管 理 体 系 认 证 规 则

CGW-ISMS-01 版本:I

信息安全管理体系认证规则

2020-09-01发布 **2020-09-01实施**

长城（天津）质量保证中心有限公司 发布

信息安全管理体系认证实施规则

1 适用范围

本实施规则适用于长城（天津）质量保证中心有限公司（以下简称：CGW）实施信息安全管理体系认证，满足第三方认证制度要求，作为提供认证服务的规范。必要时，在认证合同中补充相关的技术要求。

2 认证模式

CGW首先对受审核方的管理体系进行初次审核，经过评定，确认是否批准认证；通过认证之后，在认证证书的有效期内对获证客户的管理体系进行监督，确认是否持续满足认证要求。

3 认证流程

4 认证申请

4.1 基本条件

a) 认证客户具有明确的法律地位, 客户具有企业营业执照、事业单位法人证书、 社会团体登记证书、非企业法人登记证书、党政机关设立文件等，可独立申请认证。其他类型的客户，应由具备资格的单位代为申请；

b) 国家、地方或行业有要求时，认证客户具有规定的行政许可文件, 其申请认证范围应在法律地位文件和行政许可文件核准的范围内；

c) 认证客户按相关的管理体系标准建立了文件化的管理体系，初次认证现场审核前已至少持续稳定运行了3个月，至少已实施一次完整的内审和管理评审；

d) 认证客户承诺遵守国家的法律、法规及其他要求,承诺始终遵守认证的有关规定，承担与认证有关的法律责任，并有义务协助认证监管部门的监督检查，对有关事项的询问和调查如实提供相关材料和信息；

e) 认证客户在一年内，未发生信息安全泄露事故（包括已经或可能严重损害国家安全、社会秩序、公共利益或获证客户及其相关方的合法权益）或被执法监管部门责令停业整顿或在全国企业信用信息公示系统中被列入“严重失信企业名单”或违反国家相关法规，虚报、瞒报获证所需信息的情况；

f) 认证客户承诺获得CGW认证后，按规定使用认证证书和认证标志和有关信息，不得擅自利用管理体系认证证书的文字、符号误导公众认为其产品或服务通过认证按合同支付认证费用，并按规定接受监督；

g) 认证审核期间，认证客户能够提供与拟认证范围相关的产品/服务/活动现场。

4.2 申请评审

CGW 确认收到的认证申请资料是否齐全，并对认证申请及相关文件化信息进行评审，必要时，要求申请组织补充信息。在申请评审后，CGW决定是否受理认证申请。如果拒绝认证申请会告知申请组织被拒绝的原因。

4.3 审核准则

ISO /IEC 27001《信息安全、 网络安全和隐私保护 - 信息安全管理系统 - 要求》；

适用的信息安全方针、目标、适用性声明、程序、标准、法律法规、操作规范、合同要求或行业规范。

5 审核实施

5.1审核策划

计划管理部根据组织申请信息确定的总审核时间及现场审核时间，选择和任命经评价合格的审核员组成审核组，指定一名有能力的审核员担任审核组长。如果仅有一名审核员，该审核员应有能力履行审核组长的职责。

审核组长根据审核方案策划书及组织相关的申请材料，为每次现场审核编制审核计划及日程表，并在现场审核前提交给受审核组织确认。遇到特殊情况，需要临时变更计划时，审核组长应及时将变更情况通知受审核组织，并与之就变更后的审核计划安排协商一致。

5.2 审核过程

5.2.1 初次认证审核

初次认证审核分两个阶段实施：第一阶段和第二阶段。第一阶段的审核目的是了解受审核方的基本信息、审核管理体系文件，识别任何引起关注的、在第二阶段审核中可能被判定为不符合的问题，为第二阶段审核提供关注点。第二阶段审核的目的是评价受审核方管理体系实施的符合性和有效性。二阶段审核情况需进一步做出详细记录。

第一阶段应到现场审核。审核组长应在进入现场审核前，对受审核组织提供的管理体系文件进行审查，以确定文件所述的管理体系与审核准则的符合性。审核组长应对文件审查的结果负责。

