ICS 35.080
L 77

中华人民共和国国家标准

GB/T 34960.2—2017

信息技术服务　治理
第2部分:实施指南

Information technology service—Governance—
Part 2:Implementation guide

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 2 部分，是第 1 部分的实施指南。

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。

本部分主要起草单位：北京华胜天成科技股份有限公司、上海计算机软件技术开发中心、中国电子技术标准化研究院、上海企源科技有限公司、上海万隆信息技术咨询有限公司、快威科技集团有限公司、四川久远银海软件股份有限公司、辽宁省电子信息产品监督检验院、北京华宇信息技术有限公司、北京北咨信息工程咨询有限公司，广州市金禧信息技术服务有限公司、天津天大康博科技有限公司、广州赛宝认证中心服务有限公司、北京信城通数码科技有限公司、软通动力信息技术(集团)有限公司、北京中扬天成科技有限公司、成都信息化技术应用发展中心、成都勤智数码科技股份有限公司、辽宁北方实验室有限公司、江苏振邦智慧城市信息系统有限公司、北京神州泰岳软件股份有限公司、北京随达信科技公司、神州数码信息服务股份有限公司、上海北塔软件股份有限公司、上海市浦东新区信息化协会、上海翰纬信息管理咨询有限公司、成都安美勤信息技术股份有限公司、北京荣之联科技股份有限公司、上海谷航信息科技发展有限公司、北京易服务信息技术有限公司。

本部分主要起草人：宋俊典、王铮、杨琳、李雪、李鸣、王春涛、张明英、俞文平、孙佩、魏东、侯姗姗、熊健淞、潘蓉、张旸旸、薛君敖、李璐、邱兢、张绍华、宋跃武、温伟军、刘小茵、沈国华、郑晨光、刘玲、杨泉、李刚、但强、董跃、李海涛、夏斌辉、王庆磊、刘文海、马洪杰、徐弢、陆雯珺、郝守勤、杨爽、甘琼、陆雷、张智灵、潘纯峰、左天祖、张荣静、韩佳赟、秦佩君。

信息技术服务　治理
第2部分:实施指南

1　范围

GB/T 34960的本部分提出了信息技术治理(以下简称:IT治理)通用要求的实施指南,分析了实施IT治理的环境因素,规定了IT治理的实施框架、实施环境和实施过程,并明确顶层设计治理、管理体系治理和资源治理的实施要求。

本部分适用于:

a)　建立组织的IT治理实施框架,明确实施方法和过程;

b)　组织内部开展IT治理的实施;

c)　IT治理相关软件或解决方案实施落地的指导;

d)　第三方开展IT治理评价的指导。

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　信息技术服务　治理　第1部分:通用要求

GB/T 22081—2008　信息技术　安全技术　信息安全控制实践指南

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

3　术语和定义

GB/T 34960.1界定的术语和定义适用于本文件。

4　治理实施框架

IT治理实施框架包括治理的实施环境、实施过程和治理域,见图1。

实施环境包括组织的内外部环境和促成因素。

实施过程规定了IT治理实施的方法论,包括统筹和规划、构建和运行、监督和评估、改进和优化。

治理域定义了IT治理对象,包括顶层设计、管理体系和资源。顶层设计包括战略、组织和架构,管理体系包括质量管理、项目管理、投资管理、服务管理、业务连续性管理、信息安全管理、风险管理、供方管理、资产管理和其他管理,资源包括基础设施、应用系统和数据。

