一体化认证实施规则

ISCCC-MS-001:2017

中国信息安全认证中心

发布日期：2017 年 8 月 1 日　　实施日期：2017 年 8 月 1 日

目录

1. 适用范围

本规则用于规范中国信息安全认证中心（简称中心）的一体化管理认证活动，一体化认证涉及信息安全管理体系、信息技术服务管理体系、业务连续性管理体系、质量管理体系和数据中心服务能力成熟度。

2. 认证依据

信息安全管理体系认证以国家标准 GB/T22801-2016《信息技术 安全技术 信息安全管理体系 要求》为认证依据。

信息技术服务管理体系认证以国家标准 ISO/IEC20000-1:2011《信息技术 服务管理 服务管理体系 要求》为认证依据。

业务连续性管理体系认证以国家标准 GB/T 30146—2013《公共安全 业务连续性管理体系 要求》为认证依据。

质量管理体系认证以标准 GB/T 19001-2016《质量管理体系 要求》为认证依据。

数据中心服务能力成熟度认证以 GB/T33136-2016《信息技术服务 数据中心服务能力成熟度模型》为认证依据。

3. 术语和定义

3.1. 自评价

申请组织根据认证依据对自身的服务过程进行符合性评价，并进行评价证据的收集和分析，以确定组织满足认证依据的程度。

3.2. 现场审核

中心指派审核组到受审核方或获证组织所在办公地点进行的审核活动。

3.3. 非现场审核

中心指派的审核组在受审核方或获证组织所在办公地点以外进行的审核活动，通常以远程审核工具、电话、视频、邮件等远程审核方式进行。

3.4. 现场见证（验证）

现场见证是针对受审核方或获证组织为满足相关方利益诉求、实现组织业务目标和处置组织风险而实施的关键活动进行的，是对关键活动的执行过程进行跟踪见证；现场验证是针对关键活动所采取的关键技术进行的，以验证这些技术措施的功能能够得到实现。

3.5. 特殊审核

扩大认证范围或提前较短时间通知的审核。

4. 审核类别和审核方式

审核类别分为初次认证审核，监督审核、再认证审核和特殊审核。

审核方式分为非现场审核、现场审核和现场见证（验证）。

5. 审核人员及审核组要求

认证审核人员必须取得认证注册资格，并得到中心的专业能力评价，以确定其能够胜任所安排的审核任务。

审核组应由能够胜任所安排的审核任务的审核员组成。必要时可以补充技术专家以增强审核组的技术能力。

具有相关管理和法规等方面特定知识的技术专家可以成为审核组成员。技术专家应在审核员的监督下进行工作，可就受审核方或获证组织一体化管理中技术充分性事宜为审核员提供建议，但技术专家不能作为审核员。

6. 认证信息公开

中心应向申请认证的社会组织(以下称申请组织)至少公开以下信息：

1) 认证服务项目；

2) 认证工作程序；

3) 认证依据；

4) 证书有效期；

5) 认证收费标准。

7. 认证程序

7.1. 初次认证

7.1.1. 认证申请

中心应要求申请组织的授权代表至少提供以下必要的信息：

1) 认证申请书，包括但不限于以下内容：

a. 企业基本信息，包括业务活动、组织架构、联系人信息、物理位置和体系范围等基本内容

b. 法律地位资格证明(工商营业执照、事业单位法人证书或社会团体法人登记证书，组织代码证和税务登记证（如果有））；

c. 申请认证的范围；

d. 一体化管理涉及的管理过程

e． 一体化管理运行的时间；

f． 取得相关法规规定的行政许可文件(适用时)。

2) 自评价信息，包括但不限于：

a． 申请组织根据认证依据所进行的符合性评价；

b． 申请组织根据中心自评价要求提供自评价的报告及证据材料。

7.1.2. 申请评审

中心应根据认证依据、程序等要求，在三个工作日内对申请组织提交的认证申请书及其相关资料进行评审并保存评审记录，做出评审结论，以确定：

1) 所需要的基本信息都得到提供；

2) 申请组织的行业类别和与之相对应的管理过程特性和管理要求；

3) 国家对相应行业的管理要求；

4) 中心与申请组织之间任何已知的理解差异得到消除；

5) 中心有能力并能够实施所申请的认证活动；

6) 申请的认证范围、申请组织的运作场所、完成审核需要的时间和任何其他影响认证活动的因素；

7) 核算并确定审核人日。

中心应建立审核人日确定准则，根据受审核方的规模、特性、业务复杂程度、一体化管理涵盖的范围、认证要求和其承担的风险等因素核算并确定审核人日，以确保审核的充分性和有效性。确定的人日数记录在审核方案记录中。

