# 根据《电子交易条例》（第 553 章）对核证机关遵守规定进行评估的指引

二零一二年七月公布

(第三版)

香港特别行政区政府

政府资讯科技总监办公室

## 引言

1. 本指引(第三版)所载的资讯，并非《认可核证机关业务守则》(“《业务守则》”)的一部分。本指引的目的不是用以影响任何人的权利和义务，也不是供人作法律上的用途而倚据的声明。若根据本指引内的资讯采取任何法律上的行动，请先自行征询法律顾问的意见。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. 根据《电子交易条例》（第 553 章）（“《条例》”），评估报告必须于以下情况提交予政府资讯科技总监(“总监”)：

   (a) 按照《条例》第 20(3)(b)条，核证机关在申请认可时，必须向总监提交一份报告，而该报告须载有对该核证机关是否有能力遵守《业务守则》所指明的《条例》及《业务守则》的条文的评估(该等条文在《业务守则》附录 2 第 1 段指明)；

   (b) 按照《条例》第 27(5A)(b)条，认可核证机关在申请将认可续期时，必须向总监提交一份报告，而该报告须载有对该认可核证机关是否遵守及是否有能力遵守《业务守则》所指明的《条例》及《业务守则》的条文的评估(该等条文在《业务守则》附录 2 第 1 段指明)；

   (c) 按照《条例》第 43(1)(a)条，认可核证机关必须至少每 12 个月向总监提交报告一次，而该报告须载有对该认可核证机关在该报告所关乎的期间内是否已遵守《业务守则》所指明的《条例》及《业务守则》的条文的评估(该等条文在《业务守则》附录 2 第 1 段指明)；及

   (d) 按照《条例》第 43A(1)(c)条，总监可就认可核证机关的重大变更，要求该认可核证机关向总监提交一份报告，而该报告须载有对 —

      — 考虑到已发生的重大变更，该认可核证机关是否遵守及是否有能力遵守；或

      — 考虑到将会发生的重大变更，该认可核证机关是否有能力遵守

      《业务守则》所指明的《条例》及《业务守则》的条文的评估(该等条文在《业务守则》附录 2 第 3 段指明)。

   上述任何报告必须由获总监认可为合资格作出该报告的人拟备。

3. 本文件就根据《条例》第 20(3)(b)、27(5A)(b)、43(1)(a)或 43A(1)(c)条，规定对有意申请认可或已获认可的核证机关所作评估的范围及进行方式，提供指引，以及旨在为下列人士及机关提供参考：

- 《条例》第 20(3)(b)(ii)、27(5A)(b)(ii)、43(1)(a)(ii)或 43A(1)(c)(ii)条所提述，将拟备评估报告的人士；
- 根据《条例》第 27(5A)(b)、43(1)(a)或 43A(1)(c)条必须向总监提交一份载有评估的报告的认可核证机关；及
- 考虑根据《条例》第 20(1)条申请认可的核证机关。

以下各段适用于根据《条例》第 20(3)(b)、27(5A)(b)或 43(1)(a)条规定作出的评估，就根据《条例》第 43A(1)(c)条规定作出的评估而言，评估的范围视乎认可核证机关将会对或已对其系统、运作、控制及程序作出的重大变更的具体情况而定。以下各段(经考虑到有关评估的范围而属相关者)亦适用于根据《条例》第 43A(1)(c)条规定作出的评估。

## 评估的范围

4. 评估的目的是为了确定：

- 接受评估的核证机关在各重大方面是否能够或是否已遵守《条例》及《业务守则》有关条文的规定（视乎所属情况而定）；及
- 该核证机关在各重大方面是否已依遁在其核证作业准则内所列明的政策及业务运作模式。

5. 评估范围须包括该核证机关就其是否有能力遵守或实际上已遵守《条例》及《业务守则》的有关条文所作出的声明。

6. 评估人必须对以下的主要范围作出评估：

- 了解该核证机关的政策及业务运作模式，并评估有关资讯是否已予以适当披露；
- 评估该核证机关有否遵守关于使用稳当系统以支援其运作的规定；
- 评估该核证机关有否遵守关于按照其核证作业准则及《业务守则》认可证书的规定；及
- 审核有关该核证机关财务预测的特定资讯，以及查证和审核有关该核证机关为其发出的证书所引起的潜在法律责任而作出的保障的特定资讯。

## 核证机关政策及业务运作模式的披露

7. 评估人须了解该核证机关所订定的政策及业务运作模式。有关资讯（包括该核证机关所提供或有意提供的服务的细节）应纳入该核证机关所发出及备存的核证作业准则内。

8. 若该核证机关采用一项或以上的证书政策，包括与《业务守则》所述证书互认计划相关的证书政策，评估人亦须了解每一项政策内所列明的规定，以及该政策与核证机关的核证作业准则的关连。评估人须确定核证机关已在该等核证作业准则内适当披露有关其遵守所采用的证书政策的情况。

