措施）修改短期或長期的稽核行程表。如需增加對突發事件或計畫外措施的稽核，應將被取代的稽核重新安排到延後的日期時間。

1203稽核專案規劃

1203.1資訊稽核和從事確保工作人員應對每次資訊稽核和確保業務進行計劃，以確定所要執行的稽核程序的性質、時間安排和範圍。計畫應包括：

- 查核的領域
- 目標
- 範圍
- 資源（例如成員、工具和預算）和排程
- 時間表和交付成果
- 遵循適用法律、法規和專業稽核標準
- 對非關於法律及法規遵循業務採用風險導向方法處理
- 專案業務的特定問題
- 文件紀錄和報告要求
- 相關科技和資料分析技術的使用
- 相對於潛在效益的查核專案成本考慮
- 針對資訊稽核業務執行期間可能出現的情況（例如：範圍限制或關鍵人員不到位）的溝通和升級協議 在現場工作期間，隨著業務的進展，可能有必要修改原規劃期間所制定的稽核程序。

1203.2資訊稽核和從事確保工作人員應制定並記錄資訊稽核和確保業務稽核程序，描述用於完成稽核的步驟程序和說明。

1204執行與監督

1204.1資訊稽核和從事確保工作人員在工作中應依照核准的資訊稽核計畫，在既定的時間內進行工作，並涵蓋已識別的風險。

1204.2資訊稽核和從事確保工作人員應監督其團隊成員，以完成稽核目標並達到適用的專業稽核標準。

1204.3資訊稽核和從事確保工作人員應只接受在自己的知識和技能範圍內的任務，或有合理預期能夠在執行查核業務期間獲得相關技能或在他人督導下完成的任務。
1204.4資訊稽核和從事確保工作人員應獲得並保留充分且適當的證據來實現稽核目標。
1204.5資訊稽核和從事確保工作人員應記錄稽核過程，並對稽核工作與支持查核發現和結論的稽核證據進行說明。
1204.6資訊稽核和從事確保工作人員的查核發現和結論應有根本原因分析及證據解釋作為支持。
1204.7資訊稽核和確保從業人員應提供適當的稽核意見或結論，並包含透過其他額外測試流程獲得所需證據的範圍限制。

1205證據

1205.1資訊稽核和從事確保工作人員應獲取充分且適當的證據來得出合理的結論。
1205.2運用專業懷疑態度，資訊稽核和從事確保工作人員應評估所獲得的證據是否足以支持結論並實現稽核專案的查核目標。
1205.3與其他工作底稿一樣，資訊稽核和從事確保工作人員應在正式定義與核准的保留期限內保存證據。

1206使用其他專家的工作

1206.1資訊稽核和從事確保工作人員應考慮在適當的情況下將其他專家的工作用於稽核和確保業務。
1206.2資訊稽核和從事確保工作人員應在聘用前評估與核准其他專家的專業資格、能力、相關經驗、資源、獨立性以及品質控制流程的充分性。
1206.3資訊稽核和從事確保工作人員應評估、複核並評價其他專家的工作，以作為查核業務的一部份，並記錄對關於使用和信賴他們工作程度的結論。
1206.4資訊稽核和從事確保工作人員應確定稽核團隊之外的其他專家工作，是否足夠且完整的對目前稽核目標得出結論。從業人員還應明確地紀錄此項結論。
1206.5資訊稽核和從事確保工作人員應確定是否信賴其他專家的工作並直接納入報告，或是在報告中單獨引用。
1206.6如果其他專家的工作無法提供充分適當的證據，資訊稽核和從事確保工作人員應採用其他的測試程序來獲取充分適當的證據。
1206.7如果透過其他測試方式仍無法獲得所需的證據，資訊稽核和從事確保工作人員應提出適當的稽核意見或結論，並註明其範圍限制。

1207違規和非法行為

1207.1資訊稽核和從事確保工作人員應在工作中考量違規和非法行為的風險。
1207.2資訊稽核和從事確保工作人員應及時紀錄違規或非法行為並向適當單位通報。請注意，某些溝通（例如：與主管機關的溝通）可能會受到限制。因此，從業人員在溝通之前可能需要與負責治理和監督稽核職能部門的機構（例如董事會或審計委員會）進行討論。

報告標準

1401報告

1401.1資訊稽核和從事確保工作人員應以報告形式傳達各項稽核專案查核的結果。
1401.2資訊稽核和從事確保工作人員應確保稽核報告中所列的查核發現有充分且適當的證據予以支持。

1402追蹤改善活動

1402.1資訊稽核和從事確保工作人員應監督並定期向負責治理和監督稽核職能部門的機構（例如：董事會或審計委員會）報告管理階層在查核發現和改善建議方面的進度。報告應包括以下結論：管理階層是否已規劃並及時採取適當的行動來解決所報告的查核發現和改善建議。
1402.2應定期向審計委員會（如有）報告查核發現的總體改善執行情況。
1402.3如果確定與查核發現相關的風險已被接受，並且超出企業的風險胃納，應與高階管理階層討論此風險的接受程度。如果接受風險（尤其是未能解決風險的情況下），應提請審計委員會（如有）或董事會的注意。

本頁為空白頁

通用標準

通用標準1001：稽核組織章程

聲明	1001.1資訊稽核和確保工作應在稽核組織章程中訂定明確之稽核部門職能，指出目的、職責、職權和當責。
	1001.2資訊稽核和確保工作應將稽核組織章程提請負責治理和監督稽核部門的機構（例如：董事會或審計委員會）同意和正式核准。
	1001.3資訊稽核和確保工作應向執行階層與高階管理階層傳達稽核組織章程。此外，應在啟動會議或稽核專案委任書中與受查單位分享稽核組織章程的相關要素。
	1001.4透過定期複核稽核組織章程，確保稽核組織章程中反應的稽核和確保工作的職責與企業的使命和策略保持一致。如果企業的使命或策略發生變化，或稽核部門的職責發生變化，必須立即重新檢視稽核組織章程。

通用準則2001：稽核組織章程

2001.1從業人員應根據明確的授權來執行稽核職能。此授權一般應記錄在稽核組織章程中，並由治理機構（例如董事會或審計委員會）正式核准。如果為整個稽核職能的稽核組織章程，則應納入資訊稽核和確保的授權。

2001.2稽核組織章程的內容

2001.2.1	稽核組織章程應明訂資訊稽核和確保工作： ● 獨立性、道德倫理規範和標準。 ● 目的、職責、職權和當責。 ● 資訊稽核和從事確保工作人員在執行查核工作時遵循的協議，包括但不限於溝通和提報方式。 ● 受查單位在資訊稽核或確保專案期間的角色和職責。 ● 資訊稽核或確保工作在陳報違規和非法行為的任務。
2001.2.2	稽核組織章程應明確說明稽核職能的目的、職責、職權和當責（請參見2001.2.1）。以下部分詳述了這四個面向。
2001.2.3	稽核職能部門的目的是評估和測試管理階層實施控制措施的設計和執行。稽核組織章程應包含以下部分，以支持稽核職能達成其目的： ● **稽核職能的目標**提供了一個職能和組織框架，作為稽核職能運作的環境。 ● **稽核職能的目標和宗旨宣告**（如有）提供了一種結構化方法論，用於評估和改善風險管理流程、內部控制系統、及資訊系統運行及治理的設計與運作有效性。 ● **稽核職能的範圍**適用於整個企業或企業中的特定組織。 ● **稽核職能執行的工作**可能包括資訊系統稽核、合規性稽核、財務稽核、營運稽核、整合稽核、管理稽核、特定項目稽核（第三方服務稽核、舞弊稽核或鑑識稽核）、電腦鑑識稽核和職能稽核。此外還可能包括非稽核服務（例如：專案諮詢服務）。

2001.2.4	**稽核職能的職責**是為企業增加價值，確保將組織前景（例如：策略、宗旨、法規、和合規）整合到工作中，以及恪守職業期望（例如：道德、職業發展）。稽核組織章程應包含以下部分，以支持稽核職能的工作： ● **獨立性**，詳細說明對稽核職能和從業人員的獨立性要求的執行，如標準「1002組織獨立性」和「1003稽核的客觀性」中所述。資訊稽核和確保工作應透過以下方式確保其獨立性： ■ 定期評估其獨立性，至少每年一次。 ■ 制定與維護相關的正式協議，以識別和報告對獨立性的潛在損害。 應將獨立性評估的結果和有關損害的協議報告提供給負責治理和監督稽核職能的機構（例如：董事會或審計委員會）。 ● **與外部稽核公司的關係**，詳細說明內部資訊稽核和確保工作與外部稽核的信賴合作策略： ■ 與外部稽核員會面協調工作任務，以最大程度地減少重複工作。 ■ 提供核閱從業人員的工作底稿、文件記錄和查核證據。 ■ 在準備下一期稽核計畫時考量外部稽核所規劃的工作。 ● **受查單位的期望**，詳細說明受查單位可從稽核職能和從業人員獲得預期的服務和交付成果： ■ 說明與受查單位職責範圍有關的已發現的問題、後果和可能的解決方案。 ■ 在稽核報告中列入管理階層對查核發現的回應與矯正措施的可能性，這包括對相關服務水準協定（SLA）的引用，例如報告的交付、對受查單位申訴的回應、服務品質、績效審查、報告流程以及對查核發現的共識。 ● **受查單位要求**，詳細說明受查單位的職責，例如所有受查單位都必須配合、協助稽核職能和從業人員履行分配的職責。受查單位要求明確提供管理階層和稽核職能的職責。 ● **遵守專業標準**，這些標準由稽核員組織和以稽核員為會員標準制定機構所編製。 ● **標準合規性**，詳細說明稽核職能和從業人員應遵守的要求，例如稽核職能和從業人員將嚴格遵循所有ISACA ITAF稽核和確保標準及準則行事。

2001.2.5	稽核職能的**職權**應包含： ● 執行稽核專案的從業人員對相關資訊、系統（即系統日誌、活動和內建控制）、人員和位置的**接觸與讀取權限**。資訊稽核從業人員所代表的稽核職能： ■ 有權讀取執行稽核專案所需的任何和所有記錄、文件、系統和位置，而且可以尋求於高階管理階層的協助獲取此類讀取權限。 ■ 有權在執行稽核專案期間向員工、顧問或承包商獲取資訊。 ● 稽核職能和從業人員的職權**限制**（如有）。 ● 授權稽核職能查核的**受查作業流程**，例如稽核職能有權根據以風險為導向的稽核計畫來決定要查核的作業流程。
2001.2.6	稽核和確保工作的**當責**包括但不限於： ● 向適當的利害關係人以及負責治理和監督稽核和確保工作的機構（例如：董事會或審計委員會）**分發書面溝通文件**（例如：稽核報告和非稽核業務的備忘錄）。 ● **監控和報告管理階層**在就稽核建議達成的行動（即矯正措施）方面的**執行進度** ● 向負責治理和監督稽核和確保工作的機構（例如：董事會或審計委員會）**報告稽核和確保工作的績效指標**（例如：於稽核計畫和預算的績效）。 ● **向負責治理和監督稽核和確保工作的機構**（例如：董事會或審計委員會）**報告**職能部門的獨立性、可能對獨立性的損害，以及稽核職能的目的、職責、職權和當責等四個方面。 ● **品質確保流程**（例如：複核、客戶滿意度調查、任務績效調查），用於建立對受查單位與稽核職能相關需求和期望的理解。應依據稽核組織章程評估相關需求，以便在必要時改進服務、調整提供的服務或調整稽核組織章程。 ● **稽核業務的人員配置規則**，包括但不限於： ■ 遵循稽核組織章程，允許從業人員參與執行非稽核服務（例如：諮詢服務），以及此類服務的廣泛性質、時間和範圍，以確保獨立性和客觀性不受損害。這可消除或大幅度減少為每次非稽核服務獲得特定授權的必要性。 ■ 針對從業人員執行損害獨立性的非稽核服務後，與參與同一領域的稽核業務之前，建立最短等待時間間隔的規範。 ■ 針對稽核職能和從業人員的行為達成共識的行動，例如任何一方未履行職責時的處罰措施。 ■ 與受查單位溝通，詳細說明稽核職能與受查單位溝通的頻率和溝通管道。

標準1001和準則2001與COBIT® 2019的關聯

COBIT 2019管理目標	目的
MEA02 管理內部控制系統	使主要的利害關係人瞭解內部控制制度是否充分，進而建立起對營運的信任與實現企業目標的信心，以及對剩餘風險的充分瞭解。
MEA04 管理確保	促使組織設計和制定具效果與效率的確保機制，並採用公認的確保方法論，做為規劃，範圍界定，執行和後續追蹤提供指引。

通用標準1002：組織獨立性

聲明	1002.1對資訊稽核和確保工作對於專案所有相關的問題，應避免利益衝突和不當影響。如果發現獨立性受到（實質上或形式上的）損害，應向有關單位揭露。
	1002.2資訊稽核和確保工作應有業務報告關係（例如：向董事會報告），以支持該職能能夠免於不當影響。
	1002.3資訊稽核和確保工作應有行政報告關係，以支持該職能能夠不受阻礙的履行其職責（例如：專案範圍、現場工作或報告）。

通用準則2002：組織獨立性

2002.1簡介 本準則旨在建構為提供資訊稽核和確保工作獨立性上的資訊：

2002.2在企業中的定位

2002.3報告層級

2002.4評估獨立性

2002.2在企業中的定位

2002.2.1	為實現組織獨立性，稽核職能在企業中的定位必須使其能夠不受干擾的履行職責。可通過下列方式實現： ●在審計委員會的章程中將稽核職能確立為獨立的職能或營運部門以外的單位。不付予稽核職能分配任何營運職責或作業活動。 ●確保稽核職能的直屬上級在企業內部之層級有助於實現其組織獨立性。如果稽核職能向營運部門主管彙報工作，可能會損害其組織獨立性。
2002.2.2	稽核職能應避免在需要承擔管理職責的資訊計畫中擔任非稽核角色，因為此類角色可能會損害其未來的獨立性。稽核組織章程應確立稽核職能的獨立性和責任。如果安排稽核員規劃或參與其管理職責負責領域的業務時，稽核職能的獨立性可能會受到損害。請注意，資訊稽核和確保工作可以與企業外部稽核公司合作確認構成直接或間接管理的職責。這兩各團隊還可以確定稽核員履行直接管理職責與參與該領域內業務工作間可接受的時間間隔。

2002.3報告層級

2002.3.1	稽核職能的直屬上級在企業內部的層級將有助於實現完整的組織獨立性。該獨立性應在稽核組織章程中定義，並由稽核職能定期（至少每年一次）向董事會和治理機構進行確認。
2002.3.2	為確保稽核職能的組織獨立性，應向治理機構（例如：董事會）報告以下內容，以徵求他們的意見或核准： ●稽核資源規劃和預算。 ●以風險為導向的稽核計畫。 ●稽核職能針對資訊稽核活動執行的績效追蹤。 ●對重大範圍或資源限制的後續追蹤。
2002.3.3	為確保稽核職能的組織獨立性，董事會和高階管理階層需給予明的確支持。高階管理階層的支持可以包括與組織各個層級的書面溝通。

2002.4評估獨立性

2002.4.1	稽核職能應定期評估獨立性並與負責治理和監督稽核職能的機構（例如：董事會或審計委員會）進行確認。至少每年評估一次。評估應考慮以下因素： ●人際關係的變化。 ●經濟利益。 ●先前的工作分配和職責，及當前工作任務角色和職責的變更。
2002.4.2	稽核職能需要揭露與組織獨立性有關的潛在問題，並與董事會或治理機構討論。需要在稽核組織章程中定義並確認解決方案。

標準1002和準則2002與COBIT® 2019的關聯

COBIT 2019治理與管理目標	目的
EDM01 確保治理架構的設置和維護	提供與企業治理方法整合的一致方法。資訊與科技(I&T)相關決策應該與企業的策略和目標保持一致，並實現期望的價值。為此，應確保I&T相關流程得到有效和透明的監督，符合法律、合約和監管要求，以及滿足董事會成員的治理要求。
APO01 管理資訊與科技管理框架	實施一致的管理方法，以滿足企業治理需求，涵蓋治理的組成要素，如管理流程；組織架構；角色和職責；可靠且可重複的活動；資訊專案；政策和程序；技能和能力；文化和行為；以及服務、基礎設施和應用程式。
MEA04 管理確保	促使組織設計和制定具效果與效率的確保機制，並採用公認的確保方法論，做為規劃，範圍界定，執行和後續追蹤提供指引。

通用標準1003：稽核的客觀性

聲明	1003.1資訊稽核和從事確保工作人員，對於所有與稽核和確保專案相關的問題都應保持客觀性。

通用準則2003：稽核的客觀性

本準則為資訊稽核和從事確保工作人員提供了一個框架，使其能夠：

- 確定客觀性是否可能或看似可能受到影響。
- 在客觀性受到或看似可能受到影響時，考慮稽核流程的潛在替代方法。
- 減輕或消除因履行非稽核角色、職能和服務的資訊稽核和確保工作從業人員造成客觀性受損帶來的影響。
- 確定所需客觀性可能或看似可能受到時的揭露要求。
- 進行資訊稽核和確保專案業務時必須以一種公平、公正的心態來確認查核發現問題並得出結論。
- 在所有專案查核階段都應注意對客觀性的潛在損害。
- 向適當的機構揭露客觀性受損影響的詳細資訊。

2003.1簡介 本準則旨在建構為提供有關以下關鍵資訊稽核和確保專案查核主題的資訊：

2003.2概念框架

2003.3威脅和保障措施

2003.4管理威脅

2003.5非稽核服務或角色

2003.6不損害獨立性的非稽核服務或角色

2003.7損害獨立性的非稽核服務或角色

2003.8稽核組織章程和非稽核或諮詢服務角色

2003.9報告

2003.2概念框架

2003.2.1	在評估對客觀性或獨立性的威脅時，可能會涉及不同情況或數種情況的組合。要定義對客觀性或獨立性造成威脅的所有情況並制定相應的行動是不可能的。因此，本準則建立了一個概念框架，要求專業人員識別、評估並解決對客觀性或獨立性的潛在威脅。概念框架方法有助於遵守獨立性標準，並能夠根據可能對獨立性造成威脅的不同情況進行調整。
2003.2.2	從業人員應將概念框架方法應用於： ● 識別對客觀性或獨立性的威脅。 ● 評估所識別威脅的重要性。 ● 必要時採取保障措施，以消除威脅或將威脅降至可接受的水準。
2003.2.3	如果從業人員確定沒有適當的保障措施，或者無法應用此類措施來消除對客觀性的威脅或將威脅降至可接受的水準，則應消除造成威脅的情況或關係，或者拒絕或終止相應的稽核或確保專案。如果從業人員無法拒絕或終止專案，必須向治理機構適當揭露客觀性或獨立性受到的損害，並在稽核專案產生的報告中加以說明。
2003.2.4	從業人員在履行非稽核服務或角色時，應考慮運用ITAF準則來識別對客觀性的潛在威脅、評估威脅的重大性、和執行適當的保障措施。
2003.2.5	稽核員不應該在現在或未來的稽核或確保專案，由同一位稽核員執行同一領域範圍的非審計服務或角色，如果企業沒有其他資源（即備用的內部或外部資源），則應由稽核長（或稽核副總/主任）和正式負責治理和監督稽核職能的機構（例如：董事會或審計委員會）核准該稽核員參與該非稽核服務。

2003.3威脅和保障措施

2003.3.1	各種各樣的關係和環境都可能對客觀性造成威脅。當一種關係或情況造成威脅時，可能會損害或被認為會損害專業之客觀性。一種情況或關係可能對客觀性造成多種的威脅。威脅可以分為以下一種或多種類別： ● **自我利益**—財務或其他利益會對專業判斷或行為造成不當影響。 ● 自我檢視—從業人員無法適當的評估自己或稽核職能部門其他人員先前作出的判斷或服務結果，而從業人員在對當前查核專案形成判斷時將依賴於這些結果。 ● **倡導**—從業人員去提升受查單位的立場，以至於專業客觀性受到損害。 ● **熟識**—由於與受查單位有長期或密切的關係，從業人員過於為受查單位的利益考慮，或者過於接受受查單位的工作、觀點或論點。 ● **恐嚇**—從業人員實際受到或感知到的壓力（包括試圖對從業人員施加不當影響的行為）使其無法以正直和客觀的立場行事。 ● **偏見**—政治、思想觀點、社會、心理或其他信念影響從業人員採取不客觀的立場。 ● **參與管理階層**—從業人員擔任管理角色，或者代表接受稽核或確保業務的實際執行管理職能，從而導致客觀性受到損害。
2003.3.2	可設計和實施保障措施，以減輕或盡量減少對客觀性的威脅。針對已識別的威脅，從業人員可考慮的保障措施包括： ● 企業和稽核職能部門的內部程序，能夠確保在分配查核工作時作出客觀的選擇（例如：從業人員不稽核其過往直接管理職責的領域）。 ● 由稽核職能部門外部來指派稽核專案管理者和人員，例如從其他職能部門、事業部或外部組織借用人員，以增補稽核人員。 ● 定期輪換資訊稽核任務，從而降低從業人員對所分配查核領域人員的熟悉程度。 ● 適當的人員僱用作業，例如背景調查和審查，以增加從業人員免於偏差或利益衝突（即競爭性的職業或個人利益）的可能性。 ● 如果某人的利益或關係對客觀性造成威脅，應將其調離相關的查核專案。 ● 適當的文件記錄和報告要求，以確保專業獨立性評估記錄在工作底稿中，在可交付成果中有著一致性的報告。 ● 分配獨立的資源（來自稽核職能部門內部或之前引用的其他來源）來執行同儕審查，或在規劃、現場工作和報告過程中擔任獨立觀察員。 ● 由公認的第三方（例如：業內公認的權威機構或獨立專家）對從業人員產出的報告、溝通或資訊進行外部審查。

