資訊技術風險框架
Risk IT Framework

第2版

2nd Edition

ISACA

關於ISACA

ISACA®（www.isaca.org）50多年來，在科技領域中推動了最優秀的人才、專業知識和學習。ISACA提供個人知識、證書、教育和社群，以促進其職業發展並轉變組織，並協助企業培訓及建立優質團隊。ISACA是一個全球專業協會及學習型組織，致力在提升 145,000 名會員在資訊安全、治理、確保、風險和隱私等方面的專業知識，並藉由技術推動創新。目前在 188 個國家及地區發展，並於全球具有220多個分會。

免責聲明

ISACA 設計並創建了第2版的《資訊技術風險框架》，主要提供專業人士的教育資源。 ISACA 不聲稱使用此篇著作將確保結果成功。也不應被視為包含所有適當的資訊、流程及測試，或排除其他合理用於獲得相同結果的資訊、流程及測試。在確定任何特定資訊、流程及測試的適當性時，用於特定系統或資訊技術環境所呈現的特定情況，專業人員應將自行專業判斷。

權利保留

ISACA
1700 E. Golf Road, Suite 400
Schaumburg, IL 60173, USA
Phone: +1.847.660.5505
Fax: +1.847.253.1755
Contact us: https://support.isaca.org
Website: www.isaca.org

ISACA線上參與表單: 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/

資訊技術風險框架 第2版
ISBN 978-1-60420-820-7

致謝

ISACA 表彰:

首席開發人員
Lisa Young, CISA, CISM, CISSP, Axio, 美國

專家審查員
Luis Alberto Capua, CRISC, CISM, 阿根挺
Tom Conkle, CISSP, Optic Cyber Solutions, 美國
Andrew Foo, CISA, CRISC, CISM, CGEIT, CBCP, CCSK, CISSP, PMP, Dulwich College International, 中國
Sandra Fonseca, Ph.D., CISA, CRISC, CISM, CICA, Northcentral University, 美國
Yalcin Gerek, CISA, CRISC, CGEIT, COBIT 5 Trainer, DASA DevOps Coach, ISO 20000LI, ISO 27001LA, ITIL Expert, PRINCE2, Resilia Practitioner, TAC, 土耳其
Ahmad M. El Ghazouly, Ph.D., CISA, CRISC, CISM, PMI-ACP, AMBCI, BISL, PBA, PMP, PMI-RMP, TOGAF, PGESCo, 埃及
Demetri Gittens, CISA, CRISC, Central Bank of Trinidad and Tobago, Trinidad & Tobago
Ken Hendrie, CISA, CRISC, CISM, CGEIT, ISO27001 LI, ITIL, PRINCE2, IRAP, Cyconsol, 澳大利亞
John Hoffoss, CISA, CISSP, GCIH, CliftonLarsonAllen, 美國
Mike Hughes, CISA, CRISC, CGEIT, MIoD, Prism RA, 英國
John E. Jasinski, CISA, CRISC, CISM, CGEIT, CSX, COBIT 5 Assessor, COBIT and ITIL Accredited Instructor, AWS Practitioner, CCSK, Certified Scrum Master and Product Owner, ISO 20000, IT4IT, ITIL Expert, Lean IT, MOF, ServiceNow and RSA Archer Certified System Administrator, Six Sigma Blackbelt, TOGAF, 美國
Jack Jones, CISA, CRISC, CISM, CISSP, RiskLens, 美國
Linda Kostic, CISA, CISSP, Doctor of IT-Cybersecurity & Information Assurance, PRMIA Complete Course in Risk Management, George Washington University, Citi, 美國
Jerry M. Kathingo, CRISC, CISM, Hatari Security, 肯亞
Kamal Khan, CISA, CISSP, CITP, MBCS, 英國
Shruti S. Kulkarni, CISA, CRISC, CCSK, CISSP, ITIL v3, Interpublic Group, 英國
Jim Lipkis, Monoco Risk Analytics, Inc., 美國
Tony Martin-Vegue, CISM, CISSP, Netflix, 美國
Andre Pitkowski, CRISC, CGEIT, COBIT 5 Assessor, APIT Consultoria de Informatica Ltda,巴西
Eduardo Oscar Ritegno, CISA, CRISC, Banco Nación, 澳大利亞
Katsumi Sakagawa, CISA, CRISC, 日本
Gurvinder Pal Singh, CISA, CRISC, CISM, Qantas Airways, 澳大利亞
Darron Sun, CISA, CRISC, CISSP, CMA, CPA (Australia), CRMA, FIPA, Hong Kong Housing Society, 中國
Peter C. Tessin, CISA, CRISC, CISM, CGEIT, Discover Financial Services, 美國
Alok Tuteja, CRISC, CGEIT, CIA, CISSP, BRS Ventures, 阿拉伯聯合大公國
Ashish Vashishtha, CISA, CRISC, CISM, CIPT, CISSP, AWS Certified Cloud Practitioner, HITRUST CSF Practitioner, PROSCI Change Practitioner, AdventHealth, 美國
Greet Volders, CGEIT, Voquals N.V., 比利時
Jonathan Waldo, CISA, CRISC, ITIL 4 Foundation, CH Robinson, 美國
Larry G. Wlosinski, CISA, CRISC, CISM, CAP, CBCP, CCSP, CDP, CIPM, CISSP, ITIL v3, PMP, Coalfire-Federal, 美國
Prometheus Yang, CISA, CRISC, CISM, CFE, Standard Chartered Bank, 香港
Dušan Žikić, CISA, CRISC, CISM, CSX-P, Cybersecurity Audit, Cybersecurity Fundamentals, COBIT 5 Foundation, COBIT 2019 Foundation, COBIT 2019 Design and Implementation, ITIL (2011) Foundation, ITIL 4 Foundation, IBM Data Science,NIS Gazprom Neft, 塞爾維亞

致謝 (續)

風險資訊專案小組
Steven Babb, CRISC, CGEIT, ITIL, MUFG Investor Services, 英國
Urs Fischer, CISA, CRISC, CPA (Swiss), UBS Business Solutions AG, 瑞士
Jack Freund, Ph.D., CISA, CRISC, CISM, CISSP, RiskLens, 美國
Apolonio Garcia, CRISC, Open FAIR, HealthGuard, 美國
Jimmy Heschl, CISA, CISM, CGEIT, Red Bull, 奧地利
Gladys Rouissi, CISM, CRISC, ANC Wealth, 澳大利亞
James C. Samans, CISA, CRISC, CISM, CBCP, CISSP-ISSEP, CPP, PMP, American Institutes for Research, 美國
Ekta Singh-Bushell, CISA, CGEIT, CISSP, CPA, Datatec, 美國
Dirk Steuperaert, CISA, CRISC, CGEIT, IT In Balance, 比利時
Evan Wheeler, CRISC, IASO, Edelman Financial Engines, 美國

董事會
Brennan P. Baybeck, CISA, CRISC, CISM, CISSP, Vice President and Chief Information Security Officer for Customer Services, Oracle Corporation, 美國, Chair
Rolf von Roessing, CISA, CISM, CGEIT, CISSP, FBCI, FORFA Consulting AG, 瑞士, Vice-Chair Tracey
Dedrick, Former Chief Risk Officer with Hudson City Bancorp, 美國
Pam Nigro, CISA, CRISC, CGEIT, CRMA, Health Care Service Corporation, 美國
R.V. Raghu, CISA, CRISC, Versatilist Consulting India Pvt. Ltd., 印度
Gabriela Reynaga, CISA, CRISC, COBIT 5 Foundation, GRCP, Holistics GRC, 墨西哥
Gregory Touhill, CISM, CISSP, AppGate Federal Group, 美國
Asaf Weisberg, CISA, CRISC, CISM, CGEIT, introSight Ltd., 以色列
Rob Clyde, CISM, Board Director, Titus and Executive Chair, White Cloud Security, 美國, ISACA Board Chair, 2018-2019
Chris K. Dimitriadis, Ph.D., CISA, CRISC, CISM, Group Chief Executive Officer, INTRALOT, 希臘, ISACA Board Chair, 2015-2017
Greg Grocholski, CISA, Saudi Basic Industries Corporation, 美國, ISACA Board Chair, 2012-2013
David Samuelson, Chief Executive Officer, ISACA, 美國

目錄

圖目錄

本頁留空

摘要

風險的概念(在考慮資訊技術和資通安全的背景下)引用了廣泛的詞彙，包含威脅與脆弱性、風險胃納、容忍度、影響、優先順序與回應，及對於風險治理與管理與資訊技術評估等重要的相關術語。

資訊技術風險的從業人員需要對這些術語進行完整及清晰的定義，以便建立可供整個企業與合作夥伴所使用的通用語言。ISACA 的《資訊技術風險框架》專注在資訊技術(IT)和資通安全(IS)的背景下發展風險語彙，促進企業風險在多方面的公開思辨，建立優化風險、機會、安全及商業價值的指引準則和實務，並幫助從業人員建立關於企業所有層級之資訊技術風險決策的共識。《資訊技術風險框架》第2版及其對應書籍，資訊技術風險從業人員指引第2版，促進資訊技術風險從業人員之間的協作，將風險管理科學引入企業資訊及技術 (I&T)中。

風險管理專業並不是現代才發明，風險管理研究起源於 1600 年代，當時的數學家帕斯卡(Blaise Pascal)和費馬(Pierre de Fermat)對於機會遊戲信件的往來，他們的聯繫被認為啟動了現代機率理論[1] – 最終促成了現代定量風險分析。然而在當今資訊技術、資訊安全、資通安全和網路物理系統[2] 的背景下，風險管理原則並未得到廣泛理解 – 尤其是管理原則的量化方法，這將大幅提高在商業和財務方面對資訊與技術(I&T)風險的認知。

至於在資通風險的部分，企業的關鍵利害關係人（包括董事會成員和高階管理人）可能不太瞭解，他們依靠技術來實現策略和營運目標，藉此應對風險管理的責任。儘管資訊與技術(I&T)企業在營運的生態系統中越來越主流，若是對資訊與技術(I&T)相關風險沒有清楚的瞭解，高階管理階層就無法參考框架來確定優先順序並進行管理。

風險是定義為事件發生的可能性及其影響的組合，提供了獲益的機會（提升）或成功的危險（下降）。事實上，風險與機會並存，為了向利害關係人提供商業價值，企業必須參與各種活動及實施各項倡議（機會），所有的活動及倡議（機會）都帶有一定程度的不確定性，因此也存在風險。管理風險與機會是企業成功的關鍵策略活動。

《資訊技術風險框架》第2版涉及整體資訊與技術(I&T)風險，並使用及依靠資訊和通信技術 (ICT)[3] 、營運技術 (OT)[4] 、網路或物聯網（IOT)[5] 、電子數據與數位化或電子通訊等相關的業務或任務風險。《資訊技術風險框架》建立一個核心原則上，即透過有效的企業治理和管理所有類型的資訊與技術(I&T)相關風險來服務利害關係人並提高企業價值的核心。在本文中，資訊安全、資訊確保和資通安全被視為資訊與技術(I&T)相關風險的子領域。

本框架展現並詳細描述整個企業資訊技術風險的幾個關鍵指引原則:

- 將資訊與技術(I&T)相關風險的管理與業務及任務目標進行關聯。
- 如果企業風險管理已在企業中運作，儘可能將資訊與技術(I&T)相關業務或任務風險的管理與企業風險管理(ERM)保持一致。

