国际标准

ISO/IEC 20000-1

第二版

2011-04-15

Information technology — Service management—

Part 1:

Service management system

Requirements

信息技术-服务管理-第一部分：

服务管理体系要求

参考编号

ISO/IEC 20000-1:2011(E)

 英文版版权信息

版本记录：

版本号	版本日期	修改说明
0.80	2011-4-28	创建文档并约定翻译要素。
0.90	2011-5-9	完成整体文档翻译。
0.95	2011-5-14	根据一次评审结果对内容进行确认调整。
0.99	2011-5-22	根据相关资料及中文报批稿统一相关词汇。
1.0	2011-6-3	正式版本。

声明：

本文档为 IT 治理网（www.itzl.org）翻译版，原标准版权属 ISO 所有，本文档仅供培训、学习和研究使用，不得用于任何商业用途。

因时间仓促，加之水平有限，疏漏之处再所难免，恳请读者提出宝贵意见，以便再版时进行修改。

翻译小组成员	联系方式
翟耀纲	zhaiyaogang@itzl.org
杨延康	yangyankang@itzl.org
樊炳荣	fanbingrong@itzl.org
何亮	hl@itzl.org

感谢在此期间以下评审人员的参与：

评审人员	联系方式
霍松龄	huosongling@chinagoldgroup.com
李俊	lijun@chinagoldgroup.com
王猛	wangmeng@nxmy.com

如有任何问题请反馈至：research@itzl.org。

目录

图示

前言

ISO（国际标准化组织）和 IEC（国际电工协会）组建了世界性的标准化的专业体系。ISO 和 IEC 的成员单位如对某特定项目感兴趣，可加入由 ISO 和 IEC 组织的技术委员会，以参与相关技术工作。ISO 和 IEC 在双方感兴趣的领域设立联合委员会。与 ISO 保持联系的各国际组织（官方的或非官方的）也可参加有关工作。ISO 与 IEC 在电工技术标准领域建立了联合技术委员会 ISO/IEC JTC 1。

国际标准是根据 ISO/IEC 导则第 2 部分的规则起草。

联合技术委员会的主要任务是制定国际标准。由技术委员会通过的国际标准草案提交各成员团体投票表决。国际标准草案需取得至少 75%参加表决成员团体的同意，才能作为国际标准正式发布。

本文件中的某些内容有可能涉及一些专利权问题，对此应引起注意，ISO/IEC 不负责识别任何这样的专利权问题。

ISO/IEC 20000-1 由 ISO/IEC JTC 1/SC 7 信息技术联合技术委员会软件和系统工程分会制定。第二版替代第一版标准（ISO/IEC 20000-1:2005），以及对其进行的技术性修订。主要的不同点如下：

--更接近 ISO 9001；
--更接近 ISO/IEC 27001；
--术语的变化，以同国际惯例接轨；
--更多定义的增加，部分定义的更新和两个定义的删除；
--术语“服务管理体系（SMS）”的引入；
--整合了 ISO/IEC 20000-1:2005 的条款 3 和条款 4，使管理体系要求集中于一个条款；
--其他方运行过程的治理要求的澄清；
--对服务管理体系（SMS）的范围进行定义等要求的澄清；
--澄清 PDCA 方法论适用于服务管理体系（SMS），包括服务管理过程及服务；
--设计和转换新的或变更的服务新要求的引入。

ISO/IEC 20000 标准族由下列名为“信息技术-服务管理”标准构成，包括：

--第 1 部分：要求
--第 2 部分：应用服务管理体系指南
--第 3 部分（技术报告）：ISO/IEC 20000-1 范围定义和适用性指南
--第 4 部分（技术报告）：过程参考模型
--第 5 部分（技术报告）：实施 ISO/IEC 20000-1 计划的模型

服务管理的一个过程评估模型将在不久的将来推出，作为第 8 部分的一个章节。

引言

ISO/IEC 20000 的本部分要求包括设计、转换、交付和改进服务，以满足服务需求并向客户和服务提供方提供价值。ISO/IEC 20000 的本部分要求服务提供方在计划、建立、实施、运行、监控、回顾、维护和改进服务管理体系（SMS）时，采用整体的过程方法。

服务管理体系(SMS)协调一致的整合与实施可提供实时的控制以及更有效和更高效率的持续改进机会。ISO/IEC 20000 的本部分定义运行的过程要求要很好地组织和协调人员。要求采用适宜的工具以确保过程是有效的和有效率的。

最有效的服务提供方在服务的生命周期中的所有阶段，从战略到设计、转换和运行，包括持续改进都要考虑对服务管理体系（SMS）的影响。

ISO/IEC 20000 的本部分要求已知的“策划-实施-检查-处置”（PDCA）方法论应用于服务管理体系（SMS）和服务的所有部分。本部分采用的 PDCA 方法论，可以简单描述为：

P-策划：建立书面和协定的服务管理体系（SMS）。服务管理体系包括满足服务需求的方针、目标、计划和过程；

D-实施：实施和运行服务管理体系（SMS），以设计、转换、交付和改进服务；

C-检查：根据方针、目标、计划和服务需求，对服务管理体系（SMS）进行监视、测量和回顾，并报告结果；

A-处置：采取措施，以持续改进服务管理体系（SMS）和服务的绩效。

当用于服务管理体系(SMS)时，以下内容是整合过程方法和 PDCA 方法论最重要的方面：

a） 理解和满足服务需求以使客户满意；

b） 建立服务管理的方针和目标；

c） 基于为客户增加价值的服务管理体系（SMS）设计和提供服务；

d） 监视、测量和回顾服务管理体系（SMS）和服务；

e） 基于目标测量以持续改进服务管理体系（SMS）和服务。

图1说明了PDCA方法论可以应用到服务管理体系（SMS），包括定义条款5-9的服务管理过程和服务。PDCA方法论的元素都是成功实施服务管理体系的关键部分。ISO/IEC 20000本部分的改进过程也基于PDCA方法论。

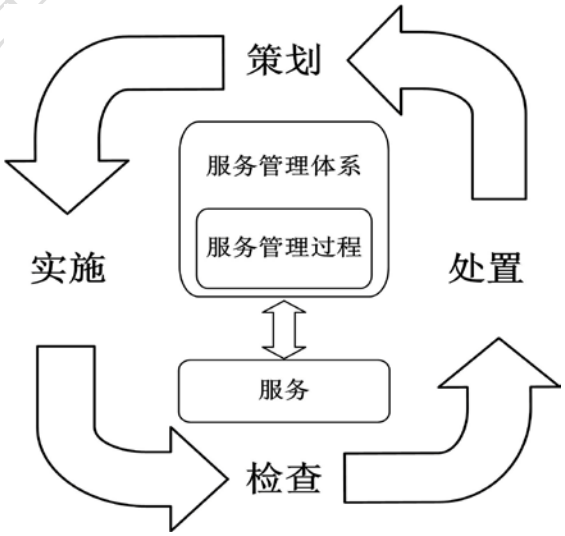

图 1 PDCA 方法论在服务管理的应用

ISO/IEC 20000本部分允许服务提供方在组织中将服务管理体系（SMS）和其他管理体系整合为一体。采用整合的过程方法和PDCA方法论可以使服务提供方能协调或完全整合多个管理体系标准。例如，服务管理体系可以与基于ISO 9001的质量管理体系和基于ISO/IEC 27001的信息安全管理体系整合。

