

图 3-6 GB/T 34960.1 IT 治理模型

该标准定义的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，如图3-7所示。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和架构；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。

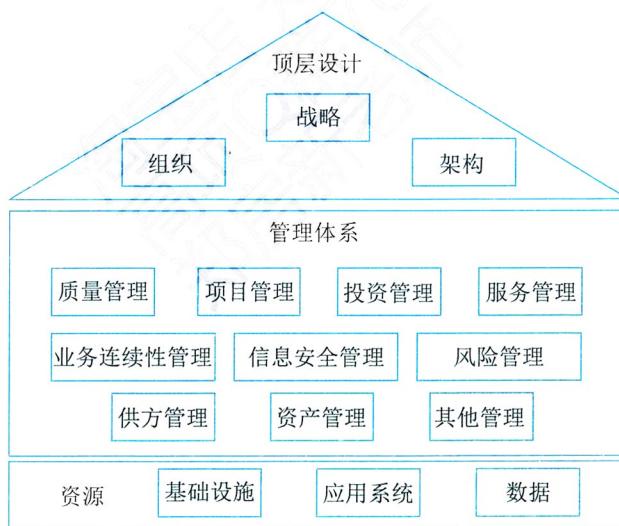


图 3-7 GB/T 34960.1 IT 治理框架

2) IT治理实施指南

GB/T 34960.2《信息技术服务 治理 第2部分：实施指南》提出了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。该标准适用于：①建立组织的IT治理实施框架，明确实施方法和过程；②组织内部开展IT治理的实施；③IT治理相关软件或解决方案实施落地的指导；④第三方开展IT治理评价的指导。

IT治理实施框架包括治理的实施环境、实施过程和治理域，如图3-8所示。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。组织可以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。

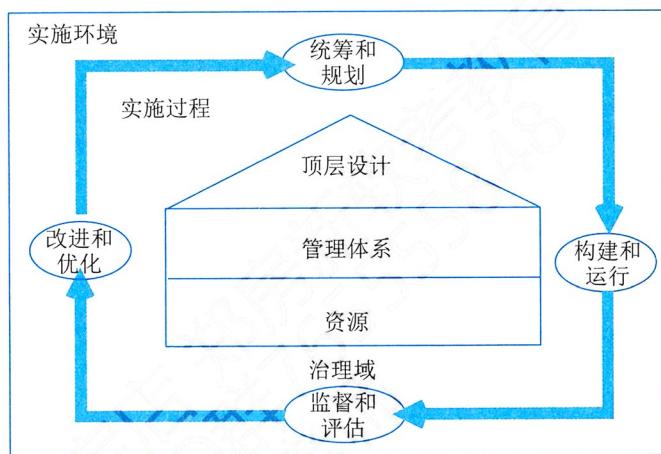


图3-8 GB/T 34960.2 IT治理实施框架

2. 信息和技术治理框架

COBIT是面向整个组织的信息和技术治理及管理框架，由成立于1969年的美国信息系统审计与控制协会（ISACA）组织设计并编制的。COBIT框架对治理和管理进行了明确区分，这两个学科涵盖不同的活动，需要不同的组织结构，并服务于不同目的：①治理确保对利益干系人的需求、条件和选择方案进行评估，以确定全面均衡、达成共识的组织目标；通过确定优先等级和制定决策来设定方向；根据议定的方向和目标监控绩效与合规性；②管理是指按治理设定的方向计划、构建、运行和监控活动，以实现组织目标。在大多数组织中，管理是首席执行官领导下的高级管理层的职责。ISACA设计并编制了《框架：治理和管理目标》《设计指南：信息和技术治理解决方案的设计》，主要供组织信息和技术治理（EGIT）、鉴证、风险和安全专业人员作为学习资料使用。

1) 治理和管理目标

COBIT框架介绍了40项核心治理和管理目标，以及其中包含的流程和其他相关组件。COBIT核心模型如图3-9所示。COBIT中治理目标被列入评估、指导和监控（EDM）领域，在

这个领域，治理机构将评估战略方案，指导高级管理层执行所选的战略方案并监督战略的实施。管理目标分为四个领域：①调整、规划和组织（APO）针对IT的整体组织、战略和支持活动；②内部构建、外部采购和实施（BAI）针对IT解决方案的定义、采购和实施以及它们到业务流程的整合；③交付、服务和支持（DSS）针对IT服务的运营交付和支持，包括安全；④监控、评价和评估（MEA）针对IT的性能监控及其与内部性能目标、内部控制目标和外部要求的一致程度。治理目标与治理流程有关，而管理目标与管理流程有关。治理流程通常由董事会和执行管理层负责，而管理流程则在高级和中级管理层的职责范围内。



图 3-9 COBIT 核心模型

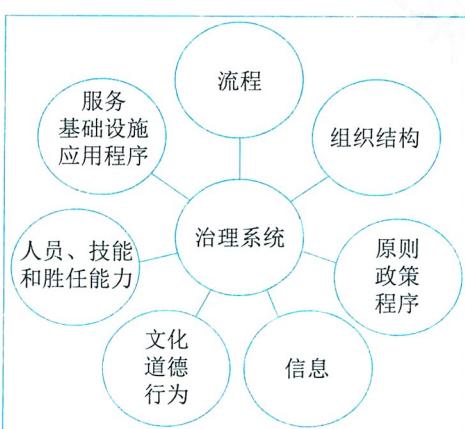


图 3-10 COBIT 治理系统组件

为满足治理和管理目标，每个组织都需要建立、定制和维护由多个组件构成的治理系统，如图3-10所示。治理系统的组件包括：①流程。流程描述了一组为实现某种目标而安排有序的实践和活动，并生成了一组支持实现整体IT相关目标的输出内容。②组织结构。组织结构是组织的主要决策实体。③原则、政策和程序。原则、政策和程序用于将理想行为转化为日常管理的实用指南。④信息。在任何组织中，信息无处不在，包括组织生成和使用的全部信息。COBIT侧重于有效运转组织治理系统所需的信息。⑤文化、道德和行为。个人和组织的文化、道德和行为作为治理和管理活动的成

功因素，其价值往往被低估。⑥人员、技能和胜任能力。人员、技能和胜任能力对做出正确决策、采取纠正行动和成功完成所有活动而言是必不可少的。⑦服务、基础设施和应用程序。服务、基础设施和应用程序包括为组织提供IT处理治理系统的基础设施、技术和应用程序。

2) 信息技术治理解决方案的设计

COBIT设计指南描述了组织如何设计量身定制的组织IT治理解决方案。高效和有效的IT治理系统是创造价值的起点。COBIT定义的IT治理系统设计因素包括组织战略、组织目标、风险概况、IT相关问题、威胁环境、合规性要求、IT角色、IT采购模式、IT实施方法、技术采用战略、组织规模和未来因素，如图3-11所示。这些设计因素可能影响组织治理系统的设计，为成功使用IT奠定基础。



图3-11 COBIT治理体系设计因素

组织开展治理系统设计通过流程化的方式进行，如图3-12所示，COBIT给出了建议设计流程：①了解组织环境和战略；②确定治理系统的初步范围；③优化治理系统的范围；④最终确定治理系统的设计。



图3-12 COBIT治理系统设计工作流程

3. IT治理国际标准

2008年4月，ISO/IEC正式发布IT治理标准ISO/IEC 38500，它的出台不仅标志着IT治理从概念模糊的探讨阶段进入了一个正确认识的发展阶段，而且也标志着信息化正式进入IT治理时代。这一标准将促使国内外一直争论不休的IT治理理论得到统一，也促使我国在引导信息化科学方面发挥重要作用。2014年，ISO/IEC发布了第二版的ISO/IEC FDIS 38500，替换了2008第一版的ISO/IEC 38500，ISO/IEC FDIS 38500: 2014提供了IT良好治理的原则、定义和模式，

以帮助最高级别组织的人员理解和履行其在组织使用 IT 方面的法律、法规和道德义务。

该标准为组织的治理机构（可包括所有者、董事、合伙人、执行经理或类似机构）的成员提供了关于在其组织内有效、高效和可接受地使用信息技术（IT）的指导原则。该标准包括：①责任。组织内的个人和团体理解并接受他们在 IT 的供应和需求方面的责任。那些负有行动责任的人也有权执行这些行动。②战略。组织的业务战略考虑到 IT 的当前和未来的能力；使用 IT 的计划满足了组织业务战略的当前和持续的需求。③收购。IT 收购是出于正当的理由，在适当和持续的分析基础上，有明确和透明的决策。在短期和长期内，在利益、机会、成本和风险之间都存在着适当的平衡。④性能。IT 适合于支持组织，提供满足当前和未来业务需求所需的服务、服务水平和服务质量。⑤一致性。IT 的使用符合所有强制性法律和法规。政策和实践有明确的定义、实施和执行。⑥人的行为。IT 团队的政策、实践和决策表明了对人的行为的尊重，包括所有“在这个过程中的人”的当前和不断发展的需求。

该标准规定治理机构应通过评估、指导和监督三个主要任务来治理 IT。

(1) 评估。治理机构应审查和判断当前和未来的使用，包括计划、建议和供应安排（无论是内部、外部或两者兼有）。在评估 IT 的使用时，治理机构应考虑作用于组织的外部或内部压力，如技术变革、经济和社会趋势、监管义务、合法的利益相关者期望和政治影响。治理机构应根据情况的变化不断地进行评价。治理机构还应考虑到当前和未来的业务需要，即他们必须实现的当前和未来的组织目标，例如维持竞争优势，以及他们正在评估的计划和建议的具体目标。

(2) 指导。治理机构应负责战略和政策的编制和执行。战略应该为 IT 领域的投资设定方向以及 IT 应该实现的目标。政策应在使用 IT 时建立良好的行为。治理机构应通过要求管理者及时提供信息、遵守方向和遵守良好治理的六项原则来鼓励其组织中的良好治理文化。

(3) 监督。治理机构应通过适当的测量系统来监测 IT 的表现。他们应该保证自己业绩符合战略，特别是在业务目标方面。治理机构还应确保 IT 符合外部义务（法规、立法、普通法、合同）和内部工作惯例等。