[1] 美國物理學會, “July 1654: Pascal’s Letters to Fermat on the ‘Problem of Points’,” *APS News*, vol. 18, no. 7, July 2009, *www.aps.org/publications/apsnews/200907/physicshistory.cfm*
[2] 美國國家標準與技術研究院 (NIST), “資訊物理系統,” *www.nist.gov/el/cyber-physical-systems*
[3] NIST, “資訊和通信技術 (ICT),” 電腦安全資源中心, *https://csrc.nist.gov/glossary/ term/information_and_communications_technology*
[4] NIST, “營運科技 (OT), ” 電腦安全資源中心, *https://csrc.nist.gov/glossary/term/Operational-technology*
[5] Voas, J.; “物聯網’,” NIST SP 800-183, July 2016, *https://csrc.nist.gov/publications/detail/sp/800-183/final*

- 平衡管理資訊與技術(I&T)相關風險與其他的企業風險之成本和利益。
- 促進有關資訊與技術(I&T)相關風險的道德和開放交流。
- 建立高層管理規則，同時定義和履行個人責任，在可接受和明確定義的容忍度範圍內運作。
- 將資訊技術風險實務整合到日常活動和流程中，尤其在本質上不利於資訊技術風險方法論的不連續、特定時間點或是偶爾付出的日常活動和流程中。
- 採用標準、可重複且與組織策略一致的方法。

資訊與技術(I&T)相關風險是企業整體風險範圍內的一部分（圖 1.1）。其他類型的風險包括策略風險、環境風險、市場風險、信用風險、營運風險和合規風險等。某些企業將資訊與技術(I&T)相關的風險歸類為營運風險，例如：在巴塞爾資本協定II的框架[6] 中所定義的金融行業風險。然而，所有類型的風險，甚至是策略風險都可能包含資訊與技術(I&T)風險的元素，尤其是資訊與技術(I&T)構成組織新業務計畫的核心。

同樣的關聯也適用於信用風險，例如：不良的資通風險管理可能會導致安全漏洞或合規性懲罰，並降低信用評級[7]。

《資訊技術風險框架》第2版解釋了與資訊與技術(I&T)相關的風險，並使從業人員能夠：

- 在企業層面廣泛識別和解決與資訊與技術(I&T)相關的風險，不僅僅是在資訊技術部門之內。
- 將傳統資訊技術風險、資訊安全和資通風險的管理整合到整個企業風險管理的流程中。
- 促進企業層面全面、整體、風險意識的決策。
- 每當資訊與技術(I&T)相關的風險超出容忍度時，指引企業如何應對風險。

《資訊技術風險框架》第2版是 ISACA 廣泛的資訊與技術(I&T)相關風險和治理產品組合的一部分，並提供了一個完整且獨立的框架，可與 COBIT® 緊密結合，並結合許多相同的原則以達成目標。其對應書籍《資訊技術風險從業人員指引》第2版也與 COBIT 保持一致。兩份出版物都假設資訊技術風險從業人員瞭解 COBIT 框架的基本概念[8]。

[6] 巴塞爾銀行監管委員會，巴爾賽協議 *II:* 資本計量和資本標準的國際趨同*:* 修訂框架, 10 June 2004, *https://www.bis.org/publ/bcbs107.htm*

[7] O'Flaherty, K.; "Equifax 成為首家因網路攻擊而期望被下修的公司," Forbes, 28 May 2019, *https://www.forbes.com/sites/kateoflahertyuk/2019/05/28/equifax-becomes-first-firm-to-see-its-outlook-downgraded-due-to-a-cyber-attack/#209549335671*

[8] 如需更多指引，見 ISACA,風險管理入門, USA, 2018, *https://www.isaca.org/bookstore/bookstore-wht_papers- digital/whpgsr*; and ISACA, *Risk IT Practitioner Guide*, 2nd Edition, USA, 2020 (forthcoming). Both publications adopt COBIT methodologies and include a range of practical examples.

第一章
介紹資訊技術風險框架

1.1 資訊技術風險的必要性

資訊與技術(I&T)相關的風險是數位化商務的生存條件（無論企業是否確定來源或認識到其潛在後果）。隨著企業技術整合及利用資訊創造價值，尤其是資通威脅（一種特殊資訊與技術(I&T)相關的風險）使其曝露風險的程度增加。如果不加以識別及適當管理，資通威脅可能會產生破壞性影響。

在此前題下，《資訊技術風險框架》提供了一種結構化及系統化的方法，使企業能夠：

- 識別整體企業中現有及新興的風險。
- 發展適當的營運能力，確保業務程序在不利事件中能持續運作。
- 充分利用在符合法規或內部控制系統方面的投資，並優化資訊與技術(I&T)相關的風險。
- 識別超出技術控制及資訊技術相關工具的技術範圍，並將其資訊與技術(I&T)相關的風險納入企業風險管理(ERM)方案。
- 提高二方面認知的平衡，一是在技術及外部夥伴利益間的平衡，另一部分則是針對認識網路威脅的潛在影響、內部控制失靈及供應商、供貨商和製造商所帶來的風險。
- 促進整個企業的風險意識、當責及負責。
- 在業務範圍內確定資訊與技術(I&T)相關的風險框架，以瞭解企業價值方面的整體曝險。
- 集中內、外部風險管理資源，實現企業目標最大化。

資訊技術風險應與企業主要的風險管理框架校準一致，包括 COSO 風險管理框架[9]及 ISO 31000 風險管理[10]；然而，風險管理框架的實施並不是採用《資訊技術風險框架》的先決條件。採用《資訊技術風險框架》的企業通常在其基本風險流程中應用許多共同的企業風險管理原則(ERM principles)，無論所管理的風險類型如何。

如果企業已經採取某種形式的風險管理，那麼重要的則是在現有企業風險管理方案的基礎上持續建立，以便：

- 利用現有的概念、術語及共識，提升利害關係人的支持及採用。
- 節省培訓與實施所耗費的時間及金錢。
- 避免因更換新的資訊技術、資通安全或資通風險管理框架或術語而出現無法持續的情況。

當識別資訊與技術(I&T)相關的風險有可能影響到整體的業務或任務時(而影響不僅僅是部分)植基於現有企業風險管理計畫的基礎上發展將更為重要。

《資訊技術風險框架》在傳統通用的風險管理框架（如 COSO ERM 和 ISO 31000）與資通安全（如 NIST 資通安全框架[11]）、資訊安全（如 ISO 27005[12]）及專案管理（如 PMBOK®[13]）等特定領域框架間建構了橋樑。《資訊技術風險框架》提供資訊與技術(I&T)相關風險的點對點及綜合的觀點，並徹底涵蓋了風險管理，從高層的文化，到一線從業人員及操作問題。

[9] COSO委員會 (COSO), “企業風險管理指引,” *https://www.coso.org/Pages/erm.aspx*
[10] 國際標準組織 (ISO®), *ISO 31000 Risk Management*, 2018, *www.iso.org/iso-31000-risk-management.html*
[11] NIST, 改善關鍵基礎設施資通安全的框架, Version 1.1, April 2018, *https://www.nist.gov/cyberframework/framework*
[12] ISO, *ISO/IEC 27005:2018* 資訊技術y — 安全技術 —資訊安全風險管理, July 2018, *https://www.iso.org/standard/75281.html*
[13] 專案管理研究所, “PMBOK® Guide and Standards,” *www.pmi.org/pmbok-guide-standards*

應用在《資訊技術風險框架》中所描述的資訊與技術(I&T)相關的風險管理做法，可以為業務及任務帶來好處。減少業務意外與中斷、提高資訊品質和可靠性、增強利害關係人的信心、減少監管單位的擔憂以及支持新業務初期的創新應用。

總體言之，《資訊技術風險框架》能使企業瞭解和管理所遭受、使用或依賴的資訊和通訊技術、電子數據及數位或電子通訊有關的危險、傷害或損失。

1.2 定義及術語

《資訊技術風險框架》第 2 版使用以下術語來描述全景、流程和活動：

- **企業** — 一群為共同目的而工作的個人，通常是在商業組織的範圍內，如：公司、合夥企業、有限公司、政府或公家機構、慈善機構、非營利機構或信託機構。
- **組織** — 企業中相互關聯組成部分的結構或安排，由特定的範圍來定義。
- **業務或任務** — 組織存在的策略目的。在資訊技術風險的範圍內，企業通常會設定策略目標，例如：提供產品或服務，達到銷售目標並創造收入。任務驅動的組織目的可能與一般企業類似，但通常是為了滿足政府、軍事或非營利性目標而運作。
- **治理** — 確保以下方面的框架和系統:
  - 對利害關係人的需求、條件和選擇進行評估，以確定平衡且一致的企業目標。
  - 確定策略方向，透過適當與及時的決策，確定目標的優先順序並給予支持。
- **風險** — 事件發生的可能性及影響的組合。
- **資訊安全** — 保護資訊不洩露給未經授權的使用者（確保機密性）、不被不當修改（確保完整性），及除非需要否則不被存取（確保可用性）的企業紀律。
- **資通安全** — 透過應對網路資訊系統處理、儲存和傳輸的資訊所面臨的威脅來保護資訊資產的企業紀律。
- **資通風險** — 因使用或依賴資訊與通訊技術、電子數據及數位或電子通訊而曝露的危險、傷害或損失。通常，資通風險的發生涉及未經授權的存取或未經授權的使用資訊與通訊技術。

在《資訊技術風險框架》第2版中，「資訊技術」一詞廣義上包括所有資訊和相關技術、數位及電子生態系統，並包括資訊安全、資通安全及相關學科與流程。本框架中的資訊技術一詞更狹義地指提供技術支援的內部或外部功能單位或部門。

《資訊技術風險框架》主要的應用為通用行業標準，當中經過驗證、普遍接受的概念，有時還發展了其他資訊與技術(I&T)風險管理框架中的關鍵概念。然而，《資訊技術風險框架》的術語可能與其他準則的術語不同。

對於熟悉其他框架或者可能已經實施了其他標準的從業人員來說，《資訊技術風險框架》第2版和《資訊技術風險從業人員指引》第2版整合並擴展了常見的行業風險管理概念和術語，並將《資訊技術風險框架》中的關鍵結構與其他標準中的邏輯對應關係進行了對照。

1.3 資訊技術風險框架的目的

在許多企業中，資訊與技術(I&T)已成為日常作業的主軸，並日漸成為整體業務價值的核心。因此，應像對待任何其他關鍵業務風險一樣對待資訊與技術(I&T)相關的風險，例如：策略風險、環境風險、市場風險、信用風險、營運及合規風險，所有這些風險都屬於最高層次的風險，使企業未能實現其策略目標。

在一些企業中，資訊技術相關的風險、資訊安全風險及資通風險被視為營運風險的子類別。雖然其他類型的關鍵風險早已被納入企業決策過程，但管理人員仍傾向於將資訊和技術相關的風險歸入董事會以外的技術專家領域。資訊與技術(I&T)相關的風險遍及整個組織，因此需要採取綜合性的風險管理做法，而不是採用單一、局部或臨時的處理辦法。

《資訊技術風險框架》解釋了與資訊與技術(I&T)相關的風險，並讓使用者能夠:

- 識別資訊與技術(I&T)相關並超出狹窄的技術判斷範圍的風險，因此需要整體及企業層面的考慮。
- 將資訊與技術(I&T)相關的風險管理整合到整個企業風險管理流程中。
- 在整體企業風險容忍度的全景下評估資訊與技術(I&T)風險及應對辦法。

