

中华人民共和国国家标准

GB/T 34960.1—2017

信息技术服务 治理 第1部分:通用要求

Information technology service—Governance—
Part 1: General requirements

2017-11-01 发布

2018-02-01 实施

中华人民共和国国家质量监督检验检疫总局 发布
中国国家标准化管理委员会

目 次

前言	I
引言	II
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 治理原则	2
5 信息技术治理模型	2
6 信息技术治理框架	3
7 顶层设计的治理	3
7.1 战略	3
7.2 组织	4
7.3 架构	4
8 管理体系的治理	4
8.1 概述	4
8.2 质量管理	4
8.3 项目管理	4
8.4 投资管理	4
8.5 服务管理	5
8.6 业务连续性管理	5
8.7 信息安全管理	5
8.8 风险管理	5
8.9 供方管理	5
8.10 资产管理	5
8.11 其他管理	5
9 资源的治理	6
9.1 概述	6
9.2 基础设施	6
9.3 应用系统	6
9.4 数据	6
参考文献	7

前 言

GB/T 34960《信息技术服务 治理》分为以下 5 个部分：

- 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 1 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、上海万隆信息技术咨询有限公司、北京华胜天成科技股份有限公司、四川久远银海软件股份有限公司、北京慧点科技股份有限公司、广州赛宝认证中心服务有限公司、用友软件股份有限公司、北京久其软件股份有限公司、上海企源科技有限公司、联通系统集成有限公司、上海翰纬信息管理咨询有限公司、成都信息化技术应用发展中心、上海北塔软件股份有限公司、辽宁省电子信息产品监督检验院、中金数据系统有限公司、北京信城通数码科技有限公司、快威科技集团有限公司、北京富通金信计算机系统服务有限公司、北京护航科技有限公司、软通动力信息技术(集团)有限公司、成都勤智数码科技股份有限公司、北京荣之联科技股份有限公司、上海瀚昌信息科技发展有限公司、东华软件股份公司、北京神州泰岳软件股份有限公司、北京随达信科技有限公司、天津天大康博科技有限公司、神州数码信息服务股份有限公司、南威软件股份有限公司、上海市浦东新区信息化协会、广州市金禧信息技术服务有限公司、北京中扬天成科技有限公司、中国电信上海理想信息产业(集团)有限公司、上海谷航信息科技发展有限公司。

本部分主要起草人：张绍华、张明英、宋跃武、俞文平、宋俊典、李鸣、李刚、李璐、蔡震宇、张旻旻、孙佩、潘蓉、刘小茵、邱兢、但强、杨琳、朱圣哲、刘越男、向纪兰、徐弢、魏东、徐飞、刘玲、王春涛、李锋、杨泉、董跃、潘纯峰、肖建一、王庆磊、刘文海、郑晨光、李娜、王铮、沈国华、王永军、甘琼、丁富强、吴越、陆雷、杨爽、熊健淞、左天祖。

引 言

随着各行业、各领域信息化的迅速发展,信息技术已成为大部分组织开展业务的有效支撑。为了促进组织有效、高效、合理地利用信息技术,有必要在组织的信息化规划、建设、运营和维护过程中,提出信息技术相关的治理要求,从而实现战略一致、风险可控、运营合规和绩效提升的目标。

GB/T 34960 的本部分参照了 GB/T 26317—2010《公司治理风险管理指南》和《OECD 公司治理原则》,引入了 ISO/IEC 38500《组织的信息技术治理》的模型,融合了《企业内部控制基本规范》及相关行业监管和风险控制要求,旨在指导组织建立信息技术治理体系。

信息技术服务 治理 第1部分:通用要求

1 范围

GB/T 34960 的本部分规定了信息技术治理(以下简称:IT 治理)的模型和框架,规定了实施 IT 治理的原则,以及开展信息技术顶层设计、管理体系和资源的治理要求。

本部分适用于:

- a) 建立组织的 IT 治理体系,并实施自我评价;
- b) 开展信息技术审计;
- c) 研发、选择和评价 IT 治理相关的软件或解决方案;
- d) 第三方对组织的 IT 治理能力进行评价。