2003.4管理威脅

2003.4.1	稽核職能部門和從業人員應確定已識別對客觀性的威脅，是否已被消除或降至可接受的水準。對客觀性的威脅必須得到管理，因為喪失客觀性可能會損害專業人士在執行稽核或確保業務期間保持專業判斷不受影響的能力，也可能使從業人員或稽核職能部門面臨一些情況，導致合理和知情的第三方認定資訊稽核和確保團隊的某個成員的誠信、客觀性或專業懷疑態度已經受到損害。

2003.5非稽核服務或角色

2003.5.1	在許多企業中，管理階層、資訊人員和內部稽核職能部門的期望是，從業人員可參與履行非稽核服務或角色，例如： ● 就科技、應用和資源等領域的相關資訊策略提供建議。 ● 評估、選擇和導入科技。 ● 評估、選擇、客制和導入第三方資訊應用程式和解決方案。 ● 設計、開發和導入客製的資訊應用程式和解決方案。 ● 建立與各種資訊職能有關的良好案例、政策和程序。 ● 設計、開發、測試和導入資訊安全和資訊控制措施。 ● 為資訊專案提供建議。
2003.5.2	履行非稽核服務或角色，通常以專職或兼職的形式參與資訊方案與資訊專案團隊，擔任顧問或諮詢角色。資訊稽核和確保從業人員可透過以下活動履行非稽核職能： ● 將資訊稽核和確保人員臨時抽調或借調給資訊專案團隊承擔專職工作。 ● 將資訊稽核和確保人員分配到資訊專案兼任其他工作，例如專案指導小組、專案工作小組、評估團隊、談判和簽約團隊、導入團隊、品質驗證團隊或問題排除團隊。 ● 臨時充當資訊專案或資訊控制的顧問或複查人員。
2003.5.3	如果從業人員當前履行非稽核服務或角色的領域，是目前或未來進行稽核或確保業務的對象，則可能會對專業客觀性或獨立性造成威脅或被視為存在這種威脅。在這種情況下，從業人員的獨立性和客觀性會被認為受到執行非稽核服務或角色的損害。
2003.5.4	履行非稽核服務或角色的從業人員，應使用概念框架來評估非稽核服務或角色是否會損害其執行目前或未來進行稽核或確保業務的客觀性或獨立性。如果執行非稽核服務或角色的領域，對於該領域的業務查核事項或利害關係人具有重要或實質性意義，那麼概念框架適用於這些業務。如有必要，從業人員應尋求資訊稽核和確保同事及管理階層或治理機構的指導，確定是否可以實施保障措施，以充分降低對客觀性的任何實際或認知的威脅。

2003.5.5	在開始執行非稽核服務或角色之前，從業人員應與資訊稽核管理階層或治理機構就以下事項達成共識並做相關的記錄： ● 非稽核服務或角色的目標。 ● 待履行的非稽核服務或角色的性質。 ● 受查單位接受有關非稽核服務或角色的職責。 ● 與非稽核服務或角色有關的專業職責。 ● 非稽核服務或角色的限制。 ● 對從業人員將來可提供的稽核服務範圍的限制。
2003.5.6	如果所履行的非稽核服務或角色，導致從業人員在執行資訊稽核或確保業務時的客觀性或獨立性可能受損或被認為受損時，則資訊稽核和確保管理階層應採取以下保障措施： ● 密切監督稽核的執行。 ● 評估所履行的非稽核服務或角色導致客觀性或獨立性受損的重大跡象，並啟動必要的保障措施。 ● 向治理機構報告客觀性或獨立性可能受到的損害，以及所採取的保障措施。

2003.6不損害獨立性的非稽核服務或角色

2003.6.1	日常、行政性或涉及瑣碎事務的活動通常被視為非管理責任，並因此不會損害其客觀性。
2003.6.2	如果落實足夠的保障措施，則不會損害獨立性或客觀性的非稽核服務或角色，包括提供資訊風險及控制方面的日常建議。
2003.6.3	為避免在接受（或可能接受）稽核或確保業務的領域，履行非稽核服務或角色時出現承擔管理職責的風險，從業人員僅在管理階層執行或將執行與非稽核服務或角色相關的以下職能時，方可履行非稽核服務或角色： ● 承擔所有管理職責。 ● 指定具備適當技能、知識或經驗的個人（最好是高級管理人員）來監督相關服務。 ● 評估所履行的服務的充分性和結果。 ● 對服務的結果承擔責任。 從業人員應記錄其對於管理階層能否有效監督所履行的非稽核服務或角色的考量。

2003.7損害獨立性的非稽核服務或角色

2003.7.1	如果從業人員承擔管理職責或執行管理活動，可能會對獨立性造成重大威脅，以至於沒有任何保障措施能將風險降至可接受水準。對於活動是否承擔管理職責取決於具體情況，需要進行專業判斷。通常被認為承擔管理職責的活動包括： ● 制定政策和策略方向。 ● 指導員工的行為並對其承擔責任。 ● 授權交易。 ● 決定執行稽核職能部門、內部稽核職能部門、組織、公司或其他第三方的建議。 ● 對內部控制的設計、執行或維護承擔責任。 ● 承擔資訊專案或行動方案的管理職責。
2003.7.2	除了承擔管理職責，以下非稽核服務或角色也可能損害獨立性和客觀性： ● 從業人員實質性參與監督或執行，對稽核或確保業務的主要事項具有實質性或重要意義的資訊系統的設計、開發、測試、安裝、配置或操作。 ● 設計對稽核或確保業務的主要事項，具有實質性或重要意義的資訊系統控制措施。 ● 從業人員擔任治理角色，在作出管理決策或核准政策和標準方面承擔獨立或聯合責任。 ● 提供建議，這些建議構成管理決策或履行管理職能的主要依據。
2003.7.3	以下非稽核服務被認為會對客觀性造成重大威脅，以至於沒有任何保障措施能夠將這種風險降至可接受的水準： ● 承擔管理職責或執行管理活動。 ● 從業人員實質性參與監督或執行，對稽核或確保業務的主要事項具有實質性或重要意義的資訊系統的設計、開發、測試、安裝、配置或操作。 ● 設計對當前或計畫未來稽核業務的主要事項，具有實質性或重要意義的資訊系統控制措施。 ● 從業人員擔任治理角色，在獨立或聯合作出管理決策或核准政策與標準方面承擔責任。 ● 提供建議，這些建議構成管理決策的主要依據。

2003.8稽核組織章程和非稽核服務或諮詢角色

2003.8.1	資訊稽核組織章程應規定是否允許從業人員履行非稽核服務或角色，以及此類服務的廣泛性、時間和範圍，以確保從業人員在可能的稽核技術方面不損害的客觀性和獨立性。這可消除或最大程度減少為每項非稽核服務或角色逐一獲得特定授權的必要性。
2003.8.2	從業人員應提供合理的保證，確保特定的非稽核服務或角色的職權範圍（TOR）符合稽核組織章程。在TOR中應明確說明偏離的情況，並由資訊稽核和確保管理階層或治理機構核准。
2003.8.3	如果稽核組織章程未規定非稽核服務或角色，或者沒有稽核組織章程，從業人員應向資訊稽核和確保管理階層以及治理機構報告其參與履行非稽核服務或角色的性質。 從業人員參與非稽核服務或角色的時間和程度，應受履行服務或角色的職能管理階層簽署個人職責範圍的範圍，並由負責治理的人員核准。

2003.9報告

2003.9.1	如果執行資訊稽核或確保業務從業人員的客觀性或獨立性受到損害或可能受到損害，並且治理機構決定繼續該業務時，則資訊稽核和確保業務報告應包含充分的資訊，使讀能夠瞭解該潛在損害的性質。 從業人員應考慮在資訊稽核和確保業務報告中揭露的資訊包括： ● 參與資訊稽核和確保業務且客觀性或獨立性可能受到損害的從業人員姓名和資歷。 ● 對客觀性或獨立性潛在損害的分析與描述。 ● 在執行業務和報告過程中，為消除或減輕對獨立性和客觀性的威脅而採取的保障措施。 ● 向治理機構揭露客觀性或獨立性可能受到損害，以及他們核准執行或繼續執行確保業務、與非稽核服務或角色的文件。

標準1003和準則2003與COBIT® 2019的關聯

COBIT 2019 管理目標	目的
MEA02 管理內部控制系統	使主要的利害關係人瞭解內部控制制度是否充分，進而建立起對營運的信任與實現企業目標的信心，以及對剩餘風險的充分瞭解。
MEA03 管理外部要求合規	確保企業符合所有適用的外部要求。
MEA04 管理確保	促使組織設計和制定具效果與效率的確保機制，並採用公認的確保方法論，做為規劃，範圍界定，執行和後續追蹤提供指引。

通用標準1004：合理預期

聲明	1004.1資訊稽核和從事確保工作人員應合理預期能夠按照適用的資訊稽核和確保標準（必要時還包括其它可得出專業性意見或結論的產業標準或適用的法律法規）來完成稽核和確保專案。
	1004.2資訊稽核和從事確保工作人員應合理預期稽核和確保業務的範圍，使他們能夠就查核事項得出結論並解決範圍限制的問題。
	1004.3資訊稽核和從事確保工作人員應合理預期管理階層瞭解其在提供執行業務所需的適當、相關和及時資訊方面的義務和責任。

通用準則2004：合理預期

2004.1簡介 本準則的目的是協助資訊稽核和確保從業人員在執行稽核業務時貫徹合理預期原則。本準則進一步協助資訊稽核和從事確保工作人員解決範圍限制問題，並提供有關接受業務條款變更的指引。

2004.2標準和法規

2004.3範圍

2004.4範圍限制

2004.5資訊

2004.6接受業務條款的變更

2004.7其他注意事項

2004.2標準和法規

2004.2.1	從業人員應在開始稽核業務之前，收集和評估稽核組織章程和法規中列出的所有適用標準，並在稽核過程中持續查閱這些標準，以確定是否能夠合理預期按照這些標準和法規完成稽核業務，並確保稽核業務能夠得出專業性的意見或結論。
2004.2.2	如果從業人員確定稽核業務無法遵循一項或多項適用的標準和法規，因此無法得出專業性的意見或結論，則應： ● 向資訊稽核和確保管理階層以及治理機構報告已發現的不符合標準和法規的問題。 ● 建議修改業務條款或拒絕建議的業務。

2004.3範圍

2004.3.1	在開始稽核業務之前，從業人員應確定稽核範圍已明確記錄在案，並且能夠就主要事項得出專業性的意見或結論。
2004.3.2	稽核業務的範圍應明確紀錄，關於業務範圍所涵蓋的領域（例如：流程、活動、系統）應沒有解釋的空間。如果範圍的描述過於籠統，將導致從業人員不能確定是否已評估範圍內的所有領域，從而無法得出專業性的意見或結論。
2004.3.3	如果從業人員確定稽核業務的範圍使他們無法得出專業性的意見或結論，則應： ● 向資訊稽核和確保管理階層以及稽核職能部門的治理機構報告已發現的範圍問題。 ● 建議修改業務條款或拒絕建議的業務。

2004.4範圍限制

2004.4.1	特定的範圍限制可能出現在稽核業務之前或期間。這些範圍限制可能到受不同因素的影響，例如： ● 無法及時獲得完成稽核業務所需的適當資訊。 ● 受查方關鍵人員無法接受稽核。 ● 分配的時間不足以完成整個稽核業務的範圍。 ● 管理階層試圖將稽核業務的範圍限制在指定的領域內。 ● 稽核業務的範圍太小或太大，無法得出有關主要事項的結論。 ● 分散式處理的程度導致從業人員難以對整個主要事項得出結論。 ● 具備相應技能的從業人員人數不足以執行目前業務範圍內的稽核業務，且。 ● 稽核職能部門的報告結構（例如：如果稽核職能部門不是向企業內部的適當層級彙報工作， 可能會被指示不要評估範圍內的某些要素）。 ● 第三方合約也可能造成範圍限制。 ● 客戶文檔交付延遲。 ● 針對之前查核發現，或受查方自己發現現有不符合項的矯正措施工作仍在進行中。

2004.4.2	從業人員應考量，範圍限制是否使他們仍能夠合理預期對稽核業務得出專業性的意見或結論。如果從業人員確定無法滿足這一條件，則不應承接該業務。
2004.4.3	從業人員應考量，範圍限制是否仍允許能合理預期稽核業務得出的專業性意見或結論，則可以接受或繼續執行稽核業務。應在資訊稽核和確保業務報告中明確說明範圍限制。
2004.4.4	考量業務範圍是否充分，使稽核師能夠對主要事項提出意見。當完成業務所需要的資訊無法取得，或當資訊稽核或確保業務的時間不足，或管理階層試圖將範圍限制在特定領域時，則有可能出現範圍限制。在這種情況下，可以考慮其他的業務類型，例如審查控制措施，遵守規定的標準與慣例、或對協議、許可、法律和法規的遵守情形。

2004.5資訊

2004.5.1	稽核組織章程將規定與稽核業務執行有關的資訊、系統、人員和位置的存取權限。
2004.5.2	在進行稽核業務之前，從業人員應識別並指出對於存取權限受到的限制問題，以及獲得適當、相關和及時的稽核業務所需的資訊， 從業人員應合理預期，完成稽核業務所需的存取權限符合稽核組織章程的規定，或者對規定的潛在偏離不會妨礙他們就主要事項達成的專業性意見或結論。

2004.5.3	如果從業人員認為，資訊存取權限使他們無法得出專業性的意見或結論，則應： ● 向資訊稽核和確保管理階層以及稽核職能部門的治理機構，報告已發現的問題，這些問題關係著他們能否及時獲取適當的相關資訊。 ● 建議修改業務條款或拒絕協議的稽核業務。
2004.5.4	執行稽核或確保業務可能需要評估高階管理階層的活動。應在執行稽核業務之前評估這種可能性。從業人員應評估他們對此類個人或相關資訊的存取是否會遇到阻礙。執行稽核業務之前可能需要採取的降低措施包括但不限於： ● 稽核組織章程規定，為稽核職能部門和專業人員分配適當的授權。 ● 治理機構（例如：董事會和審計委員會）做出明確的書面支持。 ● 當需接觸高階管理階層或高級管理階層人員的資訊時，由董事會或高階管理階層成員出席。

2004.6接受業務條款的變更

2004.6.1	如果從業人員根據自己的專業判斷，認為沒有正當理由接受稽核業務條款的變更，則不應接受。
2004.6.2	如果在稽核業務期間，從業人員被要求接受會降低確保水準的條款變更，則應根據自己的專業判斷確定這樣做是否有正當理由。
2004.6.3	如果稽核業務的條款有變更，應記錄下來並由從業人員以及稽核和確保管理階層正式核准。資訊稽核和確保業務報告應明確提及這些變更。
2004.6.4	如果從業人員不接受稽核業務條款的變更，並且與稽核和確保管理階層協商之後，管理階層不允許他們繼續執行原來的稽核業務，從業人員應： ● 退出稽核業務。 ● 根據自己的專業判斷，確定是否將情況報告給治理機構，例如董事會甚至是監管者。

2004.7其他注意事項

2004.7.1	資訊稽核和確保從業人員應： ● 只能在可以按照專業標準圓滿完成工作的情況下，承接資訊稽核或確保業務。 ● 只能在可以參照相關標準來評估所涉查核事項的情況下，承接資訊稽核或確保業務。 ● 複核資訊稽核或確保業務的範圍，以確定被明確記錄，並可以清楚地傳達給受查方。 ● 識別並指出在完成業務過程中存在的限制，包括但不限於及時存取適當的相關資訊。 ● 對於無法從受查方管理階層獲得書面聲明的情況作出準備。例如可以獲得口頭陳述並記錄在工作底稿中。

標準1004和準則2004與COBIT® 2019的關聯

COBIT 2019 管理目標	目的
MEA03 管理外部要求合規	確保企業符合所有適用的外部要求。
MEA04 管理確保	促使組織設計和制定具效果與效率的確保機制，並採用公認的確保方法論，做為規劃，範圍界定，執行和後續追蹤提供指引。

通用標準1005：應盡專業上的注意

聲明	1005.1根據ISACA的《職業道德規範》，稽核員將執行盡職調查並保持專業上的注意。他們將保持高標準的行為和品格，避免從事可能有損自身或專業信譽的行為。稽核員應維護其在履行職責過程中所獲得資訊的隱私性和機密性。此外，不得將這些資訊用於個人利益，另除法律要求外，皆不得揭露這些資訊。

通用準則2005：應盡專業上的注意

2005.1本準則的目的是闡明術語「應盡專業上的注意」，該詞意指根據《ISACA職業道德規範》誠信和謹慎地規劃、執行和報告稽核業務。請注意，應盡專業上的注意指合理的謹慎和專業能力，而不是絕對正確或超常的表現。

2005.2專業上的注意和專業能力

2005.3應用

2005.4稽核專案的生命週期

2005.5溝通

2005.6獲取和管理資訊

2005.7其他注意事項

2005.2專業上的注意和專業能力

2005.2.1	應盡專業上的注意是指在執行工作時進行專業判斷。應盡專業上的注意意味著從業人員以專業上的注意、盡職、誠信和謹慎的態度處理需要運用專業判斷的事項。他們應在整個業務過程中保持這種態度。
2005.2.2	從業人員在態度和行為上都應保持專業能力、客觀性和獨立性，以處理與稽核業務有關的所有事項。在解決問題和得出結論時，他們應做到誠實、公平和公正。
2005.2.3	進行應盡專業上的注意要求從業人員考慮是否可能存在效率不彰、濫用、錯誤、範圍受限、能力不足、利益衝突或欺詐的情況。此外，從業人員還應注意可能出現這些問題的特定條件或活動。
2005.2.4	從業人員應時刻瞭解並遵守專業標準的發展，以表現出充分理解且具備足夠的專業能力實現資訊稽核和確保目標。
2005.2.5	從業人員應盡職地執行稽核業務，同時遵守專業標準和法律、法規的要求。

2005.3應用

2005.3.1	從業人員在稽核的各個方面應盡專業上的注意，包括但不限於評估稽核風險、承接稽核業務、確立稽核範圍、制定稽核目標、規劃稽核、執行稽核工作、分配稽核資源、進行稽核測試、評估測試結果、記錄稽核工作、得出稽核結論、報告和交付稽核結果，以及執行追蹤活動。為此，從業人員應確認或評估： ● 滿足資訊稽核和確保標準所需的資源類型、層級、技能和專業能力。 ● 已識別風險的重要性，以及這些風險對稽核主題的潛在影響。 ● 收集到稽核證據的充分性、有效性和相關性。 ● 從業人員所依賴其他人的專業能力、誠信以及得出的結論。
2005.3.2	應盡專業上的注意，還要求從業人員在執行所有業務時牢記合理保證的概念。
2005.3.3	從業人員應以合法、誠實的方式維護利害關係人的利益，同時保持高標準的行為和品質，抵制有失職業誠信的行為。

2005.4稽核專案的生命週期

2005.4.1	從業人員應盡專業上的注意，及時並全面地規劃稽核業務，確保獲得適當的資源，並且能夠及時完成稽核業務。分配到專案的從業人員應具備執行稽核業務所需的技能、知識及相關的專業能力。
2005.4.2	從業人員在執行稽核業務時應盡專業上的注意，即遵守適當的專業標準，確保得出高品質和完整的稽核結論或意見。
2005.4.3	從業人員應盡專業上的注意，確認管理階層的矯正措施能夠有效地解決稽核發現的問題。

2005.5溝通

2005.5.1	在專案開始前，應將已定義的角色和職責傳達給團隊成員，確保團隊在稽核業務期間遵守適當的專業標準。
2005.5.2	在稽核期間，從業人員應與受查方和有關的利害關係人進行適當的溝通，確保他們配合工作。
2005.5.3	從業人員應將稽核結果告知稽核的受查方。
2005.5.4	從業人員應記錄關於應用專業標準方面的問題並與有關各方溝通，以解決這些情形。
2005.5.5	向有關各方通報工作結果時，從業人員應盡專業上的注意。

2005.6獲取和管理資訊

2005.6.1	從業人員應合理預期管理階層理解其承擔的義務和責任，及時提供執行稽核業務所需的適當的相關資訊。
2005.6.2	從業人員應採取合理的措施，維護其在履行職責時所獲得資訊的隱私性和機密性，除應法律要求予以揭露的情況外。不得將此類資訊用於牟取個人利益，也不得向無關的第三方人士洩漏。
2005.6.3	應根據組織政策以及相關法律、法規和規章獲取、使用、保留和妥當處置資訊。

2005.6.3	應根據組織政策以及相關法律、法規和規章獲取、使用、保留和妥當處置資訊。

2005.7其他注意事項

2005.7.1	資訊稽核和確保從業人員應： ● 誠信與謹慎的執行稽核專案。 ● 表現出足夠的知識和能力，以實現專案目標。 ● 在整個專案過程中保持專業懷疑的態度。 ● 通過及時掌握和遵循專業標準的發展以保持專業能力。 ● 向團隊成員傳達其角色和職責，並確保團隊在執行專案過程中遵循適當的標準。 ● 解決在執行專案過程中遇到的標準應用方面的所有問題。 ● 在整個專案過程中與有關的利害關係人保持有效溝通。 ● 在整個專案過程中採取合理的措施保護獲得或衍生的資訊，防止意外洩露或揭露給未經授權的人士。 ● 在執行所有專案時，要牢記合理保證的概念。測試的程度將視業務類型的不同而有所區別。 ● 考慮相關科技和資料分析技術的運用，及稽核師使用這些科技和技術的能力。 ● 相對于潛在效益考慮專案成本。

標準1005和準則2005與COBIT® 2019的關聯

COBIT 2019 管理目標	目的
EDM01 確保治理架構的設置和維護	提供與企業治理方法整合的一致方法。資訊與科技(I&T)相關決策應該與企業的策略和目標保持一致，並實現期望的價值。為此，應確保I&T相關流程得到有效和透明的監督，符合法律、合約和監管要求，以及滿足董事會成員的治理要求。
APO07 管理人力資源	優化人力資源能力，以滿足企業目標。
MEA03 管理外部要求合規性	確保企業符合所有適用的外部要求。
MEA04 管理確保	促使組織設計和制定具效果與效率的確保機制，並採用公認的確保方法論，做為規劃，範圍界定，執行和後續追蹤提供指引。

