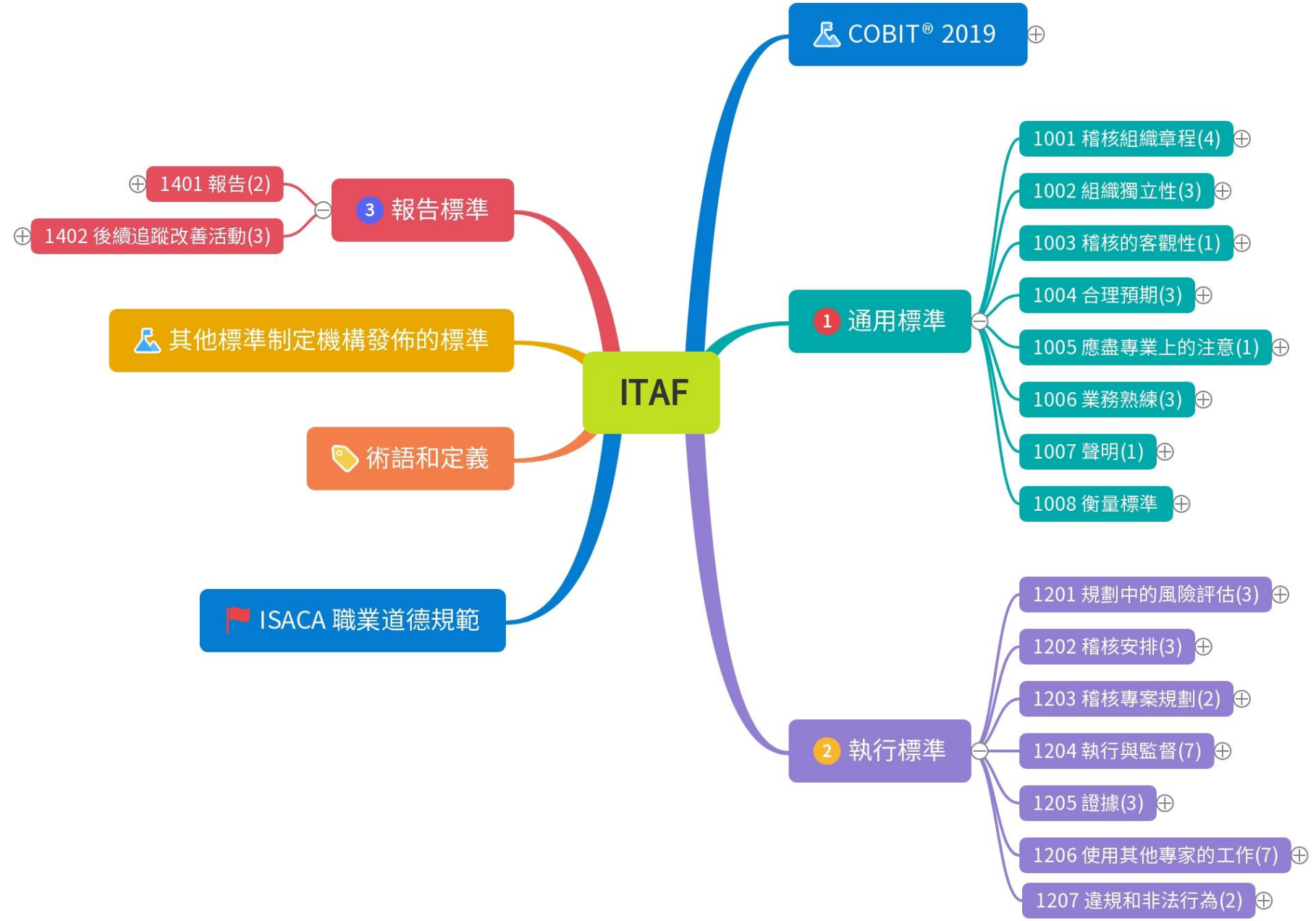
ISACA ITAF運用在GRC的實務探討「資訊稽核專案品質管理」

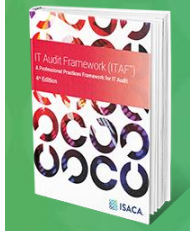
陳政龍
ISACA台灣分會 副會長
財團法人國家實驗研究院 正工程師

2022/5/31

推動 ISACA ITAF 國際資訊稽核實務準則
提升資訊風險、控制與安全之確保能力實務研討會

ISACA Taiwan Chapter





ITAF
IT Audit Framework
4th Edition 2020

COBIT An ISACA Framework

COBIT 2019

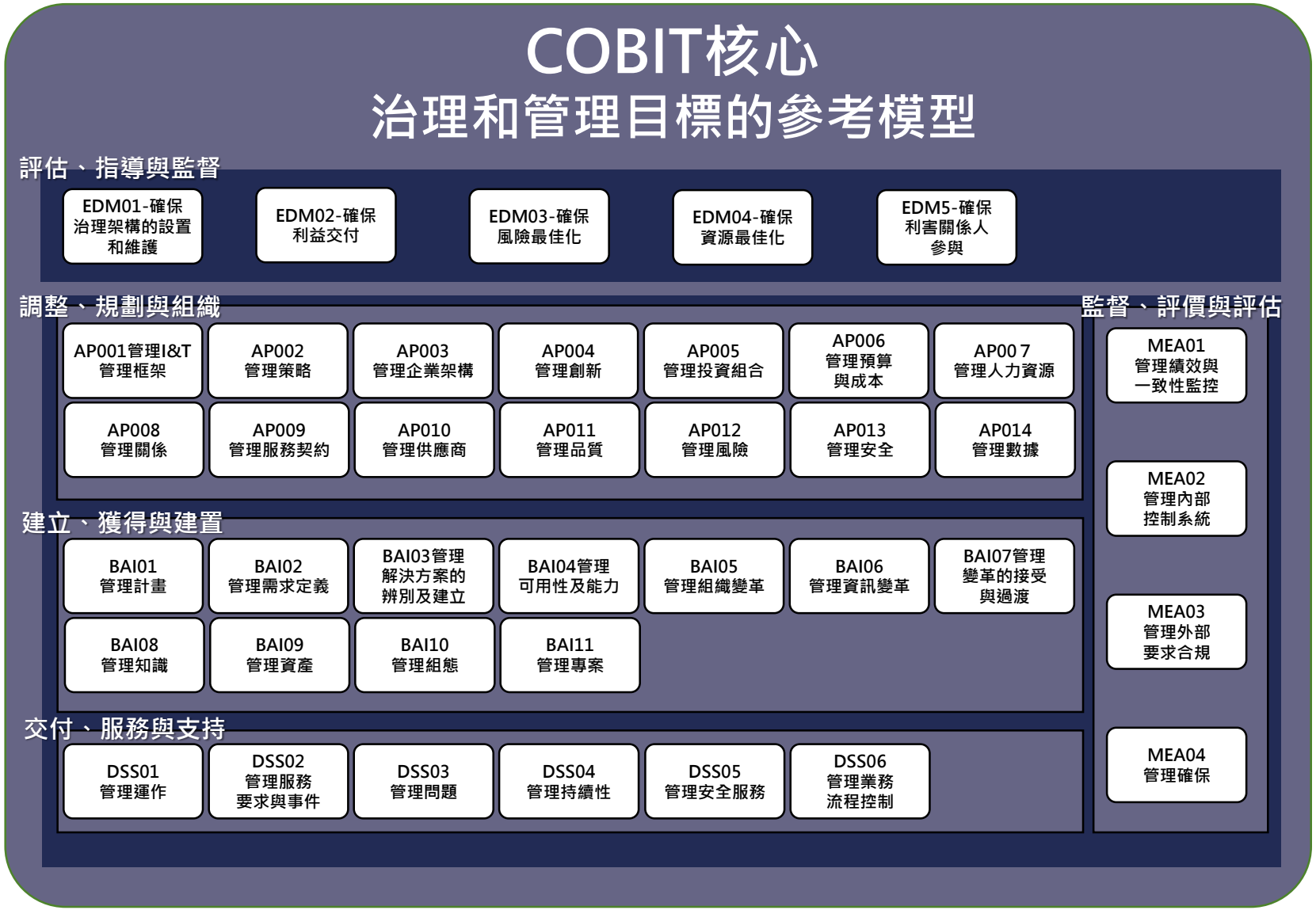
CODE OF PROFESSIONAL ETHICS

ISACA

IT audit engagement management

稽核專案管理

COBIT核心
治理和管理目標的參考模型



COBIT® 2019

COBIT An ISACA Framework

COBIT 2019

ISACA

評估、指導與監督(EDM)

EDM01 Ensure Governance Framework Setting and Maintenance Audit Program | Digital | English

0 Member Pricing

$45.00 Non-member Pricing

EDM02 Ensure Benefits Delivery Audit Program | Digital | English

0 Member Pricing

$45.00 Non-member Pricing

EDM03 Ensure Risk Optimization Audit Program | Digital | English

0 Member Pricing

$45.00 Non-member Pricing

EDM04 Ensure Resource Optimization Audit Program | Digital | English

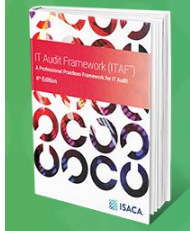
0 Member Pricing

$45.00 Non-member Pricing

EDM05 Ensure Stakeholder Transparency Audit Program | Digital | English

0 Member Pricing

$45.00 Non-member Pricing



ITAF
IT Audit Framework
4th Edition 2020

ISACA

調整、規劃與組織(APO)

APO01 Manage the IT Management Framework Audit Program | Digital | English

0 Member Pricing

$45.00 Non-member Pricing

APO02 Manage Strategy Audit Program | Digital | English

0 Member Pricing

$45.00 Non-member Pricing

APO03 Manage Enterprise Architecture Audit Program | Digital | English

0 Member Pricing

$45.00 Non-member Pricing

APO04 Manage Innovation Audit Program | Digital | English

