ICS 35.240
CCS L 80

中华人民共和国国家标准

GB/T 43710—2025

科学数据安全审计要求

Requirements for auditing of scientific data security

2025-01-24 发布　　2025-01-24 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前言 …… Ⅲ
引言 …… Ⅳ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　审计总则 …… 2
4.1　概述 …… 2
4.2　审计依据 …… 2
4.3　审计目标 …… 2
5　一般审计要求 …… 3
5.1　概述 …… 3
5.2　安全策略 …… 3
5.3　组织建设 …… 3
5.4　人力资源管理 …… 3
5.5　业务连续性管理 …… 3
5.6　管理监督 …… 4
5.7　安全管理 …… 4
5.7.1　安全管理办法 …… 4
5.7.2　分类分级管理 …… 4
5.7.3　风险管理 …… 4
5.7.4　内部审查 …… 4
5.8　科学数据生存周期业务流程 …… 4
5.8.1　科学数据生存周期 …… 4
5.8.2　通用要求 …… 5
5.8.3　采集加工 …… 5
5.8.4　存储备份 …… 5
5.8.5　传输交换 …… 6
5.8.6　开放共享 …… 6
5.8.7　使用服务 …… 6
5.8.8　安全处置 …… 7
6　专项审计要求 …… 7
6.1　概述 …… 7
6.2　个人信息安全 …… 7

6.2.1 通用管理 …… 7
6.2.2 个人信息识别与分类分级 …… 8
6.2.3 自动化决策处理个人信息 …… 8
6.2.4 个人信息安全影响评估 …… 8
6.2.5 出境安全风险评估 …… 8
6.2.6 应急管理 …… 8
6.2.7 内部审查 …… 8
6.3 汇交安全 …… 9
6.3.1 通用管理 …… 9
6.3.2 分类分级管理 …… 9
6.3.3 存储和传输安全管理 …… 9
6.3.4 汇交数据登记管理 …… 9
6.3.5 内部审查 …… 9
6.4 数据出境安全 …… 9
6.4.1 通用管理 …… 9
6.4.2 个人信息出境安全 …… 10
6.4.3 分类分级管理 …… 10
6.4.4 安全风险评估 …… 10
6.4.5 内部审查 …… 10
附录 A（资料性） 审计流程 …… 11
A.1 概述 …… 11
A.2 审计流程 …… 11
附录 B（资料性） 审计报告 …… 12
B.1 概述 …… 12
B.2 审计报告的类型 …… 12
B.3 审计报告的结构和内容 …… 12
B.4 审计报告样例 …… 13
参考文献 …… 16

前　言

本文件按照GB/T 1.1—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。

本文件由科学技术部提出。

本文件由全国科技平台标准化技术委员会归口（SAC/TC 486）。

本文件起草单位：中国科学院计算机网络信息中心、中国标准化研究院、中国网络安全审查技术与认证中心、中国信息通信研究院、中国软件评测中心（工业和信息化部软件与集成电路促进中心）、北京邮电大学、中国科学院高能物理研究所、中国科学院信息工程研究所、北京神州绿盟科技有限公司、广州物联网研究院、北京迪瞰科技有限公司、福建中信网安信息科技有限公司、福建大数据一级开发有限公司。

本文件主要起草人：廖方宇、魏金侠、赵静、李婧、龙春、杜冠瑶、万巍、杨帆、王跃达、付豫豪、胡良霖、朱艳华、于建军、李翀、李菁菁、王志强、杨青海、徐凯程、甘杰夫、景慧昀、周润松、郭盈、刘建毅、齐法制、侯丰尧、马多贺、王妍、徐震、王利明、叶晓虎、吴铁军、王伟、李东、何颖、李喆。

引　言

科学数据是战略性、基础性科技资源，具有传播速度最快、影响面最宽、开发利用潜力大的特点，深刻影响着各国的经济发展、国家安全、科技进步和综合竞争力。《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》和《中华人民共和国网络安全法》共同构成了我国网络数据领域治理的基础性法律，标志着与我国网络大国、数字大国相匹配的制度建设逐步走向成熟。《科学数据管理办法》明确提出“应加强科学数据全生命周期安全管理，制定科学数据安全保护措施；加强数据下载的认证、授权等防护管理，防止数据被恶意使用。”本文件面向自然科学领域科学数据安全与合规需求，可促进科学数据相关机构数据安全能力提升，规范科学数据安全审计工作，满足国家对合规性方面的要求。