3.2 IT 审计

随着大数据、云计算、人工智能、移动互联网、物联网等新一代信息技术快速普及和深入应用，以及商业新模式、制造新模式、运行新模式等的出现和迅速繁荣，在给组织带来快速发展的同时，也加大了组织的 IT 风险。为了有效控制 IT 风险，有必要对组织的信息系统治理及 IT 内控与管理等开展 IT 审计，充分发挥 IT 审计监督的作用，提高组织的信息系统治理水平，促进组织信息系统治理目标的实现。

3.2.1 IT 审计基础

IT 审计对组织 IT 目标的达成以及组织战略目的实现具备重要的作用，这与人们通常所说的传统审计的重要性概念不同。传统审计的重要性是指被审计单位会计报表中错报或漏报的严重程度，这一严重程度在特定环境下可能影响会计报表使用者的判断或决策。传统审计在量上表现为审计重要性水平，也就是被审计单位财务报表中可能存在的不影响报表使用者做出决策和

判断的错报及漏报最大限额。IT 审计重要性是指 IT 审计风险（固有风险、控制风险、检查风险）对组织影响的严重程度，如：财务损失、业务中断、失去客户信任、经济制裁等。

1. IT 审计定义

IT 审计经过多年的发展，国内外机构对 IT 审计从不同角度进行了描述，目前主流的 IT 审计定义如表 3-3 所示。

表 3-3 主流的 IT 审计定义

机构 / 标准名称	定义
国际信息系统审计协会 (Information Systems Audit and Control Association, ISACA)	IT 审计是一个获取并评价证据，以判断计算机系统是否能够保证资产的安全、数据的完整以及有效利用组织的资源并有效实现组织目标的过程
国际货币基金组织 (International Monetary Fund, IMF)	IT 审计是对计算机化的系统进行审计，不仅是对现有信息系统的控制，还包括对系统建立过程、计算机设备和网络管理等方面控制
最高审计机关国际组织 (International Organization of Supreme Audit Institutions, INTOSAI)	IT 审计是一个通过获取并评估证据，以判断 IT 系统是否保护组织的资产，有效地利用组织的资源，保障数据的安全性和一致性，以及有效地达到组织业务目标的过程
GB/T 34690.4《信息技术服务 治理 第 4 部分：审计导则》	IT 审计是根据 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

2. IT 审计目的

IT 审计的目的是指通过开展 IT 审计工作，了解组织 IT 系统与 IT 活动的总体状况，对组织是否实现 IT 目标进行审查和评价，充分识别与评估相关 IT 风险，提出评价意见及改进建议，促进组织实现 IT 目标。

组织的 IT 目标主要包括：①组织的 IT 战略应与业务战略保持一致；②保护信息资产的安全及数据的完整、可靠、有效；③提高信息系统的安全性、可靠性及有效性；④合理保证信息系统及其运用符合有关法律、法规及标准等的要求。

3. IT 审计范围

一般来说，IT 审计范围需要根据审计目的和投入的审计成本来确定。在确定审计范围时，除了考虑前面提及的审计内容外，还需要明确审计的组织范围、物理位置以及信息系统相关逻辑边界。IT 审计范围的确定如表 3-4 所示。

表 3-4 IT 审计范围的确定

IT 审计范围	说明
总体范围	需要根据审计目的和投入的审计成本来确定
组织范围	明确审计涉及的组织机构、主要流程、活动及人员等
物理范围	具体的物理地点与边界
逻辑范围	涉及的信息系统和逻辑边界
其他相关内容

在实际的应用实践中，审计人员在实施IT审计项目前，应先对组织与信息系统相关的总体情况进行了解和风险评估，确定主要IT风险，如与环境控制相关的风险、与系统相关的风险、与数据相关的风险等，然后根据确定的风险来判断哪些控制、流程对组织的影响比较大，并结合审计项目预计的时间、配备的审计力量等来确定重点审计范围。

4. IT 审计人员

根据GB/T 34690.4《信息技术服务治理 第4部分：审计导则》，对IT审计人员的要求包括职业道德、知识、技能、资格与经验、专业胜任能力及利用外部专家服务等方面，如表3-5所示。

表3-5 IT审计人员要求

分类	具体要求
职业道德	<ul style="list-style-type: none"> ● 在执业过程中保持独立、客观、公正 ● 在执业过程中保持正直、诚实和守信 ● 正确履行审计职责（其中包括遵守相应的职业审计标准） ● 对在实施IT审计业务中所获取的信息负有保密责任
知识、技能、资格与经验	<ul style="list-style-type: none"> ● 掌握与IT相关的专业知识和技能 ● 掌握审计、财务及管理等通用知识和技能 ● 拥有与IT审计工作相关的基本技能、专业技能和软技能 ● 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
专业胜任能力	<ul style="list-style-type: none"> ● 具备相应的IT审计专业胜任能力 ● 拥有与所处管理或业务岗位相适应的IT审计职业资格 ● 定期参加持续的职业教育和培训
利用外部专家服务	<ul style="list-style-type: none"> ● 对外部专家的专业资格及专业经验进行评价 ● 对外部专家的独立性、客观性进行评价 ● 对外部专家的专业胜任能力进行评价 ● 与外部专家签订书面协议 ● 对外部专家的服务结果进行评价和利用

5. IT 审计风险

IT审计风险主要包括固有风险、控制风险、检查风险和总体审计风险。固有风险、控制风险、检查风险的内容，如表3-6所示。

表3-6 固有风险、控制风险和检查风险的内容

类别	描述
固有风险	<ul style="list-style-type: none"> ● 含义：是指IT活动不存在相关控制的情况下，易于导致重大错误的风险 ● 分类：可从IT组织层面控制、一般控制及应用控制三个方面分析固有风险 ● 特点：固有风险是IT活动本身所具有的，审计人员只能评估，却无法控制或影响它；固有风险的衡量是主观的、复杂的，不同的IT活动其固有风险水平不同

(续表)

类别	描述
控制风险	<ul style="list-style-type: none"> 含义：是指与IT活动相关的内部控制体系不能及时预防或检查出存在的重大错误的风险 分类：可从IT组织层面控制、一般控制及应用控制三个方面分析控制风险 特点：与内部控制制度执行的有效性有关，与审计无关，属于内部控制的范畴，审计人员只能评估其风险水平而不能对其实施控制和影响。其风险水平的衡量由于需要兼顾传统内部控制的思想和计算机系统管理的知识，因而较为复杂且难以准确计量
检查风险	<ul style="list-style-type: none"> 含义：检查风险是指通过预定的审计程序未能发现重大、单个或与其他错误相结合的风险 影响检查风险的因素：由于IT审计规范不完善、审计人员自身或者技术原因等造成影响审计测试正确性的各种因素

总体审计风险是指针对单个控制目标所产生的各类审计风险总和。良好的审计计划应尽可能评估和控制审计风险，减少或控制所检查领域的审计风险，比如采取合适的审计工具，在完成审计时把总体审计风险控制在足够低的水平之内，以达到预期保证水平。

审计风险也用于描述审计人员在执行审计任务时可接受的风险水平。审计人员可通过设定目标风险水平并调整审计工作量，以合适的审计成本满足最小化总体审计风险要求。

3.2.2 审计方法与技术

1. IT 审计依据与准则

IT 审计活动的开展需要结合相关法律法规、准则与标准。国际上发布的常用审计准则有：

- 信息系统审计准则（ISACA，国际信息系统审计协会发布）。
- 《内部控制—整体框架》报告，即通称的COSO（The Committee of Sponsoring Organizations of The National Commission of Fraudulent Financial Reporting，美国虚假财务报告委员会下属的发起人委员会）报告。
- 《萨班斯法案》（Sarbanes-Oxley Act，SOX）。SOX是美国政府出台的一部涉及会计职业监管、组织治理、证券市场监管等方面改革的重要法律。
- 信息及相关技术控制目标（Control Objectives for Information and related Technology，COBIT）是目前国际上通用的信息及相关技术控制规范。

我国的 IT 审计相关法律法规、准则与标准如表 3-7 所示。

表 3-7 IT 审计相关法律法规、准则与标准（举例）

类别	名称
法律法规	《中华人民共和国审计法》《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等
审计准则	《信息系统审计指南——计算机审计实务公告第 34 号》《第 2203 号内部审计具体准则——信息系统审计》等
IT 审计国际标准	GB/T 34960.4《信息技术服务治理 第 4 部分：审计导则》等
组织内部控制	《组织内部控制基本规范》《组织内部控制应用指引第 18 号——信息系统》等

(续表)

类别	名称
行业规范	《商业银行信息科技风险管理指引》《证券期货经营机构信息技术治理工作指引（试行）》《保险公司信息化工作指引（试行）》等

2. IT 审计常用方法

IT 审计方法就是为了完成 IT 审计任务所采取的手段。在 IT 审计工作中，要完成每一项审计工作，都应选择合适的审计方法。常用审计方法包括：访谈法、调查法、检查法、观察法、测试法和程序代码检查法等，如表 3-8 所示。

表 3-8 IT 审计常用方法表（举例）

分类	说明
访谈法	<ul style="list-style-type: none"> ● 含义：是指通过访谈人和受访人面对面地交谈来了解被审计对象的信息。依据不同研究问题的性质、目的或对象，访谈法具有不同的形式 ● 分类：根据访谈进程的结构化程度，可将它分为结构型访谈和非结构型访谈
调查法	<ul style="list-style-type: none"> ● 含义：是指为了达到预期目的，在制订调研计划的基础上，通过书面或口头回答问题的方式收集研究对象的相关资料，并做出分析、综合，得到某一结论的研究方法 ● 目的：可能是全面把握当前状况，也可能是为了揭示存在的问题，弄清前因后果，以便为进一步的研究或决策提供观点和论据
检查法	<ul style="list-style-type: none"> ● 含义：是指审计人员对被审计单位内部或外部生成的记录和文件（如纸质、电子或其他介质形式存在的资料）进行审查，或对资产进行实物审查 ● 分类：从技术层面上可分为审阅法、核对法、复算法和分析法
观察法	<ul style="list-style-type: none"> ● 含义：是审计人员到被审计单位的经营场所及其他有关场所进行实地察看，来证实审计事项的一种方法 ● 应用：观察程序具有方向性，即从书面记录观察到实物或过程，反之，从实物或过程观察到书面记录。观察法既可以用于对通过其他方法获得的审计证据进行补充，证实审计证据，也可以用于直接收集相关证据。观察法可以比较准确地获得审计项目如何运行的信息，适用于正在进行中的审计事项
测试法	<ul style="list-style-type: none"> ● 含义：通过测试来评估程序的质量是一项常用的审计技术，其基本原理是从计算机输入开始，跟踪某项业务直至计算机输出，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 ● 分类：主要包括黑盒法和白盒法。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。白盒法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都能按预定要求正确工作，主要用于软件验证
程序代码 检查法	<ul style="list-style-type: none"> ● 含义：是指对被审程序的指令逐条加以审查，以验证程序的合法性、完整性和程序逻辑的正确性 ● 应用：审计人员可使用代码静态扫描工具进行程序代码的检查