0 Member Pricing

$45.00 Non-member Pricing

APO05 Manage Portfolio Audit Program | Digital | English

0 Member Pricing

$45.00 Non-member Pricing

APO06 Manage Budget and Costs Audit Program | Digital | English

0 Member Pricing

$45.00 Non-member Pricing

APO07 Manage Human Resources Audit Program | Digital | English

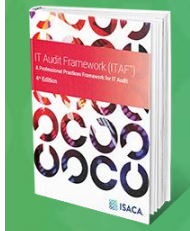
0 Member Pricing

$45.00 Non-member Pricing

APO08 Manage Relationships Audit Program | Digital | English

0 Member Pricing

$45.00 Non-member Pricing



ITAF

IT Audit Framework

4th Edition 2020

ISACA

建立、獲得與建置(BAI)

BAI01 Manage Programs and Projects Audit Program | Digital | English

0 Member Pricing

$45.00 Non-member Pricing

BAI02 Manage Requirements Definition Audit Program | Digital | English

0 Member Pricing

$45.00 Non-member Pricing

BAI03 Manage Solutions Identification and Build Audit Program | Digital | English

0 Member Pricing

$45.00 Non-member Pricing

BAI04 Manage Availability and Capacity Audit Program | Digital | English

0 Member Pricing

$45.00 Non-member Pricing

BAI05 Manage Organizational Change Enablement Audit Program | Digital | English

0 Member Pricing

$45.00 Non-member Pricing

BAI06 Manage Changes Audit Program | Digital | English

0 Member Pricing

$45.00 Non-member Pricing

BAI07 Manage Change Acceptance and Transitioning Audit Program | Digital | English

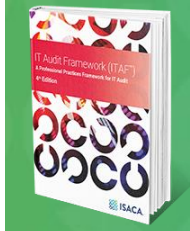
0 Member Pricing

$45.00 Non-member Pricing

BAI08 Manage Knowledge Audit Program | Digital | English

0 Member Pricing

$45.00 Non-member Pricing



ITAF

IT Audit Framework

4th Edition 2020

ISACA

交付、服務與支持(DSS)

