北京恩格威认证中心有限公司

信息技术服务管理体系认证专项管理规则

文件编号：NGV-GZ-002-2016

发布日期：2016 年 10 月 08 日

修订日期：2016 年 10 月 08 日

实施日期：2016 年 10 月 08 日

目　　录

信息技术服务管理体系认证专项管理规则

1 适用范围

为规范信息技术服务管理体系认证活动，制定本文件。该文件适用于恩格威认证中心有限公司（以下简称：NGV）信息技术服务管理体系认证受理评审、项目管理、审核实施活动。

本文件是对《管理体系认证受理管理规则》、《管理体系认证证书转换管理规则》、《管理体系认证项目管理规则》、《管理体系认证审核时间确定规则》、《管理体系认证通用审核管理规则》、《多场所审核管理规则》的补充。

2 参考和引用文件

2.1 CNAS-CC175：2017 信息技术服务管理体系认证机构要求

2.2 CNAS-SC175：2017 信息技术服务管理体系认证机构认可方案

2.3 ISO/IEC 20000-1：2018《信息技术 服务管理 第一部分：服务管理体系 要求》

2.4《管理体系认证受理管理规则》

2.5《管理体系认证证书转换管理规则》

2.6《管理体系认证项目管理规则》

2.7《管理体系认证审核时间确定规则》

2.8《管理体系认证通用审核管理规则》

2.9《多场所审核管理规则》

2.10《管理体系认证决定管理规则》

2.11《管理体系认证的批准、拒绝、保持、扩大、缩小、暂停、恢复和撤销的条件和管理规则》

3 认证受理及评审特殊要求

3.1 认证受理特殊要求

3.1.1 认证受理的通用要求按《受理认证申请及合同评审程序》的要求执行。证书转换按《证书转换控制程序》要求执行。

3.1.2 受理条件特殊要求

申请方在一年内，未发生所提供服务安全事故、服务协议违约、服务对象投诉以及对服务对象等造成重大影响、违反国家相关法规，虚报、瞒报获证所需信息的情况。

3.1.3 申请方提交资料特殊要求

申请方按《恩格威认证申请书》中“基本资料”与“信息技术服务管理体系认证补充资料清单”：

ITSMS 管理体系认证申请基本资料：

(1) 法人资格证明（工商营业执照、事业单位法人证书或社会团体法人登记证书）；

(2) 取得相关法规规定的行政许可文件(适用时)；

(3) 从事业务活动符合中华人民共和国相关法律、法规、信息技术服务标准和有关规范要求；

(4) 对信息技术服务管理体系认证范围涉及业务活动的描述，包括利用信息技术为内部或外部顾客的业务过程提供支持的说明；

(5) 已按认证依据和相关要求建立和实施了文件化的信息技术服务管理体系（含手册（适用时）及相关体系文件）；

(6) 体系有效运行3个月以上，并且已完成内部审核和管理评审。

ITSMS管理体系认证申请补充资料：

(1) 申请认证的范围；

(2) 对信息技术服务管理体系认证范围涉及的业务活动的描述，包括利用信息技术为内部或外部顾客的业务过程提供支持的说明；

(3) 申请组织如存在不完合包含在ITSMS范围内的服务活动时，应在申请书上予以说明；

(4) 经营场所、分场所、临时服务点以及各场所从事的活动等；

(5) 管理体系覆盖的有效人数；

(6) 供应商（含外包方）的数量；

(7) 服务级别协议的数量。

(8) 关于认证活动的限制条件(如出于安全和/或保密等原因，存在时)。

3.2 受理评审特殊要求

3.2.1 项目管理人员按照《受理认证申请及合同评审程序》的规定进行评审并填写《申请评审表》，以确保：

1）识别申请认证客户的行业类别和与之相应的信息技术服务提供过程的特性和服务要求；

2）掌握国家对相应行业的信息技术服务管理体系认证的管理要求；

3）申请认证的客户的管理体系信息充分，可以进行审核；

4）认证要求已有明确说明并形成文件；

5）解决了 NGV 与申请认证客户之间任何已知的理解差异；

