

中国标准文献分类号：A11

JR

中华人民共和国金融行业标准

JR/T 0074—2012

保险业 IT 服务管理基本规范

Baseline of information technology services management for insurance

2012-11-29 发布

2012-11-29 实施

中国保险监督管理委员会 发布

目 次

前 言	III
引 言	IV
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 IT 服务管理	1
5 管理体系要求	2
5.1 管理职责	2
5.2 文件要求	2
5.3 能力、意识和培训	3
6 策划和实施 IT 服务管理	3
6.1 策划 IT 服务管理（策划）	3
6.2 实施 IT 服务管理和提供服务（实施）	4
6.3 监视、测量和评审（检查）	4
6.4 持续改进（处置）	4
7 策划和实施新服务或变更的服务	4
8 服务交付流程	5
8.1 服务级别管理	5
8.2 服务报告	5
8.3 服务连续性和可用性管理	5
8.4 IT 服务的预算和核算	6
8.5 能力管理	6
8.6 信息安全管理	6
9 关系流程	7
9.1 业务关系管理	7
9.2 供方管理	7
10 解决流程	8
10.1 事件管理	8
10.2 问题管理	8
11 控制流程	8
11.1 配置管理	8
11.2 变更管理	9
12 发布流程	9
12.1 发布管理	9
附录 A（资料性附录） 服务级别协议参考模版	11
A.1 服务级别协议参考模版	11
A.1.1 基本信息	11
A.1.2 支持服务与成本	11
A.1.3 名词定义	12

A.1.4 服务测量与报告	13
A.1.5 批准	14
附录 B (资料性附录) 部分流程管理统计分析指标参考.....	15
B.1 服务级别管理绩效指标	15
B.2 IT 服务连续性管理绩效指标	15
B.3 可用性管理绩效指标	15
B.4 信息技术 IT 服务的预算与财务管理绩效指标.....	16
B.5 能力管理绩效指标	16
B.6 信息安全管理绩效指标	17
B.7 业务关系管理绩效指标	17
B.8 供方管理绩效指标	17
B.9 事件管理绩效指标	17
B.10 问题管理绩效指标	18
B.11 配置管理绩效指标	19
B.12 发布管理绩效指标	19

前 言

本标准参照GB/T 1.1-2009给出的规则起草。

本标准由全国金融标准化技术委员会保险分技术委员会提出并归口。

本标准起草单位：中国太平洋保险（集团）股份有限公司、中国太平保险集团公司。

本标准主要起草人：徐建国、张军、钱忠伟、徐宏波、曹忠华、孙小明、郭琳、丁先明、徐刚

本标准的附录A、附录B为资料性附录。

引 言

随着我国保险业的快速发展，信息技术已广泛渗透到保险行业发展的各个环节，推动着保险业发展达到一个新高度。信息化管理水平已成为衡量一个保险机构核心竞争力、经营管理水平的重要指标。

《保险业IT服务管理基本规范》旨在规范保险机构的IT服务管理体系，指导保险机构建立可持续改进的IT服务管理的方法；为保险机构信息技术部门提供信息技术服务管理的评估和管理基准，提高信息技术的监督管理水平；加强行业内信息技术合作和交流，推动保险行业整体IT服务管理水平的不断提高，为业务发展提供保障。

本规范以GB/T 24405.1-2009《IT服务管理 第1部分：规范》为编制依据，定义了保险机构IT服务管理体系的基本规范，包括有效管理和实施IT服务管理的基本策略和流程框架。

保险业 IT 服务管理基本规范

1 范围

本标准规定了中华人民共和国境内保险机构IT服务管理的基本规范,包括有效管理和实施IT服务管理的基本策略和流程框架。

本标准适用于中华人民共和国境内保险机构的IT服务管理。

2 规范性引用文件

本规范引用 GB/T 24405.1-2009《IT服务管理 第1部分:规范》。

3 术语和定义

下列术语和定义适用于JR/T074-2012本部分

3.1

**IT服务管理 information technology Service Management
ITSM**

服务提供方通过协调人员、流程和信息技术的管理活动,有效交付IT服务,满足客户和业务需求的管理活动。

3.2

流程 process

用于实现特定目标的一系列有组织的活动。

3.3

服务提供方 service provider

为保险机构提供IT服务的内部组织或外部公司。

3.4

客户 customer

与服务提供方定义和议定服务级别目标的人员或团体。

3.5

服务连续性 service continuity

识别和管理可能严重影响IT服务的(重大、灾难性)风险,建立和维护IT服务响应和恢复的能力,确保IT服务能够提供约定的最低服务级别。

3.6

供方 supplier

负责提供交付信息技术服务所需的商品或服务的第三方。

3.7

能力 capacity

配置项或信息技术服务可以提供,同时达到约定的服务级别目标的最大吞吐量。

3.8

信息技术基础架构 information technology infrastructure

开发、测试、交付、监视、控制或支持IT服务所需的所有软硬件、网络、设施等信息技术。

4 IT 服务管理

服务提供方应全面识别和管理IT服务的众多相互关联的活动。采纳流程管理的方法识别和管理IT服务的众多的相互关联的活动,通过协调人员、流程和信息技术的活动,有效交付IT服务,满足客户和业务需求的管理活动。