审核组对在第一阶段和第二阶段审核中收集的所有信息和证据进行汇总分析，评价审核发现并形成审核结论。

5.2.1.1 第一阶段审核

审核组结合受审核方的管理体系运行目标和体系覆盖活动的专业特点，根据受审核方提供的管理体系文件、体系运作过程、运作场所和现场的具体情况、内部审核与管理评审策划和实施情况，确认受审核方对标准的理解和实施的程度、对目标的实现具有重要影响的关键点、相关的法律法规要求的遵守情况以及管理体系范围，以确定第二阶段审核安排。

评价组织是否策划和实施了内部审核与管理评审，以及管理体系实施的程度能否证明其已为第二阶段审核做好准备。

如果发生任何将影响管理体系的重要变更，CGW 可能将重复整个或部分第一阶段审核。第一阶段审核的结果可能导致推迟或取消第二阶段。

5.2.1.2 第二阶段审核

审核组现场评价受审核方管理体系的实施情况，包括符合性和有效性。第二阶段审核至少包括以下方面：

a) 与适用的管理体系标准和其他规范性文件的所有要求的符合情况；
b) 依据关键绩效目标和指标，对绩效进行的监视、测量、报告和评审；
c) 管理体系和绩效中与遵守法律有关的方面；
d) 受审核方过程的运作控制；
e) 内部审核和管理评审实施情况；
f) 管理职责的落实，包括针对方针的管理职责；
g) 为实现总目标而建立的职能层次目标的策划和实现情况；
h) 规范性要求、方针、绩效目标和指标、适用的法律要求、职责、人员能力、运作、程序、绩效数据和内部审核发现及结论之间的联系。

5.2.1.2.1 信息安全管理体系应包括：

1）基于风险评估和风险处置过程，确定控制目标和控制；

2）所制确定的控制、适用性声明、风险评估和风险处置过程的、信息安全方针、信息安全目标之间的一致性；

3）控制的实施（控制措施），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及控制措施的监视、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。

5.2.1.3信息安全管理体系与其他管理体系结合审核

5.2.1.3.1信息安全管理体系文件与其他管理体系文件的整合客户可将信息安全管理体系文件的进行整合，也可将信息安全管理体系文件与其他管理体系文件（如：质量管理体系）整合。如果体系文件是结合的，应能清晰地识别出客户的信息安全管理体系。

5.2.1.3.2 管理体系结合审核

信息安全管理体系与其他管理体系结合审核时，按以下管理要求执行：

a) 对各体系分别界定审核范围，对审核时间的确定、审核方案策划进行有效管理。

b) 必须以审核活动满足信息安全管理体系认证所有要求为前提，并且审核质量不应由于结合审核而受到负面影响。在审核报告中应清晰体现所有与信息技术服务管理体系和信息安全管理体系有关的重要要素的描述。

5.2.2 监督活动

5.2.2.1 监督活动的方式

采用现场监督审核和日常监督（如关注国家有关部门发布的质量信息公报、关注获证客户相关方的信息、获证客户有关信息的日常跟踪、审查获证客户及其运作的说明、要求获证客户提供文件和记录等）相结合的方式。

5.2.2.2 获证后监督审核的内容

a) 任何变更（如资源、过程、组织结构、已识别的关键控制点等）；

b) 持续的运作控制质量目标的实现情况；

c) 内部审核和管理评审；

d) 信息安全管理体系审核《适用性声明》及版本的变化情况；

e) 管理体系实施的有效性；

f) 认证范围相关的产品/服务/活动现场情况；

g) 为持续改进而策划的活动的进展；

h) 针对上次审核中确定的不符合所采取的措施和效果；

i) 证书和标志的使用和（或）任何其他对认证资格的引用，获证客户应保存全部投诉记录，需要时提供认证机构。

CGW 根据以上信息对获证客户管理体系进行再评价，确认其是否持续满足认证要求。

监督审核时，如认证客户没有按时关闭不符合，将可能导致认证证书的暂停或撤销。

5.2.2.3 监督审核的频次

在证书有效期内，获证客户须接受监督审核，监督审核应至少每个日历年（应进行再认证的年份除外）进行一次。初次认证后的第一次监督审核应在认证决定日期起12个月内进行；此后，监督审核应至少每个日历年（应进行再认证的年份除外）进行一次。