7.1.3. 建立审核方案

在申请评审后，中心应针对申请组织建立审核方案（申请组织变更为受审核方），并由专职人员负责管理审核方案。审核方案的范围与程度应基于受审核组织的规模和性质，以及受审核一体化管理的性质、功能、复杂程度以及成熟度水平。

审核方案应包括在规定的期限内有效和高效地组织和实施审核所需的信息和资源，应包括以下内容：

1) 审核方案的目标;

2) 审核的范围与程度、数量、类型、持续时间、地点、日程安排；

3) 审核准则；

4) 审核方式；

5）审核组的选择；

6）所需的资源，包括交通和食宿；

7）确定的审核人日

8）处理保密性、信息安全、健康和安全，以及其它类似事宜。

7.1.4. 确定审核组

中心应根据受审核方的行业、规模和业务复杂程度组建审核组，指派审核组长。审核组组建原则见第 5 章。

7.1.5. 一阶段审核

审核组应对受审核方开展一阶段审核，以确定：

1）受审核方的一体化管理得到策划和实施；

2）受审核方的一体化管理已运行，并有足够的证据证明其运行情况；

3）受审核方对运行的一体化管理进行了监视、测量、分析和评价，并有充分的证据；

4）受审核方对一体化管理进行了有效的持续改进；

5）受审核方是否识别并遵守了相关的法律法规；

6）二阶段审核是否需要进行现场见证（验证）；

7）受审核方有充足的资源保障二阶段审核的进行；

8）收集关于客户的一体化管理范围、过程和场所的必要信息，包括：

a）客户的场所

b）使用的过程和设备

c）所建立的控制的水平（特别是客户为多场所时）

一阶段审核时，审核组通过对受审核方提交的自评价信息进行评审，获取一阶段审核需要的信息，对于无法从自评价信息中获取的信息，审核组通过远程审核工具进行信息获取，以确保完成一阶段审核。

一阶段审核以非现场审核为主，如果非现场审核结束后，审核组认为有必要进行现场审核，需在审核报告中进行说明，并向项目管理人员提出申请，由项目管理人员进行分析后确定。

7.1.6. 二阶段审核计划

审核组结合受审核方的申请材料、自评价信息、审核方案对二阶段审核的策划以及一阶段审核的结果对二阶段审核做出具体安排，包括但不限于具体的时间安排、审核组成员

对受审核方按岗位和活动以何种方式进行评价的安排、高层沟通的安排、现场见证（验证）（必要时）的安排和会议的安排。审核组长应至少在开展二阶段审核 3 个工作日之前，与受审核方就审核计划进行充分沟通，确保双方没有歧义。

7.1.7. 二阶段审核

7.1.7.1. 现场审核

审核组按照审核计划的安排对受审核方进行现场审核，现场审核应考虑一阶段审核结果，对受审核方的管理过程和控制措施的运行情况进行评价，对一阶段审核提出的问题改进情况进行验证。

现场审核的内容包括但不限于：

1) 认证范围及组织背景(认证审核范围，组织业务、组织生存环境、管理目标和达标计划)；
2) 领导职责（管理承诺，方针，组织的角色、责任和权限)；
3) 策划(应对风险和机会的措施，管理目标和实现计划)；
4) 支持(资源，能力，意识，沟通，文件化信息)；
5) 运行(运行的策划和控制，风险评估，风险处置)；
6) 绩效评估(监视、测量、分析和评价，内部审核，管理评审)；
7) 改进(不符合和纠正措施，持续改进)。

7.1.7.2. 现场见证（验证）(必要时)

审核组应在安排的时间对受审核进行现场见证（验证）以确定：

1) 受审核方的关键活动的执行过程与管理要求相一致；
2) 受审核方的关键活动的执行结果满足管理目标；
3) 受审核方的关键活动中的关键技术满足管理要求；
4) 受审核方的关键活动中的关键技术可以实现管理目标。

