ICS 35.080
L 77

中华人民共和国国家标准

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

2017-11-01 发布　　2018-05-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

GB/T 34960《信息技术服务　治理》拟分为如下部分：

——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；

……

本部分为 GB/T 34960 的第 4 部分。

本部分按照 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。

本部分由全国信息技术标准化技术委员会(SAC/TC 28)提出并归口。

本部分起草单位：上海万隆信息技术咨询有限公司、中国电子技术标准化研究院、上海计算机软件技术开发中心、上海谷航信息科技发展有限公司、上海翰纬信息管理咨询有限公司、四川久远银海软件股份有限公司、北京华胜天成科技股份有限公司、瑞华会计师事务所(特殊普通合伙)上海分所、广州赛宝认证中心服务有限公司、北京久其软件股份有限公司、沈阳赛宝科技服务有限公司、用友网络科技股份有限公司、上海优刻得信息科技有限公司、深圳云塔信息技术有限公司、北京护航科技有限公司、联通系统集成有限公司、中金数据系统有限公司、深圳赛西信息技术有限公司、快威科技集团有限公司、上海市浦东新区信息化协会、上海翰昌信息科技发展有限公司、成都信息化技术应用发展中心、上海企源科技有限公司、神州数码信息服务股份有限公司、北京神州泰岳软件股份有限公司、北京富通金信计算机系统服务有限公司、广州赛宝联睿信息科技有限公司、南威软件股份有限公司、深圳市艾泰克工程咨询监理有限公司、成都安美勤信息技术股份有限公司、北京北咨信息工程咨询有限公司、北京神州数码锐行快捷信息技术服务有限公司、上海北塔软件股份有限公司、宝钢资源控股(上海)有限公司、北京信城通数码科技有限公司。

本部分主要起草人：俞文平、张明英、李鸣、韩佳赟、吴越、潘蓉、陆雷、宋俊典、左天祖、张绍华、宋跃武、李璐、孙佩、刘小茵、杨泉、季昕华、朱圣哲、于浩、徐飞、魏东、王春涛、向纪兰、肖建一、但强、宋长发、钱伟峰、杨琳、王铮、王永军、甘琼、徐旭华、王庆磊、刘越男、李峰、张旸旸、沈国华、王东、梁晓雁、俞丽平、邱兢、张磊磊、何敏、郝守勤、陈宏峰、黄建新、乔春艳、李刚、孙军、谭燕齐、武艳、侯姗姗、马洪杰、刘玲、徐弢、金桥、陆雯珺。

信息技术服务　治理
第4部分：审计导则

1　范围

GB/T 34960的本部分规定了信息技术审计(以下简称IT审计)总则、审计组织管理、审计人员、审计流程、审计报告、审计适用对象和范围等内容。

本部分适用于：

a)　组织治理主体实施IT审计监督职能；

b)　建立或完善组织的IT审计体系；

c)　明确组织IT审计过程中的相关要求；

d)　规范组织IT审计业务的开展；

e)　建立或完善信息化下审计体系的指导；

f)　第三方或其他相关机构开展IT审计的指导；

g)　建立或未建立内部IT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IT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IT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—2017　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

信息技术治理　information technology governance

专注于信息技术体系及其绩效和风险管理的一组治理规则，由领导关系、组织结构和过程组成，以确保信息技术能够支撑组织的战略目标。

[GB/T 29264—2012，定义2.6]

3.2

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。

3.3

信息技术审计章程　internal audit charter

确定 IT 审计活动的宗旨、权力和职责等的正式文件。

3.4

能力　capability

完成任务或履行角色责任所需知识、技能、经验及其他资源等的组合。

3.5

信息技术内部控制　internal control

由组织治理主体和全体员工实施的、旨在实现 IT 控制目标的过程。

注：内部控制要素包括 IT 控制环境、风险评估、控制活动、信息与沟通及内部监督。

3.6

组织层面控制　organization control

在组织层面建立并实施的 IT 相关控制。

注：控制要素包括 IT 控制环境、风险评估、控制活动、信息与沟通及内部监督。

3.7

组织控制审计　organization control audit

对组织层面控制开展的审计。

3.8

一般控制　general control

为了保证信息系统安全、稳定的运行，对整个信息系统以及外部各种环境要素实施的、对所有的应用或控制模块具有普遍影响的控制。

3.9

一般控制审计　general control audit

对一般控制开展的审计。

3.10

应用控制　application control

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

3.11

应用控制审计　application control audit

对应用控制开展的审计。

3.12

网络　network

利用通信线路将地理上分散的、具有独立功能的计算机系统和通信设备按不同的形式连接起来，以功能完善的网络软件及协议实现资源共享和信息传递的系统。

3.13

网络风险　network risk

组织在运用网络过程中，由于自然因素、人为因素、技术漏洞和管理缺陷等产生的风险。

3.14

审计方法　audit method

审计人员为完成 IT 审计任务所采取的方式和手段。

3.15

审计流程　audit process

审计人员在具体审计过程中采取的行动和步骤。

3.16

审计报告　audit report

审计人员在完成对审计证据的整理、归纳、评价及确定审计发现后，形成审计意见和建议，并以适当格式提交的书面文件。

4　审计总则

4.1　审计与治理的关系

IT 治理的任务包括评估、指导与监督，IT 审计是监督的内容之一。

依据 GB/T 34960.1—2017 的规定：治理主体以组织章程、监管职责、利益相关方期望、业务压力和业务要求为驱动力，建立评估、指导、监督的治理过程并明确任务。治理主体应通过 IT 战略和方针，指导管理者对 IT 及其应用的管理体系进行完善，并对 IT 相关的方案和规划进行评估、对 IT 应用的绩效和符合性进行监督。组织应结合治理原则和模型，在 IT 治理实施的过程中，开展自我监督、自我评估和审计工作，并持续改进。