通用標準1006：業務熟練

聲明	1006.1資訊稽核和從事確保工作人員以及協助執行稽核和確保業務的其他人員應具備執行所需工作的專業能力。
	1006.2資訊稽核和從事確保工作人員應對查核事項具備充分的知識，以履行其在資訊稽核和確保業務中的職責。
	1006.3資訊稽核和從事確保工作人員應通過適當的持續專業進修和訓練來保持專業能力。

通用準則2006：業務熟練

2006.1簡介 本準則協助資訊稽核和確保從業人員獲得必備的技能和知識，以及在執行稽核專案的過程中保持專業能力，本準則旨在為以下關鍵資訊稽核和確保業務主題提供系統化資訊：

2006.2專業能力

2006.3評估

2006.4達到所需的專業能力水準

2006.5其他注意事項

2006.2專業能力

2006.2.1	專業能力是指通過適當的教育與經驗獲得的技能、知識和專業技術水準，以適當的執行稽核業務。
2006.2.2	資訊稽核和確保管理階層應基於適當的基準，傳達稽核業務中的不同角色所需或預期達到的專業能力水準，並確保這些基準得到定期的審查和更新。資訊稽核和確保管理階層應記錄不同工作層級的專業能力要求，例如記錄工作、職位描述，或制定技能矩陣來表示不同工作層級所需的專業能力。
2006.2.3	資訊稽核和確保管理階層應合理保證，可獲得執行資訊稽核計畫中定義的稽核業務所需的稱職資源。在開始稽核業務之前，應確認並確保可獲得所需的稱職資源。
2006.2.4	資訊稽核和確保管理階層應確保團隊成員有能力執行稽核業務。識別團隊成員的核心專業能力有助於有效地利用可用資源。
2006.2.5	從業人員應合理保證其具備所需的專業能力水準。他們應獲取執行任務所需的專業知識和技術技能。
2006.2.6	從業人員應具備的技能和知識因其在稽核業務中的職位和角色而異。對管理技能和知識的要求應與職責層級相稱。

2006.2.7	技能和知識包括熟練地識別和評估風險與控制，以及在稽核工作中應用和使用的稽核工具及技術。從業人員應具備分析和技術知識，以及訪談、人際關係與簡報方面的技能。
2006.2.8	從業人員應具備適當的知識，能夠識別和確定潛在或偏離情況對稽核業務的影響並進行適當的溝通。
2006.2.9	從業人員應該有能力識別潛在的舞弊跡象。
2006.2.10	除了資訊科技知識外，從業人員還應具備一般商業基礎知識，例如經濟、金融、會計、風險、稅收和法律，以防忽視潛在的問題或不足之處。
2006.2.11	從業人員應與團隊成員分享他們的經驗、被採用的較佳實務、經驗教訓及獲得的知識，以提高他們的專業能力。可以通過團隊建立活動、研討會、會議、討論會、講座和其他互動方式提高團隊成員的專業能力。
2006.2.12	為確保適當技能的可用性，應評估獲取這些技能的替代方案，例如分包特定資源，外包一部分資訊稽核和確保任務，或推遲稽核業務直到具備所需的技能。
2006.2.13	可以通過外包部分或全部業務的方式來獲得外部專業知識。外包資源與內部從業人員的通力合作可確保知識與技能在內部得到發展和保持。
2006.2.14	如果將稽核業務的部分外包或尋求專家協助，必須合理保證外包機構或外部專家擁有必備的專業能力。
2006.2.15	如果持續尋求專家協助，則應根據專業標準或基準定期衡量、監控和審查外部專家的專業能力。

2006.3評估

2006.3.1	從業人員應持續監督自己的技能和知識，以保持適當的專業能力水準。資訊稽核和確保管理階層應定期評估相關從業人員的專業能力。
2006.3.2	從業人員的績效評估方式應遵循公平、透明、易於理解、無歧異且無偏見，並在指定的就業環境中被視為普遍可接受的做法。
2006.3.3	評估衡量標準和程序應得到明確規定，但可能因地理位置、政治環境、任務性質、文化或其他類似情況而異。
2006.3.4	如果是一組從業人員，則應在團隊內部對不同組別的個人或團體進行跨職能評估。
2006.3.5	如果只有一名獨立的從業人員，則應在可行的情況下進行同儕評估。如果無法進行同儕評估，應進行自我評估並做成紀錄。
2006.3.6	應由適當層級的管理階層評估從業人員的績效。
2006.3.7	應適當的處理於評估過程中發現的差距。

2006.4達到所需的專業能力水準

2006.4.1	應記錄和分析所發現的實際專業能力水準與預期專業能力水準間的差距。如果有人員存在嚴重的能力不足情形，則不應安排其參與稽核業務。
2006.4.2	查明造成這種差距的原因，並儘快採取適當的矯正措施，例如訓練與持續專業進修 (CPE)，這一點很重要。
2006.4.3	在開始稽核活動之前，應在合理的時間內完成稽核業務所需的教育訓練。
2006.4.4	應在訓練完成後衡量訓練的有效性。
2006.4.5	資訊稽核和確保管理階層制定關於所需技能的文件（例如：技能矩陣）有助於確認差距和訓練需求。該矩陣可以作為可用資源、技能和知識交叉引用的依據。
2006.4.6	對所提供的教育訓練記錄，及有關訓練及訓練成效的回饋，應予以保留及分析，以供未來使用。
2006.4.7	CPE是ISACA用於保持專業能力與更新技能和知識的方法。
2006.4.8	CPE課程應有助於提升資訊稽核、風險、安全、隱私和治理的專業和技術要求其有相關技能和知識。 專業機構通常會表明符合CPE認可條件的課程。從業人員應遵守各自的專業機構制定的規範。
2006.4.9	專業機構通常會規定獲取CPE學分的方法，及其應定期獲取的最低學分。從業人員必須遵守各自專業機構制定的規範。如果從業人員為獲取最低學分而與多個專業機構建立聯繫，則他們可運用專業判斷，通過一種普遍的方式從符合條件的課程中獲取CPE學分，前提是這些課程符合各自專業機構制定的規則或準則。
2006.4.10	ISACA擁有關於CPE的全面政策，適用于其成員和CISA證照持有人。具有CISA證照的從業人員必須遵守ISACA的CPE政策。有關該政策的詳細資訊，請參考： *www.isaca.org/credentialing/cisa/maintain-cisa-certification*。
2006.4.11	根據各自專業機構（包括ISACA）的規定，從業人員必須維護適當的CPE課程記錄，保留一段特定的時間，並在需要時提供查核。

2006.5其他注意事項

2006.5.1	資訊稽核和確保從業人員應： ● 在工作開始前證明具備足夠的專業能力（與規劃業務有關的技能、知識和經驗）。 ● 評估獲得執行稽核業務所需技能的替代方法，包括分包、外包部分任務，推遲任務直到具備此類技能，或通過其他方式確保獲得適當的技能。 ● 確保參與資訊稽核和確保業務的團隊成員擁有CISA認證或其他相關的專業認證，並且積累了足夠的正規教育、訓練和工作經驗。 ● 領導資訊稽核或確保業務時，應合理保證所有團隊成員都具備適當的專業能力水準，來執行各自預期執行的工作。 ● 具備足夠的關鍵領域知識，能夠與其他團隊成員或參與工作的專家合作，以具效果與效率的方式執行資訊稽核和確保業務。 ● 滿足CISA或其他相關專業認證的持續進修或發展的要求。 ● 通過教育課程、研討會、會議、網路廣播和在職訓練方式不斷更新專業知識，以提供與資訊稽核或確保角色要求相稱的專業服務水準。 ● 如果在規定的時間內不太可能獲得所需的能力，可考慮使用外部資源來執行業務。

標準1006和準則2006與COBIT® 2019的關聯

COBIT 2019 管理目標	目的
MEA04 管理確保	促使組織設計和制定具效果與效率的確保機制，並採用公認的確保方法論，做為規劃，範圍界定，執行和後續追蹤提供指引。
APO07 管理人力資源	優化人力資源能力，以滿足企業目標。

通用標準1007：聲明

聲明	1007.1資訊稽核和從事確保工作人員應審查評估查核事項所參照的聲明，以確定此等聲明能夠被稽核且聲明是充分、有效和相關的。

通用準則2007：聲明

2007.1簡介 本準則的目的是詳細闡述不同的聲明，指導資訊稽核和確保從業人員確保評估查核事項所參照的衡量標準以支持聲明，並對形成的結論和報告提供指引。本準則的內容旨在為以下關鍵稽核和確保主題提供系統化資訊：

2007.2聲明

2007.3查核事項衡量標準

2007.4第三方制定的聲明

2007.5結論和報告

2007.6其他注意事項

2007.2聲明

2007.2.1	聲明指有關查核事項是否基於或符合所選衡量標準的任何或一系列的聲明。從業人員在執行稽核業務的整個過程中，都應考慮並確保符合這些聲明，以及在稽核報告中加以說明。
2007.2.2	可以考量的常見聲明包括有： ● **機密性**—通過經授權的存取和揭露限制來實現，其中包括保護隱私權及專有資訊的手段。 ● **完整性**—所有活動、資訊和其他應當記錄的資料均有記錄，例如所有佈建到正式環境的資訊系統變更均記錄在變更管理系統中。 ● **準確性**—於活動中有關的金額、日期和其他資料均已得到適當記錄，例如資訊系統變更佈建到正式環境有關的資料，均已準確的顯示在變更管理跟蹤應用程式的變更記錄中。 ● **真實性**—收到的資訊、證據和其他資料均來自於值得信任的來源，並在整個生命週期中受到保護，例如將完成備份後的雜湊值與備份還原前一刻的雜湊值進行比較，以確認是否有遭篡改的跡象。 ● **可用性**—稽核業務所需的資訊、證據和其他資料均存在且可被存取，例如請求變更的記錄存在變更管理程序中並且隨時可存取。 ● **合規性**—根據企業要求、法規或其他適用規定留存的記錄資訊、證據和其他資料，例如所要求的欄位根據適用規定存在於變更管理系統的變更記錄中。 ● **效率**—所用的效能水準，透過最少數量的輸入，創造最多數量的輸出。 ● **有效性**—產出期望的輸出或達到預期的目標。
2007.2.3	管理階層負責定義和核准查核事項及相關聲明。從業人員應確保，相比其他權威聲明的標準，管理階層制定的聲明符合知識豐富的讀者或使用者的預期。

2007.2.4	從業人員承接稽核業務的一個前提是，管理階層確認完全理解其承擔的責任，即向從業人員提供有關查核事項和聲明的所有必要資訊。如果從業人員認為管理階層無法履行此責任，則應： ● 向資訊稽核和確保管理階層以及稽核職能部門的治理機構報告已發現的問題。 ● 拒絕建議的稽核業務或依據業務相關的風險等級採取適當的行動方案。
2007.2.5	從業人員應審查為稽核業務選擇的聲明，並確保這些聲明是： ● **充分的**—足以滿足稽核業務的目的，即對範圍內的查核事項表達意見或結論。 ● **有效的**—能夠在設定範圍內的查核事項下接受測試。 ● **相關的**—與範圍內的查核事項直接相關，並有助於滿足稽核業務的目的。

2007.3查核事項衡量標準

2007.3.1	從業人員應根據預先確認的衡量標準評估稽核業務的查核事項，並得出有關查核事項的意見或結論。從業人員應評估衡量標準，確保它們支援相關聲明。
2007.3.2	一個衡量標準可以與多個聲明關聯。同樣，一個聲明可以受多個衡量標準支持。這些都有助於確保符合聲明。
2007.3.3	如果從業人員得出衡量標準不能完全支持所有相關聲明的結論，則應建議對現有衡量標準進行變更或補充。資訊稽核和確保管理階層必須審查新的或修訂後的衡量標準，並予以核准或拒絕。
2007.3.4	通過評估確認衡量標準完全支持相關的聲明後，從業人員應評估是否可以對衡量標準進行客觀及量化的分析。

2007.4第三方制定的聲明

2007.4.1	將營運外包給第三方的企業將收到有關外包營運的控制環境報告。如果資訊稽核和確保依賴于外包營運相關的報告來支持稽核業務，從業人員應審查每份報告，確定： ● 報告是否由相關的獨立專業機構發佈。 ● 稽核意見是保留的還是無保留的。 ● 控制目標的範圍是否足以涵蓋企業所需的控制。 ● 稽核時間範圍是否符合企業預期。 ● 特定的控制缺失（導致報告總體不合格）是否與企業有關。 ● 所用的聲明是否與所需的聲明一致。資訊稽核和確保管理階層應記錄所做的分析和得出的結論。從業人員應確保聲明得到管理階層的驗證和正式核准，作為涵蓋外包營運的稽核業務的一部分。
2007.4.2	企業還可能收到第三方（例如：顧問或外部稽核師）的報告。

2007.5結論和報告

2007.5.1	根據衡量標準評估了稽核業務的查核事項之後，從業人員應基於參照相關衡量標準得出的結果的匯總並運用專業判斷，對每項聲明做出結論。
2007.5.2	做出結論後，從業人員應就查核事項出具間接或直接報告： ● **間接報告**—針對查核事項的相關聲明，例如有關查核事項某一組成部分的「完整性」聲明：「根據我們的執行有效性測試結果，我們認為，在所選衡量標準規定的所有重大方面，所有應用到正式環境的資訊系統變更均已完整記錄在變更管理系統中。」 ● **直接報告**—針對查核事項本身，例如整個查核事項：「根據我們的測試，我們認為，在所選衡量標準規定的所有重大方面，資訊系統變更均遵循要求的變更管理程序。」

2007.6其他注意事項

2007.6.1	資訊稽核和確保從業人員應： ● 對在評估查核事項時所參照的衡量標準進行評估，以確保它們支持聲明。 ● 確認是否可被稽核，並得到佐證資料的支持。 ● 確認聲明是否以適當確認的標準為基礎，並可進行客觀及量化的分析。 ● 確保管理階層制定的聲明，參照其他權威公告的標準，能夠滿足聲明準確的合理預期。 ● 確保由代表企業執行控制第三方所制定的聲明，已經過管理階層認可和接受。 ● 直接對查核事項出具報告（直接報告）或對有關查核事項的某項聲明出具報告（間接報告）。 ● 基於參照相關衡量標準得出結果的匯總，並運用專業判斷，對每項聲明做出結論。

標準1007和準則2007與COBIT® 2019的關聯

COBIT 2019 管理目標	目的
EDM01 確保治理架構的設置和維護	提供與企業治理方法整合的一致方法。資訊與科技(I&T)相關決策應該與企業的策略和目標保持一致，並實現期望的價值。為此，應確保I&T相關流程得到有效和透明的監督，符合法律、合約和監管要求，以及滿足董事會成員的治理要求。
EDM02 確保利益交付	保證從資訊與科技(I&T)促成的措施、服務及資產中獲得最佳價值；以經濟效率的方式提供解決方案和服務；可靠準確地維護成本和效益資訊，從而具效果與效率地支援業務需求。
EDM03 確保風險最佳化	確保資訊與科技(I&T)相關企業風險不超過企業的風險偏好和風險容忍度，識別和管控I&T風險對企業價值的影響，以及最大程度地降低不合規的可能性。
EDM04 確保資源最佳化	確保以最佳的方式滿足企業的資源需求，優化資訊與科技(I&T)成本，提高效益實現的可能性，並為未來的改變做好準備。
MEA04 管理確保	促使組織設計和制定具效果與效率的確保機制，並採用公認的確保方法論，做為規劃，範圍界定，執行和後續追蹤提供指引。

通用標準1008：衡量標準

聲明	1008.1資訊稽核和從事確保工作人員對查核事項所選擇參照的衡量標準應客觀、完整、攸關、可靠、可衡量、易於理解、被廣泛認可、具權威性，並為所有讀者和用戶所理解或掌握的標準。
	1008.2資訊稽核和從事確保工作人員應考慮衡量標準的可接受性，並關注那些公認、權威和公開的衡量標準。

通用標準2008：衡量標準

2008.1簡介 本準則的目的是協助資訊稽核和確保從業人員選擇合適、可接受和來自相關來源的衡量標準，用作評估查核事項的參照。本準則旨在為以下關鍵稽核和確保業務主題提供系統化資訊：

2008.2衡量標準的選擇和使用

2008.3適用性

2008.4可接受性

2008.5來源

2008.6稽核業務期間的衡量標準變更

2008.2衡量標準的選擇和使用

2008.2.1	從業人員應評估查核事項選擇所參照的衡量標準。選擇衡量標準時，從業人員應仔細考慮衡量標準的適用性、可接受性和來源。
2008.2.2	從業人員應慎重選擇衡量標準。遵守當地法律、法規非常重要，應作為一項強制性要求。但要意識到，許多稽核業務包含法律或法規未涵蓋的領域，例如變更管理、一般資訊控制和存取控制。此外，有些產業（例如：支付卡行業）制定了強制性要求。應考慮當地和國際資料保護規則以及隱私和安全法規的相關性。如果法規要求不屬於強制性規範，從業人員應確保所選擇的衡量標準能夠滿足稽核目標，以確保遵守法律要求。
2008.2.3	要求使用適當和可接受的衡量標準，以確保對查核事項進行一致的評估。否則，得出的任何結論或意見都可能引起讀者的誤解和錯誤解讀。
2008.2.4	從業人員應避免基於個人期望、經驗或判斷來評估查核事項。
2008.2.5	如果衡量標準不易獲取，或者衡量標準不完整或容易被誤解，從業人員應在報告中包含對衡量標準的描述以及其他必要資訊，以確保報告公正、客觀且易於理解。
2008.2.6	應運用專業判斷，確保衡量標準的使用有助於得出公正、客觀且不會誤導讀者或使用者的意見或結論。要意識到，管理階層可能提出並非符合所有要求的衡量標準。

2008.3適用性

2008.3.1	從業人員應評估用於查核事項的衡量標準其適用性和適當性。衡量標準範例「當地法律規定，在進行資料交易時，應始終保證客戶的所有個人資訊的隱私性」用於說明衡量標準的以下屬性： ● **客觀性**—避免可能會對從業人員的稽核結果和結論造成不利影響的偏見，以免誤導稽核報告的使用者，例如經過當地法律核准的衡量標準是客觀的。 ● **完整性**—應足夠完整以使所有可能影響從業人員就對應查核事項得出結論造成影響的所有衡量標準得到確認，並在執行稽核業務時使用。因此，在考量稽核業務目標的情況下，應確保使用衡量標準的完整性。 ● **相關性**—與查核事項相關，有助於得出滿足稽核業務目標的結果和結論。衡量標準可以是上下文相關的；甚至針對同一查核事項也可能有不同的衡量標準，具體取決於稽核業務的目標和情況，例如資料交易在稽核業務的範圍之內，則該衡量標準被認為是相關的。 ● **可靠性**—當不同的從業人員在相似的情況下應用衡量標準時，能夠對查核事項進行基本一致的合理衡量或評估，並得出一致的結論。 ● **可衡量性**—確保查核事項的衡量方法一致，且不同的從業人員在類似情況下能夠得出一致的結論，例如含未受保護個人資訊的每筆資料交易都是可唯一識別的且因此而可一致衡量的，則衡量標準是可衡量的。 ● **可理解性**—表達清晰，不會使不同目標使用者有明顯不同的理解，例如法律的某一部分是多個法院裁定的依據，有助於清楚地理解法律的實際執行與解讀，則衡量標準是可理解的。

2008.4可接受性

2008.4.1	衡量標準的可接受性受可用性影響，稽核報告的使用者只有獲得衡量標準才能理解確保活動的依據，以及稽核發現和結論的相關性。 可接受的衡量標準應具有： ● **公認性**—應得到廣泛的認可，才能確保其不受到目標使用者的質疑。 ● **權威性**—能夠反應該領域的權威性聲明且適用於查核事項，例如權威性聲明可能來自專業機構、產業組織、政府或監管機構。 ● **公開提供**—包括ISACA、國際會計師聯合會 (IFAC) 等專業會計與稽核機構，以及其他公認的政府、法律或專業機構制定的標準。 ● **向所有使用者提供**—如果衡量標準不是公開的，應作為稽核報告一部分的聲明向所有使用者傳達。聲明由有關查核事項符合「適當的衡量標準」要求的公告組成，因此可被稽核。

2008.4.2	從業人員應確保稽核業務中使用的衡量標準是： ● **外部接受的**—公認、權威且公開提供；或者是 ● **外部確認的**—管理階層針對特定稽核業務制定的衡量標準不被認為是公認、權威且公開提供的。在使用這些衡量標準之前，需要由公認的獨立第三方進行外部驗證，確保管理階層不會暗中要求稽核業務，以得出符合他們期望的結果。

2008.5來源

2008.5.1	除了考慮資訊確保衡量標準的適用性和可用性，從業人員還應從使用及潛在讀者的角度考慮衡量標準的來源。例如如果查核事項涉及政府規定，根據適用於查核事項的法律、法規制定的聲明應是最恰當的，基於這些聲明的衡量標準也可能是最合適的選擇。在其他情況下，產業或專業協會的衡量標準可能更適合。以下按考慮順序列出可能的衡量標準來源，包括： ● **ISACA制定的衡量標準**—這些都是公開的準則和標準，並通過同儕審查並由公認的國際資訊稽核、風險、隱私、治理和安全領域方面專家進行全面的盡職調查。 ● **其他專家團體制定的衡量標準**—類似於ISACA標準和準則，這些切合查核事項的標準由各領域的專家編制，並通過同儕審查和全面的盡職調查。 ● **根據法律、法規確立的衡量標準**—法律法規可以作為衡量標準的依據，但必須慎重使用。法律措辭通常非常複雜，並且具有特定的法律含義。許多情況下，有必要以聲明的形式表述這些法律、法規的要求。另外，通常僅限由法律界人士表達法律意見。 ● **未遵循正當程序而制定的書面衡量標準**—包括未遵循正當程序的其他相關書面標準，因此，未經過公眾諮詢和討論。 ● **專為稽核專案制定的衡量標準**—專為稽核專案制定衡量標準也許是適當的，但需特別慎重，以確保這些標準是合適的，尤其是客觀性、完整性和可衡量性。專為稽核專案制定的衡量標準以聲明的形式出現。它們通常與特定用戶的需求有關。例如多種框架可作為評估內部控制制度有效性的既定標準。但某個用戶可能會專為特定需求（例如：授權核准的層級結構）而制定一組衡量標準。從業人員應在稽核報告中明確提及哪些衡量標準是專門針對該稽核業務設計的。他們應考慮制定的衡量標準是否會誤導目標用戶，並在必要時提供有關這些標準的更多資訊。如果由管理階層制定衡量標準，則應尋求外部確認並在報告中說明。