IT服务管理的实施过程和活动要求将服务台人员、服务支持人员、服务交付人员和运营团队很好的组织和协调。还要求具备适宜的工具以确保流程有效及高效。

IT服务管理应完整包括以下紧密相关的服务管理流程,如图1所示。

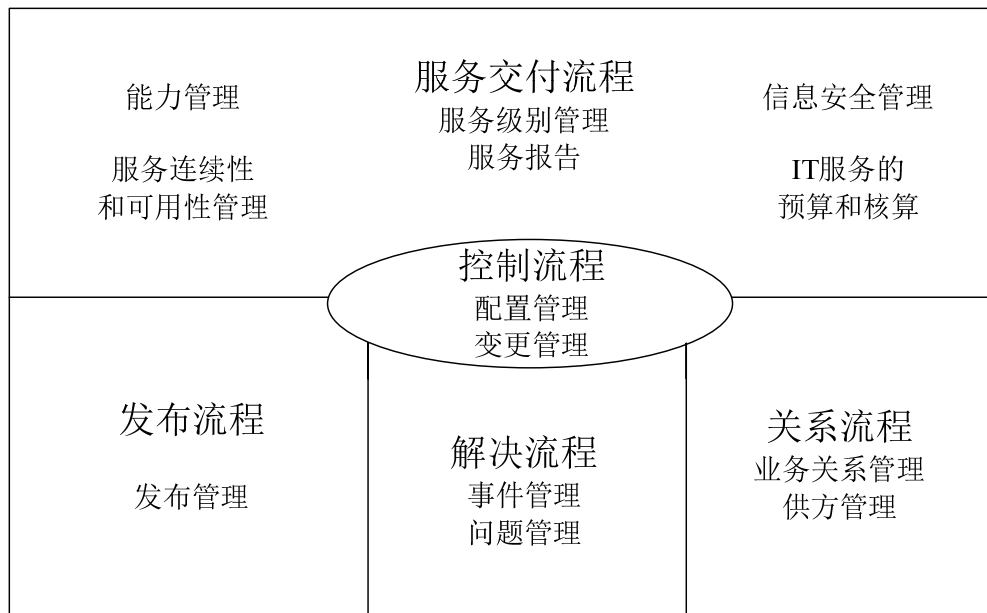


图 1 服务管理流程

保险机构的业务目标和对IT服务的需求关系决定服务提供方实施IT服务管理体系的管理方式。本规范描述的目标和控制措施并不完备,服务提供方可根据保险机构的业务目标和控制要求增加或补充完善相关流程、目标和控制措施,满足特定的业务需求。

IT服务管理体系流程之间的关系需要根据服务提供方与客户业务组织的关系和各自IT服务特点建立。

5 管理体系要求

管理体系的目标是提供一个管理体系,包括方针和框架,以有效管理和实施所有IT服务。

5.1 管理职责

服务提供方的管理层应针对所提供的IT服务制订基本的管理体系的方针,明确IT服务组织的管理目标和工作策略。

服务提供方的管理层应:

- a) 确保理解和确认客户的IT服务的需求,理解和明确提高客户满意度的目标;
- b) 确定IT服务管理的目标、策略、计划和职责分工,至少每年回顾评审一次;
- c) 组织、建立履行职能所需IT服务的管理体系和流程,明确IT服务的交付和管理改进所需要的各项资源;
- d) 负责管理在IT服务活动中组织和服务的相关风险;
- e) 组织意识宣导和培训教育,传达IT服务管理的目标;
- f) 推广IT服务管理体系,推广IT服务管理持续改进工作。

5.2 文件要求

服务提供方为确保有效计划、运行和控制IT服务管理，应建立文件体系以管理IT服务管理体系的相关文件。文件体系主要包括：

- a) IT服务管理策略和实施计划；
- b) 服务级别协议、服务支持协议或备忘录；
- c) IT服务管理流程和程序文件；
- d) IT服务管理体系执行的相关记录和证据。

服务提供方应制定文件的管理方法，实施文件体系制定、修订、批准、发布、访问控制、保存周期等控制措施。

5.3 能力、意识和培训

服务提供方管理层应明确提供IT服务所需的角色和职责，以及有效履行职责所需的能力。

为确保员工能够具有有效的技能和能力以履行IT服务的职责，应提供必要的教育、培训、训练和实践，保证员工达到所需资质、技能和能力。

管理层应在员工中推广IT服务的意识培训，确保其了解所属角色和职责，提高员工服务意识。

6 策划和实施 IT 服务管理

服务提供方应建立“策划—实施—检查—处置”的工作机制，实现持续改进IT服务管理，达到设定的服务目标。

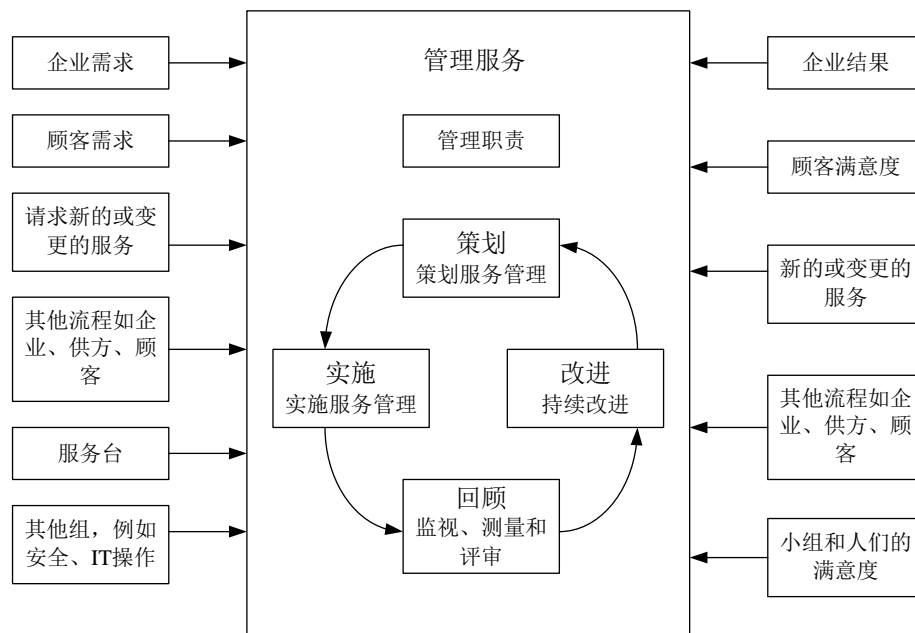


图 2 服务管理过程的PDCA方法论

“策划-实施-回顾-改进”的方法论应用于所有IT服务管理流程和工作。

- a) 策划：根据顾客的要求和组织的方针，为提供结果建立必要的目标和流程；
- b) 实施：实施流程；
- c) 检查：根据服务的方针、目标和产品要求，对流程和产品进行监视和测量，并报告结果；
- d) 处置：采取措施，以持续改进流程业绩。

