美华国际认证检验有限公司

【数据存储安全管理体系认证规则】

文件编号：MHGJ-GL-062

发布日期：2024-11-04

修订日期：2025-05-14

实施日期：2025-05-14

版本/版次：A/1

编制部门：技术部

文件制/修订履历

制/修订日期	制/修订单号	制/修订类别	版本/版次	制/修订说明（原因、内容见制修订审批单）
2024.11.04	初始制订	■制订 □修订	A/0	初始发布、实施
2025.05.14	修订	■修订	A/1	认证规则修订

数据存储安全管理体系认证规则

1 目的和范围

1.1本规则适用于美华国际认证检验有限公司（以下简称美华国际或MHGJ）的数据存储安全管理体系认证活动。

1.2本规则依据认证认可相关法律法规，结合相关技术标准，对规范数据存储安全管理体系认证过程作出具体规定，明确数据存储安全管理体系认证过程的相关责任，保证数据存储安全管理体系认证活动的规范有效。

1.3本规则作为本机构在 数据存储安全管理体系认证活动中应遵守的基本要求。

2 本机构的管理要求

2.1本机构参照 ISO/IEC 17021-1:2015 《合格评定 管理体系审核与认证机构的要求 第1部分：要求》，数据存储安全管理体系认证所涉及的能力和过程。

2.2本机构建立内部制约、监督和责任机制，实现数据存储安全管理体系认证申请评审、认证审核和认证决定等工作环节相互分开，以符合公正性要求。

3 认证人员要求

参与数据存储安全管理体系认证的认证审核人员应符合以下条件：

（1）现场审核员条件：

a）取得中国认证认可协会（CCAA）的管理体系实习审核员以上（含）或一般服务认证注册审查员资格；

b）管理体系审核员或服务认证审查员通用能力评价合格；

c）数据存储安全管理体系认证专业培训考核合格。

4 认证依据

4.1 数据存储安全管理体系认证依据：ISO /IEC 27040:2024《**信息技术 安全技术 存储安全**》和客户要求；适用时还可包括各地方与数据存储安全管理体系认证相关的标准；

4.2相关的数据存储安全管理体系认证法律法规及其它要求。

5 初次认证程序

5.1认证申请

5.1.1认证申请组织应具备以下条件：

（1）中国企业持有工商行政管理部门颁发的《企业法人营业执照》，或等效的文件；外国企业持有有关机构的登记注册证明；

（2）有相应的许可资质（有资质要求适用时）

（3）生产、加工的产品或提供的服务符合相关法律法规要求（特殊产品/服务适用）；

（4）建立和实施了数据存储安全管理体系认证管理体系，且有效运行 3个月以上；

（5）在一年内，未发生返数据存储安全管理体系认证的相关法规，或未因负面情况而被其他相关认证机构撤销数据存储安全管理体系认证证书；

（6）企业已经进行了内部审核和管理评审；

(7) 没有被执法监管部门责令停业整顿，未列入国家信用信息严重失信主体相关名录。

5.1.2 认证申请组织应提交的文件和资料：

（1）认证申请表（签字、加盖公章）；

（2）营业执照、组织机构代码证书复印件（签字、加盖公章并标注“同原件”）；

（3）行政许可文件证明文件（适用时，签字、加盖公章并标注“同原件”）；

（4）数据存储安全管理体系认证文件；

（5）多场所/网点清单（至少包括：名称、地址、距离、售后服务的商品类别、联系方式等）；

（6）适用的法律法规和标准清单；

（7）一年内无行贿犯罪记录的证明；

（8）其他需要的文件。

5.2 受理认证申请

5.2.1 申请评审

5.2.1.1基本信息及审核能力评审

本机构根据申请认证的范围、认证覆盖场所、员工总数、认证覆盖人数、体系运行状况、组织基本情况、完成认证活动所需时间、申请方和其他影响认证活动的因素，对认证申请组织提交的申请资料进行评审，并保存评审记录，综合确定是否受理认证申请。

注1：员工总数是仅指在认证覆盖的业务活动边界、地点边界、及组织边界内的直接相关人员数量，不一定是组织的所有员工数量。例如：保安服务、清洁服务、物业服务等行业的无直接关系人员，不记入员工总数。

注2：认证覆盖人数仅指在认证覆盖的业务活动边界、地点边界、及组织边界内的与该认证领域活动直接相关人员数量，不一定是组织的员工人数。例如：保安服务、清洁服务、物业服务等行业的与认证领域活动无直接关系的人员，不记入认证覆盖人数。

5.2.1.2 专业代码确定

因数据存储安全管理体系认证过程管理的重点为数据存储安全管理体系认证，围绕数据存储安全管理体系认证的过程和方法在行业有较强的通用性，因此数据存储安全管理体系认证不再因行业不同而区分不同的专业代码。

