# 中鸿认证（江苏）有限公司其他管理体系审核标准

# 数据存储安全管理体系认证技术规范

2025-07-18发布 2025-07-18实施

中鸿认证（江苏）有限公司发布

# 前言

本文件按照GB/T1.1-2020《标准化工作导则第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中鸿认证（江苏）有限公司技术部提出并归口。

本文件起草单位：中鸿认证（江苏）有限公司

本文件主要起草人：孙敬、韩自鹤、丁泽林

# 引言

本标准旨在为组织提供一个全面的数据存储安全管理体系框架，帮助组织识别和管理数据存储过程中的安全风险，确保数据存储的安全性和合规性。本标准融合了国际先进的信息安全管理体系标准（如ISO/IEC27001、ISO/IEC27040）以及质量管理培训指南（GB/T19025-2023ISO10015:2019）的相关要求，确保组织在数据存储安全管理方面具备明确的指导和可操作的实践方法。

通过实施本标准，组织能够：

a）建立明确的数据存储安全方针和目标，确保数据存储安全管理与组织的整体战略相一致；

b）识别和评估数据存储安全风险，采取有效的控制措施，降低风险至可接受水平；

c）提高员工的数据存储安全意识和能力，通过系统的培训和持续地教育，确保员工能够履行其在数据存储安全管理体系中的职责；

d）建立有效的监测和审核机制，持续监控数据存储安全管理体系的绩效，及时发现并纠正不符合项；

e）实现数据存储安全管理体系的持续改进，通过定期的管理评审和改进措施，不断提升数据存储安全管理的水平。

本标准适用于所有涉及数据存储的组织，无论其规模大小、行业类型或业务性质。组织可以根据自身的具体情况，灵活应用本标准的要求，建立适合自身的数据存储安全管理体系。

# 数据存储安全管理体系要求

## 1.范围

本标准规定了数据存储安全管理体系的要求，旨在帮助组织建立、实施、维护和持续改进数据存储安全管理体系，以确保数据存储的安全性、可用性和完整性。本标准适用于所有涉及数据存储的组织，无论其规模大小、行业类型或业务性质。