6）NGV 有能力并能够实施认证活动；

7）考虑了申请认证范围、客户组织运作的场所、完成审核需要的时间和任何其他影响认证活动的因素；

8）保持了决定实施审核的理由和记录。

当申请认证的客户进行证书转换时，项目管理人员按照《管理体系认证证书转换管理规则》进行评审，填写相应的申请评审记录。

项目管理人员在申情评审时应重点审查或与认证客户沟通了解下列信息（但不限于此）：

a) 通过其组织单元(如：单个部门、一组部门或多个部门)；所提供的服务（如：单个服务，金融服务、零售服务、电子邮件服务之一或一组服务，几种服务的组合）。交付服务的地点（如：单一办公场所、一组办公场所、区域的、全国的或全球的）、顾客及其地点：例如：一个顾客、多个客户、外部顾客或内部顾客。服务提供所用的技术（如：IT 远程运维服务等）以及其他适用的方面清晰界定其 ITSMS 的范围和边界。范围描述示例：

位于「地理位置」「组织的名称」向「顾客的组织和或组织单元的名称」交付「服务」的服务管理体系。

b) 受审核方的职能关系架构、服务支撑系统、分布区域；

c) 评审其覆盖范围的服务活动的服务风险（包括可用性、事件）。

3.2.2 初审项目评审应重点关注的特殊要求

1) 当申请认证范围覆盖的服务 / 活动有资质、许可证要求时，应核查提交的相关证明资料：认证客户与受审核方是否一致、发证的部门、证明的有效期限、覆盖服务的类别、授权的范围及特殊的限制等；

2) 当认证申请方在申请材料中明确了不可接触信息，应评价此不可接触信息是否影响后续审核取证活动，如影响，则不予受理，或者选择可以接触此类信息的审核员，此过程应该在《申请评审表》、《审核方案策划表》、《审核通知书》予以记载；

3) 信息技术服务存在服务的交付点，应仔细核查相应资料，充分了解各交付服务的物理场所的服务类别、服务内容、目标、服务级别及服务活动的进展状态或阶段、分布区域；服务点的服务类别和服务内容应与认证范围一致并相互对应，不能缺漏；

4) 应关注并了解受审核方的主要服务项、服务流程、服务目标、协议、事件活动，特别是认证客户要求在证书上表述服务或活动时，应核查认证客户申请认证覆盖的服务项、服务内容表述的规范和完整性，对不一致之处，应及时与受审核方沟通、澄清，达成共识并确认。需要时，还应了解受审核方支持性的服务/活动等信息，并做相应记录；

5) 审查申请规定应提交的服务级别协议（SLA）、供应商名单、不可接触信息清单与说明等是否缺项，是否符合要求；对于其服务会对客户造成重大影响但无法判定的，应要求审核组在第一阶段现场审核时确认；

6) 受理阶段风险评价重点关注的问题:信息技术服务项目服务级别协议（SLA）、服务内容、服务可用性、服务支持方式、服务要求、服务指标、优先级内容的完整性，对于没有提供相应资料无法准确进行合同评审的项目，原则上不能受理；

7) 对于信息技术服务管理体系，还应重点关注受审核方存在服务外包的情况时，评审服务外包活动对客户最终的业务流程的影响程度，确定是否需要对服务外包方的服务过程实施现场审核，除非服务外包方提供的服务或其他活动已获得相应的信息技术服务管理体系、信息安全管理体系认证。

3.2.3 再认证项目受理评审特殊要求

评审的程序、要求同初次审核项目，但要特别关注对获证客户新需求和变化信息的评审，如（但不限于此）：

1) 申请认证领域的变化；

2) 申请认证覆盖的服务类别的变化；

3) 受审核方的结构层次、不可接触信息及主要人员的变化；

4) 取证要求的变化；

5) 供应商的变化；

6) 服务目录的变化（或服务级别协议 SLA 的变化）；

7) 服务点的变化；

8) 资质、许可证的有效性。

对申请不通过的合同，由项目管理部与申请方联系，洽谈澄清有关事实，取得一致意见后再次评审。如因其他原因构成不能受理的，则向申请方说明情况，发出《不予受理通知书》，按申请方要求退回有关资料。拒绝申请的原因应记录并使客户清楚。

