ICS 35.080

中华人民共和国国家标准

GB/T XXXXX—XXXX
代替 GB/T 34960.4-2017

信息技术服务 治理 第4部分：审计导则

Information technology service—Governance—Part 4: Audit guidance

（征求意见稿）

（本草案完成时间：2026-07-19）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX - XX - XX 发布　　XXXX - XX - XX 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

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。

本文件是GB/T 34960《信息技术服务 治理》的第4部分。GB/T 34960已经发布了以下部分：

——第1部分：通用要求；

——第2部分：实施指南；

——第3部分：绩效评价；

——第4部分：审计导则；

——第5部分：数据治理规范。

本文件代替GB/T 34960.4—2017《信息技术服务 治理 第4部分：审计导则》，与GB/T 34960.4—2017相比，除结构调整和编辑性改动外，主要技术变化如下：

a） 增加了“缩略语”一章（见第4章）；

b） 将“审计总则”更改为“通则”（见5，2017年版的4）、增加了审计概念及关系（见5.1）、将“审计与治理的关系”更改为“审计与治理”，并更改相关内容（见5.1.1，2017年版的4.1），增加了审计相关概念关系（见5.1.2），将“审计结构及其关系”更改为“审计体系结构”，并更改相关内容（见5.1.3，2017年版的4.2），增加了审计原则（见5.2），更改了“审计依据”的内容（见5.3，2017年版的4.3），合并了“审计方法”与“审计技术”，并更改相关内容（见5.4，2017年版的4.4、4.5），更改了“审计质量控制的内容”（见5.5，2017年版的4.6），删除了“审计业务类型”（2017年版的4.7），将“审计工作的执行”更改为“审计工作执行”，并更改相关内容（见5.6，2017年版的4.8）；

c） 增加了“审计治理框架”一章（见第六章）；

d） 将审计组织管理的“总则”修改为“概述”，并更改了相关内容（见7.1，2017年版的5.1）

e） 更改了“审计环境”的相关内容（见7.2，2017年版的5.2）；

f） 更改了“审计机构”的相关内容（见7.3，2017年版的5.3）；

g） 将“审计规章制度”更改为“审计规划与制度”，并更改相关内容（见7.4，2017年版的5.4）；

h） 增加了“审计协同体”（见第8章），并将2017年版的“审计人员”相关内容修改后纳入（见8.2，2017年版的6）；

i） 增加了“信息系统审计”一章，并将2017年版的相关内容修改后合并纳入（见第9章，2017年版的第7章、第8章、第9章、第10章）。

本文件由全国信息技术标准化技术委员会（SAC/TC 28）提出并归口。

本文件起草单位： 上海霞安信息科技有限公司、中国电子技术标准化研究院、上海谷航信息科技发展有限公司、北京国家会计学院、上海计算机软件技术开发中心、北京赛西科技业有限责任公司、上海市大数据中心、江苏意源科技有限公司、立信会计师事务所(特殊普通合伙)、上海市网络与信息安全应急管理事务中心、大连海事大学、上海北宙企业管理咨询有限公司、北京可利邦信息技术服务有限公司、赛迪研究院、广州赛西标准检测研究院有限公司、上海翰纬信息科技有限公司、中科软科

技股份有限公司、上海速邦信息科技有限公司、深圳久安会计师事务所（特殊普通合伙）、山东省科技咨询中心有限公司、北京德信永道信息技术服务有限公司、苏州市软件评测中心有限公司、北京久其软件股份有限公司、西安炎黄信息系统咨询有限公司、东北大学、人保信息科技有限公司、国联民生证券股份有限公司、天津天大康博科技有限公司、北京亿百维信息科技有限公司、上海市卫生健康委员会、神州数码系统集成服务有限公司、中金云链（武汉）数字科技有限公司、上海海事大学、深圳云塔信息技术有限公司、中国电子工程设计院股份有限公司、北京赛迪认证中心有限公司、上海申康医院发展中心、广州赛宝认证中心服务有限公司、北京时代鼎典工程咨询有限公司、中电信数智科技有限公司、中国太平洋保险（集团）股份有限公司、杭州平勤信息工程咨询有限公司、湖北恒普科技有限公司、广州赛宝联睿信息科技有限公司、申万宏源证券有限公司、万达信息股份有限公司、南京南审审计大数据研究院有限公司、百信信息技术有限公司、北京信息科技大学、护航科技股份有限公司、上海市城市数字化转型应用促进中心（上海市智慧城市建设促进中心）、南京审计大学、上海海勃数科技术有限公司、北京金山办公软件股份有限公司、上海华谊集团股份有限公司、金税信息技术服务股份有限公司、浙江省烟草专卖局、上海银行股份有限公司。

本文件主要起草人：俞文平、叶康涛、郭鑫伟、施勇、宋俊典、张明英、杨琳、聂兴凯、肖筱华、谢东良、吴恩平、徐国平、薛冰玢、尹正茹、钱伟峰、王晓钊、黄胜华、张涵、米登科、陈宏峰、魏锦华、高敏、王文丹、樊铁成、郑晨光、许斯妤、李世喆、李康、许志国、王珊珊、杨泉、刘俊、史瑞超、孟彦飞、杨舸、徐建有、陈志刚、章达隆、方健、吴哲锐、王庆磊、冯骏、杨飞玉、徐飞、吴慧韫、孙军、俞丽平、王春涛、陈昌杰、马烈、刘辰昀、孙勉、夏寒、刘颋、陈艳、曹晖、徐紫荆、李洪源、刘亚东、刘随江、高峰、张素勤、马白云、严新开、黄建新、曹智华、侯秀琳、吴小平、齐本铁、左林、金春华、郭长水、于浩、魏喜燕、钱钢、孙金余、应俊、马莉、赵侍嶂、李昊然、熊健淞、毛静芳、张一民、李俊斌、罗喆帅。

本文件及其所代替的文件的历次版本发布情况为：

——本文件于 2017 年首次发布；

——本次为第一次修订。

引　言

随着新兴技术发展，以及新模式、数智化转型及数据要素化等环境的变化，组织对信息技术依赖性持续加深，面临的风险不断增大。为有效控制风险，满足“治理主体应对信息技术治理的执行过程与成效实施全过程监督，建立常态化跟踪核查、动态指标监控、偏差预警问责、定期审计验证及结果闭环回流机制”的要求，需要通过信息技术全面赋能审计领域，并纳入信息技术治理范畴进行统一管控，以保障审计工作质量与成效，为数智化转型提供监督保障与治理支撑，促进组织目标达成。另外，审计领域信息技术治理作为信息技术审计的基础与能力底座，是智能化、复杂化环境下保障审计质量与效率的必要前提；信息技术审计所揭示的问题与建议，亦为信息技术治理提供客观依据与改进动力。信息技术治理与审计之间形成的“治理引领审计，审计反哺治理”良性闭环，支撑数智化转型规范有序发展。

GB/T 34960《信息技术服务 治理》由五部分构成。

——第 1 部分：通用要求。目的在于提出信息技术治理的通用要求，明确信息技术治理的原则、模型、过程和要素等，指导组织信息技术治理体系的建立、评价和改进。

——第 2 部分：实施指南。目的是为组织信息技术治理的实施提供指导，分析实施治理的环境因素，规定治理的实施框架、实施环境和实施过程，指导顶层设计、管理体系和资源治理的实施。

——第 3 部分：绩效评价。目的在于指导组织建立信息技术治理的绩效评价模型，明确绩效评价方法和评价指标的建立程序，使组织能够定量或定性地评价信息技术及其应用的绩效。

——第 4 部分：审计导则。目的在于指导组织建立信息技术审计体系，加强审计领域信息技术应用的治理，规范信息系统审计，以完成组织的信息技术治理目标。

——第 5 部分：数据治理规范。目的是为各类组织提供数据治理框架，指导组织进行数据治理的顶层设计，对治理域中的数据管理体系、数据价值体系进行治理，并对数据治理过程进行规范。

GB/T 34960.4—2017 发布实施已近十年，与信息技术治理与审计有关的理论研究和实践以及国家标准都发生了变化。首先，信息技术治理原理与方法研究不断深入,逐步建立起以治理要素为基础、治理域为载体，依托治理阶段和治理活动驱动闭环，构建组织治理的实施方法，这将影响作为组织治理域之一的审计领域。其次,随着信息技术审计实践的逐渐深入以及新技术的广泛应用,新的审计需求不断产生。鉴于此,确有必要修订完善 GB/T 34960.4-2017，以不断适应国内外相关标准的新变化以及信息技术服务治理与审计实践发展的新需求,确保支撑信息技术服务治理与审计工作的国家标准体系整体协调。

本次对 GB/T 34960.4—2017 的修订，紧扣信息技术治理审计领域从“传统信息技术审计”向“支撑数字化转型治理审计”演进的发展趋势。在充分吸收国内外最新成果的基础上，聚焦数字化转型、数据要素化及人工智能治理等核心审计方向，构建覆盖审计通则、审计治理框架、审计组织管理、审计协同体及信息系统审计五大维度的审计体系。标准既对标国际前沿审计治理方向，又突出数智时代对“防范化解信息技术风险、规范支撑审计数智应用”的现实需求，有效引导信息技术全面赋能审计领域及与信息系统审计的深度融合，通过高质量审计监督实现高水平治理与高质量数智化发展。

信息技术服务 治理 第4部分：审计导则

1 范围

本文件确立了审计通则，提供了审计治理框架、审计组织管理、审计协同体及信息系统审计等的指南。

本文件适用于组织治理主体建立或完善组织信息技术审计体系，规范审计领域信息技术治理，实施信息技术审计的监督职能；也可指导第三方机构建立信息技术审计体系并规范信息技术审计业务的开展。

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 34960.1 信息技术服务 治理 第1部分：通用要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

