ICS 35.080
L77

团 体 标 准

T/ CESA 1078—2020

信息技术服务 治理 数据审计

Information technology service - Governance-Data audit

2020-03-01 发布　　2020-09-01 实施

中国电子工业标准化技术协会　　发布

目　　次

前　言

本标准按照GB/T 1.1-2009给出的规则起草。

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这些专利的责任。

本标准由中国电子技术标准化研究院提出。

本标准由中国电子技术标准化研究院、中国电子工业标准化技术协会归口。

本标准起草单位：上海谷航信息科技发展有限公司、中国电子技术标准化研究院、国信优易数据有限公司、上海软中信息技术有限公司、北京赛迪认证中心有限公司、无锡农村商业银行股份有限公司、江苏江阴农村商业银行股份有限公司、四川久远银海软件股份有限公司、上海瀚纬信息科技有限公司、广州赛宝联睿信息科技有限公司、神州数码系统集成服务有限公司、万达信息股份有限公司、上海安言信息技术有限公司、北京易服务信息技术有限公司、广东鑫盟管理咨询有限公司、上海计算机软件技术开发中心、首都信息发展股份有限公司、上海华讯网络系统有限公司、北京中软国际信息技术有限公司。

本标准参加起草单位：北京国家会计学院、上海市卫生健康委员会、国家计算机网络与信息安全管理中心上海分中心、上海交通大学、上海市卫生健康信息中心、东北农业大学。

本标准主要起草人：方健、张凤玲、俞文平、郭鑫伟、赵丹丹、宋俊典、马烈、王春涛、杨军、张树玲、施勇、戴沁芸、浦轶华、胡海燕、谢桦、陈宏峰、孙佩、李光亚、郑晨光、黄建新、张明英、周鹏、黄建文、宋跃武、肖筱华、钱伟峰、谢斌、何敬任、颜珠、姜亮、孙翊威、米昂、陈雯、朱永佳、王萌、俞丽平、居琰、曹剑峰、周鹏程、王铮、廖伟、杨琳、张娜、李彩虹、于宏志、陈昌杰、秦峰、高洪美、韩佳赟、王安妮、李晨光、李俊彦、李易、杨明。

信息技术服务 治理 数据审计

1 范围

本标准规定了数据审计总则、数据审计组织管理、数据审计人员、数据内部控制审计、审计流程、审计系统、审计报告等内容。

本部分适用于：

a) 组织治理主体实施数据审计监督职能；
b) 建立或完善组织的数据审计体系及相关平台；
c) 明确组织数据审计过程中的相关要求；
d) 规范组织数据审计业务的开展及相关平台的建设；
e) 第三方或其他相关机构开展数据审计的指导
f) 建立或未建立内部数据审计机构的组织，均可聘请第三方依据本标准的相关要求开展数据审计。

各级各类信息化主管部门、监管机构及审计监督机构，可根据法律法规、部门规章的要求，使用本标准对所管辖各类组织的数据审计提出要求，并进行监督。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是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 34960.1 信息技术服务 治理 第1部分：通用要求
GB/T 34960.4 信息技术服务 治理 第4部分：审计导则
GB/T 34960.5 信息技术服务 治理 第5部分：数据治理规范

3 术语和定义

3.1

数据 data

所有能输入到计算机并被计算机程序处理的符号介质的总称，是用于输入电子计算机进行处理，具有一定意义的数字、字母、符号和模拟量等的通称。

3.2

数据审计 data audit

根据数据审计依据的要求,对数据本身以及与其形成过程相关的内部控制和流程进行检查、评价，并发表审计意见。

3.3

信息技术审计 information technology audit（IT audit）

根据IT审计标准的要求，对信息系统及相关的IT内部控制和流程进行检查、评价，并发表审计意见。

[GB/T 34960.4—2017，定义3.2]