4 认证项目管理特殊要求

对于信息技术服务管理体系转版，新旧标准对比描述的审核技术要求见附录 A《信息技术服务管理体系审核技术要求》。

4.1 审核方案的策划特殊要求

4.1.1 总要求

审核方案管理人员应根据评审的结果，按照《受理认证申请及合同评审程序》或《证书转换控制程序》的过程要求进行审核方案策划。并将并将审核方案策划结果填写在《审核方案策划表》中同时传递到审核组，由审核组在现场确认，必要时根据审核组在现场确认的结果调整审核方案。

应考虑受审核组织是否有不允许 NGV 接触的包含保密性/敏感性的信息资产或 NGV 接触该类信息资产时应满足的特殊要求。同时应对客户不允许或者限制解除的信息资产对审核的影响进行评估并采取相应的措施。

4.1.2 审核时间策划的特殊要求

NGV 针对每个申请 ITSMS 认证客户的初次审核（含一、二阶段）、监督审核及再认证策划所需的审核时间。策划根据《审核时间确定控制程序》进行，并按 Tc＝Tj＋Tz＋Tf 公式进行计算。公式中的 Tj 为进行 ITSMS 认证审核的最少人日数。Tz 为服务种类增加所需的审核时间和 ITSMS 复杂度影响所需的审核时间 Tf。需要增加审核时间的因素：

1）多场所抽样、临时场所或服务网点抽样所需的审核时间；

2）工作语言超过一种（需要翻译或影响审核员个人独立工作）应增加初次审核时间 Tc 中审核时间的 20%-30%。

3）审核组成员不宜在审核过程中以任何方式记录客户的保密或敏感信息。审核组在离开客户前，宜请客户检查和确认审核组携带的文件、资料和设备中未夹带客户的任何保密或敏感信息

其他可以减少审核时间的因素：

1)、体系一体化结合的程度。

每年监督审核时间应不低于初次认证审核总时间的 40%，再认证审核时间应不低于初次认证审核总时间的 70%。

每次审核的现场审核时间不低于总审核时间的 80%。

4.1.3 审核组能力策划和人员选派的特殊要求

项目管理人员应根据实现审核目的所需的能力以及公正性要求来选择和任命审核组（包括审核组长以及必要的技术专家），审核人员必须取得信息技术服务管理体系认证注册资格。审核组由取得的人员组成，其中至少一名专职审核员。

如果仅有一名审核员，该审核员应有能力履行适用于该审核的审核组长职责。审核组应整体上具有审核范围内的所有技术领域（NGV《管理体系认证业务范围清单》）对应的能力，否则应在技术专家支持下实施审核。

具有信息技术服务、信息技术服务法规等方面的特定知识的技术专家可以成为审核组成员。技术专家和翻译人员应在审核组的指导下工作。技术专家不能作为审核员。使用翻译人员时，要避免其对审核产生不正当影响。

每次审核（包括一阶段和二阶段审核）、监督审核、再认证审核的审核组均应具备专业能力。

决定审核组的规模和组成时，应考虑下列因素：

a) 审核目的、范围、准则和预计的审核时间；

b) 结合审核、联合或一体化审核，尽量选派具有多体系注册审核员，结合审核或一体化审核的审核组长至少对一个标准非常熟悉，并了解审核所用的其他标准；

c) 实现审核目的所需要的审核组的整体能力（专业类型全覆盖）；

d) 认证要求（包括适用的法律、法规或合同要求）；

e) 语言和文化。

项目管理人员根据特定的获证组织的 ITSMS 变化情况（特别是在监督审核、再认证审核方案策划时），项目管理人员应对原有的能力分析进行审查，必要时进行更新，并按更新后的能力需求委派具备相应能力的审核组实施审核。