6.1 策划 IT 服务管理（策划）

服务提供方应制定IT服务管理的策划，确保IT服务可以被顺利实施和有效交付。

应制定清晰的评审、授权、通报、实施IT服务管理的策划和记录管理的职责分配，确保服务管理流程的策划与服务管理目标策略方针保持一致。

服务管理的策划应至少应包括以下内容：

- a) 服务提供者的IT服务管理范围；
- b) IT服务需达到的目标和要求；
- c) 实施IT服务管理的流程，以及流程间的接口和活动协调方式；
- d) IT服务管理的风险管理计划；
- e) 识别完成服务目标所必要的资源、工具和费用；
- f) IT服务管理的组织架构，明确角色和职责框架，包括高层管理者、管理体系负责人、流程负责人及供方管理等；
- g) 管理、审核并改进IT服务的计划。

6.2 实施 IT 服务管理和提供服务（实施）

服务提供方应依据服务管理策划实施IT服务管理并交付服务，包括：

- a) 管理和分配服务所需资源和费用开支；
- b) 管理服务团队的角色和职责，及时补充并发展适当的人员，维护服务团队稳定和连续；
- c) 编制并维护每个流程的方针、计划、程序和管理工具；
- d) 识别并管理服务流程的风险；
- e) 加强各领域服务管理流程的协作；
- f) 依据服务管理策划，加强服务管理的改进。

6.3 监视、测量和评审（检查）

服务提供方应对依据服务管理策划开展的实施工作进行监视、测量和评审工作，确保IT服务管理体系有效实施和维护。

应制定周期性的审核IT服务管理流程，定义审核的准则、范围、频率和方法。审核方和审核活动应确保审核的客观与公正。应至少每年开展一次完整的IT服务管理体系的质量评审。

应记录评审、评估与审核的目标，审核及评审的结果和已识别的补救措施。发现的重大的不一致内容应及时通报相关方。

6.4 持续改进（处置）

服务提供方应依据服务管理方针，对交付的IT服务的效益和质量，开展服务改进的工作。

服务改进的管理工作包括：

- a) 针对可能的风险开展的预防性改进工作；
- b) 通过监控、衡量和回顾工作发现的纠错性改进工作；
- c) 组织单个或多个流程，部分领域或整个组织的改进工作；
- d) 针对所有服务管理流程，分析执行的数据，建立服务能力标准的基线，管理和交付服务；
- e) 与所有相关方进行商议、识别、策划，测量、通报各项服务改进方案；
- f) 设定改进质量、成本和资源利用的目标；
- g) 修改服务管理涉及的方针、计划和程序；
- h) 确保所有批准的持续改进措施都已交付执行，并实现了预期目标。

7 策划和实施新服务或变更的服务

服务提供方应建立策划和实施新的或变更的服务的管理体系。针对新增加或者变更IT服务时，应与相关客户和支持方建立统一的管理方法，组织和管理各项资源，管理和交付有质量的IT服务。

策划和实施新服务或变更的服务应管理以下内容：

- 新增、变更或中止一项IT服务内容，应评估可行性和影响，评估成本、技术、业务和对组织的影响，并通过变更管理流程开展计划和审批工作；
- 新增或变更IT服务时，开展计划和方案的管理工作：
 - a) 明确服务提供方和相关方的职责分工和工作范围；

- b) 增加和调整的服务内容应通报相关方，并签署和调整符合业务需求的合同或协议；
 - c) 明确人力资源，明确技能和培训需求；
 - d) 调整相关的服务流程、工具和管理体系。例如：涉及的能力管理工作和财务管理等工作；
 - e) 明确调整新增或变更IT服务内容所需的资源预算，制订实施时间计划，制定验收标准和后续服务交付标准。
- 在实施新增或调整IT服务内容前，应组织验收工作；
 - 新增或变更IT服务后应组织评估方案的执行情况，向客户报告服务执行结果。

8 服务交付流程

8.1 服务级别管理

服务提供方应建立服务级别管理流程，与客户定义、协商、记录并管理服务级别。

服务级别管理流程应管理以下内容：

- 应制定服务级别管理流程，定义、协商、记录和管理服务级别协议，明确定义完整的IT服务，包括服务内容、服务级别目标和工作量等特性；
- 与客户签署服务级别协议或备忘，服务级别协议应明确提供IT服务的服务内容、范围和质量标准及相关方须明确的内容；
- 与相关方共同商讨和确认服务级别协议及支持的相关服务支持协议、采购合同等。服务支持协议指服务提供方为有效履行服务级别协议，与第三方合作商签订的支持合同或协议；
- 应至少每年与客户评估和确认服务级别协议内容，调整服务级别协议内容应通过变更管理流程实施；
- 应组织对服务级别协议的执行情况进行监控、报告和趋势分析，组织实施服务质量改进计划。

8.2 服务报告

服务提供方应建立服务报告管理流程，与客户建立正式的IT服务执行情况的沟通和交流渠道。

服务报告管理流程应管理以下内容：

- 服务提供方应根据提供服务的交付情况或客户的特定服务需求，向客户或相关方定期提供服务报告。服务报告的内容应包括但不限于：
 - a) 服务级别协议约定的IT服务执行情况；
 - b) 与服务级别协议的执行目标不一致的情况；
 - c) IT服务主要的流程管理指标，例如：事件、变更、发布、可用性、服务连续性、能力等；
 - d) 执行服务流程的重大事项，例如，重大事故和变更；
 - e) 开展客户满意度调研的反馈结论和客户满意度改进计划。
 - f) IT服务绩效的趋势分析
- 应定期分析服务报告中的结论和客户反馈，制订服务改进计划。