9. 评估人必须设计及进行所需的适当测试，以评估管理人员所作出的声明是否合理：该声明谓有关政策及业务运作模式已按照《条例》、《业务守则》，以及与《业务守则》所述证书互认计划相关的证书政策（如适用）的规定予以述明及披露。

## 系统、程序、保安安排和标准的评估

10. 《条例》第 37 条规定认可核证机关在提供服务时必须使用稳当系统。接受评估的核证机关必须显示其系统能充分符合此规定及其他在其核证作业准则所载列的规定。《业务守则》第 5 段就稳当系统的评估提供指引。

11. 评估人必须设计及进行所需的适当测试，以评估管理人员所作出的以下声明是否合理：该声明谓核证机关在提供服务时已实施及维持稳当系统。

## 证书生命周期控制的评估

12. 核证机关在申请其证书的认可时必须显示：

- 该等证书是按照该核证机关的核证作业准则及遵照《业务守则》的规定发出的；及
- 该核证机关为保障其法律责任而作出的安排与其业务相符。

13. 评估人必须设计及进行所需的适当测试，以评估管理人员所作出的以下声明是否合理：该声明谓核证机关已根据《业务守则》及核证机关的核证作业准则对证书的生命周期实施及维持有效的控制。

## 对遵守与《业务守则》所述证书互认计划相关的证书政策的评估

14. 核证机关如根据《业务守则》所述的证书互认计划发出证书或申请根据《业务守则》所述的证书互认计划发出证书，必须按照该计划的规定(如该计划有此规定)，证明有关证书是根据其核证作业准则发出，而该核证作业准则须符合与证书互认计划相关的证书政策。

15. 在适用情况下，除了上文第 12 和第 13 段所述的测试外，评估人还须设计及进行所需的适当测试，以评估管理人员就核证机关遵守与《业务守则》所述证书互认计划相关的证书政策所作出的声明是否合理。

## 财务预测的审核

16. 评估人必须审核核证机关就其与《条例》有关的运作在未来 12 个月所作的财务预测。在对财务预测进行审核时，评估人须考虑核证机关业务的有关方面，其中包括但不限于：

- 核证机关业务的性质及背景，例如：近期业务情况，以及对其运作可能构成影响的其他有关资料；
- 核证机关一般依循的会计政策，而该等会计政策是否与在香港特别行政区所采用获广泛接受的会计原则或国际间广泛接受的同等会计原则一致，以及该核证机关在编制财务预测时是否贯彻始终地依循这些原则；
- 财务预测所依据的假设，以及该等财务预测是否根据有关假设编制；及
- 核证机关在编制财务预测时所依循的程序。

17. 对未来 12 个月所作的财务预测须包括以每半年为预测单位的现金流量预测及财政状况预测.

18. 评估人须把以下两项已向有关核证机关查证的资料加以比较：

(a) 在下文第 19 段指明的日期当日，该核证机关的账目（包括未经审计的管理账目）内所示的流动资产净额；及

(b) 自下文第 19 段指明的同一个日期起计，该核证机关就其与《条例》有关的运作而作出的 90 日营运成本预测。

19. 作为评估核证机关的一部分，评估人必须审核核证机关就其与《条例》有关的运作在未来 12 个月所作的财务预测。核证机关须向总监确认财务预测所

涵盖的期间。上文第 18 段提述的日期，须与该核证机关就未来 12 个月所作的财务预测的开始日期相同。

20. 对于核证机关的 90 日营运成本预测，评估人须考虑：

- 该预测所依据的会计政策，是否在各重大方面均与该核证机关一般采用的政策一致，以及是否符合在香港特别行政区所采用获广泛接受的会计原则或国际间广泛接受的同等会计原则；及

- 该预测在各重大方面是否按照该核证机关所作出的假设适当地编制。如评估人根据其经验及专业判断，以及根据该核证机关最新的经审计财政报告内所披露的资料（如适用），认为该核证机关所作出的或没有作出的假设不切实际或不适当，则评估人须在评估报告中作出适当的评论。

21. 第 18 段提述的流动资产净额应指经扣除流动负债的流动资产的价值。

## 潜在法律责任的查证

22. 根据核证机关提供的资讯，评估人须查证核证机关所制订的安排，该等安排是用以判断及管理与其已发出或计划发出的认可证书有关的潜在法律责任，其中包括：

- 因核证机关、其高级人员、雇员或代理人的错误或不作为而引起的潜在申索；及

- 因其证书所指明的倚据限额而引起的潜在法律责任。

23. 凡有意申请认可的核证机关尚未开始运作，其潜在的法律责任将以其预算会在未来 12 个月内发出的证书的数目作为计算基础。

24. 为第 22 段的目的，评估人须执行适当的程序，以：

- 查证截至进行审核时核证机关就与已发出的证书有关的潜在法律责任而作出的保险安排（或其他适当形式的保障）的细节，并执行适当的程序以评估核证机关有否遵守《业务守则》第 8.2 至 8.4 段关于为法律责任投保的规定；