ISO/IEC 20000的目的是独立的特定的指南。服务提供方可以结合使用其他普遍接受的指南和自身的经验。

国际标准的使用者对标准的正确应用负责。国际标准并非旨在包括所有法律法规和服务提供方签署合同义务的要求。对国际标准的遵守并不意味着免除遵守法律法规的义务。

我们鼓励使用者分享对ISO/IEC 20000-1的观点以及对ISO/IEC 20000标准族其他标准修改的优先顺序的意见，进而促进IT服务管理标准的研究。请点击以下链接参加在线调查：

ISO/IEC 20000-1在线调查

信息技术　服务管理　第一部分：服务管理体系要求

1 范围

1.1 总则

ISO/IEC 20000的本部分是服务管理体系（SMS）标准。它为服务提供方定义了策划、建立、实施、运行、监视、回顾、维护和提高服务管理体系的要求。该要求包括服务的设计、转换、交付和改进，以满足服务需求。ISO/IEC 20000的本部分可被用于：

a） 从服务提供方寻求服务并要保证其服务需求被满足的组织；

b） 要求对所有供应商，包括供应链，采用一致性方法的组织；

c） 目的在于展示其服务的设计、转换、交付和改进能力满足服务需求的服务提供方；

d） 监视、测量和评审其服务管理过程和服务的服务提供方；

e） 通过有效的实施和运行服务管理体系（SMS）改进服务的设计、转换和交付的服务提供方；

f） 作为评估服务者的服务管理体系（SMS）满足 ISO/IEC 20000 本部分的准则的评估师或审核员。

图2说明了服务管理体系（SMS），包括服务管理过程。不同的服务提供方可采用不同的方式处理服务管理过程和过程之间的相关性。供应商和客户之间的实质关系将影响服务管理过程如何实施。

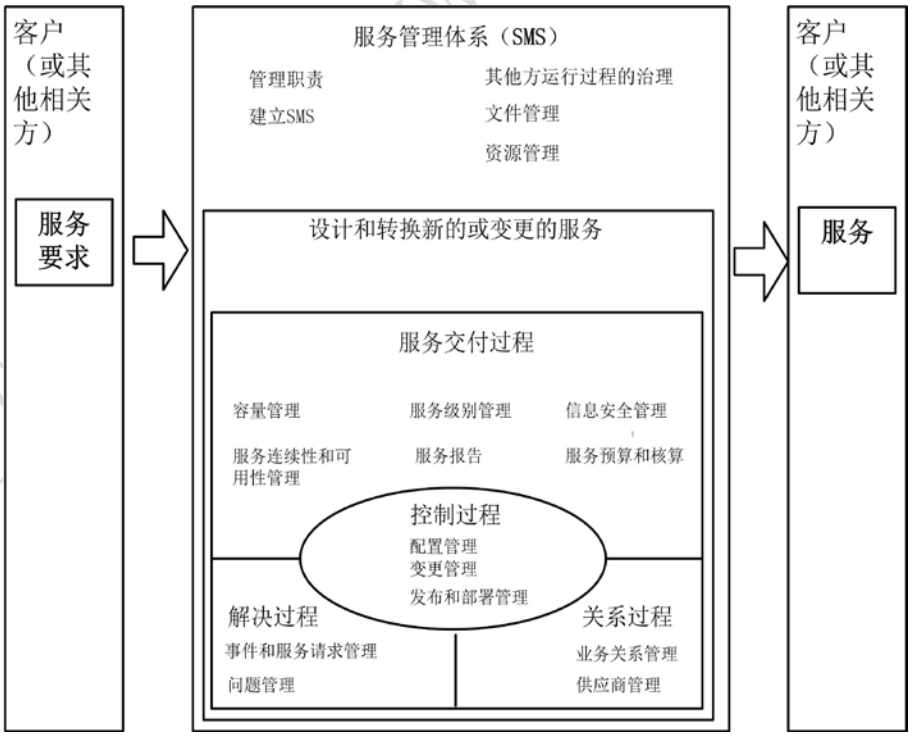

图 2 服务管理体系

1.2 应用

ISO/IEC 20000的本部分是通用的，无论供应商的类型、规模和服务交付的特性，都可被采用。无论服务提供方组织有任何特性，宣称符合ISO/IEC 20000本部分的服务提供方对条款4-9的任何裁剪都是不可接受的。

ISO/IEC 20000的本部分条款4的符合性仅限于服务提供方展示其自身证据，以说明满足条款4的所有要求。服务提供方不能将其他方运行过程治理作为条款4的证据。

服务提供方可以展示自身证据，以证明符合条款5-9的符合性的要求。另外，服务提供方也可以展示满足大多数要求的自身证据和不直接操作的、其他方管理运行全部或部分过程产生的证据。

ISO/IEC 20000的本部分排除特定的产品或工具。然而，组织可以使用ISO/IEC 20000的本部分开发支持服务管理体系（SMS）运行的产品和工具。

注：ISO/IEC 20000-3提供ISO/IEC 20000的本部分范围定义和适用性的指南。这包括更明确的关于其他方管理运行的过程的解释。

2 标准参考文献

以下引用的文献对本文件的应用是不可缺少的。凡是注日期的引用文件，仅引用的版本适用。凡是不注日期的引用文件，其最新版本（包括所有的修订）适用于本标准。

本条款中没有引用标准参考文献。本条款仅为确保条款的顺序与 ISO/IEC 20000-2：信息技术-信息管理-第 2 部分：实施服务管理体系指南保持一致。

3 术语和定义

下列术语和定义适用于ISO/IEC 20000-1:2011的本部分。

3.1 可用性 availability

在协定的中断或规定时间段内，服务组件或服务执行要求功能的能力。

注：可用性通常用客户使用的实际可用服务或服务组件的时间与约定服务时间的比率或百分比表示。

3.2 配置基线 configuration baseline

在服务或服务组件生命周期过程中特定时间段正式指定的配置信息。

注1：配置基线，附加这些基线批准的变更单，构成现行的配置信息。

注2：采纳自ISO/IEC/IEEE 24765:2010。

3.3 配置项 configuration item (CI)