7.1.8. 初次认证的审核结论

审核组应对一阶段审核和二阶段审核中收集的所有信息和证据进行汇总分析，评价审核发现并就审核结论达成一致。

如果二阶段审核发现不符合项和观察项应开具不符合项报告和观察项报告，且获得受审核方认同。

二阶段审核结束，审核组应形成是否推荐认证注册的结论，审核组应根据一阶段审核

和二阶段审核的结果对受审核方的一体化管理是否满足所有适用的认证依据的要求进行评价，并判断是否推荐认证注册。

二阶段审核结束后，3 个工作日内，审核组长完成审核报告编制工作，并与受审核方进行沟通，确保双方对报告没有歧义。

7.1.9. 认证决定

中心应指派认证决定人员，对受审核方的认证申请实施认证决定，以决定：

1）同意认证注册，颁发认证证书；

2）补充认证决定所需的信息，包括但不限于申请材料、审核材料，再行决定；

3）不同意认证注册，通知受审核方不同意的理由。

认证决定人员实施认证决定时应以认证过程中收集的信息和其他相关信息为基础，以充分的证据证实受审核方的一体化管理得到了建立、实施、运行、监视、评审、保持和改进做出决定。

注 1：参加审核的人员不能再作为认证决定人员实施认证决定。

注 2：受审核方获得认证注册资格后变更为获证组织。

7.1.10. 审核方案记录与变更

审核方案管理人员应收集一阶段审核、二阶段审核和认证决定的信息，特别是形成的结论和变化的信息，记录到审核方案中。 并确定审核方案是否需要进行变更，如需要则更新相应项目内容。

7.2. 监督审核

7.2.1. 监督频次

中心应在满足认可要求的基础上，根据获证组织一体化管理覆盖的业务活动的特点以及所承担的风险，合理设计和确定监督审核的时间间隔和频次。当获证组织一体化管理发生重大变更，或发生重大问题、业务中断事故、客户投诉等情况时，中心视情况可增加监督的频次。

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两次监督审核涉及的条款之和必须覆盖一体化管理认证范围内的所有条款。 ↑

7.2.2. 信息收集

在进行监督审核之前，中心需要收集获证组织的一体化管理相关信息，以确定获证组

织的一体化管理相关信息是否发生变化。需要客户提供的信息包括以下几个方面：

1）信息确认文件，包括但不限于：

a. 基本信息，包括组织名称、地址、联系人、法人等信息的变化情况；

b. 组织信息：包括范围、组织架构、人员数量等信息的变化情况；

c. 一体化管理相关信息，关键文件化信息的变化情况。

2）自评价信息：包括但不限于：

a. 一体化管理运行情况，包括运行说明和运行证据；

b. 一体化管理监视、测量、分析和评价的结果和证据；

c. 一体化管理运行的持续改进情况，包括改进说明和证据；

d. 满足法律法规的情况说明；

e. 申请组织根据中心自评价要求提供自评价的报告。

7.2.3. 确定审核组

中心应根据获证组织的行业、规模和业务复杂程度组建审核组，指派审核组长。审核组组建原则，见第 5 章。

7.2.4. 信息评审与审核方案维护

项目管理人员应对获证组织的信息确认文件进行评审，以确定：

1）获证组织的一体化管理变化情况，尤其是一体化管理范围的变化；

2）是否需要修订审核方案，需要时对审核方案进行维护。

7.2.5. 制定审核计划

审核组应结合获证组织的信息确认文件、自评价信息、审核方案对监督审核的策划和前一次审核的结果对现场审核做出具体安排，包括但不限于具体的时间安排、审核组成员对获证组织按岗位和活动以何种方式进行评价的安排、高层沟通的安排、现场见证（验证）和会议的安排。审核组长应至少在实施审核 3 个工作日之前，与获证组织就审核计划进行充分沟通，确保双方没有歧义。

监督审核并不覆盖标准所有条款，监督审核的抽样采取抽样的方式进行，抽样准则为：

1）两次监督审核必须覆盖标准所有条款和所有部门；

2）标准中对管理过程有决定作用的条款和部门每次监督审核都需要抽到；

3）获证组织前一次审核问题较多的部门在本次监督审核中需要抽到；

4）审核组认为重要的条款应考虑进行抽样。

每次监督审核的内容应包括对以下方面：

1）内部审核（自评价信息可以替代）和管理评审；

2）对上次审核中确定的不符合采取的措施；

3）投诉的处理；

4）一体化管理在实现获证客户目标和各一体化管理的预期结果方面的有效性；

5）为持续改进而策划的活动的进展；

6）持续的运作控制；

7）任何变更；

8）标志的使用和（或）任何其他对认证资格的引用

7.2.6. 审核实施

审核组按照审核计划的安排对获证组织进行审核，由于监督审核并不要求覆盖体系的所有方面，在监督审核的策划过程中，如果获证组织的认证范围信息有变化，应对变化的方面进行关注，必要时重新确认审核范围。