本文件是一项基础的科学数据安全标准，适用于科学数据机构，对科学数据相关活动中所涉及的安全控制活动进行审计。规定了科学数据安全审计的相关要求，包括总体要求、一般审计要求和专项审计要求。总体要求主要对审计依据、审计目标进行描述。一般审计要求是为了综合评价科学数据相关机构安全目标实现情况而进行的审计，从安全策略、组织建设、人力资源管理、管理监督、安全管理、科学数据生存周期业务流程等几个方面，对科学数据安全控制工作进行通用审计。专项审计要求是根据外部要求及内部特殊要求而进行的审计，可满足科学数据相关机构对个人信息安全、汇交安全、数据出境安全全部或部分的审计需要。鉴于国家对数据安全合规监管体系的不断完善，将对专项审计内容进行更新，满足国家的监管要求。

科学数据安全审计要求的提出旨在客观反映科学数据相关活动安全控制的执行情况，从科学数据的保密性、可用性、完整性、可靠性、可控性、可追溯性、不可否认性等安全目标及合规性等方面给出科学数据安全控制工作的评价。

科学数据安全审计要求

1 范围

本文件规定了科学数据安全审计的相关要求，包括总体要求、一般审计要求和专项审计要求。

本文件适用于科学数据机构，对科学数据相关活动中所涉及的安全控制活动进行审计。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25069 信息安全技术 术语

GB/T 35294 信息技术 科学数据引用

GB/T 36092—2018 信息技术 备份存储 备份技术应用要求

GB/T 39335 信息安全技术 个人信息安全影响评估指南

GB/T 42574 信息安全技术 个人信息处理中告知和同意的实施指南

GB/T 43705 科学数据安全分类分级指南

GB/T 43708 科学数据安全要求通则

GB/T 44024 科学数据权益保护基本要求

3 术语和定义

GB/T 25069 和 GB/T 43708 界定的以及下列术语和定义适用于本文件。

3.1

科学数据 scientific data

在自然科学、工程技术科学等领域，科学研究活动中形成的以及通过观测监测、考察调查、检验检测等方式获取的原始及其衍生信息的记录，或可用于科学研究活动的其他数据。

[来源：GB/T 43708—2025，3.1]

3.2

科学数据安全 scientific data security

通过管理和技术措施，针对国家安全、科技安全、社会公共利益和他人合法权益，确保科学数据持续得到有效保护和合规利用的状态。

[来源：GB/T 43708—2025，3.2]

3.3

科学数据生存周期 scientific data lifecycle

科学数据从采集加工、存储备份、传输交换、开放共享、使用服务、安全处置，最终实现再利用的一个循环过程。

[来源：GB/T 43708—2025，3.3]

3.4

安全审计　security audit

对信息系统记录与活动的独立评审和考察，以测试系统控制的充分程度，确保对于既定安全策略和运行规程的符合性，发现安全违规，并在控制、安全策略和过程三方面提出改进建议。

[来源：GB/T 43708—2025，3.13]

3.5

个人信息　personal information

以电子或者其他方式记录的能够单独或者与其他信息结合来识别特定自然人身份或者反映其活动情况的各种信息。

[来源：GB/T 25069—2022，3.196]

3.6

个人敏感信息　personal sensitive information

一旦泄露、非法提供或滥用就有可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。

[来源：GB/T 25069—2022，3.195]

3.7

科学数据出版　scientific data publishing

组织按照统一规范的质量管理和控制机制，利用互联网及其他方式公开发布其在科研中产生的原始数据，或对原始数据进行收集、整理和再加工形成的数据的活动。

[来源：GB/T 43708—2025，A.3.14]

3.8

科学数据汇交　scientific data archiving

科学数据所有方将各类科学数据成果按标准的元数据格式和规范的步骤进行汇集和提交，以实现统一管理、共享和利用的过程。

[来源：GB/T 43708—2025，A.2.4]

4　审计总则

4.1　概述

科学数据安全审计要求遵循现有法律法规及相关标准，以指导、规范科学数据安全审计活动为总体目标，对科学数据相关活动安全控制的真实性及合规性进行审查和评价。

4.2　审计依据

科学数据安全审计的审计依据包括但不限于：

a）　国家数据安全相关法律、法规及标准；

b）　国家数据审计相关法律、法规及标准；

c）　地方数据审计相关规范及标准；

d）　组织内部数据审计相关规范及标准。

4.3　审计目标

科学数据安全审计以客观反映科学数据相关活动安全控制的执行情况为目标，从科学数据的保密

性、可用性、完整性、可靠性、可控性、可追溯性、不可否认性等安全目标及合规性给出科学数据安全控制工作的评价。

5 一般审计要求

5.1 概述

一般审计要求旨在综合评价科学数据相关组织机构安全目标实现情况，从安全策略、组织建设、人力资源管理、管理监督、安全管理、科学数据生存周期业务流程等几个方面，对科学数据安全控制工作进行通用审计（审计流程见附录 A 中的表 A.1）。

