# **ISO20000信息安全认证咨询**

ISO20000标准着重于通过“IT服务标准化”来管理IT问题，即将IT问题归类，识别问题的内在联系，然后依据服务水准协议进行计划、推行和监控，并强调与客户的沟通。该标准同时关注体系的能力，体系变更时所要求的管理水平、财务预算、软件控制和分配。

IT组织从产生到发展的很长一段时期，一直是以搞好技术，做好技术支持配角为特征的。但今天的信息系统已不单纯是企业的技术支撑，信息化由“技术驱动”向“业务驱动”转变，IT部门的角色也逐步开始从单纯的信息技术提供者向信息服务供应者转换，职能的转变，客观上也要求信息管理向IT服务管理模式转变。

随着IT技术的发展，越来越多的组织基于IT技术构筑自己的价值链，需要IT来支持和支撑组织的运行，IT构架已经成为影响组织生存的关键要素，特别是对于银行、证券、保险、电信等高度依赖信息技术的组织。而且随着逐年IT的投入，建设了大量的软硬件系统，对客户要求的提高，对故障发生的恐惧，对投入成本逐年增加的不安，都促使现在的组织要采取措施规范IT服务的管理。

在产品生产过程中，需要遵循一定的质量控制标准（如ISO9000系列标准），可以确保产品的质量保持较高的水准（如较高的产品合格率），同时也可以降低产品制造成本。而对于服务提供（运营）过程来说，遵循相关的服务管理标准（如ISO20000）可以实现服务运营的输入（Inputs）和生产流程（Process）的标准化。只有将过程标准化了，才能保证最终的服务质量和成本符合预定的标准，才能实现过程控制，从而达到质量控制的目标。

在传统的IT管理模式下，IT部门是作为技术支持的角色被动地存在的，而在新的IT服务管理模式下，IT部门是作为一个主动的服务提供者向其客户和用户（企业的业务部门）提供赖以支撑组织业务运作的IT服务，IT部门和IT外包商往往需要向客户提供服务目录（SC）并和客户签订正式的服务级别协议（SLA）。

目前，全球的IT服务业正逐渐走向专业化和外包化。随着企业和政府组织的业务运作越来越依赖于IT，越来越多的组织考虑将其IT服务运营外包给专业的IT服务提供商或对内部的IT支持部门提出更明确的服务要求，以确保提高服务质量，降低服务成本，降低因IT服务中断所导致的业务风险。

如何控制这个IT服务的整体风险（无论是内部还是外部），提高IT的整体服务水平是一个需要高度重视的问题，而ISO/IEC20000就是解决该问题的一个很好的指南。

**标准特点**

ISO/IEC 20000-2:2005为审核人员提供行业一致认同的指南，并且为服务提供者规划服务改善或通过ISO/IEC 20000-1:2005审核提供指导。ISO/IEC 20000-2:2005基于已被替代的BS 15000-2的。

实践准则描述了在BS 15000-1中服务管理流程的最佳实践。为以最小成本满足业务需求，客户对使用先进设施会不断提出要求，服务提供就越发显得重要了。人们已经意识到服务和服务管理对于帮助组织开源节流的重要性。

ISO/IEC 20000系列能使组织了解如何从内部和外部改进其服务质量。

由于组织对服务支持的日益依赖，以及技术多样性的现状，服务提供方有可能通过努力保持客户服务的高水准。服务供应方往往被动工作，很少花时间规划、培训、检查、调查并与客户一同工作，其结果必然导致失败。其失败就源于没有采用系统、主动的工作方式。

服务供应商也常常被要求提高服务质量，降低成本、采用更大灵活性和更快反应速度。有效的服务管理能提供高水准的客户服务和较高的客户满意度。

ISO/IEC 20000-2描述了IT服务管理流程质量标准。这些服务管理流程为组织在一定环境中开展业务提供了最佳实践指南，包括提供专业服务、降低成本、调查和控制风险。