1.4 背景

資訊與技術(I&T)風險往往出現在相互關聯環境中的關鍵點上，包括網路的存取點。然而，這些環境對業務和任務相當重要，它們往往將帶來最嚴重的資訊安全和資通安全風險。

一般來說，資訊安全的目的是透過維護資訊的機密性、完整性與可用性（CIA）及保護資訊所在的資產來保護資訊。資訊安全的其他因素包括不可否認性、隱私性和敏感性。時至今日，資通安全風險經常滲透到其他類型的風險中，因為科技往往是實現資通風險的媒介或途徑。

企業在制定業務或經營策略時，往往明確地決定可接受的風險程度以實現其目標。在 COBIT 中，這種做法稱為最佳化，即把風險維持在風險胃納的容忍範圍內，這應該是風險管理的目標。《資訊技術風險框架》主要關注的是降低已發生風險對業務的影響，或降低風險發生的可能性超過可接受水準的資源及活動。該框架大致上促進了對資訊技術有關的所有風險管理；但是，作為相關的子類別，可以使用資訊安全及資通風險的例子來顯示系統及程序上的相互關聯性。

《資訊技術風險框架》主要關注的是降低已發生風險對業務的影響，或降低風險發生的可能性超過可接受水準的資源和活動。

《資訊技術風險框架》不是一個標準，而是一個框架，並參考了 COBIT 治理和管理目標與做法。企業應根據特定行業及業務背景以調整框架中的指引與指示。

1.5 目標讀者及利害關係人

《資訊技術風險框架》第2版是為廣大讀者所編寫的，因為風險管理在任何企業都是一個全方位的策略需求。《資訊技術風險框架》的目標讀者包括：

- 在企業層面設定策略方向和監控風險的高階管理階層及董事會成員。
- 負責日常營運決策和將風險管理流程納入日常工作的資訊技術、營運技術和業務部門的管理人員。
- 需要具體的資訊與技術(I&T)、資訊安全、資通安全或資通風險指引的風險管理專業人士。
- 外部利害關係人，如：客戶、監管者、供應商及合作夥伴。

資訊與技術(I&T)相關的風險涉及企業的整體風險範圍，如圖1.1。其他類型的企業風險包括策略風險、環境風險、市場風險、信用風險、營運風險及合規風險。在金融業，根據《巴塞爾資本協定II》[14] 框架的定義，資訊與技術(I&T)相關的風險往往被視為營運風險中的一個子類型。然而，策略風險可以包含資訊與技術(I&T)相關的風險，特別是當資訊與技術(I&T)是新業務建立的基礎時。這一點同樣適用於信用風險。不良的資通風險管理做法可能導致信用等級降低[15] 。《資訊技術風險框架》將資訊與技術(I&T)相關的風險視為一個連續體，與其他主要類別的風險完全共存，而不是狹隘的子類別風險，在等級上歸屬於一個或另一個上級類別。在概念上，將資訊與技術(I&T)相關的風險歸屬於另一類風險，或將其局限於企業的一個部門或分部，可能會降低風險意識與評鑑，並導致風險判斷不當或對其真正的範圍產生誤解。

圖 1.1 — 資訊技術相關的風險相對於其他主要風險類別的範圍

[14] 同上 Basel Committee on Banking Supervision
[15] 同上 O'Flaherty

第二章

資訊技術風險框架原則

2.1 介紹

《資訊技術風險框架》第2版為有效管理資訊技術有關的風險制定了指引原則，如：與使用或依賴資訊和通訊技術、電子數據以及數位電子通訊有關的業務風險。其原則以普遍接受的企業風險管理原則為基礎，並應用於資訊和通訊領域。《資訊技術風險框架》目的在幫助企業於實踐中應用這些原則。

資訊技術、資通安全和資訊安全超越了任何單一且獨立的風險來源或類別；它們涉及無數相互關聯的條件，並反映出許多具體與獨特的特徵。同時可能涉及專業技術、威脅行為者、人為錯誤、攻擊媒介、控制失敗和軟體漏洞等。特別需要注意的是，資通風險和資訊安全風險並不只限於技術，許多引人注目的風險事件都是始於人為的錯誤。

來自資訊技術、資訊安全和資通安全的風險並不是唯一值得關注資訊與技術(I&T) 的相關風險。其他業務風險類型（包括流程及業務或景氣循環中斷）也需要加以管理。任何危及組織業務或任務的資訊技術有關風險都應從企業的整體目標角度進行管理，因此屬於《資訊技術風險框架》的指引原則範圍，如圖2.1：

- 資訊與技術(I&T)相關的風險管理與業務或任務目標進行連結。
- 在可能的情況下，將資訊與技術(I&T)相關的業務或任務風險管理與組織風險管理進行整合。
- 平衡管理資訊與技術(I&T)相關風險的成本與收益。
- 促進所有資訊與技術(I&T)相關風險的道德並開放交流。
- 在高層確立組織特性，同時劃分及執行個人責任制，並在可接受的範圍內運作與明確定義的風險容忍度。
- 在日常活動中採用標準化、可重複和符合策略的一致方法。

圖 2.1 — 風險管理原則

來源: ISACA, *COBIT® 5 for Risk*, USA, 2013, fig. 15, *https://www.isaca.org/bookstore/cobit-5/wcb5rk*

2.2 連結企業的業務或任務

對資訊與技術(I&T)相關風險進行有效的企業治理並經常連結至業務或任務目標：

- 包括資通風險在內的資訊與技術(I&T)相關風險作為一種業務風險，而不是作為一種單獨的風險來處理，且管理方法是全面且跨職能的。
- 資訊與技術(I&T)相關風險的治理有助於業務或任務成果。資訊與技術(I&T)業務的目標實現，任何相關的風險都以其對業務目標或策略可能產生的影響和可能性來表示。資訊與技術(I&T)相關的風險分析考慮到業務流程與支持資訊與技術(I&T)資產、應用程式或基礎設施及第三方依賴性之間的關聯。
- 資訊與技術相關的風險管理，包括資訊安全和資通安全方面的做法，都是為了推動業務或任務，而不是限制或抑制業務或任務。

2.3 遵循企業風險管理

有效進行資訊與技術(I&T)相關風險的企業治理，並使其管理與整體企業風險管理一致：

- 業務或任務目標及風險胃納定義明確。
- 企業決策過程考慮到所有資訊與技術(I&T)相關風險的潛在後果與機會。
- 定義及說明風險胃納反映了企業風險管理政策和高層的管理風格，同時影響企業文化。
- 與資訊與技術(I&T)相關的風險評鑑在整個企業中得到協調和整合，包括：跨企業的資訊安全和資通安全。

2.4 平衡成本與收益

對資訊與技術(I&T)相關風險進行有效的企業治理，並平衡其成本與效益：

- 根據風險胃納及風險容忍度，確定與資訊與技術(I&T)相關風險的優先順序並加以處理。
- 根據成本與效益分析、替代方案分析及對企業目標具有潛在影響風險的優先順序，實施風險應對措施。
- 利用現有的控制措施和風險應對行動，盡可能有效的處理風險。

2.5 建立高層的管理風格及責任心

有效管理資訊與技術(I&T)相關的風險，促進倫理及開放交流：

- 公開、準確、及時和透明的交流及資訊與技術(I&T)相關的風險資訊，並為風險有關的決擇提供資訊。
- 風險文化和風險管理的方法應納入整體企業中。
- 技術研究結果轉換為相關且可理解的商業及財務術語。
- 向利害關係人、政府和監管機構、客戶以及公眾公開報告有關事件及相關應對措施的資訊。

2.6 建立高層的管理風格及責任心

有效管理資訊與技術(I&T)相關的風險，可以從高層建立經營的風格，同時定義與執行在可接受且明確規定的容忍範圍內運作個人的職責：

- 企業擁有者、董事會和高階管理階層應參與風險管理過程。
- 有明確的職責和風險所有權的分配。
- 風險假設有適當商業領袖的理解與支持，並在風險胃納、容忍度、組織文化、政策和執行準則文件中有明確的說明。
- 風險管理績效可以進行衡量，同時納入負責人員與其職責的績效管理中。
- 提倡風險意識文化和個人責任。
- 在組織中，由授權人員依據風險容忍度，在正確的層級上作出風險意識的決策。
- 風險管理做法應適當的列為優先事項並納入企業決策。

2.7 遵循組織策略使用一致的方法

有效管理資訊與技術(I&T)風險是日常活動的一部分且有助於不斷改進：

- 風險的動態特性要求企業進行提前考慮並做好準備以應對變化：
  - 在組織本身(合併及收購)。
  - 在風險方面。
  - 在適用的法律及條例中。
  - 在資訊與技術(I&T)方面的發展。
  - 在整體行業中。
- 風險評鑑方法、衡量範圍和標準在整體企業中是保持一致的，尤其適用於：
  - 識別關鍵流程和相關風險。
  - 識別對目標的影響。
  - 識別觸發的關鍵，以指示何時風險會超出承受能力，或何時需要更新框架或框架中的元件等。
  - 監視和測試執行中的控制措施。
  - 防止風險發生的措施。
  - 風險應對（如果發生不良事件）。
  - 在定量風險測量過程中識別並盡可能減少風險評鑑者的偏見。

本頁留空

第三章

資訊技術風險框架組件與符合 COBIT 框架

3.1 介紹

《資訊技術風險框架》將根據第三章所列出的原則，在後續章節中進一步的發展。本章將討論:

- 《資訊技術風險框架》的組成。
- 使 COBIT 與《資訊技術風險框架》保持校準。
- 獨立於 COBIT 的《資訊技術風險框架》應用。

圖 3.1 說明了資訊與技術(I&T)相關的風險管理原則與 COBIT 目標 EDM03 確保風險正規化和 APO12 管理風險的一致性。

圖3.1—資訊與技術(I&T)相關風險的管理原則與COBIT目標EDM03和APO12一致

3.2 資訊技術風險框架組成

《資訊技術風險框架》基於一套有效管理資訊與技術(I&T)相關風險的指引原則，並補充了 COBIT 框架，以用於治理和管理業務驅動型資訊與技術(I&T)解決方案和服務的綜合框架。《資訊技術風險框架》使企業能夠識別、治理與管理資訊與技術(I&T)相關的風險。

各種不同的框架、技術及方法可以幫助企業建立和維護有效的風險管理能力，無論是對風險進行整體管理，如：ERM 或是局部進行單一類型或類別管理，如：違規、資通安全或資訊安全風險，風險管理的基本原則均適用。

3.3 使 COBIT 與資訊技術風險框架保持一致

COBIT 治理和管理目標與實踐可幫助管理企業內部或外部的資訊與技術(I&T)流程、活動和服務，並幫助企業制定應對資訊與技術(I&T)相關風險的整體框架。

企業內部事件和活動可包括營運或網路事件、計畫中止、業務或技術策略改變、企業擴展及合併或收購。外部事件可能包括市場條件的變化、競爭、技術進步、影響資訊與技術(I&T)的法規及這些事件可能造成的資通威脅。所有這些因素都會帶來風險或機會；組織應識別和評鑑這些因素，並制定應對措施。風險層面及如何管理風險是《資訊技術風險框架》的主要項目。當識別出資訊與技術(I&T)驅動業務變革的機會時，COBIT 框架，特別是項目 EDM03 確保風險正規化和 APO12 管理風險可以規定能夠達成企業目標的做法和活動。風險管理包括為追求企業策略目標而創造及維護組織價值活動和文化的總和。風險管理不是單一職能或部門，也不僅限於建立及監控內部控制。

3.4 獨立於 COBIT 的資訊技術風險框架的應用

在典型的企業中，每天都會進行資訊與技術(I&T)相關的活動，這些活動按照資訊與技術(I&T)流程進行部署。事件將不間斷地發生，企業必須作出重要的技術抉擇，對營運事故必須進行修復，必須解決軟體問題與建置應用程式。在這些事件中都隱含著風險及機會。