4.2　审计结构及其关系

IT 审计包括审计组织管理体系、审计依据、审计方法、审计技术、审计质量控制、审计工作的执行、审计人员、审计业务、审计流程及审计报告。组织应建立 IT 审计组织管理体系，并根据审计规章制度、依据、方法、技术、质量控制、工作执行、人员、业务、流程及报告等的要求，开展 IT 审计活动。

4.3　审计依据

IT 审计依据包括但不限于：

a）　国家 IT 相关法律、法规及标准；

b）　行业 IT 相关规范及标准；

c）　地方 IT 相关规范及标准；

d）　组织内部 IT 相关规范及标准；

e）　国际 IT 相关标准；

f）　国内外 IT 最佳实践。

4.4　审计方法

IT 审计方法包括但不限于：

a）　访谈法；

b）　调查法；

c）　检查法；

d）　观察法；

e）　测试法；

f）　验证法；

g）　分析性复核法。

审计方法的应用参照附录 A 中表 A.1。

4.5 审计技术

IT 审计技术包括但不限于：

a） 风险评估技术；

b） 审计抽样技术；

c） 计算机辅助审计技术；

d） 大数据技术。

审计技术含义和应用说明参照附录 B 中表 B.1。

4.6 审计质量控制

IT 审计质量控制应采取的措施包括但不限于：

a） 创造并维持独立的审计环境；

b） 建立审计人员培养机制；

c） 建立项目质量管理机制；

d） 定期开展审计人员工作质量的自我检查与评估；

e） 适时开展审计机构工作质量的内部监督与检查；

f） 开展内部审计机构工作质量的外部检查。

4.7 审计业务类型

IT 审计业务类型包括 IT 内部控制审计和 IT 专项审计。IT 内部控制审计是为了综合评价组织 IT 控制目标实现过程而进行的审计；IT 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。IT 审计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 IT 审计作为综合性审计项目的一部分时，IT 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 IT 审计中的发现，并考虑依据 IT 审计结果调整其他相关审计的范围、时间及性质。

IT 审计人员应当以风险导向为基础开展 IT 审计，风险评估应当贯穿于 IT 审计的全过程。

4.8 审计工作的执行

审计工作执行包括但不限于：

a） 对审计人员进行指导，合理保证其审计目标的完成，并且符合审计标准；

b） 审计人员在从事审计工作时，应获得充分、可靠和相关的证据以完成审计目标；

c） 审计发现和审计结论应能被相关证据所支持；

d） 审计程序应以书面形式记录，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据；

e） 审计人员在审计过程中应考虑被审计单位违规和非法行为。

5 审计组织管理

5.1 总则

审计组织管理是指对审计组织机构设置和运行进行的管理，包括审计环境、审计机构、审计制度等方面。

5.2 审计环境

组织应为 IT 审计开展创造必要的环境，包括但不限于：

a) 治理主体应培养信息化下的审计管理理念，转变审计管理思路；
b) 明确治理主体的 IT 审计职责；
c) 审查批准 IT 审计战略，确保其与组织 IT 战略、业务战略相适应；
d) 建立与组织信息化规模相适应的 IT 审计机构，予以授权并明确由其向治理主体报告；
e) 指派具有专业胜任能力的人员担任 IT 审计机构负责人；
f) 配备适合的且拥有不同专业背景的审计人员，如审计、IT、业务管理等；
g) 确保 IT 审计机构进行独立有效的 IT 审计，对审计报告进行确认并落实整改；
h) 规范职业道德行为，增强内部文化建设，提高员工对 IT 审计重要性的认识；
i) 加强 IT 审计专业队伍的建设，建立人才激励机制；
j) 确保 IT 审计工作所需资金；
k) 确保员工遵守经批准的 IT 审计规章管理制度、准则及流程，并安排相关培训；
l) 明确 IT 审计机构与其他相关部门之间的关系，其他相关部门应配合 IT 审计工作；
m) 聘请第三方审计机构协助开展 IT 审计，并明确其与内部 IT 审计的关系。

5.3 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) 编制 IT 审计年度计划、预算及人力资源计划并报批；
d) 制定 IT 审计手册、规程及指南等；
e) 按 IT 审计规章制度、计划等的要求开展相关业务，并保证审计质量；
f) 承担对 IT 控制设计和执行有效性评估的责任；
g) 确保能直接与治理主体进行沟通及汇报；
h) 做好与组织内、外相关机构和人员的沟通协调工作；
i) 有权参加或者列席组织 IT 治理及管理的重要会议；
j) 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；
k) 定期对审计专业人员的知识、技能和培训情况进行评估，确保 IT 审计专业人员的专业知识和技能足以完成审计工作；
l) 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，应就范围受到的限制及其潜在影响与治理主体进行沟通；
m) 向治理主体提出提高 IT 绩效的改进意见和建议；
n) 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。

5.4 审计规章制度

5.4.1 审计章程

审计章程的内容包括但不限于：

a） 审计目标；
b） 审计机构的职责和权力；
c） 审计人员在 IT 审计过程中的角色和职责；
d） 审计范围；
e） 审计标准；
f） 审计报告的上报路径；
g） 保证 IT 审计机构的独立性和追责制；
h） 明确 IT 审计机构与其他部门之间的关系；
i） 聘请第三方审计机构协助开展 IT 审计，并明确其与内部 IT 审计的关系。

