ISMS 和 ITSMS 认证实施管理程序

编　　制	技术部
审　　核	
批　　准	
发布日期	2022 年 01 月 01 日
修订/实施日期	2022 年 01 月 01 日

中企华信认证中心有限公司

ZQHX CERTIFICATION CENTER CO.,LTD.

ISMS和ITSMS认证实施管理程序

1.目的

为确保中企华信认证中心有限公司（以下简称：ZQHX）有效、规范地开展信息安全管理体系和基于 ISO/IEC 20000-1 的服务管理体系认证活动，特制订本程序。

2.适用范围

适用于 ZQHX 信息安全管理体系和基于 ISO/IEC 20000-1 的服务管理体系认证的全过程的管理。

3.职责

3.1 市场部：作为申请受理的归口管理部门，全面负责认证受理和客户服务的管理工作；

3.1.1 负责认证项目的申请受理及监督/再认证项目的联络工作；

3.1.2 负责认证申请资料的接收及初步评价；

3.1.3 负责认证服务合同的签订及合同事宜的解释；

3.2 审核部：作为审核实施管理的归口管理部门，全面负责认证项目审核实施过程的管理工作；

3.2.1 负责认证申请评审、审核人日的策划、认证周期内审核方案的策划，包括：审核时间的策划等，对初次审核、监督审核、再认证审核方案进行策划，并根据初次审核、监督审核、再认证审核方案策划的安排，选择派遣和审核组，调度、协调审核活动，下达《审核组派遣通知书》；

3.2.2 负责审核计划、认证证书信息的上报（CNCA 统一上报信息系统）；负责向 CNCA、CNAS、CCAA 对口上报认证信息，包括：认证审核信息、获证客户信息、月报、年报、CNCA 年度工作报告的编制和报送；

3.2.3 负责审核实施管理。解决审核过程中出现的问题，对审核过程实施监控管理。对发现的审核员存在的问题及时处理（必要时会同综合部）；

3.3 技术部：

3.3.1 基于审核组的现场审核结论和必要的考虑因素，作出认证决定；

3.3.2 针对特殊审核的需要，制定审核规范；

3.4 综合部：

3.4.1 负责认证信息的制、修订及公开管理；

3.4.2 负责制备和提供认证审核所需的必要工作文件；

3.4.3 负责证书的管理，包括认证证书、证书暂停、恢复、撤销和注销通知的制作、登记；

3.4.4 负责客户证书信息在 ZQHX 网站上的公示；

4.工作程序

4.1 信息安全管理体系认证管理

4.1.1 认证申请

4.1.1.1 申请

CNAS-CC01 中 9.1 的要求适用。此外，要求申请认证组织具有一个已文件化且已实施的 ISMS，申请认证组织的 ISMS 应符合 ISO/IEC 27001 和认证所要求的其他文件。

4.1.1.2 申请评审

CNAS-CC01 中 9.1.2 的要求适用。

4.1.2 审核方案

4.1.2.1 CNAS-CC01 中 9.1.3 的要求适用。此外，ISMS 审核方案还应考虑所确定的信息安全控制。

4.1.2.2 申请认证组织 ISMS 至少实施过一次覆盖认证范围的管理评审和内部审核，才可对该 ISMS 实施认证。

4.1.2.3 认证审核范围

审核组根据所有适用的认证要求，对包含在确定范围内的申请认证组织 ISMS 进行审核。确认申请认证组织在其 ISMS 范围内满足了 ISO/IEC 27001 中 4.3 的要求。

机构验证每个认证范围至少有一个适用性声明。确保申请认证组织的信息安全风险评估和风险处置准确地体现了认证范围所界定的活动并扩展到活动的边界。机构确认其在申请认证组织的 ISMS 范围和适用性声明中得到了体现。并确保与不完全包含在 ISMS 范围内的服务或活动的接口，已在寻求认证的 ISMS 中得到说明，并已包括在申请认证组织的信息安全风险评估中。