5.2 安全策略

安全策略应符合从指导、评估、监督三方面完善数据安全管理工作的原则，审计要求包括但不限于：

a） 具有明确的数据安全策略和目标，并与机构的战略方向一致；

b） 将数据安全管理工作整合到机构过程中；

c） 确立并提供用于建立、实现、维护和持续改进数据安全控制活动所需的资源；

d） 指导并支持相关人员为数据安全管理的有效性作出贡献；

e） 对机构数据安全管理工作进行有效评估；

f） 促进安全策略持续改进；

g） 明确机构科学数据相关活动安全合规要求。

5.3 组织建设

组织建设应确保与数据安全相关角色的责任和权限得到分配和沟通，审计要求包括但不限于：

a） 相关团队各角色及承担的安全职责明确；

b） 具有确定的沟通机制，保证跨部门协同的有效性。

5.4 人力资源管理

人力资源管理应确保对安全控制工作给予相应的人力资源支持，审计要求包括但不限于：

a） 数据安全管理所需人力资源持续可用；

b） 为实现安全策略，采取适用的措施持续保障工作人员的必要能力，确保上述人员在适当的教育、培训或经验的基础上能够胜任上述工作；

注：适当的措施可包括针对现有人员提供培训、指导或重新分配；雇佣或签约有能力的人员。

c） 定期对工作人员进行安全意识宣贯，保障培训常态化；

d） 根据相应岗位的角色及职责安全需求，建立具体的入职、在职、离职人员安全管理制度。

5.5 业务连续性管理

业务连续性管理审计要求包括但不限于：

a） 制定适合机构需求的连续性计划的目标；

b） 制定适合机构需求的重要性声明、优先级声明、机构指责声明、紧急程度和时限声明；

c） 制定业务连续性风险评估办法，并定期更新；

d） 具有明确的风险接受/风险缓解说明；

e） 具有针对不同安全级别科学数据的备份计划；

f) 具有明确的应急响应办法。

5.6 管理监督

管理监督审计要求包括但不限于：

a) 具有负责管理监督的职能团队并设立审计负责人，明确责任和权限；
b) 具有科学数据安全监督与审计的制度；
c) 定期进行管理监督评审，并形成相应的报告，内容包括监督与审计目的、范围、期间、依据、内容、审计中所执行的审计程序、测试的性质和范围及对监督与审计方法和指导的说明。

5.7 安全管理

5.7.1 安全管理办法

安全管理办法审计要求包括但不限于：

a) 根据科学数据安全需求制定管理办法，明确安全管理范围、安全管理目标、相关管理角色和责任；
b) 根据科学数据处理活动的特点，明确各科学数据处理活动的安全控制要求，制定机构安全控制基线，并制定具体的办法予以监督实施。

5.7.2 分类分级管理

分类分级管理审计要求包括但不限于：

a) 应设立分类分级工作管理岗位和人员，负责定义数据分类分级原则；
b) 按照机构的数据安全需求，应按照 GB/T 43705 要求制定科学数据分类分级管理办法；
c) 按照数据分类分级要求规定采取相应的安全控制措施；
d) 针对办法的符合性和安全措施的有效性进行评估并予以更新。

5.7.3 风险管理

风险管理审计要求包括但不限于：

a) 具有明确的风险管理目标和策略；
b) 应建立风险管理团队，包括组织架构、责任人、角色、职责和权限等；
c) 制定风险管理制度流程；
d) 应对风险识别、风险分析、风险评价和风险处置进行指导和监督。

5.7.4 内部审查

内部审查审计要求包括但不限于：应对数据处理活动安全性和合规性开展安全审查并出具审计报告。（审计报告概述参见附录 B，审计报告类型参照表 B.1，审计报告结构和内容参照表 B.2，审计报告样例参照表 B.3。）

5.8 科学数据生存周期业务流程

5.8.1 科学数据生存周期

科学数据生存周期的 6 个阶段：

a) 采集加工阶段：科学数据生产方或拥有方内部系统中新产生数据，以及从外部系统收集数据的阶段；

b) 存储备份阶段：科学数据以任何数字格式进行存储，并进行备份的阶段；
c) 传输交换阶段：科学数据从一个实体传输到另一个实体，进行科学数据交换的阶段；
d) 开放共享阶段：对科学数据进行分发、出版、共享的阶段；
e) 使用服务阶段：对科学数据进行计算、分析、可视化等操作，对外提供服务的阶段；
f) 安全处置阶段：对科学数据及数据存储媒介通过相应的操作手段，对科学数据进行长期归档，或对科学数据进行销毁删除的过程。