風險反映出事件發生的可能性及其對企業影響的組合。因此，風險反映了獲益的機會及對成功的威脅。為了向利害關係人提供商業價值，企業必須參與各種活動和初步計畫（機會）。所有這些計畫和活動都具有一定程度的不確定性，因此也具有風險。管理風險和機會是企業成功的關鍵策略活動。

風險反映出事件發生的可能性及其對企業影響的組合。因此，風險反映了獲益的機會及對成功的威脅。

資訊與技術(I&T)在風險與機會的關係中可以扮演不同的角色，既可以作為價值推動者，也可以作為價值障礙：

- **價值推動者** — 新的業務計畫幾乎總是取決於資訊與技術(I&T)的參與。資訊與技術(I&T)可以擔任以下職務：
  - 支持成功的資訊與技術(I&T)專案，支持新計畫，從而創造價值。
  - 以創新方式應用新技術，實施新商業計畫並創造價值。
  - 保護資產和資源免受可能影響產品和服務交付的威脅。

- **價值障礙** — 與資訊與技術(I&T)相關的活動和過程可能會帶來一系列負面影響：
  - 支持資訊與技術(I&T)的業務專案或投資通常無法實現預期的結果，因此無法實現價值。
  - 企業可能無法發現或掌握因新技術而產生的商業機會。
  - 資訊與技術(I&T)可能無法防止或預測到可能導致的輕度甚至嚴重營運中斷狀況或網路威脅，例如：短期或長期的系統或網路中斷、資訊的偷竊，揭露及損壞。

企業在實踐中如何風險回應呢？理想情況下，企業在評估和監視所有資訊與技術(I&T)計畫時，不僅需要資訊技術部門或支持部門的參與，將風險意識和機會意識的思想都加入其中。例如：當提議針對基礎建設進行重大投資時，企業在決策時應考慮以下因素：

- 與投資相關的風險，如：專案風險。
- 新計畫在降低風險方面的好處。
- 新的資訊與技術(I&T)基礎架構帶來的商業利益。
- 新資訊與技術(I&T)資產相關的機會。

當出現新技術時，企業確定是否採用該技術時，應考慮以下標準：

- 採用該技術的影響，如：支持性、可靠性及易於整合。
- 使用新技術帶來的風險，如：安全性及可靠性。
- 不採用新技術的後果，如：過時及落後於競爭對手。
- 新技術的商業利益，如：對新商業計畫的支持性、有效性及效率增益。

企業完成對於風險及機會的初步評鑑後，應確定如何應對這些風險及機會。良好的風險分析方法應對照本框架和 ISACA 的其他出版物所描述的指引，並確定要做出的風險決策。然後，應用完善的風險管理和價值管理實踐，從而做出明智的決策。

本頁留空

第四章

風險治理的重要性

4.1 介紹

本章討論風險治理的基本組成。儘管對此做了簡要的討論，但仍可在 COBIT 中找到更多資訊和實踐指南。本章節涵蓋的主題包括：

- 風險胃納、風險容忍度和風險容量。
- 資訊與技術(I&T)相關風險管理的利害關係人。
- 風險文化。

4.2 風險胃納、風險容忍度和風險容量

在制定策略或營運計畫時，企業必須決定承擔一定程度的風險以實現其目標。風險的數量或大小通常以風險胃納及風險容忍度做為表示。儘管經常使用這些術語，但產生誤解的可能性很高。有些人可以交互使用這些術語，使其他人可以看到明顯的不同。《資訊技術風險框架》定義與 COSO ERM[16] 和 ISO 31000[17] 定義兼容：

- **風險胃納** — 企業或其他單位在追求其任務或願景時願意承擔的廣泛風險程度。
- **風險容忍度** — 相對於達成特定目標的可接受範圍（最好以相關目標的相同單位進行量化）。

風險胃納

風險胃納反映了單位為實現目標而準備接受的風險程度。考慮企業的風險胃納時，有三個主要因素需要考量：

- 企業吸收損失的客觀能力，例如：財務損失或聲譽損失。
- 管理的文化或承擔風險的傾向，例如：謹慎或冒險。企業接受追求其策略或目標的損失程度是多少？
- 業務性質與涉及風險的類型，例如：糖果工廠中的傳送帶發生故障對應客機上的飛行控制系統發生故障。

企業的風險胃納都不一樣，構成可接受和不可接受的風險沒有絕對的規範或標準。

風險胃納的描述通常範圍很廣，並往往是以假設性或一般性的表示方式來描述，例如：「企業將不接受違規風險」或「組織將不接受欺詐風險」，而不是以可量化的方式表達風險。儘管這種風險胃納的表示方法很常見，但是很難在整體組織中作為管理指令將其向下傳達：對於風險的絕對禁止是不可能維持的，且是不切實際的。在對風險的禁止情形下，將修復所有控制缺陷，並拒絕所有具有風險的業務。實際上，這種方法並不能有效的利用資源。相反的，企業應試圖確定一個可接受的損失額，並按照這個額度進行管理。一個實用、具體及量化的風險胃納的案例是：

[16] 同上COSO委員會 (COSO)
[17] 同上 ISO

雖然該企業希望不承擔資訊與技術(I&T)的風險，但意識到，這對企業達成目標是不切實際的。因此，該企業將對總損失在100萬美元或以上的損失情況進行補救。

大型企業可能會發現，為每一業務專案編制一份這種報表是有用的。企業的偏好報表應該反映或匯總出所有業務範圍的描述。

每個企業都必須確定自己的風險胃納水準並定期審查。這種風險胃納的定義應與企業希望表達的總體風險文化相互一致，如：從非常規避風險到承擔風險或尋求機會。儘管沒有絕對的對錯，但風險胃納需要被定義、充分理解和溝通。風險胃納和風險容忍度不僅應用於風險評鑑，且應適用於所有資訊與技術(I&T)有關的決策。

風險容忍度

風險容忍度反映了與風險胃納和業務目標所設定的可接受水準之誤差範圍，例如：

標準要求專案必須在估計的預算及時間範圍內完成，但可容忍超出預算10%或超出預定時間20%的情況。

關於風險胃納和風險容忍度的指引

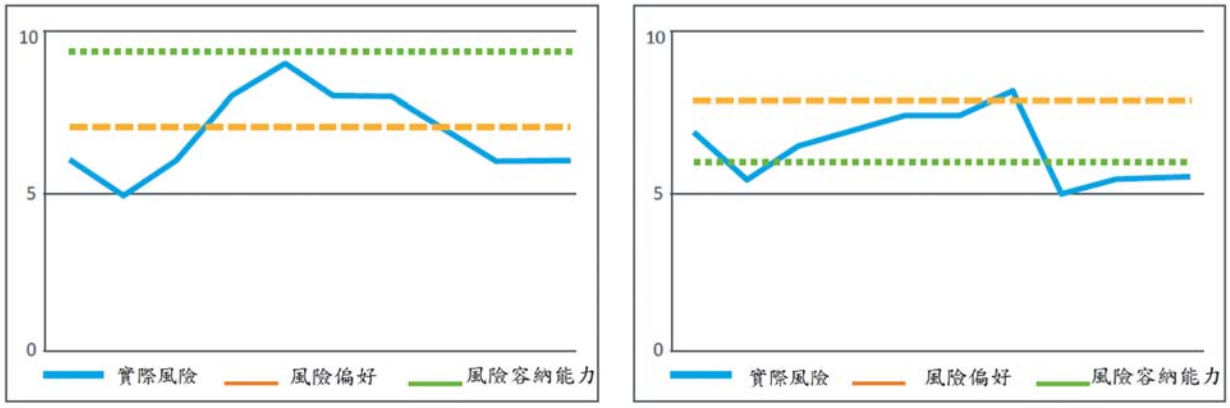
以下指引適用於風險胃納及風險容忍度:

- 風險胃納及風險容忍度是由企業高層決定的，由董事會審查或影響，並反映在執行長制定的策略和政策當中。在企業的較低層面，或在某些企業單位或子公司內，可以容忍例外情況(或設定不同的閾值)，只要企業高層的總體風險不超過所決定的風險胃納。任何業務措施都包含風險因素，因此管理階層應在風險的前提下視情況追求新的機會。風險胃納及容忍度政策在保守的企業，可能缺乏敏捷性或創新性來利用新的業務機會。相反的，風險胃納和容忍度政策可能受到法律、監管或行業要求的規定，對未能達到這些要求的風險可能需要零風險容忍度。
- 制定、審查和定期更新風險胃納及容忍度(由企業決定)，並向所有利害關係人明確告知。風險例外程序應明確規定與傳達。
- 新的市場條件、不斷變化的風險格局、修訂的策略及許多其他因素要求企業定期重新評估其風險組合並重新確認其風險胃納，從而引發風險政策審查。在這方面，企業應瞭解，風險管理可以為企業提供價值，使企業能夠實施包含風險的策略，並優化資源的分配。
- 風險應對的成本或風險對業務的影響可能會超出一個組織的能力及資源。從而迫使企業對一種或多種的風險條件有更高的容忍度。例如：如果一項法規規定必須對所有敏感的數據進行加密，但沒有可行的加密方法，或實施的方案成本過高，那麼企業可以選擇接受與不遵守法規的相關風險，這是一個根據事實數據所做出適合企業的決定。

風險容量

風險容量有時用於討論風險容忍度。風險容量通常被定義為企業所能容忍的客觀損失程度或數量，而在不危及其繼續生存的風險情況。因此，不同於風險胃納，風險容量通常反映了董事會或管理階層決定多少風險是可以容忍的決策，如圖4.1所示。

圖 4.1—風險容量、風險胃納及實際風險



來源：ISACA, *COBIT® 5 for Risk*, USA, 2013, fig. 68, *https://www.isaca.org/bookstore/cobit-5/wcb5rk*

- 左圖是一種相對可持續的情況，即風險胃納低於風險容量，實際風險在幾種情況下都超過了風險胃納，但仍始終低於風險容量。
- 右圖顯示的是一種相當不可持續的情況，管理階層將風險胃納定義為高過風險容量的水準。管理階層準備能接受的風險遠遠超過客觀能承受的損失能力。因此，實際風險經常超過風險容量，儘管大多數時候仍低於風險胃納水準。

4.3 資訊與技術(I&T)風險管理的利害關係人

在各企業中，資訊與技術(I&T)風險管理的利害關係人往往也各不相同。根據行業及企業的類型不同，對資訊與技術(I&T)風險管理的責任和職責的分配也大不相同。例如：在許多金融機構中，風險長(CRO)被降級為監督的角色或第二道防線[18]，而業務線承擔主要責任，有時甚至為風險決策負責。在其他商業企業中，資安長(CISO)負責資訊安全風險管理，而資訊長(CIO)或數位長(CDO)則負責職責分配。

資訊與技術(I&T)風險管理的責任和職責的分配，因行業和企業類型不同而有很大差異。

由於圖4.2中的角色在各企業中的實施方式不同，它們不一致地對應於相同的組織部門或職能。因此，對每個角色都提供簡要說明。圖4.2中列出的所有角色都被認為是管理、資訊與技術(I&T)相關的風險利害關係人。

[18] 關於三道防線模型，見內部稽核協會®(IIA®), *IIA立場聲明書: 有效風險管理和控制的三道防線*， USA, 2013, *https://na.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Three%20Lines%20of%20Defense%20in%20Effective%20Risk%20Management%20and%20Control.pdf*