2008.6稽核業務期間的衡量標準變更

2008.6.1	隨著稽核工作的執行，有關查核事項的其他資訊和見解可能會導致所選衡量標準發生變更： ● 可能不再需要某些衡量標準來實現稽核目標，因此沒有必要執行與這些衡量標準有關的進一步稽核工作。 ● 如果需要額外的衡量標準來實現稽核目標，從業人員應選擇相關衡量標準並進行相關的稽核工作。 ●

標準1008和準則2008與COBIT® 2019的關聯

COBIT 2019 管理目標	目的
EDM01 確保治理架構的設置和維護	提供與企業治理方法整合的一致方法。資訊與科技(I&T)相關決策應該與企業的策略和目標保持一致，並實現期望的價值。為此，應確保I&T相關流程得到有效和透明的監督，符合法律、合約和監管要求，以及滿足董事會成員的治理要求。
MEA04 管理確保	促使組織設計和制定具效果與效率的確保機制，並採用公認的確保方法論，做為規劃，範圍界定，執行和後續追蹤提供指引。

執行標準

執行標準1201：規劃中的風險評估

聲明	1201.1資訊稽核和確保工作應使用恰當的風險評估方法（即兼顧定量和定性因素的資料驅動方法）和佐證方法來制定總體的資訊稽核計畫，並確定有效分配資訊稽核資源的優先順序。
	1201.2資訊稽核和從事確保工作人員在規劃各別專案時應辨別並評估與所稽核領域相關的風險。
	1201.3資訊稽核和從事確保工作人員在規劃稽核業務時應考量查核事項風險、稽核風險以及企業所面臨的相關風險。

執行準則2201：規劃中的風險評估

2201.1簡介—本準則的目的是協助識別資訊環境中的風險和威脅。本準則提供有關如何應用風險評估方法的指導，以制定：

- 涵蓋所有年度稽核業務的資訊稽核計畫 。
- 側重應對某項具體稽核業務的稽核業務項目計畫 。

本準則詳細介紹資訊稽核和從事確保工作人員遇到的各種風險。本準則旨在為以下關鍵稽核和確保業務主題提供系統化資訊：

2201.2資訊稽核計畫的風險評估

2201.3風險評估方法

2201.4各別查核專案的風險評估

2201.5稽核風險

2201.6固有風險

2201.7控制風險

2201.8偵測風險

2201.9其他注意事項

2201.2資訊稽核計畫的風險評估

2201.2.1	應在稽核規劃過程中進行風險評估，並根據不斷變化的業務狀況和新出現的風險主動修改計畫。從業人員應考慮組織戰略計畫和目標以及企業風險管理框架和舉措。這將有助於制定資訊稽核行程表。

2201.2.2	為了正確且完整的評估與資訊稽核領域範圍的相關風險，從業人員在制定資訊稽核行程表時應考慮以下因素： ● 全面涵蓋資訊稽核範圍內的所有領域，含括所有可能的稽核活動，並考慮到系統、應用程式與流程的重要性。 ● 管理階層提供的風險評估的可靠性和適用性。 ● 管理階層監督、檢查和報告潛在風險或問題的流程。 ● 涵蓋與正在審查的活動有關的風險。
2201.2.3	採用的風險評估方法應有助於資訊稽核和確保工作的優先順序和流程安排。它應支持稽核感興趣的領域和項目的選擇。它應指導特定資訊稽核專案設計與執行的決策過程。
2201.2.4	從業人員應確保所採用的風險評估方法得到治理機構的核准，並分發給各個參與的利害關係人。
2201.2.5	從業人員應使用風險評估來量化與證明完成資訊稽核計畫，並滿足特定專案所需的資訊稽核資源的數量。
2201.2.6	從業人員應以風險評估為基礎制定資訊稽核行程表，作為資訊稽核和確保活動的框架。它應當： ● 考慮非資訊稽核和確保的要求和活動。 ● 至少每年更新一次。 ● 經治理機構核准。 ● 闡述稽核組織章程規定的職責。
2201.2.7	在制定總體資訊稽核計畫時，應運用適當的風險評估方法。風險評估的目的是確認活動中的哪些部分應作為稽核重點，並降低得出錯誤結論的風險。

2201.3風險評估方法

2201.3.1	從業人員應考慮採用適當的風險評估方法，以確保資訊稽核行程表完整並準確地涵蓋整個稽核專案。
2201.3.2	從業人員所採用的風險評估方法至少應包括與系統可用性、資料完整性和業務資訊機密性有關的企業風險分析。
2201.3.3	有許多風險評估方法可用於支持風險評估流程。這些方法包括根據從業人員的判斷將風險簡單劃分為高、中、低的方法，也包括利用具體數值詳細表示風險等級更量化的科學計算法則。還有結合這兩種方法的其他方法。從業人員應考慮適合受查企業或主題的複雜程度和詳細程度。有關執行風險評估的具體指南，請參閱ISACA出版物《*Risk IT*框架》和《*Risk IT*從業人員指南》。
2201.3.4	所有風險評估方法在過程中的某個環節都依賴於主觀判斷（例如：為各個參數分配權重）。從業人員應識別採用特定方法所需的主觀決定，並考慮是否能作出判斷，及以適當的準確性和合理性水準加以驗證。

2201.3.5	為確定最合適的風險評估方法，從業人員應考慮： ● 需要收集的資訊類型。某些系統使用財務影響作為唯一衡量指標，但這並不適用於所有資訊稽核專案。 ● 採用該方法所需的軟體或其他許可證的成本。 ● 資訊獲取到什麼程度可以滿足要求。 ● 在獲得可靠的產出之前需要收集的其他資訊量，以及收集資訊的成本（包括收集工作所需的時間投入）。 ● 該方法的其他使用者的意見，以及他們對於該方法在多大程度上幫助他們提高稽核效率與效率的看法。 ● 資訊稽核領域的治理機構是否願意接受該方法作為確認所執行稽核工作的類型和水準的方法。
2201.3.6	不存在適用於所有情況的風險評估方法。從業人員應定期重新評估所選擇的風險評估方法的適當性，因為風險、威脅、漏洞、風險偏好和風險容忍度可能會發生改變。
2201.3.7	從業人員應使用選定的風險評估技術來制定總體資訊稽核行程表，並規劃特定的稽核專案。在以下規劃決策中，應考慮結合其他稽核技術進行風險評估： ● 待稽核的領域或業務職能。 ● 分配給稽核的時間和資源。 ● 稽核程序的性質、範圍和時間。
2201.3.8	所採用的風險評估方法應輸出一致、有效、可比較和可重複的結果，並應得到管理階層的同意。該方法產生的風險評估應為一致（在一段時間內）、有效、可比較（對比之前或之後使用相同評估方法的評估）和可重複的（在類似的情況下，使用相同的評估方法將得出相似的結果）。

2201.4各別查核專案的風險評估

2201.4.1	在規劃一項各別的查核專案時，從業人員應識別和評估與待查核領域相關的風險。風險評估結果應反應在稽核業務目標中。在風險評估期間，從業人員應考慮： ● 之前稽核專案、複查和發現，並包含其補救活動。 ● 企業風險評估流程。 ● 發生特定風險的可能性。 ● 發生特定風險將造成的影響（貨幣或其他價值計量方式），如果它發生的話。
2201.4.2	從業人員應確保在風險評估之前已充分瞭解範圍內的活動。他們應徵求利害關係人和其他相關者的意見和建議。必須充分瞭解情況才能正確確認稽核專案中可能存在的風險並檢查其衍生的影響。

2201.4.3	在規劃特定的資訊稽核和確保程序時，從業人員應認識到，重要性閾值越低，稽核預期越準確，而稽核風險越高。
2201.4.4	在規劃特定的資訊稽核和確保程序時，從業人員應考慮潛在的非法行為，為應對這些行為，可能需要修改現有程序的性質、時間或範圍以及支援潛在訴訟所需的相應文件記錄。
2201.4.5	在稽核風險較高或重要性閾值較低的情況下，從業人員應通過補償措施來獲得額外保證，例如擴大資訊稽核測試的範圍或性質，或者增加或擴大實質性測試範圍。

2201.5稽核風險

2201.5.1	稽核風險指根據稽核結果得出錯誤結論的風險。 稽核風險的三個組成部分如下： ● 固有風險。 ● 控制風險。 ● 偵測風險。
2201.5.2	從業人員應考量每個風險組成部分，以確認總體風險水準。稽核風險包括查核事項風險(包含固有風險和控制風險)，及偵測風險。

2201.6固有風險

2201.6.1	固有風險指假設沒有相關的內部控制，稽核領域受到潛在重大錯誤（單個錯誤或與其他錯誤結合）損害的狀況。例如與沒有適當控制的作業系統其相關的固有風險通常較高，因為利用作業系統安全性弱點來變更甚至洩露資料可能會導致資訊管理失效或競爭劣勢。相比之下，無控制的獨立個人電腦未被用於業務關鍵目的時，與該電腦的安全性相關固有風險通常較低。
2201.6.2	由於資訊稽核師認為待測試領域的範圍會影響主要業務系統，因此固有風險預計會較高。

2201.7控制風險

2201.7.1	控制風險是指稽核領域中可能出現的錯誤（該錯誤可能是重大錯誤，可能單獨出現或與其他錯誤一起出現）將無法通過內部控制系統及時預防或檢測並予以矯正的風險。例如與手動審查電腦日誌相關的控制風險可能很高，因為記錄的資訊量過大，可能因人為錯誤導致無意中未能發現異常。由於一致的採用電腦化的方式驗證資料，與之相關的控制風險則通常較低。

2201.7.2	從業人員應將控制風險評估為高，除非相關的內部控制： ● 已識別。 ● 已通過驗證測試（即，將性能與設計進行比較），證明其能夠有效地執行。
2201.7.3	從業人員應同時考慮普遍和具體資訊控制： ● 普遍資訊控制被視為一般控制的子集，指的是側重於資訊環境管理和監控的一般控制。它們影響所有資訊相關的活動。普遍資訊控制對從業人員工作的影響不僅限於業務流程系統中的應用控制的可靠性。普遍資訊控制還會影響具體資訊控制的可靠性，例如應用程式開發、系統佈建、安全管理和備份程序。如果普遍資訊控制薄弱，造成資訊環境的管理和監控薄弱，則從業人員應注意，設計為在具體層面執行的控制措施可能無效的風險較高。 ● 具體資訊控制由應用控制以及未包括在普遍資訊控制之中的一般控制組成。按照COBIT 2019框架，具體資訊控制與資訊和科技的治理與管理有關。
2201.7.4	從業人員應考慮詳細資訊控制中存在的局限或缺失，可能是由於具體資訊控制不足所致的風險。

2201.8偵測風險

2201.8.1	偵測風險是指從業人員的實質性程序無法檢測到錯誤的風險（該錯誤可能是重大錯誤，可能單獨出現或與其他錯誤一起出現）。例如與識別應用系統中的安全違規情況相關的偵測風險通常較高，因為在執行稽核時整個稽核期間的日誌可能不可用。由於很容易驗證災難恢復計畫是否存在，因此與發現缺少災難恢復計畫相關的偵測風險通常較低。
2201.8.2	在確認所需的實質性測試水準時，從業人員應考慮： ● 對固有風險的評估。 ● 根據合規性測試得出關於控制風險的結論。
2201.8.3	通常，固有風險和控制風險的評估越高，從業人員從實質性稽核程序執行中所獲得的稽核證據越多。

2201.9其他注意事項

2201.9.1	規劃執行的活動時，資訊稽核和確保職能部門應當： ● 至少每年進行一次風險評估並建檔記錄，以促進制定資訊稽核計畫。 ● 將組織戰略計畫和目標、及企業風險管理框架和舉措納入風險評估中。 ● 在選擇稽核感興趣的領域和專案，及作出關於設計和執行特定資訊稽核和確保業務的決定時，使用風險評估。某些感興趣的領域或專案可能需要管理階層的持續監控和從業人員的持續稽核。 ● 如果依賴於管理階層的風險評估，則應確保評估得到相關方的核准。風險評估應記錄管理階層接受風險的情況。 ● 如果風險評估由稽核職能部門執行，則將與其組織中其他職能部門（例如：獨立的風險管理部門）執行的風險評估進行比較。解決存在的差異（例如：稽核職能部門將某項風險評定為高風險，而風險管理部門將其評定為低風險）。 ● 以風險評估為依據考慮和安排資訊稽核和確保工作的行程與優先順序。 ● 以風險評估為依據制定以下性質的計畫： ■ 用作資訊稽核和確保活動的框架。 ■ 考慮非資訊稽核和確保的要求和活動。 ■ 每年至少更新一次，並由治理負責人核批。 ■ 闡述稽核組織章程規定的職責。 在規劃各別查核專案時，資訊稽核和從事確保工作人員應： ● 識別和評估與所審查的領域有關的風險。 ● 針對每項業務初步評估與所稽核領域有關的風險。每項具體專案的目標應反應初步風險評估的結果。 ● 考慮先前與具體業務風險領域有關的稽核、複查和發現，包含其補救措施。並且還要考慮董事會的總體風險評估流程。 ● 在規劃和執行資訊稽核的同時，嘗試通過適當評估資訊查核事項和相關控制，將稽核風險降低到可接受的水準並符合稽核目標。 ● 為降低高重要性的稽核風險，可以通過擴大控制測試的範圍（降低控制風險）或擴大實質性測試程序的範圍（降低偵測風險）等補償措施來獲得額外保證。

標準1201和準則2201與COBIT® 2019的關聯

COBIT 2019 管理目標	目的
EDM01 確保治理架構的設置和維護	提供與企業治理方法整合的一致方法。資訊與科技(I&T)相關決策應該與企業的策略和目標保持一致，並實現期望的價值。為此，應確保I&T相關流程得到有效和透明的監督，符合法律、合約和監管要求，以及滿足董事會成員的治理要求。

EDM03 確保風險最佳化	確保資訊與科技(I&T)相關企業風險不超過企業的風險偏好和風險容忍度，識別和管控I&T風險對企業價值的影響，以及最大程度地降低不合規的可能性。
APO12 管理風險	將資訊與科技(I&T)相關的企業風險管理整合到總體企業風險管理(ERM)中，並平衡I&T相關企業風險管理的成本和效益。
MEA03 管理外部要求合規	確保企業符合所有適用的外部要求。
MEA04 管理確保	促使組織設計和制定具效果與效率的確保機制，並採用公認的確保方法論，做為規劃，範圍界定，執行和後續追蹤提供指引。

執行標準1202：稽核安排

聲明	1202.1資訊稽核和確保工作應制定總體策略計畫，形成短期和長期的稽核規劃。短期規劃包含將在一年內執行的稽核工作，而長期規劃則包含基於企業資訊和科技（I&T）環境中與風險有關事項的稽核，且這些稽核可能將在未來進行。
	1202.2應與負責治理和監督職責的機構（例如：審計委員會）就短期和長期稽核規劃達成共識，並在企業內部進行傳達。
	1202.3資訊稽核和確保工作應根據組織需求(例如：突發事件或計畫外措施)修改短期或長期的稽核行程表。如需增加對突發事件或計畫外措施的稽核，應將被取代的稽核重新安排到延後的日期時間。

執行準則2202：稽核安排

2202.1簡介 本準則提供關於從事資訊稽核和確保工作人員進行稽核安排的指引。

本準則旨在為以下關鍵稽核和確保專案主題提供系統化資訊：

2202.2制定和維護稽核行程表

2202.3稽核行程表和稽核專案規劃

2202.2制定和維護稽核行程表

2202.2.1	資訊稽核和從事確保工作人員應制定和維護基於稽核領域清單（通常稱為「稽核領域」）的稽核行程表。稽核安排有助於確保稽核組織章程中定義稽核職能部門的職責得到適當的關注，並為重要稽核領域中的企業戰略目標和組織目標提供充分的確保。
2202.2.2	應定期(至少每年一次)重新評估長期稽核行程表，以確保滿足組織的需求。通過重新評估，稽核職能部門可以在出現意外關鍵事件或情況時，考慮增加可能需要的確保和稽核業務。被取代的稽核計畫應被重新安排到未來延後的期間。

2202.3稽核行程表和稽核專案規劃

2202.3.1	可以向企業溝通稽核行程表，包括暫定的稽核開始日期、初步範圍和關鍵利害關係人。

標準1202和準則2202與COBIT® 2019的關聯

COBIT 2019 管理目標	目的
EDM01 確保治理架構的設置和維護	提供與企業治理方法整合的一致方法。資訊與科技(I&T)相關決策應該與企業的策略和目標保持一致，並實現期望的價值。為此，應確保I&T相關流程得到有效和透明的監督，符合法律、合約和監管要求，以及滿足董事會成員的治理要求。
EDM02 確保利益交付	保證從資訊與科技(I&T)促成的措施、服務及資產中獲得最佳價值；以經濟效率的方式提供解決方案和服務；可靠準確地維護成本和效益資訊，從而具效果與效率地支援業務需求。
BAI11 管理專案	通過改進與業務部門和最終用戶的溝通，並提高他們的參與度來實現定義的專案成果，並降低因意外造成的延遲、成本和價值流失所帶來的風險。確保專案交付成果的價值和品質，並最大程度地提高它們對定義的計畫和投資組合的貢獻。

執行標準1203：稽核專案規劃

聲明	1203.1資訊稽核和從事確保工作人員應對每次資訊稽核和確保業務進行計劃，以確定所要執行的稽核程序的性質、時間安排和範圍。計畫應包括： ● 查核的領域 ● 目標 ● 範圍 ● 資源（例如成員、工具和預算）和排程 ● 時間表和交付成果 ● 遵循適用法律、法規和專業稽核標準 ● 對非關於法律及法規遵循業務採用風險導向方法處理 ● 專案業務的特定問題 ● 文件紀錄和報告要求 ● 相關科技和資料分析技術的使用 ● 相對於潛在效益的查核專案成本考慮 ● 針對資訊稽核業務執行期間可能出現的情況（例如：範圍限制或關鍵人員不到位）的溝通和升級協議 在現場工作期間，隨著業務的進展，可能有必要修改原規劃期間所制定的稽核程序。
	1203.2資訊稽核和從事確保工作人員應制定並記錄資訊稽核和確保業務稽核程序，描述用於完成稽核的步驟程序和說明。

執行準則2203：稽核專案規劃

2203.1簡介 本準則提供關於資訊稽核和從事確保工作人員進行稽核專案規劃的指導。本準則旨在為以下關鍵稽核和確保業務主題提供系統化資訊：

2203.2目標

2203.3範圍和業務知識

2203.4風險為導向的方法

2203.5文件化稽核業務專案計畫和稽核程序

2203.6稽核過程中的變更

2203.2目標

2203.2.1	從業人員應定義稽核業務目標並在稽核業務專案計畫中記錄。除了確認對企業目標、營運和挑戰的理解，稽核專案業務目標的文件化還可以確保測試，有助於保證控制措施得到實施和有效運行。
2203.2.2	從業人員在制定稽核專案計畫時應考慮稽核專案的目標。這些目標可能會影響稽核業務，例如資源、時間和交付成果。

2203.3範圍和業務知識

2203.3.1	在開始稽核專案之前，從業人員應以有助於實現稽核目標的方式規劃工作。在規劃過程中，從業人員應瞭解企業及其流程。這有助於根據所複核領域與企業目標之相關性確定這些領域的重要程度。從業人員應根據稽核目標確定稽核工作的範圍。
2203.3.2	作為初步評估的一部分，從業人員應瞭解可能稽核業務所涉及的特定企業、職能部門、流程或資料等產生重大影響的人員、事件、交易和作法的類型。稽核師對企業的瞭解，應包括企業面臨的商業和財務風險、企業市場的情況、及企業依靠外包實現目標的程度。從業人員應運用這些資訊來識別潛在問題、制定工作目標和範圍、執行工作並考慮管理階層應警惕的管理行動。

2203.4風險為導向的方法

2203.4.1	應進行風險評估，以瞭解企業及其所處環境（即戰略目標、及內部與外部義務）。這樣瞭解有助於從業人員確定需要審查的領域和活動。
2203.4.2	應在必要的範圍內，針對所審查的領域和企業資訊環境中，已識別的風險進行風險評估並確認優先順序。

2203.4.3	在規劃過程中，從業人員應按照重要性進行規劃，使得稽核工作足以滿足稽核目標並有效率的利用稽核資源。例如在複核現有系統時，從業人員應在規劃稽核業務的待執行工作時評估系統各個組成部分的重要性。在確定重要性時，應兼顧定性和定量的兩個方面。
2203.4.4	在開始稽核業務前及在稽核過程中，從業人員應注意遵守適用的法律和職業稽核標準。
2203.4.5	當從業人員透過控制程序來作為更大規模稽核工作（例如：歷史財務資訊的稽核）部分所進行資訊的收集並用來評估內部控制時，，他們應對控制進行初步評估並根據評估的結果訂定稽核專案計畫。

