根據《電子交易條例》（第 553 章）對核證機關遵守規定進行評估的指引

二零一二年七月公布

(第三版)

香港特別行政區政府

政府資訊科技總監辦公室

本文件的版權屬香港特別行政區政府所有，

未經香港特別行政區政府明確批准，

不得翻印其全部或其中任何部分內容。

引言

1. 本指引(第三版)所載的資訊，並非《認可核證機關業務守則》(“《業務守則》”)的一部分。本指引的目的不是用以影響任何人的權利和義務，也不是供人作法律上的用途而倚據的聲明。若根據本指引內的資訊採取任何法律上的行動，請先自行徵詢法律顧問的意見。本指引(第三版)取代二零零四年七月出版的同一文件第二版。

2. 根據《電子交易條例》（第 553 章）（“《條例》”），評估報告必須於以下情況提交予政府資訊科技總監(“總監”)：

   (a) 按照《條例》第 20(3)(b)條，核證機關在申請認可時，必須向總監提交一份報告，而該報告須載有對該核證機關是否有能力遵守《業務守則》所指明的《條例》及《業務守則》的條文的評估(該等條文在《業務守則》附錄 2 第 1 段指明)；

   (b) 按照《條例》第 27(5A)(b)條，認可核證機關在申請將認可續期時，必須向總監提交一份報告，而該報告須載有對該認可核證機關是否遵守及是否有能力遵守《業務守則》所指明的《條例》及《業務守則》的條文的評估(該等條文在《業務守則》附錄 2 第 1 段指明)；

   (c) 按照《條例》第 43(1)(a)條，認可核證機關必須至少每 12 個月向總監提交報告一次，而該報告須載有對該認可核證機關在該報告所關乎的期間內是否已遵守《業務守則》所指明的《條例》及《業務守則》的條文的評估(該等條文在《業務守則》附錄 2 第 1 段指明)；及

   (d) 按照《條例》第 43A(1)(c)條，總監可就認可核證機關的重大變更，要求該認可核證機關向總監提交一份報告，而該報告須載有對 —

      — 考慮到已發生的重大變更，該認可核證機關是否遵守及是否有能力遵守；或

      — 考慮到將會發生的重大變更，該認可核證機關是否有能力遵守

      《業務守則》所指明的《條例》及《業務守則》的條文的評估(該等條文在《業務守則》附錄 2 第 3 段指明)。

   上述任何報告必須由獲總監認可為合資格作出該報告的人擬備。

3. 本文件就根據《條例》第 20(3)(b)、27(5A)(b)、43(1)(a)或 43A(1)(c)條，規定對有意申請認可或已獲認可的核證機關所作評估的範圍及進行方式，提供指引，以及旨在為下列人士及機關提供參考：

- 《條例》第 20(3)(b)(ii)、27(5A)(b)(ii)、43(1)(a)(ii)或 43A(1)(c)(ii)條所提述，將擬備評估報告的人士；
- 根據《條例》第 27(5A)(b)、43(1)(a)或 43A(1)(c)條必須向總監提交一份載有評估的報告的認可核證機關；及
- 考慮根據《條例》第 20(1)條申請認可的核證機關。

以下各段適用於根據《條例》第 20(3)(b)、27(5A)(b)或 43(1)(a)條規定作出的評估，就根據《條例》第 43A(1)(c)條規定作出的評估而言，評估的範圍視乎認可核證機關將會對或已對其系統、運作、控制及程序作出的重大變更的具體情況而定。以下各段(經考慮到有關評估的範圍而屬相關者)亦適用於根據《條例》第 43A(1)(c)條規定作出的評估。

評估的範圍

4. 評估的目的是為了確定：

- 接受評估的核證機關在各重大方面是否能夠或是否已遵守《條例》及《業務守則》有關條文的規定（視乎所屬情況而定）；及
- 該核證機關在各重大方面是否已依遁在其核證作業準則內所列明的政策及業務運作模式。