3. IT 审计技术

常用的 IT 审计技术包括风险评估技术、审计抽样技术、计算机辅助审计技术及大数据审计技术。

1) 风险评估技术

IT 风险评估技术一般包括：

- 风险识别技术：用以识别可能影响一个或多个目标的不确定性，包括德尔菲法、头脑风暴法、检查表法、SWOT 技术及图解技术等。
- 风险分析技术：是对风险影响和后果进行评价和估量，包括定性分析和定量分析。
- 风险评价技术：是在风险分析的基础上，通过相应的指标体系和评价标准，对风险程度进行划分，以揭示影响成败的关键风险因素，包括单因素风险评价和总体风险评价。
- 风险应对技术：IT 技术体系中为特定风险制定的应对技术方案，包括云计算、冗余链路、冗余资源、系统弹性伸缩、两地三中心灾备、业务熔断限流等。

2) 审计抽样技术

审计抽样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。审计抽样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件进行全面审计时。“总体”是指需要检查的全部事项，“样本”是用于测试总体的子集。审计抽样的方法如表 3-9 所示。

表 3-9 审计抽样方法分类表

类别	说明
统计抽样	<ul style="list-style-type: none">● 采用客观的方法来确定样本量和样本抽取标准。统计抽样采用概率学原理，涉及计算样本量、抽取样本● 评价样本结果并做出推断。利用统计抽样，审计人员可以量化描述样本与总体的接近程度（评价抽样精度）以及用百分比表示的样本能够代表总体的概念（可靠性或置信水平）。有效的统计抽样结果是量化的● 常用的统计抽样方法有：①属性抽样。固定样本量属性抽样或频率估计抽样——用于估计总体中某种特性（属性）的发生比率（百分率）的抽样方法，属性抽样回答“有多少？”的问题。可被测试的属性的一个例子是计算机访问申请表上的批准签字。②变量抽样。变量抽样也称为金额估计抽样或平均值估计抽样，是一种由样本估计总体的货币金额或其他度量单位（如重量）的抽样技术。变量抽样的一个例子是检查组织重要交易的余额表及对生成余额表的程序实施的应用系统审计
非统计抽样	常指判断抽样——采用审计人员判断来确定抽样方法、样本量（从总体中抽取的一定数量的事项以执行测试）及抽样标准（选择哪一些事项用于测试）。抽样结果是基于审计人员对抽样事项或交易的重要性及风险的主观判断

3) 计算机辅助审计技术

计算机辅助审计（Computer Assisted Audit Tools, CAAT），也称为利用计算机审计，是指审计人员在审计过程和审计管理活动中，以计算机为工具来执行和完成某些审计程序和任务的一种新兴审计技术。它并非电算化系统审计特有的一种方法，对手工系统的审计也可应用这些技术。

计算机辅助审计技术是审计人员在这种环境下收集信息的重要工具。由于系统有不同的硬件和软件环境、数据结构、记录格式或处理功能，如果没有软件工具来收集和分析记录内容，审计人员收集证据几乎是不可能的。CAAT 也使得审计人员可以独立地收集信息，CAAT

为针对既定的审计目标访问和分析数据提供了一种方法，并以系统记录的可靠性为重点报告审计发现。源信息可靠性是审计发现的保证基础。CAAT 包括多种工具和技术，如通用审计软件（GAS）、测试数据、实用工具软件、专家系统等。

4) 大数据审计技术

大数据审计是指遵循大数据理念，运用大数据技术方法和工具，利用数量巨大、来源分散、格式多样的数据，开展跨层级、跨系统、跨部门和跨业务等的深入挖掘与分析，提升审计发现问题、评价判断、宏观分析的能力。大数据审计技术包括大数据智能分析技术、大数据可视化分析技术及大数据多数据源综合分析技术等，如表 3-10 所示。

表 3-10 大数据审计技术（举例）

分类	说明
大数据智能分析技术	以各种高性能处理算法、智能搜索与挖掘算法等为主要研究内容，是目前大数据分析领域的研究主流。该技术从计算机的视角出发，强调计算机的计算能力和人工智能，如各类面向大数据的机器学习和数据挖掘方法等。常用技术包括 A/B Testing、关联规则分析、分类、聚类、遗传算法、神经网络、预测模型、模式识别、时间序列分析、回归分析、系统仿真等
大数据可视化分析技术	从人作为分析主体和需求主体的视角出发，强调基于人机交互的、符合人的认知规律的分析方法，目的是将人所具备的、机器并不擅长的认知能力融入数据分析过程中，如 R 语言、Python、D3.js、Leaflet 等
大数据多数据源综合分析技术	大多数大数据多数据源综合分析技术是对采集来的各行、各业、各类大数据，采用数据查询等常用方法或其他大数据技术方法进行相关数据的综合比对和关联分析，从而发现更多隐藏的审计线索的技术

4. IT 审计证据

审计证据是指由审计机构和审计人员获取，用于确定所审计实体或数据是否遵循既定标准或目标，形成审计结论的证明材料。审计证据是审计意见的支柱，是审计人员形成审计结论的基础。审计人员必须基于足够、相关和适当的审计证据，为其审计观点提供合理的结论。审计证据还可以被作为解除或追究被审计人经济责任的依据，并且审计证据还是控制审计工作质量的关键。

审计证据的特性是指审计证据内在性质和特征，具体体现为审计人员围绕这些性质和特征收集审计证据时应达到的基本要求。对审计证据的属性，在国际上有不同的描述。审计证据的特性如表 3-11 所示。

表 3-11 审计证据的特性

分类	说明
充分性	指要求审计人员根据所获证据足以对被审计对象提出一定程度保证的结论，是对审计证据数量的要求，主要与审计人员确定的样本量有关
客观性	指审计证据必须是客观存在的事实材料。客观的审计证据比需要判断或解释的证据可靠
相关性	指审计证据与审计事项之间必须有实质性联系
可靠性	指审计证据能够反映和证实客观经济活动特征的程度。审计证据的可靠性受到审计证据的类型、取证的渠道和方式等因素的影响
合法性	指审计证据必须符合法定种类，并依照法定程序取得

电子证据是信息环境下经常使用的一种证据类型。电子证据是指以电子的、数据的、磁性的或类似性能的相关技术形式存在并能够证明事件事实真实情况的一切材料。刑事诉讼法中指出电子证据无论是形式还是证据规则都与传统证据有很大区别，高要求的技术规范，贯穿于电子证据的收集、提取、保存到出示、审查、判断、认证的各个环节。因此，通过司法解释缓解司法实践中的矛盾仅仅是权宜之计，彻底解决电子证据法律定位问题还是要从立法上予以突破，即应通过修改诉讼法或出台证据法典来明确电子证据的法律地位，赋予电子证据独立的法律地位，以电子证据取代视听资料的证据地位。

为了使收集到的分散、个别、不系统审计证据变成充分、适当、具有证明力证据，审计人员必须按照一定的方法对审计证据进行分类整理与分析，使之条理化、系统化，然后对各种审计证据进行合理归纳，并在此基础上形成恰当的整体审计结论。审计证据评价应考虑的因素包括证据提供者的独立性、提供信息/证据的个人资质、证据的客观性、证据的时效性、与审计目标的相关性、审计证据的说服力及审计证据的充分性。此外，在审计过程中还必须考虑取得审计证据的经济性，必须考虑成本效益原则，合理把握审计证据的充分性。

5. IT 审计底稿

审计工作底稿是指审计人员对制订的审计计划、实施的审计程序、获取的相关审计证据，以及得出的审计结论做出的记录。审计工作底稿是审计证据的载体，是审计人员在审计过程中形成的审计工作记录和获取的资料。它形成于审计过程，也反映整个审计过程。审计底稿的作用表现在：

- 是形成审计结论、发表审计意见的直接依据；
- 是评价考核审计人员的主要依据；
- 是审计质量控制与监督的基础；
- 对未来审计业务具有参考备查作用。

审计工作底稿一般分为综合类工作底稿、业务类工作底稿和备查类工作底稿，具体如表 3-12 所示。

表 3-12 审计工作底稿分类

底稿类型	说明
综合类工作底稿	指审计人员在审计计划阶段和审计报告阶段，为规划、控制和总结整个审计工作并发表审计意见所形成的审计工作底稿，主要包括：审计业务约定书、审计计划、审计总结、审计报告、管理建议书、被审计单位管理当局声明书以及审计人员对整个审计工作进行组织管理的所有记录和资料
业务类工作底稿	指审计人员在审计实施阶段为执行具体审计程序所形成的审计工作底稿，包括：符合性测试中形成的内部控制问题调查表和流程图、实质性测试中形成的项目明细表等
备查类工作底稿	指审计人员在审计过程中形成对审计工作仅具有备查作用的审计工作底稿。备查类工作底稿应随被审计单位有关情况的变化而不断更新；应详细列明目录清单，并将更新的文件资料随时归档；应根据需要，将其中与具体审计项目有关的内容复印、摘录、综合后归入业务类审计工作底稿的具体审计项目之后。通常，备查类审计工作底稿是由被审计单位或第三者根据实际情况提供或代为编制，审计人员应认真审核，并对所取得的有关文件、资料标明其具体来源

审计工作底稿作为审计人员在整个审计过程中形成的审计工作记录资料，在编制上应满足内容和形式两方面的要求：

- 内容要求包括资料翔实、重点突出、繁简得当、结论明确；
- 形式要求包括要素齐全、格式规范、标识一致、记录清晰。

通常，根据审计机构的组织规模和业务范围，可以实行对审计工作底稿的三级复核制度。审计工作底稿三级复核制度是指以审计机构负责人、部门负责人和项目负责人（或项目经理）为复核人，依照规定的程序和要点对审计工作底稿进行逐级复核的制度。三级复核制度目前已成为较为普遍采用的形式，对于提高审计工作质量、加强质量控制起了重要的作用。