选派 ITSMS 审核组应补充考虑：

1) 具备了拟认证的具体范围所涉及到的专业技术知识、相关作业程序、特定行业的最新技术知识，包括诸如可能存在的事件故障、数据安全对服务提供造成的影响、涉及有关覆盖 SLA 过程及其管理、发布管理、配置管理等过程涉及使用的特定软件工具。必要时，包括软件开发、设计、运维流程设计、数据应用管理等特定的技术知识；对审

核中可能遇到的服务风险的识别和评价能力；对所提供服务及使用技术进行验证的能力；对有关程序和潜在故障、事件、问题方面进行识别和分析的知识等基本能力要求。

2) 对于依赖信息系统和网络环境进行业务活动程度的组织，宜选派具有如远程审核工具运用、软件代码审查、网络系统架构设计等能力的审核员。

4.1.4 审核策划的特殊要求

4.1.4.1 初审认证审核策划

4.1.4.1.1 初次认证审核分第一阶段和第二阶段进行。第一阶段必须安排到现场审核。考虑第一阶段与第二阶段现场审核间隔不少于 5 个工作日且不多于 60 个工作日的要求进行策划。

4.1.4.1.2 一阶段审核应在申请客户组织的现场进行，审核应包括的内容：

(1) 审核申请客户的信息技术服务管理体系文件；

(2) 评价申请客户的运作场所和现场的具体情况，并与申请客户的人员进行讨论，以确定第二阶段审核的准备情况；

(3) 审查申请客户理解和实施信息技术服务管理体系标准要求的情况；

(4) 审查申请客户是否系统而充分第识别与所提供的服务相关的法律法规和其他要求及其遵守情况；

(5) 审查第二阶段审核所需资源的配置情况；

(6) 结合申请客户信息技术服务管理体系方针和目标，了解其审核准备的状态，为策划第二阶段的额审核提供重点；

(7) 评价认证客户是否策划和实施了内审与管理评审以及信息技术服务管理体系的实施程度能否证明已为第二阶段做好准备。

4.1.4.1.3 第二阶段审核

第二阶段审核应具备实施认证审核的条件下在申请客户的场所进行。如第一阶段审核提出了影响第二阶段的审核问题，这些问题应在第二阶段审核前得到解决。第二阶段审核的目的是通过在申请组织的现场进行系统、完整地审核，评价申请客户的信息技术服务管理体系是否满足所有适用的认证依据的额要求，并判断是否推荐认证注册。并证实与申请客户的和信息技术服务活动是相适应的。

审核组应要求申请客户证实其对信息技术服务管理过程的分析和组织运作实施了适当的控制措施，应包括：

1）服务交付过程（服务级别管理、服务报告、服务连续性与可用性管理、信息技术服务

的预算与核算、能力管理、信息安全管理）；

2）关系过程（业务关系管理、供方管理）；

3）处理过程（事件管理、问题管理）；

4）控制过程（配置管理、变更管理）；

5）发布过程（发布管理）。

4.1.4.1.4信息技术服务管理体系文件与其他管理体系文件的整合

只要信息技术服务管理体系以及与其他管理体系的适当接口能够清楚被识别。可以允许申请客户将信息技术服务管理体系文件与其他管理体系文件（如：质量管理体系、环境管理体系、职业健康安全管理体系、信息安全管理体系等）相结合。

4.1.4.1.5管理体系结合审核

信息技术服务管理体系与其他管理体系结合审核时，按以下管理要求执行：

a) 对诸如审核范围、审核时间的确定、审核方案策划进行有效管理。

b) 必须以审核活动满足信息技术服务管理体系认证所有要求为前提，并且审核质量不应由于结合审核而受到负面影响。在审核报告中应清晰体现所有与信息技术服务管理体系有关的重要要素的描述并已于识别。

