GB/T 37988

数据安全能力成熟度服务认证规则

文件编号：ISCCA-S-A-0D

发布日期：2026-04-15

实施日期：2026-04-15

版　　本：v1.0

中互协（北京）检测认证中心有限公司发布

目 录

1. 适用范围

本认证规则适用于数据安全能力成熟度服务认证活动。

2. 认证依据

GB/T 37988-2019《信息安全技术　数据安全能力成熟度模型》。

3. 认证模式

选择既往服务足迹检测（验证感知）（简称模式F）、服务能力确认或验证（简称模式G）的服务特性测评方式，以及服务管理审核（简称模式I）。

4. 认证领域

本认证规则认证的服务，属于“电信服务；信息检索及提供服务”领域之下的“数据安全能力成熟度服务”。

5. 认证等级

本认证规则及对应的认证依据，对数据安全能力成熟度服务的认证划分为五个等级：

等级 1：非正式执行

等级 2：计划跟踪

等级 3：充分定义

等级 4：量化控制

等级 5：持续优化

等级 1 为最低等级，等级 5 为最高等级。

6. 认证主要流程

1）认证申请评审

2）认证方案策划

3）初次认证审核

(1) 审核实施

(2) 复核

(3) 认证决定

5) 监督审核

6) 再认证审核

7）特殊审核（需要时）

7. 认证实施

7.1 认证申请评审

7.1.1 认证委托

认证委托人可通过电话、信函、传真、邮件或登录中互协（北京）检测认证中心有限公司（以下简称“中互协认证”）网站的业务管理系统提交申请，并提供认证申请书及相关附件，附件包括但不限于：

1）数据安全能力成熟度服务提供者的社会统一机构代码营业执照或其他证明性文件；

2）数据安全能力成熟度服务提供者的组织介绍、组织架构图及各部门职能说明；

3）数据安全能力成熟度服务提供者的专职技术人员名单（包括技术负责人、技术人员等）；

4）数据安全能力成熟度服务相关的服务流程和服务规范。

7.1.2 申请评审

中互协认证对认证委托人提交的认证申请书等资料进行评审，根据评审结果发出受理通知或问题通知。认证委托人收到问题通知后，将改进情况反馈给中互协认证。对于仍不满足受理要求的申请，中互协认证再次发出问题通知。