4.1.2.4 认证审核准则

申请认证组织 ISMS 接受审核的准则包括 ISMS 标准 ISO/IEC 27001 及与所实施的业务相关的，可以作为认证要求的其他文件。

4.1.2.5 认证审核时间

CNAS-CC01 中 9.1.4 的要求适用信息安全管理体系认证审核时间确定。CNAS-CC170 附录 B、附录 C 提供了审核时间计算的进一步指南和示例。

机构给予审核员足够的时间来开展与初次审核、监督审核或再认证审核相关的所有活动。总审核时间的计算，应包括报告审核情况所需的充足时间。

4.1.2.6 多场所的抽样

CNAS-CC01 中 9.1.5 的要求适用于信息安全管理体系认证审核多场所抽样，并且以下要求和指南适用。

4.1.2.6.1 当客户拥有满足以下 a）至 c）的多个场所时，可以考虑使用基于抽样的方法进行多场所认证审核：

a）所有场所在同一 ISMS 下运行，并接受统一的管理、内部审核和管理评审；

b）所有的场所都包含在客户的 ISMS 内部审核方案中；

c）所有的场所都包含在客户的 ISMS 管理评审方案中。

4.1.2.6.2 当使用基于抽样的方法时，应确保：

a）在初次的合同评审时，最大程度地识别场所之间的差异，以便确定适宜的抽样水平；

b）结合以下因素，抽取具有代表性的场所：

--总部及其他场所的内部审核的结果；

--管理评审的结果；

--场所规模的差异；

--各场所业务目的的差异；

--不同场所的信息系统的复杂程度；

--工作实践的差异；

--控制的设计与运行的差异；

--与关键的信息系统或处理敏感信息的信息系统之间的潜在交互；

--任何不同的法律要求；

--地域和文化因素；

--场所的风险状况；

--发生在特定场所的信息安全事件；

c）从客户 ISMS 范围内的所有场所中选择具有代表性的样本，该选择应基于一个可体现上述 b）中所列因素的判定，同时也考虑随机因素。

d）在授予认证之前，机构审核了 ISMS 中每个具有重大风险的场所；

e）根据上述要求设计审核方案，且审核方案要在三年内覆盖 ISMS 认证范围内的代表性样本；

f）无论是在总部还是在单个场所发现不符合，纠正措施规程的实施适用于包括在认证

范围内的总部和所有场所。

4.1.2.7 多管理体系结合审核

CNAS-CC01 中 9.1.6 的要求适用。

ISMS 体系审核可以和其他管理体系审核相结合。结合审核或一体化审核应能够清楚地识别 ISMS 以及 ISMS 与其他管理体系的适当接口，认证机构可以接受多个管理体系文件相结合的文件（例如，信息安全、质量、健康与安全、环境）。

只要能够证实审核满足了 ISMS 认证的所有要求，ISMS 审核可以和其他管理体系审核相结合。在审核报告中，所有对 ISMS 重要的要素应清晰地体现并易于识别。审核的质量不应因结合审核而受到负面影响。

4.1.3 审核策划

4.1.3.1 确定审核目的、范围和准则

CNAS-CC01 中 9.2.1 的要求适用。审核目的应包括确定管理体系的有效性，以确保申请认证组织已根据风险评估实施了适用的控制并实现了所设立的信息安全目标。

4.1.3.2 选择和指派审核组

CNAS-CC01 中 9.2.2 的要求适用。

审核组应：

——对拟认证 ISMS 范围内的特定活动具备适当的技术知识，以及相关时，对这些活动的相关规程和其潜在信息安全风险具备适当的技术知识（技术专家可以履行此项职责）；

——理解申请认证组织，足以基于申请认证组织 ISMS 范围和组织环境对 ISMS（该体系管理着申请认证组织活动、产品和服务的信息安全）进行可靠的认证审核；

——适当地理解适用于申请认证组织 ISMS 的法律法规要求。

4.1.3.3 审核计划

CNAS-CC01 中 9.2.1 的要求适用。审核计划应考虑所确定的信息安全控制措施。

如适宜，审核计划应识别在审核中使用的网络支持的审核技术。同时机构宜与拟审核的组织就选择一个能最有效地证实其整个 ISMS 范围的审核时间达成一致意见，适当时，可考虑季度、月份、日期和班次。