各级各类信息化主管部门可根据法律法规、部门规章的要求,使用本部分对所管辖各类组织的 IT 治理提出要求,并进行评估、指导和监督。

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 19001 质量管理体系 要求
- GB/T 19668.1 信息技术服务 监理 第1部分:总则
- GB/T 28827.1 信息技术服务 运行维护 第1部分:通用要求
- GB/T 28827.2 信息技术服务 运行维护 第2部分:交付规范
- GB/T 28827.3 信息技术服务 运行维护 第3部分:应急响应规范
- SJ/T 11445.2 信息技术服务 外包 第2部分:数据(信息)保护规范

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

治理主体 governance body

评估、指导、监督组织 IT 治理的人或团体。

3.3

治理要素 governance element

实施 IT 治理应关注的关键治理对象或过程。

3.4

治理域 governance domain

按照特定层次、功能划分的治理范围,是治理要素的集合。

3.5

信息技术架构 information technology architecture

为满足组织信息技术战略、管理体系、业务发展而建立的应用和支撑体系。

3.6

能力 capability

完成任务或履行角色责任所需知识、技能、经验及其他相关资源的组合。

4 治理原则

组织应按本部分建立 IT 治理体系,形成文件并实施、持续改进并优化,确保信息技术应用的绩效和符合性。组织应遵循以下治理原则:

- a) IT 治理是公司治理的组成部分,最高决策者为 IT 治理最终责任人,决策层为 IT 治理主体;
- b) 建立 IT 治理机构,成员至少包括内部监督部门、重要业务部门和信息技术部门;
- c) 明确风险偏好和风险容忍度,防范因违规造成的重大财务和声誉损失、监管处罚、法律制裁等;
- d) 确保利益相关方理解预期收益、支持 IT 投资,接受可能存在的风险及应对措施;
- e) 建立信息技术应用的战略、制度、文化和创新机制,支撑业务模式变革、技术进步和管理提升。