圖 4.2 — 資訊與技術(I&T)風險管理利害關係人	
角色	描述
董事會	對企業資源的治理和整體控制負責的最高行政人員或非執行董事所組成的小組。
執行委員會	董事會任命的高階管理人員所組成的小組，以確保董事會能參與重大決策並隨時瞭解重大決策。 (執行委員會負責管理資訊與技術(I&T)相關的投資及資訊與技術(I&T)相關的服務和資產的專案組合，確保實現價值交付並管理風險。該委員會通常由董事會主席主持。)
執行長 (CEO)	負責企業整體管理的最高階主管。
財務長 (CFO)	對於財務管理各個方面負責的最高階主管，包括財務風險與控制及做出可靠和準確的帳目。
營運長 (COO)	負責企業營運的最高階主管。
風險長 (CRO)	負責整體企業風險管理各方面事務的最高階主管。 (可以建立資訊與技術(I&T)風險長職能來監督資訊與技術(I&T)相關的風險。)
資訊長 (CIO)	負責調整資訊技術和業務策略的最高階主管，並負責資訊與技術(I&T)相關的服務和解決方案的規劃，資源配置與管理。
技術長 (CTO)	負責資訊與技術(I&T)的技術方面的最高階主管，包括管理、監視與資訊與技術(I&T)服務、解決方案和基礎架構有關的決策。
數位長 (CDO)	負責將企業或業務部門的數位化目標付諸實踐的最高階主管。 (此角色可以由資訊長或執行委員會的另一名成員承擔。)
資訊與技術(I&T)治理委員會	利害關係人和專家所組成，負責指導資訊與技術(I&T)相關的事項和決策，包括管理資訊技術相關的投資、交付價值和監控風險。
架構委員會	利害關係人和專家所組成，負責指導與企業有關的事項和決策，並制定架構政策和標準。
企業風險委員會	負責企業等級的合作和共識的高階管理人員組成的群體，以支持企業風險管理活動和決策。 (可能會成立資訊與技術(I&T)風險委員會，以更詳細地考慮資訊與技術(I&T)相關的風險並向企業風險委員會提供建議。)
資訊安全長 (CISO)	負責整個企業的安全管理方面事務的最高階主管。
業務流程負責人	負責執行流程和實現流程目標，推動流程改進和批准流程變更的人。
專案組合經理	負責指導專案組合管理，確保選擇正確的計畫和專案，管理和監視計畫和專案以實現最佳價值及有效、快速地實現長期策略目標的人員。
指導委員會(計畫/產品)	由利害關係人和專家所組成，負責指導計畫和專案的包括管理和監視計畫、分配資源、提供收益和價值以及管理計畫和專案風險。

圖 4.2 — 資訊與技術(I&T)風險管理利害關係(續)	
角色	描述
計畫經理	負責指導特定計畫（包括陳述和後續跟進計畫的目的與目標）以及管理風險和對業務影響的個人。
專案經理	負責指導特定專案的人員，包括協調和委派專案團隊中的時間、預算、資源和任務。
專案管理辦公室	負責支持計畫和專案管理與收集，評估和報告有關計畫和組成專案行為的職能。
數據管理部門	負責在整個數據生命週期中支持企業數據資產並管理數據策略、基礎架構和資料庫的職能。
人力資源主管	負責企業人力資源計畫和政策的最高階主管。
關係經理	負責監督和管理業務和資訊技術部門間內部窗口及溝通的資深人員。
架構主管	資深人員，負責企業架構過程。
發展主管	資深人員，負責資訊與技術(I&T)相關的解決方案開發流程。
資訊技術營運主管	資深人員，負責資訊技術營運環境和基礎架構。
資訊技術管理主管	資深人員，負責資訊與技術(I&T)相關記錄並支持資訊與技術(I&T)相關的行政事務。
服務經理	為特定客戶或群體客戶管理新產品、現有產品和服務的開發、部署、評估和持續維護的人。
資訊安全經理	管理、設計、監督或評估企業資訊安全的人。
持續營運經理	管理、設計、監督或評估企業營運持續性能力的人員，以確保企業的關鍵功能在發生破壞性事件後仍能繼續運行。
計畫經理	負責指導特定計畫（包括陳述和後續跟進計畫的目的與目標）以及管理風險和對業務影響的個人。
法律顧問	負責法律和法規事務指導的職能。
法令遵循人員	負責有關外部法律合規性的職能。
稽核人員	負責提供內部稽核的職能。

來源：改編自 ISACA, *COBIT® 2019 Framework: Governance and Management Objectives*, USA, 2019, Appendix B, *https://www.isaca.org/bookstore/bookstore-cobit_19-digital/wcb19fgm*

4.4 風險文化

風險管理使企業產生的價值最大化，同時避免損失對其實現任務的能力產生負面的影響，甚至是影響持續經營的能力。風險意識文化促進對風險的公開討論、理解並維持可接受的風險水準。風險意識文化從組織高層開始，由董事會成員和企業高階管理人設定方向與傳達風險意識決策，並獎勵有效的風險管理行為。風險意識還意味著企業內部都瞭解企業為什麼和如何應對資訊與技術(I&T)有關的不利事件。

風險意識文化促進對風險的公開討論、理解並維持可接受的風險水準。

風險文化是不容易描述的，並由多種行為所組成，如下表4.3所示：

圖 4.3 — 風險治理與管理的相關行為	
一般企業行為	
始終具有風險和合規意識的文化，包括主動識別和提升風險	企業確定風險管理的方法和風險胃納，並制定了違法和監管要求的零容忍政策。
已確定的政策已被傳達，並驅動行為	所有人員理解並執行相關政策規定的企業要求。
對提出問題和承認後果表現出積極的接受態度	檢舉人被視為對企業的積極貢獻者。避免指責文化。員工需要理解提高風險意識和報告潛在的風險。
認識到風險的價值	工作人員瞭解保持風險意識的重要性，以及管理風險給他們的角色所帶來的價值。
具有透明及參與的文化	交流是開放的，事實不會被遺漏、扭曲及低估。避免了隱藏議程的負面影響。
互相尊重	鼓勵利害關係人和風險評鑑者進行合作，在工作中視為專業人員與專家。
承擔風險責任	風險實踐納入整體企業。職責能得到明確分配和接受。資訊與技術(I&T)相關的風險歸企業所有，而不僅僅是資訊技術部門或資訊技術風險部門的責任。
允許接受風險作為有效選擇	管理階層瞭解風險接受的後果。影響會確定在企業的風險容忍度之內。
風險專業行為	
努力瞭解每個風險承擔者的風險及其對目標的影響	風險專業人員瞭解風險的業務影響，包括競爭、營運、法規和合規性要求。儘管在特定行業中風險可能很常見，但是就風險如何影響其目標而言，每家企業都是獨特的。
建立對風險政策的認識與理解	風險容忍度、風險胃納和企業政策的協調產生有效的風險策略。

風險專業行為	
在風險評鑑過程中促進合作及雙向溝通	風險評鑑基本上是準確及完整的，並滿足利害關係人的需求。
明確定義風險胃納並及時與利害關係人進行溝通	利害關係人有效的管理風險，並與組織策略和目標保持一致
制定反映風險胃納和風險容忍度的政策	員工和管理階層在風險容忍度範圍內運作。業務部門將風險胃納和容忍度應用於日常業務。在高階管理階層的考慮及批准下，有一個明確的流程可以提議和更改風險容忍度。
支持有效的風險實踐	利害關係人從共同的專案組合視角（產品與過程）理解風險，並將基於風險的決策應用於日常實踐。
使用 KRI 有效的作為預警	KRI 與有效指標相關聯，可作為流程或控制失敗的指標。KRI 指標可用於定期報告，並且與目標相關聯。
根據超出偏好及容忍度外的風險指標或事件迅速採取行動	風險指標與管理階層的風險回應和補救措施相關。
管理行為	
設定方向並展現對風險實踐真正的支持	透過高階管理階層的真正支持，可以保持風險管理實踐的品質。
與所有相關利害關係人合作，確定行動並採取後續行動計畫	正確的利害關係人適當參與，以確保及時解決問題和實現業務計畫。
獲得真正的承諾，並為執行行動分配資源。	人員被授權執行風險管理決策所要求的行動。
調整政策和行動以適應風險胃納	管理階層在遵守政策方面做出適當的風險決策。經風險調整後的營收能符合管理階層的預期。
根據行動計畫監控風險和進度	補救計畫將在預期的業務時間範圍內完成，並對企業目標產生正面影響。
向高階管理階層和董事會報告風險趨勢	及時報告風險趨勢可主動管理風險並避免機會損失。
獎勵有效的風險管理	良好的風險措施得到認可。員工的業績目標和獎勵結構將激勵有效的風險管理做法和執行適當的風險抵減行動。
設定方向並展現對風險實踐真正的支持	透過高階管理階層的真正支持，可以保持風險管理實踐的品質。

來源: Adapted from ISACA, *COBIT® 5 for Risk*, USA, 2013, fig. 26, *https://www.isaca.org/bookstore/cobit-5/wcb5rk*

風險文化包括:

- **對承擔風險的行為** — 對承擔風險、識別風險和分析風險的規範和態度是什麼？
- **對政策的行為** — 政策是存在但沒有被遵守的東西嗎？政策是否會驅動行為？政策是否易於閱讀、理解和遵守？

- **對負面結果的行為** — 企業如何處理負面結果、例外政策、損失事件、網路事件、錯失機會和事件調查？會從中吸取教訓並努力調整，還是不治本的指責？

風險文化不足或有問題的症狀包括：

- 實際的風險胃納、所述的容忍度和風險政策不一致。
- 未能使風險政策與管理方向和遵守政策的組織規範保持一致。
- 存在指責文化。應避免這種文化，因為抑制了相關和有效的溝通。在指責文化中，當專案沒有按時交付或沒有達到預期時，業務部門往往會將矛頭指向資訊技術部門或其他人。此時，他們沒有意識到業務部門在前期的參與對專案成功的影響。在極端的情況下，業務部門可能會將自己從未明確傳達過的期望值歸咎於失敗。指責減少了各單位的有效溝通，進一步加劇了專案的延誤。執行主管必須查明並迅速糾正指責文化，以促進整個企業的合作。

第五章

風險管理的重要性

5.1 介紹

本章介紹風險管理過程的基本組成[19] 。討論的主題包括：

- 確定風險管理的背景和範圍。
- 瞭解風險管理工作流程。

5.2 設置環境並確定風險範圍

在企業的使命、策略和目標範圍內定位風險是確保每個流程和程序的第一步，並且每天進行檢查以確保符合企業的長期業務目標，同時與其風險狀況保持一致。這稱為建立風險管理的全景。將風險的方法與企業策略的觀點結合使用，並可以進行交流和釐清，那些不確定性或風險最有可能危害企業的目標、宗旨和使命。

在企業的使命、策略和目標範圍內定位風險是確保每個流程和程序的第一步，並且每天進行檢查以確保符合企業的長期業務目標，同時與其風險狀況保持一致。

風險管理要求企業:

- 定義風險管理步驟適用的範圍。
- 設定評估或評鑑已識別風險的標準。

範圍應在企業目標全景內確定。設置全景將幫助企業將初步風險評鑑的範圍（例如：限制為一種業務功能，如：會計）限制在一定範圍內，並瞭解該範圍如何符合整個企業的全景。

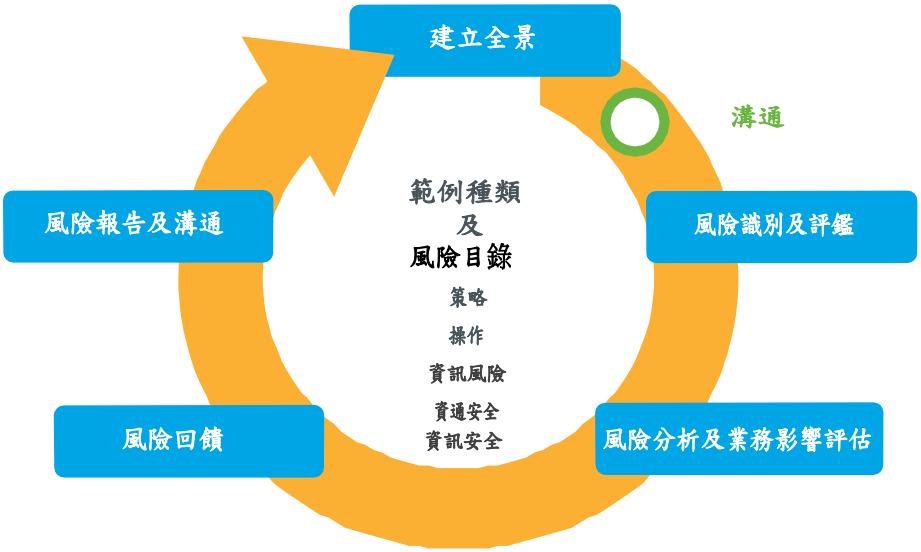
建立評估已識別風險所依據的標準，也是整個風險管理流程的重要組成部分。風險胃納和風險容忍度的發展可以幫助企業快速評估與瞭解風險是否符合企業風險容忍度，或需要進一步分析或調查。

[19] 更多指引，承上ISACA，風險管理入門和風險資訊與技術從業人員指引，第2版.