信息系统审计 information system audit

对信息系统及其相关的信息技术内部控制等进行审查与评价,并发表审计意见的活动。

注：信息技术内部控制包括信息技术组织层面控制、信息技术一般控制及信息技术应用控制。

3.2

信息技术内部控制 information technology internal control

由组织治理主体和全体员工实施的、旨在完成信息技术控制目标的过程。

3.3

信息技术组织层面控制 information technology organization control

在组织层面建立并实施的信息技术相关控制。

3.4

信息技术组织层面控制审计 information technology organization control audit

对组织层面信息技术相关控制开展的审计。

3.5

信息技术一般控制 information technology general control

作用于整个信息系统以及外部各种环境要素，并对所有应用或控制模块具有普遍影响的控制。

3.6

信息技术一般控制审计 information technology general control audit

对信息技术一般控制开展的审计。

3.7

信息技术应用控制 information technology application control

在业务流程层面为合理保证应用系统准确、完整、及时地完成业务数据的生成、记录、处理、报告等功能，而设计、执行的信息技术控制。

3.8

信息技术应用控制审计 information technology application control audit

对信息技术应用控制开展的审计。

3.9

人机协同 human-machine collaboration

为了共同完成目标，人与智能系统、算法工具等基于明确的职责界定、任务分工与交互规则，相互协作、优势互补及动态进化，实施以人为决策主体、机器为辅助支撑的工作模式。

3.10

人机协同审计 human-machine collaborative audit

在审计活动中，为了共同完成审计目标，审计人员与智能系统、算法工具等基于明确的职责界定、任务分工与交互规则，相互协作、优势互补及动态进化，实施以人为决策主体、机器为辅助支撑审计的工作模式。

3.11

审计工具 audit tools

为完成审计工作、实现审计目标，所使用的软硬件系统、方法技术、作业载体及辅助手段等的统称。

3.12

审计数字员工 audit digital employee

拥有身份标识，在授权范围内，基于规则、模型、流程和数据执行特定审计任务的智能工具或其组合等，相关工作和成果可控制、可追溯。

3.13

审计协同体 audit collaboration entity

为完成审计任务，以审计人员为主导、审计数字员工为辅助支撑的人机协同审计主体。

3.14

审计治理要素 audit governance element

实施审计领域信息技术治理时，需关注的核心治理对象与关键过程。

3.15

审计治理域 audit governance domain

在审计领域按照特定层次、功能划分的信息技术治理范围，是审计治理要素的集合。

3.16

信息技术审计机构 information technology audit Institution

独立承担信息系统审计及运用信息技术开展审计的职能部门或机构。

3.17

审计大模型 audit large model

基于通用大模型基座，结合审计领域知识图谱，用海量审计专业数据，通过深度训练、微调，具备审计专属理解、推理、取证、质控及报告生成能力等面向审计全流程的垂直行业大模型。

4 缩略语

下列缩略语适用于本文件。

AI：人工智能（Artificial Intelligence）

API：应用程序编程接口（Application Programming Interface）

BCMS：业务连续性管理体系（Business Continuity Management System）

CAATs：计算机辅助审计技术（Computer-Assisted Audit Techniques）

DevOps：开发运维一体化（Development and Operations）

ETL：抽取-转换-加载（Extract-Transform-Load）

GRC：治理、风险与合规（Governance,Risk and Compliance）

IT：信息技术（Information Technology）

KGI：关键目标指标（Key Goal Indicator）

KPI：关键绩效指标（Key Performance Indicator）

MLOps：机器学习运维（Machine Learning Operations）

NLP：自然语言处理（Natural Language Processing）

OCR：光学字符识别（Optical Character Recognition）

RPA：机器人流程自动化（Robot Process Automation）

SHAP：沙普利加性解释（SHapley Additive exPlanations）

5 通则

5.1 审计概念及关系

5.1.1 审计与治理

审计与治理关系如下：

a） 从治理视角分析，依据 GB/T 34960.1 规定的“信息技术治理核心任务为评估、指导与监督”，其中监督职能的落地执行与审计密切相关。为了满足“治理主体应对信息技术治理的执行过程与成效实施全过程监督，建立常态化跟踪核查、动态指标监控、偏差预警问责、定期审计验证及结果闭环回流机制”的要求，需要通过 IT 全面赋能审计领域，并纳入 IT 治理范畴进行统一管控（简称审计领域 IT 治理），以保障审计工作质量与成效，为数智化转型提供监督保障与治理支撑，促进组织目标达成；

b） 从审计视角分析，审计领域 IT 治理是信息系统审计的基础与能力底座，是在智能化、复杂化环境下开展审计的必要前提条件，并为审计自身的数智化转型提供系统性支撑；同时，信息系统审计所揭示的问题、风险与改进建议，亦为组织 IT 治理（包括审计领域）的规范化、有序化发展提供客观依据与持续改进动力，形成“治理引领审计，审计反哺治理”的良性闭环，支撑数智化转型规范有序发展。

5.1.2 审计相关概念关系

审计领域 IT 相关概念主要包括信息系统审计、审计领域 IT 治理、审计信息化、审计数字化转型、审计数智化转型等，相互关系如下：

a） 审计信息化、审计数字化与审计数智化是审计技术能力演进的三个阶段，后者以前者为基础，呈现螺旋上升态势；

b） 审计领域 IT 治理是贯穿上述三个阶段的方法论与实践，旨在运用 IT 赋能审计自身的能力建设，为审计数智化转型等提供支撑；而转型成果反向支撑运用 IT 审计的深化；

c） 信息系统审计既是 IT 治理监督活动的具体体现，也有利于审计领域 IT 治理，二者共同构成“IT 赋能审计，审计规范 IT”的双向支撑与制约关系。

5.1.3 审计体系结构

审计领域 IT 治理与信息系统审计统称为 IT 审计。IT 审计体系是由战略引领、组织保障、执行协同、方法技术支撑及质量控制等多维度构成的有机整体。该体系以审计战略为顶层引领，以审计组织管理体系为运行基础，以审计协同体为执行主体，在审计依据、方法与技术的规范指导下，通过标准化审计执行流程，严格遵循审计质量控制标准，系统开展审计领域 IT 治理与信息系统审计两类核心活动，最终完成对组织信息技术治理的有效监督与审计领域的 IT 价值转化。

5.2 审计原则

IT 审计原则包括但不限于：

a） 独立性，包括 IT 审计机构在组织治理架构中保持实质与形式的独立，确保审计范围、资源配置及执行过程不受干预，为治理层提供无偏见的监督评价；

b） 客观性，包括 IT 审计人员秉持职业审慎，以事实为依据作出专业判断，且在利用数字员工及智能工具时，其审计结论的最终责任不可转移，始终由审计人员承担；

c） 公正性，包括审计全过程不存在影响职业判断的利益冲突，通过机构独立与人员自律协同构建可信的 IT 审计体系，维护治理监督的公允性；

d） 透明与可追溯性，包括在智能化审计环境中，确保数字员工的算法逻辑透明、决策路径可解释、审计轨迹完整可追溯，满足 IT 治理对问责与合规的要求。

5.3 审计依据

开展 IT 审计工作应遵循或参考的依据包括但不限于：

a） 国家相关法律、行政法规及部门规章；

b） 行业监管机构发布的合规要求与技术指引；

c） 国家标准及行业标准；

d） 组织内部的章程、政策、制度、标准、合同及协议等；

e） 国际通用的标准、框架与最佳实践。

注：IT 审计机构宜建立并维护审计依据库，保持其时效性与完整性。

5.4 审计方法与技术

IT 审计方法与技术包括但不限于：

a） 审计方法，如访谈法、调查法、检查法、观察法、测试法、验证法、分析性复核法等，以及相关方法的智能化升级（如访谈升级为智能访谈、调查法升级为大数据调查、检查法升级为自动化检查等）；

b） 审计技术，如风险评估技术、审计抽样技术、CAATs、大数据技术、云计算技术、区块链技术、机器人流程自动化、可视化技术，以及相关技术的智能化升级（如 CAATs 升级为智能辅助审计技术、区块链技术升级为智能合约验证技术等）和融合创新技术（如预测性风控技术、语义核查技术等）；
c） 审计方法与技术融合创新，如数据驱动型方法（如依托大数据分析与实时日志审计实现全量、动态监控等）、AI 赋能型方法（如运用机器学习识别异常等）、可信验证型方法（如结合区块链存证审计轨迹等）、人机协同型方法（如以可解释 AI 支持审计判断）等。

5.5 审计质量控制

审计质量控制管理包括但不限于：
a） 创造并维持独立的审计环境；
b） 明确审计质量管理职责与分工；
c） 制定审计审计质量管理制度；
d） 建立复合型审计人才培养机制；
e） 定期开展审计人员工作质量的自我检查与评估；
f） 定期开展对审计数字员工作质量的检查与评估；
g） 适时开展审计机构工作质量的内部监督与检查；
h） 开展内部审计机构工作质量的外部检查；
i） 建立持续优化与改进机制。

5.6 审计工作执行

审计工作执行包括但不限于：
a） 基于风险导向制定审计计划，明确审计目标、范围与资源；
b） 在人机协同审计中，需预先明确任务分工、交互规则与复核节点；
c） 对审计人员及人机协同进行指导，合理保证其审计目标的达成，并且符合审计标准；
d） 审计人员在从事审计工作时，获得充分、可靠和相关的证据以完成审计目标；
e） 审计发现和审计结论能被相关证据所支持；
f） 持续审计环境下进行全量取证与异常穿透、全流程数字化记录，并进行动态风险监测与应对；
g） 审计程序以书面或电子形式记录，其中包含能解释审计发现和审计结论的工作细节和审计证
h） 据；
i） 审计人员在审计过程中需考虑被审计单位违规和非法行为；
j） 评估审计工作透明度、问责性和结果可靠性。

6 审计治理框架

6.1 概述

审计治理指审计领域信息技术治理，是审计主体开展信息系统审计的基础和能力底座。审计治理框架面向审计数字化转型与数智化演进，以审计平台、审计工具、审计数据及智能审计应用等为载体，贯穿审计作业（见 9.4.3、9.5.2）、管理与决策全层级，宜聚焦价值交付、风险可控、资源优化与有效监督，遵从组织 IT 治理的相关要求，保持审计独立性，并与组织业务战略对齐。