5.2.2 评审结果处理

申请材料齐全并符合有关要求的，予以受理认证申请。未通过申请评审的，本机构书面通知申请组织在规定时间内补充和完善，或不受理认证申请并明示理由。

5.2.3 签订认证合同

在实施认证评价之前，通过合同评审，本机构将与认证申请组织订立具有法律效力的书面认证合同，以明确双方的权利和义务等。

5.3 认证审核策划

5.3.1认证审核方法

数据存储安全管理体系认证周期为三年，三年中每年一次监督审核，一个认证周期完成后可进行再认证审核。初次认证分为不到受审核方现场评价的文件评价和到受审核方现场评价的现场评价两个部分，文件评价合格后才可实施现场评价。不到受审核现场实施的文件评价可通查阅标准化体系文件查阅的方式进行。监督评价、再认证评价可直接实施现场评价，但若受审核方文件体系变更较大时，应先实施文件评价。到受审核现场实施的现场评价可通过文件评价、查看、询问、操作演示、结果复核、查阅资料或报告记录、调查统计等方法实施，必要时可采取在线评价的方式实施。

5.3.2 审核时间

为确保认证评价的充分性和有效性，数据存储安全管理体系认证审核人日数应根据体系范围内覆盖的人数、组织管理复杂程度、技术和法规环境、管理体系范围内活动的分包情况、以前审核的结果、场所的数量和对多场所的考虑、与组织的产品以及过程和服务相关联的风险、是否结合审核等因素决定。

5.3.2.1初次认证审核时间

（1）初次认证审核人日数按照如下标准实施

认证覆盖的人数（人）	基础现场审核时间（人.天）
≤100	1.0

101-400	1.5
＞400	2.0

（2）最终认证审核时间因人数、产品和过程复杂程度、以往审核结果等因素，以及审核的有效性和充分性，需要增加或减少审核时间的可适当情况在增加或减少，减少人天的须注明减少的合理理由，审核时间减少最终不得超过基础现场审核时间的30%。

（3）因多场所抽样审核需要增加审核时间的，应按如下标准实施：

抽样场所数量（个）	增加现场审核时间（人.天）
1~5	0-0.5
5~10	0.5-1.0
＞10	1-1.5

（4)现场审核时间合计计算后的最终结果以0.5人天为最小核算单位，计算后不足0.5人天的，以最接近0.5人天的方向调整。

5.3.2.2 监督审核人日数

监督审核时间应不少于初次认证审核的 1/3，但至少1人日。对于与初次认证相比基本情况变化不大的已撤销数据存储安全管理体系认证证书的组织，改善后重新向本机构提出认证申请的，考虑到本机构对该公司的体系运行情况熟悉程度，可按照监督审核时间安排。

5.3.2.3再认证审核人日数

再认证审核时间应不少于初次认证审核的2/3，但至少为1人日。

5.3.3 审核组

5.3.3.1 认证审核部应有根据实现审核目标所需的能力，以及与受审核是否存在利益冲突来选择和任命审核组（包括审核组长）。如果仅有一名审核员，该审核员应有能力履行适用于该审核的审核组长职责，对申请方（受审核方）的数据存储安全管理体系认证实施可信任的审核。

5.3.3.2 决定审核组的规模和组成时，应考虑下列因素：

a) 审核目的、范围、准则和预计的审核时间；

b) 是否是结合、一体化或联合审核；

c) 实现审核目的所需的审核组整体能力；

d）认证要求（包括任何适用的法律、法规或合同要求）；

e）语言和文化；

f）审核组成员以前是否审核过该客户的管理体系。

5.3.3.3 下列情况必须充分考虑审核组专业能力：

a）审核电子化 数据存储安全管理体系认证 的审核员能力和信息安全。

b）考虑配置必要的资源，如计算机及计算机辅助的审核技术，可能包括诸如电视电话会议，网络会议，网络交流，远程电子方式获得 数据存储安全管理体系认证文档和/或数据存储安全管理体系认证过程等，并注意审核有效性和效率审核过程的完整性。

5.3.3.4 使用翻译人员时，翻译人员的选择要避免他们对审核产生不正当影响。

5.3.3.5 审核组长在与审核组商议后，应制定《审核计划》 ，结合《审核计划》，向每个审核组成员分配对特定过程、职能、场所、区域或活动实施审核的职责。所进行的分配应考虑到所需的能力、有效并高效地使用审核组以及审核员的不同作用和职责。在审核进程中，为确保实现审核目的，可以改变工作分配。

5.3.3.6 未被指派为审核员的审核组成员（翻译人员、观察员和实习审核员）所花费的时间不应计入上面所确定的审核时间。使用翻译人员可能需要额外增加审核时间。确定审核时间的过程和结果记入方案策划记录中。