由于获证组织的（季节）业务特点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（或和信息安全管理体系）认证范围内的所有业务活动。

获证客户因未在规定的时间内实施监督审核而暂停认证证书的，监督审核恢复后，下次审核时间应按原计划时间计算。

若发生下述情况则需增加监督频次，或安排提前较短时间通知的审核：

a) 获证客户对管理体系进行了重大更改或发生重大问题；

b) 有足够信息表明获证客户发生了组织机构、服务变更等影响到其认证基础的更改；

c) 获证客户出现信息安全泄露事故或用户提出对相关管理体系运行效果的投诉未得到处理时；

d) 其他需要考虑的情况。

5.2.3 再认证

获证客户在证书有效期满前须提出再认证申请。再认证审核的目的是验证作为一个整体的组织管理体系全面的持续符合性和有效性，以及认证范围的持续相关性和适宜性。再认证审核的程序和要求参照 5.2.1 条实施。

在对获证客户的日常监督中，发现获证客户的出现严重影响管理体系运作的重大变更时，或对获证客户的投诉分析和其他信息表明获证客户不再满足认证要求时，将安排特殊审核或与获证客户商定提前安排再认证审核。

再认证时通常可不进行一阶段审核，但当获证客户的管理体系和获证客户的内外部运作环境有重大变化时，再认证审核活动可能需要有第一阶段审核。

再认证审核时，认证客户应在当前认证证书到期前接受 CGW审核，并对于审核组开具的不符合在规定的时间内按要求关闭。否则，因认证客户的原因导致CGW 不能在原认证证书到期后 6个月内做出认证决定的，再认证审核失效。

5.2.4 特殊审核

5.2.4.1 扩大认证范围审核

针对已获证的客户，CGW 对扩大认证范围的申请进行评审，确定能否予以扩大的决定所需的审核活动，这一工作可与监督审核同时进行。

5.2.4.2 提前较短时间通知的审核

为调查投诉、对变更做出回应或对被暂停的获证客户进行追踪，需要在提前较短时间通知获证客户后对其进行的审核。

获证客户的产品和服务被国家行政主管部门在监督抽查中被查出不合格时， CGW 将对获证客户实施特殊审核。如获证客户不接受特殊审核，认证证书将被暂停。

5.3 现场审核活动实施

审核组在现场审核前与受审核方沟通，确认审核安排，说明首末次会议议程。

审核组按照审核计划中日程安排实施审核，通过查阅受审核方的文件和记录、与过程和活动的岗位人员面谈、座谈、观察产品、服务形成过程和活动等适当方法，抽样收集并验证有关的信息，形成审核发现，确认不符合情况。

在审核过程中，审核组及时与受审核方沟通，通报审核进程，确认审核证据，解决分歧。当审核发现表明不能达到审核目的时，应说明理由，商定后续措施。如果需要改变审核目的和范围或终止审核时，应经审核派出机构评审和批准后实施。

审核组长在现场审核结束前，与受审核方沟通现场审核的信息，请受审核方对发现的问题和不符合报告进行确认，并商定对不符合的后续措施的安排，确认审核结论。审核组长编制审核报告并提交受审核方。

如涉及远程或部分远程审核，应按照CNAS-CC170 9.1.3.3条款执行。

5.4 不符合项、纠正措施及其验证

对在审核中发现的不符合项，组织应按照审核组的要求及时进行原因分析，在规定的时限内策划和实施消除原因的纠正措施。审核组组长或指派的审查员在规定的期限内，按照已确定的验证方式确认不符合项纠正措施的有效性。

纠正措施的有效性验证结果将直接影响审查组向 CGW 推荐是否认证注册或保持认证的最终意见。

5.5 审核报告

审核组长编制审核报告并提交CGW。审核报告应准确、简明 和清晰地描述审核实施的主要内容，以及提出不符合的纠正和纠正措施 有效性验证结果、审核结论（包括关于认证的推荐性意见）。 CGW享有对审核报告的所有权。经批准后，向受审核组织提供审核报告。受审核组织请妥善保管审核报告、不符合报告及其纠正材料等相应材料。