组织应结合实施环境的分析,按照实施过程,以治理域为对象,开展IT治理实施。

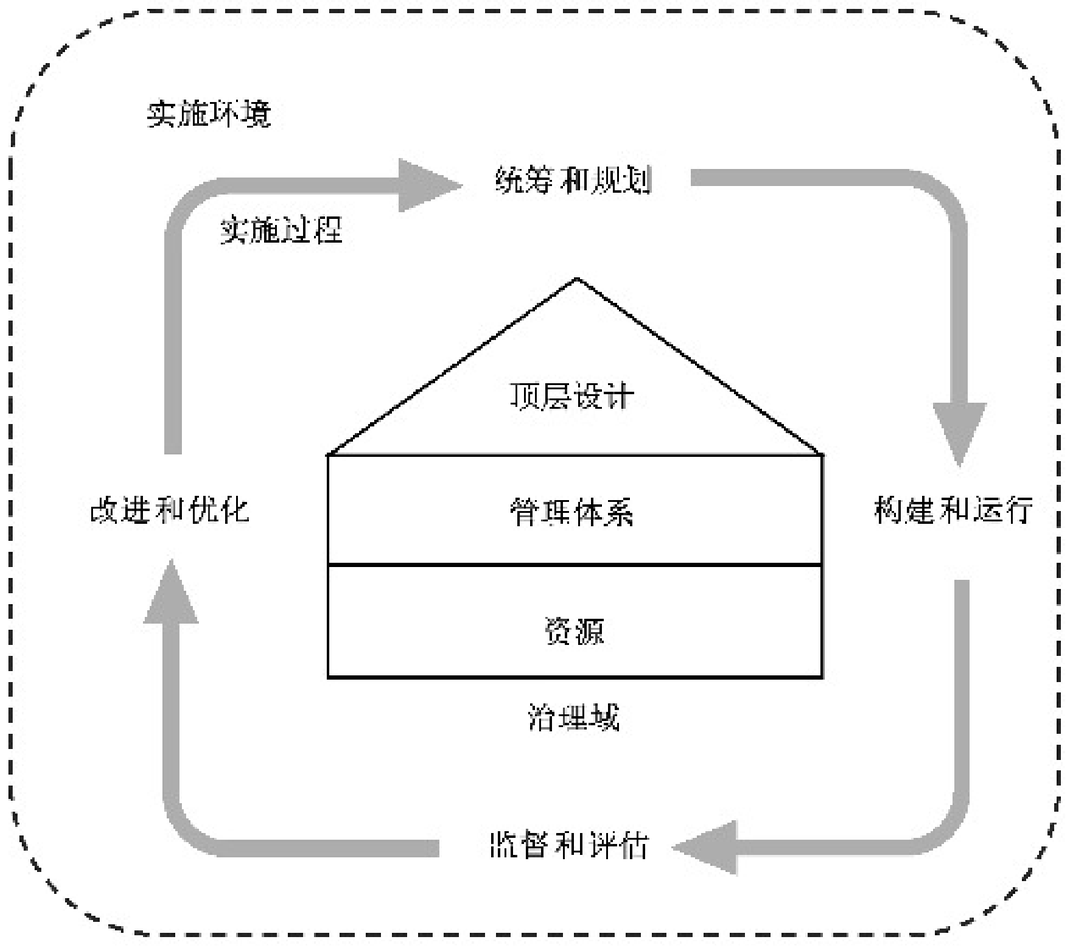

图 1　治理实施框架

5　实施环境

5.1　概述

组织应分析内外部环境的要求，识别 IT 治理的促成因素，以保障 IT 治理的实施。

5.2　内外部环境要求

组织应分析内外部环境要求，明确 IT 治理实施的策略。内外部环境要求包括但不限于：

a）　现行的政策、法律、法规等；

b）　内外部审计、监督、评估等；

c）　组织战略和业务战略的变化；

d）　市场、经济和竞争地位的变化；

e）　新兴技术变革和重大技术变更。

5.3　促成因素

组织应识别 IT 治理实施的促成因素，分析利益相关方的责权利，明确 IT 治理实施的任务和过程。促成因素包括但不限于：

a）　内外部基础信息；

b）　文化、道德规范和行为；

c）　业务需求；

d）　信息技术战略、组织和架构；

e）　信息技术资源和信息技术服务能力；

f）　人员技能和职业能力。

6 实施过程

6.1 概述

IT 治理实施主体应结合实施环境，兼顾创新、协调、绿色、开放、共享的发展理念，分配资源并构建 IT 治理实施过程，明确统筹和规划、构建和运行、监督和评估、改进和优化的目标和基本任务。