3.4

数据治理组织控制 data governance organization control

在组织层面建立并实施的数据治理相关控制，控制要素包括数据控制环境、风险评估、控制活动、信息与沟通及内部监督。

3.5

数据治理组织控制审计 data governance organization control audit

对数据治理组织控制开展的审计。

3.6

数据治理一般控制 data governance general control

为了保证数据治理信息系统安全、稳定的运行，对整个数据治理信息系统以及外部各种环境要素实施的控制。

3.7

数据治理一般控制审计 data governance general control audit

对数据治理一般控制开展的审计。

3.8

数据治理应用内部控制 data governance application internal control

为合理保证数据治理信息系统安全可靠地实现数据准备、分析、挖掘等功能，而设计、执行的控制。

3.9

数据治理应用内部控制审计 data governance application internal control audit

对数据治理信息系统控制开展的审计。

4 数据审计总则

4.1 审计与治理的关系

数据治理是 IT 治理的一部分，数据审计是 IT 审计的一部分。组织的 IT 审计与治理的关系要求见 GB/T 34960.4《信息技术服务 治理 第 4 部分：审计导则》。

4.2 审计结构及其关系

数据审计是 IT 审计的一部分，组织的 IT 审计结构及其关系要求见 GB/T 34960.4《信息技术服务 治理 第 4 部分：审计导则》。

4.3 审计依据

数据审计依据包括但不限于：

a) 国家 IT 与数据相关法律、法规及标准；
b) 行业 IT 与数据相关规范及标准；
c) 地方 IT 与数据相关规范及标准；
d) 组织内部 IT 与数据相关规范及标准；

e) 国际 IT 与数据相关标准；
f) 国内外 IT 与数据最佳实践。

4.4 审计方法

组织的数据审计方法要求见 GB/T 34960.4《信息技术服务 治理 第 4 部分：审计导则》。

4.5 审计技术

组织的数据审计技术要求见 GB/T 34960.4《信息技术服务 治理 第 4 部分：审计导则》。

4.6 审计质量控制

组织的数据审计质量控制要求见 GB/T 34960.4《信息技术服务 治理 第 4 部分：审计导则》。

4.7 审计业务类型

数据审计业务类型包括数据治理内部控制专项审计和数据特定领域专项审计。数据治理内部控制专项审计是为了综合评价组织数据治理控制目标实现过程而进行的审计；数据特定领域专项审计是组织根据外部要求及内部特殊需要而进行的审计。数据审计业务可作为独立的审计项目实施，或作为综合性审计项目的组成部分组织实施。

当数据审计业务作为综合性审计项目的一部分时，数据审计人员在进行审计计划时应考虑项目审计目标及要求，在审计实施过程中应及时与其他相关审计人员沟通数据审计中的发现，并考虑依据数据审计结果调整其他相关审计的范围、时间及性质。

数据审计人员应当以风险导向为基础开展审计，风险评估应当贯穿于审计的全过程。

4.8 审计工作的执行

组织的审计工作执行要求见GB/T 34960.4《信息技术服务 治理 第4部分：审计导则》。

4.9 审计方式

审计方式是指利用计算机辅助审计技术、大数据技术、人工智能技术等手段开展的审计，包括现场审计和远程审计。

5 数据审计组织管理

数据审计组织管理通用要求见GB/T 34960.4《信息技术服务 治理 第4部分：审计导则》，同时还应：

a) 为数据审计开展创造必要的环境；
b) 明确审计机构的职责和权力；
c) 在审计章程中明确数据审计的相关要求；
d) 制定数据审计相关制度、流程及操作规程等；
e) 建立数据审计系统；
f) 制定数据审计战略规划。

6 数据审计人员

数据审计需要拥有审计、业务、IT、数据治理与管理、数据审计等方面的专业知识和技能，相关审计人员应具备数据审计资质。数据审计与IT审计具有一定的关联关系。组织的IT审计人员要求见GB/T 34960.4《信息技术服务 治理 第4部分：审计导则》，组织的数据审计人员要求包括但不限于：

a) 职业道德，包括诚实、守信、正确履行职责及保守保密等；
b) 知识、技能、资质和经验，包括掌握与审计、业务、IT、数据治理与管理、数据审计等方面的专业知识和技能、拥有与所处管理或业务岗位相适应的数据审计职业资格及经验等；
c) 专业胜任能力，包括具备相应的数据审计专业胜任能力、拥有与所处管理或业务岗位相适应的数据审计职业资格、定期参加持续的职业教育和培训等；
d) 利用外部专家服务，包括对其专业资格、专业经验、独立性、客观性与专业胜任能力进行评价，对其服务结果进行评价与利用，并与外部专家签订书面协议等。