- 查证自上次评估以来，核证机关有否收到登记人及／或倚据人士提出的申索，及该等申索的情况；及

- 查证自上次评估以来，是否有申索针对有关保险单而提出。

## 报告

25. 评估人须就评估的结果和评估所得为核证机关拟备一份正式的书面报告。评估人须在报告中清楚述明与核证机关议定并在评估时采用的程序，及评估所得，包括重大的不正常情况的详情，例如：没有遵守《条例》或《业务守则》中有关条文的事件。

26. 评估人必须提出意见，指出接受评估的核证机关的管理人员所作出的声明是否合理，该声明是有关该核证机关在各重大方面是否有能力遵守（或有否实际遵守）《条例》及《业务守则》的有关条文。评估人在提出意见前，须特别考虑以下事项：

- 该核证机关有否按照《条例》及《业务守则》的有关条文，在其核证作业准则内披露其业务运作模式，以及有否按照这些业务运作模式提供服务；

- 该核证机关有否按照《条例》及《业务守则》的有关条文，采用稳当系统以支援其运作；及

- 该核证机关有否按照《条例》及《业务守则》的有关条文，遵守与认可其证书有关的规定，包括密码匙和证书生命周期的管理。

27. 在适用情况下，评估人必须提出意见，指出接受评估的核证机关的管理人员就以下两项所作出的声明是否合理：

- 核证机关的核证作业准则在各重大方面是否符合与《业务守则》所述证书互认计划相关的证书政策内的有关规定；以及

- 核证机关在各重大方面是否有能力遵守或已实际遵守与《业务守则》所述证书互认计划相关的证书政策内的有关规定。

28. 评估人须就核证机关的财务预测方面，述明下列事项：

- 财务预测所涵盖的期间；

- 财务预测所依据的会计政策，是否在各重大方面与该核证机关一般采用的政策一致，以及是否符合在香港特别行政区所采用获广泛接受的会计原则或国际间广泛接受的同等会计原则；及

- 财务预测在各重大方面是否按照核证机关所作出的假设适当地编制。如评估人根据其经验及专业判断，以及根据核证机关公司最新的经审计财政报告内所披露的资料(如适用)，认为核证机关所作出的或没有作出的假设不切实际或不适当，则评估人应在评估报告中作出适当的评论。

29. 除按照第 28 段载列的项目作出报告外，评估人亦须提出第 18 段载列的比较结果，以及述明就有关第 20 段的考虑结果所作的评论。从核证机关查证所得的该核证机关的账目及 90 日营运成本预测（即第 18 段所提述的两项资料），须以附录的形式附于评估报告。

30. 评估人须就核证机关对其潜在法律责任的管理提出意见，以指出核证机关所作出的以下声明是否合理：该声明谓其已采取及维持适当措施，以判断及管理其潜在法律责任。

31. 评估人必须就其执行第 24 段所载列的程序时所收集的资讯作出查证及报告。资讯的范围包括（1）核证机关的潜在法律责任；（2）对法律责任所作的保险安排或其他适当形式的保障；及（3）核证机关所收到的申索或针对核证机关保险单提出的申索。

32. 除按照第 31 段所载的项目作出报告外，评估人亦须就执行有关程序以评估核证机关有否遵守《业务守则》第 8.2 至 8.4 段一事所得的结果作出报告。

## 对内部审计工作的倚据

33. 评估人在适当的情况下，须考虑核证机关内部审计工作的可依赖程度，以修订评估人所进行的评估工作的性质、时间及范围。如计划倚据内部审计工作，评估人须考虑：

- 内部审计工作的效能和客观性；
- 内部审计工作对接受评估的特定核证工作所涵盖的范围；及
- 就发现的问题作出的跟进和解决该等问题的进度。

## 评估的进行

34. 评估人须按照其所属的专业机构或协会就进行该等评估工作所订立的有关标准及守则（如适用），进行评估工作。

35. 评估人须根据每一方面的评估工作所得结果，考虑任何不正常情况或不足之处的严重性。

36. 评估人须设计及进行测试，以核实核证机关在其核证作业准则及相关的证书政策内所列载的有关规定，是否已在核证机关的运作、技术及/或文件中获得充分反映。评估人所进行的测试应包括：

- 分析所获得的资讯；

- 重复计算、比较及其他准确度的核对；
- 观察核证机关的运作；
- 查阅有关的文件及纪录；及
- 评估人认为适当的其他测试，如核对系统设置、寻求确认等。

37. 除上述问题外，评估人亦须运用其专业判断以决定评估过程中所采用的测试程序的性质、时间和范围。

## 参考

38. 在评估核证机关有否遵守规定时，评估人必须考虑适用于核证机关运作的获广泛采纳的监控原则。在这方面现有的相关资料包括：

- 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 (原为：CS2 – Protection Profile Guidance for Near-term COTS), National Institutes of Standards and Technology, Department of Commerce, USA.