5.3 瞭解風險管理工作流程

圖5.1描述了風險管理工作流程的主要階段。圖中的步驟不一定按順序執行。每個企業都應該開發一種工作流程，以支持快速且有效的方式來完成任務。

圖 5.1 — 風險管理工作流程



來源: Adapted from ISACA, *Getting Started With Risk Management*, USA, 2018, fig. 2, *https://www.isaca.org/bookstore/bookstore-wht_papers-digital/whpgsr*

第六章

風險評鑑的重要性

6.1 介紹

本章介紹風險評鑑過程[20]的基本組成。這裡討論的主題包括:

- 風險識別。
- 風險分析。
- 評估已識別風險的業務影響。
- 資訊與技術(I&T)相關的風險情境。

6.2 風險識別

風險識別過程目的是提高企業對已識別並理解任何可能危害其目標風險的信心：

風險識別可以發生在正式場合（例如：在腦力激盪會議或研討會期間）或非正式場合（例如在會議中或辦公室對話間對偶然討論問題）。腦力激盪會議通常從一份讓參與者夜不能寐的專案清單開始，包括網路威脅或其他關注領域。通常使人們保持清醒的問題會帶來風險，而不是導致風險本身。例如，員工可能擔心未更新版本的系統，並經常將其歸類為風險。

《資訊技術風險框架》目的在確定可能影響企業使命和策略目標的損失事件。最初的識別可以發生在不同的環境中，也可以採取不同的形式，包括訪談、腦力激盪活動、網路自我報告或問卷調查。《資訊技術風險從業人員指南》第2版[21] 中提供了其他指引。

6.3 風險分析

風險分析包括在複雜的企業風險管理，特別是資訊與技術(I&T)相關的風險，可在管理中提高務實的洞察力、企業參與和組織透明度的核心方法。風險分析將用於以下方面的過程:

- 估計給定風險場景的發生頻率及嚴重程度。
- 識別並評估風險，其對企業的潛在影響及特定事件發生的可能性。

風險評鑑的範圍比風險分析的範圍略大，包括根據所定義的風險閾值，並對已識別風險進行排序或優先等級劃分，將類似風險類型分組在一起進行風險抵減的活動，同時記錄提供抵減風險的現有控制措施。

6.4 評估識別風險的業務衝擊

有意義的風險評鑑及風險決策需要以明確及業務或任務相關的術語表示資訊與技術(I&T)相關的風險。有效的風險管理需要在資訊技術與業務間，就哪些風險需要管理和為什麼需要管理達成共識。

[20] 更多指引，承上ISACA，風險管理入門和風險資訊與技術從業人員指引，第2版
[21] 前引ISACA，《風險資訊與技術從業人員指引》，第2版

有意義的風險評鑑及風險決策需要以明確及業務或任務相關的術語表示資訊與技術(I&T)相關的風險。有效的風險管理需要資訊技術與業務之間就哪些風險需要管理和為什麼需要管理達成共識。所有利害關係人必須能夠理解與表達資訊技術有關的故障、損害、錯誤或事件如何影響企業的目標，並導致直接(即財務)或間接(即資料或資訊)損失(如敏感客戶資訊的損失)。資訊與技術(I&T)有關的事件給企業造成的損失會影響企業提供關鍵服務及產品的能力。

有效的風險管理需要資訊技術與業務之間就哪些風險需要管理和為什麼需要管理達成共識。

為了瞭解不利事件的影響，需要建立資訊與技術(I&T)風險情境與最終業務或任務影響間之關聯。有幾種技術可以幫助企業透過業務或任務術語來描述資訊與技術(I&T)風險。雖然《資訊技術風險框架》要求將資訊與技術(I&T)相關的風險轉化為業務有關的術語表示，但並沒有規定任何單一的方法；《資訊技術風險從業人員指引》第2版[22] 中探討了幾種方法。

6.5 資訊與技術(I&T)風險情境

資訊與技術(I&T)風險管理的挑戰之一，是在資訊與技術(I&T)可能出現問題或資訊與技術(I&T)有關的一切情況下確定相關風險，特別是考慮到資訊與技術(I&T)在整個企業中的普遍性存在。

一種克服此挑戰的技術是建立風險情境，使資訊與技術(I&T)相關的風險複雜問題有了深刻的認識與架構的瞭解(圖6.1)。在建立情境之後，於風險分析中透過情境估計發生風險的頻率和業務影響。

可以透過兩種機制得出風險情境:

- **由上而下的方法** — 任務策略和業務目標構成了識別及分析可能與預期結果相關風險的基礎。如果影響標準與企業的實際價值驅動力能相互吻合，則可以建立相關的風險方案。
- **由下而上的方法** — 從被認為對企業重要的資產、系統或應用程式開始，編制一份威脅或一般損失情況清單。接者，將清單用於定義一套適用於企業全景的具體且客製化的情景。由下而上的方法通常用於網路威脅和脆弱性評鑑；但是，如果不將由下而上的結果與由上而下的方法結合起來考慮，可能會限制可見度或掩蓋業務的影響。

由上而下和由下而上的方法是互補的，應一起使用。風險分類法可提供風險來源和類別的分類模式，從而有助於將其結果聯繫起來。從網路威脅到已發展並紀錄的風險，需要將風險描述分解為可操作的部分。風險分類法提供了不同來源和類別的通用語言，並說明從業人員與風險承擔者進行風險溝通，從而確保風險情境是相互關聯且與實際業務或任務風險相關。

在確定了一套風險情境之後，可以用來進行風險分析，評鑑風險情境的發生頻率及影響。風險因素是這種評鑑的重要成分。風險因素會影響風險情境的頻率和業務或任務的影響；風險因素可以有不同的類型，可分為兩大類:

- **背景因素（內部或外部）** — 主要差別在於企業對有關因素的控制程度。
  - 內部背景因素在很大程度上是企業可控制因素之下，因為可能不會容易被改變。
  - 外部環境因素在很大程度上是企業無法控制的。

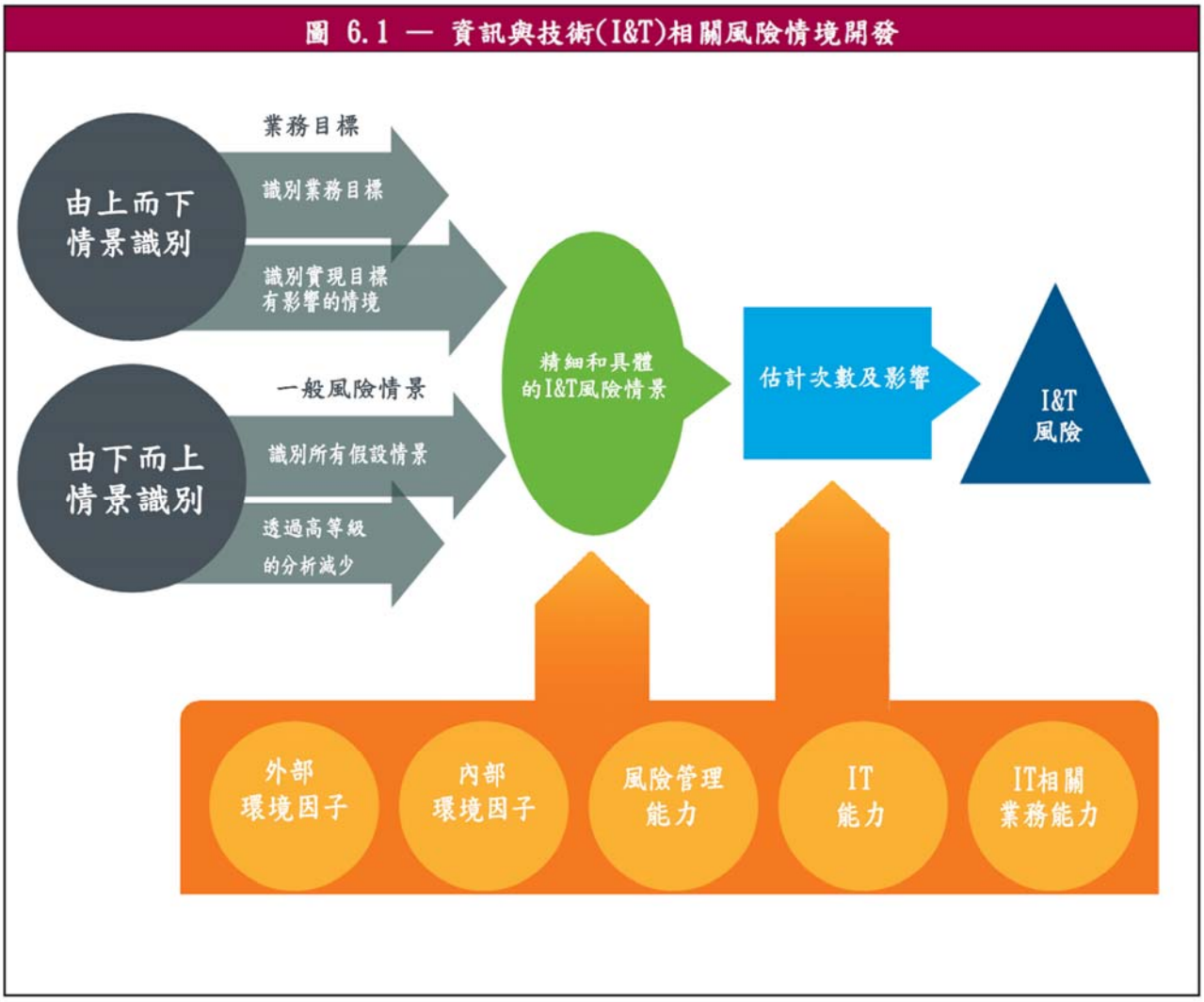
[22] 同上.