为了维护被审计单位及相关单位的利益，审计机构对审计工作底稿中涉及的商业秘密保密，建立健全审计工作底稿保密制度。但由于下列两种情况需要查阅审计工作底稿的，不属于泄密情形：

- 法院、检察院及国家其他部门依法查阅，并按规定办理了必要手续；
- 审计协会或其委派单位对审计机构执业情况进行检查。

审计工作底稿按照一定的标准归入审计档案后，应交由档案管理部门进行管理，并确保审计档案的安全、完整。

3.2.3 审计流程

审计流程是指审计人员在具体审计过程中采取的行动和步骤。科学、规范的审计流程不但是分配审计工作的具体依据，还是控制审计工作的有效工具，并同时具有的作用包括：①有效地指导审计工作；②有利于提高审计工作效率；③有利于保证审计项目质量；④有利于规范审计工作。

通常，审计流程的含义有广义和狭义两种之分。狭义的审计流程是指审计人员在取得审计证据、完成审计目标、得出审计结论过程中所采取的步骤和方法。广义的审计流程是指审计机构和审计人员对审计项目从开始到结束的整个过程采取的系统性工作步骤，一般分为审计准备、审计实施、审计终结及后续审计四个阶段，每个阶段又包含若干具体内容。

(1) 审计准备阶段。IT 审计准备阶段是指 IT 审计项目从计划开始，到发出审计通知书为止的期间。准备阶段是整个审计过程的起点和基础，准备阶段的工作是否充分、合理、细致，对提高审计工作效率，保证审计工作质量至关重要。准备阶段工作一般包括：①明确审计目的及任务；②组建审计项目组；③搜集相关信息；④编制审计计划等。

(2) 审计实施阶段。IT 审计实施阶段是审计人员将项目审计计划付诸实施的期间。此阶段的工作是审计全过程的中心环节，是整个审计流程的关键阶段，关系到整个审计工作的成败。实施阶段主要完成工作包括：①深入调查并调整审计计划；②了解并初步评估 IT 内部控制；③进行符合性测试；④进行实质性测试等。

(3) 审计终结阶段。IT 审计终结阶段是整理审计工作底稿、总结审计工作、编写审计报告、做出审计结论的期间。审计人员应运用专业判断，综合分析所收集到的相关证据，以经过核实的审计证据为依据，形成审计意见、出具审计报告。终结阶段的工作一般包括：①整理与复

核审计工作底稿；②整理审计证据；③评价相关IT控制目标的实现；④判断并报告审计发现；⑤沟通审计结果；⑥出具审计报告；⑦归档管理等。

(4) 后续审计阶段。后续审计是在审计报告发出后的一定时间内，审计人员为检查被审计单位对审计问题和建议是否已经采取了适当的纠正措施，并取得预期效果的跟踪审计。后续审计并不是一次新的审计，而是前一次审计的有机组成部分。实施后续审计，可不必遵守审计流程的每一过程和要求，但必须依法依规进行检查、调查，收集审计证据，写出后续审计报告。

3.2.4 审计内容

IT审计业务和服务通常分为IT内部控制审计和IT专项审计。IT内部控制审计主要包括组织层面IT控制审计、IT一般控制审计及应用控制审计；IT专项审计主要是指根据当前面临的特殊风险或者需求开展的IT审计，审计范围为IT综合审计的某一个或几个部分。有关IT内部控制审计与IT专项审计的具体内容如表3-13所示。

表3-13 IT审计业务分类表

大类名称	子类名称	审计内容
IT内部控制审计	组织层面IT控制审计、IT一般控制审计及应用控制审计	<ul style="list-style-type: none"> ● 组织层面IT控制审计主要指对IT战略、组织、架构、业务连续性、风险管理、外包管理、网络与信息安全及监督管理等进行审计 ● IT一般控制审计主要是指针对与应用系统、数据库、操作系统、网络相关的策略和措施等进行审计 ● 应用控制审计是指针对业务流程层面运行的人工或自动化程序进行审计，主要包括输入控制、处理控制和输出控制的审计
IT专项审计	信息系统生命周期审计	主要是对信息系统的规划、设计、开发、测试、运行和维护等进行审计
	信息系统开发过程审计	主要围绕信息系统规划、设计、建设、实施是否符合IT架构和战略进行评估和监督
	信息系统运行维护审计	主要针对IT运维能力、IT运维流程策划、实施、监控改进等情况进行审计，内容包括基础设施的运行、系统的运行、维护、质量保证及IT服务管理等
	网络与信息安全审计	主要以网络与信息安全为核心，围绕安全相关的组织、人员、系统、设备和环境等，重点关注网络与信息安全相关流程、制度的执行情况，对相关法律法规的遵从性，包括适用的数据保护，个人隐私保护等合规要求
	信息系统项目审计	主要是通过对信息系统项目管理过程的评价，向管理层提供信息系统项目管理过程得到控制、监督并遵循最佳实践要求的合理保证
	数据审计	通过控制活动，负责定期分析、验证、讨论、改进数据安全管理相关的政策、标准和活动

针对信息系统的专项审计，其目标是通过对信息系统项目管理过程的评价，向管理层提供信息系统项目管理过程得到控制、监督并遵循最佳实践要求的合理保证。信息系统项目管理审计内容与方法举例如表3-14所示。

表 3-14 信息系统项目管理审计内容与方法举例

类别	审计内容	审计方法
组织管理	<ul style="list-style-type: none"> ● 组织是否设立项目管理机构或明确项目管理职能的归属 ● 组织是否制定了项目管理制度与流程 ● 组织级的项目管理制度与流程是否全面合理 ● 是否对信息系统项目团队的组成、人员的配备及能力等进行要求 	<ul style="list-style-type: none"> ● 访谈组织级项目管理相关人员，了解组织级信息系统相关组织机构、项目管理制度及流程等的制定情况 ● 检查组织级信息系统相关组织机构的架构、职责与权限设计的合理性
项目启动与计划	<ul style="list-style-type: none"> ● 项目启动会的组织是否规范 ● 项目管理目标是否清晰定义及跟踪 ● 是否建立与项目规模及重要程度相适应的项目管理团队并明确职责 ● 团队人员是否稳定 ● 是否存在职责不相容的情况 ● 项目人员配备及能力是否满足要求 ● 是否制订项目计划 ● 项目计划是否完备 	<ul style="list-style-type: none"> ● 访谈项目负责人，了解项目启动与计划的总体情况 ● 取得项目组织机构图、职责及人员配备，检查项目组织机构图、人员职责对应表的合理性；检查团队人员变更的情况 ● 取得项目资料（如项目合同、工作说明书、项目计划等），检查文档的编制是否符合要求，内容的全面性及合理性
项目实施与控制	<ul style="list-style-type: none"> ● 项目干系人是否参与到项目活动中，发挥作用 ● 是否建立了科学、高效的项目沟通机制 ● 项目的资源是否有效利用 ● 项目是否进行了必要的配置管理 ● 项目的采购是否规范 ● 是否建立了适合组织的风险管理方法 ● 项目是否建立了绩效评价体系 ● 各阶段产生的文档是否合理、真实 ● 项目是否采取措施，有效地制订了进度计划、控制进度的活动 ● 项目是否建立规划质量、实施质量保证、实施质量控制的控制手段 	<ul style="list-style-type: none"> ● 访谈项目相关人员，了解项目实施与控制的总体情况 ● 检查与观察项目现场物理环境的控制情况 ● 访谈项目相关人员，询问文档有关内容 ● 取得项目相关文档（如项目审查记录和发布通知、项目有效性审查评估记录、项目安全事件记录等），检查文档编制的规范性以及相关控制的合理性 ● 取得应用系统的测试资料，检查测试过程控制的规范性，以及测试报告编制的合理性等
项目收尾管理	<ul style="list-style-type: none"> ● 项目验收申请材料是否完整且规范 ● 是否建立项目验收流程 ● 项目验收评审流程是否规范 ● 是否在规定时间内完成项目验收 ● 项目质量是否达标 ● 第三方项目质量检测机构的流程是否规范，报告内容是否完整 	<ul style="list-style-type: none"> ● 访谈项目验收相关人员，了解项目收尾相关情况 ● 取得项目验收相关材料，检查材料编写的规范性、内容的合理性和全面性
工程方法审计	<ul style="list-style-type: none"> ● 是否真实地进行了可行性调研 ● 可行性阶段产生文档是否合理 ● 是否对系统实施的技术方案和方法进行过论证 ● 是否编制项目需求计划？内容是否全面、合理 	<ul style="list-style-type: none"> ● 访谈相关人员了解项目可行性研究情况 ● 取得项目投资报告及其审批文档，检查手续费的规范性、完整性 ● 检查信息来源的真实性及内容的合理性

(续表)

类别	审计内容	审计方法
工程方法审计	<ul style="list-style-type: none"> ● 是否编制概要设计文档？内容是否全面合理 ● 是否进行产品技术方案选型 ● 是否制定编码规范？内容是否全面合理 ● 是否每个开发人员都熟悉编码规范 ● 是否制订测试计划 ● 测试计划的内容是否全面、合理 ● 上线前是否对系统进行了确认测试，填写业务测试验收文档？是否得到客户的确认 ● 是否有系统运行的日志 	<ul style="list-style-type: none"> ● 取得项目技术方案及其论证文档，检查对系统实施的技术方案和方法论证内容的全面性、合理性 ● 访谈相关人员，了解项目需求计划制订情况 ● 取得项目需求计划及评审、批准的相关记录 ● 检查项目需求计划的内容是否全面合理

3.3 本章练习

1. 选择题

(1) “计算机硬件故障或软件不足，易造成信息的损坏和丢失，导致数据处理过程中发生偶发错误”，描述的风险类型是_____。

- A. 固有风险 B. 控制风险 C. 检查风险 D. 审计风险

参考答案: A

(2) _____指审计人员在审计实施阶段为执行具体审计程序所形成的审计工作底稿。

- A. 综合类工作底稿 B. 业务类工作底稿
C. 备查类工作底稿 D. 技术类工作底稿

参考答案: B

(3) 关于 IT 审计范围的描述，不正确的是：_____。

- A. 总体范围需要根据审计目的和投入的审计成本来确定
B. 组织范围需明确审计涉及的组织机构、主要的流程、活动及人员等
C. 逻辑范围需明确涉及的信息系统
D. 物理范围需明确具体的物理地点与边界