5.4.2 具体制度

组织应制定 IT 审计具体制度，包括但不限于：

a） 审计质量管理办法；
b） 审计项目管理办法；
c） 审计人员管理办法；
d） 审计业务管理办法；
e） 审计报告管理办法；
f） 审计外包管理办法；
g） 审计档案管理办法；
h） 审计信息管理办法；
i） 审计平台系统管理办法；
j） 利用外部专家服务管理办法。

5.4.3 流程与操作规程

组织应制定 IT 审计流程、操作规程，包括但不限于：

a） 审计流程；
b） 审计准则与指南；
c） 审计作业操作规程；
d） 审计工作手册。

5.4.4 审计平台系统

组织应建立 IT 审计平台系统，包括但不限于：

a） 审计管理系统；
b） 审计项目作业控制系统；
c） 远程审计监控系统。

5.4.5 审计战略规划

组织应制定独立的 IT 审计中长期规划及年度计划，内容包括但不限于：

a） 制定依据；
b） 发展目标；
c） 组织建设；

d) 人才培养；
e) 制度体系建设；
f) 作业体系建设；
g) 财务预算；
h) 审计项目统筹安排(制定时应运用风险评估)。

6 审计人员

6.1 职业道德

IT 审计人员应遵守职业道德，至少应：

a) 在执业过程中保持独立、客观、公正；
b) 在执业过程中保持正直、诚实和守信；
c) 正确履行审计职责(其中包括遵守相应的职业审计标准)；
d) 对在实施 IT 审计业务中所获取的信息负有保密责任。

6.2 知识、技能、资格与经验

IT 审计人员应具备相应的知识、技能、资格与经验，至少应：

a) 掌握与 IT 相关的专业知识和技能；
b) 掌握审计、财务及管理等通用知识和技能；
c) 拥有与 IT 审计工作相关的基本技能、专业技能和软技能；
d) 拥有与所处管理或业务岗位相适应的 IT 审计职业资格及经验。

6.3 专业胜任能力

IT 审计人员应胜任所承担的相关管理或业务工作，包括但不限于：

a) 具备相应的 IT 审计专业胜任能力；
b) 拥有与所处管理或业务岗位相适应的 IT 审计职业资格；
c) 定期参加持续的职业教育和培训。

6.4 利用外部专家服务

组织可根据需要利用外部专家服务，包括但不限于：

a) 对外部专家的专业资格及专业经验进行评价；
b) 对外部专家的独立性、客观性进行评价；
c) 对外部专家的专业胜任能力进行评价；
d) 与外部专家签订书面协议；
e) 对外部专家的服务结果进行评价和利用。

7 内部控制审计

7.1 总则

IT 内部控制审计是为了综合评价组织 IT 控制目标实现过程而进行的审计，包括组织层面 IT 控制、IT 一般性控制及业务流程层面相关应用控制的审查和评价。IT 内部控制审计是组织的常规

审计。

7.2 组织控制审计

7.2.1 控制环境

审计 IT 控制环境时，审计范围包括但不限于：

a） 组织遵循的 IT 治理原则；
b） IT 战略与业务战略的一致性；
c） 决策层的 IT 风险偏好及风险容忍度；
d） IT 治理的职责分工和制衡机制；
e） IT 内部控制的监督机制；
f） IT 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） 制定和实施的人力资源政策；
i） IT 文化建设；
j） 决策层对组织 IT、网络风险概况及如何应对的了解程度；
k） 超越 IT 正常控制之外风险的控制设计，包括对系统中重大异常交易或事项的控制、对系统中非正常业务流程的控制、投诉及举报制度的建立。

7.2.2 风险评估

审计 IT 风险评估时，审计范围包括但不限于：

a） 风险管理目标和策略；
b） 风险管理原则；
c） 风险管理组织，包括组织架构、责任人、角色、职责和权限等；
d） 风险管理制度；
e） 风险管理流程；
f） 风险识别、风险分析、风险评价及风险处置的执行情况；
g） 信息资产的分类及信息资产所有者的职责；
h） 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。

7.2.3 控制活动

7.2.3.1 通用要求

审计组织层面 IT 控制活动通用要求时，审计范围包括但不限于：

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

7.2.3.2 顶层设计的治理

审计 IT 顶层设计的治理时，审计范围包括但不限于：

a) IT 战略，包括治理主体对 IT 战略的指导、评估和监督，制定的 IT 战略目标及持续改进情况；

b) IT 组织，包括治理主体对 IT 组织机制的指导、评估和监督，确保利益相关方理解和支持的实现情况；

c) IT 架构，包括治理主体对 IT 架构的指导、评估和监督，支撑 IT 战略目标的实现情况。

7.2.3.3 IT 管理体系的治理

审计 IT 管理体系的治理时，审计范围包括但不限于治理主体对以下管理情况的治理要求，以及相关的评估、指导、监督和改进情况：

a) 业务连续性管理；

b) 质量管理；

c) 项目管理；

d) 投资管理；

e) 服务管理；

f) 供方管理；

g) 信息安全管理；

h) 风险管理；

i) 资产管理；

j) 其他管理。

7.2.3.4 IT 资源的治理

审计 IT 资源的治理时，审计范围包括但不限于：

a) 基础设施，包括治理主体对 IT 基础设施相关环境、网络通信、硬件设备和基础软件的治理要求，以及相关的评估、指导、监督和改进情况；

b) 应用系统，包括治理主体对应用系统规划立项、设计开发、集成实施、运行维护和应用管理的治理要求，以及相关的评估、指导、监督和改进情况；

c) 数据，包括治理主体对数据的治理要求，数据治理战略的制定，数据治理任务的确定，以及相关的评估、指导、监督和改进情况。

7.2.4 信息与沟通

审计信息与沟通时，审计范围包括但不限于：

a) 信息系统架构及其对财务、业务流程的支持度；

b) 决策层的信息沟通模式；

c) IT 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) 组织对网络风险内部控制所需要信息的明确；