5. 評估範圍須包括該核證機關就其是否有能力遵守或實際上已遵守《條例》及《業務守則》的有關條文所作出的聲明。

6. 評估人必須對以下的主要範圍作出評估：

- 了解該核證機關的政策及業務運作模式，並評估有關資訊是否已予以適當披露；
- 評估該核證機關有否遵守關於使用穩當系統以支援其運作的規定；
- 評估該核證機關有否遵守關於按照其核證作業準則及《業務守則》認可證書的規定；及
- 審核有關該核證機關財務預測的特定資訊，以及查證和審核有關該核證機關為其發出的證書所引起的潛在法律責任而作出的保障的特定資訊。

核證機關政策及業務運作模式的披露

7. 評估人須了解該核證機關所訂定的政策及業務運作模式。有關資訊（包括該核證機關所提供或有意提供的服務的細節）應納入該核證機關所發出及備存的核證作業準則內。

8. 若該核證機關採用一項或以上的證書政策，包括與《業務守則》所述證書互認計劃相關的證書政策，評估人亦須了解每一項政策內所列明的規定，以及該政策與核證機關的核證作業準則的關連。評估人須確定核證機關已在該等核證作業準則內適當披露有關其遵守所採用的證書政策的情況。

9. 評估人必須設計及進行所需的適當測試，以評估管理人員所作出的聲明是否合理：該聲明謂有關政策及業務運作模式已按照《條例》、《業務守則》，以及與《業務守則》所述證書互認計劃相關的證書政策（如適用）的規定予以述明及披露。

系統、程序、保安安排和標準的評估

10.《條例》第 37 條規定認可核證機關在提供服務時必須使用穩當系統。接受評估的核證機關必須顯示其系統能充分符合此規定及其他在其核證作業準則所載列的規定。《業務守則》第 5 段就穩當系統的評估提供指引。

11.評估人必須設計及進行所需的適當測試，以評估管理人員所作出的以下聲明是否合理：該聲明謂核證機關在提供服務時已實施及維持穩當系統。

證書生命周期控制的評估

12.核證機關在申請其證書的認可時必須顯示：

- 該等證書是按照該核證機關的核證作業準則及遵照《業務守則》的規定發出的；及
- 該核證機關為保障其法律責任而作出的安排與其業務相符。

13.評估人必須設計及進行所需的適當測試，以評估管理人員所作出的以下聲明是否合理：該聲明謂核證機關已根據《業務守則》及核證機關的核證作業準則對證書的生命周期實施及維持有效的控制。

對遵守與《業務守則》所述證書互認計劃相關的證書政策的評估

14. 核證機關如根據《業務守則》所述的證書互認計劃發出證書或申請根據《業務守則》所述的證書互認計劃發出證書，必須按照該計劃的規定(如該計劃有此規定)，證明有關證書是根據其核證作業準則發出，而該核證作業準則須符合與證書互認計劃相關的證書政策。

15. 在適用情況下，除了上文第 12 和第 13 段所述的測試外，評估人還須設計及進行所需的適當測試，以評估管理人員就核證機關遵守與《業務守則》所述證書互認計劃相關的證書政策所作出的聲明是否合理。

財務預測的審核

16. 評估人必須審核核證機關就其與《條例》有關的運作在未來 12 個月所作的財務預測。在對財務預測進行審核時，評估人須考慮核證機關業務的有關方面，其中包括但不限於：

- 核證機關業務的性質及背景，例如：近期業務情況，以及對其運作可能構成影響的其他有關資料；
- 核證機關一般依循的會計政策，而該等會計政策是否與在香港特別行政區所採用獲廣泛接受的會計原則或國際間廣泛接受的同等會計原則一致，以及該核證機關在編製財務預測時是否貫徹始終地依循這些原則；
- 財務預測所依據的假設，以及該等財務預測是否根據有關假設編製；及
- 核證機關在編製財務預測時所依循的程序。