为交付单个或多个服务需求控制的所有要素。

3.4 配置管理数据库 configuration management database (CMDB)

存储用来记录每个配置项的特性和配置项之间关系的数据。

3.5 持续改进 continual improvement

增强满足服务需求的能力的循环活动。

注：改编自ISO 9000:2005。

3.6 纠正措施 corrective action

为消除已发现的不合格或其他不期望情况的原因所采取的措施。

注：改编自ISO 9000:2005。

3.7 客户 customer

接受单个或多个服务的组织或组织的一部分。

注1：客户可以是组织内部的或外部的。

注2：改编自ISO 9000:2005。

3.8 文件 document

信息及其承载媒介。

[ISO 9000:2005]

例如：方针、计划、过程描述、程序、服务级别协议、合同文本。

注 1："documentation"可以是任何类型的媒介。

注 2：在 ISO/IEC 20000 中的文件，除了记录，其陈述的意图都要得以实现。

3.9 有效性 effectiveness

完成计划的活动并得到计划结果的程度。

[ISO 9000:2005]

3.10 事件 incident

非计划的服务中断、服务质量的降低或尚未对客户服务造成影响的事情。

3.11 信息安全 information security

保护信息的机密性、完整性和可访问性。

注1：另外，也可以涉及其他一些特性，如真实性、可追责性、不可抵赖性和可靠性。

注2：在本定义中未使用术语"可用性"，因为在ISO/IEC 20000的本部分定义该术语是不适合的。

注3：改编自ISO27000:2009。

3.12 信息安全事件 information security incident

单个或一系列不需要的或非预期的、有明显的可能性危害业务运行和威胁信息安全的事情。

[ISO/IEC 27000:2009]

3.13 相关方 interested party

与服务提供方行为或行动的业绩或成就有利益关系的个人或团体。

示例：客户、所有者、员工、管理方、服务提供方组织内的人员、供应商银行、工会或合作伙伴。

注1：一个团体可由一个组织或其一部分组织或多个组织构成。

注2：改编自ISO 9000:2005

3.14 内部团体 internal group

服务提供方组织内部的一部分，与服务提供方有书面的协定，协助单个服务或多个服务的设计、转换、交付和改进。

注：内部团体在服务提供方服务管理体系（SMS）的范围之外。

3.15 已知错误 known error

寻找到根本原因或找到减少或降低对服务冲击的规避方法的问题。

3.16 不合格 nonconformity

未满足的要求。
[ISO 9000:2005]

3.17 组织 organization

一组职责、权限和相互关系得到安排的人员和设施。
示例：公司、集团、商业、企事业单位、研究机构、慈善机构、代理商、社团或上述组织的部分或组合。
注1：安排通常是有序的。
注2：组织可以是公有的或私有的。
[ISO 9000:2005]

3.18 纠正措施 corrective action

为避免或消除不合格的起因，或减少不合格或其他不期望情况复发的可能性所采取的措施。
注：改编自ISO 9000:2005。

3.19 问题 problem

造成一个或多个事件的根本原因。
注：问题的根本原因在问题创建通常是未知的，问题管理过程就是负责探寻这些未知。

3.20 程序 procedure

为进行某项活动或过程所规定的途径。
[ISO 9000:2005]
注：程序可以是书面的也可以是口头的。

3.21 过程 process

将输入转化为输出的相互关联或相互作用的一组活动。
[ISO 9000:2005]

3.22 记录 record

阐明所取得的结果或提供所完成活动的证据的文件。
[ISO 9000:2005]
示例：审核报告，事件报告，培训记录或会议纪要

3.23 发布 release

作为一个或多个变更的结果而同时引入现实环境的一个或多个新配置项或变更的配置项的集合。

3.24 变更请求 request for change

提出的针对服务、服务组件或服务管理体系（SMS）的变更建议。

注：对服务的变更包括准备新的服务或移除不再需要的服务。

3.25 风险 risk

对目标不确定性的影响。

注1：影响是对期望的偏离-正面和（或）负面的。

注2：目标可以有不同的方面（例如财务、健康、安全和环境目标）和不同的层级（如战略级、组织范围级、项目级、产品级和过程级）。

注3：风险的特点往往参照潜在事件和后果，或者它们的组合；

注4：风险在术语中通常表述为一个事件的后果（包括环境的变更）和相关后果发生可能性的组合。

[ISO 31000:2009]

3.26 服务 Service

意味着提供价值达到客户期望结果的服务。

注1：服务通常是无形的。

注2：服务提供方、内部团体或客户自身可以作为提供者交付的服务。

3.27 服务组件 service component

单一的服务单元与其他单元结合时将交付一套完整的服务。

示例：硬件，软件，工具，应用，文件，信息和过程或支持服务。

注：一个服务组件可以有一个或多个配置项构成。

3.28 服务的连续性 service continuity

管理一系列影响单个或多个服务的风险和事件，持续提供协定级别服务的能力。

3.29 服务级别协议（SLA） service level agreement

服务提供方与客户之间签署的，明确了服务和服务目标的书面协议。

注1：服务级别协议可在服务提供方和供应者、内部团体或作为供应商的客户之间建立。

注2：服务级别协议可以包含在合同或其他任何类型的书面的协定中。

3.30 服务管理 service management

一组能力和过程，指导和控制服务提供方的活动和资源，设计、转换、交付和改进服务，以满足服务需求。

3.31 服务管理体系（SMS）service management system

管理体系，用来指导和控制服务提供方的服务管理活动。

注1：管理体系是一组相关或交互的元素，建立方针和目标并实现这些目标。

注2：服务管理体系（SMS）包括所有服务管理的方针、目标、策略、过程、文件和资源，只要它们满足ISO/IEC 20000本部分要求，以及用于服务的设计、转换、交付和改进的相关要求。