e) 组织建立的信息安全和网络风险事件沟通机制；

f) 组织与外部的信息沟通模式及方案。

7.2.5 内部监督

审计 IT 内部监督时，审计范围包括但不限于：

a） IT 风险三道防线建立的合规性；
b） 组织的 IT 监控管理报告系统、监控反馈、跟踪处理程序；
c） IT 内部控制的自我评估机制；
d） 组织已按规定要求开展 IT 审计工作；
e） 组织对计算机网络风险控制的监督、自我评估及整改；
f） 风险管理部门是否按规定提前介入组织的大规模系统开发；
g） 内部审计部门是否按规定提前介入组织的大规模系统开发。

7.3 一般控制审计

7.3.1 通用要求

审计 IT 一般控制通用要求时，审计范围包括但不限于：
a） 控制政策与流程；
b） 授权与审批控制；
c） 预算执行与监控；
d） 信息记录与报告；
e） 资产保护；
f） 绩效考核；
g） 不相容职责分离。

7.3.2 系统采购

审计系统采购时，审计范围包括但不限于：
a） 系统采购任务分工及职责；
b） 需求计划和采购计划；
c） 请购；
d） 选择供应商；
e） 确定采购价格；
f） 订立框架协议或采购合同；
g） 供应过程的管理；
h） 验收；
i） 付款；
j） 重复建设情况；
k） 自主可控情况。

7.3.3 项目整体管理

审计项目整体管理时，审计范围包括但不限于：
a） 项目准备，包括项目章程、项目范围、项目计划等；
b） 项目实施，包括项目执行的指导和管理、项目工作的监控；
c） 项目整体变更及收尾，包括整体变更控制、项目收尾。

7.3.4 系统开发

审计系统开发时，审计范围包括但不限于：

a） 系统立项、需求、设计、实施、测试、验收、上线及迁移等活动；
b） 系统的开发环境、测试环境、生产环境分离情况；
c） 系统开发过程中的相关记录；
d） 系统文档与交付物的一致性；
e） 与系统相关的培训管理；
f） 自主可控情况。

7.3.5 系统变更

审计系统变更时，审计范围包括但不限于：
a） 系统变更流程设计的合理性；
b） 测试和质量保证情况；
c） 应用系统、相关系统基础架构变更及参数变更的分类控制；
d） 对变更执行、测试及移植到生产环境等关键环节的控制。

7.3.6 系统运行

审计系统运行时，审计范围包括但不限于：
a） 系统运行监控，包括系统日常运行监控的方式、监控的范围、监控结果的分析、处理等；
b） 系统性能与容量，包括系统性能与容量的监控与规划，以及系统性能提升与扩容等；
c） 物理环境，包括机房日常管理、机房巡检、视频监控及区域隔离等；
d） 系统和数据的备份与恢复管理，包括系统的备份与恢复管理、数据的备份与恢复管理等；
e） 事件及问题管理，包括事件定义、分级分类标准、事件上报、事件处理及问题整理、分析、处理等；
f） 应急及灾备管理，包括场景分析、预案制定、预案演练、分析总结、灾备策略、灾备设施建设与运行管理等。

7.3.7 系统与网络安全

审计系统与网络安全时，审计范围包括但不限于：
a） 信息安全事件管理，包括信息安全事件定义、分组分类标准、事件上报、事件处理及事后总结等；
b） 系统开发安全，包括系统安全需求、系统安全原则及系统安全设计；
c） 网络安全，包括网络架构、网络服务、网络性能及网络控制等；
d） 设备安全，包括设备的登记、保管、使用、维修及报废等；
e） 操作系统安全，包括操作系统选型、参数配置、使用及更新等；
f） 应用系统安全，包括应用系统架构、参数配置、使用、更新及系统下线等；
g） 数据安全，包括数据的获取、保存、使用、维护、传输及销毁等安全等。

7.3.8 其他相关控制

审计其他相关控制时，审计范围包括但不限于：
a） 文档管理，包括文档管理的任务分工与职责，文档的编制、收集、归档、保存、调阅及销毁等；
b） 培训管理，包括培训计划、通知、讲义及记录等；
c） 配置管理，包括配置管理的任务分工与职责、配备管理范围、配置库的建立与使用、配置库的安

全与使用规范、权限变更控制、配置管理计划及实施等；

d） 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 应用控制审计

7.4.1 通用要求

审计应用控制的通用要求时，审计范围包括但不限于：

a） 控制政策与流程；

b） 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 应用组织管理

审计系统应用组织管理时，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） 信息安全管理，包括系统应用环境安全、操作安全、介质与文档安全等；