17. 對未來 12 個月所作的財務預測須包括以每半年為預測單位的現金流量預測及財政狀況預測．

18. 評估人須把以下兩項已向有關核證機關查證的資料加以比較：

(a) 在下文第 19 段指明的日期當日，該核證機關的帳目（包括未經審計的管理帳目）內所示的流動資產淨額；及

(b) 自下文第 19 段指明的同一個日期起計，該核證機關就其與《條例》有關的運作而作出的 90 日營運成本預測。

19. 作為評估核證機關的一部分，評估人必須審核核證機關就其與《條例》有關的運作在未來 12 個月所作的財務預測。核證機關須向總監確認財務預測所

涵蓋的期間。上文第 18 段提述的日期，須與該核證機關就未來 12 個月所作的財務預測的開始日期相同。

20. 對於核證機關的 90 日營運成本預測，評估人須考慮：

- 該預測所依據的會計政策，是否在各重大方面均與該核證機關一般採用的政策一致，以及是否符合在香港特別行政區所採用獲廣泛接受的會計原則或國際間廣泛接受的同等會計原則；及

- 該預測在各重大方面是否按照該核證機關所作出的假設適當地編製。如評估人根據其經驗及專業判斷，以及根據該核證機關最新的經審計財政報告內所披露的資料（如適用），認為該核證機關所作出的或沒有作出的假設不切實際或不適當，則評估人須在評估報告中作出適當的評論。

21. 第 18 段提述的流動資產淨額應指經扣除流動負債的流動資產的價值。

潛在法律責任的查證

22. 根據核證機關提供的資訊，評估人須查證核證機關所制訂的安排，該等安排是用以判斷及管理與其已發出或計劃發出的認可證書有關的潛在法律責任，其中包括：

- 因核證機關、其高級人員、僱員或代理人的錯誤或不作為而引起的潛在申索；及

- 因其證書所指明的倚據限額而引起的潛在法律責任。

23. 凡有意申請認可的核證機關尚未開始運作，其潛在的法律責任將以其預算會在未來 12 個月內發出的證書的數目作為計算基礎。

24. 為第 22 段的目的，評估人須執行適當的程序，以：

- 查證截至進行審核時核證機關就與已發出的證書有關的潛在法律責任而作出的保險安排（或其他適當形式的保障）的細節，並執行適當的程序以評估核證機關有否遵守《業務守則》第 8.2 至 8.4 段關於為法律責任投保的規定；

- 查證自上次評估以來，核證機關有否收到登記人及／或倚據人士提出的申索，及該等申索的情況；及

- 查證自上次評估以來，是否有申索針對有關保險單而提出。

報告

25. 評估人須就評估的結果和評估所得為核證機關擬備一份正式的書面報告。評估人須在報告中清楚述明與核證機關議定並在評估時採用的程序，及評估所得，包括重大的不正常情況的詳情，例如：沒有遵守《條例》或《業務守則》中有關條文的事件。

26. 評估人必須提出意見，指出接受評估的核證機關的管理人員所作出的聲明是否合理，該聲明是有關該核證機關在各重大方面是否有能力遵守（或有否實際遵守）《條例》及《業務守則》的有關條文。評估人在提出意見前，須特別考慮以下事項：

- 該核證機關有否按照《條例》及《業務守則》的有關條文，在其核證作業準則內披露其業務運作模式，以及有否按照這些業務運作模式提供服務；

- 該核證機關有否按照《條例》及《業務守則》的有關條文，採用穩當系統以支援其運作；及

- 該核證機關有否按照《條例》及《業務守則》的有關條文，遵守與認可其證書有關的規定，包括密碼匙和證書生命周期的管理。

27. 在適用情況下，評估人必須提出意見，指出接受評估的核證機關的管理人員就以下兩項所作出的聲明是否合理：

- 核證機關的核證作業準則在各重大方面是否符合與《業務守則》所述證書互認計劃相關的證書政策內的有關規定；以及

- 核證機關在各重大方面是否有能力遵守或已實際遵守與《業務守則》所述證書互認計劃相關的證書政策內的有關規定。

28. 評估人須就核證機關的財務預測方面，述明下列事項：

- 財務預測所涵蓋的期間；

- 財務預測所依據的會計政策，是否在各重大方面與該核證機關一般採用的政策一致，以及是否符合在香港特別行政區所採用獲廣泛接受的會計原則或國際間廣泛接受的同等會計原則；及