4.1.4.1.6初次认证的审核结论

审核组应该对第一阶段和第二阶段审核中收集的所有信息和证据进行汇总分析，评价审核发现并就审核结论达成一致。

4.1.4.2 认证决定

执行 NGV《管理体系认证决定管理规则》。

4.1.4.3 监督审核策划的特殊要求

在满足认可要求的基础上，根据获证组织信息技术服务管理体系覆盖的业务活动的特点以及所承担的风险，合理设计和确定监督审核的时间间隔和频次。当获证组织信息技术服务管理体系发生重大变更，或发生重大问题、服务质量事故、客户投诉等情况时，应视情况可增加监督频次。

监督审核的最长时间间隔不超过 12 个月。初次认证后的第一次监督审核应在认证决定日期起不超过 12 个月内进行。由于获证组织业务运作的时间(季节)特点如有限时段(例如：临时施工场所）安排等原因，可以合理选取和安排监督周期及时机。在认证证书有效期内的监督审核必须覆盖信息技术服务管理体系认证范围内的所有业务活动。

第一个三年认证周期从初次认证决定算起。以后的周期从再认证决定算起。

4.1.4.3.1 监督审核应包括，但不限于以下内容：

1）体系保持和变换情况；

2）顾客投诉情况；

3）涉及变更的范围；

4）内部审核与管理评审；

5）服务目录的变化情况；

6）对上次审核时提出的不符合所采取纠正措施的审查和验证；

7）标志的使用和或认可其他对认证资格的引用。

8）适当时，其他选定的范围。

4.1.4.3.2 监督审核结果评价

对于监督审核合格的获证客户，NGV 应作出保持其信息技术服务管理体系认证资格的决定；否则，应暂停、撤销相应认证资格。

4.1.4.4 再认证审核策划的特殊要求

4.1.4.4.1 再认证应考虑信息技术服务管理体系在认证周期内的绩效，包括调阅以前的监督审核报告。

4.1.4.4.2 当获证客户的信息技术服务管理体系或其运作环境有重大变更时，应考虑其进行第一阶段审核。

4.1.4.4.3 对于多场所或结合审核的认证，再认证审核的策划应确保现场审核具有足够的覆盖范围，以提供对信息技术服务管理体系认证的信任。

4.1.4.4.4 NGV 根据再认证的结果，以及认证周期内的体系评价结果和认证使用方的投诉，做出是否更新认证的决定。

4.1.4.5 特殊审核策划的特殊要求

4.1.4.5.1 扩大认证范围，NGV 对认证客户认证扩大的范围的申请进行评审，策划审核活动，可以单独进行，也可与监督审核或再认证一起进行。

4.1.4.5.2 由于 NGV 为调查投诉、对变更做出回应或对暂停认证资格的获证客户进行追踪，可能需要在提前较短时间通知获证客户后对其进行审核。策划：

1）应向获证客户说明并使其提前了解将在何种条件下进行此类审核；

2）应指派具有丰富经验的审核员组成审核组。

4.2 审核任务下达特殊要求

初次认证审核分第一阶段和第二阶段进行。第一阶段审核应进入受审核方的现场进

行。

确保第一阶段与第二阶段现场审核间隔不少于 5 个工作日且不多于 60 个工作日。

5 审核实施特殊要求

审核实施活动通用要求按《管理体系认证通用审核管理规则》、《多场所审核管理规则》的要求执行。

审核所使用的信息收集方法还应包括对 ITSMS 过程有效性的测试。

5.1 审核组审核活动策划特殊要求

5.1.1 审核任务的准备

审核组长接到审核任务书时应了解客户的相关风险：专业行业风险（如涉密要求、公共数据安全、软件源代码）、不可接触信息的风险、服务对象的顾客风险、法规、政策风险（如个人信息的泄露）、舆论风险、公正性风险和财务风险（客户效益不好）等信息。