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 业务流程设计

审计业务流程控制时，审计范围包括但不限于：

a） 业务流程设计的完备性；

b） 业务流程处理的正确性和控制的有效性；

c） 业务功能的合理性。

7.4.4 数据输入、处理及输出

审计数据输入、处理及输出时，审计范围包括但不限于：

a） 数据输入控制，包括数据采集、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，包括信息共享、交换、质量、存储、传输及销毁控制等。

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 专项审计

8.1 总则

除常规的 IT 内部控制审计外，组织应根据外部要求及内部特殊需要，设计 IT 专项审计以满足审计战略要求。IT 专项审计包括(但不限于)应用系统生命周期管理专项审计、信息安全专项审计、风险管理专项审计、供方管理专项审计、业务连续性管理专项审计、质量管理专项审计、服务管理专项审计、项目管理专项审计、资产管理专项审计及投资管理专项审计等。

8.2 应用系统生命周期管理专项审计

应用系统生命周期管理专项审计应考虑行业特点，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） 项目整体管理，包括项目准备、项目实施、整体变更及收尾等；

d） 系统立项，包括可行性研究、立项申请及审批等；

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等；

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、项目验收等；

j） 系统上线，包括上线方案的制定及实施、上线报告的管理等；

k） 系统迁移，包括迁移方案、回退方案、迁移评估等；

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、应急及灾备管理等；

n） 系统运行，包括系统运行活动、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、应急及灾备管理等；

o） 系统与网络安全，包括信息安全事件管理、系统开发安全、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、绩效考核与奖惩等；

q） 系统应用，包括通用要求、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、数据质量等。

8.3 信息安全专项审计

信息安全专项审计范围包括但不限于：

a） 信息安全管理目标、方针和策略；

b） 信息安全管理组织的建立，包括责任人、角色、职责及权限等；

c） 信息安全管理制度和流程；

d） 信息安全信息分类和保护体系；

e） 信息安全事件管理，包括事件定义、分组分类标准、事件上报、处理及事后总结等；

f） 人力资源安全，包括入职前、在职期间及离职前的安全管理；

g） 信息安全教育和培训，包括信息安全意识、策略、法律、法规、制度、业务控制等；

h） 物理安全，包括访问安全及环境安全等；

i） 系统开发安全，包括系统安全需求、系统安全原则及系统安全设计；

j） 网络安全，包括网络架构、网络服务、网络性能及网络控制等；

k） 设备安全，包括设备的登记、使用、维修及报废等；

l） 操作系统安全，包括操作系统选型、参数配置、使用及更新等；

m） 应用系统安全，包括应用系统架构、参数配置、使用、更新及系统下线等；

n） 数据安全，包括数据的获取、保存、使用、维护、传输及销毁安全等；

o） 业务连续性管理，包括组织架构、业务连续性计划及演练、应急管理、灾备管理；

p） 供应商管理，包括供应商的选择、签约、管理制度及服务过程的评估等。

8.4 风险管理专项审计

IT 风险管理专项审计范围包括但不限于：

a） 风险偏好及风险容忍程度；

b） 风险管理目标和策略；

c） 风险管理原则；

d） IT 风险管理组织，包括组织架构、责任人、角色、职责和权限等；

e） IT 风险管理制度；

f） IT 风险管理流程；

g） IT 风险识别、风险分析、风险评价及风险处置的执行情况；

h） 信息资产的分类及信息资产所有者的职责；

i） 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。

8.5 供方管理专项审计

IT 供方管理专项审计范围包括但不限于：

a） 供方管理的组织构架、职责及权限；

b） 供方管理制度；

c） 供方管理流程和方法；

d） 供方评估机制；

e） 组织商业秘密、知识产权及个人隐私的保护；

f） 供方管理活动的开展，包括供方识别和选择、供方服务过程及退出管理等。

8.6 业务连续性管理专项审计

业务连续性管理专项审计范围包括但不限于：

a） 业务连续性策略、目标；

b） 业务连续性组织架构、职责及权限；

c） 业务影响分析；

d） 业务连续性计划的制定和维护；

e） 业务连续性资源保障；

f） 应急响应机制的制定和执行；

g） 业务连续性计划的培训、演练及持续改进；

h） 灾难恢复机制的制定和执行等。

8.7 质量管理专项审计

IT 质量管理专项审计范围包括但不限于：

a） 质量管理体系的建立，包括质量体系文件的建立、文件体系的实施和控制、质量手册的编制和维护等；

b） 质量管理组织架构、职责及权限；

c） 质量管理的资源保障，包括人力资源、基础设施、工作环境等；

d） 产品及服务实现过程和结果的监视和测量；

e） 质量管理体系的持续改进。

8.8 服务管理专项审计

IT 服务管理专项审计范围包括但不限于：

a） 服务管理组织构架、职责及权限；

b） 服务管理制度及流程；

c） 建立了与服务运行目标一致的流程和方法；

d） IT 服务的策划、设计、部署、运营、验收、改进和终止；

e） 服务实施的风险管理；

f） 服务质量的管理和控制；

g） IT 服务绩效的定期评价。

8.9 项目管理专项审计

IT 项目管理专项审计范围包括但不限于：

a） 项目管理总体策略和原则；
b） 项目管理组织构架、职责及权限；
c） 项目管理制度和流程的制定；
d） 项目计划的制定和维护；
e） 项目范围、成本、进度、质量、风险、配置、沟通等控制机制的建立；
f） 项目管理流程和方法的建立和维护；
g） 项目管理活动的开展，包括项目的启动、实施及终止等；
h） 项目完成情况的统计分析及评估绩效情况。