6.2 顶层设计

6.2.1 战略规划

审计领域 IT 战略规划包括但不限于：

a） 纳入组织 IT 战略规划，并与业务战略规划保持一致；
b） 分析审计领域的特点、内外部环境及促成因素，调研并评估审计领域的现状和特点；
c） 识别组织的战略类型、风险偏好、角色定位及合规要求等，明确治理的重点；
d） 指导管理体系的建立，并明确相关的治理要素；
e） 明确内控、安全、合规及伦理等相关要求，对风险进行管控；将审计领域相关的 KPI 和 KGI 纳入战略规划中；
f） 监督和评价战略规划的制定与实施，并定期审视和调整战略规划的适配性，对其进行持续改进和优化。

6.2.2 组织构建

审计领域 IT 组织构建包括但不限于：

a） 建立与业务部门、风险管理等部门的联动机制；
b） 建立支撑战略的组织机制，明确相关的实施原则和策略；
c） 明确决策、实施与监督机构，建立责权利一致的组织架构，明确管理者和成员角色；
d） 建立决策、授权和沟通机制，使利益相关方理解并接受相应的职责和权利；
e） 行使决策、执行、控制和监督等职能，评估绩效并持续改进和优化。

6.2.3 架构设计

审计领域 IT 架构设计包括但不限于：

a） 设计符合战略和组织需求的架构体系，针对相关风险（如技术方向、管理策略和支撑体系等）提出管控要求；
b） 宜考虑与业务、风险领域架构的联动与控制、技术能力、国产化软硬件适配、信创环境及资源等；
c） 监督和评价架构的设计、实施及应用成效，并持续改进和优化；
d） 监控和评价架构管理机制的运行及成效，并持续改进和优化。

6.3 治理环境

6.3.1 内外部环境

影响审计领域 IT 战略规划与实施的内外部环境因素包括但不限于

a） 现行法律、法规、规章等合规要求；
b） 组织战略与业务发展目标的变化；
c） 组织内部全面风险管控机制；

注 1：风险管控机制涵盖风险识别、评估、应对、监控与报告的制度与程序，其健全程度决定了 IT 审计的定位、重点与资源投向。

d） 内外部审计、监督检查与评估等结果；
e） 审计供应链生态；

注 2：IT 审计实施过程中，由内部审计团队、外部审计机构、第三方咨询与评估机构、审计工具或平台供应商、数据服务商等内外部实体构成的相互依赖、协同作业的产业生态，其稳定性、数据交互的安全性、服务提供

的连续性以及各主体间的权责边界，直接影响 IT 审计资源的配置效率与审计质量。审计供应链生态亦是 IT 审计需评估的供应链风险来源。

f） 新技术的应用；

g） 新兴技术演进与 IT 应用创新发展趋势。

6.3.2 促成因素

促成审计领域 IT 战略规划有效实施的要素包括但不限于：

a） 战略与价值导向，包括组织战略规划和业务发展的要求，及成本优化与价值创造要求等；

b） 治理与文化协同，包括治理主体的重视程度、治理框架优化的要求，及企业文化、愿景与价值观的一致性要求等；

c） 风险与相关方平衡，包括风险管控要求，及利益相关方诉求及其优先级；IT 审计宜聚焦核心风险领域，平衡并响应董事会、管理层、监管机构等不同利益相关方的期望，合理配置审计资源等；

d） 技术与创新驱动，包括技术变革与创新驱动，及新技术应用容错机制；新兴技术推动审计模式演进，组织宜建立对创新试错的包容机制，开展审计数智化转型与工具方法创新等待；

e） 数智化资源底座，包括高质量语料库，及可复用算法与大模型（含审计大模型）资源；构筑支撑智能审计的数智底座，形成专业数据集与模型资产的沉淀与复用能力等；

f） 复合型人才保障，包括复合型审计人才管理机制；建立涵盖引进、培养、评价与激励的制度保障，构建具备业务、IT 与数据融合的综合素养审计团队等。

6.4 治理域

6.4.1 概述

审计领域 IT 治理域是为实现有效 IT 治理划分的逻辑领域，宜集中治理、明确所有权与规则的逻辑边界或领域。用于界定审计领域 IT 治理范围、明确责任主体、统一管控规则，是治理体系的核心架构单元。其中，审计领域数据治理指审计领域数据资源形成及其应用过程中相关管控活动、绩效和风险管理等的集合；人机协同审计治理指组织治理层对审计的战略、数据治理、算法合规与人机权责界定等进行系统性重构，并嵌入审计领域 IT 治理全过程。

6.4.2 管理体系、资源与创新管理

组织宜将审计管理体系、审计资源管理及审计创新管理纳入治理范围，内容包括但不限于：

a） 审计管理体系，覆盖安全、伦理、数据、应用、合规、风险及项目等 IT 管控机制；

b） 审计资源管理，统筹基础设施、应用、数据、算法、模型及资金等 IT 资源的配置、使用及管控；

c） 审计创新管理，明确审计创新目标、权责与流程，推进审计管理、方法与技术及应用等创新，建立分级容错与风险缓释机制等。

6.4.3 数据治理

审计领域数据治理宜以该领域 IT 治理为基础，内容包括但不限于：

a） 数据战略规划，包括明确审计数据治理的目标与原则，将审计数据战略规划纳入组织 IT 规划与数据整体战略规划，保持审计数据的完整性、可用性、保密性与合规性；

b） 数据组织构建，包括明确数据组织架构、职责与分工，确定数据管理相关的授权、决策和沟通机制，实施数据管理决策、执行、控制和监督职能，评估数据治理绩效并持续改进优化；

c） 数据架构，包括审计数据源的识别与整合（如业务系统数据、日志数据、操作数据、外部监管数据等）、审计数据模型的统一设计、审计数据湖或数据仓库的规划与建设及数据血缘与元数据管理；

d） 数据生存周期管理，包括审计数据的采集、清洗、转换、存储、使用、归档及销毁等全流程管控，明确各环节的数据质量标准与安全控制措施；

e） 数据质量管理，包括建立审计数据质量评价维度（如准确性、完整性、一致性、及时性、唯一性等），实施数据质量检核与监控，建立数据质量问题发现、报告、追溯与改进的闭环机制；

注：审计数据质量评价宜与信息系统审计相结合，二者互为支撑、交叉验证，后者是前者的基础，对信息系统层面数据形成全过程控制进行审核并评价；前者反向校验信息系统控制有效性。

f） 数据安全管理，包括审计数据访问控制与权限管理、数据脱敏与匿名化处理、数据加密与传输安全、数据备份与恢复、数据使用审计与日志记录、数据跨境传输合规审查；

g） 数据合规管理，包括遵循法律法规的要求，对审计过程中涉及的重要数据、个人信息进行保护，建立数据主体权利响应机制（如查阅、更正、删除等），定期开展数据合规性自评与审计；

h） 数据共享与交换，包括审计数据与业务数据、财务数据、风险数据等的共享机制，明确数据共享的权限与审批流程，建立数据交换接口的安全控制与监控机制，确保数据在共享过程中的完整性与保密性。

6.4.4 人机协同审计治理

人机协同审计治理宜以审计领域 IT 治理为基础，内容包括但不限于：

a） 战略一致，如将人机协同审计能力建设纳入组织 IT 治理战略与审计发展规划，明确审计智能化目标与组织业务目标的一致关系；

b） 权责划分，如明确以人主导、审计数字员工为辅助支撑的协同机制，将人机权责界定纳入组织治理章程，明确审计委员会、IT 治理委员会、数据管理部门及审计部门在人机协同中的职责边界；

c） 架构设计，如覆盖数据采集、模型运行、人工复核、结论输出的端到端协同架构，明确各环节中人工节点与智能节点的定位及衔接规则；

d） 制定管理制度，如权责管理、合规管理、数据治理、算法管理及知识管理等；

e） 明确管理流程，如协同实施流程、模型验证实施流程、人机交互实施流程（见 9.4.3）、持续优化实施流程及变更管理实施流程等；

f） 确定支撑要素，如部门协同、专业能力、工具应用、算法透明、模型可解释性、AI 伦理审查、数据隐私保护、技术韧性、风险管控及审计与评估等；

g） 建立成熟度模型，如划分从“工具辅助”到“治理协同”的演进等级，指导分阶段建设等。

6.5 治理要素

6.5.1 概述

审计领域 IT 治理要素是指开展治理工作时需要关注的核心对象与关键过程，主要通过制度、流程、数据、平台、工具、人才、模型、数字员工等治理要素落实治理域的执行效果。IT 治理要素在审计体系中构成“规范层、资产层、主体层”的协同关系，制度与流程构成规范层，制度确立方向策略与授权责任的静态规则，流程实现其动态流转与管控落地；数据、模型、平台、工具与数字员工构成

资产层，在规范约束和权责管控下将信息资源转化为可复用的生产要素，价值沉淀；人才构成主体层，主导规范制定与业务运营，实现人机协同和价值创造。

6.5.2 治理要素构成

审计领域 IT 治理要素包括但不限于：

a） 制度，包括统筹管理办法、专项管理制度及操作执行规范等；
b） 流程，包括审计计划、作业实施、审计报告、整改跟踪及档案管理等；
c） 数据，包括数据采集与整合、数据治理与标准、数据清洗、脱敏与质量校验、数据安全与权限、数据血缘与溯源；
d） 平台，包括平台的规划、建设、部署、运维及退役；
e） 工具，包括工具管理（如准入、部署、应用、工具间协同集成、运维、迭代、安全及退役）、工具应用（如审计作业自动化、数据采集与分析、查证工具集成及质量控制与权限管理等）；
f） 人才，包括选拔、培养、考核、激励及晋升等；
g） 模型，包括模型规划、设计、开发、训练、验证、部署、监控、迭代及退役等生存周期管理；
h） AI 供应链治理要求，包括外部模型来源审查、数据来源审查、第三方服务依赖管理、开源组件风险识别和供应商责任边界；
i） 数字员工（详见 8.3）。