监督审核原则上采取非现场审核的方式进行，非现场审核结束后，审核组根据审核结果确定是否需要进行现场审核和（或）现场见证（验证），如果需要进行现场审核和（或）现场见证（验证），审核组需向项目管理人员进行申请，项目管理人员根据受审方的相关信息确定是否进行现场审核和（或）现场见证（验证）并进行相关活动的安排。

7.2.7. 监督审核结论

审核组应对收集的所有信息和证据进行汇总分析，评价审核发现并就审核结论达成一致。

如果监督审核发现不符合项和观察项应开具不符合项报告，且获得获证组织认同。

监督审核结束，审核组应形成是否推荐保持认证注册的结论；如果采用了现场审核，且现场审核和现场见证（验证）需要分开实施，现场见证（验证）需要在现场审核结束后进行，审核组可以在现场审核结束后对获证组织的一体化管理是否满足所有适用的认证依据的要求进行评价，并判断是否推荐保持认证注册。

监督审核结束后，3 个工作日内，审核组长完成审核报告编制工作，并与获证组织进行沟通，确保双方对报告没有歧义。

7.2.8. 认证决定

中心应指派认证决定人员，对获证组织的认证申请实施认证决定，以决定：

1）同意保持认证注册，颁发认证标志；

2）补充认证决定所需的信息，包括但不限于申请材料、审核材料，再行决定；

3）不同意保持认证注册，做出暂定或撤销的决定，通知获证组织不同意保持的理由。

认证决定人员实施认证决定时应以认证过程中收集的信息和其他相关信息为基础，以充分的证据证实获证组织一体化管理得到了建立、实施、运行、监视、评审、保持和改进。

7.2.9. 审核方案记录与变更

审核方案管理人员应收集监督审核和认证决定的信息，特别是形成的结论和变化的信息，记录到审核方案中。 并确定审核方案是否需要进行变更，如需要则更新相应项目内容。

7.3. 再认证

认证证书有效期满前，中心根据获证组织的申请对获证组织实施再认证，以保证一体化管理认证证书持续有效。

再认证审核的形式和过程与初次认证保持一致，但再认证的一阶段审核可以与二阶段审核一起进行，但当获证组织或其一体化管理的运作环境（如法律的变更）有重大变更时，再认证审核活动可能需要有单独的第一阶段审核。

再认证审核将包括针对下列方面的现场审核

1）结合内部和外部变更来看的整个一体化管理的有效性，以及认证范围的持续相关性和适宜性；

2）经证实的对保持一体化管理有效性并改进一体化管理，以提高整体绩效的承诺；

3）一体化管理在实现获证客户的目标和一体化管理预期结果方面的有效性。

7.4. 特殊审核

7.4.1. 变更或扩大认证范围

获证组织申请变更或扩大认证范围时，中心应按再认证的过程对获证组织变更或扩大认证范围进行特殊审核，最终形成是否同意变更或扩大认证注册范围的决定。变更或扩大认证范围的审核活动可单独进行，也可和对获证组织的监督审核或再认证一起进行。

中心为调查投诉、对变更做出回应或对被暂停认证资格的获证组织进行追踪时，应指派审核组在提前较短时间通知获证组织后对其进行特殊审核。特殊审核以现场审核方式进行，此时：