8.3 服务连续性和可用性管理

服务提供方应建立整合的IT服务连续性和可用性管理流程。确保在各种风险场景下能够经济有效的实现服务级别约定的IT服务的可用性和连续性的目标。

可用性和连续性管理管理流程应管理以下内容：

- 应根据客户业务需求和风险管理策略有效识别IT服务的可用性和连续性的需求。
 - a) 定义系统可用性、可靠性、可维护性需求；
 - b) 有效识别支持业务的关键IT服务，识别威胁IT服务实现服务级别目标的各种风险；
 - c) 明确不同风险场景下支持业务运行的IT服务的最低需求。
- 应持续监控、测评管理IT服务的可用性
 - a) 确保所有服务组件的可用性，记录所采取的纠正措施并实施；
 - b) 识别IT服务与可用性目标的差距，预测和管理可用性；

- c) 对潜在影响信息技术组件和IT服务可用性的风险开展预防和改进措施。
- 制定IT服务可用性和连续性管理策略, 开发和管理可用性和连续性计划, 包括:
 - a) 可用性计划应有效识别可用性管理的策略和方法, 确保现在和未来的服务期间都能经济有效的满足可用性目标;
 - b) IT服务连续性计划应支持机构的灾难恢复工作和业务连续管理工作;
 - c) IT服务连续性计划应明确触发和调用条件, 恢复IT服务所涉及的组织机构和岗位职责、恢复流程、所需资源和工作操作流程等。
- 应周期性开展可用性和IT服务连续性计划评估工作, 可用性和连续性计划应至少每年进行一次修订;
- 应周期性开展可用性和连续性计划测试和演练工作, 应每年至少开展一次可用性和IT服务连续性计划测试, 评估计划的有效性;
- 当业务和信息系统发生重大变更时, 应及时验证、测试和演练可用性和IT服务连续性计划。对发现的失败信息应制定改进方案, 并纳入服务改进计划。

8.4 IT 服务的预算和核算

服务提供方应根据提供的服务内容, 建立预算和核算的政策和程序, 经济高效地实现符合服务级别协议需求的资源的财务资源。

IT服务预算和核算管理流程应:

- 管理符合服务级别目标的资源的预算, 资源包括: 信息技术资产、共享资源、日常开支、第三方供应服务、人员、软件等领域;
- 应开展有效的财务的控制和授权管理, 监控资源使用情况;
- 当发起变更时, 应评估和批准服务变更对财务资源的影响。

8.5 能力管理

服务提供方应有效建立能力管理流程, 确保IT服务的能力可以经济高效地实现与客户当前和未来业务对IT服务的需求。能力管理的范围应至少包含提供IT服务所需的信息技术基础架构资源。

能力管理流程应:

- 有效的建立和实施能力管理的流程, 实施能力与绩效管理相关技术手段。
- 服务提供方应周期性开展能力需求分析工作, 并应至少每年开发能力计划。分析管理应包括有效识别、理解和掌握客户的业务部门当前和中远期业务需求:
 - a) 预测业务量的变化量和时限
 - b) 业务模式和特点的变化对业务需求的影响
 - c) 特定时段(特定时间窗口)对业务量的影响等
- 识别当前和规划能力可以支持的IT服务的时间、成本、业务量等要素的支持边界。
- 分析IT服务和信息技术设施的服务能力, 分析和预测当前和未来的业务需求对IT服务和信息技术基础架构的能力和性能需求, 并制定合理的IT服务的预算。
- 开展持续的能力管理活动, 采取合适的技术和流程管理手段, 实现资源的优化使用, 包括:
 - a) 绩效管理包括监视、阈值检测、性能分析和调整, 发起与性能和能力有关的变更, 跟进解决能力和性能领域的事件和问题;
 - b) 在实施变更管理, 以及实施新的或变更IT服务管理中, 开展对能力和性能的影响和风险评估;
 - c) 建立和管理能力和性能的基础数据, 支持能力和性能的分析预测和优化管理工作;
 - d) 跟踪掌握能力和性能优化的先进技术手段。

8.6 信息安全管理

服务提供方应有效建立信息安全管理体系, 确保在所有IT服务活动中有效的管理信息安全。

信息安全管理流程应:

- 具有授权的安全管理组织，建立有效的信息安全管理体。
- 制订信息安全策略，并通报给IT服务涉及相关人员，包括员工、客户、供方等。
- 为有效贯彻信息安全策略，针对控制IT服务或系统访问控制的信息安全风险，应制订适当的信息安全控制措施，并使之文档化，有效识别、控制和管理风险。
- 对信息系统和信息服务的访问，应与访问方建立正式的信息安全协议。
- 开展变更时，应有效评估其对信息安全的影响。
- 建立安全事件的响应流程，安全事件应遵循事件管理流程开展报告和记录，有效分析信息安全事件的类型、数量和影响，作为改进服务质量的输入。

9 关系流程

9.1 业务关系管理

服务提供方应基于对客户业务的理解，建立与客户良好的合作关系管理。

业务关系管理流程应管理以下内容：

- 应有效识别客户和IT服务涉及的利害相关方，及时了解客户对服务的需求；
- 应至少每年或与客户开展重大服务级别协议变更时，与客户讨论服务范围、服务级别协议以及客户对服务的需求或变更，并形成文档化记录；
- 接受客户对新增或变更服务的需求，并通过发起变更流程开展评估和管理工；
- 与客户协商建立投诉流程，所有正式的客户投诉应有效记录，调查原因，并与客户协商解决方案。
- 应管理客户对IT服务的满意度，定期开展客户满意度调查，针对反馈结果实施服务质量改进计划。
- 负责把服务的变化等通知给相关客户。