DSS01 Manage Operations Audit Program | Digital | English

0 Member Pricing

$45.00 Non-member Pricing

DSS02 Manage Service Requests and Incidents Audit Program | Digital | English

0 Member Pricing

$45.00 Non-member Pricing

DSS03 Manage Problems Audit Program | Digital | English

0 Member Pricing

$45.00 Free Resource

DSS04 Manage Continuity Audit Program | Digital | English

0 Member Pricing

$45.00 Non-member Pricing

DSS05 Manage Security Services Audit Program | Digital | English

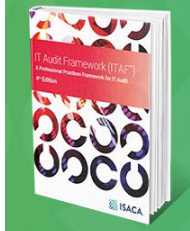
0 Member Pricing

$45.00 Non-member Pricing

DSS06 Manage Business Process Controls Audit Program | Digital | English

0 Member Pricing

$45.00 Non-member Pricing



ITAF

IT Audit Framework

4th Edition 2020

ISACA

國際資訊稽核實務準則
ITAF, 4th Edition

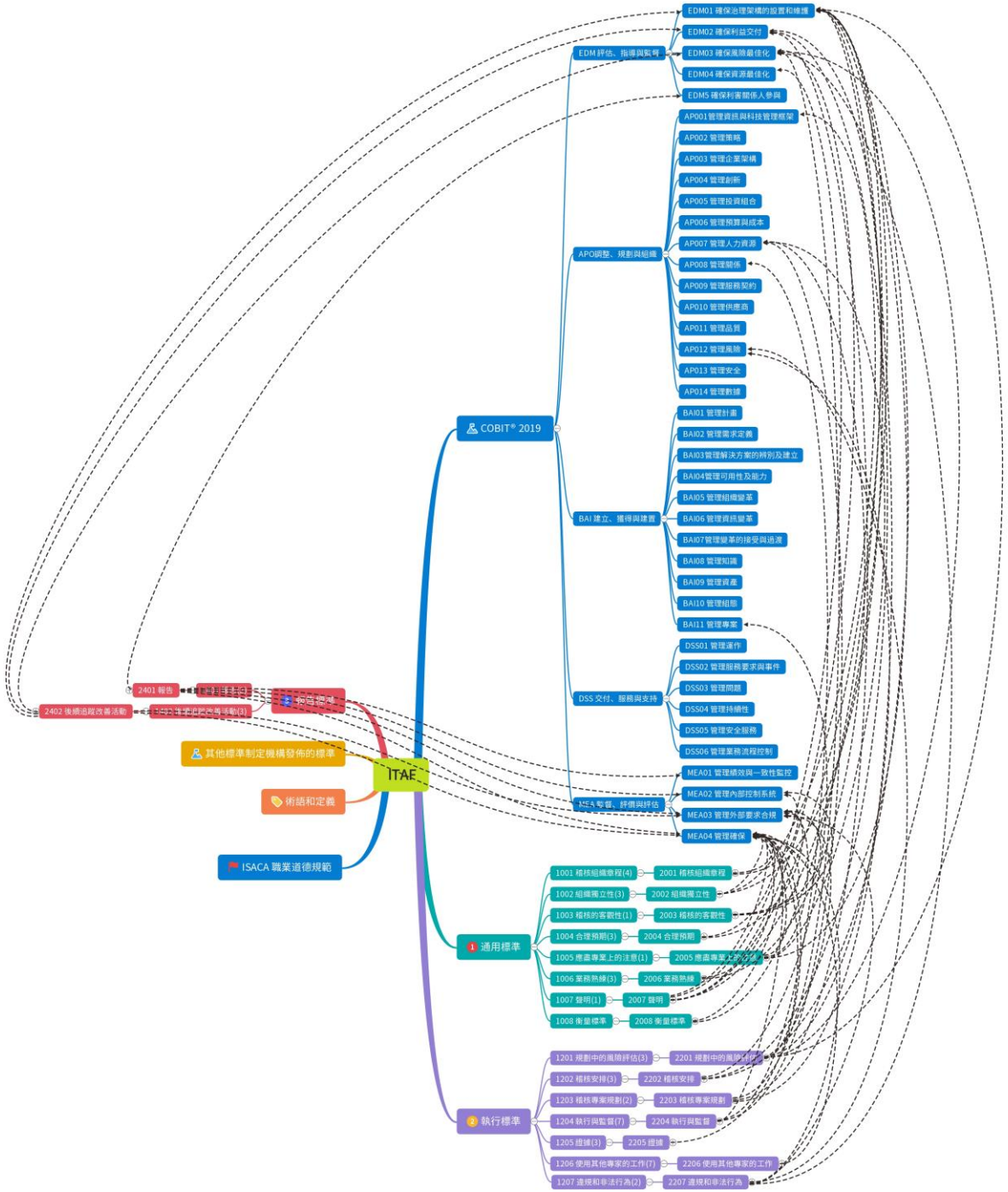
稽核專案管理

- 1001 稽核組織章程
- 1002 組織獨立性
- 1003 稽核的客觀性
- 1004 合理預期
- 1005 應盡專業上的注意
- 1006 業務熟練
- 1007 聲明
- 1008 衡量標準

- 1201 規劃中的風險評估
- 1202 稽核安排
- 1203 稽核專案規劃
- 1204 執行與監督
- 1205 證據
- 1206 使用其他專家的工作
- 1207 違規和非法行為