6.2 统筹和规划

目标：统筹和规划 IT 治理实施的过程，营造必要的治理环境，做好 IT 治理实施的准备工作。

统筹和规划的基本任务应包括：

a) 明确 IT 治理实施的组织机构、实施主体、职责分工，以及利益相关方的沟通机制；

b) 设计 IT 治理实施框架，明确实施内容、程序和机制；

c) 根据组织战略、业务要求和利益相关方期望，规划 IT 治理实施的目标、方法和范围；

d) 结合信息技术顶层设计、管理体系和资源的治理要求，识别 IT 治理的任务；

e) 建立与 IT 治理实施相适应的路线图和绩效考评体系；

f) 规划 IT 治理实施的绩效评价和审核机制，明确审计监督的相关要求。

6.3 构建和运行

目标：构建 IT 治理实施的管理机制，确保 IT 治理实施的有序运行。

构建和运行的基本任务应包括：

a) 建立 IT 治理实施相关的管理机制，确立实施要点；

b) 制定满足整体规划的构建和运行计划，并按计划实施；

c) 制定 IT 治理实施的工作标准与方法；

d) 建立信息交流与共享途径；

e) 对构建和运行过程进行管理，确保过程可追溯，结果可计量或可评估。

6.4 监督和评估

目标：监督 IT 治理的实施过程，评估 IT 治理实施的符合性和质量。

监督和评估的基本任务应包括：

a) 依据绩效评价和审计要求，对 IT 治理实施过程进行监督；

b) 评估 IT 治理实施团队和人员的能力，必要时可聘请外部团队和人员；

c) 监督和评估 IT 治理实施的适宜性和有效性；

d) 监督和评估顶层设计、管理体系、资源治理要求的实施。

6.5 改进和优化

目标：组织应持续改进 IT 治理实施的过程，提升 IT 治理实施的有效性。

改进和优化的基本任务应包括：

a) 建立 IT 治理实施的改进和优化机制，并对改进和优化过程进行监督；

b) 依据统筹规划的目标和要求，对未达成的指标进行检查和分析；

c) 确定改进措施，制定 IT 治理实施改进计划；

d) 持续推进 IT 治理实施的改进和优化。

7 顶层设计治理的实施

7.1 战略

7.1.1 概述

组织应对 IT 治理的实施环境进行分析和评估，制定信息技术战略，并推进战略规划的实施和改进。

7.1.2 实施环境的评估

组织在评估当前环境和能力过程中，应：

a) 建立实施环境的评估方法和机制；

b) 评估业务战略及组织发展战略；

c) 评估信息技术建设及服务能力；

d) 评估 IT 治理实施的内外部环境和促成因素。

7.1.3 信息技术战略的制定

信息技术战略制定中，应：

a) 考虑组织战略、信息技术对业务的支撑能力；

b) 考虑相关标准、最佳实践、成熟技术和创新建议；

c) 评估信息技术战略与组织战略的一致性，确保其与组织战略相匹配。

7.1.4 战略规划的实施和改进

信息技术战略规划实施和改进时，应：

a) 符合组织战略，并与业务战略目标一致；

b) 建立满足信息技术目标的管理体系；

c) 配置资源以满足战略目标要求；

d) 持续优化和改进信息技术管理体系。

7.2 组织

7.2.1 概述

组织应建立 IT 治理实施的机制和机构，确保治理团队、机构和人员能力满足 IT 治理的要求。

7.2.2 IT 治理机制

组织应明确 IT 治理的授权机制、决策机制和沟通机制。IT 治理机制应：

a) 满足组织的信息技术战略和目标要求；

b) 保证利益相关方理解、接受相应的职责和权利；

c) 确保沟通信息的准确、可靠和有效；

d) 适应 IT 治理体系持续改进的方法和策略。

7.2.3 IT 治理机构

组织应根据战略和业务需求，建立 IT 治理机构，包括但不限于信息技术战略委员会、信息技术管理和服务机构、业务部门、风险管理部门、审计监督部门等：

a) 明确 IT 治理机构的职能、岗位和职责，明确角色和职责；
b) 宜建立首席信息官制度，参与组织决策；
c) 建立互信、高效、目标一致的 IT 治理实施团队；
d) 确保 IT 治理实施人员具备业务及信息技术知识，并不断得到提升；
e) 建立 IT 治理实施人员的培养机制。