9.2 供方管理

服务提供方应有效管理供方，整合相关的供方的服务，提供给客户整合后的高质量IT服务。

供方管理流程应管理以下内容：

- 应有效识别相关供方的服务内容，包括需求、范围、服务级别和交付流程，并与相关方协商，与供方形成统一的服务级别协议或合同。各方的服务接口应形成统一记录；
- 应有效管理供方的服务分包风险，主供方与分包供方的职责和关系应明确记录，主供方应有效管理分包商。相关服务内容和协议应至少每年进行回顾和评审。确保能实现总体服务需求。

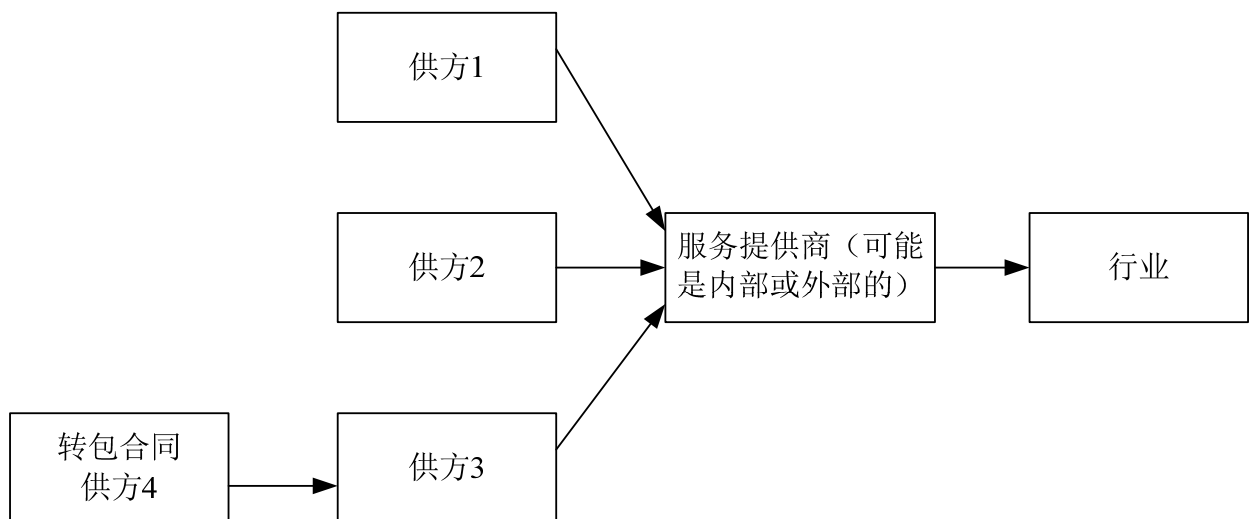


图 3 服务提供商与供方间关系的示例

- 与服务供方的服务内容发生重大变化，应通过变更管理流程进行审核管理；

- 应建立针对合同纠纷的处置管理流程，并与相关方达成统一协议；
- 应定期回顾和评估供方的服务质量，评估结论应纳入服务质量改进计划。

10 解决流程

解决流程包括密切相关的事件管理和问题管理两个单独的流程。

10.1 事件管理

服务提供方应建立事件管理流程，快速恢复受事件影响的IT服务，快速响应用户事件或服务请求，以最快的速度帮助用户解决事件或进行事件升级，力求使事件对用户的影响最小化。

事件管理流程应：

- 定义所有事件的记录、优先次序、业务影响、分类、更新、增加、解决和正式关闭，有效分析事件的影响；
- 建立服务台统一管理事件，确保所有的事件都应记录，应依照已定义流程对主要事件进行分类和管理；
- 及时通知客户有关他们所报告的事件或服务请求的进展情况，如果不能满足服务级别，则应事先警告，并且进行协商；
- 应定义重大事件的标准和处理流程。明确重大事件管理负责人负责组织协调、升级、客户沟通重大事件的处置。应明确定义重大事件/问题的变更的授权。重大事件的处理流程应定期评估，评估结果应纳入服务质量改进计划；
- 建立已知错误库、问题解决方案和配置管理数据库（CMDB）等信息库，事件管理的人员都应有权使用这些信息帮助开展事件流程管理。

10.2 问题管理

服务提供方应建立问题管理流程，通过对服务事件原因的主动式识别、分析和管理，直至问题关闭。避免相关事件的再次发生，以使对业务的破坏最小化。

问题管理流程应：

- 记录所有已识别的问题，应对问题解决的有效性进行监视、评审和报告。
- 定义所有问题的记录、分类、更新、增加、解决和结束；
- 采取程序来识别、最小化或避免事件和问题的影响；
- 采取预防性措施来减少潜在问题，例如，分析事件影响大小和类型的趋势；
- 为改正潜在问题而进行的变更，应传达给变更管理流程。
- 确保事件管理可以获得有关已知错误和已改正问题的当前信息；
- 记录问题管理流程识别的改进机会，并纳入服务改进计划。

11 控制流程

11.1 配置管理

服务提供方应建立配置管理流程，定义和控制IT服务所需基础设施的部件配置项及相关关系信息，确保配置项信息可靠性和准确性。

配置管理流程应管理以下内容：

- 应根据IT服务管理的目标，创建配置项信息的建立和维护流程；制定完整的配置管理方案；
- 配置项信息应提供充分和有效的基础设施部件的信息，配置项应可以支持评估变更对IT服务和基础设施配置的影响。应定义配置项信息的内容和关系，建立配置管理数据库（CMDB），确保配置项都应是唯一可识别的。配置项信息可包含：
 - a) 支持IT服务的基础设施
 - b) 信息系统和软件（包括第三方软件）、发布以及相关的系统文件，例如：规范、设计、测试报告和发布文档、配置基线或每个应用环境、标准硬件的建立和发布的说明；