ISO/IEC 20000-2推荐服务管理者采用一致的术语和统一的方法进行服务管理，这可以为改进服务交付基础，并有助于服务提供者建立一个服务管理框架。

ISO/IEC 20000-2为审核人员提供指南，并可为组织规划服务的改进提供帮助，以便组织通过ISO/IEC 20000-1认证。

ISO20000 与 ISO9000比较

·ISO20000 与 ISO9000 的实用范畴不同：ISO20000 只针对 IT 服务管理，在 IT 服务提供商和政府及企业的IT部门应用较多；而 ISO9000 适用各行业的质量标准，在制造企业应用得最多。

·ISO20000 与 ISO9000 的侧重点不同：ISO20000 与 IT 服务流程相关，其流程的名称和控制采用的IT 人员容易接受的术语，对 IT 系统变更的风险进行管理；而 ISO9000 与质量框架相联系。

·ISO20000关注的内容和ISO9000相比，除IT服务质量外，如还关注财务、信息安全。

·ISO20000也可以说是ISO9000在IT服务行业的具体应用和拓展。

ISO20000和ITIL的关系

·ISO20000 作为 IT 服务管理的国际标准，是从 IT 服务管理最佳实践 ITIL 中发展而来。

·ISO20000 是13个管理流程，而 ITIL 是10个管理流程（不含服务台）。

·ISO20000 新增了业务关系管理与供应商管理，对应于 ITIL 中的服务等级管理。

·ISO20000 新增的服务报告，涵盖在 ITIL 的每个管理流程之中。

·ITIL 提供最佳实践指南

·ISO/IEC20000 提供基于 ITSM 的度量

**认证条件**

1、中国企业持有工商行政管理部门颁发的《企业法人营业执照》、《生产许可证》或等效文件；外国企业持有关机构的登记注册证明。

2、申请方的IT服务管理体系已按ISO/IEC 20000-1:2005标准的要求建立，并实施运行3个月以上。

3、至少完成一次内部审核，并进行了管理评审。

4、信息技术服务管理体系运行期间及建立体系前的一年内未受到主管部门行政处罚。

**认证步骤**

1.1 开展培训，职能分工

1.1.1 培训：

1.1.1.1 全员ISO20000基础知识培训。

培训目的 ：

了解ISO20000标准的内容；了解ISO20000标准的基本要求；了解ISO20000标准的实施办法；了解企业推行ISO20000意义和计划。

学习内容：

什么是ISO20000标准？对标准的理解；该公司推行ISO20000意义；该公司推行ISO20000的计划和要求。

1.1.1.2 骨干培训

培训目的

了解ISO20000标准的基本内容；领导在体系中的作用；了解为什么要推行ISO20000；要了解如何推行ISO20000。

学习内容

ISO20000标准的结构、原理和内容概述；重要的质量概念；实施标准的指导思想；领导在体系中的作用； IT服务管理体系认证、维护和改进的过程。

参加人员

公司总经理、副总经理、各有关部门经理和主管。

1.1.1.3 文件编写技能培训

培训目的

掌握文件编写方法；结合该公司实际如何编制有关文件。

学习内容

IT服务管理体系文件总论； IT服务管理体系编写；程序文件编写；工作文件编写；管理计划制定；管理记录。

参加人员

企业各有关部门领导、ISO20000工作小组内的成员，专职管理人员。

1.1.2 建立组织：

1.1.2.1 领导小组 ISO20000委员会

推行ISO20000，领导是关键，企业领导应作正确决策，并积极地带头参加这项工作；给出人力和物力支援；成立领导小组，主要领导都应当参与；任命管理代表，负责标准中规定的职责； 及时处理有关重大问题；组织管理评审。

1.1.2.2 工作机

为了推行ISO20000，公司应成立专门工作机构，负责全公司推行ISO20000组织协调工作，作为一个办事核心。应保证：

所有各有关部门都能参与工作小组；

有专职人员；

有骨干力量。骨干人员应对ISO20000有较全面系统的学习，最好有一定相关工作经历。

1.1.2.3 管理者代表

公司应按标准要求任命管理者代表。

应由最高管理者指定；管理者代表应是公司管理层成员；

管理者代表应具有如下职责：

确保按照标准规定建立、实施和维持IT服务管理体系要求；向管理者报告体系的执行情况，以便评审和改进管理体系；管理者代表的职责还可以包括就IT服务管理体系方面与外部机构的联络。