7.3 架构

7.3.1 概述

组织应建立满足企业架构的 IT 架构、架构管理策略和管理体系，满足 IT 治理的要求。

7.3.2 建立

信息技术架构的建立，应：
a) 与组织战略目标、IT 治理目标保持一致；
b) 满足信息技术战略的目标和要求；
c) 满足功能集成、信息集成及数据共享等应用需求。

7.3.3 管理

信息技术架构管理机制的制定，应：
a) 满足 IT 治理战略规划的要求；
b) 评估架构设计的合理性、先进性和开放性；
c) 持续改进和优化架构及其管理机制。

8 管理体系治理的实施

8.1 质量管理

8.1.1 概述

组织应建立信息技术服务及产品质量管理体系，明确质量管理的职责和权限、提供资源保障并持续改进和优化。

8.1.2 质量管理体系的建立

信息技术服务及产品质量管理体系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。质量管理体系的建立，应：
a) 明确质量管理体系的过程，以及质量管理体系应用的策略；
b) 制定质量管理体系的实施方法和措施；
c) 制定质量管理职责和权限的划分机制，并提供资源保障；
d) 定义质量管理体系各个过程的输入和输出；
e) 分析质量管理体系各个过程的顺序和相互作用；
f) 分析非预期输出或过程失效所带来的风险；
g) 明确质量准则、测量及评价方法，确保质量体系有效运行和控制；
h) 监测、分析质量管理体系的过程，确保过程符合预期。

8.1.3 质量管理责权的明确

质量管理责权的明确包括责任人的明确、职责权限的沟通和理解，内外部沟通机制的建立。质量管理责权的明确，应：

a） 确保质量管理责权与管理体系符合性；

b） 确保质量管理体系各个过程相互作用并产生预期结果；

c） 向最高管理者报告质量管理体系的绩效和改进需求；

d） 提升组织满足顾客需求的意识；

e） 明确内外部沟通的内容、时机和对象。

8.1.4 质量管理的资源保障

质量管理的资源保障包括人力资源、相应的教育培训、基础设施资源支撑、工作环境和条件等，应：

a） 持续改进和完善质量管理团队，开展人员教育和培训，提升人员意识和技能；

b） 确保质量管理所需的基础设施支撑，包括建筑物及相关设施设备、软硬件、通信和系统；

c） 明确质量管理体系所需的工作环境，包括物理的、社会的、心理等环境因素。

8.1.5 质量管理体系的持续改进

质量管理体系的持续改进包括监视、测量、分析和改进等过程，应：

a） 证实信息技术相关质量需求的符合性；

b） 确保信息技术质量管理体系的符合性；

c） 持续改进信息技术质量管理体系的有效性。

8.2 项目管理

组织应建立项目管理机制，制定项目计划，确定项目范围，建立成本、进度和质量控制机制，建立和维护项目管理的流程和方法，统计分析项目的完成情况，并评估绩效。项目管理的实施，应：

a） 定义项目管理的总体策略和原则，建立项目管理制度及流程；

b） 制定详细的项目计划，识别项目范围，估算项目规模、工作量及成本；

c） 组建项目团队，与利益相关方明确项目计划并达成共识；

d） 明确项目管理的要求，包括进度管理、配置管理、问题管理、风险管理、质量管理、沟通管理、评价管理、成本管理等具体要求和策略；

e） 对项目实施进行跟踪和监督，包括需求的变更管理、交付物的配置管理、风险跟踪分析及管理、成本管理、沟通管理等；

f） 明确项目质量保证策略、过程和活动，解决并跟踪质量保证活动中发现的不符合问题。

8.3 投资管理

8.3.1 概述

组织应根据投资目标和规划，合理安排资金投放结构，科学确定投资项目，建立投资的拟定方案、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等。