7 数据治理内部控制专项审计

7.1 总则

数据治理内部控制专项审计是为了综合评价组织数据治理控制目标实现过程而进行的审计，包括数据治理组织控制、数据治理一般性控制和数据治理应用控制的审查和评价。数据治理内部控制专项审计是组织常规审计内容的一部分。组织宜依据GB/T 34960.5《信息技术服务 治理 第5部分：数据治理规范》、行业数据治理规范等开展数据治理内部控制专项审计。

7.2 数据治理组织控制审计

7.2.1 控制环境

审计数据治理控制环境时，审计范围包括但不限于：

a) 组织遵循的数据治理原则；
b) 数据治理战略、IT 战略与业务战略的一致性；
c) 决策层的数据风险偏好及风险容忍度；
d) 数据治理与管理的职责分工和制衡机制；
e) 数据治理内部控制的监督机制；
f) 数据治理内部控制机构的设置、职责与权限；
g) 内部审计机构设置、人员配备和工作独立性；
h) 数据治理相关人力资源政策；
i) 决策层对组织数据风险概况及如何应对的了解程度。

7.2.2 风险评估

审计数据治理风险评估时，审计范围包括但不限于：

a) 数据治理风险管理目标和策略；
b) 数据治理风险管理原则；
c) 数据治理风险组织管理，包括组织架构、责任人、角色、职责和权限等；
d) 数据治理风险管理制度；
e) 数据治理风险管理流程；
f) 数据风险识别、风险分析、风险评价及风险处置的执行情况；
g) 数据资产的所有权和控制权；
h) 数据资产所有者的职责。

7.2.3 控制活动

7.2.3.1 通用要求

审计组织层面数据治理控制活动的通用要求时，应结合数据治理控制环境的审计进行，审计范围包括但不限于：

a) 数据治理控制政策与流程；
b) 数据治理授权与审批控制；
c) 数据治理预算控制；
d) 数据治理信息记录与报告；
e) 数据治理资产保护；
f) 数据治理绩效考核；
g) 数据治理不相容职责分离。

7.2.3.2 顶层设计

审计数据治理顶层设计是控制环境要求的具体体现，此部分审计应结合安全控制环境的审计进行，审计范围包括但不限于：

a) 战略规划控制措施的合理性、有效性；
b) 组织构建控制措施的合理性、有效性；
c) 架构设计控制措施的合理性、有效性。

7.2.3.3 数据治理域

审计数据治理域是控制环境要求的具体体现，此部分审计应结合安全控制环境的审计进行，审计范围包括但不限于治理主体对以下管理情况要求，以及相关的评估、指导、监督和改进情况：

a) 数据管理体系建设控制措施的合理性、有效性；
b) 数据价值体系建设控制措施的合理性、有效性。

7.2.3.4 数据治理过程

审计数据治理过程是控制环境要求的具体体现，此部分审计应结合安全控制环境的审计进行，审计范围包括但不限于：

a) 统筹和规划控制措施的合理性、有效性；
b) 构建和运行控制措施的合理性、有效性；
c) 监控和评价控制措施的合理性、有效性；
d) 改进和优化控制措施的合理性、有效性。

7.2.4 信息与沟通

审计数据治理的信息与沟通时，审计范围包括但不限于：

a) 与数据治理相关的信息系统架构，以及对决策与业务的支持度；
b) 决策层有关数据治理的信息沟通模式；
c) 数据治理战略、政策及制度等方面的传达与沟通的连续性、完整性及有效性；
d) 组织对数据治理风险内部控制所需要信息的明确；
e) 组织与外部的信息沟通模式及方案。

7.2.5 内部监督

审计数据治理内部监督时，审计范围包括但不限于：

a) 数据治理是否纳入内部监督范畴；

b) 数据治理监控管理报告系统、监控反馈、跟踪处理程序；
c) 数据治理内部控制的自我评估机制；
d) 已按规定要求开展数据治理审计工作；
e) 组织对数据治理风险控制的监督、自我评估及整改情况。