5 信息技术治理模型

IT 治理模型包含治理的内外部要求、治理主体、治理方法,以及信息技术及其应用的管理体系,见图 1。

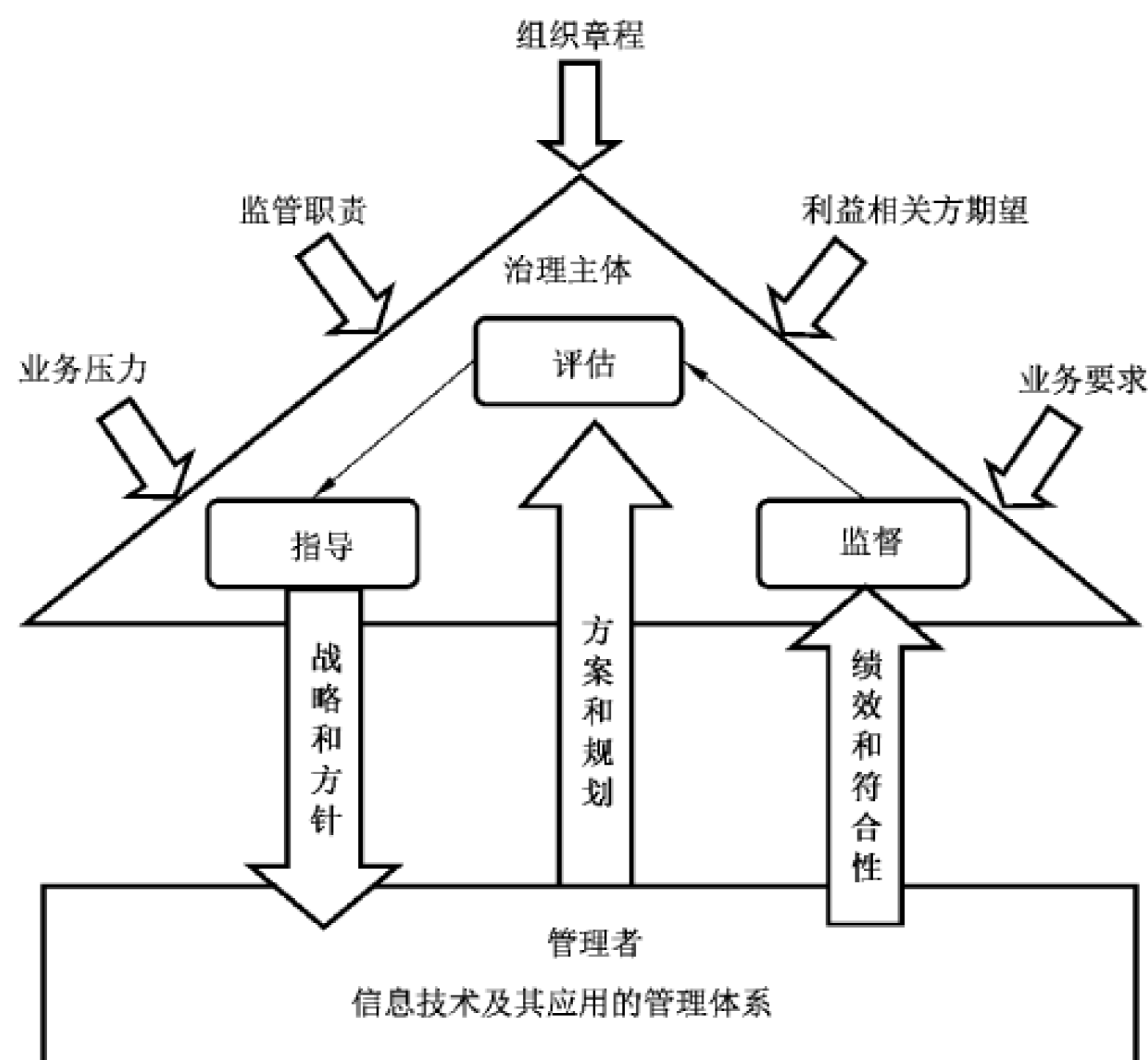


图 1 治理模型

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。

治理主体应通过信息技术战略和方针,指导管理者对信息技术及其应用的管理体系进行完善,并对信息技术相关的方案和规划进行评估、对信息技术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。

6 信息技术治理框架

IT 治理框架包含信息技术顶层设计、管理体系和资源三大治理域,每个治理域由如下若干治理要素组成,见图 2。

- 顶层设计治理域包含信息技术的战略,以及支撑战略的组织 and 架构;
- 管理体系治理域包含信息技术相关的质量管理、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;
- 资源治理域包含信息技术相关的基础设施、应用系统和数据。