5.3.3.7 审核组任务的沟通

选派审核组应明确说明审核组的任务，并告知客户组织，审核组应：

a）检查和验证客户组织与管理体系相关的结构、方针、过程、程序、记录及相关文件；

b）确定上述方面满足与拟认证范围相关的所有要求；

c）确定客户组织有效地建立、实施并保持了管理体系过程和程序，以便为建立对客户管理体系的信任提供基础；

d）告知客户其方针、目标及指标(与相关管理体系标准或其它规范性文件的期望一致）与结果之间的任何不一致，以使其采取措施。

e)审核组应当全员完成审核计划的全部工作。除不可预见的特殊情况外，审核过程中不得更换审核计划确定的审核员。

5.3.3.8 审核组成员信息的通报

本机构以《审核任务书及派出令》向客户提供审核组每位成员的姓名，并允许客户对审核任组背景确认及合理的调整。

5.3.3.9 审核组成员的任务分工与所具备的专业能力相适应，审核组工作的分配应当考虑审

核员的独立性和能力的需要、资源的有效利用以及审核员的不同作用和职责。

5.3.3.10 审核组成员的所有审核记录都应当交给审核组长，由 MHGJ 集中妥善保管，特别是涉及保密或知识产权信息的工作文件/记录。

5.3.4 多场所审核策划

5.3.4.1 临时场所审核策划

5.3.4.1.1 如果认证申请方或获证客户在临时场所提供其产品（包括服务），该临时场所应被纳入审核方案。

5.3.4.1.2 临时场所可以是较大的项目管理现场，也可以是较小的服务/安装现场。公司宜对临时场所进行抽样审核，但是，可以考虑用下列方法来代替一部分现场审核：

- ✧ 通过面对面或电视电话会议的方式，与客户及（或）其顾客进行访谈，或者参与他们的进度会议；
- ✧ 对临时场所的活动实施文件审查；
- ✧ 远程访问包含同管理体系与临时场所的评审有关的记录或其他信息的电子化场所；
- ✧ 使用电视电话会议及其他技术实施有效的远程审核。

在每种情况下，宜完整地记录审核方法，并充分证明审核方法的有效性。

5.3.4.1.3 临时多场所抽样应按照如下规则来抽样。

a) 不相同/相似经营/服务/经营场所，需全数抽样。（用 Nu 表示）

b) 相同/相似经营/服务/经营场所，按以下表格所对应的抽样数予以抽样。（用 Ns 表示）

相同/相似场所抽样审核(N_s)对照表

相同/相似数量	抽样审核数量	相同/相似数量	抽样审核数量
≤20个	1个	41~50	4个
21~30个	2个	51~60个	5个
31~40个	3个	61~70个	6个
71~80个	7个	81~90个	8个
91~100个	9个	≥101个	10个

认证审核临时多场所总抽样数（用 Nz）：=Nu+Ns

年度监督审核抽样数：不少于按初次认证审查抽样原则总抽样数的 1/3。

再认证审核抽样数：不少于按初次认证审查抽样原则总抽样数的 2/3。

5.3.4.1.4 多场所抽样审核需增加时间的，按照5.3.2.1 条第（3）款要求实施。

5.3.4.2 固定多场所审核策划

5.3.4.2.1 多场所组织是指组织有一个确定的中心职能机构（以下称为中心办公室，但不一定是组织的总部）来策划、控制或管理某些活动，并且有一个由地方办公室或分支（即场所）

组成的网络来实现（或部分实施）这些活动，应被纳入审核方案。一个多场所组织可以包括一个以上的法律实体，但该组织的所有场所应与该组织的中心办公室具有法律或合同联系，并有共同的管理体系。该管理体系应由中心办公室建立，并由中心办公室对其进行持续的监督和内部审核，中心办公室有权要求各场所在必要时采取纠正措。

5.3.4.2.2 多场所抽样按如下标准实施

a) 不相同/相似经营/服务/经营场所，需全数抽样。（用 Nu 表示）

b) 相同/相似经营/服务/经营场所，按以下表格所对应的抽样数予以抽样。（用 Ns 表示）

相同/相似场所抽样审核(N_s)对照表

相同/相似数量	抽样审核数量	相同/相似数量	抽样审核数量
≤20个	1个	41~50	4个
21~30个	2个	51~60个	5个
31~40个	3个	61~70个	6个
71~80个	7个	81~90个	8个
91~100个	9个	≥101个	10个

认证审核多场所总抽样数（用Nz）：=Nu+Ns

年度监督审核抽样数：不少于按初次认证审查抽样原则总抽样数的1/3.

再认证审核抽样数：不少于按初次认证审查抽样原则总抽样数的2/3.