4.1.4 初次认证

4.1.4.1 第一阶段审核

（1）在该审核阶段，应获取有关 ISMS 设计的文件，其中包括 ISO/IEC 27001 所要求的文件。

（2）第一阶段的结果应形成书面报告。在决定进行第二阶段之前，审查第一阶段的审核报告，以便为第二阶段选择具有所需能力的审核组成员。

4.1.4.2 第二阶段审核

（1）第二阶段的目的是确认申请认证组织遵守自身的方针、策略和规程。

（2）审核应重点关注客户：

——最高管理者的领导力和对信息安全方针与信息安全目标的承诺；

——ISO/IEC 27001 中所列的文件要求；

——评估与信息安全有关的风险，以及评估可产生一致的、有效的、在重复评估时可比较的结果；

——基于风险评估和风险处置过程，确定控制目标和控制；

——信息安全绩效和 ISMS 有效性，以及根据信息安全目标对其进行评审；

——所确定的控制、适用性声明、风险评估与风险处置过程的结果、信息安全方针与目标，它们相互之间的一致性；

——控制的实施，考虑了外部环境、内部环境与相关的风险，以及组织对信息安全过程和控制的监视、测量与分析，以确定控制是否得以实施、有效并达到其所规定的目标；

——方案、过程、规程、记录、内部审核和对 ISMS 有效性的评审，以确保其可被追溯至管理决定和信息安全方针与目标。

4.1.5 审核实施

CNAS-CC01 中 9.4 的要求适用于信息安全管理体系认证审核的实施。

4.1.5.1 实施审核要求申请认证组织证实对信息安全相关风险的评估与 ISMS 范围内的 ISMS 运行是相关的和充分的。

4.1.5.2 确定申请认证组织识别、检查和评价信息安全相关风险的规程及其实施结果是否与申请认证组织的方针、目标和指标相一致。确定用于风险评估的规程是否健全并得到正确实施。

4.1.5.3 审核报告

4.1.5.3.1 除了 CNAS-CC01 9.4.8 中对审核报告的要求之外，审核报告应提供一下信息或对

这些信息的应用：

a）审核说明，其中包括了文件评审摘要；

b）对客户信息安全风险分析进行认证审核的说明；

c）与审核计划的偏离；

d）ISMS 的范围。

4.1.5.3.2 审核报告应足够详细，以帮助和支持认证决定。审核报告应包括：

a）所采用的主要审核路线和所使用的审核方法；

b）形成的观察结果，包括正面的（例如，值得注意的特征）和负面的（例如，潜在的不符合）；

c）对申请认证组织 ISMS 与认证要求的符合性的评价意见、对不符合的清楚说明、所引用的适用性声明的版本，以及适用时，与申请认证组织以往认证审核结果的任何有用的对照。

完成的问卷、检查清单、观察结果、日志或审核员笔记可以构成完整的审核报告的一部分。如果使用这些方法，这些文件应作为支持认证决定的证据提供给机构技术部。在审核过程中，有关被评价的样本的信息应包含在审核报告或其他认证资料中。

报告应考虑申请认证组织所采用的内部组织和规程的充分性，以便对其 ISMS 建立信心。除了 CNAS-CC01 的 9.4.8 中对审核报告的要求，报告还应包括：

a）关于 ISMS 要求和信息安全控制的实施与有效性的、最重要的观察（正面的和负面的）的摘要；

b）审核组关于申请认证组织的 ISMS 是否获得认证的建议，以及支持该建议的信息。

4.1.6 认证决定

4.1.6.1 除 CNAS-CC01 的要求外，认证决定基于审核报告中审核组对申请认证组织 ISMS 是否通过认证的建议。

4.1.6.2 只有具备充分的证据证实管理评审和 ISMS 内部审核的安排已经实施，且是有效的并将得到保持，才可向申请认证组织授予认证。

4.1.6.3 通常情况下，对于授予认证决定做出决定的人员不宜推翻审核组的负面建议。如果发生这种情况，机构技术部应记录其作出推翻建议的决定的依据，并说明其合理性。

4.1.7 保持认证

4.1.7.1 CNAS-CC01 中 9.6.1 的要求适用。

4.1.7.2 CNAS-CC01 中 9.6.2 的要求适用于信息安全管理体系的监督审核。监督的目的是验证已被认证的 ISMS 得到持续实施、考虑申请认证组织运作变化所引起的管理体系变化的影响并确认与认证要求的持续符合。

（1）监督审核方案至少包括：

--管理体系的保持要素，如信息安全风险评估与控制的维护、ISMS 内部审核、管理评审和纠正措施；

--根据 ISMS 标准 ISO/IEC 27001 和认证所需的其他文件的要求，与来自外部各方沟通；

--文件化管理体系的变更；

--发生变更的区域；

--所选择的 ISO/IEC 27001 的要求；

--适宜时，其他所选择的区域.