6.6 治理过程

审计领域 IT 治理过程包括但不限于：

a） 统筹和规划，包括制定审计领域 IT 战略规划、IT 组织规划、IT 架构规划及相关管理体系等；
b） 构建和运行，包括审计平台与工具构建、审计流程与制度固化、审计人员与审计数字员工部署、系统试运行与优化等；
c） 监控和评价，包括全维度审计监测体系搭建、多维度评价体系构建、评价成果输出等；
d） 改进和优化，包括审计问题整改与闭环管理、体系持续优化与迭代及建立长效机制等。

7 审计组织管理

7.1 概述

审计组织管理是指对 IT 审计机构的设置和运行进行管理，包括审计环境、审计机构、审计制度等。

7.2 审计环境

信息系统审计开展的必要环境包括但不限于：

a） 治理主体树立数智化转型下的审计管理理念，转变审计管理思路；
b） 推进信息系统审计与审计领域 IT 治理的双向联动，为审计数智化转型提供支撑；
c） 将人工智能技术的审计应用纳入组织伦理审查范畴；
d） 明确治理主体的 IT 审计职责；
e） 审查批准 IT 审计战略规划，使其与组织的 IT 战略规划、业务战略规划保持一致；

f） 建立与组织信息化规模相适应的审计机构，予以授权并明确由其向治理主体报告；
g） 指派具有专业胜任能力的人员担任审计机构负责人；
h） 构建融合审计、IT、业务与 AI 等多领域知识与技能的复合型人才团队；
i） 审计机构开展独立有效信息系统审计业务，对审计报告进行确认并落实整改；
j） 规范职业道德行为，增强 IT 审计文化建设，提高员工对 IT 审计重要性的认识；
k） 加强 IT 审计专业队伍建设，建立人机协作审计机制与人才激励机制；
l） 提供 IT 审计工作所需资金、设施设备及数据资源等；
m） 员工遵守经批准的 IT 审计规章管理制度、准则及流程，并安排相关培训；
n） 建立审计协同体的组织保障机制，明确数字员工部署、运行及退役的管理责职，保障所需的算力、算法、模型及语料等专项资源；
o） 建立审计机构与内控、风险及业务部门等协作机制；
p） 建立审计机构与外部组织的协作机制。

7.3 审计机构

IT 审计机构的职责和权力包括但不限于：

a） 拟定 IT 审计章程、相关制度、准则及流程等并报批；
b） 拟定 IT 审计中长期规划并报批；
c） 明确信息系统审计、审计领域 IT 治理的职责分工；
d） 编制 IT 审计年度计划、预算及人力资源计划并报批；
e） 制定 IT 审计手册、规程及指南等；
f） 按照 IT 审计规章制度、计划等要求开展相关业务，并保证审计质量；
g） 承担对 IT 控制设计和执行有效性评估的责任；
h） 能直接与治理主体进行沟通及汇报；
i） 做好与组织内、外相关机构和人员的沟通协调工作；
j） 有权参加或者列席组织 IT 治理及管理的重要会议；
k） 有权进行现场实物勘查，或者就与审计事项有关的问题对有关机构和个人进行调查、质询和取证；
l） 组织开展审计协同体能力建设，审批数字员工部署方案与审计大模型选型方案，明确人机协同模式下的责任分工与质量控制要求；
m） 定期评估审计大模型的运行效果与合规性，组织开展数字员工工作质量检查，确保算法可解释性、可追溯且输出可靠；
n） 定期对审计专业人员的知识、技能和培训情况进行评估，以使 IT 审计专业人员的专业知识和技能足以完成审计工作；
o） 每年至少一次确认本部门在组织中的独立性，若审计过程中审计范围受到限制影响审计目标和计划的实现，需就范围受到的限制及其潜在影响与治理主体进行沟通；
p） 向治理主体提出提高 IT 绩效的改进意见和建议；
q） 对审计发现的违反 IT 法律、法规等规定或者内部管理制度行为予以制止，并对相关机构和人员提出责任追究或者处罚建议。

7.4 审计规划与制度

IT 审计规划与制度包括但不限于：

a） 审计规划，包括制定独立的 IT 审计中长期规划及年度计划，明确制定 IT 审计的发展目标、组织建设、人才培养、制度与作业体系建设、财务预算、信息系统建设、审计项目统筹安排等内容；
b） 审计章程，包括审计目标、审计机构的职责和权力、角色与职责，审计范围、标准、审计报告上报路径、独立性与追责机制、与其他部门及第三方审计关系等；
c） 具体制度，包括审计相关的质量、项目、人员、过程、平台与信息，以及信息安全、AI 伦理审核、数字员工管理、审计大模型使用管理、人机协同审计等方面的要求；
d） 流程与操作规程，包括审计的流程、准则与指南、作业操作规程、工作手册等；
e） 审计信息系统管理规范，包括审计数据平台、审计管理平台、审计作业平台、审计查证分析平台、AI 审计专用平台及人机协同审计平台等规范。

8 审计协同体

8.1 概述

审计协同体是为完成审计任务，以审计人员为主导、审计数字员工为辅助支撑的人机协同审计主体，通过协同工作提高整体工作效率。审计人员主导审计全流程，负责审计方案制定、风险研判、专业判断、问题定性、结论审定等核心决策与创造性工作，把控审计质量与方向，并对审计结果承担最终责任。审计数字员工作为智能化辅助工具，依托算法与数据能力，承担数据筛查、流程复刻、重复核算、台账整理等机械、标准化、重复性基础工作。

8.2 审计人员

IT 审计人员宜具备与其工作相适应的职业道德、专业知识、资质、技能等，内容包括但不限于：
a） 职业道德，包括在执业过程中保持独立、客观、公正，正确履行审计职责、遵守职业审计标准及 AI 伦理准则，坚守人为最终责任主体原则，规范审计数据及 AI 应用行为，尊重数据主权、权属与隐私保护，对审计业务中获取的信息负有保密责任；
b） 知识、技能、资格与经验，包括掌握审计、财务及管理等通用知识，以及 IT、数据资产等专业技能；具备与岗位相适应的 IT 审计专业资质与经验；
c） 专业胜任能力，包括具备 IT 审计及 AI 治理审计的专业胜任能力与相应资质；定期参加后续教育，具备在人机协同环境中进行职业判断、复核与决策的综合能力，以及指导、监督数字员工开展审计作业的管理能力；
d） 利用外部专家服务，包括对外部专家的专业资格、经验、独立性、客观性，以及专业胜任能力及人机协同适配性进行评价，与外部专家签订书面服务协议，对其服务结果及数字员工输出进行复核、评价和综合利用，建立外部专家与内部审计人员、数字员工的协同工作机制。

8.3 审计数字员工

审计数字员工宜明确责任归属、任务分工、运行规则与伦理约束及生存周期管理等，内容包括但不限于：
a） 责任归属,包括审计数字员工为辅助工具，输出结果责任由相应的审计人员承担等；
b） 角色分工与协调，包括设置数据采集与清洗专员、持续监控与预警哨兵、自动化测试工程师、智能分析辅助员、审计大模型调度专员、算法合规审计人员及流程自动化助理等角色，并对多个数字员工之间的工作进行协调；

c） 运行规则与伦理约束，包括严格遵循“人在回路”原则，关键环节保留人工介入点；每个数字员工部署时应明确其可处理的审计任务类型、不可逾越的决策红线；遵守数据安全与隐私保护规定，不得超越授权访问或处理敏感数据；保持算法逻辑的透明性与可解释性等；

d） 生存周期与安全控制，包括建立准入、运行与退役机制，新部署需测试验证，退役时确保数据和日志妥善归档；定期评估任务完成质量、效率、准确率等效能，模型版本管理及定期重评估，访问权限遵循最小必要原则；输入数据需来源可信验证和完整性校验，输出结果嵌入人工抽查复核，重大风险领域100%复核，操作日志不可篡改，保留年限不低于审计档案要求；异常时自动熔断并告警，推动上下文至审计人员，同时暂停自动化作业等；

e） 监测与绩效管理，如建立效能评价指标体系，实施动态的运行监测，建立异常熔断机制等。

注1：人在回路指异常数据强制人工复核阈值规则。

注2：部署审计数字员工前，由审计机构负责人批准，并完成算法合规性、数据安全性及伦理影响等评估。

9 信息系统审计

9.1 审计业务类型

信息系统审计业务类型分为内部控制类审计（如IT内部控制审计、数据治理内部控制审计、IT安全内部控制审计）和专项类审计。IT内部控制审计是为了综合评价组织IT控制目标完成过程而进行的审计；数据治理内部控制审计是为了综合评价组织数据治理控制目标完成过程而进行的审计；IT安全内部控制审计是为了综合评价组织IT安全控制目标完成过程而进行的审计；IT专项类审计是组织根据外部要求及内部特殊需要而进行的审计。信息系统审计即可作为独立的审计项目实施，又可作为综合性审计项目的组成部分组织实施。

当信息系统审计作为综合性审计项目的组成部分时，IT审计人员宜在计划阶段统筹考虑整体审计目标与要求；在实施过程中及时与相关审计人员沟通审计发现，并据此动态调整其他相关审计的范围、时间及性质。

IT审计人员宜以风险导向为基础开展信息系统审计，风险评估贯穿于信息系统审计的全过程。

注：根据项目所处的生存周期阶段，可合理调整审计重点、方法和报告形式，实现“事前预防、事中控制、事后评价”的全流程覆盖。

9.2 内部控制类审计

9.2.1 IT内部控制审计

IT内部控制审计范围（见附录A）包括：

a） 组织控制审计，包括控制环境、风险评估、控制活动、信息与沟通及内部监督；

b） 一般控制审计，包括通用要求、IT采购管理、系统全生命周期管理、DevOps管理、网络安全管理及其他相关IT控制管理；

c） 应用控制审计，包括通用要求、应用组织管理、业务流程设计、数据输入、处理及输出、系统接口与信息共享及数据质量。

9.2.2 数据治理内部控制审计

数据治理内部控制审计范围（见附录A）包括：

a） 组织控制审计，包括控制环境、风险评估、控制活动、信息与沟通及内部监督；

b） 一般控制审计，包括通用要求、采购管理、项目整体管理，数据治理信息系统的开发、交付、运营管理，以及其他相关控制；
c） 应用控制审计，包括通用要求、数据治理信息系统应用组织管理、数据流程设计、数据采集、处理及输出、系统接口与信息共享，以及数据质量。