5.3.4.2.3 多场所审核时间

5.3.4.1.4多场所抽样审核需增加时间的，按照5.3.2.1 条第（3）款要求实施。

5.3.5 审核计划

5.3.5.1 总则

MHGJ任命的每一次审核组应编制《审核计划》，以便为有关各方就审核活动的日程安排和实施达成一致提供依据。

5.3.5.2 确定审核目的、范围和准则

审核组长应根据《审核任务书》的要求，确定或引用审核目的、范围和准则，对于审核目的、范围和准则及其它任何更改，应在与客户商讨后确定。

5.3.5.3 编制审核组任务计划

审核组编制的日程安排计划应与《审核任务书》相一致，包括但不限于

a) 审核日程；

b) 审核范围，包括识别拟审核的组织和职能单元或过程；

c) 审核准则（条款）；

d）拟实施现场审核活动（适用时，包括对临时场所的访问）日期；

e）现场审核活动预期的时间和持续时间；

f）审核组成员及与审核组同行的人员的角色和职责。

5.3.5.4 审核计划的沟通

审核组长制定《审核计划》，明确分工，审核小组的成员则应准备各自的检查清单。

a）审核组长或其指定人员负责文件审核/复检，前期资料审查，只有文件基本符合标准的情况下才能进行审核。

b）审核组长应确保审核及审核计划的制订，应由具备相应专业能力的审核员进行或复检。

c）审核员应根据审核计划的分工编写或补充“检查表”。

5.4 实施审核

5.4.1 总则

审核组应按计划实施现场审核，除了访问有形场所（如工厂）外，“现场”还可以包括远程访问包含管理体系审核相关信息的电子化场所。

5.4.2 召开首次会议

审核组应与客户的管理层（适用时，还包括拟审核职能或过程的负责人员）召开正式的首次会议，并记录参加人员。首次会议通常应由审核组长主持，会议目的是简要解释将如何进行审核活动，并应包括下列要素。详略程度可与客户对审核过程的熟悉程度相一致：

a）介绍参会人员，包括简要介绍其角色；

b）确认认证范围；

c）确认审核计划（包括审核的类型、范围、目的和准则）及其任何变化，以及与客户其他相关安排，例如末次会议的日期和时间，审核期间审核组与客户管理层的会议的日期和时间；

d）确认审核组与客户之间的正式沟通渠道；

e）确认审核组可获得所需的资源和设施；

f）确认与保密有关的事宜；

g）确认适用于审核组的相关的工作安全、应急和安保程序；

h）确认可得到向导和观察员及其角色和身份；

i）报告的方法，包括审核发现的任何分级；

j）说明可能提前终止审核的条件；

k) 确认审核组长和审核组代表 MHGJ 对审核负责，并应控制审核计划（包括审核活动和审核路径）的执行；

l) 适用时，确认以往评审或审核的发现的状态；

m) 基于抽样实施审核的方法和程序；

n) 确认审核中使用的语言；

o) 确认在审核中将告知客户审核进程及任何关注点；

p) 让客户提问的机会。

5.4.3 审核中的沟通

5.4.3.1 在审核中，审核组应定期评估审核的进程，并沟通信息。审核组长应在需要时在审核组成员之间重新分配工作，并定期将审核进程及任何关注告知客户。

5.4.3.2 当可获得的审核证据显示审核目的无法实现，或显示存在紧急和重大的风险（例如安全风险）时，审核组长应向客户（如果可能还应向认证审核部）报告这一情况，以确定适当的行动。该行动可以包括重新确认或修改审核计划，改变审核目的或审核范围，或者终止审核。审核组长应向认证审核部报告所采取行动的结果。

5.4.3.3 如果在现场审核活动的进行中发现需要改变审核范围，审核组长应与客户审查该需要，并报告认证审核部。

5.4.4 观察员和向导

5.4.4.1 观察员

认证审核部与客户应在实施审核前就审核活动中观察员的到场及理由达成一致。审核组应确保观察员不影响或不干预审核过程或审核结果。观察员可以是客户组织的成员、咨询人员、实施见证的认可机构人员、监管人员或其他有合理理由的人员。

5.4.4.2 向导

审核员应由向导陪同，除非审核组长与客户另行达成一致。为审核组配备向导是为了方便审核。审核组应确保向导不影响或不干预审核过程或审核结果。

向导的职责可以包括：

a)为面谈建立联系或安排时间；

b)安排对现场或组织的特定部分的访问；

c)确保审核组成员知道并遵守关于现场安全和安保程序的规则；

d)代表客户观察审核；

e)应审核员请求提供澄清或信息。

5.4.5 收集和验证信息

5.4.5.1 在审核中应通过适当的抽样来收集与审核目的、范围和准则相关的信息（包括与职能、活动和过程之间的接口有关的信息），并对这些信息进行验证，使之成为审核证据。

5.4.5.2 信息收集方法应包括（但不限于）：

a)面谈；

b)对过程和活动进行观察；

c)审查文件和记录。

5.4.6 确定和记录审核发现

5.4.6.1 审核发现应简述符合性，详细描述不符合以及为其提供支持的审核证据，并予以记录和报告，以便为认证决定或保持认证提供充分的信息。

5.4.6.2 可以识别和记录改进机会，除非某一管理体系认证方案的要求禁止这样做。但是属于不符合的审核发现不应作为改进机会予以记录。

5.4.6.3 关于不符合的审核发现应对照审核准则的具体要求予以记录，包含对不符合的清晰陈述，并详细标识不符合所基于的客观证据。应与客户讨论不符合，以确保证据准确且不符合得到理解。但是，审核员应避免提示不符合的原因或解决方法。

a)下列情况之一者判为严重不符合项：

- ✧ 受审核方的数据存储安全管理体系认证某一个要素/要求缺少或出现严重问题，导致不能满足法律法规要求；
- ✧ 受审核方 数据存储安全管理体系认证 的某一活动/过程要求出现多项（根据规模大小、复杂程度掌握 3—5 项）轻微不符合项，导致出现系统性和/或区域性的不符合；
- ✧ 严重相关方投诉，无法及时采取适宜措施进行整改，从而影响其数据存储安全管理体系认证 满足要求的信心；
- ✧ 严重违反相关法律法规或其他要求；
- ✧ 严重的欺骗行为。