7.1.3 签订认证合同

在实施认证审核前，中互协认证与申请组织应订立具有法律效力的书面认证合同，合同应至少包含以下内容：

（1）申请组织获得认证后持续有效提供服务的承诺。

（2）申请组织对遵守认证认可相关法律法规，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的承诺。

（3）申请组织承诺获得认证后发生以下情况时，应及时向中互协认证通报：

①客户及相关方有重大投诉。

②生产、销售的产品或提供的服务被监管部门认定不合格。

③发生产品和服务的质量事故、数据安全事故或其他事故。

④相关情况发生变更，包括：法律地位、生产经营状况、组织状态或所有权变更；取得的行政许可资格、强制性认证或其他资质证书变更；法定代表人、最高

管理者变更；生产经营或服务的工作场所变更；服务覆盖的活动范围变更；服务和重要过程的重大变更等。

⑤出现影响服务提供的其他重要情况。

（4）申请组织承诺获得认证后正确使用认证证书、认证标志和有关信息，不利用服务认证证书和相关文字、符号误导公众认为其产品或管理体系通过认证。

（5）拟认证的服务范围。

（6）在认证审核实施过程及认证证书有效期内，中互协认证和申请组织各自应当承担的责任、权利和义务。

（7）认证服务的费用、付费方式及违约条款。

7.2 审核方案策划

7.2.1 审核模式

依据“3.认证模式”的内容，确定初次认证审核、监督审核、再认证审核所选用的审核模式。

初次认证审核：选择既往服务足迹检测（验证感知）（简称模式F）、服务能力确认或验证（简称模式G）的服务特性测评方式，以及服务管理审核（简称模式I）。

监督审核：选择既往服务足迹检测（验证感知）（简称模式F）、服务能力确认或验证（简称模式G）的服务特性测评方式，以及服务管理审核（简称模式I）。

再认证审核：选择既往服务足迹检测（验证感知）（简称模式F）、服务能力确认或验证（简称模式G）的服务特性测评方式，以及服务管理审核（简称模式I）。

服务特性测评要求见附录B。

服务管理审核要求见附录C。

7.2.2 审核时间

初次认证审核的内容为认证依据标准规定的全部条款。初次认证现场审核按3 人日计费。

监督审核的内容为认证依据标准规定的部分条款。一次监督审核按1人日计费。

再认证审核的内容为认证依据标准规定的全部条款。再认证审核按2人日计费。

7.2.3 审核组

中互协认证根据服务领域选择具备相关能力的审查员组成审核组，必要时可以选择技术专家参加审核组。审核组中的审查员承担审核任务和责任。

技术专家主要负责提供认证审核的技术支持，不作为审查员实施审核，不计入审核时间，其在审核过程中的活动由审核组中的审查员承担责任。

审核组可以有实习审查员，其要在审查员的指导下参与审核，不计入审核时间，不单独出具记录等审核文件，其在审核过程中的活动由审核组中的审查员承担责任。

7.2.4 审核抽样

多场所抽样：

如果服务覆盖范围包括在多个场所进行相同或相近的活动，且这些场所都处于申请组织授权和控制下，中互协认证可以在审核中对这些场所进行抽样，但应根据相关要求实施抽样以确保对所抽样本进行的审核对服务的所有场所具有代表性。如果不同场所的活动存在明显差异、或不同场所间存在可能对服务提供有显著影响的区域性因素，则不能采用抽样审核的方法，应当逐一到各现场进行审核。多场所抽样的条件及抽样规则见“附录A：多场所组织的服务认证审核”。

7.2.5 审核计划

中互协认证为每次审核制定书面的审核计划。审核计划至少包括以下内容：审核目的，审核准则，审核范围，现场审核的日期和场所，现场审核持续时间，审核组成员（其中：审查员应标明审核员注册号;技术专家应标明专业代码、工作单位及专业技术职称）。

为使现场审核活动能够观察到服务活动情况，现场审核应安排在认证范围覆盖的服务活动正常提供时进行。

在审核活动开始前，审核组应将审核计划交申请组织确认，遇特殊情况临时变更计划时，应及时将变更情况通知申请组织，并协商一致。

7.3 初次认证审核

7.3.1 审核实施

中互协认证通知认证委托人进行现场审核， 并委派审核组对数据安全能力成熟度服务提供者实施现场审核。

初次认证审核的内容为认证依据标准规定的全部条款。

初次认证审核的审核组应通过既往服务足迹检测（验证感知）（简称模式F）、服务能力确认或验证（简称模式G）方式对受审核方提供的服务进行服务特性测评，以确认受审核方所提供的服务是否符合服务特性要求；初次认证审核的审核组应通过服务管理审核（简称模式I）方式对受审核方所提供服务的管理情况进行审核，以确认受审核方所提供的服务是否符合服务管理要求。

服务特性测评要求见附录B。

服务管理审核要求见附录C。

按以下步骤对服务特性进行测评、对服务管理进行审核：

1）对数据采集安全、数据传输安全、数据存储安全、数据处理安全、数据交换安全、数据销毁安全、通用安全这7大过程域共30个过程域（PA）中适用的PA进行审核；

2）评价每个适用的PA在组织建设、制度流程、技术工具、人员能力这4个方面的能力具备情况；

3）对每个适用的PA的5个级别的每个级别满足要求的符合度进行评分，评分标准为：

完全不满足：0分

部分满足：0.5分

大部分满足：0.7分

全部满足：1分

4）计算每个PA的等级分值，每个PA的等级分值等于5个级别的符合度分值之和；同时得出每个PA达到的能力级别，PA等级判断依据：

PA = 一级符合度 + 二级符合度 + 三级符合度+ 四级符合度 + 五级符合度

0 < PA < 1: 一级

1 < PA < 2: 二级

2 < PA < 3: 三级

3 < PA < 4: 四级

4 < PA < 5: 五级

5）计算7大过程域的得分，每个大过程域的得分等于所含PA的等级分值之和除以PA个数:

数据采集安全 = (PA01 + PA02 + PA03 + PA04)/4

数据传输安全 = (PA05 + PA06)/2

数据存储安全 = (PA07 + PA08 + PA09)/3

数据处理安全 = (PA10 + PA11 + PA12 + PA13 + PA14)/5

数据交换安全 = (PA15 + PA16 + PA17)/3

数据销毁安全 = (PA18 + PA19)/2

通 用 安 全 = (PA20 + PA21 + ...+ PA29 + PA30)/11

6）计算能力成熟度等级得分，能力成熟度等级得分等于7大过程域得分值之和除以7:

能力成熟度等级得分 = 7大过程域的总分/ 7（小数点后取两位）

=（数据采集安全 + 数据传输安全 + 数据存储安全 + 数据处理安全 +

数据交换安全 + 数据销毁安全 + 通用 安全）/ 7

7）确定能力成熟度等级：

0 < 能力成熟度等级得分 < 1: 一级

1 < 能力成熟度等级得分 < 2: 二级

2 < 能力成熟度等级得分 < 3: 三级

3 < 能力成熟度等级得分 < 4: 四级

4 < 能力成熟度等级得分 < 5: 五级

审核组完成审核任务后， 向中互协认证提交审核资料，包括审核记录和审核报告等材料。

7.3.2 复核

中互协认证对认证申请相关信息及审核结果进行复核，形成复核结论。复核应由未参与审核过程的中互协认证人员承担。

7.3.3 认证决定

中互协认证对认证申请相关信息、复核结果及其他信息进行综合评价， 做出认证决定。符合认证要求中互协认证将颁发认证证书， 不满足认证要求不予颁发认证证书，并通知认证委托人。

7.4 监督审核

7.4.1 频次和方式

中互协认证在一个认证周期内委派审核组对获证组织进行两次现场监督审核。监督审核周期不大于12个月。

7.4.2 监督实施

监督审核内容为认证依据标准规定的部分条款。两次监督审核覆盖认证依据标准规定的所有条款。

监督审核的审核组应通过既往服务足迹检测（验证感知）（简称模式F）、服务能力确认或验证（简称模式G）方式对获证组织提供的服务进行服务特性测评，以确认获证组织所提供的服务是否持续符合服务特性要求；监督审核的审核组应通过服务管理审核（简称模式I）方式对获证组织所提供服务的管理情况进行审核，以确认获证组织所提供的服务是否持续符合服务管理要求。

服务特性测评要求见附录B。

服务管理审核要求见附录C。

审核组完成审核任务后， 向中互协认证提交审核资料，包括审核记录和审核报告等材料。

7.4.3 复核

中互协认证对认证申请相关信息及审核结果进行复核，形成复核结论。复核应由未参与审核过程的中互协认证人员承担。

7.4.4 认证决定

中互协认证对监督审核相关信息、复核结果及其他信息做出认证决定，符合认证要求保持认证证书，并通知获证组织；不满足认证要求暂停或撤销认证证书，通知获证组织，并予以公示。

7.5 再认证审核

7.5.1 审核方式

在认证证书到期前3个月内应进行再认证审核。中互协认证委派审核组对获证组织进行现场审核。

7.5.2 审核实施

再认证审核内容为认证依据标准规定的全部条款。

再认证审核的审核组应通过既往服务足迹检测（验证感知）（简称模式F）、服务能力确认或验证（简称模式G）方式对获证组织提供的进行服务特性测评，以确认获证组织所提供的服务是否持续符合服务特性要求；再认证审核的审核组应通过服务管理审核（简称模式I）方式对获证组织所提供服务的管理情况进行审核，以确认获证组织所提供的服务是否持续符合服务管理要求。

服务特性测评要求见附录B。

服务管理审核要求见附录C。

审核组完成审核任务后， 向中互协认证提交审核资料，包括审核记录和审核报告等材料。

7.5.3 复核

中互协认证对认证申请相关信息及审核结果进行复核，形成复核结论。复核应由未参与审核过程的中互协认证人员承担。

7.5.3 认证决定

中互协认证对再认证审核相关信息、复核结果及其他信息做出认证决定，符合认证要求的换发新的认证证书，并通知认证委托人；不满足认证要求的不换发新的认证证书，通知认证委托人，原证书过期失效。