注3：改编自ISO 9000：2005中“质量管理体系”的定义。

3.32 服务提供方 service provider

为客户提供单个或多个服务的组织或组织的一部分。

注：对于服务提供方的组织来说，客户可以是内部的或外部的。

3.33 服务请求 service request

请求提供信息、建议、访问某个服务或预先核准的变更。

3.34 服务需求 service requirement

客户和用户对服务的需求，包括服务级别的要求，以及对服务提供方的要求。

3.35 供应商 supplier

服务提供方组织之外的组织或服务提供方组织的一部分，与服务提供方签订合同，协助单个服务或多个服务或过程的设计、转换、交付和改进。

注：供应商包括指定的主供应商，但不包括他们的分包商。

3.36 最高管理者 top management

在最高层指挥和控制服务提供方的一个人或一组人。

注：改编自ISO 9000:2005。

3.37 转换 transition

将新的或变更的服务纳入现实环境或从现实环境移出的一组活动。

4 服务管理体系总要求

4.1 管理职责

4.1.1 管理承诺

最高管理者应通过以下活动，对其策划、建设、实施、运行、监控、评审、维护和改进服务管理体系（SMS）和服务提供证据：

a） 建立和沟通服务管理的范围、方针和目标；

b） 确保服务管理计划的创建、实施和维护，以坚持服务方针、实现服务目标和满足服务需求；

c） 传达满足服务需求的重要性；

d） 传达满足法律法规要求和合同义务的重要性；

e） 确保提供资源；

f） 按照计划的时间间隔实施管理评审；

g） 确保已经评估和管理服务风险。

4.1.2 服务管理方针

最高管理者应确保服务方针：

a） 与服务提供方的宗旨相适应；

b） 包括对满足服务需求的承诺；

c） 包括通过条款4.5.5.1的持续改进方针对持续改进服务管理体系（SMS）和服务有效性的承诺；

d） 提供制定和评审服务管理目标的框架；

e） 传达至服务提供方的每个人，并统一认识；

f） 在持续适宜性方面得到评审。

4.1.3 权限、职责和沟通

最高管理者应：

a） 已规定确保服务管理的职责、权限，并沟通；

b） 已经建立并实施书面的沟通程序。

4.1.4 管理者代表

最高管理者应指定服务提供方管理层的一个成员，无论该成员在其他方面的职责如何，具有以下方面的职责和权限：

a） 确保执行识别、记录和满足服务需求的活动；

b） 分配权限和职责，确保根据服务管理的方针和目标设计、实施和提高服务管理过程；

c） 确保服务管理过程是与其他服务管理体系（SMS）管理组件整合的；

d） 确保用于交付服务的资产（包括许可证），其管理遵从法律法规要求和合同义务；

e） 向最高管理者报告服务管理体系（SMS）的业绩和任何改进的机会。

4.2 其他方运行过程的治理

对于条款5-9的过程，服务提供方应识别所有被其他方全部或部分运行的过程。其他方可以是内部团体、客户或供应商。服务提供方应通过以下活动说明对其他方运行过程的治理：

a） 说明问责的过程和遵守过程要求的证明；

b） 控制过程的定义和与其他过程的接口；

c） 确定过程的性能和对过程需求的遵守；

d） 控制过程改进的计划和优先级。

当供应商运行过程的一部分时，服务提供方应通过供应商管理过程对其进行管理。当内部团体或客户运行部分过程时，服务提供方应通过服务级别管理对内部团体或客户进行管理。

注：ISO/IEC TR 20000-3提供了ISO/IEC 20000本部分范围定义和实用性的指导。包括未来对其他方运行过程的解释。

4.3 文件管理

4.3.1 建立和维护文件

服务提供方应建立和维护包括记录在内的文件，以确保有效的计划、运行和控制服务管理体系（SMS）。这些文件应包括：

a） 形成服务管理方针和目标的文件；
b） 形成服务管理计划的文件；
c） 形成本部分要求的特定过程方针和策略的文件；
d） 形成服务目录的文件；
e） 形成服务级别协议（SLAs）的文件；
f） 形成服务管理过程的文件；
g） 形成本部分要求的过程和程序的文件；
h） 附加的文件，由服务提供方确定保证服务管理体系（SMS）运行有效和服务交付必要的文件，包括外部来源文件。

4.3.2 文件控制

服务管理体系（SMS）所要求的文件应予以控制。记录是一种特殊类型的文件，应依据条款4.4.3的要求进行控制。

应编制形成文件的程序，包括权限和职责，以规定以下方面所需的控制：

a） 文件发布前得到批准；
b） 通知相关方新的或变更的文件；
c） 必要时对文件进行评审与维护；
d） 确保文件的更改和现行修订状态得到识别；
e） 确保在使用处可获得有关版本的使用文件；
f） 确保文件清晰、易于识别；
g） 确保外来文件得到识别并控制其分发；
h） 防止作废文件的非预期使用，若因任何原因而保留作废文件时，对这些文件进行适当的标识。

4.3.3 记录控制

为符合要求和服务管理体系（SMS）有效运行应保留记录。

应编制形成文件的程序，以规定记录的标识、储存、保护、检索、保存和处置所需的控制记录应保持清晰、易于识别和检索。

4.4 资源管理

4.4.1 资源提供

服务提供方应确定和提供以下活动所需要的人员、技术、信息和财务资源：

a） 建立、实施和维护服务管理体系（SMS）和服务，并持续改进它们的有效性；
b） 通过提供满足服务需求的服务增强客户的满意度。

4.4.2 人力资源

基于适当的教育、培训、技能和经验，从事影响服务需求的符合性工作的服务提供方人员应是能够胜任的。服务提供方应：

a） 确定人员必须的能力；
b） 适用时，提供培训或采取其他措施以使人员获得所需的能力；
c） 评价所采取措施的有效性；
d） 确保人员认识到他们如何为实现服务管理目标和满足服务需求做出贡献；
e） 确保教育、培训、技能和经验的适当记录。

4.5 建立和改进服务管理体系

4.5.1 定义范围

服务提供方应在服务管理策划中定义和包含服务管理体系（SMS）的范围。范围应定义提供服务的组织单元名称和所交付的服务。

服务提供方应考虑其他影响服务交付的因素，包括：

a） 服务提供方交付服务的地理位置；
b） 客户和他们的位置；
c） 用于提供服务的技术。

注：ISO/IEC TR 20000-3 提供了 ISO/IEC 20000 本部分的范围定义和适用性的指南。

4.5.2 策划服务管理体系（策划）

服务管理者应创建、实施和维护服务管理策划。策划应考虑服务管理方针、服务需求和ISO/IEC 20000本部分的要求。服务管理策划应包含或包括至少引用以下方面：

a） 服务提供方要达到的服务管理目标；
b） 服务需求；
c） 冲击服务管理体系（SMS）的已知限制；
d） 方针、标准、法律法规需求和合同义务；
e） 权限、职责和过程角色框架；
f） 针对策划、服务管理过程和服务的权限和职责；
g） 完成服务管理目标所需的人员、技术、信息和财务资源；
h） 涉及设计和转换新的或变更的服务过程时，与其他方共同工作所采取的方法；
i） 服务管理过程之间的接口和与服务管理体系（SMS）其他组件整合，要执行的过程；
j） 管理风险和风险接受准则所采取的方法；
k） 用于支持服务管理体系（SMS）的技术；
l） 如何测量、审核、汇报和改进服务管理体系（SMS）和服务的有效性。