## 2.规范性引用文件

以下文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

•ISO/IEC27000：信息技术-安全技术-信息安全管理体系-概述和词汇

•ISO/IEC27001：信息技术-安全技术-信息安全管理体系-要求

•ISO/IEC27002：信息技术-安全技术-信息安全控制实践指南

•ISO/IEC27040:2024数据存储安全

•GB/T19025-2023/ISO10015:2019质量管理培训指南

## 3.术语和定义

基于本标准的目的，ISO/IEC27000以及下列术语和定义适用于本文件。

### 3.1数据存储安全管理体系Data Storage Security Management System

组织为确保数据存储的安全性、可用性和完整性而建立的管理体系，包括组织结构、策略、计划、程序、过程和资源。

**3.2数据存储安全风险Data Storage Security Risk**

数据存储过程中可能面临的威胁、漏洞和影响的组合，可能导致数据泄露、损坏、丢失或不可用。

**3.3数据存储安全控制Data Storage Security Control**

为降低数据存储安全风险而采取的管理、技术和物理措施。

**3.4培训training**

为使员工获得或提高与数据存储安全相关的知识、技能和意识，以满足数据存储安全管理体系要求而进行的有计划的活动。

**4.组织环境**

**4.1理解组织及其环境**

组织应确定与其目标和战略方向相关并影响其实现数据存储安全管理体系预期结果的各种外部和内部因素。这些因素应包括但不限于：

a）法律法规要求；

b）技术环境；

c）数据存储的性质和规模；

d）组织的文化和价值观。

**4.2理解相关方的需求和期望**

组织应确定与数据存储安全管理体系有关的相关方，以及这些相关方的要求。相关方可能包括但不限于：

a）客户；

b）员工；

c）监管机构；

d）第三方服务提供商。

### 4.3确定数据存储安全管理体系的范围

组织应确定数据存储安全管理体系的范围，确保其涵盖所有与数据存储相关的活动、产品和服务。范围应明确界定，并形成文件。

### 4.4数据存储安全管理体系

组织应建立、实施、维护和持续改进数据存储安全管理体系，以确保数据存储的安全性、可用性和完整性。数据存储安全管理体系应包括但不限于以下方面：

a）数据存储安全方针和目标；

b）数据存储安全策略和程序；

c）数据存储安全风险评估和管理；

d）数据存储安全控制措施的实施；

e）数据存储安全的监测、审核和改进。

## 5.领导作用

### 5.1领导作用和承诺

最高管理者应通过以下活动，对其建立、实施、维护和持续改进数据存储安全管理体系的承诺提供证据：

a）向组织传达满足数据存储安全要求的重要性；

b）制定数据存储安全方针；

c）确保数据存储安全目标的制定；

d）进行管理评审；

e）确保资源的获得。

**5.2数据存储安全方针**

最高管理者应制定数据存储安全方针，方针应：

a）与组织的宗旨相适应；

b）包括对满足适用的数据存储安全要求的承诺；

c）包括对持续改进数据存储安全管理体系的承诺；

d）提供制定和评审数据存储安全目标的框架；

e）在组织内得到沟通和理解；

f）可为相关方所获取；

**5.3组织的岗位、职责和权限**

最高管理者应确保组织内相关角色的职责和权限得到分配、沟通和理解。这些角色应包括但不限于：

a）数据存储安全负责人；

b）数据存储安全团队成员；

c）数据存储管理员；

d）数据所有者。

**6.策划**

**6.1应对风险和机遇的措施**

组织应策划应对风险和机会的措施，以：

a）确保数据存储安全管理体系能够实现其预期结果；

b）预防或减少不利影响；

c）实现持续改进。

### 6.2数据存储安全目标及其实现的策划

组织应制定数据存储安全目标，并策划实现这些目标的措施。目标应：

a）与数据存储安全方针一致；

b）可测量；

c）考虑适用的要求；

d）与组织的业务目标相适应。

## 7支持

### 7.1资源

组织应确定并提供实施、维护和持续改进数据存储安全管理体系所需的资源，包括但不限于：

a）人力资源；

b）技术资源；

c）财务资源；

d）物理资源。

### 7.2能力

组织应确保其员工具备必要的能力，以履行其在数据存储安全管理体系中的职责。能力可以通过培训、教育或经验获得。

### 7.3意识

组织应确保其员工意识到：

a）数据存储安全的重要性；

b）个人在数据存储安全管理体系中的角色和职责；

c）偏离数据存储安全方针和程序的潜在后果。

### 7.4沟通

组织应建立和维护数据存储安全的内部和外部沟通机制，以确保数据存储安全信息的有效传递和共享。沟通应包括但不限于：

a）数据存储安全方针和目标的沟通；

b）数据存储安全策略和程序的沟通；

c）数据存储安全风险评估和管理的沟通；

d）数据存储安全事件的沟通。

### 7.5文件化信息

组织应建立和维护数据存储安全管理体系所需的文件化信息，以确保其有效性和可追溯性。文件化信息应包括但不限于：

a）数据存储安全方针和目标；

b）数据存储安全策略和程序；

c）数据存储安全风险评估和管理计划；

d）数据存储安全控制措施的实施记录；

e）数据存储安全监测和审核报告。

### 7.6培训

组织应根据GB/T19025-2023ISO10015:2019的要求，制定和实施数据存储安全培训计划，以提高员工对数据存储安全的认识和理解。培训计划应包括但不限于：