1） 应向获证组织说明并使其提前了解将在何种条件下进行此类审核；

2） 由于获证组织缺乏对审核组成员的任命表示反对的机会，中心应在指派审核组时给

予更多的关注；

3) 审核组应制订审核计划，形成审核结论；

4) 中心应根据审核结论作出认证决定。

7.4.2. 审核方案记录与变更

审核方案管理人员应收集特殊审核的信息，特别是形成的结论和变化的信息，记录到审核方案中。 并确定审核方案是否需要进行变更，如需要则更新相应项目内容。

7.5. 暂停、撤消认证或缩小认证范围

7.5.1. 中心应有暂停、撤消认证或缩小一体化管理认证范围的政策和形成文件的程序，并规定中心的后续措施。

7.5.2. 发生以下情况(但不限于)时，中心应暂停获证组织的一体化管理认证资格：

1) 获证组织的一体化管理持续地或严重地不满足认证要求，包括对一体化管理有效性的要求；

2) 获证组织不允许按要求的频次实施监督或再认证审核；

3) 获证组织不接受或不配合认证认可监督管理部门的监督管理；

4) 获证组织主动请求暂停。

7.5.3. 认证资格暂停期最长不超过 6 个月。

7.5.4. 在暂停认证期间，获证组织的一体化管理认证证书暂时无效。中心应做出具有强制实施力的安排，避免暂停认证期间获证组织继续宣传一体化管理认证资格。中心应使认证证书的暂停信息可公开获取。

7.5.5. 如果获证组织未能在中心规定的时限内解决造成暂停认证的问题，中心应撤消其一体化管理认证或缩小其相应的认证范围。

7.5.6. 如果获证组织在认证范围的某些部分持续地或严重地不满足认证要求，中心应缩小其一体化管理认证范围，以排除不满足要求的部分。认证范围的缩小应与认证标准的要求一致。

7.5.7. 中心应与获证组织就撤消一体化管理认证时的要求做出具有强制实施力的安排，以确保获证组织接到撤消认证的通知时，立即停止使用任何引用一体化管理认证资格的广告材料。

7.5.8. 在任何组织提出请求时，中心应正确说明获证组织的一体化管理认证被暂停、撤消或缩小的情况。

8. 认证证书

8.1. 证书有效期

信息安全一体化管理认证证书有效期为三年

8.2. 证书内容

8.2.1. 认证证书内容应以中文书写，至少包括以下方面：

1) 认证证书名称，例如：信息安全管理体系认证证书；
2) 符合本规则 8.2 项规定的证书编号；
3) 获证组织名称、注册地址、获证地址和邮政编码；
4) 符合本规则 2 项的认证依据；
5) 通过认证的业务类别；
6) 颁证日期、换证日期以及证书有效期的起止年月日。如颁证日期：2002 年 5 月 1 日，有效期：2002 年 5 月 1 日至 2005 年 4 月 30 日；
7) 中心的名称及其标志；
8) 中心的印章和法定代表人代表或其授权人的签字；
9) 认可标识及认可注册号(应为国家认监委确定的认可机构的标识，以申请认可为目的发出的证书可没有此内容)；

8.2.2. 如果认证所覆盖业务(或服务)的类别及其所涉及的过程和覆盖的场所较多，需在证书附件上加以注明。

8.3. 证书编号

8.3.1. 对同一个受审核方实施的同一套一体化管理进行认证，赋予一个认证证书编号。

8.3.2. 证书编号规则由中心进行明确规定

8.3.3. 同一个组织的认证范围覆盖多个场所并需要颁发子证书时，在子认证证书编号后加上“-”和序号，如-1(-2，-3，…)。

8.3.4. 有效期内换发证书，认证证书编号中的机构注册号、年份号、顺序号和认证的有效期保持不变，应注明换证日期。

8.3.5. 撤销证书后，原认证证书编号废止，不再它用。

8.3.6. 认证证书上的中心名称应与相应的中心批准书上的名称一致。

8.4. 对获证组织正确宣传认证结果的控制

中心应采取授权使用标识的方式来要求获证组织在认证结果的宣传和使用中采用本规则确定的认证依据，同时注明通过认证的业务类别和认证证书编号。在认证证书被暂停期间或撤销后，应收回相应的授权。

不应授权获证组织在产品上使用上述标识，或以表示产品合格的方式使用上述标识。

9. 对获证组织的信息通报要求及响应

为确保获证组织的一体化管理持续有效，中心应要求获证组织建立信息通报制度，及时向中心通报以下信息：

1) 业务、地点、组织机构变化等情况的信息(及时通报)；

2) 顾客投诉的相关信息(每三个月通报一次)；

3) 组织的体系文件和业务重大变化时进行通报；

4) 有严重一体化管理相关事故的信息(及时通报)

5) 其他重要信息。(视情况)

中心应对上述信息以及收集到的相关公共信息进行分析，视情况采取相应措施，包括增加监督审核频次在内的措施和暂停或撤销认证资格的措施。在发生重大客户投诉等严重情况时，中心需立即采取措施。