（2）每一次监督应至少审查以下方面：

--ISMS 在实现申请认证组织信息安全方针的目标方面的有效性；

--对与相关信息安全法律法规的符合性进行定期评价与评审的规程的运行情况；

--所确定的控制的变更，及其引起的 SoA 的变更；

--控制的实施和有效性（根据审核方案来审查）。

（3）监督审核可以与其他管理体系的审核相结合，告应清晰地指出与每个管理体系相关的方面。在监督审核过程中，认证机构应检查申请认证组织提交给认证机构的申诉和投诉记录，并且在发现任何不符合或不满足认证要求时，还应检查申请认证组织是否对其自身的 ISMS 和规程进行了调查并采取了适当的纠正措施。监督报告应包括有关消除以往出现的不符合、SoA 版本和从上次审核之后发生的重大变更的信息。

4.1.7.3 CNAS-CC01 中 9.6.3 的要求适用于信息安全管理体系再认证。

4.1.7.4 CNAS-CC01 中 9.6.4 的要求适用于信息安全管理体系特殊审核。

4.1.7.5 CNAS-CC01 中 9.6.5 的要求适用于信息安全管理体系认证暂停、撤销或缩小认证范围。

4.2 信息技术服务管理体系认证管理

4.2.1 认证申请及申请评审

CNAS-CC01 中 9.1.1、9.1.2 的要求适用。

申请认证组织须说明其适用的关于 ITSMS 认证机构的资质、诚信守法记录或认证人员身份背景的要求，以及适用的与保守国家秘密或维护国家安全有关的法律法规要求，以便判断是否具备对该申请认证组织组织实施认证活动的资格或条件。

适用时，要求客户指明其在申请认证的 SMS 范围内与其他方共同提供服务的情况。

机构应评审客户的申请，以确保清晰地了解客户的活动区域，以及 SMS 和服务的可能风险。

4.2.2 审核方案

CNAS-CC01 中 9.1.3 的要求适用。

遵循 ISO 19011 相关指南针对每个申请认证组织组织建立审核方案，并对该审核方案进行管理。

4.2.3 多场所抽样

CNAS-CC01 中 9.1.5 的要求适用于信息技术服务管理体系认证审核多场所抽样。

如果客户具有多个地点且所有的地点满足以下条件时，可以使用基于抽样的方法来实施多场所认证审核：

--在同一个实施集中管理的 SMS 下运行；

--包含在客户的内部审核方案中；

--包含在客户的管理评审方案中。

4.2.4 多管理体系结合审核

（1）CNAS-CC01 中 9.1.6 的要求适用。

（2）ITSMS 体系审核可以和其他管理体系审核相结合。结合审核或一体化审核应确保审核证据在审核范围内满足 ISO/IEC 20000-1 的要求。在审核报告中，应容易辨识出与 ISO/IEC 20000-1 相关的所有审核发现。ISO/IEC 20000-1 审核的完整性，不应因结合审核而受到负面影响。

（3）在 ISMS 和 ITSMS 的结合审核时，应审核 ISO/IEC 20000-1 中的信息安全管理过程，以确保：

--信息安全方针是与 SMS 和服务相关的；

--识别相关的信息安全风险并实施信息安全控制，以支持 SMS 和服务；

审核员可以从 ISMS 中找到一些支持性的证据，如果 ISMS 的范围是在 SMS 的范围之外，则 ISO/IEC 20000-1 中的信息安全管理过程是没有 ISMS 支持的，应作为一个独立的过程来审核。

应审核信息安全方针、风险和控制，以确保他们与客户 SMS 范围内的服务相适宜。

4.2.5 初次认证

CNAS-CC01 中 9.3 的要求适用。

（1）当申请认证组织由于信息技术服务的原因在申请评审阶段不能提供给认证机构足够的信息时，认证机构应通过第一阶段审核在申请认证组织组织的现场补充对上述信息的确认，并完成申请评审任务。这种情况下宜增加第一阶段现场审核时间。