9.2.3 安全治理内部控制审计

IT 安全治理内部控制审计范围（见附录 A）包括：
a） 组织安全控制审计，包括控制环境、风险评估、控制活动、信息与沟通及内部监督；
b） 一般安全控制审计，包括总体安全管理（含网络运行安全、网络信息安全、监测预警与应急处置、信息系统建设与运维安全、AI 安全、数据安全、个人信息保护、关键基础设施保护等）、信息系统建设与运维安全等；
c） 应用安全控制审计，包括应用安全管理目标、方针和策略、组织管理、管理制度和流程、信息分类和保护体系、业务流程处理安全、数据输入、处理及输出安全、系统接口与信息共享安全、操作安全、物理安全、访问控制、应急计划。

9.3 专项类审计

IT 专项类审计（审计范围见附录 B）包括但不限于：
a） 应用系统生存周期管理专项审计；
b） 网络与信息安全治理专项审计；
c） 数据安全治理专项审计；
d） 个人信息保护专项审计；
e） 数据资产治理专项审计；
f） IT 合规管理专项审计；
g） IT 绩效管理专项审计；
h） 业务连续性管理专项审计；
i） 人工智能治理专项审计；
j） 软件供应链安全专项审计；
k） 源代码管理专项审计；
l） 开源软件管理专项审计。

9.4 审计流程

9.4.1 概述

审计流程是审计协同体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、审计完成和后续审计四阶段。

9.4.2 信息系统审计流程

信息系统审计流程包括但不限于：
a） 审计准备，包括明确审计目的及任务、组建审计项目组；明确角色和责任、确定所有人员均具备完成该项目相应的专业胜任能力；搜集相关信息、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；
b） 审计实施，包括深入调查并调整审计计划、了解并初步评估 IT 内部控制、进行控制测试、进行实质性测试；

c） 审计完成，包括整理与复核审计工作底稿、整理审计证据、评价相关 IT 控制目标的完成、判断并报告审计发现、沟通审计结果、编写审计报告并进行沟通、提交审计报告、归档管理；
d） 后续审计，项目组根据 IT 审计流程的相关要求，进行检查、调查，收集审计证据，编写后续审计报告。

注：在确定实质性测试的性质、时间和范围时，充分考虑实质性及其与审计风险之间的关系。

9.4.3 人机协同审计要点

人机协同审计是对信息系统审计流程的优化，审计要点包括但不限于：

a） 审计准备，包括明确审计目的及任务（含人机协同审计范围）、组建具备 AI 素养与数据审计能力的项目组、明确人机权责分工与复核机制；AI 辅助信息搜集、风险画像与审计计划编制，审计人员进行专业判断与计划审定；
b） 审计实施，包括 AI 辅助深入调查与计划动态调整、人机协同评估 IT 及 AI 融合内控；AI 辅助控制测试（如异常检测、模式识别、日志挖掘及全量数据分析）与实质性测试（如大数据验证、算法审查及边界场景测试），审计人员进行关键判断、访谈核实与审计决策；关键审计结论不得由算法单独出具，须经审计人员确认；
c） 审计完成，包括 AI 辅助底稿整理、证据归集与初步分析；人机协同评价控制目标的完成、判断并报告审计发现；AI 辅助报告初稿生成，审计人员复核定稿、沟通审计结果、提交审计报告、归档管理；
d） 后续审计，包括 AI 辅助持续监控、整改追踪与证据收集；人机协同评价整改效果并编写后续审计报告。

注：人机协同审计治理内容见 6.4.4

9.5 审计报告

9.5.1 信息系统审计报告

信息系统审计报告（见附录 C）包括但不限于：

a） 明确审计报告接收人；
b） 明确被审计单位名称；
c） 明确审计目的、范围、期间、依据、双方责任及内容；
d） 写明审计发现的问题、可能导致的潜在风险及改进建议；
e） 写明审计总体结论和意见；
f） 写明对该审计的所有保留意见、限制性或局限性；
g） 以充分、适当的审计证据支持审计发现和审计结果；
h） 明确审计单位名称；
i） 明确审计报告出具时间。

注：审计发现是指审计人员在审计过程中发现的问题和异常情况，包括违规行为、违法行为、操作失误、效率低下、资源浪费、无效操作及潜在利益冲突等。

9.5.2 实时审计监测分析报告

实时审计监测分析报告是 IT 审计机构基于持续审计机制，对系统运行状态、交易流水及控制有效性进行实时监测生成的动态分析报告。分析报告内容包括但不限于：

a） 报告接收，包括系统自动推送的接收对象及告警触发阈值等；
b） 监测对象：包括被监测的系统、模块、接口或数据流标识等；

c） 监测概况，包括监测指标、规则引擎、时间窗口及基准依据等；
d） 异常告警，包括实时捕捉的异常交易、违规操作、控制失效点及风险评分等；
e） 告警分级：包括根据影响后果与范围进行分级，如一般 、重要、非常重要等；
f） 处置建议，包括针对异常情况的即时阻断建议或人工干预指令等；
g） 置信说明，包括 AI 模型的置信度水平、误报率及监测盲区说明；在确保审计独立性和不泄露核心技术细节的前提下，平衡透明度要求与技术保密需要；
h） 证据支撑，包括以全量数据流日志、快照及算法分析结果作为审计证据等；
i） 出具单位，包括自动化审计平台名称及监管责任人等；
j） 出具时间，包括报告生成的精确时间戳（精确到秒/毫秒）；
k） 汇总与回顾，包括在一定周期（如季度）进行人工复核汇总，形成阶段性综合报告，以便于人机责任的追溯。

附 录 A
（资料性）
内部控制类审计

A.1 IT 内部控制审计

A.1.1 组织控制审计

组织控制审计范围包括但不限于：

a） 控制环境，包括 IT 治理原则、IT 战略与业务战略的一致性、决策层 IT 风险偏好及风险容忍度、IT 治理职责分工和制衡机制、人工智能伦理审核机制、IT 内部控制监督机制、IT 内部控制机构的设置、职责与权限、内部审计机构设置、人员配备和工作独立性、制定和实施人力资源政策、IT 文化建设等；

b） 风险评估，包括风险管理的目标、策略、原则、组织架构、制度与流程，风险识别、风险分析、风险评价及风险处置的执行情况，信息资产的分类及信息资产所有者的职责，组织和重要的利益相关者对其运营、报告、合规目标的评估及网络风险的考虑；

c） 控制活动，包括通用要求（如控制政策与流程、授权与审批控制、预算控制、信息记录与报告、资产保护、绩效考核及不相容职责分离等）及 IT 治理活动（如战略、组织、IT 架构，管理体系、资源管理及创新管理等）；

d） 信息与沟通，包括信息系统架构及其对财务、业务流程的支持度，决策层的信息沟通模式，IT 战略、政策及制度等传达与沟通的连续性、完整性及有效性，对网络风险内部控制所需信息的明确，信息安全和网络风险事件沟通机制及组织与外部的信息沟通模式及方案等；

e） 内部监督，包括 IT 风险三线建立的合规性，IT 监控管理报告系统、监控反馈、跟踪处理程序，IT 内部控制的自我评估机制，已按规定要求开展 IT 审计工作，对计算机网络风险控制的监督、自我评估及整改等。

注：IT 风险三线（兼具风险的防守）包括一线（包括 IT 部门、业务部门及相关委员会）、二线（包括内部控制、合规、安全、风险等管理部门及相关委员会）、三道防线（包括审计、监察等部门及相关委员会）。

A.1.2 一般控制审计

一般控制审计范围包括但不限于：

a） 系统采购，包括采购管理机制、需求规划与采购计划、请购与立项审批、供应商遴选与评估、定价机制与成本评估、合同与协议管理、供应过程与交付管理、验收与效能评估、付款与资金控制、重复建设与资源复用及自主可控与供应链安全；

b） 项目管理，包括项目准备（如项目章程、项目范围、项目计划等）、项目实施（如项目执行的指导和管理、项目工作的监控）、项目整体变更及收尾（如整体变更控制、项目收尾），以及 AI 相关特殊性考虑，如项目准备的伦理与合规风险评估、数据与算力就绪度评价、假设驱动的实验计划等；项目实施的数据工程与模型迭代、算法性能与偏见监控、人机协同机制落实等；项目变更与演进的模型漂移与动态变更控制、持续学习机制移交、算法审计与伦理审查验收等；

c） 系统开发，包括立项、需求、设计、实施、测试、验收、移交及迁移等活动，各类环境分离情况，系统文档与交付物的一致性及自主可控情况，以及 AI 相关的特殊性考虑（如数据工程与设计、模型训练与实施、评估与测试、伦理审查与验收、持续演进移交等）；

d） 系统变更，包括系统变更流程设计、测试质量保证、应用系统、相关系统基础架构变更及参数变更的分类控制等，以及 AI 相关的特殊性考虑（如模型迭代、数据更新、算法调整及人机协同机制变更的流程设计与伦理影响评估，模型性能验证、偏见检测、鲁棒性测试及 A/B 或影子验证的质量保证等）；

e） 系统运行，包括系运行监控、系统性能与容量、物理环境、系统和数据备份与恢复管理、事件与问题管理、应急及灾备管理等，以及 AI 相关的特殊性考虑（如模型运行监控、算力与数据管道管理、AI 运行环境管控、模型版本、数据版本管理、知识库管理、AI 事件与问题管理、AI 应急及灾备管理等）；

f） 系统开发运维一体化，包括项目管理、过程改进、支持和保障、产品研发、服务管理及基础设施等；

g） 网络与信息安全，包括网络运行安全、网络信息安全、监测预警与应急处置、信息系统建设与运维安全、信息系统开发运维一体化安全等，以及 AI 相关的特殊性考虑（如 AI 算力与智能集群网络运行安全、模型与智能交互信息安全、AI 专项风险监测预警与应急处置、AI 平台与人机协同系统建设运维安全等）；

