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

二零零零年一月公布

香港特别行政区政府

引言

1 本指引所载的资讯，并非《认可核证机关业务守则》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。

2 《电子交易条例》（第 553 章）（「条例」）第 20（3）（b） 条要求核证机关在申请认可时，必须向资讯科技署署长（「署长」）提交一份由一位获署长接纳为合资格拟备报告的人士所拟备的报告。该报告须评估核证机关是否有能力遵守条例中适用于认可核证机关的条文和《认可核证机关业务守则》（「业务守则」）。根据条例第 43（1）及（2）条，认可核证机关必须最少每 12 个月向署长提交报告一次，该报告须载有对该核证机关在报告涵盖的期间内有否遵守条例中适用于认可核证机关的条文的评估，及在该期间是已遵守业务守则的评估。该报告必须由署长认可为合资格拟备该报告的人士拟备。

3 本文件为根据条例第 20 （3）（b）条及第 43（2）条要求，有意申请或已获认可的核证机关遵守规定的评估的范围及进行提供指引，及旨在为下列人士提供参考：

- 条例第 20 （3）（b）（ii） 条及第 43（2）条所提述，将拟备评估报告的人士；
- 根据条例第 43（1）条必须向署长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。

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有关条文及业务守则的规定（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有关条文及业务守则所作出的声明。

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，并评估这些资讯是否已作出适当的披露；
- 评估该核证机关是否符合关于使用稳当系统以支援其运作的规定；
- 评估该核证机关是否根据其核证作业准则及业务守则运作，以符合有关证书认可的规定；及
- 审核有关该核证机关财政预测的特定资讯，及有关该核证机关为其发出的证书所产生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 评估人应了解该核证机关所订定的政策及业务运作模式。该等资讯（包括该核证机关所提供或有意提供的服务的细节）应载列在该核证机关发出及备存的核证作业准则内。

8 若该核证机关采用一个或以上的证书政策，评估人亦须了解每一个政策内所载列的规定。

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，该声明关于其已根据条例及业务守则的规定述明及披露其政策及业务运作模式。

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要求。业务守则第 5 段就评估稳当系统提供指引。

11 评估人必须设计及进行所需的适当测试，以评估管理人员就其已实施及维持稳当系统来提供服务所作出的声明是否合理。

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：

- 该等证书是根据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声明是否合理，该声明是关于证书的生命周期已根据业务守则及核证机关的核证作业准则实施及维持有效的控制。

财政预测的审核

14 评估人必须审核核证机关就其与条例有关的业务在未来 12 个月所作的财务预测。在进行审核时，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采用的或国际广泛接受的会计原则一致，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。

15 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.

潜在法律责任的审核

16 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，以判断及管理因其已发出或计划发出的已获及未获认可的证书所可能引致的法律责任，其中包括：

- 因核证机关、其职员、员工或代理人的过失或失责所引致的潜在索偿；及

- 与其证书所指明的倚据限额有关的潜在法律责任。

17 凡未开始运作而有意申请认可的核证机关，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。

18 此外，评估人须按照第 16 段的规定执行适当的程序，以：

- 查证就已发出的证书而导致的潜在法律责任而作出的保险安排（或其他保障）的细节；

- 查证自上次评估以来，核证机关有否遭受登记人及／或倚据人士索偿，及该等索偿的情况；及

- 查证自上次评估以来，核证机关有否提出保险索偿。

报告

19 评估人须就评估结果和发现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指出与核证机关议定并在评估时采用的程序，及评估的发现，包括重大的不正常情况的详情，例如：不能遵守条例中有关条文或业务守则的事件。

20 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）条例有关的条文及业务守则。评估人在提出意见前，须特别考虑以下事项：

- 该核证机关有否根据条例有关条文及业务守则的规定，在其核证作业准则内披露其业务运作模式，及有否根据这些业务运作模式提供服务；

- 该核证机关有否根据条例及业务守则的规定，采用稳当的系统来提供服务；及

- 该核证机关有否根据条例及业务守则，依从就认可其证书的有关规定，包括密码匙和证书生命周期的管理。

21 评估人须就核证机关的财务预测方面，述明下列事项：

- 财务预测所涵盖的时段；

- 财务预测所依据的会计政策在各重大方面与该核证机关一般采用的及在香港或国际广泛接受的会计原则一致；及

- 财务预测在各重大方面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，认为核证机关所作出的或未能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。

22 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声明是否合理，该声明是有关其已采取及维持有效措施，以判断及管理其潜在法律责任。

23 评估人必须就其执行第 18 段所载列的程序时所收集的资料作出确认及汇报。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或其他适当形式的保障、（3）向核证机关提出的索偿或核证机关作出的保险索偿。

对内部审计工作的倚据

24 评估人员在适当的情况下，应考虑核证机关内部审计工作的可依赖程度，以修订评估工作的性质、时间及程度。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

25 评估人须依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。

26 评估人须根据每一个评估方面的结果，考虑任何不正常情况或不足之处的严重性。

27 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。

28 除上述问题外，评估人亦须运用其专业判断以决定评估的性质、时间和所采用的测试程序的程度。

参考

29 **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) ASC draft X9.79 standard, PKI Policies and Practices Framework（**包括规范附件** 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.