a）确定培训需求：组织应识别员工在数据存储安全方面的知识和技能差距，确定培训需求。

b）设计培训内容：培训内容应涵盖数据存储安全方针和目标、策略和程序、风险评估和管理、控制措施、事件响应和处理等方面。

c）实施培训：组织应采用适宜的培训方法，如课堂培训、在线培训、实践操作等，确保培训的有效性。

d）评估培训效果：组织应通过考试、实际操作测试、反馈等方式，评估培训效果，确保员工具备必要的知识和技能。

e）记录培训信息：组织应记录培训计划、培训内容、培训实施情况和培训效果评估结果，以备审核和改进。

## 8运行

### 8.1运行的策划和控制

组织应策划、实施和控制满足数据存储安全要求所需的过程，包括但不限于：

a）数据存储访问控制；

b）数据存储加密；

c）数据存储备份和恢复；

d）数据存储监控和审计；

e）数据存储漏洞管理。

### 8.2数据存储安全风险评估和管理

组织应建立、实施和维护数据存储安全风险评估过程，以识别和评估数据存储安全风险。风险评估应包括：

a）确定数据存储资产；

b）识别数据存储面临的威胁；

c）识别数据存储的漏洞；

d）评估数据存储安全风险的可能性和影响；

e）确定数据存储安全风险的优先级。

组织应根据风险评估的结果，制定和实施数据存储安全风险管理计划，以降低数据存储安全风险至可接受水平。风险管理计划应包括：

a）风险处理措施；

b）风险接受准则；

c）风险沟通和咨询；

d）风险监控和评审。

**8.3数据存储安全控制措施**

组织应根据数据存储安全风险评估的结果，选择和实施适当的数据存储安全控制措施，以确保数据存储的安全性、可用性和完整性。数据存储安全控制措施应包括但不限于：

a）数据存储访问控制；

b）数据存储加密；

c）数据存储监控和审计；

d）数据存储漏洞管理；

e）数据存储安全培训和意识提升。

**8.4数据存储安全事件的响应和处理**

组织应建立和实施数据存储安全事件的响应和处理机制，以确保数据存储安全事件得到及时、有效地处理。响应和处理应包括：

a）数据存储安全事件的检测和报告；

b）数据存储安全事件的影响评估；

c）数据存储安全事件的应急响应；

d）数据存储安全事件的恢复和修复；

e）数据存储安全事件的后续改进。

## 9绩效评价

### 9.1监视、测量、分析和评价

组织应建立和实施数据存储安全监测机制，以确保数据存储安全管理体系的有效运行。监测应包括：

a）数据存储安全事件的检测和记录；

b）数据存储安全控制措施的有效性评估；

c）数据存储安全风险的变化监测。

组织应定期对数据存储安全管理体系的绩效进行测量、分析和评价，以验证其符合性和有效性。测量、分析和评价应包括：

a）数据存储安全方针和目标的达成情况；

b）数据存储安全策略和程序的实施情况；

c）数据存储安全控制措施的有效性；

d）数据存储安全风险评估和管理的效果。

### 9.2内部审核

组织应定期进行数据存储安全内部审核，以验证数据存储安全管理体系是否符合本标准的要求，并得到有效实施和维护。内部审核应：

a）依据策划的安排进行；

b）由与被审核活动无直接责任的人员进行；

c）形成审核报告，记录审核发现和结论；

d）对审核中发现的不符合项采取纠正措施，并验证其有效性。

### 9.3管理评审

最高管理者应按照策划的时间间隔对数据存储安全管理体系进行评审，以确保其持续的适宜性、充分性和有效性。管理评审应包括：

a）评审数据存储安全管理体系的绩效和有效性；

b）评审数据存储安全方针和目标的达成情况；

c）评审数据存储安全风险评估和管理的效果；

d）评审数据存储安全控制措施的有效性；

e）评审数据存储安全培训和意识提升的效果；

f）评审数据存储安全事件的响应和处理情况；

g）评审数据存储安全管理体系的改进机会。

## 10改进

### 10.1不符合和纠正措施

组织应采取措施，以消除数据存储安全管理体系中的不符合原因，防止不符合的再次发生。

纠正措施应：

a）与不符合的影响相适应；

b）包括对不符合的评审和分析；

c）包括制定和实施纠正措施计划；

d）包括对纠正措施的有效性进行验证

### 10.2持续改进

组织应持续改进数据存储安全管理体系的适宜性、充分性和有效性。持续改进应包括：

a）对数据存储安全管理体系的绩效进行监测和测量；

b）对数据存储安全管理体系的评审结果进行分析；

c）对数据存储安全管理体系的改进机会进行识别；

d）对数据存储安全管理体系的改进措施进行策划和实施。

## 附录A （资料性）

A.1数据存储安全管理体系文件化信息示例：

组织应建立和维护数据存储安全管理体系所需的文件化信息，以确保其有效性和可追溯性。

文件化信息应包括但不限于：

a）数据存储安全方针和目标；

b）数据存储安全策略和程序；

c）数据存储安全风险评估和管理计划；

d）数据存储安全控制措施的实施记录；

e）数据存储安全监测和审核报告；

f）数据存储安全培训计划和记录；

g）数据存储安全事件的响应和处理记录。

A.2数据存储安全培训计划示例

组织应根据GB/T19025-2023ISO10015:2019的要求，制定和实施数据存储安全培训计划，以提高员工对数据存储安全的认识和理解。培训计划应包括但不限于：

a）确定培训需求：组织应识别员工在数据存储安全方面的知识和技能差距，确定培训需求。

b）设计培训内容：培训内容应涵盖数据存储安全方针和目标、策略和程序、风险评估和管理、控制措施、事件响应和处理等方面。

c）实施培训：组织应采用适宜的培训方法，如课堂培训、在线培训、实践操作等，确保培训的有效性。

d）评估培训效果：组织应通过考试、实际操作测试、反馈等方式，评估培训效果，确保员工具备必要的知识和技能。

e）记录培训信息：组织应记录培训计划、培训内容、培训实施情况和培训效果评估结果，以备审核和改进。

## 附录B（资料性）

B.1数据存储安全管理体系审核指南

组织应定期进行数据存储安全内部审核，以验证数据存储安全管理体系是否符合本标准的要求，并得到有效实施和维护。审核指南应包括但不限于：

a）审核计划的制定；

b）审核团队的组建；

c）审核实施的步骤；

d）审核报告的编写；

e）不符合项的纠正措施跟踪。