7.3 数据治理一般控制审计

7.3.1 通用要求

审计数据治理一般控制的通用要求时，审计范围包括但不限于：

a) 数据治理控制政策与流程；
b) 数据治理授权与审批控制；
c) 信息记录与报告；
d) 资产保护；
e) 绩效考核；
f) 不相容职责分离。

7.3.2 采购管理

组织的数据治理一般控制采购管理审计要求见 GB/T 34960.4《信息技术服务 治理 第 4 部分：审计导则》。

7.3.3 项目整体管理

组织的数据治理一般控制项目整体管理审计要求见 GB/T 34960.4《信息技术服务 治理 第 4 部分：审计导则》。

7.3.4 数据治理信息系统开发管理

审计数据治理信息系统开发管理时，审计范围包括但不限于：

a) 组织模式；
b) 需求管理；
c) 过程管理。

7.3.5 数据治理信息系统交付管理

审计数据治理信息系统交付管理时，审计范围包括但不限于：

a) 配置管理；
b) 构建与持续集成；
c) 测试管理；
d) 配置与发布管理。

7.3.6 数据治理信息系统运营管理

审计数据治理信息系统运营管理时，审计范围包括但不限于：

a) 监控管理；
b) 物理环境；
c) 变更管理；
d) 容量与性能管理；
e) 成本管理；
f) 事件管理；
g) 问题管理；

h) 备份与恢复管理；
i) 应急及灾备管理；
j) 安全管理。

7.3.7 其他相关控制

数据治理一般控制中的其他相关控制审计要求见GB/T 34960.4《信息技术服务 治理 第4部分：审计导则》。

7.4 数据治理应用控制审计

7.4.1 通用要求

审计数据治理应用控制的通用要求时，审计范围包括但不限于：

a) 应用控制政策与流程；
b) 应用授权与审批控制；
c) 信息记录与报告；
d) 资产保护；
e) 绩效考核；
f) 不相容职责分离。

7.4.2 数据治理信息系统应用组织管理

审计数据治理信息系统的组织管理时，审计范围包括但不限于：

a) 组织结构，包括组织架构设置、部门及岗位职责等；
b) 用户管理，包括用户账号及权限等；
c) 参数管理，包括参数设置的范围与依据、参数调整的授权与审批及参数调整的日志记录等；
d) 操作管理，包括操作环境、功能使用、操作要求等；
e) 网络与信息安全管理，包括网络安全、系统应用环境安全、操作安全、介质与文档安全、数据脱敏等；
f) 事件管理，包括事件记录、上报、处理、跟踪与监控等；
g) 问题管理，包括问题的确定、记录、分类、处理、解决及跟踪等；
h) 文档与数据管理，包括文档与数据介质的生成、分类、归档、保存、调用及销毁等；
i) 绩效考核与奖惩，包括绩效考核指标、评价方法、评价结果及奖惩措施等。

7.4.3 数据治理信息系统数据流程设计

审计数据治理信息系统数据流程控制时，审计范围包括但不限于：

a) 数据流程设计的完备性；
b) 数据流程处理的正确性和控制的有效性；
c) 数据治理信息系统功能的合理性。

7.4.4 数据采集、处理及输出

审计数据采集、处理及输出时，审计范围包括但不限于：

a) 数据采集控制，包括数据导入、修改、删除、校验、备份的恢复、权限控制及错误处理机制等；
b) 数据处理控制，包括数据清洗、数据转换、数据整理、数据计算、数据汇总控制及错误处理机制等；
c) 数据输出控制，包括输出外设、输出范围和内容、输出信息分发、保存和访问、备份、权限控制及错误处理机制等。