h） 其他相关控制，包括文档管理、培训管理、配置管理、绩效考核与奖惩（含 AI 相关的特殊性考虑）。

A.1.3 应用控制审计

应用控制审计范围包括但不限于：

a） 应用组织管理，包括组织结构、用户管理、参数管理、操作管理、安全管理、事件与问题管理及人机协同相关管理等；

b） 业务流程设计，包括业务流程设计的完备性、业务流程处理的正确性和控制的有效性、业务功能的合理性）、人机协同的特殊性考虑（如 AI 决策处理的正确性、公平性与控制的有效性，AI 业务功能的合理性与合规性等）；

c） 数据输入、处理及输出，包括数据输入控制相关的数据采集、修改、删除等，数据处理控制相关的数据转换、整理及计算等，数据输出控制相关的输出外设、输出范围、内容及信息分发等）、AI 相关系统的特殊性考虑（如数据输入控制相关的多模态与提示词输入、训练语料采集与清洗、数据对齐等；数据处理控制相关的特征提取与向量化、模型推理与概率计算、动态转换与加工等，数据输出控制相关的生成内容过滤与护栏拦截、输出边界与可信度标识、人机协同审查等）；

d） 系统接口与信息共享，包括系统接口相关的标准与接口/转换控制，信息共享相关的共享信息分类与控制等，以及 AI 相关系统的特殊性考虑(如 AI 系统接口标准、模型服务接口与数据管道控制，AI 数据与模型知识共享分类、共享控制等)；

e） 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，数据的规范性、完整性、准确性、一致性、时效性、可访问性等， 以及 AI 相关的特殊性考虑（如标注准确性、样本代表性、数据偏见、特征一致性、时效性等）。

A.2 数据治理内部控制审计

A.2.1 组织控制审计

数据治理组织控制审计范围包括但不限于：

a） 控制环境，包括数据治理战略与 IT 战略及业务战略的一致性、决策层的数据风险偏好与容忍度、数据治理职责分工与制衡机制、数据治理委员会（或等效机构）的设置与职责权限、数据认责机制（如数据所有者、管理者、使用者等角色）及数据文化建设等；
b） 风险评估，包括数据风险管理目标、策略、制度与流程，数据风险（含数据质量风险、安全风险、合规风险等）的识别、分析、评价及处置执行情况，数据资产分类分级及所有者职责等；
c） 控制活动，包括数据治理政策与流程、授权与审批、预算控制、信息记录与报告等通用要求的遵循情况，以及与数据战略、数据组织、数据架构、数据管理体系及数据价值体系等相关治理活动的合理性、有效性；
d） 信息与沟通，包括数据治理相关信息系统架构及其对业务的支持度，数据战略、政策及制度传达与沟通的连续性与有效性，数据安全事件沟通机制，与外部相关方的数据共享与沟通机制等；
e） 内部监督，包括数据治理监控体系、自我评估机制，数据治理审计工作的开展情况，以及对数据风险控制的监督、评估及整改等。

A.2.2 一般控制审计

数据治理一般控制审计范围包括但不限于：
a） 数据采购管理，包括数据工具/平台采购机制、供应商遴选与评估、合同与交付管理、验收与效能评估、自主可控情况等；
b） 数据项目整体管理，包括项目准备（项目章程、范围、计划）、实施（指导管理、监控）、变更及收尾等；
c） 数据治理信息系统开发、交付与运营管理，包括数据治理平台/系统需求、设计、开发、测试、验收、移交、运行维护、变更管理等活动的规范性与有效性；
d） 其他相关控制，包括元数据管理、主数据管理、数据标准管理等相关管控。

A.2.3 应用控制审计

数据治理应用控制审计范围包括但不限于：
a） 数据治理信息系统，包括应用组织管理，包括组织结构、用户管理与权限、参数管理、操作管理等；
b） 数据治理信息系统，包括数据流程设计，包括数据采集、集成、加工、共享、归档等流程的完备性与合规性，数据流转路径的可追溯性等；
c） 数据采集、处理及输出控制，包括数据采集的合法性与来源可追溯性，数据处理的一致性与准确性，数据输出的完整性、及时性与授权控制等；
d） 系统接口与信息共享，包括数据接口标准与转换控制、数据共享分类与控制、跨系统数据交换的安全性与合规性等；
e） 数据质量，包括数据质量管理的组织、制度、流程及控制执行情况，数据的规范性、完整性、准确性、一致性、时效性及可访问性等。

A.3 安全治理内部控制审计

A.3.1 组织安全控制

组织安全控制审计范围包括但不限于：

a） 控制环境，包括安全治理相关的原则、战略，安全战略与 IT 战略、业务战略的一致性，安全治理与管理的职责分工和制衡机制等；
b） 风险评估，包括安全风险管理的目标、策略、原则、管理组织、制度、流程及信息资产安全分类及保护机制等；
c） 控制活动，包括安全治理政策与流程、授权与审批、预算控制、信息记录与报告等通用要求的遵循情况，以及与安全战略、安全组织、安全架构及安全管理体系等相关治理活动的合理性、有效性；
d） 信息与沟通，包括安全相关的信息沟通模式，安全战略、政策及制度等传达与沟通的连续性、完整性及有效性；
e） 内部监督，包括安全风险是否纳入内部监督范畴、安全内部控制的自我评估机制及安全审计开展等。

A.3.2 一般安全控制审计

一般安全控制审计范围包括但不限于：

a） 总体安全管理，包括一般规定中的国家网络安全等级保护制度落实情况、一般规定中的其他事项、关键信息基础设施的运行安全等；
b） 个人信息保护，包括个人信息保护制度的建立、收集、使用个人信息遵循的原则与规则、对个人信息采取的安全防护措施、对用户发布的个人信息的管理等；
c） 监测预警与应急处置，包括网络安全应急工作机制的建立、网络安全事件应急预案的制定、网络安全事件应急预案的定期演练、记录、分析与总结等；
d） 信息系统建设与运维安全，包括信息系统建设安全（如立项、需求、设计、实施、测试、验收、上线等环节的安全控制），信息系统运维安全（如物理安全、网络安全、设备安全、操作系统安全、应用系统安全、数据安全及安全事件管理等）、开发运维一体化安全及 AI 安全等。

A.3.3 应用安全控制审计

应用安全控制审计范围包括但不限于：

a） 组织管理，包括应用安全组织架构完整性、责任人设定机制、各类管理角色设定及之杂而分配合理性、应用安全管理权限分配合理性等；
b） 业务流程处理安全，包括不相容岗位的职责分离、流程各环节的安全控制等；
c） 数据输入、处理及输出安全，包括输入环境数据来源合规性检查机制与方法、数据输入内容校验控制机制与执行情况、数据输入环节权限管控措施落实情况、数据处理规则建立及变更的审批机制、中间数据管理要求与执行情况、数据处理期间异常情况的处理机制与执行情况、数据输出校验机制的执行情况等；
d） 系统接口与信息共享安全，包括接口统一管理、接口准入审批要求落实情况、系统接口安全防护机制与落实情况、接口变更审批机制及执行情况、信息共享范围的界定与审批、信息共享审批流程合理性与执行情况、信息共享合规要求遵循情况等。

附 录 B
（资料性）
专项类审计

B.1 应用系统生存周期管理

应用系统生存周期管理专项审计范围包括但不限于：

a） 通用要求，包括控制政策与流程、授权与审批控制、预算执行与监控、信息记录与报告、资产保护、绩效考核、不相容职责分离、伦理审查及人机职责分离等；
b） 系统采购，包括系统采购任务分工及职责、需求计划和采购计划、请购、选择供应商、确定采购价格、订立框架协议或采购合同、供应过程的管理、验收、付款、重复建设情况、自主可控情况等；
c） 项目管理，包括项目准备、项目实施、整体变更及收尾等（含 AI 相关的特殊性考虑）；
d） 系统立项，包括可行性研究、立项申请及审批（含 AI 相关的特殊性考虑）等；
e） 系统需求，包括需求计划、需求调研与分析、需求规格说明书、需求评审及需求变更（含 AI 相关的特殊性考虑）；
f） 系统设计，包括技术方案选型、概要设计、详细设计、数据库设计及评审确认（含 AI 相关的特殊性考虑）等；
g） 系统实施，包括编码规范、源代码与代码的版本管理、代码测试、单元测试、缺陷管理、集成测试计划、集成测试设计、集成测试实现和集成测试执行（含 AI 相关的特殊性考虑）等；
h） 系统测试，包括测试计划、测试用例、测试版本、缺陷及测试报告的管理（含 AI 相关的特殊性考虑）等；
i） 系统验收，包括目标实现、成本收益、功能验收、文档验收、测试评估、过程质量评估、项目验收（含 AI 相关的特殊性考虑）等；
j） 系统移交，包括移交方案的制定及实施、移交报告的管理（含 AI 相关的特殊性考虑）等；
k） 系统迁移，包括迁移方案、回退方案、迁移评估（含 AI 相关的特殊性考虑）等；
l） 系统变更，包括系统变更流程设计的合理性、测试和质量保证情况、应用系统、相关系统基础架构变更及参数变更的分类控制、变更执行、测试及移植到生产环境（含 AI 相关的特殊性考虑）等；
m） 系统运行，包括系统运行监控、系统性能与容量、物理环境、系统和数据的备份、恢复管理、事件及问题管理、应急及灾备管理（含 AI 相关的特殊性考虑）等；
n） 系统开发运维一体化，包括项目管理、过程改进、支持和保护、产品研发、服务管理及基础设施（含 AI 相关的特殊性考虑）等；
o） 系统安全，包括信息系统的建设安全、运行与服务安全、应用安全、数据安全及个人信息安（含 AI 相关的特殊性考虑）等；
p） 系统其他相关控制，包括文档管理、培训管理、配置管理、绩效考核与奖惩（含 AI 相关的特殊性考虑）等；
q） 系统应用，包括应用组织管理、业务流程设、输入、处理与输出、系统接口与信息共享、数据质量（含 AI 相关的特殊性考虑）等。