- 1401 報告
- 1402 追蹤改善活動

ISACA



ITAF

IT Audit Framework

4th Edition 2020

COBIT An ISACA Framework

COBIT 2019

ISACA

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。

- 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。

稽核專案管理

2201.1 簡介

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

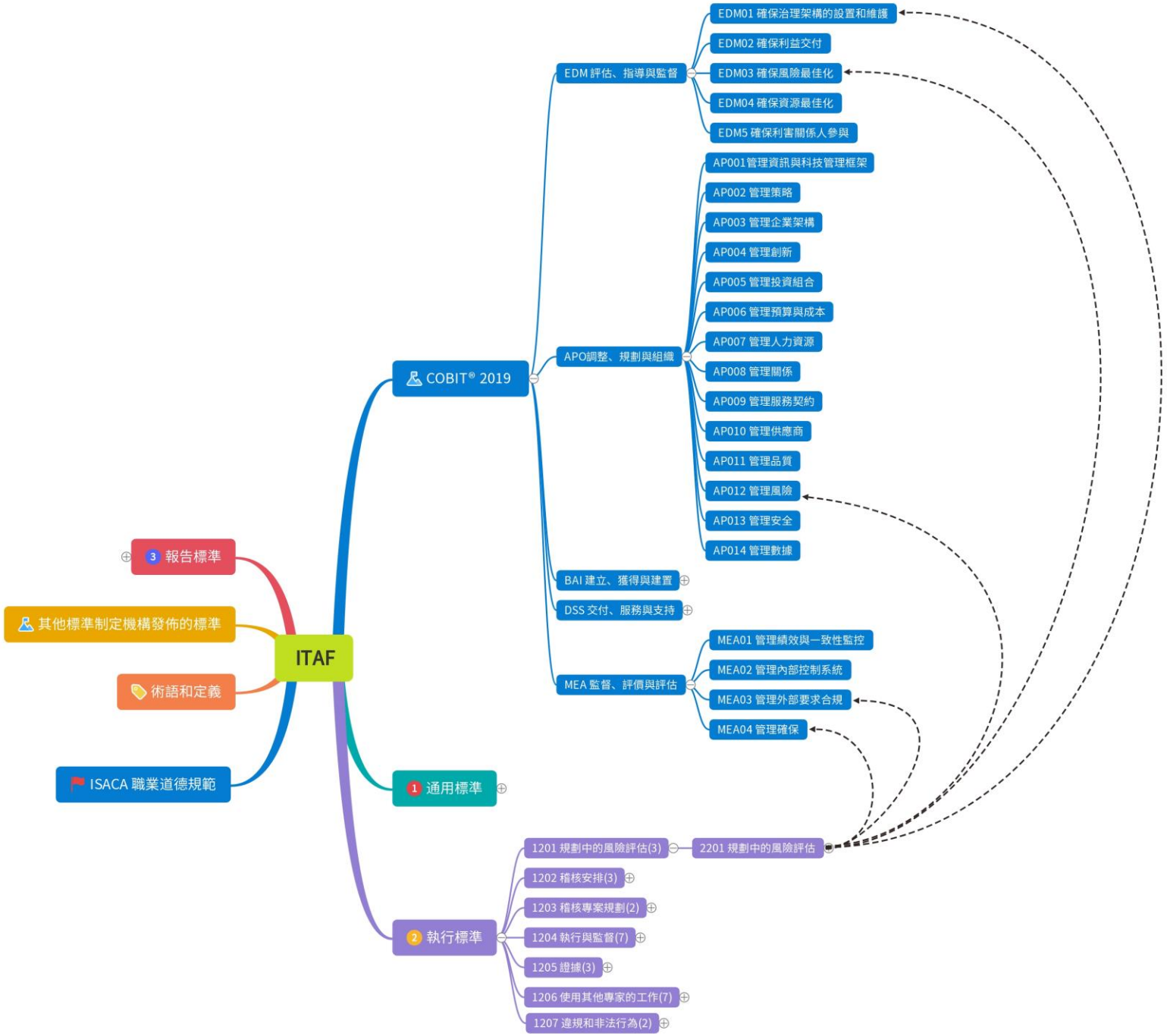
2201.7控制風險

2201.8偵測風險

2201.9其他注意事項

ISACA

稽核專案管理



ISACA®

稽核專案管理

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。

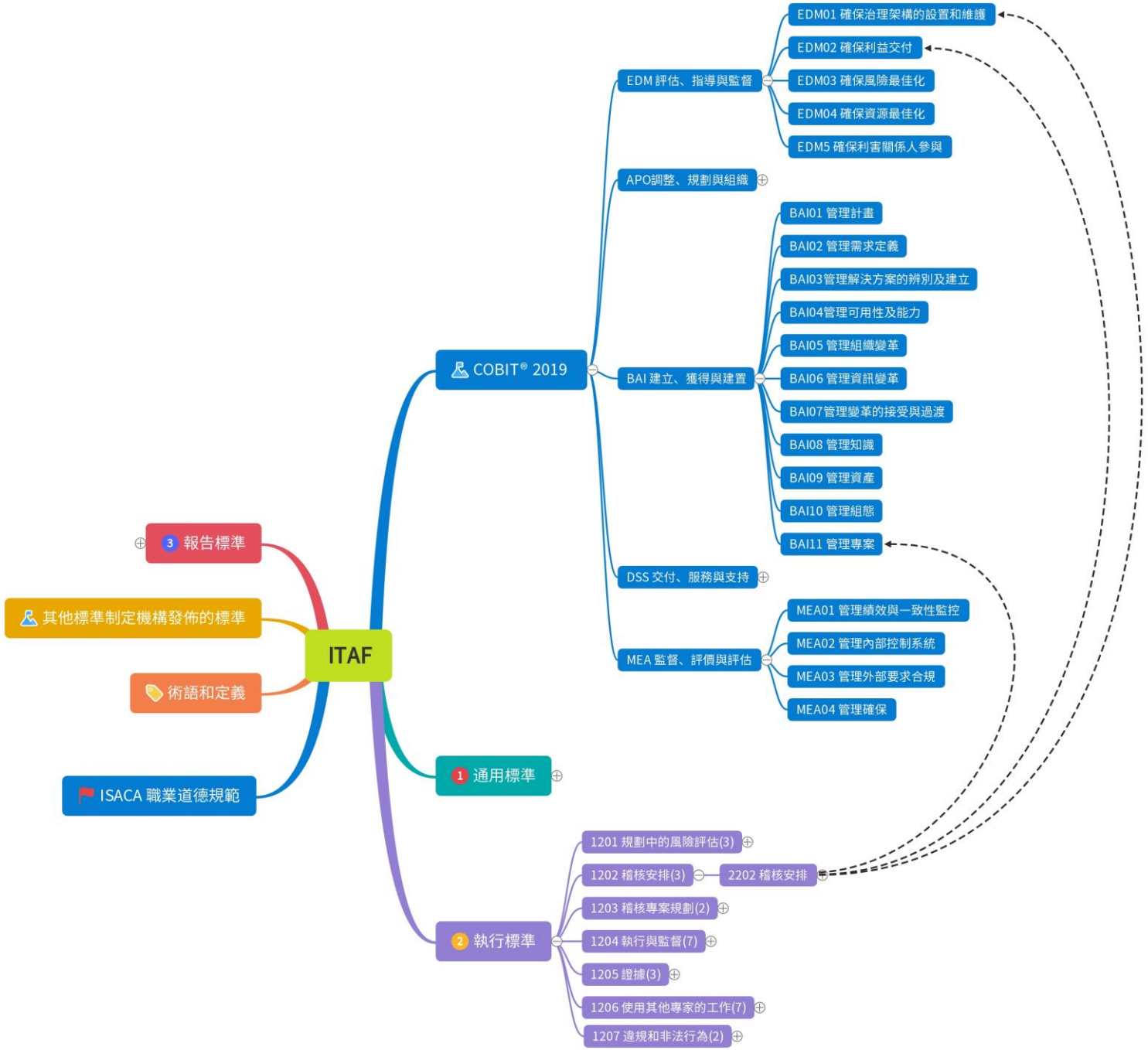