7.4.5 系统接口与信息共享

7.4.5.1 系统接口

审计系统接口时，审计范围包括但不限于：

a) 系统接口标准；
b) 接口/转换控制，包括数据采集、校验、转换、传输、权限控制及错误处理机制等。

7.4.5.2 信息共享

审计信息共享时，审计范围包括但不限于：

a) 共享信息分类；
b) 共享信息的控制。

7.4.6 数据质量

审计数据质量时，审计范围包括但不限于：

a) 数据质量管理，包括数据质量管理的组织、制度、流程及控制执行等；
b) 数据质量，包括完整性、准确性、有效性、合法性、一致性等。

8 数据特定领域专项审计

8.1 总则

数据特定领域专项审计是组织根据外部要求及内部特殊需要而进行的审计。数据特定领域专项审计是组织常规审计内容的一部分。数据特定领域专项审计包括（但不限于）数据库管理专项审计、外部数据管理专项审计、业务数据管理专项审计、数据生存周期管理专项审计、数据应用管理专项审计、数据安全管理专项审计、云数据管理专项审计、数据合规管理专项审计、数据治理绩效专项审计、数据质量管理专项审计及数据资产管理专项审计等。

8.2 数据库管理专项审计

数据库管理专项审计是指针对存储数据的数据库管理开展专项审计，审计范围包括但不限于：

a) 数据库管理目标、方针和策略；
b) 数据库组织管理，包括组织架构、责任人、角色、职责和权限等；
c) 数据库管理制度和流程；
d) 业务需求说明书；
e) 数据库架构设计方案；
f) 数据结构的规范性、合理性；
g) 数据标准；
h) 数据库管理风险评估与审计机制的建立。

8.3 外部数据管理专项审计

外部数据管理专项审计是指针对从组织外部获取数据的管理开展专项审计，审计范围包括但不限于：

a) 外部数据管理目标、方针和策略；
b) 外部数据组织管理，包括组织架构、责任人、角色、职责和权限等；
c) 外部数据管理制度和流程；
d) 外部数据来源的合理性、合规性；

e) 外部数据安全的分级分类和保护机制；
f) 外部数据质量，包括完整性、准确性、有效性、合法性、一致性等；
g) 外部数据生存周期管理，包括数据获取、处理、使用、存储、传输及销毁等；
h) 外部数据应用领域的规范性、合理性；
i) 外部数据风险评估与审计机制的建立。

8.4 业务数据管理专项审计

业务数据管理专项审计是指针对业务数据的管理开展专项审计，审计范围包括但不限于：

a) 业务数据管理目标、方针和策略；
b) 业务数据组织管理，包括组织架构、责任人、角色、职责和权限等；
c) 业务数据管理制度和流程；
d) 业务数据安全的分级分类和保护机制；
e) 业务数据获取方式和来源的可靠性；
f) 业务数据敏感信息的保护机制；
g) 业务数据标准与模型；
h) 数据的合规与隐私保护；
i) 业务数据质量，包括完整性、准确性、有效性、合法性、一致性等；
j) 业务数据生存周期，包括数据获取、处理、使用、存储、传输及销毁等；
k) 业务数据应用领域的规范性、合理性；
l) 业务数据风险评估与审计机制的建立。

8.5 数据生存周期管理专项审计

数据生存周期管理专项审计是指针对数据生存周期的管理开展专项审计，审计范围包括但不限于：

a) 数据生存周期管理目标、方针和策略；
b) 数据生存周期组织管理，包括组织架构、责任人、角色、职责和权限等；
c) 数据生存周期管理制度，包括数据质量、数据安全、数据模型、数据标准及元数据等；
d) 数据生存周期管理流程，包括数据获取、处理、使用、存储、传输及销毁等；
e) 数据生存周期管理风险评估与审计机制的建立。

8.6 数据应用管理专项审计

数据应用管理专项审计是指针对数据应用的管理开展专项审计，审计范围包括但不限于：

a) 数据应用管理目标、方针和策略；
b) 数据应用组织管理，包括组织架构、责任人、角色、职责和权限等；
c) 数据应用管理制度和流程；
d) 数据应用安全的分级分类和保护机制；
e) 数据的合规与隐私保护；
f) 数据应用相关标准与模型；
g) 数据获取方式和来源的可靠性；
h) 数据应用个人信息的保护机制；
i) 数据质量，包括数据完整性、准确性、有效性、合法性、一致性等；
j) 数据应用生存周期管理，包括数据获取、处理、使用、存储、传输及销毁等；
k) 数据应用领域的规范性、合理性；
l) 数据应用风险评估与审计机制的建立。