7.6 特殊审核

中互协认证可视情况对获证组织实施特殊审核。

8. 认证证书及认证标志

8.1 认证证书内容

证书内容应至少包括以下方面：

1）认证证书名称；

2）证书编号；

3）认证委托人名称、地址；

4）认证依据的标准、技术要求；

5）获得认证的服务所覆盖的业务范围；

6）首次颁证日期、发证日期以及证书有效期；

7）认证标志（中互协认证的LOGO）；

8）相关的认可标识及认可注册号（适用时）。

8.2 认证证书状态管理

8.2.1 认证证书的保持

证书有效期为 3 年。在有效期内，证书的有效性依赖中互协认证的监督审核获得保持。

8.2.2 认证证书的变更

证书内容发生变更时， 认证委托人应向中互协认证提出变更申请，并按照要求提交相关资料。中互协认证进行必要的审核、复核并做出认证决定。

8.2.3 认证证书的注销

认证委托人有下列情形之一，中互协认证进行必要的审核、复核并做出认证决定，注销认证证书，通知认证委托人，并予以公示：

1） 因自身原因申请注销；

2） 认证依据标准、实施规则换版，认证委托人未按时提交换版申请；

3） 其他应注销认证证书的情况。

8.2.4 认证证书的暂停

认证委托人有下列情形之一，中互协认证进行必要的审核、复核并做出认证决定， 暂停认证证书，通知认证委托人， 并予以公示：

1）监督结果证明数据安全能力成熟度服务提供者/认证委托人不满足认证要求，但不需要立即撤销认证证书的；

2）逾期未按规定接受监督；

3）违规使用认证证书，且未造成不良影响；

4）因自身原因申请暂停；

5）其他应暂停认证证书的情况。

6）证书暂停期限最长为6个月。

8.2.5 认证证书的恢复

1）证书暂停期限内，认证委托人可向中互协认证提出恢复申请。

2）获证客户已针对暂停认证资格的原因采取了有效的纠正措施，产生原因已经消除，认证资格的恢复符合相关的认证要求，同时已证实在暂停期内没有使用、引用认证资格（如广告宣传）和使用认证标志。

3） 需要时，获证客户应提交相关纠正措施和有效性验证材料。

4）中互协认证进行必要的审核、复核，确认获证客户在暂停认证资格的认证范围内已恢复符合相关的认证要求，作出同意恢复认证资格的认证决定，颁发《恢复使用认证证书和标志的通知》并公告。

8.2.6 认证证书的撤销

认证委托人有下列情形之一，中互协认证进行必要的审核、复核并做出认证决定，撤销其认证证书，通知认证委托人，并予以公示：

1）在认证证书暂停期限届满，认证委托人未提出认证证书恢复申请、未采取整改措施或整改后仍不合格的；

2）因8.2.4 2）条款被暂停认证证书后，仍拒绝接受监督的；

3）违规使用认证证书，造成不良影响；

4）数据安全能力成熟度服务提供者出现严重责任事故、被投诉且经核实，影响其继续有效提供服务；

5）其他应撤销证书的情况。

9. 认证证书的使用

认证委托人在经营活动中使用认证证书时，应当与认证证书的内容相一致。

10. 认证收费

中互协认证按照对外公开的有关规定收取认证费用。

11. 与技术争议、申诉相关的流程及时限要求

1）认证委托人可通过电话、电子邮件等方式，对于认证环节的技术争议或其他问题向中互协认证进行申诉。

2）中互协认证收到申诉后，对反映情况和提供资料进行核实。

3）认证委托人对于处理结果仍存在争议时，可在收到处理结果后15个工作日内再次提出争议处理申请。

12. 认证责任

1）中互协认证遵循国家法律法规、认证实施规则的要求和程序从事认证活动。

2）中互协认证及其认证人员根据实施规则做出认证结论，并保证认证结论的客观性、真实性。

3）中互协认证向认证委托人出具认证证书，并对认证结果负责。

4）中互协认证派遣具备资格的审查员实施审核。审查员应根据中互协认证要求，及时有效完成审核任务。中互协认证及审查员对审核结论负责。

5）认证委托人应配合中互协认证开展认证活动。

6）认证委托人应对提交的认证资料和信息的真实性、合法性负责。当认证信息发生变化时， 认证委托人应及时通知中互协认证。

附录A：多场所组织的服务认证审核

A.0 术语定义

A.0.1 常设场所

客户组织持续进行工作或提供服务的场所（有形或虚拟）。

A.0.2 临时场所

客户组织为在有限时期内进行特定工作或提供服务而设立的场所（有形或虚拟），该场所不准备作为常设场所。

A.0.3 多场所组织

提供服务的一个组织，其构成包括经识别的中心职能以及多个场所，中心职能（并不必须是组织的总部）对某些过程、活动进行策划和控制，在多个场所（常设的、临时的或虚拟的）中这些过程、活动得到全部或部分实施。