2202.1 簡介

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

ISACA

稽核專案管理



ISACA

稽核專案管理

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。

2203.1 簡介

2203.2目標

2203.3範圍和業務知識

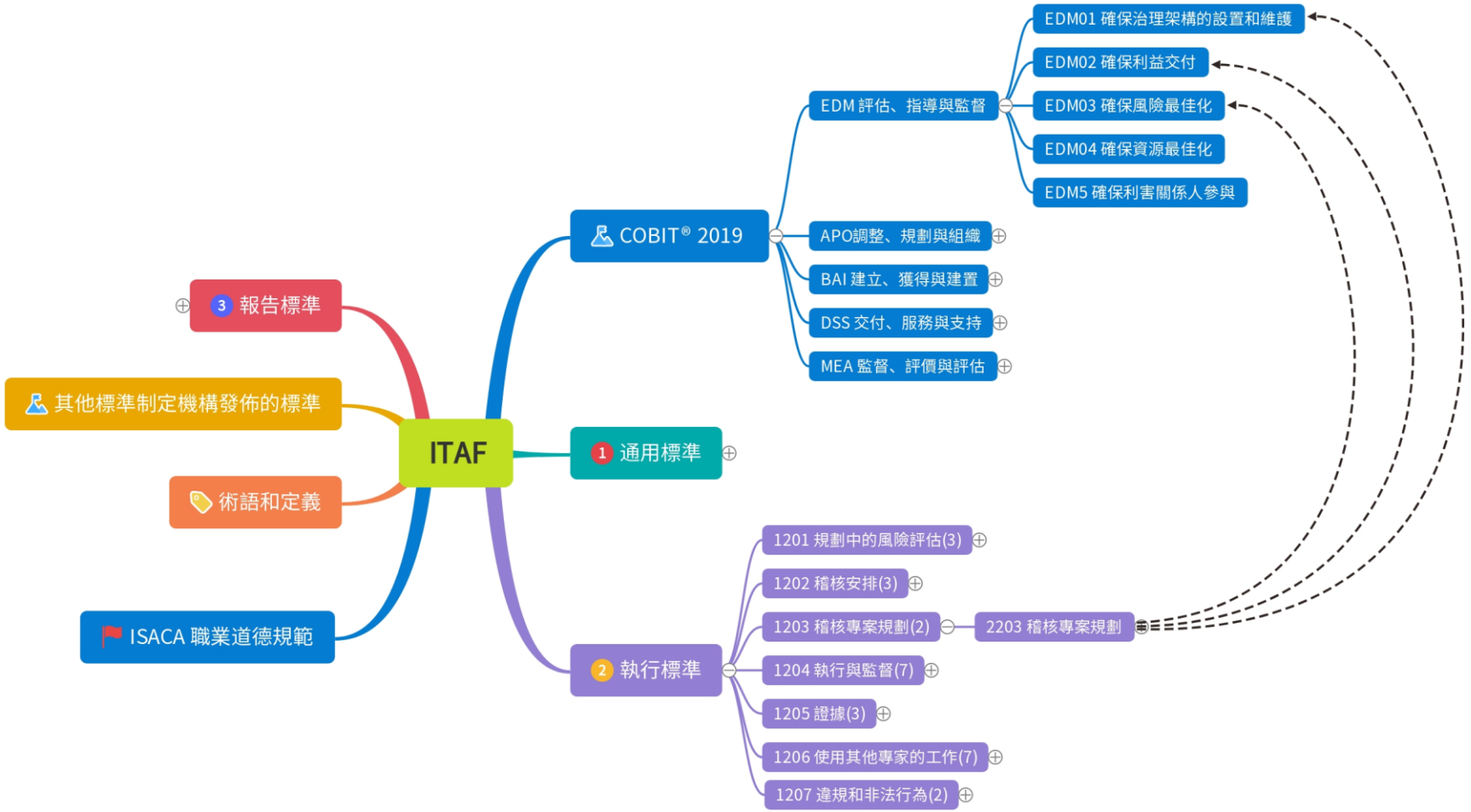
2203.4風險為導向的方法

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

ISACA

稽核專案管理



ISACA

稽核專案管理

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。

2204.1 簡介

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

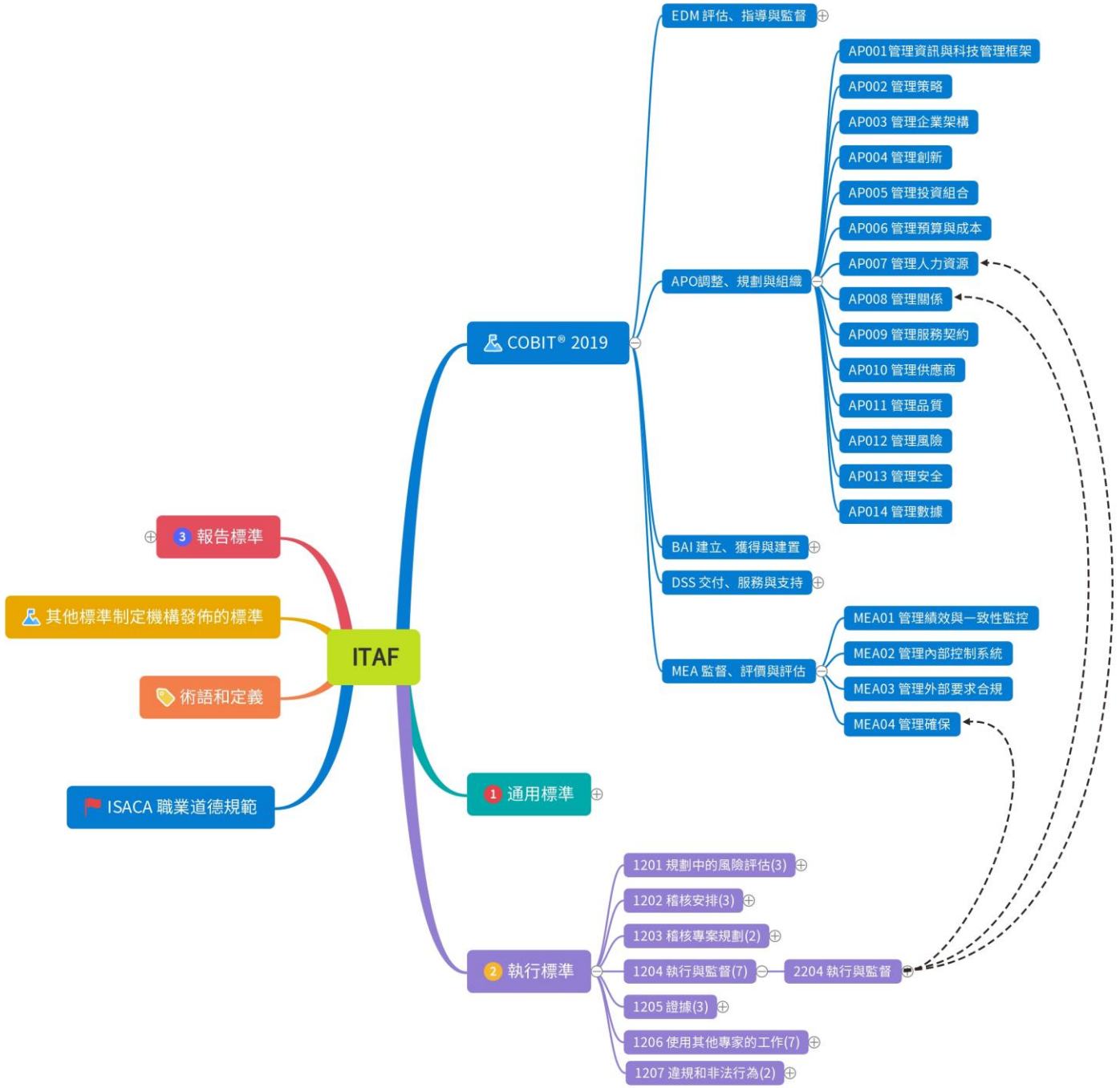
2204.6文件記錄

2204.7查核發現

2204.8其他注意事項

ISACA

稽核專案管理


ITAF
COBIT® 2019
EDM 評估、指導與監督
APO調整、規劃與組織
AP001管理資訊與科技管理框架
AP002 管理策略
AP003 管理企業架構
AP004 管理創新
AP005 管理投資組合
AP006 管理預算與成本
AP007 管理人力資源
AP008 管理關係
AP009 管理服務契約
AP010 管理供應商
AP011 管理品質
AP012 管理風險
AP013 管理安全
AP014 管理數據
BAI 建立、獲得與建置
DSS 交付、服務與支持
MEA 監督、評價與評估
MEA01 管理績效與一致性監控
MEA02 管理內部控制系統
MEA03 管理外部要求合規
MEA04 管理確保
3 報告標準
其他標準制定機構發佈的標準
術語和定義
ISACA 職業道德規範
1 通用標準
2 執行標準
1201 規劃中的風險評估(3)
1202 稽核安排(3)
1203 稽核專案規劃(2)
1204 執行與監督(7)
2204 執行與監督
1205 證據(3)
1206 使用其他專家的工作(7)
1207 違規和非法行為(2)