任何针对特定过程生成的策划都应与服务管理策划保持一致。服务管理策划和为特定过程生成的策划应按照计划的时间间隔评估，如果适用的话，要进行更新。

4.5.3 实施和运行服务管理体系（实施）

服务提供方应实施和运行服务管理体系（SMS），根据服务管理设计、转换、交付和改进服务，活动至少包括以下：

a） 资金和开支的分配；

b） 权限、职责和过程角色的分配；
c） 管理人员、技术和信息资源；
d） 识别、评估并管理服务的风险；
e） 服务管理过程的管理；
f） 监视和报告服务管理活动的绩效；

4.5.4 监视和评审服务管理体系（检查）

4.5.4.1 总要求

服务提供方应采用适当的方法来监视、测量服务管理体系（SMS）和服务。这些方法应包括内部审核和管理评审。

任何内部审核和管理评审的目标应是书面的。内部审核和管理评审应证明服务管理体系（SMS）和服务达到服务管理目标和满足服务需求的能力。违反ISO/IEC 20000本部分要求、服务提供方自身服务管理体系要求或服务需求的不合格应予以识别。

内部审核管理评审的结果，包括不合格、关注和识别的改进都应记录。结果和改进都应与相关方沟通。

4.5.4.2 内部审核

服务提供方应按照计划的时间间隔进行内部审核，以确定服务管理体系（SMS）和服务是否：

a） 符合 ISO/IEC 20000 本部分的要求；
b） 符合服务需求以及服务提供方确定的服务管理体系（SMS）的需求；
c） 得到有效实施和保持。

应编制形成文件的程序，以规定审核的策划、实施以及报告结果和保持记录的职责和要求。

审核方案应进行策划。应考虑虚拟审核的过程和区域的状况和重要性以及以往审核的结果。审核的准则、范围、频次和方法应形成书面文件。

审核员的选择和审核的实施应确保审核过程的客观性和公正性。审核员不应该审核自己的工作。

不合格应被沟通、分优先顺序并分配职责进行处置。负责受审区域的管理者应确保及时采取必要的纠正措施，以消除所发现的不合格及其原因。跟踪活动应包括对采取措施的验证和验证结果的报告。

注：作为管理体系审核的指南，参见ISO 19011。

4.5.4.3 管理评审

最高管理者应按计划的时间间隔评审服务管理体系（SMS），以确保其持续性的适宜性和有效性。评审应包括评价服务管理体系改进的机会和变更的需要，包括服务管理方针和服务管理目标。

管理评审的输入应包括至少以下信息：

a） 客户反馈；
b） 服务和过程的绩效和符合性；
c） 现在和未来人员、技术、信息和财务资源级别；
d） 现在和未来人员和技术能力；

e） 风险；
f） 审核结果和跟踪措施；
g） 以往管理审核的结果和跟踪措施；
h） 预防和纠正措施的状况；
i） 可能影响服务管理体系（SMS）的变更；
j） 改进机会。

应保持管理评审的记录。

管理评审的记录应至少包括对资源的决策和处置，服务管理体系（SMS）有效性的改进和服务的改进。

4.5.5 维护和改进服务管理体系（处置）

4.5.5.1 总要求

应有持续改进服务管理体系（SMS）和服务的方针。方针应包括评价改进机会的准则。

应制定书面的程序，包括识别、记录、评估、批评、排定优先级顺序、管理、测量和报告改进的权限和职责。改进的机会包括纠正和预防措施，应以书面形式确定。

已确定不合格的原因应被纠正。纠正措施应用于消除已确定不合格的原因，防止不合格再次发生。预防措施应用于消除潜在不合格的原因，以预防不合格的发生。

注：更多纠正和预防措施的信息，参照ISO 9001:2008的条款8.5。

4.5.5.2 管理改进

改进机会应排出优先顺序。决策改进机会时，服务提供方应使用持续改进方针中的评价标准。

批准的改进应被策划。

服务提供方应管理改进活动，至少包括：

a） 在质量、价值、能力、成本、生产率、资源利用率和风险降低等一个或多个方面设定改进目标；
b） 确保批准的改进被实施；
c） 必要时，修订服务管理方针、策划、过程和程序；
d） 根据设定的目标测量实施的改进，当目标不能实现时，采取必要的措施；
e） 报告实施的改进。

5 设计和转换新的或变更的服务

5.1 总要求

任何对现有服务或客户有潜在重大冲击的新服务或对服务的变更，服务提供方应使用变更管理过程。作为变更管理过程的一部分，变更管理方针应确定在条款5范围内的变更。

评估、批准、安排和评审条款5范围内的新的或变更的服务应由变更管理过程控制。条款5范围内的新的或变更的服务影响配置项（CIs）应由配置管理过程控制。

服务提供方应依据协定的服务需求和条款5.2、5.3相关的要求，评审策划和设计活动的输出。基于评审，服务提供方应接受或拒绝输出。服务提供方应采取必要的措施，保证新的或变更的服务的开发和转换执行是有效的、是使用接受的输出的。