- c) 主拷贝和电子资料库，例如：最终软件库、许可证等；
 - d) 安全组件，例如：防火墙；
 - e) 服务相关文件、例如：服务级别协议、服务支持协议等；
 - f) 服务支持设施，例如：机房电源、制冷设备等；
 - g) 配置项之间的关系和依赖性；
 - h) 其他信息也可能作为配置项，例如其它文档、其它资产、其它设备、业务单元和人员等。
- 确保配置项信息的可靠性和完整性，配置项的变更应可追踪的和可审核的；
 - 应定期开展配置项信息的检查和审计，应记录、评估差异及不符合项，制定纠正措施并纳入服务改进计划；
 - 应定期建立配置基线，对配置基线的准确进行审计检查。

11.2 变更管理

服务提供方应建立变更管理流程，以受控的方式对管理影响生产系统的所有变更进行的评估、批准、实施和回顾工作。

变更管理流程应：

- 定义和记录IT服务和基础架构的变更；
- 评估变更请求的风险和对技术及业务的影响。例如风险包括：可用性影响、技术风险、人力成本等，并分类记录。例如变更分类包括：紧急、重大、标准、简单等；
- 制订变更实施方案，应包括变更失败计划以及采取的取消或补救措施；
- 在检查和批准变更后，以受控方式实施变更过程。对所有变更执行结果及其实施之后所采取的行动进行评审；
- 制定控制紧急变更的授权和实施紧急变更的流程；
- 维护当前的变更计划并按计划通报相关方；
- 对变更记录进行定期分析，以分析逐渐增长的变更级别、频繁重现的类型的趋势和其他相关信息；
- 对从变更分析中所得到的结果和结论进行记录。有效识别变更管理的改进方案，并将其纳入服务管理改进计划。

12 发布流程

12.1 发布管理

服务提供方应建立发布管理流程，管理向生产环境的交付、分发并追踪一个或多个变更。

发布管理流程应：

- 服务提供方应文档化定义发布管理范围，并制定发布计划。
 - a) 针对服务、系统、软件和硬件的发布，制定包括发布频率和类型定义的发布策略；
 - b) 与所有相关方商议实施发布的计划，并达成一致。相关方包括顾客、用户、操作和支持人员等；
 - c) 发布计划应包括中途退出发布或发布不成功时的补救方式；
 - d) 记录发布日期、交付物、涉及的有关变更请求、已知错误和问题；
 - e) 发布计划应评估变更请求的影响。应定义与突发变更管理流程相互联系的接口，应对突发的发布进行管理。
- 建立受控的验收测试环境，在分发之前对所有发布项进行测试。
- 对发布和分发进行设计和实施。管理和维护硬件与软件在安装、处理、包装和交付流程中的完整性；
- 包括配置信息和变更记录的更新，发布管理流程应传递相应的信息给事件管理流程。
- 对发布的成功和失败进行评估和测量。包括对业务、信息技术运维和支持人力资源的影响的评

估，测量发布之后某段时间内与发布有关的事件，并为服务改进计划提供输入。

附录 A
(资料性附录)
服务级别协议参考模版

A.1 服务级别协议参考模版

A.1.1 基本信息

协议签订双方

本服务级别协议（SLA）是_____与_____间有关协议中详细描述_____服务的协议，本协议明确了双方的职责，以确保客户的IT服务的需求能够及时得到满足。

客户：[客户名称]

客户环境：[描述客户的信息技术环境，包括客户使用的PC、服务器、OS、中间件、应用系统等相关环境信息，同时还应包含每个应用系统的用户数、每小时的平均交易量、峰值交易量、报表数量与频率等信息]

联系人：[列出服务提供方和客户方的相关联系人]

服务提供方联系人	客户方联系人
<姓名>	<姓名>
<职位>	<职位>
<E-mail 地址>	<E-mail 地址>
<联系电话>	<联系电话>

协议有效期：

[指出本SLA有效的开始时间和结束时间，需要让双方了解SLA需要定期更新。客户需求的变化、服务支持技术手段的改善和技术水平的提升，均会对服务级别产生影响]

协议检查与评估：

<服务提供方>在协议生效运行每<90天>后与客户共同进行SLA实施状况评估，双方代表将对评估结果分别提交评估报告。

依据评估检查结果，SLA应每<1年>进行一次更新，在更新SLA尚未完成和发布前，仍执行原始SLA。

A.1.2 支持服务与成本

服务内容

<服务提供方>承诺为客户提供如下服务：

A:

B:

C:

本协议中不包含 X, Y 和 Z 服务。

服务成本

<上述的服务成本为xxx元。>

责任与分工

[描述客户与服务提供方双方的职责范围]

客户的职责:

遵循相应的流程

按照相关的信息技术操作规程和要求操作

出现问题时及时与帮助台联系, 以便尽早排除故障

不在桌面系统上安装非法软件

...

服务提供方的职责:

创建和维护知识库来记录客户问题及解决方案

满足不同优先级问题的响应时间

维持合理数量的经过培训的信息技术维护人员

...

A. 1.3 名词定义

[明确SLA中关键名词的含义, 使双方对同一个名词的理解相同]

可用性:

在规定时刻或规定时间段内, 部件或服务执行要求功能的能力。IT服务的可用性应测量信息技术服务的端到端的业务输出, 通常用机构使用的实际可用服务时间与约定服务时间的比率来表示。

某月某服务的可用性为:

$$\frac{\text{(承诺的某月全部服务时间)} - \text{(在承诺的某月服务时间内无法提供服务的时间)}}{\text{(承诺的某月全部服务时间)}}$$

无法提供服务的时间是指从服务提供方或客户发现服务中断开始, 直至服务恢复的时间间隔。

可靠性:

衡量配置项或IT 服务可以不间断执行其约定功能的时间长度的指标。

平均问题响应时间:

问题响应时间是指从发生问题的发生, 到相关维护人员到位开始解决问题间的时间段, 平均问题响应时间是指每个问题发生时, 所用的平均响应时间, 即:

$$\frac{\text{所有问题响应时间之和}}{\text{全部问题的数量}}$$

平均问题解决时间:

问题解决时间是指从发生问题的发生, 到服务恢复正常工作间的时间段, 平均问题解决时间是指每个问题发生时, 所用的平均解决时间, 即:

$$\frac{\text{所有问题解决时间之和}}{\text{全部问题的数量}}$$

A. 1. 4 服务测量与报告

服务时间

[描述各个服务承诺的服务时间]

服务	服务时间
服务1	AM 8:00—PM 5:00 周一—周五
服务2	AM 0:00—PM 24:00 7X24
...	