（2）审核组应获取客户识别了参与服务提供的其他地方和客户如何按照 ISO/IEC 20000-1 对其他方进行管理的证据。

4.2.6 审核实施

4.2.6.1 总则

CNAS-CC01 中 9.4.1 的要求适用。

4.2.6.2 召开首次会议

CNAS-CC01 中 9.4.2 的要求适用。

4.2.6.3 审核中的沟通

CNAS-CC01 中 9.4.3 的要求适用。

4.2.6.4 获取和验证信息

CNAS-CC01 中 9.4.4 的要求适用。

4.2.6.5 确定和记录审核发现

CNAS-CC01 中 9.4.5 的要求适用。

4.2.6.6 准备审核结论

CNAS-CC01 中 9.4.6 的要求适用。

4.2.6.7 召开末次会议

CNAS-CC01 中 9.4.7 的要求适用。

4.2.6.8 审核报告

CNAS-CC01 中 9.4.8 的要求适用。审核报告应足够详细，以支持认证决定。审核报告应

包含认证范围的界定，提及范围的任何变更，并描述所遵循的重要审核路线和所使用的审核方法。报告应包括审核组对客户 SMS 认证的推荐意见，以及证实该推荐意见的信息。

4.2.6.9 不符合的原因分析

CNAS-CC01 中 9.4.9 的要求适用。

4.2.6.10 纠正和纠正措施的有效性

CNAS-CC01 中 9.4.10 的要求适用。

4.2.7 认证决定

CNAS-CC01 中 9.5 的要求适用。

技术部应以认证过程中收集的信息和其他相关信息为基础，以充分的证据证实申请组织建立信息技术服务管理体系的管理评审和内部审核的方案已经得到有效实施并且将得到保持，才可决定申请组织通过认证。

4.2.8 保持认证

CNAS-CC01 中 9.6 的要求适用。

4.2.8.1 监督审核

（1）监督审核的最长时间间隔不超过 12 个月，由于获证组织业务运作的时间（季节）特定及其内部审核安排等原因，可以合理选取和安排监督周期及时机，在认证证书有效期内的监督审核必须覆盖信息技术服务管理体系认证范围内的所有业务活动。

（2）监督审核应包括，但不限于以下内容：

--体系保持和变化情况；

--顾客投诉情况；

--涉及变更的范围；

--内部审核与管理评审；

--服务目录的变化情况；

--对上次审核时提出的不符合所采取纠正措施的审查；

--标志的使用和（或）任何其他队认证资格的引用；

--适当时，其他选定的范围。

4.2.8.2 CNAS-CC01 中 9.6.3 的要求适用于信息技术服务管理体系再认证。

4.2.8.3 CNAS-CC01 中 9.6.4 的要求适用于信息技术服务管理体系特殊审核。

4.2.8.4 CNAS-CC01 中 9.6.5 的要求适用于信息技术服务管理体系认证暂停、撤销或缩小认证范围。

5.相关文件

5.1 CNAS-CC01《管理体系认证机构要求》

5.2 CNAS-CC170《信息安全管理体系认证机构要求》

5.3 CNAS-CC175《基于 ISO/IEC 20000-1 的服务管理体系认证机构要求》

5.4 CNAS-SC-170《信息安全管理体系认证机构认可方案》

5.5 CNAS-SC175《信息技术服务管理体系认证机构认可方案》

5.6 GB/T 19011《管理体系审核指南》

5.7 GB/T28450《信息安全管理体系审核指南》

6.相关记录

6.1 《认证服务合同》

6.2 《认证申请书》

6.3 《审核组派遣通知书》

6.4 《管理体系文件审核报告》

6.5 《审核计划》

6.6 《会议签到表》

6.7 《核查记录表》

6.8 《管理体系第一阶段审核报告》

6.9 《不符合项报告》

6.10《改进事项清单》

6.11《管理体系审核报告》

6.12《客户信息确认单》

6.13《客户信息变更单》

6.14《终止审核报告及流转单》

6.15《保密及公正性声明》

6.16《申请评审及审核方案策划表》