Enhance the quality of the engagement

資訊稽核品質

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。

2205.1 簡介

2205.2證據類型

2205.3取得證據

2205.4評估證據

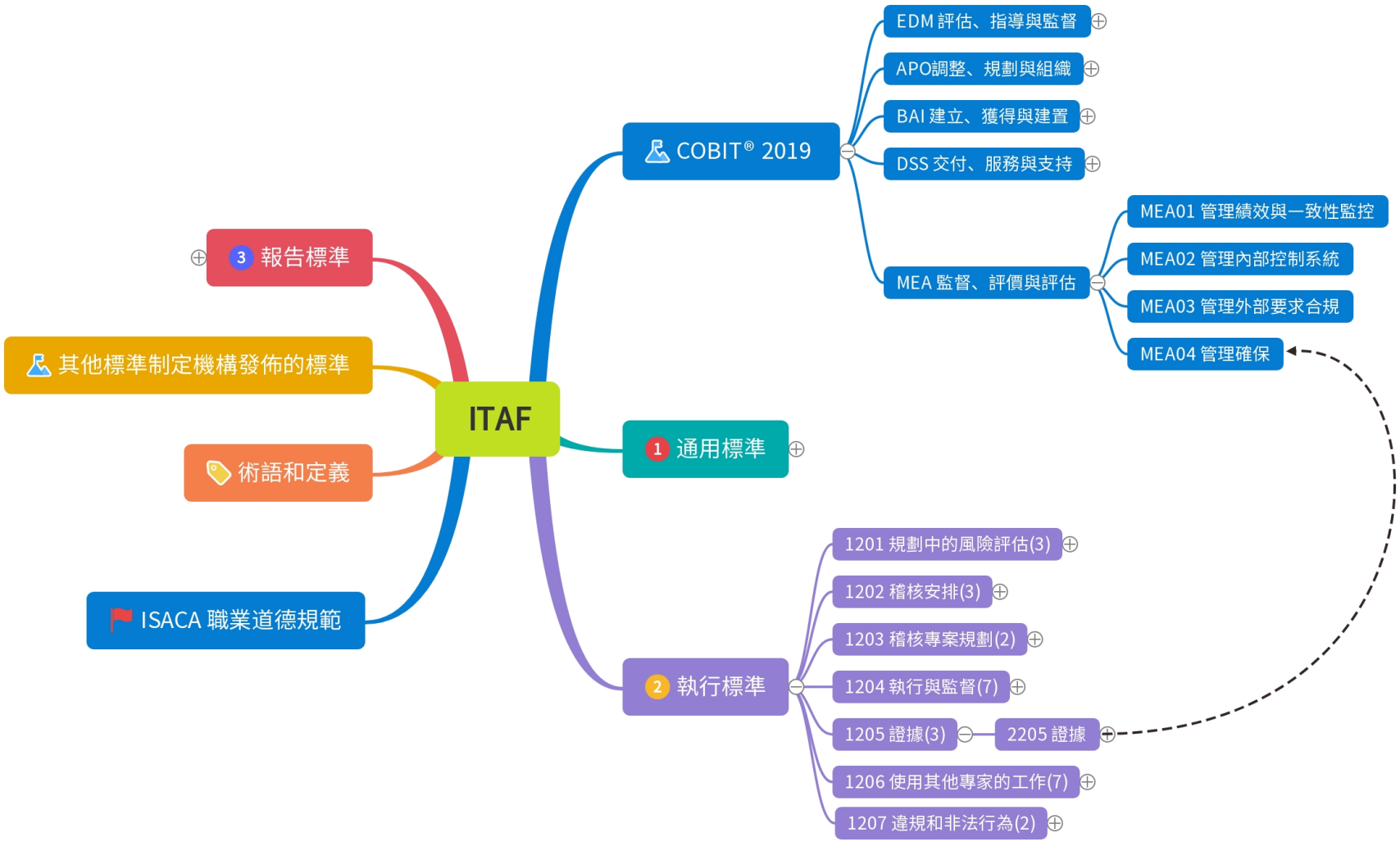
2205.5準備稽核文件

2205.6其他注意事項

資訊稽核品質

ISACA

資訊稽核品質



ISACA

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。

2206.1 簡介

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

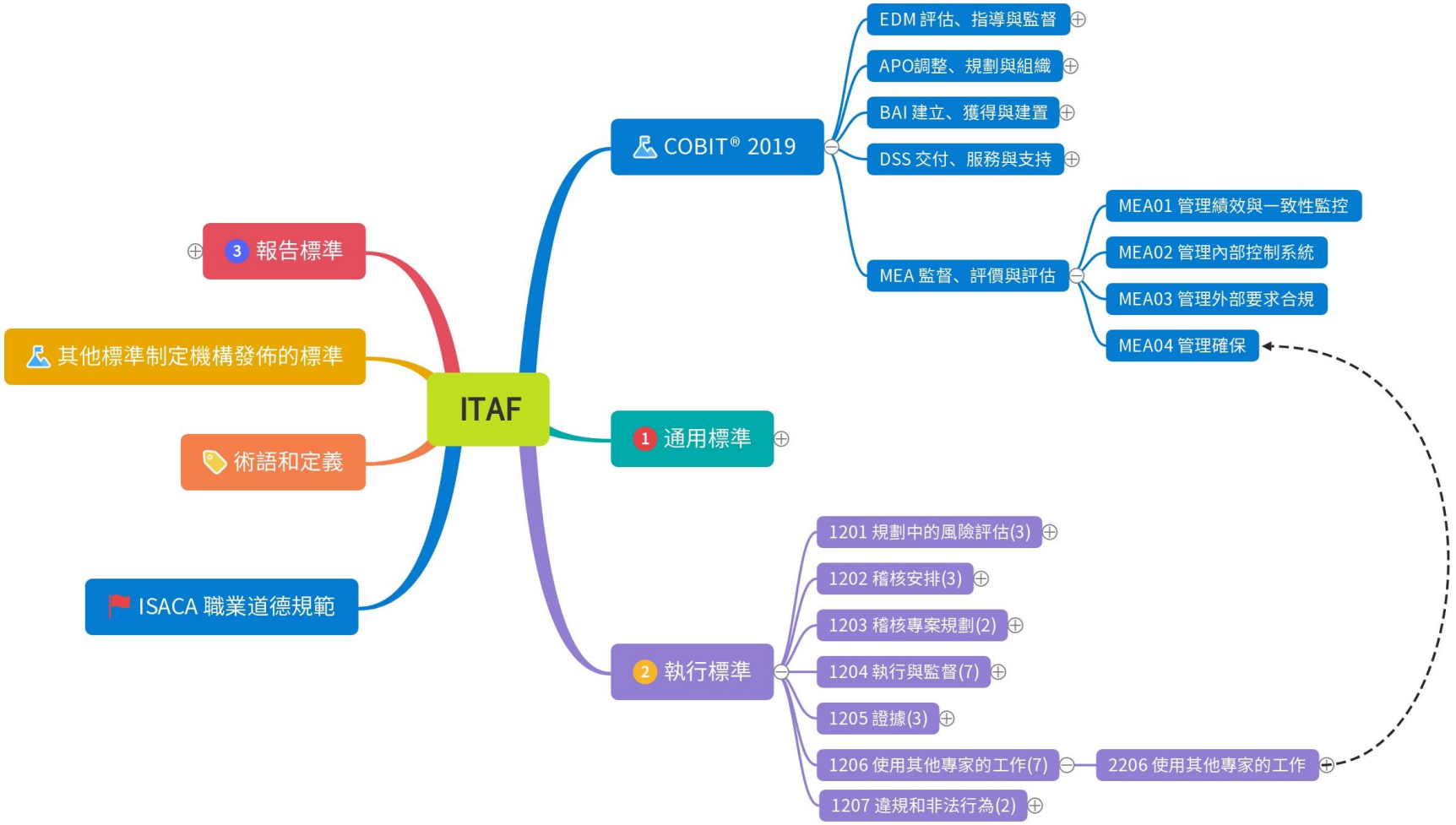
2206.7稽核意見或結論

2206.8其他注意事項

資訊稽核品質

ISACA

資訊稽核品質



ISACA

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。

2207.1 簡介

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