5.8.2 通用要求

通用要求审计包括但不限于：

a) 组织建设：应设立生存周期各业务流程管理团队，明确工作职责、责任人、角色和权限；
b) 制度流程：具有完善的安全制度流程，并监督执行及定期审核修订；
c) 操作行为安全管理：应具备人员操作行为相关安全管理制度，包括用户账号、权限、操作要求等；
d) 技术工具：应采取安全控制技术措施，对科学数据进行安全防护，具体内容包括：
   1) 完整性检测，采用科学数据完整性检测技术，保障数据的完整性；
   2) 数据加密，依据机构科学数据分类分级目录及相应安全需求对数据采用加密等技术进行保护；
   3) 身份验证，根据机构安全需求，对科学数据相关方进行身份鉴别，核验其合法身份；
   4) 访问控制，依据数据安全级别对访问科学数据的主体的访问进行控制；
   5) 安全风险评估，执行常态化的安全风险评估工作；
   6) 安全日志审计，对各业务环节进行行为审计、日志审计、流量审计，并存留审计记录。

5.8.3 采集加工

应保障数据采集加工过程的合规性和可追溯性，采集数据的完整性和可用性，审计要求包括但不限于：

a) 数据源鉴别：应对采集的科学数据的数据源进行鉴别和记录，防止数据仿冒和数据伪造；
b) 数据资源目录：定期形成科学数据资源目录，并进行周期性检查与核对，确保科学数据资源目录及其与实体资源对应关系的正确性；
c) 数据分类分级：依据数据分类分级结果对数据进行标识，并采用相应的安全控制措施进行分级保护；
d) 最小化采集加工：针对个人信息的采集，遵守最小化原则，并在采集数据前，明确数据的使用目的、采集数据范围；
e) 数据临时存储：针对采集终端临时数据存储需求，采用安全控制措施保障存储设备及环境的安全，对不同安全级别的数据采取分级保护措施。

5.8.4 存储备份

数据存储备份过程应保障数据的保密性、可用性和完整性，审计要求包括但不限于：

a) 存储备份设备及环境安全：
   1) 应建立存储设备及环境安全保护机制，保障存储媒介、核心交换机等设备安全可用，提供设备容错能力和故障恢复措施；
   2) 应对数据存储系统进行分域分级设计，将不同安全级别的数据存储在不同的媒介中，并定

期对媒介中的科学数据进行核对，检验媒介的安全性，保证科学数据的可用性；

3） 应对数据库管理系统和文件系统运行状况进行实时或定期监控，并定期进行安全风险评估。

b） 数据备份恢复，应建立应急管理和容灾备份机制，对重要的科学数据进行异地备份，数据备份的技术及应用要求应符合 GB/T 36092—2018 中第 4 章和第 5 章的规定。

c） 数据安全存储：

1） 按照不同数据类型、容量和合规性等需求，建立相应数据存储及管理系统；

2） 应对访问用户进行身份鉴别和访问控制，并对用户权限变更进行审核并记录；

3） 针对不同安全级别的数据采取相应数据加密措施，并选用安全的密码算法。

d） 数据导入导出，对科学数据导入导出过程进行安全管理，采用数据下载认证等技术防止导入导出过程中数据变更、篡改、泄露、丢失和破坏等。

5.8.5 传输交换

数据传输交换过程应保障数据的完整性、保密性，过程的可控性、可追溯性、不可否认性，审计要求包括但不限于：

a） 用户授权管理：应对科学数据传输交换中的用户进行授权管理，包括对用户角色、权限进行级别划分，并采取相应的授权管理措施；

b） 抗抵赖机制：应采用数字证书、访问控制等机制保障科学数据传输交换中的抗抵赖性；

c） 分级安全保护：针对不同安全级别的数据，在传输、线下交换过程中采用相应保护技术，分级保障数据的安全性；

d） 过程追溯：对科学数据传输交换进行过程追溯，核验是否留有日志，可对科学数据传输交换过程进行追踪和溯源。

5.8.6 开放共享

数据开放共享过程，特别是跨境流动提供过程，应保障数据的可用性、可控性、保密性，审计要求包括但不限于：

a） 数据发布：应对科学数据的发布内容、发布条件、发布方式、发布对象、审核程序等进行必要控制，根据分类分级结果进行脱敏处理或进行授权访问管理，建立科学数据发布应急处理流程，以确保在科学数据发布过程中的安全可控和合规；