8.3.2 投资管理规划

组织应建立信息技术投资规划，并对其进行统筹管理，应：

a） 明确信息技术投资的目的；

b） 制定信息技术投资规划；

c） 明确信息技术投资的原则，保证其符合组织战略、业务战略和信息技术战略；

d） 建立信息技术投资管理组织，明确投资决策管理、风险管理、监督管理等机构的责任和权力。

8.3.3 投资管理程序和方法

组织应制定信息技术投资的管理程序和方法，应：

a） 确定投资项目，拟定投资方案；

b） 开展项目可行性研究，论证投资方案；

c） 编制投资计划并按规定程序报批；

d） 按照规定的权限和程序，对投资项目进行审批；

e） 实施投资计划，指定专职人员进行跟踪管理；

f） 按照规定流程和方法对到期的投资项目进行处置。

8.3.4 投资计划与项目管控

组织应制定信息技术的投资计划，推进实施并进行管控，应：

a） 制定信息技术投资计划，包括资金规模、投资内容、项目进度、质量标准与要求等要求；

b） 实施 IT 投资计划，监督和管控项目日常运作、合规审查等，确保项目的立项、实施进度、项目质量、项目费用等合规性；

c） 按照投资计划的总体要求，保质、保量并在预算范围内完成投资项目。

8.4 服务管理

组织应建立信息技术的服务管理机制，控制服务实施的风险，提升服务管理能力，并定期评价服务绩效。应：

a） 建立、实施、监督、测量、保持和改进信息技术服务管理机制，实现服务管理能力的提升；

b） 明确组织内的相关职责、权限，并得到有效沟通；

c） 识别并提供建立、实施、保持和持续 IT 服务管理机制所需要的基础条件和内外部资源；

d） 以服务管理机制有效运行和客户满意为目标，对组织的信息技术服务进行策划、设计、部署、运营、验收、改进和终止；

e） 定期评价信息技术服务的绩效和信息技术服务管理机制的有效性。

8.5 业务连续性管理

8.5.1 概述

组织应构建信息技术应急响应和灾难恢复机制，明确信息技术管理程序、资源保障，制定应急响应预案和灾难恢复方案并持续改进，定期开展培训、测试和演练等保障活动，以降低信息技术实现价值交付时的风险。

8.5.2 业务连续性管理框架

组织应建立业务连续性管理框架，包括业务连续性管理程序、程序维护和评审、连续性恢复后评价，并把业务连续性植入组织文化，应：

a） 制定业务连续性策略、目标和范围；

b） 制定和维护业务连续性管理程序；

c） 制定和执行应急响应机制；

d) 演练、测试、评价、维护和改进连续性计划；

e) 实施业务连续性恢复后评价。

8.5.3 应急管理

组织应建立应急事件的管理程序，并保证程序得到有效实施。应：

a) 建立应急响应组织，制定应急响应制度；

b) 识别信息技术服务活动中可能出现的风险；

c) 划分应急事件级别，制定应急预案，开展培训和演练；

d) 开展日常监测，对应急事件进行核实和评估；

e) 启动应急预案，对应急事件进行处理和跟踪，及时通报并对结果进行评价；

f) 分析应急事件发生原因、处理过程和结果，持续改进应急预案。

8.5.4 灾难恢复

组织宜建立灾难应对措施和恢复方案，保证信息系统的高可用性和业务恢复能力，应：

a) 定义所需防范的灾难范围，开展业务影响分析；

b) 明确需要防范的灾难类型；

c) 依据业务关键程度，设定灾难容忍时间指标；

d) 风险结合成本控制，平衡等级和业务连续性的关系；

e) 开展测试和演练，完善业务连续恢复方案。

8.6 信息安全管理

8.6.1 概述

组织应制定信息安全管理目标、方针和策略，建立信息安全组织并明确责任，制定信息安全管理制度，定期开展信息安全培训，确保制度落实。组织宜参照 GB/T 22081—2008 开展信息安全管理实施和持续改进。