8.10 资产管理专项审计

IT 资产管理专项审计范围包括但不限于：

a） 资产管理组织构架、职责及权限；
b） 资产应用管理，包括制度建立以及计划、采购、部署、管理、报废等环节的控制，如了解组织的整体发展目标；制定适合组织的资产管理目标和管理计划；明确资产管理人员的相关职责，明确资产获取方式等；
c） 资产财务管理，包括制度建立以及相关活动的开展，如建立资产分类目录，对关键资产进行识别；新购资产到货后，进行盘点和确认；确保内容及数量和采购订单的一致性等；
d） 资产有效性管理，包括资产授权和许可协议的维护，实施信息技术资产的许可证管理，定期对组织的信息技术资产管理进行审阅等。

8.11 投资管理专项审计

IT 投资管理专项审计范围包括但不限于：

a） IT 投资的目的与规划；
b） IT 投资原则；
c） IT 投资管理组织结构的设置、责任和权力；
d） IT 投资管理的程序和方法，包括拟定方案、可行性论证、方案决策、投资计划编制、投资计划实施、投资项目到期处置制度；
e） IT 投资计划，包括对不同阶段的资金投资数量、投资具体内容、项目进度、完成时间、质量标准与要求等进行的安排；
f） IT 投资项目的管控，包括项目运作的日常监督、合规审查和管控，投资项目的立项、实施进度、项目质量、项目费用等符合相关制度的情况；
g） 项目质量与预算的执行情况。

8.12 合规性专项审计

IT 合规性专项审计范围包括但不限于：

a） 合规性管理组织架构、职责及权限；
b） 合规性管理制度的建立，包括现行政策、程序、标准、法律以及法规的识别、分析及控制等；
c） 合规性管理制度的执行。

8.13 数据治理专项审计

数据治理专项审计范围包括但不限于：

a） 数据治理战略；
b） 数据治理任务；
c） 数据治理范围；
d） 数据治理促成因素和环境；
e） 数据治理框架，包括明确数据战略文化和思维，评估自身数据治理能力，建立明确的数据治理组织机构、团队和人员，明确职责和权利等；
f） 数据治理的组织和管理机制，包括职责分配模型、组织架构、相关职责及角色，绩效管理和评估机制等；
g） 数据治理的生命周期，包括识别环境和促成要素，实施数据治理；获得阶段性成果，形成需求调研及分析报告，评估组织内外数据应用水平现状，形成现状评估报告或成熟度评估报告等。

8.14 绩效专项审计

IT 绩效专项审计范围包括但不限于：
a） IT 绩效组织管理；
b） IT 绩效管理制度；
c） IT 绩效考核指标体系；
d） IT 绩效评价方法；
e） IT 绩效考核步骤；
f） 奖励与惩罚措施；
g） IT 绩效考核活动的开展，包括考核计划、考核实施、考核记录、考核评价结果等。

9 审计流程

9.1 总则

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四阶段。

9.2 审计准备

审计准备工作包括但不限于：
a） 明确审计目的及任务；
b） 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；
c） 搜集相关信息；
d） 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。

9.3 审计实施

审计实施工作至少应包括：
a） 深入调查并调整审计计划；
b） 了解并初步评估 IT 内部控制；
c） 进行控制测试；
d） 进行实质性测试（在确定实质性测试的性质、时间和范围时，应充分考虑实质性及其与审计风险之间的关系）。

9.4 审计终结

审计终结工作至少应包括：

a） 整理与复核审计工作底稿；

b） 整理审计证据；

c） 评价相关 IT 控制目标的实现；

d） 判断并报告审计发现；

e） 沟通审计结果；

f） 编写审计报告并进行沟通；

g） 提交审计报告；

h） 归档管理。

9.5 后续审计

在开展后续 IT 审计时，项目组宜根据 IT 审计流程的相关要求，进行检查、调查，收集审计证据，写出后续审计报告。

10 审计报告

IT 审计项目完成后，应以适当的格式递交审计报告。编制审计报告时应：

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、范围、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。

审计报告的概述参照附录 C，审计报告的类型参照附录 C 中表 C.1，审计报告的结构和内容参照附录 C 中表 C.2。

附 录 A
（资料性附录）
审计方法的应用

可以采用一系列的审计方法实施审计。本附录提供了常用审计方法应用说明见表 A.1。选择审计方法取决于所规定的审计目标、范围、依据和内容。灵活运用各种不同的审计方法及其组合，可以提高审计的效率和效果。