b） 数据出境：应根据本领域科学数据属性及特点，采用相应的数据出境风险管理、审计、持续监控机制，并定期评估新技术手段对数据出境安全的影响，建立统一的数据共享交换系统及完善的数据出境管理制度流程，确保数据出境的安全；

c） 数据接口，应制定数据接口研发和调用过程中的安全控制措施，规避在通过接口方式提供科学数据服务时引发数据泄露等安全隐患。

5.8.7 使用服务

数据使用服务应保障数据可用性和保密性，过程可控性和可追溯性，审计要求包括但不限于：

a） 数据引用：科学数据的引用应符合 GB/T 35294 中对引用格式的要求，采用数据标识、数据引用等技术对科学数据引用和共享过程进行规范化管理，规避在科学数据生产、发布传播、访问获取等过程中的安全风险；

b） 数据分析：采取适当的安全防控措施，规避在对科学数据进行分析挖掘，形成科学数据产品的

过程中价值信息和个人隐私泄露等安全风险；

c) 服务环境：应提供安全的数据服务集成开发环境，将开发测试环境与真实生产环境分离，提供安全的开发调试工具；

d) 增值服务：应采用数据下载认证、授权、密码技术等安全控制措施，保障科学数据分析挖掘和形成数据产品过程的安全性；

e) 数据出版：应符合 GB/T 44024 中科学数据权益保护的要求，采用数据标识、数据引用、数据评审、数据出版审查等手段，保障数据出版的安全和合规，应对政府财政资金支持产生的跨境出版数据进行汇交。

5.8.8 安全处置

数据归档与销毁过程应保障数据完整性、可用性、保密性及过程可控性，审计要求包括但不限于。

a) 归档设备及环境安全：

1) 建立历史性科学数据长期归档机制，定期开展归档数据存储安全的风险评估；

2) 定期对长期归档设备及运行环境进行检查和维护，并定期检查和报告归档数据的状态；

3) 建立档案管理系统，确保归档数据的真实性、完整性和可用性，并定期进行数据迁移；

4) 根据数据安全级别要求，制定相应归档备份策略并定期对数据进行归档，对数据归档流转过程进行监控与审计。

b) 数据清除净化安全，建立针对数据内容的清除、净化机制，采用逻辑删除、物理销毁以及媒体擦除等方式对其进行安全处置。

6 专项审计要求

6.1 概述

专项审计旨在根据外部要求及机构内部特殊要求，从个人信息安全、汇交安全、数据出境安全方面，对机构专项科学数据活动的安全控制工作进行审计。

6.2 个人信息安全

6.2.1 通用管理

通用管理审计要求包括但不限于：

a) 组织建设：应建立个人信息安全管理团队，确保个人信息保护工作的方针、目标、原则合规有效，达到规定数量的个人信息处理者，应指定个人信息保护负责人，对个人信息处理活动合规性负责；

b) 制度流程：明确个人信息保护安全需求，建立个人信息保护管理制度和操作流程；

c) 技术措施：应采取与所处理个人信息规模、类型相适应的安全技术措施，对个人敏感信息的保护宜采用加密、去标识化、访问控制等安全技术措施，避免数据泄露和滥用；

d) 教育培训：定期对管理人员、技术人员、全员开展相应的安全教育和培训，并进行考核；

e) 个人信息采集：应当限于实现处理目的的最小范围，不得过度收集个人信息；

f) 告知义务：个人信息处理者应按照 GB/T 42574 中所确定的告知和同意要求，对符合告知和同意适用情形的个人信息处理活动，取得个人同意、向个人告知个人信息处理规则，保障个人权益，满足合规要求；

g) 其他要求，对于外籍人士个人信息的境内采集应符合相关规定；

h） 符合法律法规的相关规定。

6.2.2 个人信息识别与分类分级

个人信息识别与分类分级审计要求包括但不限于：

a） 建立满足领域特性及合规性的个人信息分类分级制度流程；

b） 应对个人信息和个人敏感信息进行有效识别；

c） 应根据分类分级结果制定相适应的安全控制措施。

6.2.3 自动化决策处理个人信息

自动化决策处理个人信息审计要求包括但不限于：

a） 事前对算法模型进行安全评估，并根据应用场景的改变重新进行评估；

b） 采取必要措施对算法和参数模型进行保护；

c） 对个人信息处理、标签管理、模型训练等自动化决策过程中的人工操作进行记录；

d） 其他可能影响自动化决策透明度和结果公平、公正的事项。

6.2.4 个人信息安全影响评估

数据处理者进行如下个人信息处理活动时，应按照 GB/T 39335 中确定的评估实施流程进行个人信息安全影响评估，并对处理情况进行记录，可能的个人信息处理活动包括：