- **能力因素(表明實現資訊與技術(I&T)有關的活動能力)** — 這些因素對風險管理的成功結果至關重要。能力因素被加入許多相關的 ISACA 工具、技術、方法及框架中，並支持企業定義與改進資訊與技術(I&T)相關流程，以繼續實現資訊與技術(I&T)相關活動。能力因素有助於回答下列問題:
  - 與資訊與技術(I&T)相關的風險管理能力 — 企業在執行風險管理方面的成熟程度如何?
  - 與資訊與技術(I&T)相關的業務或任務能力（或價值管理） — 資訊與技術(I&T)相關的業務或任務能力有多強？是否有能力支援企業目標，並同時管理可能危及目標的風險?

資訊與技術(I&T)風險情境描述的是資訊與技術(I&T)相關的事件，一旦發生就會對業務產生影響。為了使風險情境完整並可用於風險管理與決策分析，風險情境應描述圖6.2所示的下列項目:

- **產生威脅的行為者 — 行為者可以是內部，也可以是外部，同時可以是人為，也可以不是人為造成的。**
  - 內部行為者是指企業內部的行為者，如員工或承包商。
  - 外部行為者包括外部人員、競爭者、監管者和市場。
  - 並非每一種威脅都需要一個行為體，例如，流程故障或自然災害。
- **條件的類型或事件的性質** — 條件或事件的類型包括：惡意、意外、流程中斷、自然事件（即不可抗力）、景氣循環等。
- **事件影響或結果的類型** — 影響或結果的類型包括：資訊揭露、系統中斷、意外修改或變更、盜竊、破壞等。這些事件可能反映出（系統及流程等）設計不良、流程執行沒效率（如變更管理程式、採購程式或專案優先順序流程）、規定的影響及使用不當。影響還包括該情景下的清除及補救所耗費的成本。
- **目標資產或資源** — 資產是指在履行企業使命或業務策略方面對企業有價值的任何事物，這些事物可能會受到不利影響並導致業務或使命受影響。資源是指有助於實現資訊與技術(I&T)相關目標的任何事物。資產和資源可以是相同的。例如：資訊與技術(I&T)硬體是一種重要的資源（因為所有資訊與技術(I&T)相關的應用都會使用），同時也是一種資產（因為對企業有一定的價值）。資產或資源包括：
  - **人員** — 如：員工、承包商、人力公司和協力廠商。
  - **資訊與技術(I&T)流程** — 如：業務和資訊技術流程、資料流程圖或資訊流。
  - **實體基礎設施** — 如：設施及設備。
  - **資訊與技術(I&T)基礎設施** — 如：運算硬體、網路基礎設施和中介軟體。
  - **其他企業架構組成，包括:**
    - 資訊
    - 應用程式

圖 6.1 — 資訊與技術(I&T)相關風險情境開發



一些資產可能被列為關鍵資產，而另一些資產則被視為非關鍵資產(或在業務週期的某些階段只是間歇性的關鍵資產)。關鍵資源可能會成為更多網路攻擊者的目標；因此，相關情境的發生頻率可能會更高。區分關鍵資產和非關鍵資產需要技巧、經驗和可靠性的透徹理解。

時間也可能與某些情況有關，描述如下:

- **事件的持續時間** — 如：服務或資料中心的長時間中斷。
- **時間** — 事件是否發生在關鍵時刻？時間可以進一步區分：
  - **事件與影響之間的時間差** - 是否有直接的後果（例如：網路故障和立即停機），或在較長的時間內的延遲影響（例如：資訊技術架構的陳舊，數年內累積的成本較高）？

風險情境架構(圖6.2)區分了損失事件(產生負面影響的事件)、脆弱性或脆弱性事件(造成損失事件規模或頻率的事件)和威脅事件(威脅行為者帶來的可能引發損失事件的情況或事件)。

- 行為者/威脅群體
- 意圖/動機
- 威脅事件
- 資產
- 效果
- 時間安排

圖 6.2 — 風險情境/損失事件架構及組成

必須描述和理解風險情境的不同組成部分，以便採取適當行動。如要做到這一點，很難用一個大型清單來列舉可能發生的未經優先考慮的情況。因此，從業人員更願意用一個有重點、有發展、有細微差別的清單來列舉按業務影響進行分析和優先考慮的相關風險項目。風險登記冊可用於記錄和追蹤已識別、分析和優先考慮的風險。

《資訊技術風險從業人員指引》第2版[23] 包括了編制相關的、可管理的資訊與技術(I&T)風險情境的進一步指引，並包括一套風險情境範例。

[23] *Ibid.*

此頁留白

第七章

風險意識、報告及溝通

7.1 介紹

風險意識包括確認不確定性或確認風險是業務不可或缺的一部分。這並不意味著要避免或消除所有風險，而是資訊與技術(I&T)相關的風險應為：

- 可識別的
- 公認的
- 眾所周知且廣為人知
- 透過使用適當資源進行管理

風險報告和溝通是風險意識的關鍵部分。決策者和利害關係人(包括董事會)必須及時收到準確的風險資訊，並以此採取行動。人們往往對談論風險感到不自在；他們傾向於推延對於風險的討論，因為涉及對未來不確定性思考，畢竟可能不會真正實現。然而，儘管有這些主觀反應，但就風險進行良好的溝通是必不可少的，即在風險成為一個問題、事件或重大危機之前。

風險報告和溝通是風險意識的關鍵部分。決策者和利害關係人(包括董事會)必須及時收到準確的風險資訊，並以此採取行動。

7.2 風險意識及溝通的好處

資訊與技術(I&T)相關風險公開交流的好處包括:

- 對實際曝露和已實現風險的潛在影響的共識，從而能夠做出適當而明智的風險應對決策。
- 向所有利害關係人提供有關潛在風險曝露水準、風險管理流程和使用功能的透明性。

風險的溝通不暢通常會導致:

- 對實際面臨的風險程度產生錯誤的信任感。
- 由上而下的風險管理缺乏明確的方向。
- 利害關係人對風險程度的理解不足。
- 認為企業對利害關係人、監管者、投資者或協力廠商(如客戶)隱瞞了已知的風險。
- 不能及時對可能造成傷害或損失的問題作出反應。
- 當高階管理階層被視為負有責任，但卻沒有採取糾正行動，或沒有向利害關係人充分說明改善行動時，就會對利害關係人的聲譽造成重大損害或降低其期望。

7.3 風險報告與溝通

資訊與技術(I&T)相關的風險溝通涉及廣泛的資訊流。如圖7.1所示，《資訊技術風險框架》區分了以下主要類型的資訊與技術(I&T)有關風險溝通:

- **關於風險管理策略、政策、程序、認知、培訓等方面的期望** — 企業應不斷根據企業資訊與技術(I&T)相關的風險總體策略進行溝通，並強化各項原則等。清晰且一致的風險認知溝通推動了後續的風險管理工作，提高了風險意識，並為風險管理行為設定了總體期望。
- **當前風險管理的能力** — 溝通企業風險管理能力表明企業管理風險和減少風險的情況，促進風險管理能力差距的透明度，通常是良好風險管理的關鍵指標。
- **管理中已識別風險的狀況** — 風險狀況的溝通可包括以下與風險有關的產物資訊:
  - **風險概況** — 即企業所面臨的已識別資訊與技術(I&T)相關風險的整體組合，包括組合中每一種風險情況的衡量標準。
  - **關鍵風險指標** 支持管理層報告風險的關鍵風險指標(KRI)
  - **事件/損失資料** 有關已實現風險的事件或損失資料
  - **根本原因分析** 已實現損失事件的根本原因分析
  - **抵減方案**（成本和效益方面）

圖 7.1 — 資訊與技術(I&T)風險溝通的組成

為使資訊溝通有效，所有資訊交流－無論其類型如何－應清晰、簡明、完整、準確、及時，並能為所有利害關係人所理解。這些標準對於資訊安全、技術、資通風險尤為重要。應避免使用有關風險的技術及專業的術語。不相干或過於詳細的資訊會造成妨礙，而無助於清楚地瞭解風險，特別是關於網路威脅、脆弱性和事件的資訊，因為幾乎沒有事實證明其根本原因或任何損失的實際程度。

從識別風險及其對業務或任務的影響到風險回應活動之間可能會有一段關鍵時間。例如：當建立了一個不適當的資訊技術組織時，就可能出現風險情況。對組織的業務影響(最終)表現為較沒效率的資訊與技術(I&T)操作及較差的業務和服務傳遞。資訊技術專案失敗的情境可能會導致業務計畫的最終延誤或無法完成。溝通是及時的，當它允許在適當的時刻採取行動，以識別及處理風險。

資訊必須以適當的詳細程度傳達，並須因應使用者及監管者的需要。在這個過程中，彙總不能掩蓋風險的根本原因。例如：安全管理人員需要關於入侵和病毒的技術性資訊與技術(I&T)資料來實施解決方案。資訊與技術(I&T)指導委員會可能不需要這種程度的細節，但它確實需要彙總的資訊來決定政策變化或額外的預算來處理同樣的風險。

資訊必須以適當的詳細程度傳達，並須因應使用者及監管者的需要。

資訊必須在適當的使用者及監管者需要時提供。請注意，風險登記手冊（包括所有已記錄的風險）並不是公開資訊，應受到適當保護，防止內部和外部的人士在沒有必要的情況下獲得。

溝通不一定要透過書面報告或資訊進行正式溝通。利害關係人之間應及時舉行面對面的會議也是傳達資訊與技術(I&T)相關風險資訊的重要方式。

7.4 關鍵風險指標

關鍵風險指標（KRI）能夠顯示企業承受的風險或具有很高承受風險能力的風險指標，這些風險超過了定義的風險胃納或容忍度。顧名思義， KRI 只是風險的指標，而不是風險的直接衡量指標。重要的是不要將風險衡量（以及相應的風險評級分配）與 KRIs 混淆。
KRI 是每間企業所獨有的，KRI 的選擇取決於內部和外部環境中的許多參數，包括企業的規模和複雜性、監管環境（即是否在一個高度監管的市場中經營）和策略重點。
辨識 KRI 應考慮到以下步驟(除其他外):

1. **基於資訊需求的利害關係人**–適合利害關係人參與風險指標的選擇，也能確保更大的認同感和自主權。
2. **隨著時間的推移，對指標進行疊代和改進**–選擇指標時，要採取平衡的方法，既要有前瞻性的指標，也要有領先性的指標，還要有落後性的指標，也要有滯後性的指標。

領先指標包括防止事件發生的資料、資訊或能力。領先指標可能有上限和下限，以說明企業瞭解何時需要在風險發生之前關注某一狀況。

滯後指標包括在事件或條件發生後衡量的資料、資訊或能力，例如：達到性能目標或服務水準可用性目標。從已發生的風險、中斷的控制或流程以及隨時間推移而錯過的目標中分析根本原因，可以幫助企業開發新的指標、趨勢或相關條件，以此獲得洞察力。

一個企業可以制定一套廣泛的衡量標準作為風險指標；然而，維持廣泛的關鍵風險指標一般而言是不可行的。根據定義，關鍵指標需區分為高度相關且具有高機率的預測或顯示風險結果。

選擇適當的關鍵風險指標可以為企業帶來以下好處：

- **早期預警** – 企業發出風險可能很快發生的前瞻性信號，使企業能夠在風險成為損失之前作出積極的反應。
- **對已發生的風險進行歷史背景的回溯** – 進一步為未來的風險應對提供依據，推動改進，並支援對風險趨勢的記錄和分析。
- **風險胃納和容忍度的回饋** – 改進風險管理策略和流程，並最佳化風險治理和監督。

關鍵風險指標相關的常見挑戰或陷阱包括：

- 衡量目標不明確，沒有明確的或預期的結果，或者缺乏可以用關鍵風險指標的資料來回答明確問題。
- 蒐集容易獲得或已經掌握的資料，而不是特定風險相關或與風險類型有重大關聯的資料。
- 關鍵風險指標與具體的風險或業務目標之間缺乏明確的邏輯關係。
- 衡量標準過多，沒有明確的衡量目標或目的。
- 繁瑣的彙總過程。
- 在企業級整合及解釋關鍵風險指標的結果過於複雜。