可用性

[描述各个服务在一段时间内服务可用的比例]

服务	可用性
服务1	N%
服务2	M%
...	

可靠性

[描述各个服务在一段时间内可以忍受的最大服务中断次数，指标可以是服务中断次数或平均中断间隔时间（MTBF）]

功能与性能

[描述各个服务的功能要求和性能要求，如服务应具备的功能、支持的用户数、并发用户数、交易响应时间等]

安全

[描述各个服务的安全要求]

服务	安全事件引起的 停机时间	安全事件级别	安全事件数量
服务1	N小时	1	x
		2	y
		3	z
...			

问题响应与解决

[不同的服务，依据优先级的不同会有不同的问题响应和解决时间要求，在下表中描述各个值]

服务	指标	优先级	值
服务1	平均问题响应时间	1	
		2	
		3	
	最大问题响应时间	1	
		2	
		3	
	平均问题解决时间	1	
		2	
		3	
	最大问题解决时间	1	
		2	
		3	
...			

报告

[描述SLA报告的内容, 报告的间隔时间, 报告人以及向谁汇报]

报告名称	报告间隔	报告递交方式	报告人	报告接受人
[列出报告名称如: 系统可用性报告、事件报告问题响应与解决报告等]				

A.1.5 批准

[客户与服务提供方授权代表签署SLA]

<客户>:

姓名	职务	签字	日期

<服务提供方>:

姓名	职务	签字	日期

附录 B
(资料性附录)
部分流程管理统计分析指标参考

B.1 服务级别管理绩效指标

指标名称	管理含义	统计方法
SLA 达成率	该指标体现 SLA 服务达成情况,如未达成则需经过协商解决乃至服务重签。	SLA 达成数/SLA 指标数
SLA 之外的服务数量	该指标是 SLA 流程控制幅度的一个量度,如果大量的服务没有商定并签字认可的 SLA,那么服务水平级别管理则失去了对交付水平的控制。	SLA 协议之外提供的服务数量
通过服务改进计划识别出并处理的改进项目数量	监督服务定期回顾并进行有效改进。	服务改进点数量

B.2 IT 服务连续性管理绩效指标

指标名称	管理含义	统计方法
连续性计划外服务数量	任何服务不包含在信息技术 IT 服务连续性之内都存在风险,该指标确保任何存在风险的服务都得到监测和处理。	不在服务连续性计划内的服务数量
连续性计划完成或更新的延误时间	如果连续性计划不按时完成或更新,会导致连续性计划不完整的风险。该指标评估连续性计划不会在规定时间内完成更新或编制	超过计划完成的时间
连续性认知调查通过率	所有信息技术人员必须对影响、需求保持认知。可定期调查认知水平,但每次应针对信息技术部门的不同成员。所得分值是认知水平的一个量度。	调查通过人数/调查总人数

B.3 可用性管理绩效指标

指标名称	管理含义	统计方法
服务不可用时长	服务停止的时间长度,是可用性指标的简单量度。	服务停止的时间长度
事件检测时长	从事件开始到被发现经历的时间。为了保障事件尽快解决,该指标应处于低值。	从事件开始到被发现经历的时间

事件响应时长	事件探明之后到最初修复行动开始之前的时间。技能熟练的服务台、知识库等有助于响应时长的缩短。	事件探明之后到最初修复行动开始之前的时间
事件修复时长	事件诊断之后到修复之前的时间,该时间的管理对尽量迅速解决事件是重要的。	事件诊断之后到修复之前的时间
事件恢复时长	恢复故障组件的时间。一旦所涉及的组件被修复之后,需要恢复到正常功能才能继续服务。这可能依赖于设备的启动时间、需要创建的条件等。	恢复故障组件的时间
事件复原时长	服务恢复到商定的水平的的时间	服务恢复到商定的水平的的时间
事件解决时长	从发现事件到事件恢复的时间,该指标为事件响应时间、修复时间、恢复时间与复原时间之和。	从发现事件到事件恢复的时间
重复事件数量	配置项反复故障的次数,降低反复出现的故障是可用性管理的职责的一部分,其是否有效由该指标来体现。	配置项反复故障的次数

B.4 信息技术 IT 服务的预算与财务管理绩效指标

指标名称	管理含义	统计方法
预算编制准确率	核查编制预算、实际使用预算的差异情况	编制预算金额/实际使用金额
预算执行率	机构编制预算的依据是服务计划与目标,通过预算执行情况可间接反映服务达标情况。	已使用预算金额/下达预算金额

B.5 能力管理绩效指标

指标名称	管理含义	统计方法
由于能力问题导致的事件次数	应使用检测、微调,结合趋势分析的方法,确保不发生与能力有关的事件。	因能力问题导致的事件总数
与能力有关的硬件计划外采购量	除了能力计划内列出的,任何与能力有关的采购需求都是计划外的。	不在能力计划范围内采购的硬件数量
能力富余百分比	能力管理提供有效的能力而不是富余的能力,因为富余意味不必要的成本支出。	现有能力/实际需求能力

受到能力监测的配置百分比	受到能力监测的配置项的一个量度。通过能力监测排除与能力没有直接关系的配置项。	能力监测配置项数/配置项总数
--------------	--	----------------