注：新服务或服务的变更可源于客户，服务提供方、内部团体或供应商，其目的是为满足业务需求或改进服务的有效性。

5.2 策划新的或变更的服务

服务提供方应识别新的或变更的服务的需求。应策划新的或变更的服务以满足服务需求。策划新的或变更的服务应与客户和相关协商。

作为策划的输入，服务提供方应考虑提供新的或变更的服务，对财务、组织和技术的潜在冲击。服务提供方应同时考虑新的或变更的服务对服务管理体系（SMS）的潜在冲击。

策划新的或变更的服务应至少包含或包括引用以下内容：

a） 设计、开发和转换活动的权限和职责；

b） 由服务提供方和其他方执行的活动，包括从服务提供方到相关方接口的活动；

c） 通报给相关方；

d） 人员、技术、信息和财务；

e） 策划活动的时间跨度；

f） 识别、评估和管理风险；

g） 依赖的其他方；

h） 新的或变更的服务的测试要求；

i） 服务验收准则；

j） 以可测量术语表示的提供新的或变更的服务而产生的预期结果。

对于将要删除的服务，服务提供方应做出服务的删除计划。计划应包括移除、归档、销毁或传递的数据、文件和服务组件。服务组件可包括基础架构和有授权的应用。

服务提供方应识别新的或变更的服务的其他方，只要他们协助提供服务组件。服务提供方应评估他们满足服务需求的能力。应记录评估结构并采用必要的措施。

5.3 设计和开发新的或变更的服务

应设计并以书面形式明确新的或变更的服务，至少包括：

a） 交付新的或变更的服务的权限和职责；

b） 交付新的或变更的服务所需由服务提供方、客户和其他方执行的活动；

c） 新的或变更的人力资源要求，包括适当的教育、培训、技巧和经验要求；

d） 交付新的或变更的服务的财务资源要求；

e） 支持交付的新的或变更的服务的新的或变更的技术；

f） ISO/IEC 20000 本部分要求的新的或变更的策划和方针；

g） 与服务需求一致的新的和变更的合同和其他文件；

h） 对服务管理体系（SMS）的变更；

i） 新的或变更的 SLAs；

j） 服务目录的更新；

k） 用于交付新的或变更服务的程序、测量和信息。

服务提供方应当确保设计以使新的或变更的服务满足服务需求；

应根据书面的设计开发新的或变更的服务。

注：关于设计的更多信息，参见ISO 9001:2008的条款7.3设计和开发过程或ISO/IEC 15288:2008的条款6.4.3结构化设计过程。

5.4 转换新的或变更的服务

应通过对新的或变更的服务测试以证明满足服务需求和设计文件。新的和变更的服务应验收通过，服务验收准则由服务提供方和相关方事先协定。如果未达到服务验收标准，服务提供方和相关方应决定采取必要的措施修正。

发布和部署管理过程应应用在实际环境中部署已批准的新的或变更的服务。

转换活动完成后，服务提供方应向相关方汇报期望成果和实际结果的对比。

6 服务交付过程

6.1 服务级别管理

服务提供方应与客户协定交付的服务。

服务提供方应与客户协定服务目录。服务目录应包括服务和服务组件之间的依赖关系。

所交付的每个服务，应与客户协定在一个或多个服务级别协议(SLAs)中。当创建服务级别协议时，服务提供方应考虑服务需求。SLAs应包括协定的服务目标、工作量特性和期望。

服务提供方应与客户按照计划的时间间隔评审服务和SLAs。

变更管理过程应对书面的服务需求、服务目录、SLAs和其他书面协议的变更控制。服务和SLAs变更后，服务目录应及时更新，以确保它们是一致的。

服务提供方应按照计划的时间间隔，依据服务目标监视趋势和绩效。结果应记录和评审以识别造成不合格的原因和改进的机会。

针对由内部团体或客户提供的服务组件，服务提供方应开发、协定、评审和维护书面的协议，以定义双方的活动和接口，依据协定的服务目标和其他协定的承诺，服务提供方应按照计划的时间间隔监视内部团体或客户的绩效。结果应记录和评审以识别不合格的原因和改进的机会。

6.2 服务报告

服务提供方与相关方协定形成书面服务报告，报告描述应包含识别、目的、读者、频率和数据源的详情。

针对服务生成的报告应使用所交付服务和服务管理体系（SMS)的信息，包括服务管理过程。服务报告至少包括：

a) 与服务级别目标相对应的绩效；

b) 有关重大事件信息，至少包括重大事故、部署新的或变更的服务和触发业务连续性计划；

c) 工作量特征，包括工作量和周期性变化；

d) 与 ISO/ IEC 20000 本部分要求、服务管理体系(SMS)要求或服务需求相对应识别出的不合格以及对应的原因；

e) 趋势信息；

f) 客户满意度测量、服务投诉和对满意度测量和投诉的分析。

服务提供方应基于服务报告的发现做出决策并采取措施。协定的措施应与相关方沟通。

6.3 服务的连续性和可用性管理

6.3.1 服务的连续性和可用性要求

服务提供方应评估并以书面形式明确服务连续性和服务可用性的风险。服务提供方应与客户和相关方识别和协定服务连续性和可用性要求。协定的要求应考虑适用的业务计划、服务需求、SLAs和风险。

协定的服务连续性和可用性要求应至少包括：

a) 访问服务的权利；
b) 服务响应时间；
c) 端到端的可用性。

6.3.2 服务的连续性和可用性计划

服务提供方应创建、实施和维护服务连续计划和可用性计划。这些计划的变更应受变更管理控制。

服务连续性计划至少应包括：

a) 服务重大损失情况下要执行的程序，或对程序的引用；
b) 计划启动时的可用性目标；
c) 恢复要求；
d) 返回正常工作状态的方法；

当正常服务地点的访问被阻止时，应具有服务连续性计划、联系清单和配置管理数据库。

服务连续性计划应至少包含可用性要求和目标。

服务提供方应评估服务连续性计划和服务可用性计划的变更需求的影响。

注：服务连续性计划和可用性计划可整合在一个文件中。

6.3.3 服务的连续性和可用性的监视和测试

应监视服务可用性，记录结果并与协定的目标比较。应对计划之外的不可用性进行调查并采取必要的措施。

针对服务连续性要求，服务连续性计划应被测试。可用性计划应针对服务可用性要求测试。服务提供方操作运行的服务环境发生重大变化时，服务连续性和可用性计划应重新测试。

测试的结果应被记录。每次测试和服务连续性计划启动后，应实施评审。当发现不足时，服务提供方应采取必要的措施并报告采取的措施。

6.4 服务的预算和核算

服务的预算和核算过程与其他财务管理过程之间应有明确的接口。

应有方针和书面的程序：

a) 服务组件的预算和核算至少包括
    1) 用于提供服务的资产（包括许可证），
    2) 共享资源，
    3) 管理费用，
    4) 资金和运行费用，
    5) 外部供应的服务，
    6) 人员，

