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

二零零零年一月公布

香港特別行政區政府

引言

1 本指引所載的資訊，並非《認可核證機關業務守則》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。

2 《電子交易條例》（第 553 章）（「條例」）第 20（3）（b）條要求核證機關在申請認可時，必須向資訊科技署署長（「署長」）提交一份由一位獲署長接納為合資格擬備報告的人士所擬備的報告。該報告須評估核證機關是否有能力遵守條例中適用於認可核證機關的條文和《認可核證機關業務守則》（「業務守則」）。根據條例第 43（1）及（2）條，認可核證機關必須最少每 12 個月向署長提交報告一次，該報告須載有對該核證機關在報告涵蓋的期間內有否遵守條例中適用於認可核證機關的條文的評估，及在該期間是已遵守業務守則的評估。該報告必須由署長認可為合資格擬備該報告的人士擬備。

3 本文件為根據條例第 20（3）（b）條及第 43（2）條要求，有意申請或已獲認可的核證機關遵守規定的評估的範圍及進行提供指引，及旨在為下列人士提供參考：

- 條例第 20（3）（b）（ii）條及第 43（2）條所提述，將擬備評估報告的人士；
- 根據條例第 43（1）條必須向署長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。

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有關條文及業務守則的規定（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有關條文及業務守則所作出的聲明。

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，並評估這些資訊是否已作出適當的披露；
- 評估該核證機關是否符合關於使用穩當系統以支援其運作的規定；
- 評估該核證機關是否根據其核證作業準則及業務守則運作，以符合有關證書認可的規定；及
- 審核有關該核證機關財政預測的特定資訊，及有關該核證機關為其發出的證書所產生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 評估人應了解該核證機關所訂定的政策及業務運作模式。該等資訊（包括該核證機關所提供或有意提供的服務的細節）應載列在該核證機關發出及備存的核證作業準則內。

8 若該核證機關採用一個或以上的證書政策，評估人亦須了解每一個政策內所載列的規定。

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，該聲明關於其已根據條例及業務守則的規定述明及披露其政策及業務運作模式。

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要求。業務守則第 5 段就評估穩當系統提供指引。

11 評估人必須設計及進行所需的適當測試，以評估管理人員就其已實施及維持穩當系統來提供服務所作出的聲明是否合理。

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：

- 該等證書是根據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聲明是否合理，該聲明是關於證書的生命周期已根據業務守則及核證機關的核證作業準則實施及維持有效的控制。

財政預測的審核

14 評估人必須審核核證機關就其與條例有關的業務在未來 12 個月所作的財務預測。在進行審核時，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採用的或國際廣泛接受的會計原則一致，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。

15 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.

潛在法律責任的審核

16 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，以判斷及管理因其已發出或計劃發出的已獲及未獲認可的證書所可能引致的法律責任，其中包括：

- 因核證機關、其職員、員工或代理人的過失或失責所引致的潛在索償；及

- 與其證書所指明的倚據限額有關的潛在法律責任。

17 凡未開始運作而有意申請認可的核證機關，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。

18 此外，評估人須按照第 16 段的規定執行適當的程序，以：

- 查證就已發出的證書而導致的潛在法律責任而作出的保險安排（或其他保障）的細節；

- 查證自上次評估以來，核證機關有否遭受登記人及／或倚據人士索償，及該等索償的情況；及

- 查證自上次評估以來，核證機關有否提出保險索償。

報告

19 評估人須就評估結果和發現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指出與核證機關議定並在評估時採用的程序，及評估的發現，包括重大的不正常情況的詳情，例如：不能遵守條例中有關條文或業務守則的事件。

20 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）條例有關的條文及業務守則。評估人在提出意見前，須特別考慮以下事項：

- 該核證機關有否根據條例有關條文及業務守則的規定，在其核證作業準則內披露其業務運作模式，及有否根據這些業務運作模式提供服務；

- 該核證機關有否根據條例及業務守則的規定，採用穩當的系統來提供服務；及

- 該核證機關有否根據條例及業務守則，依從就認可其證書的有關規定，包括密碼匙和證書生命周期的管理。

21 評估人須就核證機關的財務預測方面，述明下列事項：

- 財務預測所涵蓋的時段；

- 財務預測所依據的會計政策在各重大方面與該核證機關一般採用的及在香港或國際廣泛接受的會計原則一致；及

- 財務預測在各重大方面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，認為核證機關所作出的或未能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。

22 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聲明是否合理，該聲明是有關其已採取及維持有效措施，以判斷及管理其潛在法律責任。

23 評估人必須就其執行第 18 段所載列的程序時所收集的資料作出確認及匯報。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或其他適當形式的保障、（3）向核證機關提出的索償或核證機關作出的保險索償。

對內部審計工作的倚據

24 評估人員在適當的情況下，應考慮核證機關內部審計工作的可依賴程度，以修訂評估工作的性質、時間及程度。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

25 評估人須依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。

26 評估人須根據每一個評估方面的結果，考慮任何不正常情況或不足之處的嚴重性。

27 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。

28 除上述問題外，評估人亦須運用其專業判斷以決定評估的性質、時間和所採用的測試程序的程度。

參考

29 **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) ASC draft X9.79 standard, PKI Policies and Practices Framework（**包括規範附件** Certification Authority Control Objectives）；
- AICPA/CICA CATrust Principles and Criteria；
- Evaluation Criteria for Information Technology Security (Common Criteria)；
- IETF PKIX Drafts and Requests for Comment；**及**
- CS2 – Protection Profile Guidance for Near-term COTS, National Institue of Standards and Technology, Department of Commerce, USA.