8.6.2 信息安全策略

组织应制定信息安全策略，应：

a) 制定信息安全的目标、原则和范围；

b) 明确组织的信息安全策略、标准和符合性要求等；

c) 明确信息安全管理人员的职责；

d) 与利益相关方沟通信息安全策略。

8.6.3 信息安全职责分配

组织应建立信息安全的组织机构，并明确职责和任务，应：

a) 明确信息安全管理机构和责任人，负责组织的信息安全实施；

b) 明确信息资产的具体责任人，负责相应信息资产的日常安全；

c) 确保信息安全的职责被正确地履行；

d) 对信息安全职责分配及要求予以清晰的规定，并形成文档。

8.6.4 信息安全管理制度

组织应建立信息安全管理制度，包括但不限于：

a） 内外部人员安全管理；
b） 保密制度；
c） 用户及权限管理；
d） 系统开发、运维安全管理；
e） 系统定级与测评；
f） 网络安全管理；
g） 设备与环境安全管理；
h） 数据与介质管理。

8.6.5 信息安全教育和培训

组织应按计划开展信息安全教育和培训，包括但不限于：
a） 信息安全意识培训；
b） 组织信息安全策略培训；
c） 信息安全管理制度培训；
d） 安全要求、法律职责、业务控制等相关培训；
e） 信息安全设施的操作和使用培训等。

8.7 风险管理

组织应建立信息技术风险管理机制，制定信息技术风险管理原则、目标和策略，建立管理制度和组织，明确责任人、角色和职责，识别、分析、评价、处置信息技术风险，提升风险应对能力，确保风险降低到组织可接受的程度，应：
a） 制定风险管理策略和目标，明确风险偏好及风险容忍程度；
b） 综合考虑风险管理原则，包括但不限于全面管理原则、系统管理原则、动态管理原则；
c） 组织应建立风险管理机制，明确风险管理责任人、角色和职责；
d） 确定风险识别、分析、评价方法；
e） 制定风险管理与审批流程；
f） 监控风险管理目标，并跟踪、分析和改进风险管理。
g） 建立信息技术风险管理流程，包括但不限于风险来源分析、风险识别、风险监控、风险记录、风险评估与分析、风险量化与处理、风险管理效果评价等。

8.8 供方管理

8.8.1 概述

组织应建立供方管理机制，明确供方管理的职责、流程和方法，建立供方评估机制，保护组织的商业秘密和知识产权，以及组织所涉及的个人隐私。

8.8.2 供方管理制度

组织建立供方管理制度，应：
a） 制定供方分类方法和评价标准；
b） 制定供方管理流程；
c） 制定供方管理改进机制。

8.8.3 供方识别和选择

组织识别和选择合适的供方，应：

a） 识别建立供方列表，并进行分类；
b） 根据供方评估标准进行评估；
c） 对关键供方进行现场和内部管理情况评审。

8.8.4 供方服务管理

组织对供方的服务进行管理，应：
a） 监督供方的服务过程；
b） 评审供方服务交付质量；
c） 制定供方持续改进计划。

8.8.5 供方退出管理

组织对供方的退出进行管理，应：
a） 建立供方退出机制；
b） 制定供方退出时的应对策略。

8.9 资产管理

8.9.1 概述

组织应建立信息技术资产应用、资产财务、资产有效性的管理体系，并对管理内容进行关联。

8.9.2 资产应用管理

建立完善的资产应用管理制度，覆盖计划、采购、部署、管理、报废等环节，应：
a） 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；
b） 明确资产管理人员的相关职责；
c） 明确资产获取方式；
d） 制定报价管理流程，根据采购的规模对供应商选择进行约束；
e） 建立资产部署管理的政策和流程，统一由被授权人员进行资产部署；
f） 管理、记录并解决最终用户在资产应用过程中遇到的事件和问题；
g） 建立资产的处置和报废流程，明确资产报废的条件并做处置和报废记录；
h） 将资产管理相关计划和内容纳入组织信息化总体战略目标中，定期进行审阅和修正。