A.0.4 中心职能

对提供服务负责并对服务集中控制的职能。

中心职能是组织的一部分并且不应被分包给外部的组织。

中心职能应有责任确保来自于所有场所的数据得到收集和分析，并且应能够证明其权威和能力，以便在需要时（包括但不限于下述情况）发起组织的变更：

(1) 服务文件和服务变更；

(2) 投诉；

(3) 纠正措施的评价；

(4) 与适用标准有关的法律法规要求。

中心职能是实施控制并得到组织最高管理者授权的，是对所有场所产生影响的。

并不要求中心职能仅处于某个单一场所。

A.0.5 虚拟场所

虚拟地点指客户组织完成工作或提供服务所用到的，允许处于不同物理地点的人员执行过程的在线环境。

A.0.6 子范围

单个场所的范围。

单个场所的范围可能与多场所组织的全部范围相同，但也有可能是多场所组织范围的一小部分。

本文件中所说的“子范围”针对认证范围而言。

A.1 多场所抽样方法

A.1.1 应用场所抽样对多场所组织审核的方法

A.1.1.1 条件

A.1.1.1.1 当每个场所均运行非常相似的过程、活动时，允许对这组场所抽样。

A.1.1.1.2 不适用场所抽样的情况：

所有场所实施的过程、活动与服务的范围有关且存在显著差别；

客户要求对每个场所审核；

有专门的方案或法规要求规定了系统性地对每个场所审核。

A.1.1.2 抽样

A.1.1.2.1 样本中应有一部分根据以下因素选取，一部分随机抽取；并且其结果应选到在有代表性的不同场所，确保认证范围内覆盖的所有过程将被审核到。

A.1.1.2.2 至少 25%的样本应随机抽取。

A.1.1.2.3 考虑到下述规定，其余部分的选择应使得证书有效期内所选场所之间的差异尽可能大。

A.1.1.2.4 场所选取应考虑，但不限于以下方面：

以前认证审核的结果；

投诉记录以及纠正和预防措施的其他相关方面；

各场所在规模上的显著差异；

在倒班安排和工作程序上的差异；

服务以及在场所实施过程的复杂程度；

上次认证审核后的变化；

服务的成熟度和组织的理解程度；

文化、语言和法律法规方面的差异；

地理位置的分散程度；

场所是常设的、临时的或虚拟的。

A.1.1.3 抽样数量

A.1.1.3.1 确定抽样数量，应考虑本部分描述的所有因素。

A.1.1.3.2 应对每个多场所组织每次应用抽样形成记录，证明符合本规则的要求。

A.1.1.3.3 每次审核最少审核的场所数量是：

初次认证审核：样本的数量应为场所数量的平方根（$y=\sqrt{x}$），计算结果向上取整为最接近的整数，其中 y 为将抽取场所的数量、x 为场所总数。

监督审核：每年的抽样数量应为场所数量的平方根乘以 0.6 即（$y=0.6\sqrt{x}$），计算结果向上取整为最接近的整数。

再认证审核：样本的数量应与初次审核相同。然而，如果证明服务在认证周期中是有效的，样本的数量可以减少至乘以系数 0.8 即（$y=0.8\sqrt{x}$），计算结果向上取整为最接近的整数。

A.1.1.3.4 在初次认证审核、每次再认证审核以及作为监督的一部分在每个日历年至少一次的审核中，都应对中心职能审核。

A.1.1.3.5 当对拟认证或获证服务涵盖的过程、活动进行风险分析，发现涉及下列因素的特殊情况时，应增加抽样的数量或频率。

场所的规模和员工的数量；

过程、活动以及服务复杂程度和风险水平；

工作方式的差异（如：倒班）；

所从事过程、活动的差异；

投诉记录，以及纠正措施和预防措施的其他相关方面；

与跨国经营有关的任何方面。

A.1.1.3.6 如果组织的分支机构分为不同等级（如：总部办公室/中心办公室，全国性办公室，地区办公室，地方分支），上述的初次认证审核抽样模式适用于每个等级的场所。