2203.5文件化稽核專案計畫和稽核程序

2203.5.1	從業人員的工作底稿應包括稽核專案計畫。
2203.5.2	明確的專案定義是確保專案有效性和效率的關鍵因素。稽核專案計畫（「專案計畫」）應在職權範圍中列明以下事項： ● 待稽核的領域。 ● 規劃的工作類型。 ● 工作的高層次目標和範圍。 ● 待進行的實情調查訪談。 ● 待獲取的相關資訊。 ● 核實或驗證所獲資訊及其稽核證據用途的程序。 ● 一般性議題，例如： ■預算。 ■資源可用性和分配。 ■日期安排。 ■報告類型。 ■目標受眾。 ■可交付成果。 ● 特定主題，例如： ■識別收集證據、執行測試和準備與歸納報告資訊所需要的工具。 ■用於評估現有實務的衡量標準（企業政策、程序或協議）。 ■風險評估文件。 ■報告要求和分發。 ■可用的外部報告（可依賴的資訊，如果有的話）。 ■必要時應要求提供報告，例如簽證服務準則第18號公報（SSAE18）。
2203.5.3	專案計畫應包含與稽核業務時間表有關的要求。這些內容包括但不限於在約定的行程表內執行稽核專案，所涵蓋的時間範圍與不同階段的完成日期。專案計畫應包括每個專案階段的預算支出和稽核團隊資源配置。

2203.5.4	從業人員應確保分配給稽核專案中的稽核團隊資源具備適當的技能、知識和經驗，能夠成功完成稽核業務。從業人員應分配最符合資訊稽核團隊成員能力的角色和職責。
2203.5.5	專案計畫應列出與稽核業務有關的所有可交付成果。
2203.5.6	專案計畫及其變更均應得到資訊稽核和確保管理階層的核准。
2203.5.7	在獲得資訊稽核和確保管理階層核准之後，應將專案計畫的部分內容（例如：範圍、時間表、文件要求、訪談時間表）傳達給受查方，以確保可存取和獲得所需的文件和資源。

2203.6稽核過程中的變更

2203.6.1	在稽核專案過程中，應根據需要更新和變更專案計劃（由資訊稽核和確保管理階層的適當核准）。 如果在稽核過程中出現值得稽核師注意的問題，從業人員應確定解決問題的方式。可選擇的方式包括但不限於擴大稽核範圍或安排單獨的評估。資訊稽核從業人員應立即通知受查方根據新發現的問題作出的稽核範圍或行程表變更。
2203.6.2	稽核專案的規劃是一個持續且反覆的過程。意外事件、情況變化或獲得的稽核證據可能導致，從業人員需要修改稽核程序的性質、時間與範圍。例如當有新的法規發布時，可能需要立即對其進行評估，以確定對企業合規性的潛在影響。
2203.6.3	稽核計畫應考量可能給企業帶來風險的意外事件。因此，稽核專案計畫應在稽核和確保流程中進行事件風險的優先順序排序。

2203.7其他注意事項

2203.7.1	資訊稽核和從事確保工作人員應： ● 瞭解被稽核的活動。應依據企業的性質、環境、業務目標、風險領域和專案目標來確認所需的知識範圍。 ● 考慮使用通過政府或產業頒佈的法律、法規、規則、指令和準則提供有關稽核事項的指引或方向。 ● 執行風險評估，以合理保證在專案過程中適當涵蓋了所有重要事項。之後可以制定稽核策略、重要性水準和資源要求。 ● 利用適當的專案管理方法制定專案計畫，確保工作不會偏離軌道且在預算範圍內。 ● 如果業務需要依賴稽核職能部門以外的專業人員（協力資源或外包）或其他實體（外部稽核師或監管機構）之前執行的測試結果，應制定需要遵循的協定。協議應定義： ■ 適合依賴他人的工作的情況。 ■ 對將執行稽核職能工作的稽核職能部門外部人員的資歷，進行的初步評估和持續監控。 ■ 由於依賴他人的工作，而可能排除在業務範圍之外的情況： • 例1：如受查的電子商務系統的支付閘道流程已符合支付卡產業資料安全標準(PCI DSS)，則稽核職能部門不需要再對支付閘道流程稽核，因為它已通過另一個框架的稽核。 • 例2：如果一家大型製造企業已通過相關機構認證的「環境、健康與安全(EHS)」框架，則稽核專案的範圍可以排除環境安全控制。 ● 在稽核計畫中包含任務特有的問題，如： ■ 具備適當的知識、技能和經驗的資源的可用性。 ■ 確認收集證據、執行測試、和準備與歸納報告資訊所需的工具。 ■ 待使用的評估標準。 ■ 報告的要求和分發。 ● 將資訊稽核和確保專案計畫和稽核程序的文件化，以明確指出： ■ 目標、範圍和時間安排。 ■ 資源。 ■ 角色和職責。 ■ 識別的風險領域及其對專案計畫的影響。 ■ 待部署的工具和技術。 ■ 待進行的實況調查訪談。 ■ 待獲取的相關資訊。 ■ 驗證或確認所獲得資訊及其作為證據使用的程序。 ■ 有關方式、方法論、程序及預期結果和結論的假設。 ● 盡可能依據管理階層和受查方的時間、可用性，及其他的承諾和要求對專案進行安排。

2203.7.1 (續)	● 在資訊稽核或確保專案過程中調整稽核計畫，以解決專案過程中出現的問題，例如新風險、錯誤假設或從已執行的程序中發現的結果。 ● 在後期規劃的階段，確保正在執行的工作與業務目標保持一致。 ● 對於內部業務： ■ 針對每項內部資訊稽核和確保專案準備一份單獨的專案委任書。 ■ 將稽核組織章程的相關內容傳達給受查方，並使用專案委任書或具同等效力的文件，來進一步澄清或確認對特定業務的參與。 ■ 向受查方傳達計畫，確保其充分知情，並在需要時對個人、文件及其他資源的訪談與資料存取。 ● 對於外部業務： ■ 針對每項外部資訊稽核和確保業務準備一份單獨的專案委任書。 ■ 針對每項外部資訊稽核和確保業務準備專案計畫和稽核程序，其中至少應將專案的目標和範圍文件化。 ● 為滿足每個資訊稽核和確保業務要求所需的資源，應進行量化並證明其合理性。

標準1203和準則2203與COBIT® 2019的關聯

COBIT 2019 管理目標	目的
EDM01 確保治理架構的設置和維護	提供與企業治理方法整合的一致方法。資訊與科技(I&T)相關決策應該與企業的策略和目標保持一致，並實現期望的價值。為此，應確保I&T相關流程得到有效和透明的監督，符合法律、合約和監管要求，以及滿足董事會成員的治理要求。
EDM02 確保效益交付	保證從資訊與科技(I&T)促成的措施、服務及資產中獲得最佳價值；以經濟效率的方式提供解決方案和服務；可靠準確地維護成本和效益資訊，從而具效果與效率地支援業務需求。
EDM03 確保風險最佳化	確保資訊與科技(I&T)相關企業風險不超過企業的風險偏好和風險容忍度，識別和管控I&T風險對企業價值的影響，以及最大程度地降低不合規的可能性。

執行標準1204：執行與監督

聲明	1204.1資訊稽核和從事確保工作人員在工作中應依照核准的資訊稽核計畫，在既定的時間內進行工作，並涵蓋已識別的風險。
	1204.2資訊稽核和從事確保工作人員應監督其團隊成員，以完成稽核目標並達到適用的專業稽核標準。
	1204.3資訊稽核和從事確保工作人員應只接受在自己的知識和技能範圍內的任務，或有合理預期能夠在執行查核業務期間獲得相關技能或在他人督導下完成的任務。
	1204.4資訊稽核和從事確保工作人員應獲得並保留充分且適當的證據來實現稽核目標。
	1204.5資訊稽核和從事確保工作人員應記錄稽核過程，並對稽核工作與支持查核發現和結論的稽核證據進行說明。
	1204.6資訊稽核和從事確保工作人員的查核發現和結論應有根本原因分析及證據解釋作為支持。
	1204.7資訊稽核和確保從業人員應提供適當的稽核意見或結論，並包含透過其他額外測試流程獲得所需證據的範圍限制。

執行準則2204：執行與監督

2204.1簡介 本準則旨在指導資訊稽核和從事確保工作人員執行稽核業務和監督資訊稽核團隊成員。本準則旨在為以下關鍵稽核和確保業務主題提供系統化資訊：

2204.2執行工作

2204.3角色和職責、知識和技能

2204.4監督

2204.5證據

2204.6文件記錄

2204.7查核發現

2204.8其他注意事項

2204.2執行工作

2204.2.1	從業人員應依照核准的資訊稽核計畫規劃和執行每項稽核業務。參照1203「稽核專案規劃」標準來制定稽核專案計畫，使從業人員能夠瞭解範圍內的所有要素，涵蓋所有已識別的風險，並確保在規範的時程內執行稽核業務所需的技能和知識。
2204.2.2	執行稽核專案時的主要任務包括： ● **規劃和風險評估。** ● **識別控制**—根據資訊稽核計畫中定義的範圍、目標和主要風險領域識別稽核專案範圍內的控制。 ● **評估控制並收集證據**—從業人員應透過收集和分析有關控制的設計有效性和運作有效性的資訊和證據，來評估範圍內的控制。 ● **記錄已執行的工作並識別稽核結果**—從業人員應記錄已執行的工作以及收集到的資訊和證據，並將稽核結果建檔。 ● **確認稽核結果並追蹤矯正措施**—從業人員應與受查方確認稽核結果。如果受查方在稽核業務結束前對稽核結果採取矯正措施，從業人員應在文件（和結論）中說明矯正措施及最初的稽核發現。 ● **得出結論並報告**—從業人員應得出結論並報告稽核發現對實現稽核目標的影響。僅關注有關控制的稽核結果而不評估對稽核目標的影響，是不夠充分的。

2204.3角色和職責、知識和技能

2204.3.1	負責稽核業務的從業人員應定義和管理資訊稽核團隊成員在整個專案過程中的角色和職責，至少涵蓋以下方面： ● 設計方式和方法。 ● 創建稽核工作方案。 ● 定義執行和審查角色。 ● 處理出現的各種事件、顧慮和問題。 ● 記錄和整理稽核發現。 ● 撰寫報告。
2204.3.2	根據專案需求，負責的從業人員應考量具體稽核專案所需的專業能力。他們應組建一支具備技能、知識和經驗的團隊，以成功完成稽核專案。從業人員應確保將這些角色和職責分配給最符合專案要求的技能組合的資訊稽核團隊成員。

2204.3.3	從業人員應只接受與其知識和技能相符的角色、職責和相關任務。時間和成本問題可能使從業人員無法在開始稽核專案前獲得所有必要的知識和技能；因此，如果從業人員合理預期能夠在稽核期間採取適當的措施來確保成功完成專案，則可以接受這些角色、責任和相關任務。以下措施可支持這樣的合理預期： ● **在職進修**—在某些情況下，從業人員可在稽核專案過程中獲得必要的技能和知識。 ● **監督**—負責的從業人員可以安排資訊稽核團隊成員接受充分的監督，使他們能夠在監督下順利完成任務。 ● **外部資源**—負責的從業人員可以為團隊內缺乏足夠的知識和技能的稽核專案領域聘請外部專家。負責的從業人員應考量促進內部資訊稽核團隊成員的發展，讓他們與外部專家緊密合作，確保知識和技能移轉至團隊中。

2204.4監督

2204.4.1	資訊稽核團隊成員在稽核專案期間執行的每項任務，應在負有監督職責的從業人員的監督下進行，以確保滿足稽核目標和適用的行業稽核標準。所需的監督情況在很大的程度上取決於執行稽核任務從業人員的技能、知識和經驗，以及稽核專案的複雜性。
2204.4.2	監督是一個過程，存在稽核專案的每個步驟中。監督包括： ● 確保資訊稽核團隊成員具備成功完成工作的技能、知識和經驗。 ● 確保制定並核准了適當的稽核專案計畫和稽核程序。 ● 審查稽核專案工作底稿。 ● 確保與受查方和其他利害關係人就稽核業務進行準確、清晰、簡要、客觀、及時且具有建設性的溝通。 ● 確保在稽核專案結束時完成已核准的工作方案(除非變更是合理性的且事先已獲得核准），並且滿足了稽核專案目標。 ● 為資訊稽核團隊成員提供發展技能和知識的機會。
2204.4.3	要求審查稽核專案工作底稿，以確保所有必要的稽核程序得到執行；收集的證據是充分且適當的；並能充分支持稽核發現、業務目標以及結論或意見。考量這些目標，審查工作應由執行稽核工作的從業人員(負有對資訊稽核團隊成員具監督責任)來進行。
2204.4.4	在審查過程中，審查員應記錄提出的問題。在從業人員回答問題時，應保留問題被提出和回答的證據。

2204.4.5	審查證據應被記錄與保留。關於已執行審查的證據，其記錄方式包括但不限於： ● 審查後在每份稽核專案工作底稿上簽字並註明日期 ● 填寫稽核專案工作底稿審查清單。 ● 準備一份已簽署的文件，提供接受稽查的稽核專案工作底稿的參考，並詳細說明審查的性質、時間、範圍和結果。 所有這些選項中的數位檔案和紙本文件均為有效。
2204.4.6	監督有助於評估從業人員的發展和績效。審查員對其他資訊稽核團隊成員執行的工作有特殊看法時，這可以對其表現進行詳細和充分的評估。審查員應指出有待改善績效的發展領域，並提出加強技能和知識的建議。

2204.5證據

2204.5.1	從業人員應獲取充分和適當的證據，以形成意見或支持結論，並實現稽核目標。判斷證據是否充分和適當，應基於稽核目標的重要性及所獲得證據所付出的努力來決定。
2204.5.2	如果從業人員判斷所獲得的證據不符合充分和衡量標準，不足以形成意見或支持結論與實現稽核目標，則應獲取更多的證據。
2204.5.3	從業人員應根據稽核的查核事項選擇最合適的程序來收集證據。
2204.5.4	從業人員應考慮稽核證據的可靠性（即證據提供者的獨立性、資訊提供者的資格、證據的客觀性及證據的時間）。
2204.5.5	從業人員應進行適當的分析和解釋，以支持稽核發現並得出結論。應將收到的證據和資訊與從業人員確認或制定的期望進行比較。從業人員應注意： ● 意外的差異。 ● 未出現預期差異的情況。 ● 潛在錯誤。 ● 欺詐或非法行為。 ● 違反法律、法規的情況。 ● 異常或非經常性活動。
2204.5.6	如果發現與預期存在偏差，從業人員應向管理階層詢問出現差異的原因。如果管理階層的解釋是充分的，從業人員應基於專業判斷調整自己的預期並重新分析證據和資訊。
2204.5.7	如果受查方未能充分解釋重大偏差，應形成稽核發現並傳達給高階管理階層或負責管理和監督稽核職能部門的治理機構。從業人員可根據具體情況建議應採取的適當行動。

2204.6文件記錄

2204.6.1	從業人員應及時準備充分、適當和相關的文件資料，為結論提供依據，並包含所執行審查的證據。充分、適當和相關的文件應能使先前與稽核專案無關的謹慎和知情人員，能夠重新執行從業人員在稽核專案期間執行的任務並得出相同的結論。文件應包括： ● 稽核專案目標和工作範圍。 ● 稽核專案計畫。 ● 稽核工作方案。 ● 執行的稽核步驟。 ● 收集到的證據。 ● 結論和建議。
2204.6.2	文件有助於規劃、執行和審查稽核專案，因為它： ● 明確了執行每個稽核任務的資訊稽核團隊成員，及其在準備和審查文件中的角色。 ● 記錄了所需的證據。 ● 支持所執行工作的準確性、完整性和有效性。 ● 為得出的結論提供了支援。 ● 促進了審查過程。 ● 記錄了是否已實現專案目標。 ● 為品質改進計畫提供了基礎。
2204.6.3	從業人員應在工作開始之前制定初步審查方案。稽核程序的記錄方式應有助於從業人員記錄稽核工作的完成情況，並識別尚待完成的工作。隨著工作的進行，從業人員應根據在稽核專案期間收集到的資訊來評估稽核程序的充分性。如果從業人員確定計畫的程序不充分時，則應對稽核程序做出對應的修改。
2204.6.4	應將績效和監督活動記錄在稽核專案的工作底稿中。稽核專案工作底稿的設計和內容因稽核業務的具體情況而異。但是，資訊稽核和確保管理階層應針對不同類型的稽核業務創建有限數量的工作底稿標準範本。標準工作底稿可提高稽核專案的效率且便於監督。資訊稽核和確保管理階層還應確定要使用的媒介或載體以及工作底稿的儲存及保存程序。
2204.6.5	從業人員應確保及時完成所執行工作的文件記錄。應在稽核報告的發佈日期之前獲取得出結論或意見所需的所有資訊和證據。稽核專案工作底稿應包括編製和審查的日期。
2204.6.6	資訊稽核和確保管理階層負責控管稽核專案的文件，並為授權人員提供存取權限。外部稽核師對稽核業務工作底稿的調閱請求，應得到高階管理階層和治理機構的核准。除了外部稽核師，其他單位的調閱請求，應由高階管理階層以及負責管理和監督稽核職能部門的治理機構，在法律顧問的評估意見下予以核准。

2204.7查核發現

2204.7.1	從業人員應分析收集到的證據和資訊。應將顯著偏離預期的情況形成稽核發現。從業人員應與受查方確認稽核發現，並評估這些稽核發現對控制環境其他方面的影響。
2204.7.2	從業人員可建議矯正措施，但不得執行這些措施。如果受查單位在稽核專案結束前採取了矯正措施來補正最初的稽核發現，從業人員應在文件中說明採用的矯正措施。
2204.7.3	從業人員應根據稽核發現做出結論，並評估其對稽核目標的影響。結論應基於最初的稽核發現得出。如果已採行了矯正措施，可以在結論中附上附錄，說明矯正措施，以及矯正措施其對最初結論的影響。
2204.7.4	所有結論以及關於是否已實現稽核目標的結論，都應記錄在稽核專案報告中。有關報告的詳細指導，請參閱報告標準1401和準則2401。

2204.8其他注意事項

2204.8.1	資訊稽核和從事確保從業人員應： ● 指派團隊成員，使其技能和經驗符合專案需求。 ● 適當情況下，將外部資源加入資訊稽核團隊，並確保其工作得到適當的監督。 ● 在整個專案過程中，管理特定資訊稽核團隊成員的角色和職責，至少涵蓋以下方面： ■ 分配執行和審查角色。 ■ 分配設計方式和方法論的職責。 ■ 創建稽核或確保程序。 ■ 進行工作。 ■ 處理出現的各種事件、顧慮和問題。 ■ 分析根本原因。 ■ 與團隊協調、審查、記錄和整清稽核發現。 ■ 撰寫報告。 ● 安排一名團隊成員執行業務，並由另一名適當的團隊成員進行審查。 ● 根據稽核目標的重要性以及獲得證據所需的時間和精力，使用可得到的最佳稽核證據。 ● 如果根據專業人員的判斷，所獲證據不符合衡量標準，不足以形成意見或支持發現和結論，則需要獲得更多證據。 ● 按照預先定義的文件和核准程序，組織並記錄在專案期間所執行的工作。

2204.8.1 (續)	● 在記錄中包含： ■ 稽核目標、工作範圍、稽核程序、執行的稽核步驟、收集的證據、稽核發現、結論和建議。 ■ 細節要足以讓謹慎的知情人員能夠重新執行已在專案期間執行的任務，並得出相同的結論。 ■ 確認每項任務的執行者，及每位團隊成員在準備和審查文件中的角色。 ■ 準備和審查文件的日期。 ● 獲得受查方提供的書面陳述，其中明確詳述業務的關鍵領域、已出現的問題及其解決方案，以及受查方作出的聲明。 ● 確任受查方的陳述已經過受查方簽字並署明日期，以表示承認其在專案方面的職責。 ● 在工作底稿中記錄並保留執行業務過程中收到的書面或口頭陳述。

標準1204和準則2204與COBIT® 2019的關聯

COBIT 2019 管理目標	目的
APO07 管理人力資源	優化人力資源能力，以滿足企業目標。
APO08 管理關係	掌握正確的知識、技能和行為，來創造更好的成果，增強信心和相互信任，以及有效地利用資源，以促進與業務利害關係人建立富有成效的關係。
MEA04 管理確保	促使組織設計和制定具效果與效率的確保機制，並採用公認的確保方法論，做為規劃，範圍界定，執行和後續追蹤提供指引。

執行標準1205：證據

聲明	1205.1資訊稽核和從事確保工作人員應獲取充分且適當的證據來得出合理的結論。
	1205.2運用專業懷疑態度，資訊稽核和從事確保工作人員應評估所獲得的證據是否足以支持結論並實現稽核專案的查核目標。
	1205.3與其他工作底稿一樣，資訊稽核和從事確保工作人員應在正式定義與核准的保留期限內保存證據。

執行準則2205：證據

2205.1簡介 本準則的目的是指導資訊稽核和從事確保工作人員如何獲得有效和適當的證據，如何評估得到的證據與如何準備適當的稽核記錄。本準則旨在為以下關鍵稽核和確保主題提供系統化資訊：

2205.2證據類型

2205.3取得證據

2205.4評估證據

2205.5準備稽核文件

2205.6其他注意事項

2205.2證據類型

2205.2.1	在規劃和執行稽核專案時，從業人員應考慮要收集的證據類型、如何通過這些證據達成稽核目標，以及不同的可靠性程度。從業人員應考慮採用的不同類型的證據包括： ● 觀察到的流程和實物。 ● 證明文件。 ● 陳述。 ● 分析。
2205.2.2	觀察到的流程和實物可包括對活動、財產和資訊職能的觀察，例如： ● 運行中的網路安全監控系統。 ● 異地存儲地點的媒體清單。
2205.2.3	記錄在書面或其他媒介上的證據包括： ● 書面政策和程序。 ● 資料提取的結果。 ● 交易記錄。 ● 程式清單。 ● 日常業務過程中產生的其他文件和記錄。 ● 第三方的外部確認。
2205.2.4	受查方的書面和口頭陳述可包括： ● 管理階層的書面陳述：，例如關於內部控制是否存在、及其有效性、或新系統實施計畫的陳述。 ● 口頭陳述：例如流程的運作方式、或管理階層對安全意識計畫有關的行動與跟進追蹤計畫。
2205.2.5	通過比較、模擬、計算和推理得出的資訊分析結果也可作為證據。例子包括： ● 對照其他企業或以往時期的績效為基準來衡量資訊績效。 ● 比較不同應用程式、交易和用戶間的錯誤率。 ● 重新執行流程或控制。