B.6 信息安全管理绩效指标

指标名称	管理含义	统计方法
安全事件数量	安全管理流程意识与安全有关的事件是至关重要的,良好的流程将会逐渐减少事件的数量和降低事件的严重性。	安全事件发生数
已发现的风险数量	安全管理必须主动专注于发现新的风险或威胁。该指标测量此项工作的成功程度。	已发现存在安全隐患的风险数量
重大安全事件年度发生数	安全管理流程应做好安全事件发生的预防和解决工作,尽量避免重大安全事件的发生。	年度内发生的重大安全事件数

B.7 业务关系管理绩效指标

指标名称	管理含义	统计方法
服务投诉量	信息技术部门所收到的服务投诉总数。该指标是客户满意度的量度,也是部门关系质量的一个量度。	信息技术部门所收到的服务投诉总数
上次服务评审提出的行动未完成的数量	该指标显示组织在处理其评审流程和完成行动事项方面的效能。	上次服务评审提出的行动未完成的数量

B.8 供方管理绩效指标

指标名称	管理含义	统计方法
供方服务考核满意率	对供方服务质量进行考评,统计整体满意度。	考评合格供方数量/参与考评供方数量
供方改进次数	对供方提出实施服务改进要求的次数,该指标衡量供方服务达成指标。	对供方提出实施服务改进要求的次数

B.9 事件管理绩效指标

指标名称	管理含义	统计方法
一线支持解决率	通过一线支持人员解决的事件占所	一线解决事件数/事件总数

	有事件的比例，比例的高低取决于事件处理的能力。	
工单一次分派率	事件被一次正确分派的比例，比例的高低体现了解决事件的速度、团队的效能。	一次分派正确数/事件分派总数
二线支持平均响应时间	从事件被分配到二线支持到被受理之间的时间，该指标是对二线支持效能的一个衡量。	事件被分配到二线支持到被受理之间的时间
事件平均解决时间	从呼叫开始到呼叫解决的分钟数，它是一个广泛使用的指标，体现了事件管理流程的总体效能。	从呼叫开始到呼叫解决的分钟数
事件归类准确率	事件在首次归类时被给予正确的描述或分类的比率，良好的准确率可以加速问题的解决。	事件归类准确数/归类事件总数
一线支持呼叫百分比	通过一线支持提交事件的比率，比率的高低体现了事件管理流程的成熟度。	一线支持事件提交数/事件提交总数
一次正确解决率	第一次尝试就得到解决的事件的百分比。这样的事件不需要重新开启，也不用为同一事件生成新的事件。	事件一次正确解决数/事件总数
主动解决率	在客户报告差错之前就得到解决的事件百分比。该指标对于事件管理流程所增加的价值至关重要，起到了不干扰业务流程的作用。	事件主动解决数/事件总数

B.10 问题管理绩效指标

指标名称	管理含义	统计方法
问题关闭率	问题的关闭可能需要较长的时间，但是如果问题的关闭比例较高，则表明该流程越有效。	问题关闭数量/问题总数
问题平均解决时间	该指标体现了问题解决的效率，如果问题平均在很长时间悬而未决，则表明该流程效能低下。	问题总解决时间/问题总数
无对应问题的事件百分比	所有的事件都是问题造成的，当它们与一个问题相关联时，则表明最终的解决方案已经在问题的管理掌握之中。如果没有关联问题的事件百分比非常高，则反应问题管理的效能低下或问题管理资源不足。	无对应问题的事件数量/事件数量
问题按时解决率	按预定的时间解决问题所占	按约定的时间成功解决数/问

	的比例,该指标反应了问题解决的效能。	题总数
--	--------------------	-----

B.11 配置管理绩效指标

指标名称	管理含义	统计方法
配置项与变更工单的匹配率	配置管理库为变更管理提供数据支持,变更后的信息需及时在配置管理库中体现,满足后续管理需求。	变更后配置项更改数量/配置变更数量
未授权配置数量	配置管理库中配置项都应得到恰当的授权。	配置管理库中没有恰当授权的配置项数量
配置项变更请求比率	每一次配置项经历变更都必须有一个对应的变更请求和相应的 CMDB 更新以反映变更的完成。	配置项变更请求数/配置项变更总数
配置项正确率	配置管理库的正确率是至关重要的,需要在配置项的输入环节做好相关工作,保证正确率的提升。	正确配置项/配置项总数

变更管理绩效指标

指标名称	管理含义	统计方法
变更一次成功率	变更一次成功实施占有所有变更的比率,一次成功率反映了变更管理的成熟度和效率。	变更一次成功次数/变更总数
未授权变更数	所有的变更都必须受到变更控制,禁止任何未经授权的变更请求。	未通过授权进行变更的数量
变更事故发生率	因变更引起的计划外的服务中断占变更总数的比例。	变更事故数/变更总数
变更请求通过率	变更请求需经过仔细筛选,不符合变更要求的应及早筛除。变更请求过程应有效沟通,提高变更请求通过率。	变更请求通过数/变更请求总数
变更实施准时率	所有变更都有一个既定的完成时间,超过既为变更延时。	准时实施变更数/变更总数
紧急变更数	偶尔的紧急变更是合理存在的,但不能变成常态,且必须保持在一个低值范围内。	紧急变更数量

B.12 发布管理绩效指标

指标名称	管理含义	统计方法
紧急发布数量	紧急发布具有很高的风险性，应合理控制紧急发布数量，尽可能降低该数值。	紧急发布数量
事故率	发布前应经过妥善测试和规划以减少因发布引起的事故发生。	发布事故数/发布总数
发布按时率	发布管理包括 CMDB 中所有发布项的各个部分的计划时间。如果这些时间有任何变化，则计入该指标。	按时发布数/发布总数
未经测试的发布数量	所有的发布都应经过测试，进行测试并签署确认的人应当独立于建立这项发布的人。	没有经过测试直接发布的数量
发布内容在 DSL 中更新率	任何发布内容均需及时在 DSL 中进行更新，以保证配置管理的有效执行。	发布内容更新 DSL 次数/发布总数