示例：

1 个总部办公室：每个审核周期（初次审核、监督审核或再认证审核）都审核；

4 个全国性办公室：样本数量＝2，至少 1 个为随机抽样；

27 个地区办公室：样本数量＝6，至少 2 个为随机抽样；

1700 个地方分支：样本数量＝42，至少 11 个为随机抽样。

地区办公室的样本中宜至少覆盖到每个全国办公室控制的地区办公室。地方分支的样本中宜至少覆盖到每个地区办公室控制的地区分支。这样可能导致每个等级的场所抽样数量超过按照第 1.1.3.3 条计算的最小抽样数量。

A.1.1.3.7 抽样过程应作为审核方案管理的一部分。在任何时候（即：在策划监督审核之前、或组织的任何场所变更其结构时、或将在认证边界之内增加新的场所时），应预先评审审核方案中的抽样安排，以便在为保持认证对样本审核之前能确定抽样数量调整的需求。

A.1.1.4 增加场所

A.1.1.4.1 如果对已认证的多场所组织增加新场所或增加一组新的场所，应确定在证书中增加这些新场所前所需实施的必要活动。这应包括考虑是否对新场所审核。

在新场所纳入证书后，需要确定后续监督或再认证审核的抽样数量。

A.1.2 对不适用 B.1.1 条场所抽样的多场所组织审核的方法

A.1.2.1 审核方案的构成应包括对所有场所的初次认证审核和再认证审核。在监督审核中，应在每个日历年覆盖 30%的场所（向上取整至整数）。每次审核都包括中心职能。第二次监督审核选取的场所通常不同于第一次监督审核所选取的场所。

A.1.2.2 审核方案的设计应确保在认证范围覆盖的所有过程在每个周期内被审核到。

A.1.2.3 增加场所

如果对已认证的多场所组织增加一个新场所，除了在审核方案中策划监督之外，该场所应在被增加到证书中之前被审核到。在新场所纳入证书后，为确定后续监督或再认证审核的审核时间应将其与以前的场所累计。

A.1.3 对场所构成中部分可抽样部分不可以抽样的多场所组织审核的方法

应按照第 A.1.1 条对可抽样的场所并按照第 A.1.2 条对组织中剩余不适用抽样的场所建立审核方案。

A.2 审核与认证

A.2.1 申请与申请评审

A.2.1.1 应获得有关申请组织的必要信息，以：

确定服务提供范围及寻求认证的范围，以及适用时的子范围；

理解每个场所的法律与合同安排；

理解“在哪里发生了什么”，即：确定每个场所提供的过程、活动，并识别中心职能；

确定向所有场所提供的过程、活动的集中化程度；

确定在不同场所之间的接口；

确定哪些场所适用抽样（即，哪些场所提供非常相似的过程、活动），以及哪些场所不具备抽样资格；

纳入考虑的其他相关因素；

确定组织的审核时间；

确定审核组的能力要求；

识别服务的过程、活动的复杂程度和规模范围（如：一个或多个）。

A.2.2 审核方案

A.2.2.1 除了 “7.2审核方案策划”的要求外，审核方案还应至少包括或引用下述内容：

每个场所的过程、活动；

识别哪些场所可以被抽样、哪些场所不能；

识别哪些场所被抽样覆盖、哪些场所未被抽样覆盖。

A.2.2.2 当确定审核方案时，由于被审核组织的特定结构，应为额外活动给予充分的时间，这些活动的时间不计入审核时间，例如：用于路途、审核组成员之间联系、审核后会议等。

如果拟审核过程的属性适用于远程审核，可使用远程审核技术。

A.2.2.3 在任何时候使用多于一名成员构成审核组时，审核策划人员应有责任与审核组长协同识别出对每个场所及每一部分审核所需的技术能力，并为审核的每一部分分派适当的审核组成员。

A.2.3 审核时间计算

A.2.3.1 符合资格准则的组织，可以由可抽样场所构成、不可抽样场所构成，或由这两种情况组合构成。无论组织由何种方式构成，必须有充足的审核时间来实施有效的审核。