表 A.1 审计方法应用说明

名称	应用说明
访谈法	——可利用数据采集工具通过电话或者面对面访谈的方式收集数据，称为结构化访谈。访谈时，审计人员应以准确方式向不同访谈者提出相同的问题，并向其提供标准的答复选项。 ——可采用非结构化访谈方式，此方式更多包含开放式问题
调查法	——可对审计过程中发现的疑点和问题，通过口头询问或质疑的方式获取事实真相，并取得口头或书面证据； ——可向有关单位或个人发函以证明某一或多个审计事项
检查法	——审查书面资料的真实性、合法性，如政策、制度、流程等； ——审查各种相关资料的一致性，对各类资料之间的相关数据，按照其内在联系进行相互对照检查，以获取审计证据。 ——对书面资料或信息系统的相关数据进行重新计算，以验证原计算结果是否正确。 ——对重要的比率或趋势进行的分析，包括调查异常变动以及这些重要比率或趋势与预期数额和相关信息的差异，以获取审计证据
观察法	观察相关人员正在从事的活动或实施的程序。观察法所提供的审计证据仅限于观察发生的地点，由于观察人员的行为可能因被观察而受影响，从而导致观察提供的审计证据受到限制
测试法	基本原理是从计算机输入开始，跟踪某项业务直至输出，以检验计算机应用程序、控制程序和系统可靠性。执行此类方法使用的是用于测试目的的业务数据，称之为测试数据。 ——黑盒法测试是把程序看成黑盒子，完全不考虑其内部结构和处理过程，只检查程序的功能是否符合它的需求规格说明，这是一种宏观上的测试，适合大单元、大系统的测试。此方法是审计人员在已知组织的信息系统功能情况下，通过测试来检测每个功能是否正常使用。 ——白盒法测试是通过测试来检测产品内部动作是否按照规格说明书的规定正常进行，按照程序内部的结构测试程序，检验程序中的每条通路是否按预定要求正确工作，主要用于软件验证，称为白盒法
验证法	——可验证系统的控制是否有效和计算逻辑的正确性； ——对系统采集数据、转换数据及处理数据的过程和结果进行控制和实质性测试，验证系统数据的合规性、一致性及准确性，并对系统的相关指标进行分析和评价

表 A.1（续）

名称	应用说明
分析性复核法	是通过分析和比较信息之间的关系或者计算相关的比率，以确定合理性，并发现潜在差异和漏洞的一种审计方法。使用分析性复核方法： ——在审计计划阶段，以了解被审计事项的基本情况，确定审计重点； ——在审计实施阶段，对业务活动、内部控制和风险管理进行审查，以获取审计证据； ——在审计终结阶段，验证其他审计程序所得结论的合理性，以保证审计质量

附 录 B
（资料性附录）
审计技术含义和应用说明

本附录提供了审计方法含义和应用说明见表 B.1。

表 B.1 审计技术含义和应用说明

名称	含义	应用说明
风险评估技术	是指对风险进行识别、分析和风险评价的方法	主要风险评估方法包括： (1)定性法 基于审计人员的判断把风险简单划分为高、中、低三个等级。 (2)定量法 基于审计人员的判断通过复杂计算对风险进行量化排序。 (3)评分系统 基于对各种风险因素的评价排定审计优先级。该机制所考虑的因素有技术复杂性、现有控制程序的水平以及财务损失大小，可以加权或其他评估方法，最后对所有风险值进行比较并作为审计计划的依据。 (4)判断法 由审计人员根据业务知识、执行管理层指导、历史经验、业务目标和环境因素等进行自主判断。 风险评估的流程包括： (1)风险识别 是指发现、列举和描述风险要素的过程。识别业务目标、信息资产、支撑系统或相关信息资源，风险识别的重点应集中于对组织最为敏感和关键的事项上。 (2)风险分析 是指理解风险的性质和确定风险程度的过程。风险分析需要系统地运用相关信息来确认风险的来源，并对风险进行估计。 (3)风险评价 是指通过对比风险分析结果和风险标准，对识别出的威胁所对应的风险进行评价，决定是否接受或容忍风险及其重要程度的过程，即对识别出的威胁所对应的风险进行评价，风险评价是依据计算所标识的各风险造成损失大小来度量的。常用的计算方法如下： 风险额＝预估每次风险的损失额 * 损失发生的概率 (4)风险处置 风险处置需要选择一个或多个方案来缓释风险，并执行这些方案。在考虑处置风险前，组织应当首先确定风险的可接受标准。对那些决定采用适当控制进行处置的风险，所选择的控制应当能确保降低风险至可接受水平。可考虑的内容包括国内外相关法律、法规的要求；限制条件；组织目标；运营要求和限制条件以及成本有效性等

表 B.1（续）

名称	含义	应用说明
审计抽样技术	是指审计人员在实施审计程序时，从审计对象总体中选取一定数量的样本进行测试，并根据测试结果，推断审计对象总体特征的一种方法	适用范围：适用于时间及成本都不允许对既定总体中的所有交易或事项进行全面审计时。 审计抽样的目的是提供信息，以使审计人员确信能够实现审计目标。 抽样的风险是由于从总体中抽取的样本也许不具有代表性，从而可能导致审计人员的结论出现偏差，导致与对总体进行全面检查的结果不一致。其他风险可能源于抽样总体内部的变异和所选择的抽样方法。 典型的审计抽样包括以下步骤： (1)样本设计 ——确定测试目标； ——定义总体与抽样单元，审计人员应当确保总体的适当性和完整性； ——定义误差构成条件。 (2)选取样本 ——确定样本规模； ——选取样本。 (3)对样本实施审计程序 ——评价样本结果； ——分析样本误差； ——推断总体误差； ——形成审计结论。 抽样时，应充分考虑可用数据的质量，因为抽样数量不足或数据不准确将不能提供有用的结果，因此应根据抽样方法和所要求的数据类型(如为了推断出特定行为模式或得出对总体的推论)选择适应的样本。 对样本的报告应考虑样本量、选择的方法以及基于这些样本和一定置信水平做出的估计。 审计可以采用统计抽样和非统计抽样。 审计人员在对信息系统内部控制进行评估时，应获取相关、可靠、充分的审计证据以支持审计结论完成审计目标，并应充分考虑系统自动控制效果的一致性及可靠性的特点，在选取审计样本时可根据情况适当减少样本量。在系统未发生变更的情况下，可以考虑适当降低审计频率