审核组如果需要改变审核目的和范围或终止审核时，应经 CGW评审和批准后实施。对终止审核的项目，审核组应将已开展的工作情况形成报告，认证机构应将此报告及终止审核的原因提交受审核组织。

5.6 认证决定

CGW对审核组提交的审核报告、不符合的纠正和纠正措施及实施证据等信息进行审查，确定认证要求满足程度和认证范围，接受和验证了不符合的纠正和纠正措施。

在对审核组提供的信息有效审查的基础上，综合考虑其它来源获得的补充信息，做出认证决定。

CGW 认为申请组织在认证范围内已满足授予认证资格条件，做出同意授予认证的决定。经CGW技术委员会和总经理批准后，向申请组织颁发认证证书和相关文件，并要求获证组织按要求正确使用认证证书、标志和向CGW通报相关信息。 对于不符合认证要求的申请人，CGW以书面的形式告知其不能通过认证的原因。

6 批准、拒绝、保持、扩大、缩小、暂停、恢复和撤销的条件和程序

具体要求参照《认证中心对授予、保持、扩大、更新、缩小、暂停/恢复及撤销认证条件的规定》要求执行，详见中心网站文件。

7 认证证书和认证标志

7.1 认证证书

认证证书应至少包含以下信息：

a. 获证组织名称、地址和统一社会信用代码（或组织机构代码）。该信息应与其法律地位证明文件的信息一致。
b. 管理体系覆盖的生产经营或服务的地址和业务范围。若认证的管理体系覆盖多场所，表述覆盖的相关场所的名称和地址信息。
c. 管理体系符合对应标准的表述。
d. 证书编号。
e. 认证机构名称。
f. 有效期的起止年月日。
g. 相关的认可标识及认可注册号（适用时）。

h. 证书查询方式。认证机构除公布认证证书在本机构网站上的查询方式外，还应当在证书上注明：“本证书信息可在国家认证认可监督管理委员会官方网站（www.cnca.gov.cn）上查 询”，以便于社会监督。

初次认证认证证书有效期最长为3 年。再认证的认证证书有效期不超过最近一次有效认证证书截止期再加3 年。通常情况下，获证客户应在当前认证证书截止期前至少3个月接受再认证审核或已做好接受再认证审核的准备。否则，因获证客户接受再认证审核时间过晚或因不符合的关闭导致CGW的认证决定无法在原认证证书到期前作出时，再认证证书有效期将不足3年。证书（证书二维码）应注明：获证组织必须定期接受监督审核并经审核合格此证书方继续有效的提示信息。

7.2 认证证书和认证标志的使用

获证客户认证证书的使用应按照CGW网站公开文件《认证证书和认证标识、认可标识的使用规定》执行。

8 获证客户的信息通报

获证客户通过填报《获证组织信息变更申报表》向 CGW 通报最新信息，并及时通报其重大投诉、国家监督检查结果、重大事故及获证客户变更的各种信息等。变更申报表见中心网站公示文件。

9 认证要求变更

获证客户认证证书变更应按照 CGW 网站公开文件《证书变更所需材料》提交相关资料，CGW 审定通过后决定是否换发证书。

10 保密

CGW 承诺为认证客户保密（提前告知认证客户的需公开信息除外）。对客户的保密信息如需公开或向第三方提供时，将拟提供的信息提前通知认证客户 （法律限制除外）。

11 申诉/投诉、争议及处理

相关方的申投诉、争议按照中心公开文件《申诉、投诉和争议的处理办法》执行。

12 费用和审核时间

按中心公开文件《认证收费标准》执行，审核时间按CNAS-CC170；CNAS-CC106执行。

13 公告

对获得认证、暂停、恢复或撤销的认证客户，在CGW 网站及国家认监委网站公布。

14 附则

本实施规则由长城（天津）质量保证中心有限公司负责解释。