2205.3取得證據

2205.3.1	從業人員應取得足夠和適當的證據，以得出合理的稽核結論。此類證據包括： ● 已執行的程序。 ● 已執行的程序的結果。 ● 原始檔（電子或紙質格式）、記錄和用於支持稽核專案的佐證資訊。 ● 有關已完成工作並遵守適用的法律、法規和政策的文件。
2205.3.2	如果以口頭陳述方式所獲取的證據對稽核意見或結論至關重要，從業人員應考慮以書面或電子方式（例如：通過電子郵件）獲得對陳述的確認。從業人員還應考慮其他證據作為此類陳述的佐證，以確保其可靠性。
2205.3.3	在收集證據時，專業人員應考慮以下事項： ● 獲取證據所需的時間、精力和成本，與證據在降低稽核風險方面的充分性比較，。 ● 被評估的事項和需要證據的稽核程序，對於實現稽核目標和降低稽核風險的重要性。 ● 隨著時間的推移，全部或部分電子證據可能無法被檢索到。

2205.3.4	用於收集證據的程序因受稽核資訊系統的特點、稽核時間、稽核範圍和目標以及專業判斷不同而存在差異。可以使用手動稽核程序、電腦輔助稽核技術（CAAT）或結合兩者來收集證據。從業人員應選擇與資訊稽核目標相關的最適當程序。應考慮以下程序： ● **詢問和確認**—向熟悉查核事項的有經驗人員尋求資訊的過程。有經驗的人員不一定是受查企業的成員。此程序可以是正式的書面詢問也可以是非正式的口頭詢問。 ● **觀察**—觀察係指由負責執行的人員通常執行的程序或流程，或者觀察實物，例如設施、電腦硬體或資訊系統設置或配置等。這類證據僅限於觀察發生時所處的時間點。從業人員應考慮到，對流程或程序的觀察可能會影響到流程或程序的執行方式。 ● **檢查**—檢查內部或外部檔案和記錄。待檢查的項目可以是紙本或電子形式提供。檢查也可以包括實體的資產檢查。 ● **分析程序**—通過檢查資料內部或資料與其他相關資訊間的可能關係來評估資料。這包括檢查波動、趨勢和不一致的關係。 ● **重新計算與運算**—手動或使用CAATs來檢查檔案或記錄的算術與數學準確性的過程。 ● **重新執行**—獨立執行最初由資訊系統或企業執行的程序或控制。 ● **其他普遍接受的方法**—從業人員可採用其他普遍接受的程序來收集足夠和適當的證據，例如參與社交工程、充當秘密客或執行道德滲透測試。
2205.3.5	收集證據時，從業人員應考量提供證據的獨立性和品質。例如一般情況下，獨立第三方提供的確切稽核證據，比受查企業提供的稽核證據更為可靠。稽核證據通常比個人陳述也更可靠。
2205.3.6	如果收集到的證據有可能成為法律訴訟的一部分，從業人員應諮詢適當的法律顧問，確定是否有特殊要求會影響收集、提交和揭露證據的方式。
2205.3.7	在從業人員無法獲得充分稽核證據的情況下（例如：個人或管理階層拒絕提供實現資訊稽核目標所需的適當證據），從業人員應根據組織的既定程序向稽核管理階層揭露此一情況，必要時向稽核治理機構報告。在溝通稽核結果時，應說明稽核範圍和稽核目標的實現受到的限制或局限。

2205.3.8	從業人員在完成稽核工作後應保留證據，確保證據得以： ● 在一段時間內可用，並採用符合稽核組織的政策以及相關專業標準、法律和法規的格式。 ● 在整個準備和保留期間得到保護，防止未經授權的揭露或修改。 ● 在保留期結束時得到妥善處理。

2205.4評估證據

2205.4.1	當證據在稽核目標範圍內為稽核結果或結論提供了合理依據時，則證據是充分且適當的。如果從業人員判斷，證據不符合這些衡量標準，則應獲取更多證據或執行其他程序，以減少與證據有關的限制或不確定性。例如如果沒有其他證據可以佐證某程式清單代表正式環境中實際使用的程式，則該程式清單可能不足以作為證據。
2205.4.2	在評估稽核期間獲得證據的可靠性時，從業人員應考慮證據的特徵和屬性，例如來源、性質（書面、口頭、視覺或電子形式）、真實性（存在數位或人工簽名、日期/時戳）以及提供多個來源佐證的證據之間的關係。通常依據用於獲取證據的程序，將證據的可靠性從低到高排序，具體如下： ● 詢問和確認。 ● 觀察。 ● 檢查。 ● 分析程序。 ● 重新計算或運算。 ● 重新執行。 對於上述每個程序，當滿足以下條件時，證據可靠性通常更高： ● 採用書面形式，而不是口頭陳述。 ● 由從業人員直接獲取，而不是受查方提供。 ● 獲得自獨立來源。 ● 經過獨立方鑒定。 ● 由獨立方維護。
2205.4.3	在確定實質性測試和符合性測試（如適用）的性質、時間和範圍時，從業人員應考慮資訊存在或可用的時效性。例如對於由電子資料交換（EDI）、數位影像處理（DIP）和試算表處理的證據，如果未控制檔案的變更或者檔案未備份，則其可能在一段時間之後便無法被檢索到。文件可用性還可能受到企業文件保留政策的影響。
2205.4.4	如果有獨立的第三方稽核，從業人員應考慮與稽核主題相關的控制是否經過了測試，以及是否可以依賴於該測試的結果。
2205.4.5	從業人員獲取的證據應充分且適當，能夠讓合格的獨立方重新執行測試並得出相同結果和結論。

2205.5準備稽核文件

2205.5.1	在執行稽核的過程中，從業人員應記錄所獲得的證據，確保稽核文件在預定時間期限內得到保留與可用，並且是採用符合企業政策以及相關專業標準、法律和法規的格式。
2205.5.2	應適當地識別和交叉引用在執行稽核的過程中獲得的證據並編成目錄，以便於確定證據的總體充分性和適當性。這些步驟是必要的，有助於在稽核目標範圍內為稽核發現或結論提供合理依據，並使其他資訊稽核團隊成員或獨立方能夠輕鬆地檢索到這些證據。
2205.5.3	在整個證據準備和保留期間，從業人員都應保護該證據文件不受未經授權的存取、揭露或修改。保留期限可能受外部要求的影響。例如對於須遵守美國證券交易委員會（SEC）要求的企業，財務稽核師必須將某些記錄保留七年（自稽核或審查結束之日起計算）[1]。
2205.5.4	從業人員應在規定的保留期結束時處置證據文件。

2205.6其他注意事項

2205.6.1	執行某個業務時，資訊稽核和從事確保工作人員應： ● 適當地識別、交叉引用證據並編成目錄。 ● 考慮收集必要證據、滿足業務目標和風險要求的最有效和最及時方式。然而，困難或成本不能成為省略必要程序的有效理由。 ● 獲得與項目的重要性及相關風險相稱的證據。 ● 當資訊稽核或從事確保工作人員利用獲得自企業的資訊來執行稽核程序時，要適當強調資訊的準確性和完整性。

標準1205和準則2205與COBIT® 2019的關聯

COBIT 2019 管理目標	目的
MEA04 管理確保	促使組織設計和制定具效果與效率的確保機制，並採用公認的確保方法論，做為規劃，範圍界定，執行和後續追蹤提供指引。

[1] 美國證券交易委員會，「最終規則:查核紀錄之保留」，*www.sec.gov/rules/final/33-8180.htm#:~:text=Under%20the%20new%20rule%2C96,of%20the%20audit%20or%20review*

執行標準1206：使用其他專家的工作

聲明	1206.1資訊稽核和從事確保工作人員應考慮在適當的情況下將其他專家的工作用於稽核和確保業務。
	1206.2資訊稽核和從事確保工作人員應在聘用前評估與核准其他專家的專業資格、能力、相關經驗、資源、獨立性以及品質控制流程的充分性。
	1206.3資訊稽核和從事確保工作人員應評估、複核並評價其他專家的工作，以作為查核業務的一部份，並記錄對關於使用和信賴他們工作程度的結論。
	1206.4資訊稽核和從事確保工作人員應確定稽核團隊之外的其他專家工作，是否足夠且完整的對目前稽核目標得出結論。從業人員還應明確地紀錄此項結論。
	1206.5資訊稽核和從事確保工作人員應確定是否信賴其他專家的工作並直接納入報告，或是在報告中單獨引用。
	1206.6如果其他專家的工作無法提供充分適當的證據，資訊稽核和從事確保工作人員應採用其他的測試程序來獲取充分適當的證據。
	1206.7如果透過其他測試方式仍無法獲得所需的證據，資訊稽核和從事確保工作人員應提出適當的稽核意見或結論，並註明其範圍限制。

執行準則2206：使用其他專家的工作

2206.1簡介 本準則指導資訊稽核和從事確保工作人員如何使用其他專家的工作。本準則旨在為以下關鍵稽核和確保業務主題提供系統化資訊：

2206.2考慮使用其他專家的工作

2206.3評估其他專家的勝任能力

2206.4規劃和審查其他專家的工作

2206.5評估其他專家的工作

2206.6其他測試流程

2206.7稽核意見或結論

2206.8其他注意事項

2206.2考慮使用其他專家的工作

2206.2.1	如果從業人員不具備執行稽核業務所需的全部或部分能力，應考慮尋求其他具備所需技能專家的幫助。
2206.2.2	如果存在可能影響即將執行的稽核工作的限制，例如缺少待執行任務性質所需的技術知識、稽核資源匱乏、時間限制和潛在的獨立性問題，則應考慮使用其他專家的工作方式。如果有助於提高專案品質，也應考慮使用其他專家的工作。
2206.2.3	不要求從業人員具備與其他專家同等水準的知識。但是，從業人員應對所執行的工作有充分的瞭解，以便指導和審查其他專家的工作。當依賴他人的工作成果時，從業人員應出具客觀證據，證明專家的能力和技能水準。
2206.2.4	從業人員應根據客觀的衡量標準，來選擇特定的專家和使用其他專家的工作。
2206.2.5	從業人員應在專家開始參與專案之前，以合約或協議的方式與其他專家溝通並記錄績效要求。
2206.2.6	如果企業內部政策禁止其他專家存取記錄或系統，從業人員應確定在多大程度上可以使用和依賴其他專家的工作。
2206.2.7	如果無法獲得必要的專家，從業人員應記錄對實現稽核目標的影響，並在稽核計畫中說明具體任務，以管理由此產生的稽核風險。如果無法管理由此產生的稽核風險，從業人員可能需要拒絕稽核業務。
2206.2.8	在審查時，資訊稽核和從事確保工作人員可能會依賴系統和組織控制(SOC)報告。

2206.3評估其他專家的勝任能力

2206.3.1	如果稽核業務涉及使用其他專家的工作，則從業人員在規劃資訊稽核工作時應考慮其他專家的勝任能力，即評估其他專家的專業資格、能力、相關經驗、資源以及品質控制流程的使用。
2206.3.2	在依賴其他專家的工作之前，從業人員應考慮其獨立性和客觀性。選拔任用流程、組織狀態、彙報關係以及其他專家的建議對管理實務的影響，是評估其他專家的獨立性和客觀性的典型指標。

2206.4規劃和審查其他專家的工作

2206.4.1	從業人員應核實稽核組織章程或專案委任書中規定了他們使用其他專家的工作的權利。從業人員應有權使用其他專家建立的所有工作底稿、證明文件和報告，只要此類使用不會造成法律或隱私問題。

2206.4.2	從業人員在規劃資訊稽核工作時應考慮其他專家的活動，及其對資訊稽核目標的影響，包括： ● 瞭解其他專家的工作範圍、方法、時間以及使用的品質控制流程。 ● 確定所需的審查水準。
2206.4.3	所需稽核證據的性質、時間和範圍將取決於其他專家工作的重要性和範圍。在規劃過程中，從業人員應確定所需的審查水準，以提供充分且適當的稽核證據，從而以有效的方式實現總體資訊稽核目標。從業人員應審查其他專家的最終報告、方法或稽核程序以及工作底稿。
2206.4.4	在審查工作底稿時，從業人員應評估其他專家的工作是否經過適當的規劃、監督、記錄和審查，以考慮所提供的稽核證據的適當性和充分性，並確定在多大程度上使用和依賴專家的工作。該評估可能包括對其他專家的工作進行重新測試。還應評估是否符合相關專業標準。總的來說，從業人員應評估其他專家的工作是否充分且完整，使他們能夠就當前的資訊稽核目標得出結論並進行記錄。
2206.4.5	從業人員應充分審查其他專家的最終報告，確認是否： ● 滿足稽核組織章程、職權範圍或專案委任書中規定的範圍。 ● 識別出其他專家採用的重要假設。 ● 有充分的證據支持所報告的稽核結果和結論。

2206.5評估其他專家的工作

2206.5.1	客戶與供應商在非核心活動的處理和外包方面的相互依賴關係造成了複雜的稽核環境。部分被稽核的環境可能由其他獨立職能部門或企業控制和稽核。外包企業將收到這類第三方提供的有關外包營運控制環境的報告。在某些情況下，這些營運可能會縮減資訊稽核的覆蓋範圍，即使從業人員無法獲取支持文件和工作底稿。在這種情況下，從業人員應慎重提出意見。

2206.5.2	從業人員應評估其他專家的工作的有用性和適當性，並考慮其他專家報告的重大發現。從業人員負責確定在多大程度上依賴其他專家的工作，以及是直接納入報告，還是在報告中單獨引用。從業人員還應評估其他專家的發現和結論對總體資訊稽核目標的影響。從業人員還應驗證完成總體資訊稽核目標所需的其他工作。其他專家提出的所有聲明應得到管理階層的驗證和正式核准。有關此主題的詳細指導，請參閱標準1007「聲明」。

2206.6其他測試流程

2206.6.1	從業人員應基於對其他專家的工作的評估，如果其他專家的工作工作沒有提供這樣的證據，則應採用其他測試流程來獲取充分且適當的稽核證據。
2206.6.2	從業人員應考慮是否需要對其他專家的工作進行補充測試。

2206.7稽核意見或結論

2206.7.1	從業人員負責形成稽核意見或結論。從業人員需要確定其他專家執行的工作是否足以支持稽核意見或結論。
2206.7.2	如果執行的其他測試流程未能提供充分且適當的稽核證據，從業人員應提供適當的稽核意見或結論，必要時包括範圍限制。
2206.7.3	如果從業人員在形成意見時採用了專家的報告，則應在稽核業務報告中包含從業人員對於其他專家報告的可採納性和相關性的觀點和評論。
2206.7.4	適當情況下，從業人員應考慮管理階層在多大程度上採納了其他專家的建議。這應該包括評估管理階層是否致力於在適當的期限內矯正其他專家發現的問題以及矯正工作的當前狀態。

2206.8其他注意事項

2206.8.1	資訊稽核和從事確保工作人員應： ● 以文件記錄下如果無法獲得需要的專家對實現專案目標的影響，並在專案計畫中加入具體的工作任務，以管理風險和證據要求。 ● 如果由於法律問題，從業人員未被授予記錄的存取權限，則應決定對其他專家工作的使用和依賴程度並就此作出結論。 ● 在報告中記錄對其他專家工作的使用情況。

標準1206和準則2206與COBIT® 2019的關聯

COBIT 2019 管理目標	目的
MEA04 管理確保	促使組織設計和制定具效果與效率的確保機制，並採用公認的確保方法論，做為規劃，範圍界定，執行和後續追蹤提供指引。

執行標準1207：違規和非法行為

聲明	1207.1資訊稽核和從事確保工作人員應在工作中考量違規和非法行為的風險。
	1207.2資訊稽核和從事確保工作人員應及時紀錄違規或非法行為並向適當單位通報。請注意，某些溝通 （例如：與主管機關的溝通）可能會受到限制。因此，從業人員在溝通之前可能需要與負責治理和監督稽核職能部門的機構（例如董事會或審計委員會）進行討論。

執行準則2207：違規和非法行為

2207.1簡介 本準則詳細闡述管理階層及資訊稽核和從事確保工作人員在違規和非法行為方面的職責。本準則旨在為以下關鍵稽核和確保業務主題提供系統化資訊：

2207.2違規和非法行為

2207.3管理階層的職責

2207.4從業人員的職責

2207.5稽核專案規劃期間的違規和非法行為

2207.6設計和審查稽核專案程序

2207.7應對違規和非法行為

2207.8內部報告

2207.9外部報告

2207.10其他注意事項

2207.2違規和非法行為

2207.2.1	違規和非法行為會直接對企業的財務和聲譽造成許多的負面影響，並間接影響生產力和員工保留。企業必須建立意識、預防和偵測機制，以迅速發現違規和非法行為。如果缺乏控制、控制的設計不當或控制出現問題，便會增加發生違規和非法行為的可能性。
2207.2.2	企業內部任何層級的員工都有可能做出違規和非法行為。此類活動包括但不限於： ● 欺詐，即通過欺騙手段獲取非法利益的行為。 ● 故意歪曲事實，以謀取利益或隱瞞違規和非法行為。 ● 違反法律法規的行為，包括未能確保資訊系統或流程符合適用的法律法規要求。 ● 未經授權揭露受隱私法保護的資料。 ● 資料保留做法違反適用的隱私法律和法規。 ● 涉及不遵守與第三方（例如：銀行、供應商、服務提供者和係害關係人）簽訂企業協議和合約的行為。 ● 篡改、歪曲、偽造或更改電子或紙本形式的記錄或文件。 ● 隱匿或忽略電子、紙本記錄或文件中交易的影響。 ● 不當或故意洩露機密資訊。 ● 記錄缺乏實質且已知為虛假的交易（無論是電子還是紙本形式），例如虛假付款、工資欺詐、逃稅。 ● 盜用和濫用資產。 ● 竊取或挪用公款，在現金被記錄到企業的財務記錄前即進行盜用。 ● 侵犯智慧財產權（IP）的行為，例如有意或無意地侵犯版權、商標和專利。 ● 允許未經授權的資訊和系統存取權限。 ● 由於未經授權存取資料和系統而導致的財務或其他記錄錯誤。
2207.2.3	要確定某個行為是否違法，通常依據知情的法律專業人士的建議，或者需要等待法院的最終裁定。從業人員應首先關注違規行為的後果或潛在後果，無論是被懷疑還是已被證實違法的行為。
2207.2.4	不應將所有違規行為都視為欺詐活動。欺詐活動的確定取決於所在司法管轄區對欺詐的法律定義。 欺詐性違規行為包括但不限於： ● 故意規避控制，以圖掩蓋持續的欺詐行為。 ● 未經授權使用資產或服務。 ● 教唆或協助掩蓋此類活動。 非欺詐性違規行為可能包括： ● 重大過失。 ● 無意的非法行為。

2207.2.5	在某些情況下，從業人員在舉報潛在非法行為或欺詐後可能受到報復或恐嚇。考慮到相關各方，首席稽核執行官（或稽核副總裁/董事）、高階管理階層以及負責治理和監督稽核職能部門的機構(例如：董事會或審計委員會)應與法律顧問合作解決此問題。他們的工作應包括解決與威脅或恐嚇有關的問題，並可能需要與當地執法機構合作。

2207.3管理階層的職責

2207.3.1	管理階層和董事會的首要職責是提供控制，以制止、預防和偵測違規和非法行為。
2207.3.2	管理階層通常使用以下手段來合理保證違規和非法行為及時得到制止、預防或偵測： ● 設計、執行和維護內部控制系統（包括交易審查和核准，及管理階層審查程序），以預防和偵測違規和非法行為。 ● 規範員工行為的政策和程序。 ● 合規性驗證和監控程序。 ● 設計、執行和維護合適的系統，用於報告、記錄和管理與違規和非法行為有關的事件。 ● 管理合規性和法規要求的政策和程序。
2207.3.3	管理階層應向從業人員揭露其對任何違規或非法行為的瞭解、及受影響的領域與所採取的行動，無論是宣稱、懷疑還是已證實的違規或非法行為。
2207.3.4	如果有宣稱、懷疑或發現的違規或非法行為，管理階層應協助調查和詢問。

2207.4從業人員的職責

2207.4.1	從業人員應考慮在稽核組織章程中定義管理階層以及資訊稽核和確保管理階層在預防、偵測和報告違規行為方面的職責，使他們在所有稽核工作中清楚地瞭解這些職責。如果企業政策或類似文件中已定義這些職責，則稽核組織章程應包括相關聲明。
2207.4.2	從業人員應瞭解，控制機制無法完全消除出現違規或非法行為的可能性。從業人員負責評估出現違規或非法行為的風險，以及已識別的違規行為的影響，並根據稽核業務的性質設計和執行合適的測試。
2207.4.3	從業人員不負責預防或發現違規或非法行為。稽核專案無法保證可以發現出違規行為。即使適當地規劃和執行了稽核，也可能無法發現出違規行為，例如員工之間互相勾結或員工與外部人員串通，或者管理階層參與了違規行為。稽核旨在確定是否實施了控制，以及控制是否適當、有效且得到遵循。
2207.4.4	如果從業人員知悉有關違規或非法行為的具體資訊，則有義務進行舉報。
2207.4.5	如果從業人員認為存在違規或非法行為風險較高的情況，即使沒有發現，也應向管理階層和治理機構報告。
2207.4.6	從業人員應適度熟悉所審查的領域，能夠識別可能導致違規或非法行為的風險因素。