参考答案: C

(4) 组织外包其软件开发，_____是该组织 IT 管理的责任。

- A. 作为开发人员参加系统设计 B. 支付服务提供商
C. 与服务提供商谈判合同 D. 控制服务提供商遵守服务合同

参考答案: D

(5) _____不属于 IT 治理的三大主要目标。

- A. 与业务目标一致 B. 质量控制
C. 有效利用信息与数据资源 D. 风险管理

参考答案: B

(6)《信息技术服务治理 第1部分：通用要求》标准不适用于_____。

- A. 建立组织的IT治理体系并实施自我评价
- B. 组织的IT治理能力进行自我评价
- C. 研发、选择和评价IT治理相关的软件或解决方案
- D. 开展信息技术审计

参考答案：B

(7) COBIT[®] 2019核心模型中的治理和管理目标分为五个领域，_____领域是由董事会和执行管理层负责。

- A. 评估、指导和监控(EDM)
- B. 调整、规划和组织(APO)
- C. 内部构建、外部采购和实施(BAI)
- D. 交付、服务和支持(DSS)

参考答案：A

2. 思考题

(1) IT治理的管理层次可分为三层：最高管理层、执行管理层、业务与服务执行层，请简要描述这3个层次的主要职责分别是什么？

参考答案：略

(2) IT治理的核心内容包括哪6个方面，请简述？

参考答案：略

(3) 请指出IT审计的常用方法，并根据你的理解举例说明信息系统项目管理可能使用的方法及具体运用。

参考答案：略

第4章 信息系统管理

在信息技术和数据资源要素的推动下，社会各领域已经并正在加速进入数字化的全新发展时期，基于智能、网络和大数据的新经济业态正在形成，从“数字融合”向“数字原生”的发展是这个时期的主要特征，表现为信息技术和工业制造深度融合、人和机器的融合、信息资源和材料资源的融合等，进而基于这种深度融合所构造的数字化新世界，将引发社会各个领域为完全适应数字世界而产生各种数字原生发展模式，这些模式将不断诞生、发展、凋亡和重塑，从而极大地改变了人们的生活方式和行为模式。这个进程是一场比过往的工业化和信息化更加广泛的社会变革。支撑这场变革的重要基础，是不断与社会发展各方面深度融合的信息系统，只有对信息系统实施有效管理，才能承担变革赋予的重任。

4.1 管理方法

信息系统管理是一项需要组织各层级充分参与的业务运行工作。大多数组织都拥有专门用于信息系统管理的职能部门，这些部门配备了相关技术领域的高技能专业人员。同时，组织的管理者也需要了解并参与相关的决策。

4.1.1 管理基础

对信息的高效管理与利用，是在新时代发展环境中取得成功的关键技能。现代化组织做出的所有决策在某种程度上都与信息系统的管理和使用密切相关。对管理者来说，了解其组织能力和信息的开发利用，与懂得如何获取金融资源和平衡预算一样至关重要。随着智能手机、笔记本电脑和平板电脑等个人设备的广泛使用，通过互联网访问组织内外部的应用程序以执行日常工作和业务动作的频度越来越高，凸显了“技术底座构成了几乎所有业务模式的支柱”这一事实。当这种技术底座具备全球可达的特性时，对管理者的技能又增加了全球化能力的要求。基于信息系统技术底座，协作工具和数字化引擎的可用性产生了变化，即信息系统与业务流程日益集成，逐渐变成业务流程演变的革命性因素。迫切需要组织管理者参与技术决策，以确保信息系统对业务的正向支撑，并避免技术的负面影响。

1. 层次结构

信息系统是对信息进行采集、处理、存储、管理和检索，形成组织中的信息流动和处理，必要时能向有关人员提供有用信息的系统。它是由人、技术、流程和数据资源组成的人机系统，目的是及时、正确地收集、加工、存储、传递和提供信息，以实现组织中各项活动的管理、调节和控制。信息系统是为组织用来生产和管理信息（数据）的技术（“什么”）、人员（“谁”）和过程（“如何”）的组合。信息系统包括四个要素：人员、技术、流程和数据，如图 4-1 所示。

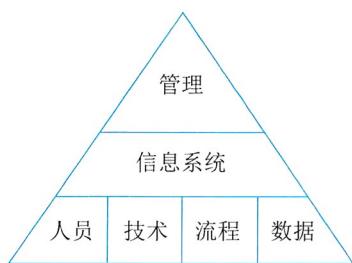


图 4-1 信息系统层次架构

在信息系统层次架构中，信息系统之上是管理，它监督系统的设计和结构，并监控其整体性能。同时，组织管理层制定信息系统层应满足的业务需求和业务战略。信息系统层次架构提供了一个蓝图，可以将业务和系统策略转换为组件或基础架构，并以恰当的人员、技术、流程和数据组合加以实现。

2. 系统管理

信息系统的管理需要提高各组织管理人员对信息系统相关问题的认识。信息技术及其系统在本质上都具有矛盾性，一方面具备前瞻性，不可或缺，因为它们为充满潜力的创新（大数据、人工智能和万物互联等）铺平了道路。另一方面则是主要漏洞（网络安全、数字化和隐私丧失等）的载体，且目前难以衡量其范围和后果。这就是为什么信息系统的管理越来越重要且必要的原因。除了纯粹的运行问题之外，还可以清楚地看到信息系统的管理与道德问题，以及其与世界的复杂性的关联程度越来越密切。基于信息系统构建和执行业务部门的流程，越来越多地限制了价值链中利益干系人之间的关系，那么关于信息系统的决策就会越来越对战略产生影响。一旦信息系统的影响不再局限于工作效率和劳动强度，将不断地为个人空间提供连续性的能力，信息系统的决策也会对每个人产生影响。

信息系统管理覆盖四大领域：

- 规划和组织：针对信息系统的整体组织、战略和支持活动。
- 设计和实施：针对信息系统解决方案的定义、采购和实施，以及他们与业务流程的整合。
- 运维和服务：针对信息系统服务的运行交付和支持，包括安全。
- 优化和持续改进：针对信息系统的性能监控及其于内部性能目标、内部控制目标和外部要求的一致性管理。

4.1.2 规划和组织

信息系统的规划和组织需要根据组织的发展目标和其他相关因素规划信息系统的战略、组成、建设、运行和运营等。目标是通过实施具备一致性的管理方法，满足业务对信息系统的管理需求。规划和组织的相关内容涵盖信息系统管理所需的所有组件，如：管理流程与组织结构的执行，角色和职责的部署管理，可靠且可重复的活动规范，信息化项目的执行，技能和能力的建设优化，以及服务、基础设施和应用程序的运行管理等。

1. 规划模型

战略是实现目标、意图和目的的一组协调行动。战略往往始于使命，而使命是对组织的宗旨给出的一个清晰并令人信服的陈述。信息系统战略三角突出了业务战略、信息系统和组织机制之间的必要一致性，如图 4-2 所示。它用于描述信息系统与业务系统必要的协同关系，以及理解信息系统与组织机制间的相互影响。当业务战略、组织机制与信息系统运转良好时，这种多方战略决策的一致性往往很难被组织认知。但是，当发生重大生产事故和灾难时，在规划一

项业务时，需要正确调整业务战略、信息系统和组织机制之间的协同实践。

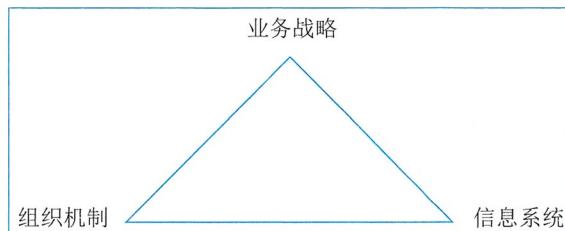


图 4-2 信息系统战略三角

成功的组织有一个压倒一切的业务战略，可以推动组织机制和信息系统的有机融合。有关组织机制的结构、招聘实践和其他组成部分的决策，以及有关应用程序、硬件和其他信息系统组件的决策，都是由组织的业务目标、总体战略与战术驱动的。成功的组织会仔细平衡信息系统战略三角，对自己的组织和信息系统战略进行细致规划，以补充其业务战略。

信息系统战略本身可以影响并受到组织业务和组织机制战略变化的影响。为了保持成功运行所需的平衡，信息系统战略的改变必然伴随着组织机制战略的变化，并且必须适应整体业务战略。如果组织在规划其业务战略时利用信息系统来获得战略优势，那么信息系统的领导地位必须通过不断创新来维持。业务、信息和组织机制战略需要不断进行动态调整。

信息系统战略总是涉及业务和组织机制战略造成的影响。信息系统规划时应努力避免有害的意外后果，这意味着在设计信息系统部署时要记住所需考虑的业务和组织策略。例如，信息系统部署并期望员工使用平板电脑提升生产率，但没有对职位描述、流程设计、薪酬计划和业务策略等进行一系列变更，将无法产生预期的生产力改进。信息系统的这类调整只有通过专门设计战略三角的所有三个组成部分才能取得成功。

2. 组织模型

观察历史上曾经发生的重大系统失效灾难，常常发现信息系统战略三角在灾难发生时会出现协同方面的问题。例如：组织机制战略（例如，关于系统运行监测、测试和相应的人事策略、安全策略和实践）不支持信息系统战略（例如，在危机情况下实施监测，管理和中止自动化生产过程的分布式系统网络的运行机制）。而这意味着上述两种策略在规划时都没有充分支持组织的业务战略。而实现三种战略的协同，达成三种战略的一致性代表实现了三角之间的平衡，在一致性基础上，可以向同步与融合方向发展。通过同步，技术不仅可以支撑实现当前的业务战略，还可以预测和塑造未来的业务战略。而融合更进一步，业务战略和信息战略交织在一起，管理团队成员甚至可以互换运作。