b)下列情况之一者判为轻微不符合项：

- ✧ 对照审核准则，出现的不符合对 数据存储安全管理体系认证 没有产生严重的影响；
- ✧ 对于受审核区域、过程的管理现状而言，是偶尔发生的、个别的问题。

c) 改进机会

- ✧ 对于不能界定为不符合，但是可能对受审核方的 数据存储安全管理体系认证 有帮助之处，由审核组以改进机会的形式向受审核方提出。

c)在证后监督、再认证时不符合项还包括：

✧错误使用认证标记和证书，若属明知故犯恶意违规、造成严重后果的，应判定为严重不符合项；其情节及后果并不严重的，应被判定为轻微不符合项。应该注意的是，凡属此类不符合项应当即要求受审核方进行整改。

✧前次审核发现的不符合项的现场整改情况不佳的，将视其情节及后果的严重程度形成轻微/严重不符合项。

✧没有足够的措施、证据证明其 数据存储安全管理体系认证 具备持续改进能力、取得持续改进绩效的，也将判定为不符合项。

5.4.6.4 审核组长应尝试解决审核组与客户之间关于审核证据或审核发现的任何分歧意见，未解决的分歧点应予以记录。

5.4.7 准备审核结论

在末次会议前，审核组应：

a)对照审核目的审查审核发现和审核中收集的任何其他适用的信息；

b)考虑审核过程中内在的不确定性，就审核结论达成一致；

c)确定任何必要的跟踪活动；

d)确认审核方案的适宜性，或识别任何所需要的修改（例如范围、审核时间或日期、监督频次、能力）。

5.4.8 召开末次会议

5.4.8.1 审核组应与客户的管理层（适用时，还包括所审核的职能或过程的负责人员）召开正式的末次会议，并记录参加人员。末次会议通常应由审核组长主持，会议目的是提出审核结论，包括关于认证的推荐性意见。不符合应以使其被理解的方式提出，并应就回应的时间表达成一致。“被理解”不一定意味着客户已经接受了不符合。

5.4.8.2 末次会议还应包括下列要素。详略程度应与客户对审核过程的熟悉程度一致：由组长主持，受审核方各部门主要负责人参加。议程如下：

a）感谢致辞/签到；

b）重申审核目的、范围、依据及审核原则、方法，审核发现的分类及对审核结论的影响；

c）重申“公正性声明及保密声明”及审核的局限性（如抽样，但应强调审核组通过控制抽样的典型性和代表性已使此种风险降至最低限度，从而确保审核结论能尽可能反映受审核方数据存储安全管理体系认证 的客观情况）；

d) 向客户说明所收集的审核证据基于对信息的抽样，因而会有一定的不确定性；

e）审核员宣读“不符合通知单”，必要时宣读观察项；不符合项应取得企业管理者代表或其它负责人的确认。

f）征询受审核方对不符合事实是否仍存在异议；

g）审核综述（从以下方面总结受审核方 数据存储安全管理体系认证 的符合性及有效性）：

✧ 文件评审结果；

✧ 现场审核观察综述；

✧ 数据存储安全管理体系认证 运行过程的符合性、有效性；（数据存储安全管理体系认证 的活动、产品、服务过程中遵守有关法律、法规的情况；无相关方投诉；资源配置；职责权限；员工特别是管理者的环境意识；培训管理评审、内审、纠正、预防措施等要素的实施有效性；数据存储安全管理体系方针、目标、指标的实现及监测情况；数据存储安全管理体系认证控制情况；严重不符合项情况；不符合项的数量及分布……）

h）审核结论

✧ 现场审核通过：审核小组建议 MHGJ 对申请组织的 数据存储安全管理体系认证 给予注册；

✧ 待改进：审核小组建议推迟时，申请单位应对审核小组提出的不符合项采取纠正措施并经审核小组成员现场跟踪，确认不符合项已关闭，审核小组才推荐 MHGJ 对申请单位的 数据存储安全管理体系认证 给予注册。

✧ 现场审核不通过：审核小组建议 MHGJ 不对申请单位的 数据存储安全管理体系认证 给予注册，建议申请单位在条件成熟后重新申请认证。

审核小组应给申请组织提供针对审核结果和说明提出质疑的机会，包括：

i）客户为审核中发现的任何不符合的纠正和纠正措施提出计划的时间表；

j）MHGJ 在审核后的活动；

k）说明投诉处理过程和申诉过程；

l）纠正/纠正措施要求

强调不能仅采取就事论事的“补救”措施，应按如下步骤制定并实施纠正/纠正措施：

·纠正（如不符合项为孤立事件，则无需下述措施）；

·检查类似的问题是否存在；

·分析产生原因，制订并实施纠正措施。

纠正/纠正措施方案经受审核方管理者代表审批后实施，验证合格后，交审核组长确认；

纠正/纠正措施期限根据不符合项性质及严重程度决定，一般不超过 3 个月。

5.4.8.3 客户应有机会提出问题。审核组与客户之间关于审核发现或结论的任何分歧意见应得到讨论并尽可能获得解决。任何未解决的分歧意见应予以记录并提交 MHGJ。