8.7 数据安全管理专项审计

数据安全管理专项审计是指针对数据安全的管理开展专项审计，审计范围包括但不限于：

a) 数据安全管理目标、方针和策略；
b) 数据安全组织管理，包括组织架构、责任人、角色、职责和权限等；
c) 数据安全管理制度、流程；
d) 数据的分级分类和保护机制；
e) 数据标准与数据模型；
f) 数据安全事件管理；
g) 人力资源安全；
h) 安全教育和培训；
i) 物理安全；
j) 系统开发安全；
k) 网络安全；
l) 设备安全；
m) 操作系统安全；
n) 应用系统安全；
o) 数据生存周期的安全，包括数据的获取、处理、使用、存储、传输及销毁安全等；
p) 数据供方安全管理；
q) 数据安全风险评估与审计机制。

8.8 云数据管理专项审计

云数据管理专项审计是指针对云端数据的管理开展专项审计，审计范围包括但不限于：

a) 云数据管理目标、方针和策略；
b) 云数据组织管理，包括组织架构、责任人、角色、职责和权限等；
c) 云数据管理制度和流程；
d) 云数据标准与云数据模型；
e) 云数据的分级分类和保护机制；
f) 云数据的合规与隐私保护；
g) 云数据质量，包括数据完整性、准确性、有效性、合法性、一致性等；
h) 云数据生存周期，包括数据的获取、处理、使用、存储、传输及销毁等；
i) 云数据的安全管理；
j) 云数据应用领域的规范性、合理性；
k) 云数据风险评估与审计机制的建立。

8.9 数据合规管理专项审计

数据合规管理专项审计是指针对数据合规的管理开展专项审计，审计范围包括但不限于：

a) 数据合规纳入组织合规管理的情况；
b) 数据合规性管理目标、方针和策略；
c) 数据合规组织管理，包括组织架构、责任人、角色、职责和权限等；
d) 数据合规管理制度与流程；
e) 数据标准与数据模型的合规；
f) 数据边界相关的合规性；

g) 数据生存周期的合规性；
h) 数据合规风险评估与审计机制的建立。

8.10 数据治理绩效专项审计

数据治理绩效专项审计是指针对数据治理的绩效开展专项审计，审计范围包括但不限于：
a) 数据治理绩效管理目标、方针和策略；
b) 数据治理绩效组织管理，包括组织架构、责任人、角色、职责和权限等；
c) 数据治理绩效管理制度与流程；
d) 数据治理绩效考核指标体系；
e) 数据治理绩效考核步骤；
f) 奖励与惩罚措施；
g) 数据治理绩效考核；
h) 数据治理风险评估与审计机制的建立。

8.11 数据质量管理专项审计

数据质量管理专项审计是指针对数据质量的管理开展专项审计，审计范围包括但不限于：
a) 数据质量管理目标、方针和策略；
b) 数据质量组织管理，包括组织架构、责任人、角色、职责和权限等；
c) 数据质量管理制度与流程；
d) 数据质量管理的资源保障；
e) 数据生存周期的安全性、可靠性和有效性；
f) 数据的完整性、准确性、有效性、合法性、一致性等；
g) 数据产品及服务实现过程和结果的监视和测量；
h) 数据质量管理风险评估与审计机制的建立。

8.12 数据资产管理专项审计

数据资产管理专项审计是指针对数据资产的管理过程开展专项审计，审计范围包括但不限于：
a) 数据资产管理目标、方针和策略；
b) 数据资产管理规划；
c) 数据资产组织管理，包括组织架构、责任人、角色、职责和权限等；
d) 数据资产管理制度与流程；
e) 数据资产管理过程；
f) 数据资产评估；
g) 数据资产安全；
h) 数据资产管理内外部环境及技术资源保障等；
i) 数据资产管理风险评估与审计机制的建立。