8.9.3 资产财务管理

建立资产财务管理制度，优化资产应用成本，应：
a） 建立资产分类目录，对关键资产进行识别；
b） 将资产纳入财务管理的范围，形成台账；
c） 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；
d） 定期对资产进行盘点和抽查，更新资产清单，做到账实相符；
e） 结合资产应用成效，制作优化方案和报告，定期和财务部门沟通，以优化资产应用成本。

8.9.4 资产有效性管理

维护资产的授权和许可协议，降低法律法规风险，应：
a） 实施信息技术资产的许可证管理；
b） 定期评审信息技术资产管理的符合性和合规性；

c) 定期审核软件资产依从性，统计组织现有的软件资产状况，分析软件许可需求并进行比对；
d) 核对信息技术资产大规模变更时（如：硬件批量升级、软件批量升级或部署）的部署、使用许可清单，审核资产相关的依从性；
e) 审核组织架构变更、重组等情况下的软件资产及其体系的依从性，并持续改进。

8.10 其他管理

对于本部分未明确的变更管理、预算管理、需求管理、绩效管理等其他信息技术管理体系，组织实施治理时，宜依据相关的标准、规范，制定相应的管理策略、机制和方法。

9 资源治理的实施

9.1 基础设施

9.1.1 概述

组织应制定信息技术基础设施的规划，建立基础设施建设、采购、实施和运维机制，制定基础设施管理策略和方法，评估、指导、监督和改进基础设施相关的管理机制和服务能力。

9.1.2 规划设计

组织应开展基础设施规划设计，满足日常运行、维护管理、维护成本和人力资源需求，应：
a) 开展可行性分析，结合基础设施的可用性和连续性要求，确定资金来源和规模；
b) 参照资产管理相关标准，对基础设施的运行生命周期进行管理；
c) 明确管理与执行、实施与运维的分工和界面，明确在各阶段的关键节点和任务；
d) 理解和收集需求，确定基础设施、设备的功能和技术要求，制定需求评审、审批和变更流程；
e) 基础设施的设计应符合绿色、环保、节能理念，具备扩展性，满足业务需求。

9.1.3 建设实施

组织应制定基础设施建设实施的总体方案，按项目管理计划，完成系统设计、系统部署、系统测试、系统验收和系统上线活动，应：
a) 明确项目管理团队、项目目标、监控机制和管理流程；
b) 制定实施方案，明确基础设施的技术架构、网络拓扑、部署方式、测试要求；
c) 制定设施采购和部署计划，明确实施责任，确定采购、部署、安装和测试内容；
d) 制定测试方案，明确测试人员、测试环境要求和测试工具，跟踪测试过程；
e) 验收阶段，根据实施方案进行基础设施的功能、性能、控制要求的验收测试；
f) 评审实施方案和计划，应符合国家相关规范和标准；
g) 根据实施性质制定新旧系统转换的应急预案和恢复计划。

9.1.4 运行维护

组织应建立基础设施的运行与维护管理机制，确保信息系统持续稳定运行。
a) 建立运行维护的能力体系，确保运行维护的能力；
b) 通过策划、实施、检查和改进，实现运维能力的提升；
c) 配备具有运行维护服务能力的人员、资源，满足信息系统运行维护需求；
d) 具备与运行维护相适应的产品、技术、工具和方法；
e) 建立运行维护管理过程，包括但不限于：服务级别管理、服务报告、事件管理、问题管理、配置管

理、变更管理、发布管理、信息安全管理；

f) 对已按照 GB/T 28827.1—2012 要求建立运行维护管理的组织，宜按照本部分的要求对已建立的内容实施改进。

9.2 应用系统

9.2.1 概述

组织应建立信息技术应用系统设计、开发、变更和测试的保障机制，保证功能、性能和安全等满足设计需求，制定应用系统上线、迁移、新旧系统切换、应急预案等相关的策略、制度和保障机制，评估、指导、监督和改进应用系统管理机制和服务能力。