1.1.3 系统调查、诊断

1.1.3.1 通过诊断，达到以下目的：

现有体系与标准的符合性：找出与标准之间差距；找出形成这些差距原因。

1.1.3.2 选择合适的IT服务管理体系标准及其补充要求：

根据公司运作需要、合同要求、产品特点从ISO9000或其他标准中选择适合于企业的管理体系标准；

在此的基础上对选定标准进行必要的增删，提出对IT服务管理体系补充要求。

1.1.3.3 识别确定对服务管理体系进行修改的内容：

体系标准和要素选择；机构调整内容；体系文件清单；需新编制的文件（清单）

1.1.3.4 诊断的依据

诊断工作一般应按某一合适的IT服务管理体系标准、主要合同和本单位一些基本法规。根据各单位具体情况，诊断的依据可以归纳成如下几个方面：

管理体系标准：例如ISO20000标准；

诊断所选择的标准与申请认证的标准应是同一类型的。

合同：

IT服务管理体系应能基本满足各客户的要求，因此，合同应是论断的一个重要依据。

本单位的基本规定、规程：

如有关标准化方面的、有关监控方面的、有安全方面的等等，这些规定、规程是否合理及合理的内容是否被有效运行，诊断时要检查的内容。

社会或行业有关法规

IT服务管理体系不仅要满足管理体系标准、合同和公司有关规定，还应该符合国家、地区、行业有关法律、法规、规章制度的要求，诊断时应作为考虑。

⑴.有关安全法规；

⑵.有关服务法规；

⑶.有关环保法规；

⑷.有关劳动法规

1.1.3.5 实施诊断的人员

实施诊断员可以是公司内部的人员，也可以公司委托的外部机构，如谘询机构的人员，因此实施诊断的人员可以有如下几方面：

谘询人员：

如果公司聘请了谘询人员，诊断工作可以其为主进行。为此谘询机构可以委派专门诊断、检查工作组，制订计划，在企业确认的基础上按计划进行诊断。

内部审核员：

如果公司有经培训合格并胜任该项工作的人员，可以授权其进行诊断工作。

第三方审核机构的人员：

如果公司有需要，可以聘请外部审核机构的审核员为公司进行诊断

1.1.3.6 诊断工作的实施过程

确定诊断小组。

确定诊断依据和诊断物件。

制订诊断计划，编制诊断工作文件。

现场诊断检查

⑴.与现场人员交谈，了解情况；

⑵.检查现场文件和记录；

⑶.如实记录体系运行现状。

提交诊断报告

⑴.不合格报告；

⑵.诊断结论；

⑶.体系文件清单；

⑷.需新编制和修订的文件（清单）。

1.1.4 职能分工、体系设计

1.1.4.1 制订IT服务管理方针；

1.1.4.2 任命管理者代表主要责任：

协助管理者确保按标准的要求建立IT服务管理体系。

负责体系的实施和维护。负责组织内部管理体系审核，向最高管理者报告体系执行情况，以便评审和改进。

就IT服务管理体系方面问题与外部联系。

1.1.4.3 选择体系标准和要素

管理体系要素选择

⑴.根据合同要求，可删去所选择标准中包含的某些服务管理体系要素或分要素，还可以涉及体系要素证实程度的调整；

⑵按合同要求，规定对管理体系的补充要求，例如统计程序控制要求、安全性要求等。

设计调整组织机构

⑴各部门职责应覆盖标准要求.