表 B.1（续）

名称	含义	应用说明
计算机辅助审计技术	是指审计人员在审计过程和审计管理活动中，以计算机为工具执行和完成某些审计程序和任务的一种审计技术	计算机辅助审计技术（CAAT）包括多种工具和技术，如：通用审计软件（GAS）、作业管理软件、高级程序语言、安全工具（如漏洞扫描、入侵检测等）、审计工具（如网络审计、主机审计、数据库审计等）、测评工具（如网络分析检测、系统配置检测、日志分析检测等）、系统运行监测工具（如网络流程、应用进程、CPU 利用率、内存利用率等监测）、系统监控检测工具（如机房测控、服务器监控、软件运行与监控、网站运行监控等）、测试工具、专家系统等。 在准备投入精力、时间和费用来购买或开发 CAAT 前，审计人员应当衡量其成本和收益。 需要考虑的问题包括： ——易操作，包括对现有及未来的审计人员； ——培训需求； ——安装需求； ——编码及维护的复杂性； ——使用的灵活性； ——处理效率（特别是 PC 机上的 CAAT）； ——源数据导入 CAAT 所需的精力； ——保护导入数据的真实性和完整性； ——记录关键处理点所下载数据的时间戳，以支持检查的可信度； ——获得在被审计服务器上安装软件的许可； ——软件的可靠性； ——处理数据的机密性
大数据技术	是指依托大数据平台，开展系统内业务数据或跨系统业务数据的综合比对分析，实现审计从单点向多点、从局部向整体、从离散向连续性等的过渡	大数据时代能够收集和分析组织的所有相关数据，审计模式发生了改变，已从抽样审计模式向总体审计模式发展：即对大数据总体进行多角度的深层次分析，以发现其中隐藏的更具价值的信息及判断总体的特征。 大数据分析技术的特点是全样本分析，并从可视化分析、数据挖掘算法、预测性分析能力、语义引擎、数据质量和数据管理等方面开展深入分析

附 录 C
（资料性附录）
审计报告

C.1 概述

IT 审计报告是 IT 审计监督活动的“交付产品”，是 IT 审计意见的书面文件。

C.2 审计报告的类型

IT 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	——IT 内部控制审计报告 ——IT 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

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，则应拒绝发表意见。

C.3 审计报告的结构内容

IT 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

表 C.2（续）

报告结构	报告内容
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
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论提供较高水平的支持
详细的审计发现和建议	审计人员应当决定在报告中包含哪些审计发现，这应当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应包括哪些内容也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，审计人员应根据重要性的原则，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 19001—2018 质量管理体系 要求

[2] GB/T 20269—2006 信息安全技术 信息系统安全管理要求

[3] GB/T 20984—2007 信息安全技术 信息安全风险评估规范

[4] GB/T 22080—2008 信息技术 安全技术 信息安全管理体系 要求

[5] GB/T 22081—2008 信息技术 安全技术 信息安全管理实用规则

[6] GB/T 22239—2008 信息安全技术 信息系统安全等级保护基本要求

[7] GB/T 24405.1—2009 信息技术 服务管理 第1部分:规范

[8] GB/T 24353—2009 风险管理 原则与实施指南

[9] GB/T 26317—2010 公司治理风险管理指南

[10] GB/T 28827.1—2012 信息技术服务 运行维护 第1部分:通用要求

[11] GB/T 28827.2—2012 信息技术服务 运行维护 第2部分:交付规范

[12] GB/T 28827.3—2012 信息技术服务 运行维护 第3部分:应急响应规范

[13] GB/T 29264—2012 信息技术服务 分类与代码

[14] R/T 0099—2012 证券期货业信息系统运维管理规范

[15] SJ/T 11445.2—2012 信息技术服务 外包 第2部分:数据(信息)保护规范

[16] 信息安全等级保护管理办法.公安部、国家保密局、国家密码管理局、国务院信息工作办公室(公通字〔2007〕43号)2007-06-22.

[17] 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.

[18] 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.

[19] 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)2008-05-22.

[20] 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)2010-04-15.

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

[22] 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(2013年第1号公告)2013-08-20.

[23] 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)2012-02-01.

[24] 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)2003-03-04.

[25] 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)2006-06-06.

[26] 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)2009-06-01.

[27] 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)2008-09-03.

[28] 保险公司信息系统安全管理指引(试行).中国保险监督管理委员会(保监发〔2011〕68号)2011-11-16.

[29] 胡克瑾等.IT审计(第二版)[M]. 电子工业出版社,2004.

[30] 中国注册会计师协会编.企业内部控制审计底稿编制指南[M]. 中国财政经济出版社,2011.

[31] 《CISA Review Manual》 International Information Systems Audit and Control Association (ISACA),2015.

[32] OECD Principles of Corporate Governance. OECD, 2004.

[33] Report of the Committee on the Financial Aspects of Corporate Governance[R]Sir Adrian-Cadbury, London, 1992.

[34] ISACA Cobit5.0 Control Objectives for Information and related Technology, ISACA, April 10, 2012.

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

中 华 人 民 共 和 国
国 家 标 准
信息技术服务 治理
第 4 部分：审计导则
GB/T 34960.4—2017
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲 2 号(100029)
北京市西城区三里河北街 16 号(100045)
网址 www.spc.net.cn
总编室：(010)68533533 发行中心：(010)51780238
读者服务部：(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 2.25 字数 56 千字
2017 年 11 月第一版 2017 年 11 月第一次印刷
*
书号：155066·1-57857 定价 33.00 元

GB/T 34960.4-2017