a） 处理敏感个人信息；

b） 利用个人信息进行自动化决策；

c） 委托处理个人信息、向其他个人信息处理者提供个人信息、公开个人信息；

d） 向境外提供个人信息；

e） 其他对个人权益有重大影响的个人信息处理活动。

6.2.5 出境安全风险评估

出境安全风险评估审计要求包括但不限于：

a） 因业务需要向境外提供个人信息的机构，应依据个人信息规模、类型进行出境安全风险评估，满足合规性要求；

b） 个人信息处理者向境外提供个人信息，应采取必要措施，保障境外接收方处理个人信息活动达到我国法律法规规定的个人信息保护标准。

6.2.6 应急管理

应急管理审计要求包括但不限于：

a） 个人信息处理者应制定个人信息安全事件应急预案，对面临的个人信息安全风险作出系统性评估和预测；

b） 从组织机构、人员、技术、物资保障及指挥处置流程和支持措施等方面确保足以应对预测风险；

c） 对相关人员进行应急预案培训，定期对应急预案进行演练；

d） 应对应急响应处置情况进行评价及改进。

6.2.7 内部审查

内部审查应定期对个人信息处理活动进行审查和评价，审计要求包括但不限于：

a） 组织架构、制度流程、管理程序、技术措施与个人信息的性质、规模、复杂程度、风险程度的适

应性；

b） 个人信息保护职责分工合理、职责明确、报告关系清晰；

c） 为个人信息保护提供的资源与合规风险的匹配性。

6.3 汇交安全

6.3.1 通用管理

汇交安全通用管理审计要求包括但不限于：

a） 科学数据中心等相关数据管理机构在授权范围内开展科学数据汇交工作，并保障其安全；

b） 建立数据汇交安全管理制度流程，保障汇交数据的安全性和汇交工作的规范性，确保由国家公共财政支出产生的科学数据有效保存和合理应用。

6.3.2 分类分级管理

审计分类分级管理时，应根据 5.7.2 中所述的要求对汇交数据分类分级管理进行审查。

6.3.3 存储和传输安全管理

存储和传输安全管理审计要求包括但不限于：

a） 存储安全管理：应根据 5.8.4 和 5.8.8 中所述的要求对汇交数据进行存储及备份管理进行审查，保证汇交数据的保密性、可用性、完整性和可控性；

b） 传输安全管理：应根据 5.8.5 中所述的要求对汇交数据的传输进行管理和审查，保证科学数据的完整性、保密性、可控性、可追溯性、不可否认性。

6.3.4 汇交数据登记管理

汇交数据登记管理审计要求包括但不限于：

a） 组织建设：设立数据汇交专员负责进行登记管理；

b） 制度流程：

1） 制定数据资源登记管理流程，建立数据资源清单，明确数据源管理的相关方；

2） 对于密钥类数据，明确密钥管理安全要求，应至少涵盖密钥生产、备份、存储、使用、分发、更新等相关的流程和要求。

6.3.5 内部审查

内部审查工作审计要求包括但不限于：

a） 组织建设：应设立负责人对数据汇交定期进行安全审查；

b） 制度流程：应建立内部审查相关规则，并对其有效性进行评估并予以更新。

6.4 数据出境安全

6.4.1 通用管理

数据出境安全通用管理审计要求包括但不限于：

a） 组织建设：应指定数据出境安全负责人，对数据出境活动进行有效管理和监督；

b） 制度流程：应制定科学数据出境安全管理文件，明确数据出境安全管理范围、具体安全管理目标；

c） 技术措施：应对跨境数据的传输采取有效的安全保护措施，完善访问控制和授权机制，对数据

流转全过程进行记录，监控和防范数据泄露风险，并制定应急处置预案；

d） 教育培训要求，定期对从业人员进行安全教育和培训；

e） 符合法律法规的相关规定。

6.4.2 个人信息出境安全

个人信息出境安全审计应满足 6.2 中所述的要求，审查对个人信息出境活动的管理和监督是否合规。

6.4.3 分类分级管理

分类分级管理审计应满足 5.7.2 中所述的要求，确保为数据出境安全控制措施和风险评估提供依据。

6.4.4 安全风险评估

数据处理者向境外提供数据满足国家规定需进行数据出境安全评估的情形，应保障事前评估和持续监督相结合、风险自评估与安全评估相结合，防范数据出境安全风险，审计要求包括但不限于：