⑵各部门有清楚的职责。

⑶各部门工作之间有合理的衔接。

⑷职能分工形成书面文件，并经充分讨论。

⑸应把有关管理的策划、控制、协调、检查、改进工作都反映出来。

确定新体系中文件结构

⑴典型文件层次

编写文件、试点运

1.1.5 编写文件

1.1.5.1 列出文件清单：

IT服务管理体系

⑴手册的构

⑵职能的分配

⑶组织结构

⑷手册中要素描

⑸有关支持性文件（针对某个具体事件的管理办法、工作流程、或者详细说明）

程序文件

⑴需编制哪些程序文

⑵每个程序文件对应标准哪个要

⑶各程序文件之间有无重复、有无遗

⑷各程序文件形成的记录

⑸有关支援性文件

工作文件

⑴作业指导

⑵技术类文

⑶管理文件

⑷报告和表格

1.1.5.2 明确哪些旧文件作废、哪些保留

1.1.5.3 分配文件编写任务：

各部门参与

1.1.5.4 起草文件

1.1.5.5 文件讨论：

内部讨论─适用性

外部检查─完整性

1.1.5.6 文件批准发效

审核、批准

复印、装订

受控、登记

发效、签收

1.1.6 试点运行

1.1.6.1 向工作人员进行体系文件的交代：

手册：特点、使用、保管要求；

程序：特点、注意事项、形成记录、各程序之间介面；

工作文件：需要掌握关键问题如何记录，报告不合格品。

1.1.6.2 培训、宣传：

培训：岗位培训；

特殊岗位培训考核；

管理人员程序文件培训；

全员IT服务管理方针、目标培训。

宣传：管理方针；

试运行计划；

ISO20000认证计划；

体系文件内容介绍。

1.1.6.3 其他配套工作：

监控；

合格分承包方许定；

标识的制作。

1.1.6.4 试运行：

补充完善基础工作：边运行，边完善第三层次文件；

修改体系文件：边运行，边修改不合适的文件；

作为记录并保存好记录以推供证据。

1.2 内部审核、正式运行

1.2.1 部审核、管理评审：

至少进行一次内部审核，按ISO20000要求制订审核计划、审核清单、审核报告、不合格项的跟踪和监督等有关活动记录和文件应保存完好，以便以认证检查。

至少安排一次管理评审，以评价新体系的有效性和适用性，同时积累一次管理评审活动记录，评审按程序文件要求进行。

1.2.2 正式运行：

通过内部审核、管理评审，对体系文件中不切合实际或规定不合适之处进行及时的修改，在一系列修改後，发布第二版管理手册、程序文件进行正式运行。

1.3 内部审核，准备认证

1.3.1 为了减少认证一次通过可能存在的某种风险，在由第三方正式审核之前，可以由内部审核组成类似的外部机构进行一次内部审核或请已确认的认证机构进行预审。

1.3.2 企业应本着对自己有利的观点选择认证机构，一般应从以下几个方面考虑：

客户要求；

企业所在地区；在选择认证机构时应在原则上既近又便；

认证机构的认证范围和有效性；

费用；正常认证收费和交通、食宿等其他费用。

1.4 正式审核，体系维持

1.4.1 接受所选择的认证机构的正式审核。

1.4.2 体系维持与提高

检查现场中问题，不断地改进和巩固；

进一步完善体系文件，加强协调监督工作

**认证好处**

企业建立IT服务管理体系的目标是为了企业建立起一套行之有效的以客户为中心的自我完善的体系。在实施认证ISO20000管理体系后，在各个流程中，各个工作岗位上都建立了一个自我完善的循环，工作的策划、执行、检查，以及持续的发现问题改善问题的体系建立起来，使每个员工都拥有问题意识，自觉的发现自己工作当中的问题，并通过系统的解决问题的方法，将问题一个一个的解决。IT服务提供商通过实施IT服务管理体系，可以获取如下收益：

·保持服务目标与企业业务目标一致，有效的支持业务战略

·建立规范的服务流程，提高信息技术服务和运营效率

·有效及高效地整合和利用信息、基础架构、应用及人员等IT资源

·建立持续改进的服务管理机制，快速应对市场需求，提供客户满意度

·向国际标杆靠齐，增强市场竞争力，提高组织声誉，提升投资回报

·控制IT风险及相关的成本，提高与控制IT服务质量、降低长期的服务成本

·灵活应对来自客户、认证机构、内部机构等不同的合规审核要求，增加投资者信心

对于众多IT服务提供商，ISO20000认证的意义并不仅仅限于IT服务符合规程和提高服务质量。它在服务量化，员工绩效考核，衡量IT部门投资回报方面更具有积极的意义。