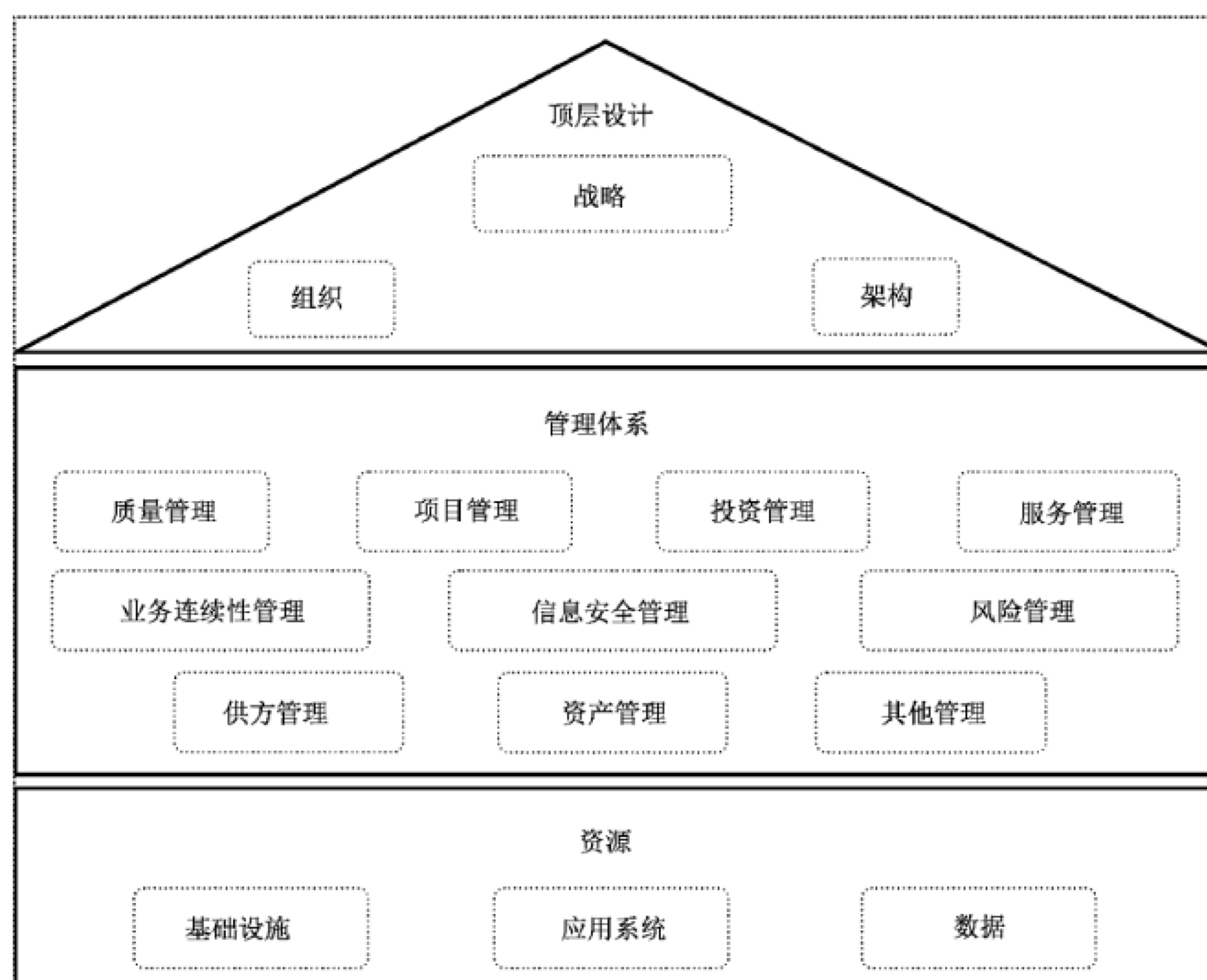


图 2 治理框架

7 顶层设计的治理

7.1 战略

IT 治理主体应指导、评估和监督信息技术战略,明确信息技术战略目标并持续改进。至少应:

- 评估信息技术内外部环境、制定与组织战略一致的信息技术战略;
- 指导和评估信息技术规划和方案,并促进其管理体系的持续优化和改进;
- 明确风险偏好、符合性、绩效和审计等要求,并进行评估和监督。

7.2 组织

IT 治理主体应指导、评估和监督信息技术组织机制,并确保利益相关方的理解和支持。至少应:

- a) 指导信息技术组织架构的建立和完善,明确授权、决策和沟通机制,并进行评估和监督;
- b) 营造适宜于 IT 治理的组织文化;
- c) 提升人员的 IT 治理意识、专业胜任能力,定期开展相关教育培训。

7.3 架构

IT 治理主体应指导、评估和监督信息技术架构,支撑信息技术战略目标的实现。至少应:

- a) 指导信息技术架构的建立,并对规划、设计、实施、服务等过程进行评估和监督;
- b) 评估信息技术发展内外部环境的变化,并对信息技术架构进行持续改进;
- c) 建立与信息技术架构相适应的管理体系,并进行评估和持续改进。

8 管理体系的治理

8.1 概述

治理主体应从完整性、有效性、适宜性、符合性、成本效益和一致性等视角,指导管理者遵循计划、执行、检查、改进(PDCA)的方法,提出信息技术管理体系的治理要求,持续改进和优化信息技术管理体系。

8.2 质量管理

组织宜依据 GB/T 19001 管理信息技术相关产品和服务的质量。至少应:

- a) 建立质量管理体系,编制质量手册,并对体系文件进行控制;
- b) 定义质量管理的职责和权限,并确保质量管理体系的有效沟通;
- c) 提供质量管理的资源保障,包括人力资源、工作环境和制度等;
- d) 监视和测量产品及服务实现的过程和结果,并进行持续改进。

8.3 项目管理

组织应建立项目管理机制。至少应:

- a) 制定项目计划;
- b) 建立项目范围、成本、进度、变更和质量控制机制;
- c) 建立和维护项目管理的流程和方法;
- d) 统计分析项目的完成情况,并评估绩效。

8.4 投资管理

组织应建立信息技术投资管理机制。至少应:

- a) 明确信息技术投资的目的及原则;
- b) 建立信息技术投资管理组织,明确责任人、角色和职责;
- c) 明确信息技术投资管理的程序和方法;
- d) 制定并实施信息技术投资计划;
- e) 对信息技术投资项目进行管控。