1) 业务战略

业务战略阐明了组织寻求的业务目标以及期望如何达成的路径。业务战略是组织传达宣示其目的的方法。管理层根据经济与社会情况、产品与服务对象需求和组织能力构建业务战略计划。经济与社会情况为该类业务构建了竞争环境。产品与服务对象需求是个人及组织想要和需要的可用产品和服务。组织能力包括知识、技能和经验，这些知识、技能和经验为组织提供了

一种可以在经济与社会中增加价值的能力。

描述业务战略的经典框架是迈克尔·波特（Michael E. Porter, 1947—）提出的竞争力优势模型，如图 4-3 所示。

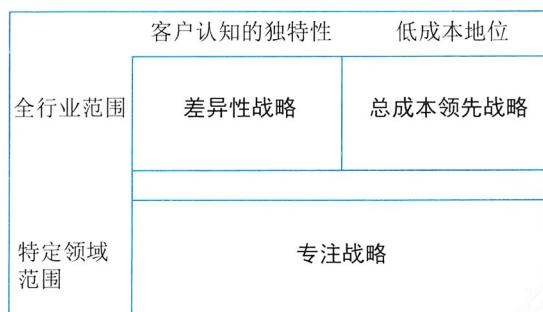


图 4-3 获得竞争力优势的三种战略

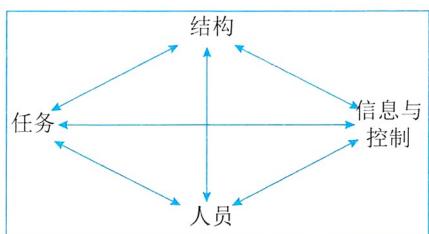
当组织的目标是成为市场上成本最低的生产者时，总成本领先战略就会产生。采用该战略的组织通过最大限度地降低成本，从而获得高于平均水平的绩效。所提供的产品或服务必须在质量上与业内其他人提供的产品或服务相当，以便客户对象感知其相对高性价比。通常，一个行业中只存在一个成本引领者。

采用差异性战略时，组织通过差异化，以一种在市场上显得独特的方式，定义其产品或服务。组织确定哪些定性维度对其客户对象最重要，然后找到在其中一个或多个维度增加产品和服务价值的方法。为了使此策略起作用，差异化因素向客户对象收取的价格必须相对于竞争对手收取的价格，是公平的。

采用专业化战略时，专业化允许组织将其范围限制在更狭窄的细分市场，并为该组客户对象量身定制其产品。该策略有两种变体：①专注成本，在其细分市场内寻求成本优势；②专注差异化，寻求细分市场内的产品或服务的差异化。这种策略使组织能够实现区域竞争优势，即使它没有在整个经济与社会中实现竞争优势，也可以通过专注于某些细分市场的方式获得局部的竞争优势。

2) 组织机制战略

组织机制战略包括组织的设计以及为定义、设置、协调和控制其工作流程而做出的选择。组织机制战略本质上需要回答“组织将如何构建以实现其目标并实施其业务战略”这一问题，并围绕这一问题形成有效的规划。理解组织设计的经典框架是哈罗德·莱维特（Harold J. Leavitt,



1922–2007）提出的钻石模型，如图 4-4 所示。钻石模型将组织计划的关键组成部分标识为其信息与控制、人员、结构和任务，所有组件都是相互关联的。这个简单的框架对于设计新组织和诊断组织问题非常有用。例如，试图改变员工但未能改变其信息与控制方式的组织无法有效运行，因为所有这些组件都会相互影响。

图 4-4 莱维特钻石模型

新时代的组织，其组织机制战略的成功执行包括组织、控制和文化的变量的最佳组合。组织变量包括决策权、业务流程、正式报告关系和非正式沟通网络。控制变量包括数据的可得性、规划的性质和质量、业绩计量和评价制度的有效性以及做好工作的激励措施。文化变量构成组织的价值观。这些组织、控制和文化的变量是决策者用来影响组织变革的管理杠杆。

组织管理人员应具备一套框架，用于评估组织设计的各个方面。使用这些框架，管理人员可以审查当前的组织，并评估哪些组件可能缺失以及未来有哪些可用的选项。基于此框架，管理人员应回答如下问题：

- 组织内有哪些重要的结构和报告关系；
- 谁拥有关键决策的决策权；
- 什么是重要的以人为本的网络（社交和信息网络），我们如何利用它们来更好地完成工作；
- 组织内人员的特征、经验和技能水平是什么；
- 关键业务流程是什么；
- 有哪些控制系统（管理和测量系统）到位；
- 组织的文化、价值观和信仰是什么。

3) 信息系统战略

信息系统战略是组织用来提供信息服务的计划。信息系统支撑组织实施其业务战略。业务战略是关于竞争（服务对象想要什么，竞争做什么），定位（组织想以什么方式竞争）和能力（公司能做什么）的功能。信息系统帮助确定组织的能力。现在使用一个基本的矩阵框架来理解组织必须做出的与信息系统相关的决策，如表 4-1 所示。

表 4-1 信息系统战略矩阵

	有什么	谁使用	在哪里
硬件	信息系统的物理组件清单	系统用户和管理者	组件的物理位置（云端、数据中心等）
软件	程序、应用和工具的清单	系统用户和管理者	软件驻留的硬件，以及硬件的物理位置
网络	硬件和软件组件如何联接的图表	系统用户和管理者；提供服务的组织	节点、线路和其他传输介质所在地
数据	系统中存储的信息位	数据所有者；数据管理者	信息所在地

矩阵框架的目的是为管理者提供一个信息系统组件与策略间关系的观察视图，整体信息系统的四个基础结构组件与其他资源相关事项之间的关系构成了信息系统战略的关键点。基础结构包括：①硬件，如桌面单元和服务器；②软件，如用于开展业务，管理计算机本身以及在系统之间进行通信的程序；③网络，它是硬件组件之间交换信息的物理手段，例如通过专用数字网络实现信息交换；④数据，数据包括存储在系统中的位和字节。在当前的系统中，数据不一定与使用它们的程序一起存储；因此，了解系统中有哪些数据以及它们的存储位置非常重要。

4.1.3 设计和实施

开展信息系统设计和实施，首先需要将业务需求转换为信息系统架构，信息系统架构为将组织业务战略转换为信息系统的计划提供了蓝图。信息系统是支持组织中信息流动和处理的所有基础，包括硬件、软件、数据和网络组件，并以最适合计划的方式进行选择和组装，因此其最能体现组织总体业务战略。

1. 设计方法

大量的可选信息技术，加上技术快速进步，使得组织完成信息系统的“不可完成的任务”。这就需要组织首先将业务战略转化为信息系统架构，然后将该架构转化为信息系统设计，如图 4-5 所示。

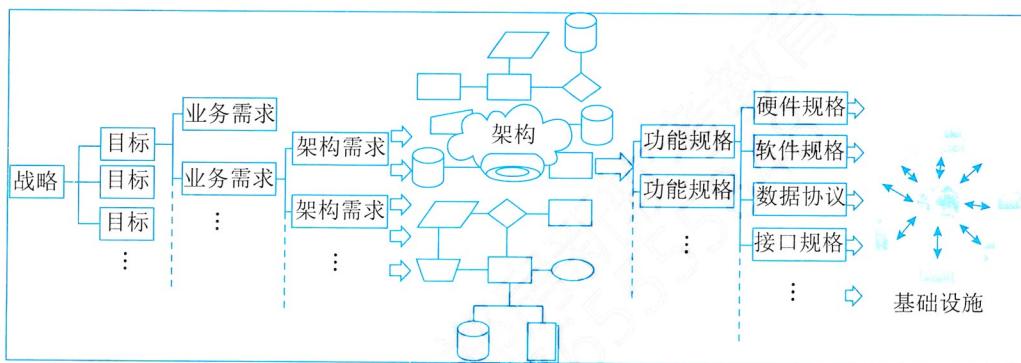


图 4-5 从战略到信息系统设计转换示意图

1) 从战略到系统架构

组织必须从业务战略开始，使用该战略制定更具体的目标。然后从每个目标派生出详细的业务需求。组织需要与架构设计人员合作，将这些业务需求转换为构成信息系统架构的系统要求、标准和流程的更详细视图。这个更详细的视图，即信息系统架构要求，包括考虑数据和流程需求以及安全目标等事项。组织还可以向架构设计人员清楚地了解信息系统必须完成的工作以及确保其顺利开发、实施和使用所需的治理安排。治理安排指定组织中哪个人保留对信息系统的控制权和责任。

2) 从系统架构到系统设计

将信息系统架构转换为系统设计时，需要继承信息系统架构并添加更多细节，包括实际的硬件、数据、网络和软件。进而扩展到数据的位置和访问过程、防火墙的位置、链路规范、互联设计等。信息系统架构被转换为功能规格。功能规格可以分为硬件规格、软件规格、存储规格、接口规格、网络规格等。然后决定如何实现这些规范，并在信息系统基础架构中使用什么硬件、软件、存储、接口、网络等。

信息系统指的不仅仅是组件，这些组件必须根据设计蓝图进行组装，硬件、软件、数据和网络必须以一致的模式组合在一起，才能拥有可行的信息系统。信息系统具有多个级别：①全

局级别可能侧重于整个组织，并构成整个组织的信息环境；②组织间级别信息系统则为跨组织边界的服务对象、供应商或其他利益干系人的沟通交流奠定基础；③应用级信息系统是在考虑特定业务应用时，通常重点考虑的数据库和程序组件，以及它们运行的设备和操作环境。

3) 转换框架

转换框架将业务战略转化为信息系统架构进而转变为信息系统设计，转换框架提出了三类问题：内容、人员和位置，需要为每个信息系统组件回答这些问题。“内容”相关问题是常被问到的，需要回答组件是什么，并确定特定类型的技术等。“人员”相关问题旨在了解相关组件涉及哪些个人、团体和部门。例如，在大多数情况下，单个用户并非系统的所有者；在另外情况下，系统也可能由组织租赁，而不是拥有，这样系统的所有者就成为了组织的外部一方。第三类问题涉及“何处”，随着网络的激增，许多信息系统的功能可能跨越多个位置使用组件，了解信息系统意味着需要了解所有内容各自的位置，如表 4-2 所示。