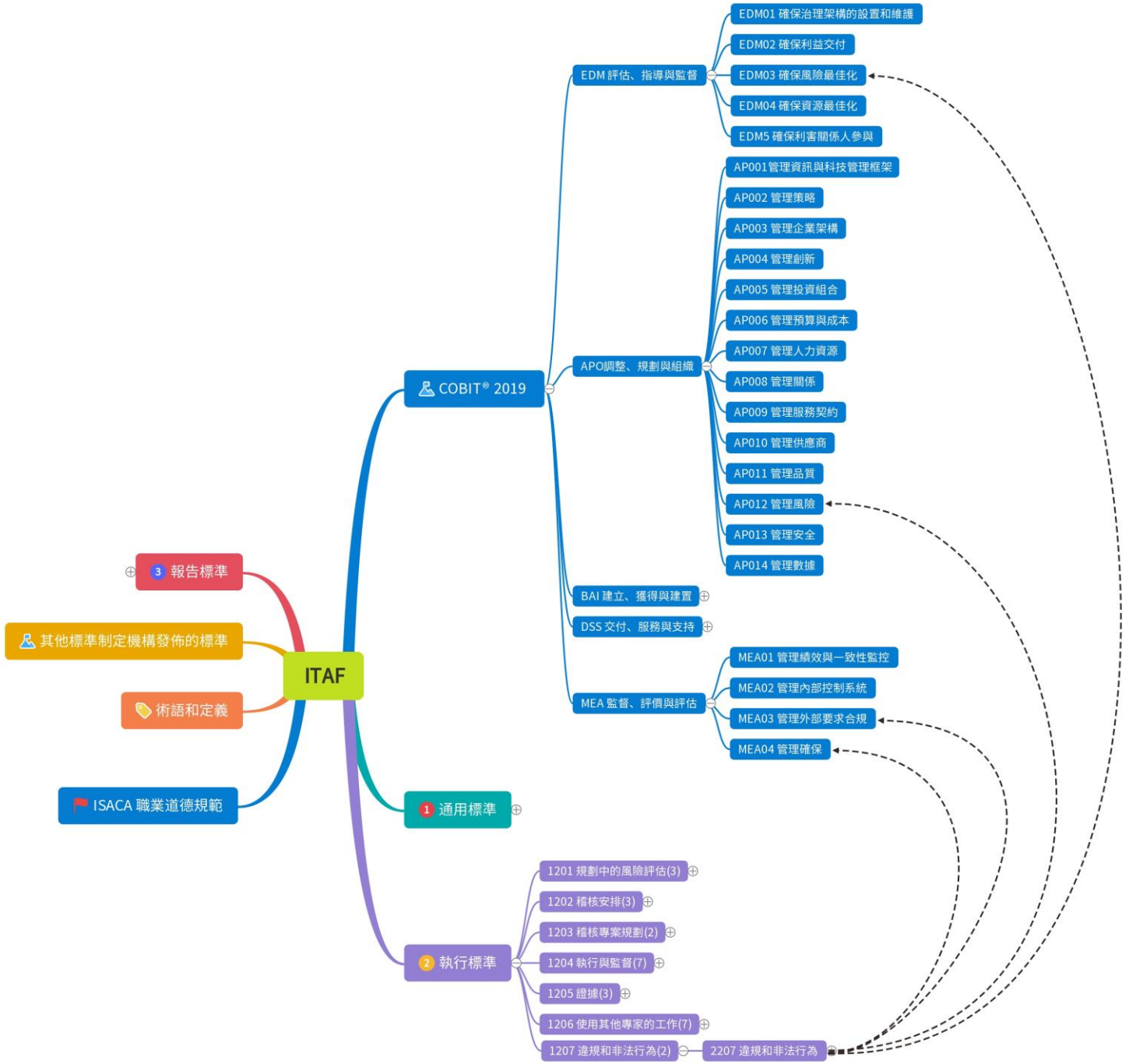
2207.7應對違規和非法行為

2207.8內部報告

2207.9外部報告

2207.10其他注意事項

資訊稽核品質



ISACA

Scope limitations

稽核範圍受限

2005.2專業上的注意和專業能力

稽核範圍受限

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。

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。

執行標準1203：稽核專案規劃

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

ISACA

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。

ISACA®

Taiwan Chapter

連結國際專業組織　提升國家永續競爭力

中華民國電腦稽核協會

11070台北市信義區基隆路一段143號7樓之4

電話：(02)2528-8875

isaca@caa.org.tw

http://www.isaca.org.tw/