8.5 服务管理

组织应对信息技术服务生命周期进行管理。至少应：

- a) 建立与服务运行目标一致的流程和方法；
- b) 规划和设计信息技术服务,制定信息技术服务计划；
- c) 管理和控制服务实施过程中的质量、风险和变更等；
- d) 定期评价信息技术服务绩效。

8.6 业务连续性管理

组织应构建信息技术应急响应和灾难恢复机制。至少应：

- a) 明确信息技术管理程序、资源保障；
- b) 制定应急响应预案和灾难恢复方案并持续改进；
- c) 定期开展培训、测试和演练等保障活动。

8.7 信息安全管理

组织应制定信息安全管理机制。至少应：

- a) 制定信息安全管理目标、方针和策略；
- b) 建立信息安全管理组织,明确责任人、角色和职责；
- c) 建立信息安全管理流程和控制措施；
- d) 定期开展信息安全宣传、教育和培训。

8.8 风险管理

组织应建立信息技术风险管理机制,至少应：

- a) 制定风险管理目标和策略；
- b) 建立信息技术风险管理制度；
- c) 建立信息技术风险管理组织,明确责任人、角色和职责；
- d) 建立信息技术风险管理流程,识别、分析、评价、处置信息技术风险。

8.9 供方管理

组织应建立供方管理机制。至少应：

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

8.10 资产管理

组织宜参照资产管理相关标准,建立资产管理体系并对其生命周期进行管理,至少应：

- a) 建立资产的计划、采购、部署、管理、报废制度；
- b) 建立资产分类目录和台账,定期对资产进行盘点和抽查；
- c) 维护资产的授权和许可协议,降低法律法规风险。

8.11 其他管理

对于本部分未明确的其他信息技术管理体系,组织在提出治理要求时,宜依据相应的标准规范,包含但不限于：

- a) GB/T 19668.1—2014;
- b) GB/T 28827.1—2012;
- c) GB/T 28827.2—2012;
- d) GB/T 28827.3—2012;
- e) SJ/T 11445.2—2012。

9 资源的治理

9.1 概述

治理主体应结合信息系统总体架构,建立资源的目录体系,从基础设施、应用系统和数据 3 个层次,提出信息技术资源及其应用的治理要求,并进行评估、指导、监督和改进。

9.2 基础设施

组织应明确信息技术基础设施相关环境、网络通信、硬件设备和基础软件的治理要求。至少应:

- a) 制定基础设施的规划,以支撑战略发展、满足业务需要;
- b) 建立基础设施建设、采购、实施和运维机制,制定相应的管理策略和方法;
- c) 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。

9.3 应用系统

组织应明确应用系统规划立项、设计开发、集成实施和运行维护的治理要求。至少应:

- a) 确保应用系统规划满足组织战略和业务目标,评估、监督应用系统的绩效和符合性;
- b) 建立应用系统设计、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;
- c) 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;
- d) 评估、指导、监督和改进应用系统管理机制及服务能力。

9.4 数据

组织应明确数据的治理要求,制定数据治理的战略,明确数据治理任务。至少应:

- a) 构建数据治理的框架,确定数据治理的范围、促成因素和环境;
- b) 建立数据治理的组织,明确数据治理的决策、授权和控制机制;
- c) 制定满足业务需求的元数据规范、数据质量标准,保障数据的唯一性、权威性和有效性;
- d) 建立数据安全、隐私、合规等保障机制,明确数据的使用范围、责权利等相关要求;
- e) 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。