- 財務預測在各重大方面是否按照核證機關所作出的假設適當地編製。如評估人根據其經驗及專業判斷，以及根據核證機關公司最新的經審計財政報告內所披露的資料(如適用)，認為核證機關所作出的或沒有作出的假設不切實際或不適當，則評估人應在評估報告中作出適當的評論。

29. 除按照第 28 段載列的項目作出報告外，評估人亦須提出第 18 段載列的比較結果，以及述明就有關第 20 段的考慮結果所作的評論。從核證機關查證所得的該核證機關的帳目及 90 日營運成本預測（即第 18 段所提述的兩項資料），須以附錄的形式附於評估報告。

30. 評估人須就核證機關對其潛在法律責任的管理提出意見，以指出核證機關所作出的以下聲明是否合理：該聲明謂其已採取及維持適當措施，以判斷及管理其潛在法律責任。

31. 評估人必須就其執行第 24 段所載列的程序時所收集的資訊作出查證及報告。資訊的範圍包括（1）核證機關的潛在法律責任；（2）對法律責任所作的保險安排或其他適當形式的保障；及（3）核證機關所收到的申索或針對核證機關保險單提出的申索。

32. 除按照第 31 段所載的項目作出報告外，評估人亦須就執行有關程序以評估核證機關有否遵守《業務守則》第 8.2 至 8.4 段一事所得的結果作出報告。

對內部審計工作的倚據

33. 評估人在適當的情況下，須考慮核證機關內部審計工作的可依賴程度，以修訂評估人所進行的評估工作的性質、時間及範圍。如計劃倚據內部審計工作，評估人須考慮：

- 內部審計工作的效能和客觀性；
- 內部審計工作對接受評估的特定核證工作所涵蓋的範圍；及
- 就發現的問題作出的跟進和解決該等問題的進度。

評估的進行

34. 評估人須按照其所屬的專業機構或協會就進行該等評估工作所訂立的有關標準及守則（如適用），進行評估工作。

35. 評估人須根據每一方面的評估工作所得結果，考慮任何不正常情況或不足之處的嚴重性。

36. 評估人須設計及進行測試，以核實核證機關在其核證作業準則及相關的證書政策內所列載的有關規定，是否已在核證機關的運作、技術及/或文件中獲得充分反映。評估人所進行的測試應包括：

- 分析所獲得的資訊；

- 重複計算、比較及其他準確度的核對；
- 觀察核證機關的運作；
- 查閱有關的文件及紀錄；及
- 評估人認為適當的其他測試，如核對系統設置、尋求確認等。

37. 除上述問題外，評估人亦須運用其專業判斷以決定評估過程中所採用的測試程序的性質、時間和範圍。

參考

38. 在評估核證機關有否遵守規定時，評估人必須考慮適用於核證機關運作的獲廣泛採納的監控原則。在這方面現有的相關資料包括：

- Institute of Internal Auditors' Systems Auditability and Control Report；
- Information Systems Audit and Control Association and Foundation, Control Objectives for Information and Related Technology (CobiT)；
- ANSI (American National Standards Institute) X9.79-2001, Financial Services Public Key Infrastructure (PKI) Policy and Practices Framework；
- AICPA/CICA CATrust Principles and Criteria；
- Evaluation Criteria for Information Technology Security (Common Criteria)；
- IETF PKIX Drafts and Requests for Comment；及
- CSPP – Guidance for COTS Protection Profiles (原為：CS2 – Protection Profile Guidance for Near-term COTS), National Institutes of Standards and Technology, Department of Commerce, USA.