5.4.9 审核报告

5.4.9.1 审核组应为每次审核提供书面报告。审核组可以识别改进机会，但不应提出具体解决办法的建议。MHGJ 应享有对审核报告的所有权。

5.4.9.2 在现场审核的末次会议上，审核组应口头说明申请组织是否符数据存储安全管理体系定的认证要求，以及审核小组的结论。审核组长一周内应向审核部提交书面的审核报告，并应对审核报告的内容负责。审核报告应提供对审核的准确、简明和清晰的记录，以便为认证决定提供充分的信息，并应包括或引用下列内容：

a)本机构名称；

b)客户的名称和地址及其管理者代表；

c) 审核的类型（例如初次、监督或再认证审核）；

d) 审核准则；

e) 审核目的；

f) 审核范围，特别是标识出所审核的组织或职能单元或过程，以及审核时间；

g) 审核组长、审核组成员及任何与审核组同行的人员；

h) （现场或非现场）审核活动的实施日期和地点；

i) 与审核类型的要求一致的审核证据、审核发现和审核结论；

j) 已识别出的任何未解决的问题；

j）审核组向本机构所作的推荐结论。

5.4.10 不符合的原因分析

对于审核中发现的不符合，审核组应要求客户在规定期限内分析原因，并说明为消除不符合已采取或拟采取的具体纠正和纠正措施。

5.4.11 纠正和纠正措施的有效性

审核组应审查客户提交的纠正和纠正措施及相应的整改证据，以确定其是否可被接受。审核组应验证所采取的任何纠正和纠正措施的有效性。所取得的为不符合的解决提供支持的证据应予以记录。对不符合的解决进行审查和验证的证据应予以记录。应将审查和验证的结果告知客户。可通过审查客户提供的文件，或在必要时实施现场验证来验证纠正和纠正措施的有效性。

5.5 现场审核

5.5.1 现场审核主要内容

现场审核的主要目的是评价受审核方管理体系的实施情况(包括有效性)。第二阶段审核应在受审核方的现场进行，除了访问物理场所(如工厂)外，“现场”还可以包括远程访问包含管理体系审核相关信息的电子站点，并至少覆盖以下方面：

a) 与适用的管理体系标准或其他规范性文件的所有要求的符合情况及证据；

b) 根据关键绩效目标和指标(与适用的管理体系标准或其他规范性文件的期望一致），对绩效进行监视、测量、报告和评审的情况；

c) 受审核方的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；

f) 针对受审核方方针的管理职责；

g) 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。

5.5.2 初次认证的审核结论

审核组应对现场审核中收集的所有信息和证据进行分析，以评审审核发现并就审核结论达成一致。为使 MHGJ 做出认证决定，审核组至少应向 MHGJ 提供以下信息：

a) 审核报告；

b) 对不符合的意见，适用时，还包括对受审核方采取的纠正和纠正措施的意见；

c) 对提供给 MHGJ 用于申请评审的信息的确认；

d) 对是否授予认证的推荐性意见及附带的任何条件或评论。

MHGJ 在评价审核发现和结论及任何其他相关信息(如公共信息、受审核方对审核报告的意见)的基础上，进入本程序“5.8 认证决定”阶段。

5.6 结合审核

当数据存储安全管理体系认证 及其与其他体系适宜的接口可以清晰地界定，数据存储安全管理体系认证文件亦能详细描述该体系，并清晰界定与组织内运行的其他相关体系的关系，或其他管理体系对拟认证的数据存储安全管理体系认证 的影响，就可以将 数据存储安全管理体系认证 文件与其他体系文件（如质量、环境、职业健康安全）合在一起审核，具体要求详见“11 与其它管理体系结合审核”部分。

5.7 补充审核

如果需要进行全面或部分的补充审核，或需要形成文件的证据（在将来的监督审核中予以确认），以验证纠正和纠正措施的有效性，则审核组应告知受审核的组织。补充审核时间应视补充审核的项目内容、涉及的人数、组织的产品/服务类别、过程的复杂程度等因素决定。

5.8 认证决定

5.8.1 MHGJ 由专业技术人员对审核报告及认证过程中收集到的信息进行评审，评审合格或问题改善后，做出同意或不同意注册或保持注册的决定，必要时组织有专业技术能力的人员共同讨论决定。做出认证决定的人员不应是参加此次审核的人员。

5.8.2 做出决定前应确认：

a) 审核组提供的信息足以确定认证要求的满足情况和认证范围；

b) 对于所有反映以下问题的不符合，MHGJ 已评审、接受并证实了纠正和纠正措施的有效性：未能满足管理体系标准的一项或多项要求，或使人对受审核方管理体系实现预期结果的能力产生重大怀疑的情况；