由於內外部環境不斷變化，風險環境也是高度動態的，一套關鍵風險指標需要隨著時間的推移而變化。每一個關鍵風險指標都應與風險胃納及風險容忍度有明確相關，以便確定觸發水準，並支持採取適當與及時的行動。

第八章

風險回應的重要性

8.1 介紹

本章簡要討論風險回應的基本內容:

- 風險處置。
- 風險彙總。
- 風險應對措施的選擇和優先次序的確定。

以下四種風險處理方式有助於企業有效管理風險，關注對目標影響最大的風險（如果風險發生）:

- 風險規避。
- 風險抵減。
- 風險分擔或轉移。
- 接受風險。

風險應對措施目的是在風險分析之後使風險與確定的風險胃納保持一致。需要確定應對措施，以使未來的剩餘風險(即在確定和實施風險應對措施後的當前風險)儘可能地(通常取決於可用預算)保持在風險容忍限度內。無論情況如何，管理層都可以決定接受任何風險。

有關風險應對的更多資訊和實用指引可參見《資訊技術風險從業人員指引》第2版[24]。

8.2 風險規避

避免風險意味著要退出風險引起的活動或條件。在沒有其他風險應對措施的情況下，避險適用：

- 在沒有其他成本效益高的應對措施下，能夠成功地將已發生風險的影響降低到規定的損失閾值以下。
- 風險不能分擔或轉移。
- 管理層認為該風險是不可接受的。

一些與資訊與技術(I&T)相關風險規避的例子包括:

- 將資料中心遷離有重大自然災害的地區。
- 當企業案例顯示出明顯的失敗風險時，拒絕加入較大的專案。

8.3 風險抵減

風險抵減可降低風險發生的頻率和影響。風險抵減的常見策略包括:

- **加強整體風險管理做法**--企業應考慮將責任分配到各部門。將風險識別和管理交給最接近產生風險的活動或流程的人。

[24] 同上

- **將風險意識納入常規工作流程**--在日常活動中加強風險意識，有助於工作人員在事件發生之前更好地理解和識別產生風險的行為。
- **改進風險管理流程並制定相關的容忍度**--企業應尋找機會將風險管理從策略面逐層推進並擴展到企業的第一線。
- **自動化觸發或警報**--當閾值超出容忍度時，自動化通常能提供最先進且最及時的指示。
- **加入控制措施**--控制措施的目的是降低已發生風險發生的頻率或影響。以下各節將討論各種控制技術。

8.4 風險分擔或轉移

分擔需要透過轉移一部分風險來降低風險發生的頻率或影響。常見的技術包括:

- 為資訊與技術(I&T)相關的事件或資通事故購買保險。
- 委外辦理的資訊與技術(I&T)相關活動。
- 透過固定價格安排或共同承擔，並與協力廠商及供應商分擔資訊與技術(I&T)有關的專案風險及投資安排。

無論是從具體的經驗來看，或是從更抽象的法律意義來看，這些技術都不能解除企業的風險。不過，當發生不利事件時，這些技術可以透過另一方的技能來管理風險，從而減少其對財務的影響。

8.5 風險接受

接受是指對某一特定風險不採取任何行動，當風險發生時，接受損失。這種反應與僅僅對風險一無所知有很大的不同。接受風險的前提是，風險是已知的。也就是說，管理層作出了接受風險的知情決定。

如果企業採取接受風險的立場，就應該仔細考慮誰能接受風險。特別是在資訊與技術(I&T)相關的風險中，只有業務管理部門（和業務流程所有者）與資訊技術(IT)部門或資訊技術(IT)支援職能的部門合作（並得到其支持）才能接受風險。必要時，應將接受情況告知適當的利害關係人，如：高階管理階層及董事會，並由政策規定。識別或減輕每一個風險可能並不相關，也不符合成本效益。

8.6 風險彙總

風險彙總是一種方法或程序，透過這種方法或程序，可以將單一風險合併起來，以便進行報告或處理，或獲得綜合風險狀況或風險評分。如果從點對點風險彙總的角度來管理風險，則有關資訊與技術(I&T)風險管理的決策對企業更有利。對風險的整體看法支持對風險胃納和風險容忍度進行完整及徹底的審查，並且在企業利益方面總是超過相對獨立的風險識別與處理。

資訊與技術(I&T)相關的風險通常按風險類型、風險回應的相似性或特定的控制處理方式進行分組。例如：如果企業存取管理方法在不同的業務或任務領域反覆產生稽核發現或控制缺陷，那麼存取管理的企業措施可能會解決這個問題。

基於向執行委員會或董事會報告的目的，影響財務風險往往被彙總為，如某些類型的風險發生時可預期的財務損失範圍。許多企業都有一套以財務術語表示的影響標準和風險容忍度。

風險彙總及報告是當前許多受巴塞爾銀行監管委員會（巴塞爾委員會）監管程序約束的金融機構的要求[25]。這一要求推動了高階管理階層(或其代表)、風險管理部門或人員、和董事會之間的討論，討論什麼是可以接受的、有助於董事會作出知情決定的適當風險彙總和量化水準。

出於向執行委員會或董事會報告的目的，影響財務的風險往往被彙總為如果某些類型的風險發生時可預期的財務損失範圍。

8.7 風險應對措施的選擇和優先次序的確定

前面幾節列出了風險應對方案。本節的重點是在特定的風險背景下，區分、評估及選擇這些應對方案中的適當對策。在這一過程中需要考慮到以下參數:

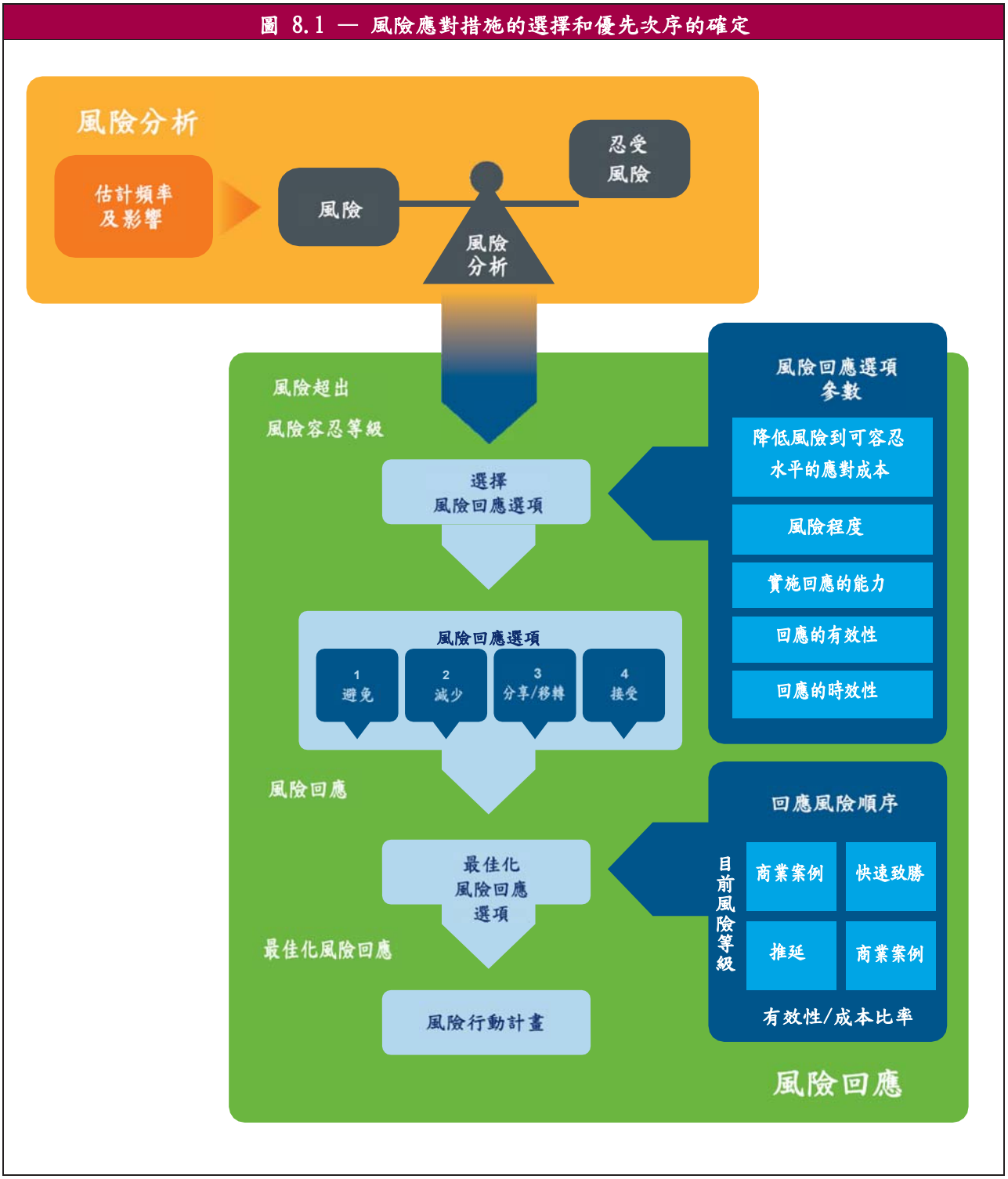
- **應對措施的成本** — 在風險轉移的情況下，考慮保險費的成本；在風險抵減的情況下，考慮實施、維護和測試控制措施的成本。
- **應對措施所處理風險的重要性** —考慮風險登記冊上的優先順序或等級。
- **應對措施的實施和維護能力** — 企業的風險管理能力越成熟，能夠實施的應對措施就越好；當企業相當不成熟時，可以使用一些非常基本的應對措施，並隨著時間的推移而改進。
- **應對措施的有效性** — 考慮應對活動在多大程度上會降低風險發生的頻率，或者當風險發生時，則要考慮到它的影響。
- **其他資訊與技術(I&T)相關投資** — 考慮一旦風險發生，應對活動將在多大程度上降低風險的頻率或影響。
- **其他應對措施** — 應對措施可能涉及幾種風險類型，而另一種可能不涉及；風險可能會被彙總。並隨後以共同的對策加以解決。

有時，風險回應的工作或資源（例如：需要實施或加強的控制措施的集合）將超出企業的可負擔能力。在這種情況下，需要確定優先次序，組織技能和專業知識。風險應對方案可分為以下幾類:

- **快速致勝** — 包括對高影響風險的非常短期、省時和有效的反應。
- **有不可商量的要求及合規義務** — 對不合乎規定及法規的風險管理應與其他風險應對措施一起進行，以避免重複或重疊的工作[26]。
- **所需的業務案例** — 對高影響風險的應對措施費用較高或難度較大，需要在投資前進行認真分析和作出管理決定。這類應對措施還可包括將企業內部無法解決的風險管理外包。
- **推遲和繼續監測情況** — 企業可推遲應對措施，並持續進行監測以確定風險或環境的變化是否需要採取不同的對策。

[25] 同上 巴塞爾銀行監管委員會
[26] 另請參閱本出版品中的第 8.6 節風險彙總

圖 8.1風險應對措施的選擇和優先次序的確定



中文版致謝名單

ISACA台灣分會葉奇鑫理事長

翻譯(按姓名筆劃): 吳易昇、魏銪志

校稿 (按姓名筆劃):陳政龍、簡宏偉

編輯排版:游恬欣