2207.5稽核專案規劃期間的違規和非法行為

2207.5.1	從業人員應採用適當的方法，評估出現與被稽核領域關聯的違規或非法行為的風險。在準備此評估時，從業人員應考慮以下因素： ● 組織特徵，例如公司道德、組織結構、監督的充分性、薪酬和獎勵結構、公司績效壓力水準以及企業發展方向。 ● 企業的歷史、過去發生的違規行為，以及之後為降低或盡可能減少與違規有關的稽核發現而採取的行動。 ● 管理、營運或資訊系統的最新變更以及企業當前的戰略方向。 ● 新的策略夥伴關係帶來的影響。 ● 持有的資產或提供的服務的類型，及其對違規行為的敏感性。 ● 評估相關控制的強度，以及可能使已建立的控制被規避或繞過的漏洞。 ● 適用的法律法規要求。 ● 內部政策，例如吹哨者政策、內幕交易政策以及員工和管理人員的道德規範。 ● 利害關係人關係和金融市場。 ● 人力資源能力。 ● 市場關鍵資訊的機密性和完整性。 ● 以往稽核的結果。 ● 企業所處的產業和競爭環境。 ● 在稽核範圍之外進行的稽核發現，例如來自顧問、品質保證團隊或特定管理階層調查的結果。 ● 日常業務中的發現。 ● 存在的過程檔案或品質管制系統。 ● 被稽核領域資訊系統的技術複雜性。 ● 與套裝軟體相比，內部是否存在為核心業務系統而開發與維護的應用系統。 ● 員工不滿造成的影響。 ● 潛在的裁員、外包、撤資或結構重組。 ● 是否存在容易被盜用的資產。 ● 組織財務或營運績效不佳。 ● 管理階層對道德的態度。 ● 特定產業常見的或在類似企業中發生過的違規和非法行為。

2207.5.2	在規劃和執行風險評估的過程中，從業人員應詢問管理階層，並在適當的情況下獲得有關以下面向的書面聲明： ● 管理階層對企業中出現違規和非法行為的風險水準的理解。 ● 管理階層是否瞭解企業內部已經發生或可能發生的違規和非法行為，或是否注意過相關跡象。 ● 管理階層在設計和執行內部控制來預防違規和非法行為方面的職責。 ● 如何監控或管理出現違規或非法行為的風險。 ● 實施了哪些流程向相應的利害關係人通報宣稱、懷疑或實際發生的違規或非法行為。 ● 組織營運所在司法管轄區適用的國家和地區法律，以及法務部門與風險委員會或審計委員會合作的程度。

2207.6設計和審查稽核專案程序

2207.6.1	從業人員對違規和非法行為的偵測和預防不承擔具體的職責，但在設計稽核業務程序時應考慮到已發現的違規和非法行為。
2207.6.2	從業人員應使用風險評估的結果來確認所需測試的性質、時間和程度，以獲得充分的稽核證據，合理保證能夠識別： ● 可能對被稽核領域或整個企業產生重大影響的違規行為。 ● 可能導致無法預防或偵測出重大違規行為的控制缺失。 ● 內部控制的設計或運作中存在的所有可能影響發行者之記錄、處理、總結和報告業務資料能力的重大缺失。
2207.6.3	從業人員應審查專案程序的結果，以確定是否存在可能已發生違規和非法行為的跡象。使用計算機輔助稽核技術（CAATs）可大大提高違規或非法行為偵測的效率和有效性。

2207.6.4	在評估專案程序的結果時，凡已識別的風險因素應對照實際執行的程序審查，以合理保證所有已識別的風險皆已提及。

2207.7應對違規和非法行為

2207.7.1	在稽核專案期間，從業人員可能會注意到存在違規或非法行為的跡象。在這種情況下，應考慮違規或非法行為對專案查核事項、稽核目標、稽核業務報告和企業的潛在影響。
2207.7.2	從業人員應展現出應盡專業上注意的態度。存在違規或非法行為的跡象（有時稱為「欺詐」或「紅旗警示」）包括： ● 管理階層淩駕於控制之上。 ● 管理階層行為不規範或缺乏合理的解釋。 ● 績效一直高於設定的目標。 ● 在接收所請求的資訊或證據時，出現問題或延遲。 ● 不符合正常核准週期的交易。 ● 特定客戶的活動增加。 ● 客戶投訴增加。 ● 某些應用程式或使用者的存取控制出現偏差。 如果從業人員注意到上述跡象，應予以密切關注。
2207.7.3	如果從業人員獲悉潛在違規或非法行為的相關資訊，應尋求相應法律機構的指示，然後考慮採取以下步驟： ● 瞭解行為的性質。 ● 瞭解行為發生的具體情況。 ● 收集行為的證據（例如：信件、系統記錄、電腦檔案、安全記錄檔以及客戶或供應商訊息）。 ● 確定參與該行為的所有人員。 ● 獲得充分的支援資訊，以評估該行為的後果。 ● 執行一定數量的其他程序，以確定該行為的後果以及是否存在其他行為。 ● 記錄並保存所有證據和工作成果。
2207.7.4	對潛在違規或非法行為採取適當的步驟後，從業人員應諮詢稽核管理階層，以確定下一步行動，例如向企業管理階層報告「事件」、轉交由內部欺詐調查人員採取進一步行動，或者向執法部門或監管機構報告。
2207.7.5	如果違規行為涉及管理階層成員，從業人員應重新考慮管理階層所作陳述的可靠性。從業人員應與適當層級的管理階層合作，後者通常應高於涉嫌違規或非法行為的管理人員的層級。

2207.8內部報告

2207.8.1	從業人員應及時以書面或口頭方式向企業相關人員通報發現的違規和非法行為。應通知更高層級（高於涉嫌違規或非法行為的管理人員的層級）的管理階層。此外，應向企業治理機構（例如：董事會、受託人、審計委員會或同等組織）報告違規和非法行為。對財務影響明顯不大且控制缺失跡象不明顯的事項可能不需要向更高層級報告。 如果從業人員懷疑各級管理階層均有參與，應根據適用的當地法律、法規，向企業治理機構（例如：董事會、受託人、審計委員會或同等組織）秘密報告稽核結果。當地法律、法規可能禁止向規定的法律機構以外的其他方報告。
2207.8.2	從業人員在舉報違規或非法行為時應運用專業判斷。他們應與適當層級的管理階層（至少比涉嫌參與違規或非法行為的人員高一個層級）討論稽核結果，以及將要執行的進一步程序的性質、時間和範圍。在這種情況下，保持獨立性對從業人員來說尤其重要。
2207.8.3	從業人員應慎重考慮向哪些內部人員分發有關違規和非法行為的報告。識別發生的違規或非法行為及其影響是一個敏感問題，報告分發也伴隨著風險，包括： ● 由於發佈了有關控制缺失的詳細資訊而招致進一步濫用。 ● 當揭露（授權或未授權）發生在企業外部時，而造成客戶、供應商和投資者流失。 ● 關鍵人員和管理人員（包括那些未參與違規或非法行為的人員）對管理階層和企業前景的信心下降而導致這些人員流失。
2207.8.4	從業人員應考慮將違規或非法行為與其他稽核問題分開報告，以作為控制報告派發的一種方式。
2207.8.5	從業人員應避免驚動任何可能牽涉或參與違規或非法行為的人員，以減少證據被破壞或藏匿的可能性。
2207.8.6	稽核組織章程應明確定義從業人員在報告違規或非法行為方面的職責。

2207.9外部報告

2207.9.1	對外報告欺詐、違規或非法行為可能是一項法律或監管法規義務。該義務可能適用於企業管理階層或發現違規行為的個人。稽核師的法律報告要求受當地管轄，並取代內部政策或合約協議。可能需要對外報告的其他情況包括： ● 法律、法規要求的遵守情況。 ● 法院命令。 ● 資助機構或政府機構根據接受政府財政援助的實體稽核要求所參與的情況。 ● 外部稽核師的要求。
2207.9.2	如果需要對外報告，所報告資訊的形式和內容，應經過適當層級的資訊稽核和確保管理階層核准，並在對外發佈之前與受查方的高階管理階層共同審查，除非適用法規或稽核業務的特定情況禁止這樣做。可能妨礙獲得受查方高階管理階層同意的特定情況包括： ● 受查方高階管理階層主動參與違規或非法行為。 ● 受查方高階管理階層被動默許違規或非法行為。
2207.9.3	如果受查方高階管理階層不同意對外發佈報告，並且對外報告是一項法律或法規義務，從業人員應考慮向審計委員會和法律顧問諮詢，瞭解對企業外部發佈稽核結果的適當性和風險。即使在受律師委託人特權保護的情況下，從業人員也應在對外揭露之前尋求法律意見和建議，確認確實受此特權的保護。
2207.9.4	獲得資訊稽核和確保管理階層的核准後，從業人員應及時向相關監管機構報告違規或非法行為。如果企業未能揭露已知的違規或非法行為，或要求從業人員隱瞞這些稽核結果，從業人員應尋求法律意見和建議。
2207.9.5	如果從業人員檢測到違規或非法行為，應及時通知外部稽核師。
2207.9.6	如果從業人員知道管理階層被要求向外部組織報告欺詐活動，應正式告知管理階層其責任。

2207.10其他注意事項

2207.10.1	資訊稽核和從事確保工作人員應： ● 在規劃和執行業務時通過以下方式將稽核風險降低到可接受的水準： ■ 意識到由於存在違規和非法行為造成的重大錯誤、控制缺失或誤報仍可能存在，無論違規和非法行為的風險評估結果如何。 ■ 瞭解企業及其環境，包括與業務查核事項、範圍和目標的相關性，旨在預防或偵測違規和非法行為的內部控制。 ■ 獲取充分和適當的證據，以確定企業內部的管理階層或其他人員是否知悉實際、懷疑或宣稱的違規和非法行為。 ● 考慮可能表明存在因違規和非法行為造成重大錯誤、控制缺失或誤報的風險的異常或意外關係。 ● 設計和執行相關程序，以測試內部控制的適宜性以及管理人員淩駕于旨在預防或偵測違規和非法行為的控制之上的風險。 ● 評估已識別的錯誤、控制缺失或錯誤陳述是否表明存在違規或非法行為的跡象。如果確有這種跡象，考慮這對業務其他相關方面的影響，尤其是管理階層陳述。 ● 獲得管理階層的書面聲明（至少每年一次，具體取決於業務情況），以確認其設計和執行內部控制來預防或偵測違規和非法行為的職責。 ● 揭露表明違規或非法行為可能造成錯誤、控制缺失或誤報的風險評估的中肯結果。 ● 揭露管理階層知悉影響企業的違規和非法行為的瞭解，涉及到擔任重要內部控制角色的管理階層和員工。 ● 揭露由員工、前員工、監管機構和其他人員通報，且管理階層已知悉影響企業的宣稱或懷疑違規或非法行為。 ● 及時的溝通： ■ 適當層級的管理階層，發現或獲得可能存在重大違規或非法行為的任何資訊。負責治理的人，任何涉及管理階層或擔任重要內部控制角色的員工的重大違規或非法行為。 ■ 負責治理的人，在內部控制設計和執行中預防和偵測違規和非法行為的措施存在重大漏洞，即使這些缺陷不在範圍內。 ■ 考慮適用於該情形的法律及專業報告要求。 ■ 如果重大錯誤、控制缺失、誤報或非法行為影響業務的持續有效性，則應考慮退出專案。 ■ 記錄並報告給管理階層、治理機構、監管機構及其他人員，有關重大違規或非法行為的所有溝通、計畫、結果、評估及結論。

標準1207和準則2207與COBIT® 2019的關聯

COBIT 2019 管理目標	目的
EDM03 確保風險最佳化	確保資訊與科技(I&T)相關企業風險不超過企業的風險偏好和風險容忍度，識別和管控I&T風險對企業價值的影響，以及最大程度地降低不合規的可能性。
APO12 管理風險	將資訊與科技(I&T)相關的企業風險管理整合到總體企業風險管理(ERM)中，並平衡I&T相關企業風險管理的成本和效益。
MEA03 管理外部要求合規	確保企業符合所有適用的外部要求。
MEA04 管理確保	促使組織設計和制定具效果與效率的確保機制，並採用公認的確保方法論，做為規劃，範圍界定，執行和後續追蹤提供指引。

報告標準

報告標準1401：報告

聲明	1401.1資訊稽核和從事確保工作人員應以報告形式傳達各項稽核專案查核的結果。
	1401.2資訊稽核和從事確保工作人員應確保稽核報告中所列的查核發現有充分且適當的證據予以支持。

報告準則2401：報告

2401.1簡介 本準則詳細闡述了稽核作業報告應包含的所有方面，並向資訊稽核和從事確保工作人員提供起草和最終完成稽核專案報告時需考慮的因素。本準則旨在為以下關鍵稽核和確保查核目標提供系統化資訊：

2401.2稽核業務報告的必要內容

2401.3後續事件

2401.4其他溝通

2401.5其他注意事項

2401.2稽核業務報告的必要內容

2401.2.1	稽核報告應包含按照ISACA的資訊稽核和確保標準或其他適用的專業標準執行稽核業務的聲明：報告中應明確提及不符合這些標準的情況。 稽核報告還應包含稽核業務的範圍。範圍包括：對稽核目標或活動的定義或描述；接受稽核的期間和執行稽核的期間；所執行的工作的性質和範圍；以及範圍內的任何限定或限制。
2401.2.2	稽核報告應包含所執行工作的總結，這有助於報告的使用者更好地瞭解所提供確保的性質。
2401.2.3	稽核報告應包含專門的章節，說明稽核師意見。在撰寫稽核報告時，從業人員應考慮所有相關證據，無論是有助於證實目標事項資訊還是與之相悖的證據。意見應該得到基於既定衡量標準控制程序結果的支持。從業人員應確定是否已獲得充分和適當的證據來支持稽核業務報告中的結論。 報告應就所有重大方面發表意見，即與活動領域有關的控制程序設計或運作是否有效。

2401.2.4	稽核報告應包含聲明，說明管理階層對於控制程序有效性聲明的來源。此外還應指出，管理階層有責任維護有效的內部控制結構（包括活動領域的控制程序）。
2401.2.5	稽核報告應說明稽核目標。
2401.2.6	稽核報告應包括對衡量標準的描述，及衡量標準的來源。此外，從業人員應考慮揭露： ● 應用衡量標準時做出的重要解釋。 ● 當衡量標準允許在多種衡量方法中進行選擇時，所採用的衡量方法。 ● 所採用的標準衡量方法的變更。
2401.2.7	稽核報告應包含預期的使用者和分發限制。
2401.2.8	稽核報告應包含負責報告的個人或機構的簽名和地點。
2401.2.9	稽核報告應包含稽核報告的發佈日期。在大多數情況下，報告日期即為發佈日期。如果未在執行工作概要中註明執行稽核工作的日期，則建議在報告中提及。
2401.2.10	稽核報告應提及分發（即預期的使用者和取閱限制）需要符合稽核組織章程或委任書中的條款。在某些地區，可能要求資訊稽核和確保從事確保工作人員揭露其證書（例如：ISACA或其他專業組織的證照編號或會員編號）。
2401.2.11	稽核報告應包含觀察、稽核發現、結論和建議，並附上矯正成本（如果可確定）。稽核發現、結論和矯正措施建議應包含管理階層的回饋。從業人員應可從每個管理階層回饋中，瞭解有關稽核建議對應的矯正措施資訊，即為實施或解決所報告的稽核建議而採取的措施以及計畫的執行或行動日期。 如果從業人員與受查方就特定的建議或稽核評論未能達成一致意見，則應在專案溝通中說明雙方的立場和出現分歧的原因。受查方的書面意見可作為稽核報告的附錄，或者納入報告正文或附函中。高階管理階層或負責資訊稽核和確保職能部門的治理人員應決定支持哪一方的觀點。

2401.3後續事件

2401.3.1	有時，在測試結束後到稽核報告發佈前這段期間，會發生對稽核目標或活動有重大影響的事件。此類事件稱為「後續事件」，可能需要揭露，因為它們可能會導致聲明或結論的改變。在執行稽核專案時，從業人員應考慮那些他們應該關注的後續事件資訊。但是，從業人員不承擔偵測後續事件的職責。
2401.3.2	從業人員應獲得管理階層表明沒有發生後續事件的書面陳述。

2401.4其他溝通

2401.4.1	從業人員應在定稿和發佈之前與有關的管理階層討論報告草案的內容，並在最終報告中包含管理階層對稽核發現、結論和建議的回饋。
2401.4.2	從業人員應告知負責治理的組織和主管部門（如適用）控制環境中存在的重大缺失和漏洞。此外，還應在報告中明確揭露，已經通報存在的缺失和漏洞。
2401.4.3	從業人員應與受查方管理階層溝通沒有達到嚴重情形，但也並非無關緊要的內部控制缺失。在這種情況下，從業人員應通知負責治理組織或主管部門，已經將這些內部控制缺失通報給了管理階層。
2401.4.4	從業人員應獲取管理階層的書面陳述，至少確認以下聲明： ● 管理階層負責建立和維護適當且有效的內部控制(包括所審查的營運活動和資訊系統的內部會計和管理控制系統)，以及確認查核目標範疇的所有監管法律、法規和規章，並確保這些法律、法規和規章均得到遵守。 ● 要求所有與稽核目標相關的資訊已提供給參與團隊，包括但不限於： ■ 記錄、相關資料、電子檔和報告。 ■ 政策和程序。 ■ 相關人員。 ■ 相關內部和外部資訊稽核、審查和評估的結果。 ■ 管理階層負責報告任何後續事件。 ■ 管理階層不知道與受查目標領域有關的任何欺詐或涉嫌欺詐行為、違規和非法行為，包括尚未揭露的管理階層和負責內部控制的員工。 ■ 管理階層不知道有任何詐欺或涉嫌詐欺的指控。包含從員工、客戶、承包商或其他尚未揭露的其他方所收到影響受查領域的任何欺詐或涉嫌欺詐行為、違規和非法行為的指控。 ■ 管理階層承認有責任設計和實施計畫及控制措施，以防止和發現欺詐、違規和非法行為。

2401.5其他注意事項

2401.5.1	資訊稽核和確保從業人員應： ● 獲得受查方提供的書面陳述，其中明確說明專案的關鍵領域、已出現的問題及其解決方案以及受查方作出的聲明。 ● 確定受查方的陳述已經過受查方簽字並署明日期，以表示承認其在業務方面的職責。 ● 如果未能獲得負責的受查方管理階層的書面陳述，可在工作底稿中紀錄獲得的口頭陳述。 ● 在工作底稿中記錄並保留在執行專案過程中所收到的任何書面或口頭的聲明。對於鑑證專案而言，從受查方獲取的聲明應當採用書面形式，以減少可能產生的誤解。 ● 在報告中描述重大或重要缺失，及其對實現稽核目標的影響。 ● 在報告定稿和發佈之前，與有關的管理階層討論報告草案的內容，並根據情況在最終報告中包含管理階層對稽核發現、結論和建議的回應。 ● 在告知負責治理組織和主管部門（如適用）之前，從業人員應與管理階層討論重大的缺失和漏洞。並應在報告中揭露，已經通報存在的重大缺失和漏洞。 ● 在最終報告中引用相關單獨的報告。 ● 從業人員應與受查方管理階層溝通沒有達到嚴重情形，但也並非無關緊要的內部控制缺失。在這種情況下，從業人員應通知負責治理組織或主管部門，已經將這些內部控制缺失通報給了管理階層。 ● 確認執行專案過程中採用的標準。根據情況傳達任何不符合標準的情況。

標準1401和準則2401與COBIT® 2019的關聯

COBIT 2019 管理目標	目的
EDM05 確保利害關係人參與	確保利害關係人支持資訊與科技(I&T)戰略和路線圖，與利害關係人保持及時有效的溝通，以及建立報告基礎以提高績效。識別待改善的領域，並確認I&T相關目標和策略與企業策略保持一致。
MEA01 管理績效與一致性監控	提供透明的績效和一致性，並推動目標的實現。
MEA02 管理內部控制系統	使主要的利害關係人瞭解內部控制制度是否充分，進而建立起對營運的信任與實現企業目標的信心，以及對剩餘風險的充分瞭解。

MEA03 管理外部要求合規	確保企業符合所有適用的外部要求。
MEA04 管理確保	促使組織設計和制定具效果與效率的確保機制，並採用公認的確保方法論，做為規劃，範圍界定，執行和後續追蹤提供指引。

報告標準1402：追蹤改善活動

聲明	1402.1資訊稽核和從事確保工作人員應監督並定期向負責治理和監督稽核職能部門的機構（例如：董事會或審計委員會）報告管理階層在查核發現和改善建議方面的進度。報告應包括以下結論：管理階層是否已規劃並及時採取適當的行動來解決所報告的查核發現和改善建議。
	1402.2應定期向審計委員會（如有）報告查核發現的總體改善執行情況。
	1402.3如果確定與查核發現相關的風險已被接受，並且超出企業的風險胃納，應與高階管理階層討論此風險的接受程度。如果接受風險（尤其是未能解決風險的情況下），應提請審計委員會（如有）或董事會的注意。

報告準則2402：追蹤改善活動

2402.1簡介 本準則的目的是指導從業人員監督管理階層是否及時對報告的建議和稽核結果採取適當的行動。本準則內容部分的結構在提供以下關鍵稽核和確保業務主題資訊：

2402.2後續追蹤流程

2402.3管理階層提議的行動

2402.4承擔不採取矯正措施的風險

2402.5後續追蹤程序

2402.6後續追蹤活動的時間和安排

2402.7後續追蹤活動的性質和範圍

2402.8延遲後續追蹤活動

2402.9後續追蹤回應的形式

2402.10從業人員對外部稽核建議的後續追蹤

2402.11後續追蹤活動的報告

2402.2後續追蹤流程

2402.2.1	後續追蹤活動是一個流程，從業人員通過該流程確定管理階層對其報告的觀察和建議（包括外部稽核師和其他人員的觀察和建議）所採取的行動的充分性、有效性和及時性。
2402.2.2	應建立一個後續追蹤流程，要求管理階層按承諾實施針對審查結果達成的共識，或要求高階管理階層承認延遲或不實施提議的行動或風險，以合理保證從業人員的每次審查都能為企業帶來最佳利益。