c) 对于任何其他不符合，MHGJ 已评审并接受了受审核方计划采取的纠正和纠正措施。

5.8.3 MHGJ 不应把批准、保持、扩大、暂停和撤销认证的权力委任给外部人员和机构。

5.8.4 获准认证注册的企业将得到认证结果通知单及 MHGJ 总经理签发的认证证书等文件。如授权人员签署的信件或认证证书。这些文件应表明认证所覆盖的场所及其每个场所的：

a) 每个获证组织的名称和地理位置(或多场所认证范围内总部和所有场所的地理位置)；

b) 授予、扩大或更新认证的日期；

c) 认证有效期或与认证周期一致的应进行再认证的日期；

d) 唯一的识别代码，即证书编号；

e) 对获证组织的审核所用的标准和(或）其他规范性文件，包括版次和(或）修订号；

f) 认证范围(述及每个场所的相关产品(包括服务)、过程等)；

g) MHGJ 的名称、地址和认证标志，总经理签名；

h) 认证用标准和(或)其他规范性文件所要求的任何其他信息；

i) 在颁发经过修改的认证文件时，区分新文件与任何已作废文件的方法。

5.8.5 认证证书的有效期为三年。

6证后监督与管理

6.1 监督审核通常审核时间间隔，第 1 次监督审核应在初次认证决定后的第 12 个月内进行，两次监督审核之间时间间隔不能超过 15 个月，一般第三次监督转为再认证。每次监督审核的内容只是 数据存储安全管理体系认证的一部分。

6.2 每三年必须进行一次完整的复评，持证者应在有效期期满前三个月向 MHGJ 提出复评的申请，MHGJ 根据复评的结果决定是否重新发放注册证书。

6.3 如果有其它组织对持证者的数据存储安全管理体系认证有重大投诉时，MHGJ 有权给持证企业通知后在短期内进行非例行监督。

6.4 数据存储安全管理体系认证监督审核的时间不少于初次认证评价人日数的 1/3，但最低不少于 1 个人.日，再认证审核的时间不少于初次认证审核时间的 2/3，但最低不少于 1 人.日。

6.5 监督和再认证审核档案应妥善保管，形成完整的审核卷宗。

7获证组织文件的修改

7.1 对本证组织管理手册的重大修改，必须加以记录，并交给 MHGJ 审核并备案。

7.2 MHGJ 在收到重大修改的通知后应及时地将其手册进行更新。

7.3 审核组长收到文件更改的通知时将对有关的重大更改加以审查。对确已影响到数据存储安全管理体系认证的修改，应进行一次全面的“文件审查”或附加的现场审查，有时二者兼有。（持证企业须承担所有这些额外的文件审查和现场审核的费用）。

7.4 如 MHGJ 对于某组织的 数据存储安全管理体系认证 在一段时期内持续表明有效的组织，MHGJ 经与该组织协商一致的，可按照监督和复评程序对其设计一个个性化的监督和复评方案，实施监督或复评，但必须事前向报告。

8 暂停、撤销或恢复认证证书

8.1暂停

获证组织有下列情形之一的，本机构将当暂停其使用数据存储安全管理体系认证证书，暂停期限最长为六个月：

（1）数据存储安全管理体系认证持续或严重不满足认证要求的；

（2）不承担、履行认证合同约定的责任和义务；

（3）被有关执法监管部门责令停业整顿；

（4）发生相关方数据存储安全管理体系投诉，但尚不需立即撤销认证证书；

（5）未能按规定间隔期接受监督认证评价；

（6）主动申请暂停认证证书。

8.2 撤销

获证组织有下列情形之一的，本机构将当撤销其 数据存储安全管理体系认证证书：

（1）被注销或撤销法律地位证明文件或有关的行政许可证明和资质证书；

（2）出现重大数据存储安全管理体系事故，经执法监管部门确认是获证组织违规造成的；

（3）针对数据存储安全管理体系事故或相关方重大投诉，未能采取有效处理措施；

（4）暂停认证证书的期限已满但导致暂停的问题未得到解决或纠正；

（5）虚报、瞒报获证所需信息；

（6）不接受相关监管部门或本机构对其监督。

（7）主动申请撤销认证证书。

8.3 恢复

暂停状态的认证证书，除下列情况外，须经全要素现场审核消除暂停原因后，经认证决定通过可恢复认证资格。因以下几种原因被暂停注册资格的认证证书，在暂停原因消除后经认证决定人员审查通过，可直接恢复注册资格：

a) 因企业未按期提交不符合报告整改资料而被暂停的，在取得企业整改资料后须经现场验证可申请恢复注册资格。

b) 因企业资质证书（如 3C 证、工业许可证、计量证、特种设备制造许可证等）被暂停或等待办结发证而被 MHGJ 暂停认证注册资格的，企业在取得有效资质证书后可申请恢复注册资格。

c) 公司根据监管部门稽查所发现问题意见暂停企业注册资格的，经监管部门确定问题点不存在或已消除后，可根据企业提供相关证据提请认证决定恢复注册资格。

d) 因欠费暂停注册资格的，在费用交齐后由财务资源部提请认证决定恢复注册资格。

8.4 处置信息

机构将以书面方式通知获证组织有关暂停、撤销或恢复数据存储安全管理体系认证证书的信息和要求，同时按规定程序和要求报国家认监委。对于撤销认证证书的，本机构将收回撤销的数据存储安全管理体系认证证书。