9 数据审计流程

数据审计流程要求见GB/T 34960.4《信息技术服务 治理 第4部分：审计导则》。

10 数据审计系统

数据审计系统属于 GB/T 34960.4《信息技术服务 治理 第 4 部分：审计导则》中审计平台的一部分，是在审计中充分利用信息技术管理和支持完成相关数据审计工作的信息系统。组织宜使用数据审计系统并进行有效管理，包括但不限于：

a) 数据审计系统规模应与组织业务复杂程度、信息技术依赖程度等相匹配；
b) 数据审计系统组织管理，包括组织架构、责任人、角色、职责和权限等；
c) 数据审计系统管理制度与流程；
d) 数据审计系统建设，包括建设方式、立项、需求、设计、开发、测试、验收及上线等管理；
e) 数据审计系统应用，包括审计业务流程控制、审计模型管理、操作管理、网络与信息安全管理、审计数据生存周期管理、文档与审计数据管理等；
f) 数据审计系统运行，包括基础设施管理、网络与信息安全管理、事件管理及问题管理等。

11 数据审计报告

数据审计报告要求见 GB/T 34960.4《信息技术服务 治理 第 4 部分：审计导则》。

参 考 文 献

[1] GB/T 19001-2016 质量管理体系
[2] GB/T 26317-2010 公司治理风险管理指南
[3] GB/T 29264-2012 信息技术服务 分类与代码
[4] GB/T 20269-2006 信息安全技术 信息系统安全管理要求
[5] GB/T 20984-2007 信息安全技术 信息安全风险评估规范
[6] GB/T 22080-2016 信息技术 安全技术 信息安全管理体系 要求
[7] GB/T 22081-2016 信息技术 安全技术 信息安全控制实践指南
[8] GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求
[9] GB/T 20984-2007 信息安全技术 信息安全风险评估规范
[10] GB/T 20918-2007 信息技术 软件生存周期过程 风险管理
[11] GB/T 24353-2009 风险管理 原则与实施指南
[12] GB/T 24405.1-2009 信息技术 服务管理 第1部分：规范
[13] GB/T 27921-2011 风险管理 风险评估技术
[14] GB/T 31509-2015 信息安全技术 信息安全风险评估实施指南
[15] GB/T 33132-2016 信息安全技术 信息安全风险处理实施指南
[16] GB/T 34960.1-2017 信息技术服务 治理 第1部分：通用要求
[17] GB/T 34960.2-2017 信息技术服务 治理 第2部分：实施指南
[18] GB/T 34960.3-2017 信息技术服务 治理 第3部分：绩效评价
[19] GB/T 34960.4-2017 信息技术服务 治理 第4部分：审计导则
[20] GB/T 34960.1-2018 信息技术服务 治理 第5部分：数据治理
[21] GB/T 36073-2018 数据管理能力成熟度评估模型
[22] 全国人民代表大会常务委员会.中华人民共和国保守国家秘密法.[中华人民共和国主席令第二十八号].2010-04-29.
[23] 国务院.中华人民共和国保守国家秘密法实施条例.[中华人民共和国国务院令第646号].2014-01-17.
[24] 中华人民共和国财政部.企业内部控制基本规范.[财会〔2008〕7号].2008-05-22.
[25] 中华人民共和国财政部财会.企业内部控制审计指引. [财会〔2010〕11号].2010-04-15.
[26] 中国内部审计协会.内部审计基本准则.[公告2013年第1号]. 2013-08-20.
[27] 中国内部审计协会.内部审计具体准则第2203号——信息系统审计.[公告2013年第1号].2013-08-20.
[28 中华人民共和国审计署.信息系统审计指南——计算机审计实务公告第34号.[审计发〔2012〕11号].2012-02-01.
[29] 中华人民共和国审计署.审计署关于内部审计工作的规定.[审计署令第4号].2003-03-04.
[30] 中国银行业监督管理委员会.商业银行信息科技风险管理指引.[银监发〔2009〕19号].2009-06-01.
[31] 中国证券业协会和中国期货业协会.证券期货经营机构信息技术治理工作指引（试行）.[中证协发〔2008〕113号]. 2008-09-03.
[32] 中国保险监督管理委员会.保险公司信息系统安全管理指引（试行）.[保监发〔2011〕68号].2011-11-16.
[33] 中国银行保险监督管理委员会.银行业金融机构数据治理指引.[银保监发〔2018〕22

号].2018-5-21.

[34] 美国反虚假财务报告委员会下属发起组织委员会.网络时代的内部控制.COSO,2015-1.

[35] The Committee of Sponsoring Organizations of the Treadway Commission.Enterprise Risk Management Integrating With Strategy and Performance.COSO,2017