a） 应按规定进行风险自评估；

b） 应按照规定向相关部门申请数据出境风险评估；

c） 应依照规定对评估的有效性进行持续监督。

6.4.5 内部审查

审计内部审查工作时，审计要求包括但不限于：

a） 组织建设：应设立负责人对数据出境合规性进行定期安全审查；

b） 制度流程：应建立内部审查制度流程，并对其有效性进行评估并予以更新。

附 录 A
（资料性）
审计流程

A.1 概述

审计流程是审计人员开展审计活动所采取的系列行动和步骤，包括审计准备、审计实施、审计终结和后续审计4个阶段。

A.2 审计流程

表 A.1 审计流程表

阶段	内容
审计准备	(1)明确审计目的及任务； (2)组建审计项目组，明确角色和责任，并确保所有人员均具备完成该项目相应的专业胜任能力； (3)搜集相关信息； (4)编制审计项目计划及审计程序，并在审计计划中运用风险评估
审计实施	(1)深入调查并调整审计计划； (2)了解并初步评估安全控制目标达成及合规情况； (3)进行控制测试； (4)进行实质性测试
审计终结	(1)整理和复核审计工作底稿； (2)评价相关安全控制目标的实现和合规情况； (3)判断并报告审计发现； (4)沟通审计结果； (5)编写审计报告并进行沟通； (6)提交审计报告； (7)归档管理
后续审计	对审计中发现的重大问题和控制缺陷，整改效果不明显的审计项目，开展后续审计

附 录 B
（资料性）
审计报告

B.1 概述

审计报告是数据安全审计监督活动的“交付产品”，是数据安全审计意见的书面文件。

B.2 审计报告的类型

审计业务的种类、目的不同，审计报告的具体格式和内容也会有所变化，具体分类如表 B.1 所示。

表 B.1 审计报告分类表

分类	说明
按审计范围和内容划分	(1)一般审计报告 (2)专项审计报告
按审计意见类型划分	(1)无保留意见的审计报告 注明没有发现异常情况，或发现的任何异常情况均未累积成为重要缺陷。 (2)保留意见的审计报告 注明累积成为重要缺陷的异常情况(但并非重大漏洞)。 (3)否定意见的审计报告 注明一种或多种重要缺陷累积成为重大漏洞

B.3 审计报告的结构和内容

审计报告通常具有以下结构和内容，如表 B.2 所示。

表 B.2 审计报告的结构和内容

报告结构	报告内容
报告送达	报告接收人
报告摘要	应包括被审计单位名称、审计目的、审计范围、审计期间、审计依据、双方责任、审计内容、审计中所执行的审计程序、测试的性质和范围及对审计方法和指导的说明
现状描述	描述机构目前数据安全(与审计范围相关)现状，描述内容包括但不限于： (1)安全策略、组织建设、人力资源管理、管理监督、安全管理、生存周期管理等一般审计要求的符合情况； (2)个人信息安全、汇交安全等专项审计要求的符合情况
审计发现	依据审计要求分章节描述数据安全管理、技术控制的缺失及风险程度，章节可按审计发现的重要性或预期接收人划分

表 B.2　审计报告的结构和内容（续）

报告结构	报告内容
审计结论和意见	(1)对审计中所测试的控制及程序的真实性作出整体结论和意见； (2)指出所发现缺陷及可能导致的潜在风险 注：当审计人员无法获得充分和适当的审计证据，或由于多重不确定性潜在因素、累积影响而导致不可能形成审计意见时，则可拒绝发表意见。
保留意见和限制因素	陈述所测试的控制或程序是充分或不充分的。审计报告应当支持审计结论，审计中收集的所有证据也应当为审计结果提供较高水平支持
详细的审计发现和建议	审计发现应依据审计发现的重要性和审计报告的预期接收人编制。审计发现的内容包括但不限于： (1)数据安全战略于组织战略的一致性、数据安全目标与业务目标一致性、风险的有效评估和控制、业务活动的合法合规控制； (2)科学数据安全管理中存在的一致性、符合性及合规性问题； (3)生存周期业务流程中的安全控制工作的符合性、完备性问题； (4)专项安全控制中的合规性等问题
其他(如备忘录等)	针对审计发现，审计人员应根据重要性原则，对不重要的审计发现可采取备忘录等其他的方式向管理层提交