7） 设施；

b） 与服务相关的间接成本和直接成本的分摊，并为每个服务提供总体成本；

c） 有效的财物控制和授权。

应对支出进行预算，使交付的服务能有效地进行财务控制和业务决策。

服务提供方应对比预算监视并报告预算的支出，评审财务预报，从而管理支出。

信息应提供给变更管理过程以支持变更请求的成本计算。

注：许多服务提供方对他们的服务计费。服务的预算和核算过程范围不包括计费。

6.5 能力管理

服务提供方应与客户和相关方明确和协定能力和性能要求。

服务提供方应生成、实施和维护一个考虑到人员、技术、信息和财务资源的能力计划。能力计划的变更应受变更管理过程的控制。

能力计划至少应包含：

a） 当前和预计的对服务的需要；

b） 协定的要求对可用性、服务连续性和服务级别的预期冲击；

c） 服务能力升级的时间跨度、阀值和支出；

d） 法律、法规、合同或组织变更的潜在影响；

e） 新技术和和新技巧的潜在影响；

f） 能够进行预期分析的程序，或参考它们；

服务提供方应监视能力使用，分析能力数据并调整性能。服务提供方应提供足够的能力满足协定的能力和性能要求。

6.6 信息安全

6.6.1 信息安全方针

拥有适当权限的管理者应批准考虑到服务需求、法律法规要求和合同义务的信息安全方针。管理者应

a） 向服务提供方、客户和供应商的适当人员传达信息安全方针以及遵守该方针的重要性；

b） 确保建立信息安全管理目标；

c） 明确管理信息安全风险所采取的方法和接受风险的准则；

d） 确保信息安全风险评估按照计划的时间间隔实施；

e） 确保信息安全内审的进行；

f） 确保审核结果被评审以识别改进的机会。

6.6.2 信息安全控制措施

服务提供方应实施和运行物理的、管理的和技术的信息安全控制措施以便于：

a） 保护信息资产的机密性、完整性和可访问性；

b） 满足信息安全方针的要求；

c） 达到信息安全管理的目标；

d） 管理信息安全相关的风险。

信息安全控制措施应以书面形式描述控制措施对应的风险，以及控制措施的运行和维护。

服务提供方应评估信息安全控制措施的有效性。信息安全提供者应采取必要的措施并汇报采取的措施。

服务提供方应识别需要访问、使用或管理服务提供方的信息或服务的外部组织。服务提供方应与这些外部组织一起协定和实施信息安全控制措施并形成文件。

6.6.3 信息安全的变更和事件

变更请求应被评估以确定：

a) 新的或变更的信息安全风险；

b) 对已有信息安全方针和控制措施的潜在影响。

信息安全事件应采用事件管理流程管理，其优先级别与信息安全风险相适应。服务提供方应分析信息安全事件的类型、数量和冲击。信息安全事件应报告和评审以识别改进的机会。

注：ISO/IEC 27000标准族提出了明确要求为支持实施和运行信息安全管理体系提供指导。

7. 关系过程

7.1 业务关系管理

服务提供方应识别并记录服务的客户、用户和相关方。

对于每个客户，服务提供方应指定专人负责管理客户关系和客户满意度。

服务提供方应与客户建立沟通机制。沟通机制应事先了解业务环境对服务运行和新的或变更服务的要求。该信息应使服务提供方响应这些要求。

服务提供方和客户应按计划的时间间隔评审服务的绩效。

形成书面的服务需求的变更应受变更管理过程的控制。SLAs的变更应与服务级别管理过程协调。

服务投诉的定义应与客户协商一致。应有书面的程序管理来自客户的投诉，服务提供方应记录、调查、采取措施、报告和关闭服务投诉。当服务投诉不能通过正常渠道解决时，应为客户提供升级服务。

通过对服务的客户和用户进行代表性的抽样调查，服务提供方应按照计划的时间间隔测量客户满意度。该结果应用于分析和评审以识别改进的机会。

7.2 供应商管理

服务提供方可使用供应商实施和运行部分服务管理过程。图3说明了一个供应链关系的示例。

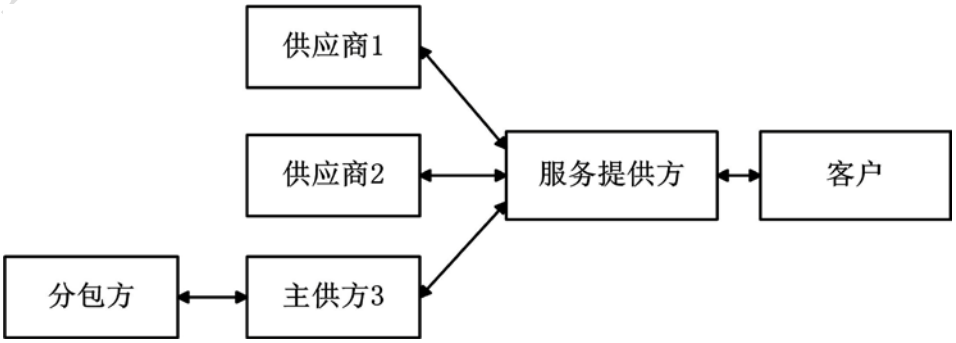

图 3 供应链关系示例

对于每个供应商，服务提供方应有一个指定的个体负责管理与供应商的关系、合同和绩效。

服务提供方和供应商应协定书面合同。合同应包含或包括以下引用：

a) 供应商交付的服务的范围；
b) 服务、过程和相关方的依赖关系；
c) 供应商须满足的要求；
d) 服务目标；
e) 供应商和其他方在服务管理过程运行中的接口；
f) 将供应商活动整合至服务管理体系（SMS）；
g) 工作量特性；
h) 合同中的例外情形以及该如何处理例外；
i) 服务提供方和供应商的权限和职责；
j) 供应商提供的报告和通告；
k) 支付基础；
l) 预期的或提前结束合同和将服务传递到不同方的活动和职责。

服务提供方应与供应商协定服务级别，以支持服务提供方与客户订立的SLAs，并保持一致。

服务提供方应确保主供方与分包方之间的角色和关系并形成文件。服务提供方应证实主供应商为满足合同义务而对分包方进行了管理。

服务提供方应按照计划的时间间隔监视供应商的绩效。测量的绩效应与服务目标和其他合同义务比较。其结果应被记录和评审，识别不合格的原因和改进的机会。评审应确保合同反映现实的要求。

合同的变更应受变更管理过程控制。

应具备解决服务提供方和供应商合同纠纷的书面的程序。

注1：供应商管理的范围不包括功放的选择和服务的采购。

注2：更进一步的供应链关系的示例见ISO/IEC TR 20000-3。

8 解决过程

8.1 事件和服务请求管理

应以书面程序形式对所有事件进行明确：

a) 记录；
b) 分配优先顺序；
c) 分类；
d) 记录更新；
e) 升级；
f) 解决；
g) 关闭。

应有书面的程序管理服务请求从记录到关闭的全过程。事件和服务请求应根据该程序管理。

当排定时间和服务请求的优先顺序时，服务提供方应考虑事件和服务请求的影响和紧急程度。

服务提供方应确保涉及事件和服务请求管理流程的个人能访问和使用相关信息。相关信息应包括服务请求管理流程、已知错误、解决的问题和配置配置管理数据库。从发布部署管理过程得到的发布成功或失败的信息、未来的发布日期，应被事件和服务请求管理过程使用。

服务提供方应及时向客户通告所报告的事件或服务请求的进展。如果服务目标不能满足，服务提供方应通知客户和相关方，并依据程序进行升级。

服务提供方应与客户协定重大事件的书面化定义。重大事件应依据书面的程序分类和管理。重大事件应通知最高管理者。最高管理者应确保指定专人负责管理重大事件。当协定的服务恢复后，重大事件应被评审以识别改进的机会。