表 4-2 信息系统架构与基础设施分析框架举例

组件	有什么		谁使用		在哪里	
	系统架构	系统设计	系统架构	系统设计	系统架构	系统设计
硬件	用户将使用什么类型的个人设备	笔记本电脑配备什么尺寸的硬盘驱动器	谁最了解组织中的服务器	谁将运营服务器	架构需要集中式还是分布式服务器	将在 C 地数据中心放置哪些特定的计算机
软件	业务战略是否需要 ERP 软件支持	应该选择 A 品牌还是 B 品牌应用	谁会受到系统向 B 品牌迁移的影响	谁需要 B 品牌的系统培训	组织的地理状况是否需要部署多个数据库基础设施	可以使用一个 D 品牌云数据库实例作为系统数据库吗
网络	需要多大带宽来实现战略	E 单位交换机能否满足需要	哪些人需要连接到网络	无线网络是谁提供的	是否允许每一个用户的手机成为无线接入热点	是否会租赁线缆或使用卫星来支持通信
数据	销售管理系统需要哪些数据	使用什么格式存储数据	哪些人需要访问敏感数据	授权用户如何识别他们自己	备份数据是现场存储还是异地存储	数据是存放于云端系统还是存放于自己的数据中心

2. 架构模式

传统上，信息系统体系架构有三种常见模式（见表 4-3）：①集中式架构。集中式架构下所有内容采用集中建设、支持和管理的模式，其主体系统通常部署于数据中心，以消除管理物理分离的基础设施带来的困难。②分布式架构。硬件、软件、网络和数据的部署方式是在多台小型计算机、服务器和设备之间分配处理能力和应用功能，这些设施严重依赖于网络将它们连接在一起。③面向服务的系统架构（Service-Oriented Architecture, SOA）。SOA 架构中使用的软件通常被引向软件即服务（Software-as-a-Service, SaaS）的相关架构，同时，这些应用程序在通过互联网交付时也被称为 Web 服务。

表 4-3 常见信息系统架构模式

系统架构	描述	别称术语	什么时候使用
集中式架构	大型中央计算机系统处理系统的所有功能。通常，计算机位于数据中心，并由 IT 部门直接管理。存储的数据和应用程序都运行于中央计算机上。网络连接允许用户从远程位置访问大型机	主机架构	当需要系统易于管理时：所有功能都在同一个地方；当业务本身高度集中的时候
分布式架构	运行业务所需的计算能力分散在许多设备中，包括不同位置的服务器、PC 和笔记本电脑、智能手机和平板电脑。设备（有时也被称为客户端）具有足够的处理能力来执行所需的许多服务，并根据数据和专用服务的需要连接中央服务器	基于服务器的架构	当担心可伸缩性时，模块化在这里会有所帮助；当业务主要是非集中化的时候
面向服务的架构	在被称为编排的过程中，将较大的软件程序分解为相互连接的服务。基于此，它们共同构成了一个应用来运行整个业务流程。通常，这些服务可以从互联网上的一系列供应商处获得，而应用程序则是这些服务链接在一起形成的组合	基于 Web 的架构	当希望系统成为敏捷架构：可重用性和组件化利于创造新应用；当业务对新应用和快速设计迭代要求较高时

组织在考虑集中式与分布式架构决策时，必须注意权衡与取舍。例如，分布式架构比集中式架构更加模块化，允许相对容易地添加其他服务器，并能为特定用户添加具有特定功能的客户端，从而提供更大的灵活性和多中心化的组织治理机制，这有可能令架构决策与组织治理目标更协调。相比之下，集中式体系架构在某些方面更易于管理，因为所有功能都集中在主机或小型机中，而不是分布在所有设备和服务器中。集中式架构往往更适合具有高度集中式治理的组织。而 SOA 则越来越受欢迎，因为该设计允许几乎完全从现有的软件服务组件构建大型功能单元。它对于快速构建应用程序非常有用，因为它为管理人员提供了模块化和组件化设计，是一种更易于变更的构建应用程序的方法。

4.1.4 运维和服务

信息系统的运维和服务应从信息系统运行的视角进行整合性的统筹规划，包括对信息系统、应用程序和基础设施的日常控制进行综合管理，以有效支持组织目标达成和流程实现。信息系统的运维和服务由各类管理活动组成，主要包括：运行管理和控制、IT 服务管理、运行与监控、终端侧管理、程序库管理、安全管理、介质控制和数据管理等。

1. 运行管理和控制

IT 团队发生的所有活动都应受到管理和控制。这意味着操作人员执行的所有操作和活动，都应是由管理层批准的控件、过程和项目的一部分。过程和项目应具有足够的记录保存，以便管理层能够了解这些活动的状态。管理层最终负责信息系统运行团队发生的所有活动。管理信息系统运行的管理控制主要活动包括：

- 过程开发：操作人员执行的重复性活动应以过程的形式记录下来，需要开发、审查和批准描述每个过程及其每个步骤的相关文档，并将其提供给运营人员。

- 标准制定：从运行执行任务的方式到所使用的工作，采用标准化定义和约束，从而有效推动信息系统运行相关工作的一致性。
- 资源分配：管理层分配支持信息系统运行的各项能力，包括人力、技术和资源。资源分配应与组织的使命、目标和目的保持一致。
- 过程管理：应测量和管理所有信息系统运行的相关过程，确保过程在时间上和预算目标内被正确和准确地执行。

2. IT 服务管理

IT 服务管理是通过主动管理和流程的持续改进来确保 IT 服务交付有效且高效的一组活动。IT 服务管理由若干不同的活动组成：服务台、事件管理、问题管理、变更管理、配置管理、发布管理、服务级别管理、财务管理、容量管理、服务连续性管理和可用性管理。

(1) 服务台。服务台（Service Desk）是组织体现 IT 服务的重要环节，也是服务干系人体验的重要感知窗口。服务台是服务中与服务干系人沟通和交互的重要界面，负责对服务干系人遇到的问题和需求进行响应和处理；服务台是 IT 服务干系人的“官方”接口和信息发布点，组织内部各个团队之间相互协作的纽带和协调者；服务台对 IT 服务质量及服务干系人体验的管理至关重要，是组织 IT 服务能力持续提升的战略单元。

(2) 事件管理。事件是 IT 服务管理遭遇计划外中断或服务质量出现下降，以及尚未影响服务的配置项故障。事件可能是服务中断、服务速度变慢、软件缺陷以及其他任何组件发生故障。事件管理是 IT 服务中最常见的流程之一，也是 IT 服务必须建立和使用的流程，良好的事件管理必须具备快速解决事件的能力，从而在出现事件时能够尽快恢复服务的正常运作，可以有效提高服务的质量，提升服务干系人满意度。组织应该建立与事件管理过程一致的流程，流程中应该包括：事件受理、分类和初步支持、调查和诊断、解决、进展监控与跟踪、关闭等活动，通过有效执行所定义的活动，能够保障事件响应与处理的效果与效率。

(3) 问题管理。当发生了几个看起来具有相同或相似根本原因的事件时，就会启动问题管理活动。问题管理的总体目标是减少事件的数量和严重性，这种对事件的控制既包括发生事件后的被动性措施，也包括采取主动措施（如：利用系统监控衡量系统运行状况和容量管理等）预防与容量相关的事件发生。与事件管理类似，当确定问题的根本原因时，应制定变更管理和配置管理以进行临时或永久修复。

(4) 变更管理。变更是使一个或更多信息系统配置项的状态发生改变的行动。可见，变更管理的流程更多的是与过程相关，并且重在管理而不是技术，这与事件管理不同，后者建立在技术手段的基础上，强调其管理过程的机械性。变更管理可确保在信息技术环境中执行的所有变更都得到控制和一致化的执行。变更管理的目标是确保使用标准化的方法和程序来高效、及时地处理所有更改，以最大限度地减少与变更相关的事件对服务质量造成的影响，从而改善组织的日常运行。变更管理的主要目的是确保对信息技术环境的所有建议更改都经过适用性和风险管控的审查，并确保变更不会相互干扰，也不会干扰其他计划内或计划外的活动。为了有效，每个干系人都应该审查所有更改，以便正确、全方位地审查每项变更。

(5) 配置管理。配置管理是通过技术或者行政的手段对信息系统的状态进行管理的一系列

活动，这些信息不仅包括信息系统具体配置项信息，还包括这些配置项之间的相互关系。配置项通常包括：硬件详细信息、硬件配置、操作系统版本和配置、软件版本和配置等。配置管理的核心工作是识别、记录、控制、更新配置项信息，主要包含配置管理数据库（Configuration Management Databases, CMDB）的建立以及配置管理数据库准确性的维护，以支持信息系统的正常运行。在IT服务中，配置管理数据库可用于故障定位、问题分析、变更影响度分析、故障分析等，因此，配置管理数据库与真实环境的匹配度和详细度非常重要。

(6) 发布管理。发布管理负责计划和实施信息系统的变更，并且记录该变更的各方面信息。发布是由其实施的变更请求定义的，发布一般是由许多问题修复和IT服务质量改进组成的。发布不仅包括软件方面的变更、硬件方面的变更，同时也包括IT服务管理体系的变更。发布管理通过实施合理的工作程序和严格的监控，保护现有的运营环境和服务不受冲击，负责对软件、硬件、体系发布进行计划、设计、生成、配置和检测，影响范围可能涉及现有的信息系统及其环境、IT用户和组织各分支机构等。

(7) 服务级别管理。服务级别管理就是对IT服务的级别进行定义、记录和管理，并在可接受的成本之下与干系人达成一致的管理过程，通过服务水平协议（Service Level Agreement, SLA）、服务绩效监控和报告的不断循环，持续维护和改进服务质量，以及触发采取行动消除较差服务，从而满足干系人的服务需求。组织需要通过服务目录定义其提供的所有服务和目标。服务目录可被其他文件引用，如SLA，以避免同样的文本和目标被多次重复。服务目录是建立服务干系人预期的关键文件，相关人员都能容易并广泛地获取和阅读。

(8) 财务管理。IT服务财务管理是负责对IT服务运作过程中所有资源进行财务管理的流程，主要活动包括：预算编制、设备投资、费用管理、项目会计和项目投资回报率（Return On Investment, ROI）管理等。财务管理考虑了支持组织目标的IT服务的财务价值。

(9) 容量管理。容量管理用于确认信息系统中有足够的容量满足服务需求。如果信息系统的性能在可接受的范围内，则其具有足够的容量。容量管理不仅仅关注当前需求，还必须考虑未来的需求。容量管理主要活动包括：定期测量、计划变更、战略优化和技术变化等。容量管理由三个子过程组成：业务容量管理、服务容量管理、资源容量管理。