2402.3管理階層提議的行動

2402.3.1	在與受查方討論的過程中，從業人員應與受查方就稽核專案的結果和改善營運的矯正行動計畫（如需要）達成共識。
2402.3.2	從業人員應與管理階層討論，為實施或解決所報告的稽核建議事項而提出的行動建議。管理階層應向從業人員回饋提議的行動，從業人員應將其作為管理階層回饋記錄在最終報告中，並註明承諾的執行或行動日期。
2402.3.3	如果從業人員和受查方就提議的行動達成共識，從業人員應啟動追蹤改善活動的程序。

2402.4承擔不採取矯正措施的風險

2402.4.1	管理階層可能會因成本、矯正措施的複雜性或其他考慮因素而決定不矯正所報告的情況，並承擔相應風險。如果管理階層接受不矯正所報告情況帶來的風險，應將相關建議告知董事會或負責治理的組織。對管理階層接受此項風險的情況應紀錄在案，並由高階管理階層正式核准，之後傳達給負責治理的組織。
2402.4.2	如果從業人員認為受查方接受的殘餘風險水準對企業而言過高，應與資訊稽核和確保管理階層以及高階管理階層討論此項事宜。如果從業人員仍對於殘餘風險的決定存在分歧，應與高階管理階層一同提請董事會或負責治理組織決議。

2402.5後續追蹤程序

2402.5.1	應制定後續追蹤改善活動的程序，包括： ● 記錄管理階層應就約定的建議提出回應的期限。 ● 評估管理階層的回應。 ● 確認回應（如適用）。 ● 後續追蹤工作（如適用）。 ● 溝通程序，將未解決和不滿意的回應或行動，升級上報給適當層級的管理階層和負責治理的組織。 ● 在矯正措施被延遲或提議不實施的情況下，獲得管理階層對相關風險接受的過程。
2402.5.2	運用自動後續追蹤系統或資料庫可協助執行後續追蹤活動。
2402.5.3	在確定適當的後續追蹤程序時，應考慮的因素包括： ● 稽核發現和建議對所有關的資訊環境或資訊系統的重要性和影響。 ● 資訊環境發生的任何改變，可能影響稽核發現和建議的重要性和影響程度。 ● 矯正所報告情況的複雜性。 ● 矯正所報告情況所需的時間、成本和精力。 ● 未能矯正所報告的情況將造成的影響。
2402.5.4	應在稽核組織章程中定義後續追蹤行動、報告和升級的責任。

2402.6後續追蹤活動的行程和安排

2402.6.1	在決定後續追蹤活動的行程時，應考慮到稽核發現的重要性，以及不採取矯正措施將對企業策略和目標造成的影響。應運用專業判斷，確認與原始報告有關的後續追蹤活動的時間，並考量到一些因素，例如相關風險的性質或影響程度以及給企業帶來的成本。
2402.6.2	後續追蹤活動是資訊稽核流程不可或缺的一部分，應做好後續追蹤活動的排程，並計畫好執行每次審查的其他必要步驟。具體的後續追蹤活動及時間可能會受到困難的程度、涉及的風險和暴露、審查結果、需要實施矯正措施的時間以及其他因素的影響，可與管理階層協商決定。
2402.6.3	從業人員應在行動截止日期後立即追蹤與高風險問題有關的議定結果，並可以採取漸進的監督方式。
2402.6.4	雖然管理階層承諾的實施日期可能不一樣，仍可以定期（例如：每季一次）追蹤管理階層對不同稽核業務的所有回應的實施情況。另一種方法是根據與管理階層議定的截止日期，分別追蹤管理階層各個回應的實施情況。

2402.7後續追蹤活動的性質和範圍

2402.7.1	通常會給受查方設定一個期限，要求其在時間內提供針對建議所採取的行動的詳細資訊。
2402.7.2	如果可能，應由執行原始審查的從業人員來評估管理階層回應中有關這些行動的詳細說明。盡可能獲得所採取行動的稽核證據。
2402.7.3	如果管理階層提供了針對建議所採取行動的資訊，但從業人員對所提供的資訊或所採取的行動的有效性存有疑慮，則應在進行進一步的後續追蹤活動之前執行適當的測試或其他稽核程序，以確認真實的處境或狀況。
2402.7.4	作為後續追蹤活動的一部分，從業人員應評估尚未付諸實施的建議是否仍然相關或變得更加重要。從業人員可能決定特定的建議不適合繼續實施。出現這種情況可能是因為：應用系統發生變更、實施了補償性控制，或者業務目標或優先順序發生變化，從而有效消除或顯著降低了原始風險。同樣，資訊環境變化也可能導致先前觀察的重要性和影響程度，以及解決該問題的急迫性增加。
2402.7.5	可能需要安排後續追蹤專案，以確認關鍵或重要行動的實施情況。
2402.7.6	從業人員對不滿意管理階層回應或行動的意見，應傳達給適當的管理階層。

2402.8延遲後續追蹤活動

2402.8.1	從業人員負責安排後續追蹤活動，將其作為專案工作行程表的一部分。後續追蹤活動的安排應基於所涉及的風險、暴露、及實施矯正措施的難度和所需時間。
2402.8.2	在某些情況下，從業人員會在權衡業務觀察或建議的相對重要性後，根據管理階層的口頭或書面反應判斷已採取的行動是否充分。這種情況下，可以在針對相關系統或問題的下一次稽核活動中執行具體的後續追蹤活動確認。

2402.9後續追蹤回應的形式

2402.9.1	最有效的方式是以書面形式接收管理階層的後續追蹤回應，因為書面回應有助於強化和確認管理階層對後續追蹤行動及所取得執行的責任。此外，書面回應還可確保準確記錄行動、職責和當前狀態。 從業人員也可以接收並記錄口頭回應，並在可能的情況下獲得管理階層的核准。回應時可一併提供所採取行動或實施建議的證明。
2402.9.2	從業人員應要求管理階層定期更新其負責實施的議定行動的執行情形，以接收和評估管理階層的執行狀況， 尤其是與高風險問題和前置時間較長的矯正措施有關的執行情形。

2402.10從業人員對外部稽核建議的後續追蹤

2402.10.1	根據稽核業務的範圍和條款以及相關的資訊稽核標準，外部從業人員可依賴內部從業人員後續追蹤議定的建議。並可在稽核組織章程或專案委任書中確定有關後續追蹤的職責。

2402.11後續追蹤活動的報告

2402.11.1	應向適當層級的管理階層和負責治理的組織（例如：審計委員會）提交一份報告，根據稽核專案報告議定矯正措施的狀態（包括已議定但尚未付諸實施的建議）。
2402.11.2	如果在後續的稽核業務中，從業人員發現管理階層報告稱「已執行」的矯正措施實際上並未得到實施，應向適當的管理階層和治理機構報告。在適當情況下，從業人員應獲得最新的矯正措施計畫和計畫的實施日期。
2402.11.3	在議定的所有矯正措施得到實施後，可將所有已實施或已完成行動的詳細報告轉發給高階管理階層和負責治理的組織。

標準1402和準則2402與COBIT® 2019的關聯

COBIT 2019 管理目標	目的
EDM01 確保治理架構的設置和維護	提供與企業治理方法整合的一致方法。資訊與科技(I&T)相關決策應該與企業的策略和目標保持一致，並實現期望的價值。為此，應確保I&T相關流程得到有效和透明的監督，符合法律、合約和監管要求，以及滿足董事會成員的治理要求。
EDM02 確保效益交付	保證從資訊與科技(I&T)促成的措施、服務及資產中獲得最佳價值；以經濟效率的方式提供解決方案和服務；可靠準確地維護成本和效益資訊，從而具效果與效率地支援業務需求。
EDM03 確保風險最佳化	確保資訊與科技(I&T)相關企業風險不超過企業的風險偏好和風險容忍度，識別和管控I&T風險對企業價值的影響，以及最大程度地降低不合規的可能性。
MEA03 管理外部要求合規	確保企業符合所有適用的外部要求。
MEA04 管理確保	促使組織設計和制定具效果與效率的確保機制，並採用公認的確保方法論，做為規劃，範圍界定，執行和後續追蹤提供指引。

中文版致謝名單

ISACA 台灣分會葉奇鑫理事長

翻譯校稿：(依姓名筆畫排序)
周嘉明、莊盛祺、陳立群、陳怡如、陳政龍
張益紳、張碩毅、黃淙澤、黃誌緯、楊期荔

編輯排版：游恬欣

導讀文件：(依發表順序)
1.方建國 和通投資控股有限公司總稽核
2.高進光 上海商業儲蓄銀行稽核部資深經理
3.呂伯雲 財團法人棕櫚山莊基金會董事長/中央銀行前金檢處稽核
4.陳政龍 財團法人國家實驗研究院稽核室正工程師

附錄A：各標準間的關聯與準則

標準	相關標準	相關準則
1001 稽核組織章程	沒有與標準1001相關的標準	● 準則2001稽核組織章程
1002 組織獨立性	沒有與標準1002相關的標準	● 準則2002組織獨立性
1003 稽核的客觀性	沒有與標準1003相關的標準	● 準則2003稽核客觀性
1004 合理預期	沒有與標準1004相關的標準	● 準則2004合理預期
1005 應盡專業上的注意	沒有與標準1005相關的標準	● 準則2005應盡專業上的注意
1006 業務熟練	沒有與標準1006相關的標準	● 準則2006業務熟練
1007 聲明	沒有與標準1007相關的標準	● 準則2007聲明
1008 衡量標準	沒有與標準1008相關的標準	● 準則2008衡量標準
1201 規劃中的風險評估	沒有與標準1201相關的標準	● 準則2201規劃中的風險評估
1202 稽核安排	沒有與標準1202相關的標準	● 準則2202稽核安排
1203 稽核專案規劃	沒有與標準1203相關的標準	● 準則2203稽核專案規劃
1204 執行與監督	● 標準1005應盡專業上的注意 ● 標準1205證據 ● 標準1401報告	● 準則2204執行與監督 ● 準則2201規劃中的風險評估
1205 證據	沒有與標準1205相關的標準	● 準則2205證據
1206 使用其他專家的工作	沒有與標準1206相關的標準	● 準則2206使用其他專家的工作

標準	相關標準	相關準則
1207 違規和非法行為	● 標準1008衡量標準 ● 標準1201規劃中的風險評估 ● 標準1205證據	● 準則2206使用其他專家的工作 ● 準則2207違規和非法行為
1401 報告	沒有與標準1401相關的標準	● 準則2401報告
1402 追蹤改善活動	沒有與標準1402相關的標準	● 準則2402追蹤改善活動

附錄B：各準則的相關標準

準則	相關標準
2001稽核組織章程	● 1001稽核組織章程 ● 1002組織獨立性 ● 1003稽核的客觀性
2002組織獨立性	● 1001稽核組織章程 ● 1002組織獨立性 ● 1003稽核師的客觀性 ● 1004合理預期 ● 1006業務熟練
2003稽核的客觀性	● 1001稽核組織章程 ● 1002組織獨立性 ● 1003稽核的客觀性 ● 1005應盡專業上的注意
2004合理預期	● 1001稽核組織章程 ● 1004合理預期
2005應盡專業上的注意	● 1002組織獨立性 ● 1003稽核的客觀性 ● 1005應盡專業上的注意 ● 1006業務熟練 ● 1205證據
2006業務熟練	● 1005應盡專業上的注意 ● 1006業務熟練 ● 1203稽核專案規劃 ● 1204執行與監督
2007聲明	● 1007聲明 ● 1008衡量標準 ● 1206使用其他專家的工作 ● 1401報告
2008衡量標準	● 1007聲明 ● 1008衡量標準
2201規劃中的風險評估	● 1201規劃中的風險評估 ● 1203稽核專案規劃 ● 1204執行與監督 ● 1207違規和非法行為
2202稽核安排	● 1201規劃中的風險評估 ● 1203稽核專案規劃 ● 1204執行與監督 ● 1207違規和非法行為
2203稽核專案規劃	● 1201規劃中的風險評估 ● 1203稽核專案規劃 ● 1204執行與監督
2204執行與監督	● 1005應盡專業上的注意 ● 1006業務熟練 ● 1203稽核專案規劃 ● 1204執行與監督 ● 1205證據 ● 1401報告

本頁為空白頁

附錄C：術語和定義

A

適當的證據 (Appropriate evidence)—衡量證據品質的標準。

聲明 (Assertion)—由管理階層作出的有關查核事項的正式宣言或一系列宣言。

範圍說明：聲明應經查以包含關於查核事項或關於牽涉查核事項流程的特定屬性表列。

確保業務（Assurance engagement)—對證據的客觀檢查，目的在於為企業提供有關風險管理、控制或治理流程的評估。

範圍說明：實例可包括財務、業務執行、合規性和系統安全性方面的確保業務。

證明（Attestation)—資訊稽核師參與審查管理階層關於特定查核事項的聲明，或直接審查查核事項的一項業務。

稽核組織章程（Audit charter)—經治理機構核准的一種文件，用於定義內部稽核活動的目的、職權和責任。

範圍說明：該章程應當：

- 明確內部稽核職能部門在企業內部的定位
- 授權存取與IS稽核和確保業務的執行有關的紀錄、人員和實物財產
- 定義稽核職能部門的工作範圍

稽核業務（Audit engagement)—具體的稽核作業、任務或審查活動，如稽核、控制自我評估審查、舞弊行為的檢查或諮 詢。稽核業務可能包括為達到特定的相關目的而執行的多項任務或活動。

稽核計畫（Audit plan)— 1. 一種計畫，包含業務團隊成員執行的稽核程序的性質、時間和範圍，以便獲得充分、適當的稽核證據來形成意見。

範圍說明：計畫內容包括待稽核的領域、所規劃工作的類型、工作的高層次目標和範圍，以及預算、資源配置、排程、報告類型、報告目標受眾、工作的其他常規方面等主題。

2. 對需要在一定時段內執行的稽核工作的高層次描述。

稽核程序（Audit program)—為了完成稽核而執行的一組步驟(step-by-step)稽核流程和指令。

稽核風險（Audit risk)—根據稽核結果得出錯誤結論的風險。

範圍說明：稽核風險的三個組成部分如下：

- 控制風險
- 偵測風險
- 固有風險

稽核意見（Auditor's opinion)—IS稽核或確保專業人員表達的正式聲明，它描述稽核的範圍、用於產生報告的程序以及結論是否證實已達到稽核標準。

範圍說明：意見的類型如下：

- **無保留意見(Unqualified opinion)—** 註明沒有異常情況，或發現的異常情況均未累積成為顯著缺失(significant deficiency)
- **保留意見（Qualified opinion)**—註明累積成為顯著缺失的異常情況（但並非重大缺失(material weakness)）
- **否定意見(Adverse opinion)**—註明一種或多種顯著缺失累積成為重大缺失(material weakness)

C

控制風險（Control risk)—存在內部控制系統無法及時預防或偵測到重大錯誤的風險（請參閱固有風險）。

衡量標準（criteria)—用於衡量和表述查核事項、同時供IS稽核師參照評估查核事項的標準和基準。

範圍說明：衡量標準應該：

- **客觀（Objective)**—不存在偏差
- **可衡量(Measurable)**—提供一致的衡量結果
- **完整（Complete)**—包含得出結論所需的所有相關因素
- **相關（Relevant)**—切合主題相關事項

在簽證服務**(attestation engagement)**中，可參照基準指標評估管理階層有關查核事項的書面聲明。從業人員通過引述適用的衡量標準，形成有關查核事項的結論。

D

設計有效性（Design effectiveness)—如果公司的控制是按照具備有效執行控制所需許可權和能力的人員規定的方式運行，並且滿足公司的控制目標，可有效預防或檢測可能導致財務報表出現重大誤報的錯誤或欺詐，

則被認為是有效設計的控制。

請參閱上市公司會計監管委員會（PCAOB）稽核標準2201，“An Audit of Internal Control Over Financial Reporting That Is Integrated With an Audit of Financial Statements”，2007年11月15日，

第42節：

https://pcaobus.org/Standards/Auditing/Pages/AS2201.aspx

偵測風險（Detection risk）—IS稽核或確保專業人員的實質性程序無法檢測到單獨或與其他錯誤相結合的重大錯誤的風險。範圍說明：見稽核風險

F

追蹤改善活動（Follow-up activity）—確定管理階層是否已採取適當的矯正措施來解決缺失的活動。

I

損害（Impairment）—帶來漏洞或導致能力下降，影響完成稽核目標的狀況

範圍說明：對組織獨立性和個人客觀性的損害可包括個人利益衝突；範圍限制；對紀錄、人員、設備或設施的存取限制；以及資源限制（例如資金或人員配備）。

獨立性（Independence）—進行自我治理，以及避免威脅客觀性或出現客觀性受威脅的狀況。這種對客觀性的威脅必須在個別稽核師、參與、職能和組織層面進行管理。獨立性包括斯響獨立和外表獨立。

固有風險（Inherent risk）—未將已採取或可能會採取的管理措施（例如：實施控制）考慮在內的風險水準或風險曝險

完整性（Integrity）—防止不適當的資訊修改或損壞，包括確保資訊的不可否認性和真實性

違規（Irregularity）—違反既定的管理政策或法規要求。可能包括有意誤報或遺漏有關受查領域或整個企業的資訊，以及重大過失或無意的非法行為。

M

重大漏洞（Material weakness）—內部控制中的某個缺失或多個缺失的組合，存在合理的可能性導致無法及時預防或檢測出重大誤報。如果控制缺失導致無法合理保證實現控制目標，則控制漏洞被視為重大漏洞。如果某個漏洞被歸為重大漏洞，則意味著：

- 控制不到位及/或控制未投入使用及/或控制不足
- 有必要升級

重要性與IS稽核或確保專業人員可以接受的稽核風險水準之間存在反比關係，即重要性水準越高，稽核風險的可接受程度越低，反之亦然。

重要性（Materiality）—這是一個與資訊項的重要性相關的稽核概念，涉及到資訊項對受稽核實體的營運情況的影響。將企業看作一個整體時，表示特定事件在企業環境下的相對意義或重要性。

O

表現客觀（Objective in appearance）—避免出現這樣一種重大的事實和情形，即合理和知情的第三方可能根據具體的事實和情形推定，某個公司、稽核職能部門或某個稽核團隊成員的誠實性、客觀性或應盡專業上的注意已經受到損害。

思想客觀（Objective of mind）—以不曾受到損害專業判斷力的因素影響而表達結論的思想狀態，從而允許個人誠實行事並表現出客觀性和專業的懷疑態度。

客觀性（Objectivity）— 公正地作出判斷、表達觀點和提出建議的能力

運行有效性（Operating effectiveness）—如果控制按設計預期運行，並且執行人員具備有效執行控制所需的權威和能力，則該控制的運行被視為有效。

請參閱上市公司會計監管委員會（PCAOB）稽核標準2201，“AS 2201: An Audit of Internal Control Over Financial Reporting That Is Integrated With an Audit of Financial Statements”，2007年11月15日，https://pcaobus.org/Standards/Auditing/Pages/AS2201.aspx。

其他專家（Other expert）—企業內部或外部的其他專家可以指：

- 來自外部公司的資訊稽核師
- 管理顧問
- 最高管理階層或團隊指定的業務領域的專家

P

專業能力（Professional competence）—經過檢驗的能力水準，通常與相關專業機構認定的資格有關，並符合其產業準則和標準。

專業判斷（Professional judgment）—適當地運用相關知識和經驗作出明智的決定，形成針對IS稽核和確保業務的行動方案

專業懷疑(Professional Skepticism)— 一種態度，例如以質疑和批判性思維評估稽核證據。

範圍說明：資料來源：美國註冊會計師協會（AICPA) AU 230.07

R

合理保證（Reasonable assurance）— 一種未達預期程度的保證，但考慮到實施控制的成本和可能獲得的收益，這種保證被認為是充分的。

相關資訊（Relevant information）—與控制有關，讓評估員瞭解到有關基礎控制或控制元件運行情況的有用資訊。直接能夠確認控制運行情況的資訊是最相關的。間接涉及控制運行情況的資訊也可能相關，但相關性不如直接資訊。

範圍說明：參見COBIT 2019資訊品質目標

充分的資訊 (Reliable Information)—資訊是準確，可驗證且來自客觀來源的。

範圍說明：參見COBIT 2019資訊品質目標

陳述（Representation）—管理階層提供給專業人員的簽字聲明或口頭聲明，聲稱據其所知，當前或將來的事實（例如：流程、系統、程序、政策）處於或將處於某種狀態。

剩餘風險（Residual risk）—管理階層實施風險應對措施後剩餘的風險。

風險評估（Risk assessment）—用於識別和評估風險及其潛在影響的一種流程

範圍說明：風險評估用於識別為企業帶來高風險、漏洞或暴險的專案或領域，以便納入資訊系統年度稽核計畫。

風險評估也用於管理專案交付風險與專案效益風險。

S

重大缺失（Significant deficiency）—內部控制中的某個缺失或多個缺失的組合，嚴重性低於重大漏洞，但值得負責監督的人員密切關注。

範圍說明：重大漏洞指一個重大缺失或多個重大缺失的組合，導致預防或檢測到不良事件的可能性微乎其微。

查核事項（Subject matter）—IS稽核師報告和相關程序的特定資訊，例如內部控制的設計或運行情況，以及對隱私實務或標準或指定的法律法規（活動領域）的遵守情況。

證實性測試（Substantive testing）—在稽核期間獲取關於活動或交易的完整性、準確性或存在性的稽核證據。

充分的證據（Sufficient evidence）—稽核證據數量的衡量指標；支援稽核目標和範圍方面的所有重大問題。

範圍說明：參見「證據」

可靠資訊 (Sufficient information)—準確、可考證和來自客觀來源的資訊。

範圍說明：參見COBIT 2019資訊品質目標

合適的資訊（Suitable information）—相關（即適用於預期目的）、可靠（即準確、可核對總和來自客觀來源）和及時（即在適當的時限內產生和使用）的資訊。

範圍說明：參見COBIT 2019資訊品質目標

T

威脅（Threat）— 能夠對資產造成傷害的事物(例如：物體、物質、人）

範圍說明：意外事故的潛在原因（ISO/IEC 13335）

本頁為空白頁