8.2 问题管理

应有书面的程序来识别、最小化或避免事件和问题的影响。该程序应定义：

a) 识别；
b) 记录；
c) 分配优先顺序；
d) 分类；
e) 记录更新；
f) 升级；
g) 解决；
h) 关闭。

问题应根据该程序管理。

服务提供方应分析事件和问题的数据和趋势，以识别根本原因和潜在预防措施。

问题所需的配置项（CI）变更应通过提交变更请求解决。

当发现根本原因，但问题并没有彻底解决时，服务提供方应采取措施以减轻或消除问题对服务的影响。已知错误应被记录。

应对问题解决的有效性监视、评审和报告。

已知错误的更新信息和问题解决方案应提供给事件和服务请求管理过程。

9 控制过程

9.1 配置管理

每种类型的配置项应有书面的定义。每个配置项记录的信息应确保是有效控制的，并至少包含：

a) 配置项的描述；
b) 配置项和其他配置项之间的关系；
c) 配置项和服务组件之间的关系；
d) 状态；
e) 版本；
f) 位置；
g) 相关的变更请求；
h) 相关的问题和已知错误。

配置项应是唯一可识别的，并记录在CMDB中。CMDB应管理以确保其可靠性和准确性，包括更新访问控制。

应有书面的程序记录、控制和跟踪配置项的版本。考虑到服务需求和配置项的相关风险，控制程度应保证服务和服务组件的完整性。

按照计划的时间间隔，服务提供方应审核储存在配置管理数据库中的记录。当发现缺失时，服务提供方应采取必要的措施并报告采取的措施。

配置管理数据库中的信息应提供给变更管理过程，以支持对变更请求的评估。

对配置项的变更应是可追溯的和可审核的，以保证配置和配置管理数据库中数据的完整性。

部署一个发布到现实环境前，应确定受影响配置项的配置基线。

记录在配置管理数据库中配置项的主要副本应存储在安全的物理介质或电子库中以便于被配置记录引用。配置项至少包括文件、许可证信息、软件，如果可能的话应提供硬件配置图。

配置管理过程和财务资产管理过程应有明确的接口。

注：配置管理过程不包含财务资产管理过程。

9.2 变更管理

应建立变更管理方针，明确：

a) 变更管理控制下的配置项；

b) 判定变更时服务或客户有潜在重大影响的准则。

删除服务应被分类为对服务有潜在重大影响的变更。服务从服务提供方转移到客户或不同方应被分类为有潜在重大影响的变更。

应有书面程序记录、分类、评估和批准变更请求。

服务提供方与客户应书面协定紧急变更的定义。应有书面的程序管理紧急变更。

所有对服务或服务组件的变更应提出变更请求。变更请求应有明确的范围。

应对所有变更请求进行记录和分类。分类为对服务或客户有潜在重大影响的变更请求，应采用设计和转换新的或变更的服务过程管理。所有其他定义在变更管理方针中的配置项的变更请求应由变更管理过程管理。

应对变更请求进行评估，评估信息采自变更管理过程和其他过程。

服务提供方和相关方应对变更请求做出决定。做决定应考虑风险、对服务和客户潜在的冲击、服务需求、业务收益、技术便利性和财务影响。

批准的变更应被开发和测试。

变更安排，包含被批准变更的细节和它们建议的部署日期，应被建立并通告相关方。变更安排应作为计划发布部署的基础。

应策划取消或补救不成功变更需要的相关活动，有条件尽量进行测试。若不成功，变更应取消或补救。不成功变更应被调查并协定采取的措施。

配置管理数据库中的记录应随成功部署的变更更新。

服务提供方应评审变更的有效性并与相关方协定要采取的措施。

变更请求应根据计划的时间间隔分析以识别趋势。由分析得出的结果和结论应予以记录和评审以识别改进的机会。

9.3 发布和部署管理

服务提供方应建立并与客户协定发布策略，描述发布的频率和类型。

服务提供方应与客户和相关方策划、部署新的或变更的服务和服务组件到实际环境中去。策划应与变更管理过程协调并包含对相关的变更请求、已知错误和通过该发布所关闭问题的引用。策划应包括对每个发布的部署日期、部署的可行性和部署的方法。

服务提供方应与客户协定紧急发布的书面定义，紧急发布应根据与紧急变更程序接口的书面的程序管理。

部署前，应建立和测试发布。建立和测试发布应在可控的验收测试环境下进行。

发布的验收准则应与客户和相关方协定。对比协定的验收准则，发布应被验证并在部署前获批。如果验收准则无法满足，服务提供方应与相关方决定采取的必要措施及部署。

发布应部署至实际环境中，并在发布部署中保持硬件、软件和其他服务组件的完整性。

应对撤销或修复不成功发布的部署所需的活动进行策划，有可能的话，进行测试。如果不成功，应撤销或修复发布部署。不成功的发布应予以调查并采取协定的措施。

应对成功和失败的发布进行测量和分析。测量内容应包括发布之后某段时间内与发布有关的事件。分析应包括发布对客户影响的评估。应对分析的结果和结论进行记录并评审以识别改进的机会。

有关发布成功或失败和未来发布日期的信息，应提供给变更管理过程、事件和服务请求管理过程。

信息应提供给变更管理过程，以支持针对发布的变更请求和对策划的部署的评估。

参考文献

[1] ISO/IEC 20000-2:2005 信息管理-服务管理-第 2 部分：实施服务管理体系指南
[2] ISO/IEC TR 20000-3 信息管理-服务管理-第 3 部分：范围定义和适用指南
[3] ISO/IEC TR 20000-4 信息管理-服务管理-第 4 部分：过程参考模型
[4] ISO/IEC TR 20000-5 信息管理-服务管理-第 5 部分：实施计划示例
[5] ISO 9000:2005 质量管理体系-基础和词汇
[6] ISO 9001 质量管理体系-要求
[7] ISO 9004:2000 质量管理体系-绩效改进指南
[8] ISO 10002 质量管理-客户满意度组织投诉处理指南
[9] ISO 10007 质量管理体系-配置管理指南
[10] ISO/IEC 15288 系统工程系统生存周期过程
[11] ISO/IEC 15504-1 信息技术-过程评估-第 1 部分：概念和词汇
[12] ISO/IEC 15504-2 信息技术-过程评估-第 2 部分：执行评估
[13] ISO/IEC 15504-3 信息技术-过程评估-第 3 部分：执行评估的指南
[14] ISO 19011 质量/环境管理体系审核指南
[15] ISO/IEC 19770 信息技术-软件资产管理-第 1 部分：过程
[16] ISO/IEC/IEEE 24765:2010 系统和软件工程-词汇
[17] ISO/IEC 27000:2009 信息技术-安全技术-信息安全管理体系 框架和词汇
[18] ISO/IEC 27001 信息技术-安全技术-信息安全管理体系 要求
[19] ISO/IEC 27005 信息技术-安全技术-信息安全管理风险管理
[20] ISO 31000 风险管理 原则和指南