(10) 服务连续性管理。服务连续性管理是一组与组织持续提供服务的能力相关的活动，主要是在发生自然或人为灾难时继续保持服务有效性的活动。服务连续性管理活动分为服务连续性管理的治理、业务影响分析、制订和维护服务连续性计划、测试服务连续性计划、响应与恢复五个过程。

(11) 可用性管理。可用性管理是有关设计、实施、监控、评价和报告IT服务的可用性以确保持续地满足服务干系人的可用性需求的服务管理流程。可用性是指一个组件或一种服务在设定的某个时刻或某段时间内发挥其应有功能的能力，即在约定的服务时段内，IT服务实际能够使用的服务的时间比例。

3. 运行与监控

有效的IT运行要求IT人员按照既定流程和过程理解并正确执行任务。同时，IT运行还强调对人员进行培训，以有效识别异常和错误，并做出正确反应。IT运行的任务常包括：①按照

计划执行作业；②监控作业，并按照优先级为作业分配资源；③重新启动失败的作业和进程；④通过加载或变更备份介质，或通过确保目标的存储系统就绪来优化备份作业；⑤监控信息系统、应用程序和网络的可用性，保证这些系统具备足够的性能；⑥实施空闲期的维护活动，如设备清洁和系统重启等。

IT组织通常制订工作计划，安排定期（每天、每周、每月、每季度等）执行的活动或任务。计划内的活动包括系统承载的活动（如备份）以及人工执行的活动（如访问评审、对账和月末结算）。系统中的计划内活动可以自动或手动调度。大型组织可能具备网络运营中心，也可能具备安全运营中心，这些中心由负责监控相关安全设备、网络、系统和应用程序中的活动的人员组成。在IT运行环境中发生的异常和错误，通常按照IT服务管理体系中的事件管理和问题管理流程进行处理。

1) 运行监控

IT团队应对信息系统、应用程序和基础设施进行监控，以确保它们继续按要求运行。监控工具和系统使IT运行人员能够检测软件或硬件组件何时未按计划运行等。检测和报告的错误类型包括：系统错误、程序错误、通信错误和操作员错误等。IT团队应记录任何意外或异常活动的事件，并基于流程对事件进行管理。

2) 安全监控

组织需要执行不同类型的安全监控，并把安全监控作为其整体策略的一部分，以预防和响应安全事件。组织可能执行的监控类型包括：防火墙策略规则中的例外情况、入侵防御系统的告警、数据丢失防护系统的告警、云安全访问代理的告警、用户访问管理系统的告警、网络异常的告警、网页内容过滤系统的告警、终端管理系统的告警（含反恶意软件）、供应商发布的安全公告、第三方发布的安全公告、威胁情报咨询、门禁系统的告警和视频监控系统的告警等。

4. 终端侧管理

IT团队职能的一个关键环节是它向组织人员提供的服务，以改善他们对IT访问和使用的情况。组织通常使用IT管理工具来促进对用户终端计算机的高效和一致的管理。一般来说，最终用户计算机是“锁定”的，这限制了最终用户可能在其设备上执行的配置更改的数量和类型，包括操作系统配置、补丁安装、软件程序安装、使用外部数据存储设备等，最终用户可能会将此类限制视为不便。但是，这些限制不仅有助于确保最终用户的设备和整个组织的IT环境具有更高的安全性，而且还促进了更高的一致性，从而降低了支持成本。

5. 程序库管理

程序库是组织用来存储和管理应用程序源代码和目标代码的工具。在大多数组织中，应用程序源代码非常敏感。它可能被视为知识产权，并且可能包含算法、加密密钥和其他敏感信息，这些信息应由尽可能少的人员访问。应用程序源代码应被视为信息，并通过组织的安全策略和数据分类策略进行管理。程序库的控制使组织能够对其应用程序的完整性、质量和安全性进行高度控制。程序库通常作为具有用户界面和多种功能的信息系统存在，其中主要功能包括：访问控制、程序签出、程序签入、版本控制和代码分析等。

6. 安全管理

信息安全管理可确保组织的信息安全计划充分识别和解决风险，并在整个运维和服务过程中正常运行。该领域的管理要点详见4.2.3节。

7. 介质控制

组织需要采取一系列活动，以确保数字介质得到适当管理，包括对其保护以及销毁不再需要的数据。这些过程通常与数据保留和数据清除过程相关联，以便通过物理和逻辑的安全控制充分保护所需的数据，同时有效丢弃和擦除不再需要的数据。处置不再需要的介质相关的程序，包括擦除该介质上的数据或使该介质上的数据无法以其他方式恢复的所有相关步骤。组织应考虑包含在介质管理、销毁策略和程序范围内的介质主要包括：备份介质、虚拟磁带库、光学介质、硬盘驱动器、固态驱动器、闪存、硬拷贝等。介质清理的策略和程序需要包含在服务提供商的相关要求中，以及记录保存活动以跟踪介质随时间推移的销毁情况。

8. 数据管理

数据管理是与数据的获取、处理、存储、使用和处置相关的一组活动。该领域管理要点见4.2.1节。

4.1.5 优化和持续改进

优化和持续改进是信息系统管理活动中的一个环节，良好的优化和持续改进管理活动能够有效保障信息系统的性能和可用性等，延长整体系统的有效使用周期。传统上，优化和持续改进常用的方法为戴明环，即PDCA循环。PDCA循环是将持续改进分为四个阶段，即Plan（计划）、Do（执行）、Check（检查）和Act（处理）。

优化和持续改进基于有效的变更管理，使用六西格玛倡导的五阶段方法DMAIC/DMADV，是对戴明环四阶段周期的延伸，包括：定义（Define）、度量（Measure）、分析（Analysis）、改进/设计（Improve/Design）、控制/验证（Control/Verify）。当第四阶段的“改进”替换为“设计”，“控制”替换为“验证”时，五阶段法就从DMAIC转变为DMADV。

1. 定义阶段

定义阶段的目标包括待优化信息系统定义、核心流程定义和团队组建。

(1) 待优化信息系统定义。该活动关注定义协同的范围、优化目标和目的、系统团队成员和出资人，以及优化时间表和交付成果。待优化信息系统范围与关键业务实践、服务对象交互有关，该定义需要了解信息系统相关的业务。可使用“延伸目标”概念来定义待优化的信息系统。延伸目标是那些超出当前组织结构、资源和技术可预见范围的优化目标。可以帮助超越渐进式改进，重新思考信息系统相关业务、运行或流程，以达到可以实现重大改进的程度。

(2) 核心流程定义。该活动关注定义利益干系人、投入和产出以及广泛的功能。SIPOC(Supplier、Input、Process、Output、Customer)分析是定义核心流程视图的首选工具。任何一个组织都是一个由提供人、输入、流程、输出，还有服务对象这样相互关联、互动的5个部分组成的系统。

(3) 团队组建。该活动重点关注从关键利益干系人群体中确定人员组建高能力团队，对信息系统的问题和收益达成共识。有效的团队形成对于建立利益干系人的支持至关重要。从每个关键利益干系人群体中选出可靠的团队成员，以代表他们在优化和持续改进中的职能或领域。有效的团队通常限制为5~7名参与者。较大的团队更难管理，成员可能会失去对团队的责任感。其他团队成员可能是来自非关键利益干系人组的临时成员，他们仅在需要时参与，例如需要流程专业知识时。

2. 度量阶段

度量阶段目标包括流程定义、指标定义、流程基线和度量系统分析。

(1) 流程定义。流程定义通常使用流程图工具定义度量阶段的流程，以图形方式实现给定信息系统的输入、操作和输出。流程图的目的是帮助人们理解流程，应当尽可能简单，但又不能太简单。当流程图指示太多的决策点时，通常表示可能出现了一个过于复杂的过程，可能会出错。因此，决策点恰恰是信息系统优化的一个潜在改进重点。

(2) 指标定义。待优化信息系统的定义包括将用于评估流程的指标。选择能够切实提高系统质量、业务绩效和服务对象满意度的指标非常重要。正确选择的指标将为基于数据的决策提供输入，并将成为用于描述信息系统状态的标准化和数据化的语言。度量指标一旦建立，可用于确定影响信息系统的各种因素及其相对重要性，并可比较信息系统不同组件对业务的整体贡献。指标为信息系统的持续改进提供了对质量、成本和进度的重要描述。如何衡量和报告这些情况，以及这些分别对质量敏感、成本敏感和进度敏感的指标，如何与信息系统的关键流程变量和控制相关联，以实现系统范围的持续改进。

(3) 流程基线。当明确了度量指标之后，必须通过基线确定现有系统的能力，以确定当前系统在多大程度上较好地满足了服务对象的要求，并验证定义阶段中确立的信息系统目标达成情况。当系统处于控制优化状态时，可以统计其系统能力，将统计出的系统变异与明确的服务对象要求进行比较。只有在使用基线清晰描述了系统稳定性之后，才能评估系统变异，只有稳定的系统才能预测。当系统指标数据不稳定或不在控制优化中时，可以使用系统性能指标作为粗略估计，将给定周期内观察的系统变化与服务对象要求进行比较。

(4) 度量系统分析。质量始于度量。只有当质量被量化时，才能开始讨论优化和持续改进。度量是根据某些规则将数值分配给被观察到的现象。在对信息系统进行优化和持续改进过程中，需要十分注意度量水平、度量的可靠性与有效性问题。一个良好的度量系统具备特性可包括：

- 准确：应该产生一个“接近”被测量的实际属性的数值。
- 可重复：如果测量系统反复应用于同一物体，则产生的测量价值应彼此接近。
- 线性：测量系统应能够在整个关注范围内产生准确和一致的结果。
- 可重现：当任何经过适当培训的个人使用时，测量系统应产生相同的结果。
- 稳定：应用于相同的项目时，测量系统将来应产生与过去相同的结果。

3. 分析阶段

分析阶段的三个目标包括价值流分析、信息系统异常的源头分析和确定优化改进的驱动因素。

(1) 价值流分析。价值流分析首先定义信息系统使用者眼中相关产品或服务的价值。价值也可以定义为：①组织愿意投资的系统组件；②改变信息系统形式、适合度或功能的活动；