应用系统运行维护的治理实施，可参考基础设施运行维护的治理实施。

9.2.2 规划设计

组织在实施应用系统规划设计时，应：

a) 选择并制定满足业务需求的应用系统规划设计方案，包括但不限于信息技术战略、架构、技术、管理项目组合、自建或外购决策、信息安全策略和标准、内部控制规划和审计规划；

b) 开展应用系统的可行性分析，考虑优势和劣势，识别机会和威胁，定义投资组合，确定资金来源及可用性等；

c) 确定应用系统的功能和技术要求，制定需求评审、审批和变更流程；

d) 制定实施方案，包括但不限于功能模块、技术路线、网络拓扑、部署方式等；

e) 评审应用系统规划设计的合规性和一致性。

9.2.3 建设实施

组织应根据总体方案和实施方案，按项目管理计划，开展应用系统的建设实施时，应：

a) 建立信息系统建设实施的验证机制，确保与总体架构一致，满足业务需求；

b) 明确应用系统建设实施的目标，明确监控机制和管理流程；

c) 开发阶段，建立开发规范和制度，并对软件进行版本管理；

d) 测试阶段，制定测试计划，跟踪测试过程，开展测试分析并执行验收测试；

e) 验收阶段，开展系统功能、性能、控制和安全性要求的验收；

f) 上线阶段，制定系统上线计划、新旧系统转换方案、应急预案、数据迁移计划和恢复计划；

g) 明确建设实施完成后的工作交接机制和交接内容。

9.3 数据

9.3.1 概述

组织应明确数据治理框架、建立数据治理的机构和管理机制，完善数据治理的生命周期。

9.3.2 数据治理框架

数据治理框架的实施包括战略、任务、框架、范围、促成因素和环境等，应：

a) 明确数据战略文化和思维，评估自身数据治理能力；

b) 建立数据治理机构、明确团队和人员，以及其职责和权利；

c) 定义数据质量业务规则，持续度量和监控数据质量；

d) 明确数据资产使用过程中的认证、授权、访问和审计等机制。

9.3.3 数据治理的组织管理

组织应建立数据治理决策、授权和控制机制等机制，应：

a) 建立职责分配模型，明确组织架构、职责及角色；

b) 明确数据治理的绩效管理和评估机制；

c) 建立有效的管理体系，配备合理的资源；

d) 建立元数据、主数据管理的框架、方法和标准；

e) 建立数据质量、安全、隐私、合规等保障机制。

9.3.4 数据治理的过程管理

组织应建立数据生命周期管理和服务能力体系，并进行评估、指导、监督和改进。应：

a) 明确数据治理目标，利益相关方的愿景等；

b) 分析数据治理的范围和流程，设计步骤和实施阶段，形成数据治理路线图；

c) 识别环境和促成因素，形成需求调研及分析报告；

d) 评估组织内外数据应用水平现状，形成评估分析报告；

e) 制定数据治理的策略、流程、制度和考核指标体系；

f) 监督数据治理的实施、评估数据治理能力和水平，并持续改进。

参 考 文 献

[1] GB/T 19001—2008 质量管理体系 要求

[2] GB/T 19668.1—2014 信息技术服务 监理 第1部分:总则

[3] GB/T 20269—2006 信息安全技术 信息系统安全管理要求

[4] GB/T 20984—2007 信息安全技术 信息安全风险评估规范

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

[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 24353—2009 风险管理 原则与实施指南

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

[9] GB/T 26317—2010 公司治理风险管理指南

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

[11] 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

[12] JR/T 0099—2012 证券期货业信息系统运维管理规范

[13] 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

[14] 《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

[15] 《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

[16] 《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.

[17] 《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.

[18] 《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.

[19] ISO/IEC 38500 Governance of information technology for the organization

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

[21] Report of the Committee on the Financial Aspects of Corporate Governance[R]. Sir AdrianCadbury: London, 1992.

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