B.2 网络与信息安全治理

网络与信息安全治理专项审计范围包括但不限于：

a） 顶层设计， 如网络与信息安全治理战略（含 AI 安全战略）与 IT 战略、业务战略的一致性，AI 科技伦理审查；网络与信息安全战略规划（含 AI 风险评估）、组织构建（含 AI 安全专项组织及人机协作安全职责等）、架构设计（含 AI 安全架构）等；
b） 管理体系， 如网络运行安全、信息安全、监测预警与应急处置、数据安全、个人信息保护、系统建设安全、运行与服务安全、开发运维一体化安全等，以及 AI 安全的特殊考虑（如模型安全、对抗攻击防护、模型防窃取等）的管理等；
c） 治理过程，如网络与信息安全的统筹规划（含 AI 资产梳理与风险评估）、构建运行（含 AI 安全控制的部署）、监控评价（含安全监控与 AI 模型漂移监控、AI 异常行为检测等）及改进优化（含安全整改与 AI 安全模型迭代的联动改进）等；
d） 治理平台， 如网络与信息安全治理平台的建设、运维、安全及应用，以及 AI 安全治理平台（含模型安全监测平台、AI 风险评估平台、AI 伦理审查平台、AI 资产管理平台等）的建设、运维、安全及应用等。

B.3 数据安全治理

数据安全治理专项审计范围包括但不限于：

a） 顶层设计，如数据安全战略与 IT 战略（含 AI 战略）及业务战略的一致性；数据安全战略规划、数据安全组织架构建设、业务数据安全架构与 AI 数据治理、模型数据安全、人机协同数据防护架构的一体化设计及实施合规性；
b） 管理体系，如数据安全标准规范体系建设、业务数据与 AI 样本数据质量安全管控、全量元数据安全管理等；
c） 价值体系，如业务数据与 AI 智能数据的安全合规应用、跨场景安全流通共享、数据安全服务赋能等；
d） 全周期数据安全治理过程，如 IT 与 AI 融合数据安全的统筹规划、治理体系搭建与常态化运行及融合数据安全动态监控等；
e） 数据安全治理平台管控，如适配 IT 与 AI 融合场景的数据安全治理平台的建设合规性、日常运维稳定性及平台自身安全防护水平等。

B.4 个人信息保护专项审计

个人信息保护专项审计范围包括但不限于：

a） 管理目标与原则，包括管理目标（如个人信息处理合法合规、保障个人信息权益、实现个人信息全流程安全可控等）、管理原则（如合法正当、最小必要、知情同意、全程可追溯、风险可控等）；
b） 组织架构、职责及权限，包括合规架构与职责（如个人信息保护负责人、隐私合规专员、个人信息保护审计岗等）、团队协作机制，以及在信息收集、对外共享、跨境传输、应急处置等环节的合规审批权限等；
c） 管理制度，包括系统识别并整合个人信息保护相关法律法规、政策、国家标准，建立统一的隐私合规知识库，覆盖现行法律要求、内部程序、技术安全标准及行业规范，并定期分析合规差距与补强控制措施；
d） 管理流程，包括个人信息全生命周期合规审查流程、合规风险识别与评估机制、个人信息安全事件调查与整改闭环流程，以及合规例外事项的上报与决策路径；
e） 合规相关培训教育，包括分层分类的合规意识宣贯、专业技能提升、岗位合规资质管理，以及面向管理层与执行层的差异化合规责任教育；

f） 合规管理活动，包括常态化合规监测、专项合规检查、第三方合规尽职调查，以及合规绩效分析与持续改进活动；
g） 合规管理审计与评估机制，包括合规管理体系有效性内部审计、外部合规评估、合规缺陷根因分析与整改跟踪机制，以及个人信息保护管理成熟度评价与动态优化机制。

B.5 数据资产治理

数据资产治理专项审计范围包括但不限于：
a） 顶层设计，如数据资产治理战略与 IT 战略（含 AI 战略）及业务发展战略的一致性；数据资产的战略规划（含 AI 数据资产风险评估）、组织构建（含 AI 数据资产专项管理组织及人机协作资产管理职责等）、架构设计（含 AI 数据架构，如训练数据层、模型资产层等）；
b） 管理体系，如数据资产全过程管理（如盘点、目录、确权、登记、安全及合规管理等），以及 AI 相关的特殊考虑（如模型资产盘点与模型卡片管理、训练数据确权与合规、AI 生成内容资产登记等）；
c） 业务体系， 如数据资产的采购、加工、研发、营销及人力资源等管理，以及 AI 相关的特殊性考虑（如训练数据采购与加工、模型研发与迭代、AI 营销数据应用等）；
d） 治理过程， 如数据资产的统筹规划（含 AI 数据资产的梳理）、构建运行（含 AI 数据资产管理的部署）、监控评价（含 AI 数据资产质量监控）及改进优化（含 AI 数据资产迭代的联动改进）等；
e） 治理平台， 包括数据资产管理平台的建设、运维、安全及应用，以及 AI 相关的特殊性考虑（如模型资产管理平台、训练数据管理平台等）。

B.6 合规管理

IT 合规管理专项审计范围包括但不限于：
a） 合规管理范围，包括明确合规管理覆盖 IT 领域，考虑 AI 领域的特殊性（如算法备案、模型可解释性、公平性评估等），以及应用场景（如人机协同决策、自动化流程）的合规边界；
b） 合规管理目标与原则，包括管理目标（如系统合法性、合规性与 AI 系统的可信、透明、负责等）、管理原则（如风险导向、主动预防、持续监控、可解释性等）；
c） 合规组织架构、职责及权限，包括合规架构与职责（如 IT 合规官、AI 伦理委员会、算法审计岗等）、团队协作机制，以及在模型开发、数据标注、系统运维、人机交互等环节的合规审批权限等；
d） 合规管理制度，包括系统识别并整合适用的法律法规、政策、标准，建立统一的合规知识库，覆盖现行政策、程序、技术标准及行业准则，并定期分析差距与控制措施；
e） 合规管理流程，包括全生命周期合规审查流程、合规风险识别与评估机制、违规事件调查与整改闭环流程，以及合规例外事项的上报与决策路径；
f） 合规相关培训教育，包括分层分类的合规意识宣贯、专业技能提升、岗位合规资质认证，以及面向管理层与执行层的差异化合规责任教育；
g） 合规管理活动，包括常态化合规监测、专项合规检查、第三方合规尽职调查，以及合规绩效分析与持续改进活动；
h） 合规管理审计与评估机制，包括合规管理体系有效性内部审计、外部合规评估、合规缺陷根因分析与整改跟踪机制，以及合规管理成熟度评价与动态优化机制。

B.7 绩效管理

IT 绩效管理专项审计范围包括但不限于：

a） 组织管理，包括绩效管理组织架构、岗位设置与权责分工，IT 绩效、AI 模型治理、算力资源利用、人机协同运营等板块的绩效管理主体、协同职责与管控边界等；
b） 管理制度，包括 IT 管理制度、AI 智能应用绩效规范、人机协同作业绩效管理规范等；
c） 考核指标体系，包括 IT 系统稳定运行、运维质量、资源利用率等基础指标，以及 AI 模型精度、推理效能、算力使用率人机协同作业效率等智能化专项考核指标；
d） 评价方法，包括 IT 运维量化评价方式、常态化考核手段，以及 AI 智能成效动态评估、模型迭代效果评价、人机协同协同效能综合研判等多元化评价方法；
e） 考核范围，包括常规 IT 考核、AI 智能化绩效考核、人机协同效能考核等；
f） 奖励与惩罚措施，包括针对 IT 履职成效、AI 治理工作质量、模型优化成果、人机协同作业合规性与高效性等，落实相应的差异化奖惩措施，强化 IT 激励约束效能；
g） 考核活动，包括考核计划编制、IT 绩效（含 AI 智能绩效）实施、考核过程记录、综合评价结果审定、结果公示与应用落地等全流程管控情况。

B.8 业务连续性管理

业务连续性管理专项审计范围包括但不限于：
a） 组织环境，如内外部环境分析、IT 法规（含 AI 相关的算法备案、生成式 AI 管理等）要求的识别、应急机制（含 AI 相关的模型漂移、幻觉、AI 服务中断、数据投毒等）的建立、外部应急协调联防（含 AI 供应链应急联动）以及应急管理体系（含 AI 相关应急管理体系）的建立等；
b） 领导力，如组织各级管理者在业务连续性方针（含 AI 伦理应急决策、人机协同应急指挥等）等方面的承诺和领导力，以及 AI 突发事件中人类最终决策责任机制的落实等；
c） 策划，如 IT 风险（含模型失效、算法偏见突发等 AI 相关风险）的应对措施、业务连续性策略（含模型降级、AI 服务熔断、人机协同切换等 AI 相关策略）的目标设定、BCMS 组织的构建及业务连续性实施计划管理等；
d） 支持，如对 BCMS 资源管控的重视程度、备用资源（含算力冗余、模型热备、推理服务降级资源等）、承担 BCMS 工作人员的技能（含 AI 应急能力的要求）及业务连续性文化及沟通协调机制等；
e） 实施，如实施策划和控制、开展业务影响分析（含 AI 相关的业务影响分析）、制定和维护业务连续性计划、应急响应及灾难恢复机制的建立和维护、演练测试及资源支持等；
f） 绩效评估，包括监测测量（含 AI 相关模型性能漂移监测、AI 服务可用性监测、AI 异常事件监测等）的评价、内部审核的开展及管理评审等；
g） 改进，包括 BCMS 整改计划（含 AI 相关模型迭代及 AI 应急预案优化等）的制定、整改计划的实施、检查及持续优化等。