应考虑不同场所之间往来路上所需要的时间。这部分不计入审核时间，需要额外预留出来，以保证现场审核的时间满足规定的要求。

A.2.4 审核计划

A.2.4.1 除了 “7.2.5 审核计划”的要求外，在准备审核计划时还应至少考虑下述内容：

认证范围以及每个场所的子范围；

在同时申请多个服务认证的情况下，每个场所提供的服务；

拟审核的过程、活动；

每个场所的审核时间；

分派审核组。

A.2.5 初次认证审核

初次认证审核的输出中，审核组对每个场所抽取了哪些过程来审核应形成文件。

这些信息将用于修正审核方案以及后续监督审核的审核计划。

A.2.6 认证文件

A.2.6.1 认证文件应反映认证范围以及多场所认证所覆盖的场所、法律实体（适用时）。

A.2.6.2 认证文件应包含所有场所的名称和地址，反映出组织与认证文件相关。范围或认证文件引用的其他信息应清晰表明经认证的活动由清单中所列场所实施。然而，如果某一场所的活动仅是包含于组织范围内的一部分，认证文件应包括该场所的子范围。当在认证文件上展示临时场所时，应注明这些场所为临时场所。

A.2.6.3 如果向一个场所颁发认证文件，其中应包括：

该认证所覆盖对特定场所、法律实体的活动；

与主证书之间的可追溯性，如：编号/代码；

声明：子证书的有效性取决于主证书有效。

A.2.6.4 一旦任何场所不能满足保持认证的必要规定，认证文件将被整体撤销。

A.2.7 监督审核

A.2.7.1 对可以抽样多场所组织的监督审核应与 A.1.1 条一致。

A.2.7.2 对不能按照 A.1.1 条抽样的多场所组织，监督基于对 30%场所的审核外加对中心职能的审核。认证周期中第二次监督选取的场所通常应不包括第一次监督所选取的场所。

A.2.8 再认证审核

A.2.8.1 对可以抽样多场所组织的再认证审核应与 A.1.1 条一致。

A.2.8.2 对不能抽样的多场所组织，再认证应按照初次认证审核，即对所有场所外加中心职能审核。

附录B：服务特性测评要求

数据安全能力成熟度服务的服务特性测评要求包括数据采集安全、数据传输安全、数据存储安全、数据处理安全、数据交换安全、数据销毁安全六大方面的测评：

服务特性		测评要求
B.1 数据采集安全	PA01 数据分类分级	满足认证依据6.1条款的要求
	PA02 数据采集安全管理	满足认证依据6.2条款的要求
	PA03 数据源鉴别及记录	满足认证依据6.3条款的要求
	PA04 数据质量管理	满足认证依据6.4条款的要求
B.2 数据传输安全	PA05 数据传输加密	满足认证依据7.1条款的要求
	PA06 网络可用性管理	满足认证依据7.2条款的要求
B.3 数据存储安全	PA07 存储媒体安全	满足认证依据8.1条款的要求
	PA08 逻辑存储安全	满足认证依据8.2条款的要求
	PA09 数据备份与恢复	满足认证依据8.3条款的要求
B.4 数据处理安全	PA10 数据脱敏	满足认证依据9.1条款的要求
	PA11 数据分析安全	满足认证依据9.2条款的要求
	PA12 数据正当使用	满足认证依据9.3条款的要求
	PA13 数据处理环境安全	满足认证依据9.4条款的要求
	PA14 数据导入导出安全	满足认证依据9.5条款的要求
B.5 数据交换安全	PA15 数据共享安全	满足认证依据10.1条款的要求
	PA16 数据发布安全	满足认证依据10.2条款的要求
	PA17 数据接口安全	满足认证依据10.3条款的要求
B.6 数据销毁安全	PA18 数据销毁处置	满足认证依据11.1条款的要求
	PA19 存储媒体销毁处置	满足认证依据11.2条款的要求

附录C：服务管理审核要求

服务管理		审核要求
通用要求	PA20 数据安全策略规划	满足认证依据12.1条款的要求
	PA21 组织和人员管理	满足认证依据12.2条款的要求
	PA22 合规管理	满足认证依据12.3条款的要求
	PA23 数据资产管理	满足认证依据12.4条款的要求

	PA24 数据供应链安全	满足认证依据12.5条款的要求
	PA25 元数据管理	满足认证依据12.6条款的要求
	PA26 终端数据安全	满足认证依据12.7条款的要求
	PA27 监控与审计	满足认证依据12.8条款的要求
	PA28 鉴别与访问控制	满足认证依据12.9条款的要求
	PA29 需求分析	满足认证依据12.10条款的要求
	PA30 安全事件应急	满足认证依据12.11条款的要求