8.5 处置原则

被暂停或撤销 数据存储安全管理体系认证证书的获证组织，不得以任何方式使用认证证书、认证标识或引用认证信息。

8.6 先认证后申报资质的处理

按相关规定要求企业首先取得数据存储安全管理体系认证证书方可申报资质的，在初审时可颁发三年有效证书，并在监督时跟踪资质申报进度。如三年证书期满仍未能取得相应资质的，不应再接受再认证申请。

9认证证书

9.1 证书信息

数据存储安全管理体系认证证书包括（但不限于）以下基本信息：

（1）获证组织名称、地址和统一社会信用代码（或组织机构代码）；

（2）认证覆盖的地址和业务范围；

（3）认证依据；

（4）证书编号；

（5）证书颁证日期、证书有效期；

（6)本机构名称、地址；

（7）证书查询方式。

9.2 证书有效期

数据存储安全管理体系认证证书有效期为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。

9.3 认证信息通报

本机构按照认监委相关信息通报制度上报 数据存储安全管理体系认证证书信息。

9.4 认证标志

MHGJ认证标志

按照国家相关法律法规和MHGJ认证标志管理制度，获证组织可以采用认证机构允许的加施方式，获证组织应当在广告等有关宣传中正确使用认证标志，不得混淆使用产品认证、管理体系认证、服务认证标志。因故被暂停认证注册资格时，应暂停使用认证证书和认证标志；因故被撤销认证注册资格时，应停止使用认证证书和认证标志，向本机构交回全部认证证书并销毁全部认证标志。

10认证范围的变更

10.1获证组织数据存储安全管理体系认证范围变更时，应告知本机构，并按本机构的要求提交相关材料。

10.2本机构根据获证组织的变更情况，策划并实施适宜的认证评价活动，并按照 5.8要求做

出关于是否扩大、缩小或变更认证范围的决定。相关认证评价活动可单独进行，也可结合获证组织的监督或再认证认证评价进行。

11与其他认证的结合审核

11.1 与QMS、EMS、OHSMS或其它体系认证结合审核

当数据存储安全管理体系认证 及其与其他体系适宜的接口可以清晰地界定，数据存储安全管理体系认证文件亦能详细描述该体系，并清晰界定与组织内运行的其他相关体系的关系，或其他管理体系对拟认证的数据存储安全管理体系认证 的影响，就可以将 数据存储安全管理体系认证 文件与其他体系文件（如质量、环境、职业健康安全）合在一起审核。

MHGJ 应给审核员安排足够时间的完成与审核相关的所有活动，可视情况取 0.8~1.0 的结合系数,MHGJ 应有能力证实和判断任何初评，监督和复评所需的人日合适的。

结合审核应满足 数据存储安全管理体系认证 体系的所有要求，且不能受到结合审核的负面影响。

结合审核或依次进行时，对于共有要素，在确定审核员能力时，主要原则是保持每个体系审核的完整性，所以应配备适当的能力。

12增发 数据存储安全管理体系认证证书

12.1增发申请

已同时获得本机构数据存储安全管理体系认证某一范围数据存储安全管理体系认证项目的，现需增加某一新范围或其它环境标准且符合数据存储安全管理体系认证申请条件的获证组织，可向本机构申请增发数据存储安全管理体系认证证书。

12.2 增发认证审核人日

本机构将结合数据存储安全管理体系认证监督或再认证审核的时机，确定增发认证审核不少于 1人日。

12.3 增发实施

申请组织通过数据存储安全管理体系认证追加认证评价，并按照 5.4.3要求完成整改的，本机构将在认证决定通过后，向其增发 数据存储安全管理体系认证证书。

13 转换 数据存储安全管理体系认证证书

13.1 转换申请

已通过本机构实施的数据存储安全管理体系认证第二方评价的组织，可向本机构申请转换数据存储安全管理体系认证证书。

13.2 转换审核时间

本机构将结合 数据存储安全管理体系认证监督评价的时机，向申请组织实施数据存储安全管理体系认证转换认证评价。转换审核时间可在原数据存储安全管理体系认证审核的基础上适当减少人日，但减少后总的审核人日不少于1人日。

13.3 转换实施

申请组织通过数据存储安全管理体系认证转换认证评价，并按照 5.4.11要求完成整改的，本机构将在认证决定通过后，向其颁发数据存储安全管理体系认证证书。

14申诉和投诉

14.1 申诉

申请组织或获证组织对认证决定有异议时，可在 10个工作日内向本机构提出申诉。本机构自收到申诉之日起，在一个月内进行处理，并将处理结果书面通知申诉人。

14.2 投诉

若申诉人认为认证机构未遵守认证相关法律法规或本规则并导致自身合法权益受到严重侵害的，可以直接向认证监管部门投诉。

15 收费

认证收费参考本机构的质量管理体系认证收费标准收取或按合同约定。