参 考 文 献

- [1] GB/T 20269—2006 信息安全技术 信息系统安全管理要求
- [2] GB/T 20984—2007 信息安全技术 信息安全风险评估规范
- [3] GB/T 22080—2008 信息技术 安全技术 信息安全管理体系 要求
- [4] GB/T 22081—2008 信息技术 安全技术 信息安全管理体系 实用规则
- [5] GB/T 22239—2008 信息安全技术 信息系统安全等级保护基本要求
- [6] GB/T 24353—2009 风险管理 原则与实施指南
- [7] GB/T 24405.1—2009 信息技术 服务管理 第1部分:规范
- [8] GB/T 26317—2010 公司治理风险管理指南
- [9] GB/T 29264—2012 信息技术服务 分类与代码
- [10] JR/T 0099—2012 证券期货业信息系统运维管理规范
- [11] 《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年5月22日
- [12] 《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年6月6日
- [13] 《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年6月1日
- [14] 《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年9月3日
- [15] 《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年11月16日
- [16] ISO/IEC 38500 组织的信息技术治理(Governance of information technology for the organization)
- [17] OECD Principles of Corporate Governance. OECD, 2004.
- [18] Report of the Committee on the Financial Aspects of Corporate Governance. Sir Adrian-Cadbury, London, 1992, ISBN0852589131.
- [19] ISACA Cobit5.0 Control Objectives for Information and related Technology, ISACA, April 10, 2012.
-

中 华 人 民 共 和 国
国 家 标 准
信息技术服务 治理 第 1 部分：通用要求
GB/T 34960.1—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.org.cn

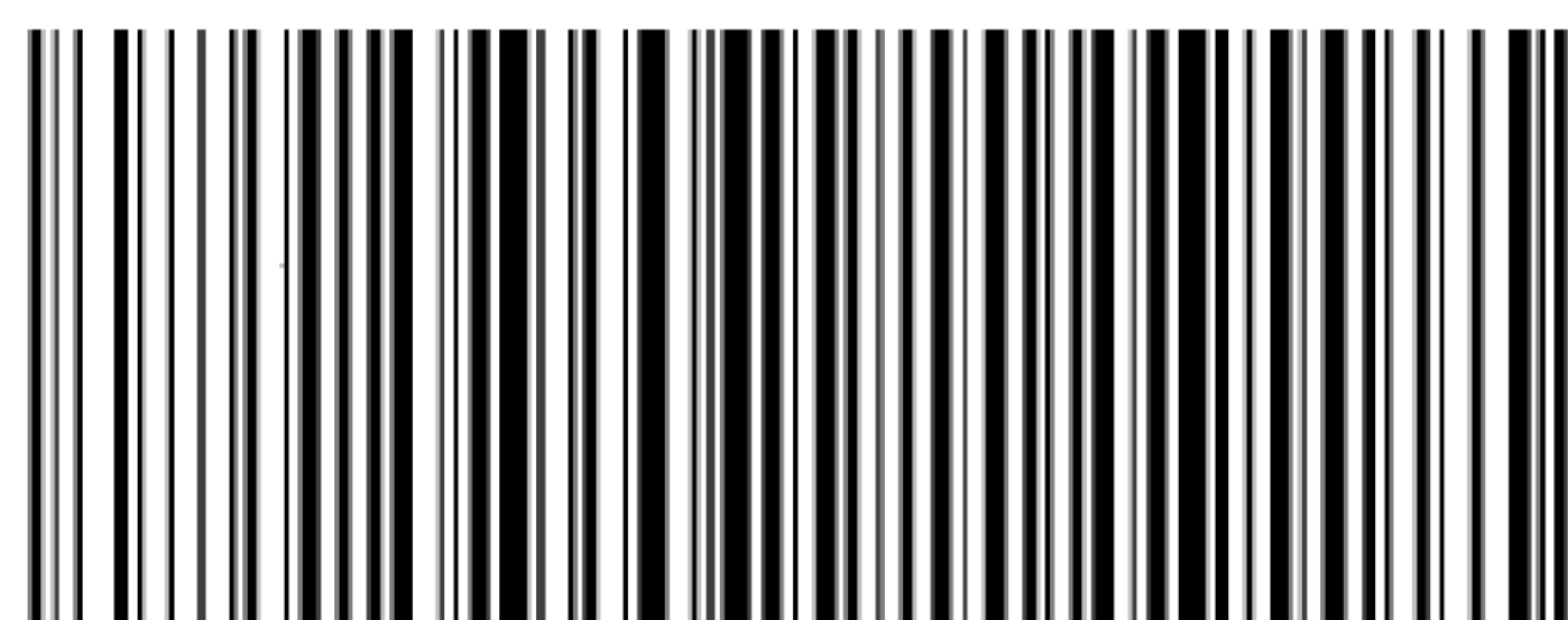
服务热线：400-168-0010

2017 年 11 月第一版

*

书号：155066·1-58156

版权专有 侵权必究



GB/T 34960.1—2017