B.4　审计报告样例

个人信息安全管理专项审计报告样例如表 B.3 所示。

表 B.3　＊单位个人信息安全管理专项审计报告

编　号：　　共　页　第　页

<table>
<tr><td colspan="3">被审计单位名称：＊数据中心</td></tr>
<tr><td colspan="2">审计项目名称：个人信息安全管理情况</td><td>审计目的：个人信息处理过程的合规性</td></tr>
<tr><td colspan="3">审计事项期间：＊年＊月至＊年＊月</td></tr>
<tr><td>审计事实描述</td><td colspan="2">示例：
（一）审计依据
《＊数据中心个人信息安全管理条例》
（二）审计内容及目标
1.通用管理
是否针对个人信息，进行个人信息保护的管理和风险管理，相关策略规范的制定是否能满足合规的要求。
2.个人信息生存周期环节管理
如在个人信息收集环节，是否制定安全策略和规范，安全措施是否有效落实，对个人信息实现保护。
（三）审计的主要方法和程序
1.访谈组织数据管理部门，了解是否基于业务量和个人信息处理数量，设立专职的个人信息保护负责机构与负责人，并明确相关工作职责；检查组织是否制定个人信息和个人隐私保护管理规范；检查组织是否具有个人信息安全影响评估制度并定期开展个人信息安全影响评估，并查阅历史评估记录；是否制定个人信息安全事件应急预案并定期开展应急响应培训和应急演练。
2.访问组织数据安全管理部门数据，检查组织是否基于组织安全需求采取分类分级管理。
3.访谈组织个人信息采集等岗位负责人，了解个人信息生存周期各环节安全管理情况。
4.访谈组织数据管理部门，是否具有个人信息出境需求，检查组织是否建立安全风险评估和审批流程，满足国家合规监管要求。

附件</td></tr>
<tr><td></td><td>审计人员：＊＊＊</td><td>编制日期：20＊＊年＊月＊日</td></tr>
</table>

编　号：　　共　页　第　页

（续）

<table>
<tr><td rowspan="2">复核意见</td><td colspan="3"></td></tr>
<tr><td colspan="2">复核人员：＊ ＊ ＊</td><td>复核日期：20＊ ＊年＊月＊日</td></tr>
<tr><td rowspan="2">被审计单位意见</td><td colspan="3"></td></tr>
<tr><td colspan="2">签字：</td><td>盖章：</td></tr>
<tr><td rowspan="2">审计结论及意见</td><td colspan="3">（一）审计发现举例（常见的问题和风险）
1. 未建立个人信息保护组织或缺乏相关负责人，不利于个人信息保护工作的推广和执行，也无法有效落实个人信息保护的责任。
2.未建立规范化的个人信息保护制度和流程，可能造成个人信息的收集、存储、使用、变更、销毁等操作不合法的情况。
3. 组织在使用个人信息时，没有开展安全影响评估，无法判断个人信息使用与保护的程度，容易造成侵权与违规风险。
4. 在收集个人信息时，没有注意最小化要求，或者在没有得到允许的情况下公开记录个人信息，容易造成侵权与违规风险。
5. 组织在处理个人敏感信息时，个人信息的传输、处理、存储、销毁未采用加密，访问控制等安全措施，容易造成泄露个人敏感信息的风险。
（二）审计结论及意见
审计整体结论和意见，参见表 B.1 审计意见类型划分。
（三）其他说明</td></tr>
<tr><td colspan="2">审计人员：＊ ＊ ＊</td><td>编制日期：20＊ ＊年＊月＊日</td></tr>
<tr><td rowspan="2">复核意见</td><td colspan="2"></td><td></td></tr>
<tr><td colspan="2">复核人员：＊ ＊ ＊</td><td>复核日期：20＊ ＊年＊月＊日</td></tr>
</table>

参 考 文 献

[1] GB/T 22080—2016 信息技术 安全技术 信息安全管理体系 要求
[2] GB/T 25069—2022 信息安全技术 术语
[3] GB/T 32923—2016 信息技术 安全技术 信息安全治理
[4] GB/T 34960.4—2017 信息技术服务 治理 第4部分:审计导则
[5] GB/T 35274—2023 信息安全技术 大数据服务安全能力要求
[6] GB/T 36344—2018 信息技术 数据质量评价指标
[7] GB/T 37988—2019 信息安全技术 数据安全能力成熟度模型
[8] T/CIIA 018—2022 科学数据 安全管理指南
[9] T/CIIA 019—2022 科学数据 安全能力成熟度模型
[10] T/CIIA 020—2022 科学数据 安全传输技术要求
[11] T/CIIA 021—2022 科学数据 安全防护技术要求
[12] T/CIIA 022—2022 科学数据 云存储环境运维流程与服务要求
[13] T/CIIA 023—2022 科学数据 云平台运维流程与要求
[14] T/CIIA 030—2022 微生物数据库安全体系设计要求
[15] 中华人民共和国网络安全法
[16] 科学数据管理办法
[17] 中华人民共和国密码法
[18] 中华人民共和国数据安全法
[19] 中华人民共和国个人信息保护法
[20] 数据出境安全评估办法