**基础要求**

ISO20000是以流程化管理方式为基础的，IT工作被分解成了不同的流程，每个小部门、每个人的工作都是若干流程中不同工作的组合，流程对工作量化的输入输出为员工的工作量化提供了可能。员工的量化考核这个IT部门的普遍难题得到了初步解决，尤其是服务台的一线员工基本做到了完全的工作量化衡量。

流程的量化数据为员工的工作分配，工作成绩的反映提供了基础，同时对于工作人员的责任也有了相应的考核体系。

同时，IT对服务也有了量化指标，建立了量化的质量控制体系，设定了完整准确的考核指标，提供完善的报表。对客户满意度等还选用第三方进行调查，保证数据的可信性。

量化管理不仅是IT部门自身管理的需要，也是衡量IT部门价值与投资回报的基础，流程化管理方式为量化管理的实现提供了可能。借用ISO20000，CIO也同时找到了一个衡量IT服务好坏的国际公认的标准。用这么一个标准来证明公司的ITSM实施达到了怎样一个阶段，在一个标准的平台上跟CEO、CIO沟通IT服务管理的标准化、规范化。

**试用范围**

ISO/IEC 20000是一个针对管理流程系统的标准，ISO/IEC 20000的认证适合IT服务的提供者，可以内部的IT部门，也可以是外部的服务提供商。获取ISO/IEC 20000的认证，意味着提供服务的IT组织，对ISO/IEC 20000中定义的这些管理流程，具有足够好的管理控制力。这里所谓对流程的管理控制力包括：

·对流程输入的了解和控制

·对流程输出的了解、使用和诠释

·制定和执行对流程效能的衡量机制

·有客观的证据表明，对流程的功能负责，使之符合ISO 20000标准要求

·制定流程的改进提高计划，衡量和回顾改进结果

IT服务组织要获得ISO/IEC 20000的认证，必须证明它能够对标准中涉及的所有5组13个流程都具有以上的管理控制力。ISO/IEC 20000系列对流程的最佳实践进行了总结，可适用于不同规模、类型和结构的组织，服务管理流程最佳实践要求并不会因为组织形式不同而被改变。

**组成部分**

ISO 20000-1是一个正式的规范，它界定了一个组织向客户提供品质合格、管理良好的服务的有关要求。

另一方面，ISO 20000-2是一个行为准则，它描述了ISO 20000-1范围内的服务管理程序的最佳范例。这个行为准则对于要准备通过ISO 20000-1审核或计划改进服务的公司来说尤其有用。

**实施效益**

· 得以获得业界普遍认同的国际证书ISO20000认证；

· 就服务质量和服务承诺与业务及供货商达成一致，建立和业务及供货商统一的沟通平台；达到相关利益方均满意的IT服务管理目标；

· 提高IT服务的可用性、可靠性和安全性，为业务用户提供高质量的服务；

· 持续优化服务流程，提升服务水平，提高业务满意度；

· 提高项目的可提供性并确保如期交付；

· 从总体上提高组织/企业IT投资的报酬率，提升组织/企业的综合竞争力；

· 建立IT部门一整套行之有效的持续改善机制和内控机制；

· 明晰IT管理成本和组织/企业业务战略和IT战略目标的结合点，完善现有IT服务结构和资源配置，使各项IT资源的运用符合公司业务战略和IT战略目标；

· 通过建立优化、透明的管理流程和权责的定义，监控管理流程、进行绩效评价；降低IT运营的管理成本和风险；

· 易于整合服务管理流程和其它管理系统，如：信息安全管理体系ISMS 、质量管理体系ISO9000等；

· 将现有管理体系和业务流程整合，规范IT部门服务水平，规范工作流程，降低由人员变动导致的风险；

· 提高IT部门相关员工的专业素质，提高员工的服务能力和工作效率；

· 提升IT部门整体运作及部门间沟通的能力。