B.9 人工智能治理

人工智能治理专项审计范围包括但不限于：
a） 顶层设计， 包括 AI 战略（如伦理战略、安全战略、合规战略等）与 IT 战略、业务战略的一致性，AI 战略规划、组织构建（如 AI 伦理委员会、AI 安全官、算法备案管理岗等）、架构设计（如模型治理层、数据治理层、算法治理层的部署）等；
b） 管理体系， 包括 AI 伦理管理（如公平性、可解释性、透明性、问责制等）、AI 风险管理（如模型风险、算法风险、数据风险等）、AI 模型全生命周期管理、AI 数据治理、AI 安全管理（如对抗攻击防护、模型防窃取、AI 生成内容安全等）、AI 合规管理（如算法备案、模型卡片、数据说明书）及 AI 质量管理等；

c） 业务体系， 包括 AI 研发管理、AI 应用管理（如人机协同应用管控等）、AI 采购管理（如算力、数据、预训练模型采购等）、AI 人力资源管理（如 AI 人才与人机协同岗位管理等）、AI 供应商管理（如 AI 模型供应商与算力供应商管理等）等；

d） 治理过程， 包括 AI 治理统筹规划、治理体系构建与常态化运行、模型运行与智能风险动态监控、治理成效考核评价、问题复盘整改及治理机制持续改进优化的闭环管理；

e） 治理平台， 包括 AI 治理平台（如 AI 伦理审查平台、算法备案管理平台、模型安全监测平台、AI 风险评估平台、模型卡片管理平台、AI 合规审计平台等）的建设与应用等。

B.10 软件供应链安全专项审计

软件供应链安全专项审计范围包括但不限于：

a） 通用要求，包括软件供应链安全控制政策与流程、开源软件、第三方组件、商业软件、外包开发成果、构建工具、制品、模型、数据集、插件、API 及云服务等准入要求，授权与审批控制、预算和资源控制、信息记录与报告、软件资产保护、知识产权保护、密钥与凭据保护、绩效考核及不相容职责分离等；

b） 组织管理，包括机构管理及职责范围，人员职责及范围（权限、能力、资质、背景、技能培训等）、资源管理（资金、场地、人力、预算等）和供方知识产权管理（防范相应法律风险，防止侵权）；

c） 制度管理，包括确定软件供应链安全的总体方针、安全制度和策略、应急预案和演练等，及时制定、修订、宣贯、执行各项软件供应链安全管理制度、流程以及机制；

d） 识别资产,包括梳理一般软件资产（至少包含软件产品信息）、重要软件资产（另需包含软件产品信息、软件组件成分信息、组件漏洞信息、合规信息）、核心软件资产（另需包含软件部署和运行依赖的其他软件产品信息），构建、及时更新软件供应链安全图谱；

e） 风险评估，包括确定软件供应链风险评估对象（软件、环境及工具、外部组件、AI 底层应用等）范围和边界，制定相应的防范、缓解或消除措施；

f） AI 风险防范，包括数据层风险防范（训练数据遭投毒攻击、存在数据偏见或隐私泄露风险等）、模型层风险防范（开源训练模型被污染或植入后门等）、生态层风险防范（底层算力芯片、开源框架等强外部依赖产品可用性风险）；

g） 防控闭环管理，包括持续优化监测预警（漏洞扫描等）、风险防范（供应商及产品安全动态评价）、应急处置（数据-算法-算力相结合的动态治理）一体化闭环管理，重点防范产品与服务被非法控制、遭受干扰破坏、供应中断等风险。

B.11 源代码管理专项审计

源代码管理专项审计范围包括但不限于：

a） 管理基础与责任边界，包括源代码管理目标、制度规范、代码资产权属、岗位职责、授权审批、不相容职责分离、编码规范、分支策略、评审规则、发布准入、保密要求、知识产权保护、密钥与凭据保护，以及智能辅助编码工具使用边界、生成代码责任归属和人机协同审核要求等；

b） 代码资产与仓库环境管理，包括代码仓库、项目、分支、标签、基线、版本、配置文件、脚本、测试代码、外部代码片段和生成代码等资产的登记、分类分级、授权、备份、恢复、归档及保护，代码托管平台、开发环境、访问认证、权限模型、参数配置、审计日志，以及与需求管理、缺陷管理、CI/CD 流水线、制品仓库等工具链的衔接管理等；

c） 开发提交与变更流转控制，包括需求或任务与代码提交关联、代码创建、修改、删除、提交、分支创建、合并、冲突处理、代码评审、缺陷修复、紧急变更、回退和版本标识等流程

设计的完备性、处理正确性和控制有效性，以及辅助编码输出的来源标识、人工确认和敏感信息防护等；

d） 质量安全与发布准入控制，包括静态代码分析、代码质量检查、漏洞扫描、敏感信息检测、恶意代码检测、许可证合规审查、依赖声明核查、提交签名、完整性校验、生成代码验证、质量门禁、发布审批、构建输入确认和上线准入评估等；

e） 追溯审计、归档与持续改进，包括提交记录、评审记录、合并记录、扫描报告、缺陷记录、发布记录、权限变更记录、异常操作记录和审计日志等留痕追溯，代码备份恢复、转交、归档、废弃仓库清理、离职人员权限回收、历史版本保护，以及代码质量、安全缺陷、流程问题和事件处置的复盘整改与持续优化等。

B.12 开源软件管理专项审计

开源软件管理专项审计范围包括但不限于：

a） 策略与规划：包括开源软件管理战略与政策（如许可合规战略、开源组件风险管理战略）、与 IT 战略、业务战略及安全战略的一致性，开源软件关键组件识别、风险偏好设定、审批与准入流程、责任边界及治理目标等；

b） 组织与管理体系：包括开源软件管理组织架构、职责分工、跨部门协作机制、开源治理委员会及审批机制、培训及伦理考量、权限和配置管理、开发与使用人员管理、外部社区协作及供应商管理、考核与问责机制等；

c） 软件生存周期管理：涵盖开源软件选型、引入、开发修改、构建、测试验证、发布交付、部署使用、维护更新、退役替换等全生命周期管理；包括开源组件、开源框架、开源工具、插件、模型、数据集、API、SDK 及自动化开发工具的纳入、使用规范及安全控制；流程设计应保证完整性、正确性、有效性及合规性；

d） 运行监控与风险处置：包括运行态监控、漏洞扫描、依赖安全监测、异常行为检测、事件响应、应急预案、补丁管理、版本升级与退役、违规或恶意行为处置、风险报告及整改闭环等，确保开源软件供应链持续安全；

e） 管理平台与技术支撑：包括代码托管平台、制品仓库、依赖管理平台、镜像仓库、漏洞与许可证管理平台、模型仓库、数据集管理平台、审计与追溯平台等的建设、运维、安全及应用，以支撑开源软件生命周期管理、风险监控、合规执行及闭环改进。

附 录 C
（资料性）
信息系统审计报告

C.1 概述

审计报告是信息系统审计监督活动的“交付产品”，是审计意见的书面文件。

C.2 审计报告的类型

信息系统审计业务的种类、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C.1所示。

表 C.1 审计报告分类表

分类	说明
按审计范围和内容划分	审计报告按范围和内容可分为： 1）内部控制审计报告 2）专项审计报告
按审计意见类型划分	审计报告按审计意见类型可分为： 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。

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的潜在因素、累积影响而导致不可能形成审计意见时，则拒绝发表意见。

C.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C.2所示。

表 C.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	说明被审计单位名称、审计目的、审计范围、审计期间、审计依据、审计范围、双方责任、审计内容、审计中所执行审计程序、测试的性质和范围及对IT审计方法和指导的说明
现状描述（如需要）	描述组织目前IT（与审计范围相关）现状，如IT组织架构、制度建设、人力资源管理、风险管理审计管理、信息安全管理、业务连续性管理等
审计发现	分章节描述，章节可以按审计发现的重要性或预期接收人来划分
整体结论和意见	对审计中所测试的控制及程序的充分性做出整体结论和意见，以及所发现缺陷会导致的潜在风险

表 C.2 审计报告的结构和内容（续）

报告结构	报告内容
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。审计报告支持审计结论，审计中收集所有证据为审计结论提供较高水平的支持
详细的审计发现和建议	审计人员决定在报告中包含哪些审计发现，基于审计发现的重要性和审计报告的预期接收人而定。如在直接提交给董事会下属的审计委员会的报告中，可以不包括那些只对当事管理人员重要，但对整个组织无重要控制意义的审计发现 通常情况下，确定各层级审计报告中包括哪些内容依赖于高级管理层提出的指导意见
其他（如备忘录等）	针对审计发现，审计人员根据重要性的原则，对不重要的审计发现可采用备忘录等其他的方式向管理层提交

参 考 文 献

[1] GB/T 20984 信息安全技术 信息安全风险评估规范

[2] GB/T 24353 风险管理 原则与实施指南

[3] GB/T 26317 公司治理风险管理指南

[4] GB/T 28827.1 信息技术服务 运行维护 第1部分：通用要求；

[5] GB/T 34960.1 信息技术服务 治理 第1部分：通用要求

[6] GB/T 34960.2 信息技术服务 治理 第2部分：实施指南

[7] GB/T 34960.3 信息技术服务 治理 第3部分：绩效评价

[8] GB/T 34960.5 信息技术服务 治理 第5部分：数据治理规范

[9] GB/T 43046 信息技术服务 应对突发公共安全事件的信息技术应急风险管理

[10] 企业内部控制基本规范（中华人民共和国财政部财会〔2008〕7号）2008-5-22.

[11] 企业内部控制审计指引（中华人民共和国财政部财会（2010）11号）2010-4-15.

[12] 内部审计基本准则（中国内部审计协会公告2013年第1号）2013-8-20.

[13] 内部审计具体准则第2203号——信息系统审计（中国内部审计协会公告2013年第1号）2013-8-20.

[14] 信息系统审计指南——计算机审计实务公告第34号（中华人民共和国审计署审计发〔2012〕11号）2012-2-1.

[15] 审计署关于内部审计工作的规定（中华人民共和国审计署审计署令第4号）2003-3-4.

[16] 中央企业全面风险管理指引（国务院国有资产监督管理委员会国资发改革〔2006〕108号）2006-6-6.

[17] 商业银行信息科技风险管理指引（中国银行业监督管理委员会银监发〔2009〕19号）2009-6-1.

[18] 证券期货经营机构信息技术治理工作指引（试行）（中国证券业协会和中国期货业协会中证协发〔2008〕113号）2008-9-3.

[19] 胡克瑾等. IT审计（第二版）[M].电子工业出版社出版，2004.

[20] CISA Review Manual International Information Systems Audit and Control Association（ISACA）, 2024