5.1.2 文件评审要求

1） 信息技术服务管理体系文审重点：

a) 标准中所要求的建立文件化的 ITSMS 是否完整；

b) ITSMS 文件层次、结构及相互关系是否清晰；

c) 是否明确 ITSMS 各个职能与层次的组织机构与职责；

d) 外包服务商及管理要求；

e) 方针和目标、措施计划、运行、监测、纠正与预防措施等有逻辑关系的要素之间的接口关系是否描述清楚；

f) 运行规则是否明确阐述其管理和控制范围；职责是否清楚；方法描述是否清晰并具可操作性；

g) 服务改进的策划及实施情况。

5.2 审核计划特殊要求

5.2.1 制定审核计划总体上应：

1) 审核范围与合同评审及审核任务通知书中范围一致；

2) 审核计划覆盖审核任务书中的审核时间、人日数、审核员；

3) 审核的条款按照专业类别及技术领域能力安排。

5.2.2 应安排专业审核员实施对 5、6.3、6.5、9.1、9.2、软件维护 9.3；5 条款专业审核把关（设计和转换新的或变更的服务、服务连续性和可用性管理、能力管理、配置管理、

变更管理、发布和部署管理）。

5.2.3 审核组长在编制审核计划时，应识别客户的服务管理体系、服务交付过程和服务控制过程、解决过程、关系过程，并考虑部门集合、相关过程的集合来编制审核计划。审核计划在安排分组时，既要考虑过程的关联性、又要考虑审核人员专业和领域的能力。

5.2.4 多地点抽样时，应关注现场业务活动的差异性，当服务点所提供的服务类别/使用技术一致时可对其抽样，抽取的服务点的服务类别应覆盖标准“十三”个管理过程，所有场所在同一 ITSMS 下运行，并接受统一的管理、内部审核和管理评审。

a） 审核组应审核 ITSMS 中每个有重大信息安全风险的场所；

b） 无论在其总部（中心职能机构）或其他任一单一场所发现不符合，纠正措施的实施适用于该组织的所有场所；

c） 在审核周期内（3 年获证期间），监督审核方案应覆盖其组织的所有场所。

5.2.5 区域的表述应具体到单元（楼层，门牌号），不应笼统进行描述。

5.3 初次审核特殊要求

初次审核应按本文件 4.1.4.1 要求实施，审查客户理解和实施标准要求的情况，特别是对信息技术服务管理体系的服务连续性和可用性等过程、服务交付情况，相关的要求及 SLA 的遵守情况。

审核组长根据对其服务类别、包含的服务活动及 SLA 的要求确定所取样本应尽可能覆盖标准中“十三”个管理要求的内容。

多现场的客户至少安排一个分场所（总部所在地的分场所除外）进行现场审核，选择抽样的场所时应考虑不同的区域、不同的服务类别、服务过程、SLA，应首先选择服务风险及影响较大的分场所。

5.3.1 第一阶段审核

第一阶段审核包括文件审核及现场审核。第一阶段审核应进入受审核方的现场进行，现场审核时间不能少于 1 人日。

当受审核方由于信息安全的原因在申请评审阶段不能提供给本机构足够的信息时，审核组应通过第一阶段审核在受审核方现场补充对上述信息的确认，并完成申请评审。

1）第一阶段审核应侧重于组织的策划过程，主要内容为：

a） 通过现场观察，了解组织的基本概况，包括受审核方的范围，组织机构及职能，信息技术服务的流程和特点、活动的现场分布情况。应关注在生产、服务和活动过程中控制点的场所；

- 服务点；
- 关键过程，如灾备中心、核心机房等；
- 相关基础设施（环境、设施、设备、工具）；
- 临时现场、分现场 ；
- 特殊的人员要求；
- 重要的供应商（外包方）管理。

b） 文审包括信息技术服务方针、目标；

c） 确认受审核方的 ITSMS 范围和边界的界定是否清晰和充分；

d） 组长提供第一阶段审核报告。报告内容如下：

1） 文件符合性结论；

2） 体系建立和运行的基本情况；

3） IT服务管理范围、过程、场所得必要信息；

4） 组织机构和职责的合理性；

5） 关键/重要IT服务活动的识别、评价和基本控制情况；

6） 适用于组织的法律、法规以及顾客要求的获取和遵守情况；

7） 方针、目标、指标和IT服务管理措施建立的合理性；

8） 与IT服务管理体系相关的信息交流及相应措施记录；

9） 必要的监控机制建立；

10） 内审的可信性及持续改进机制建立；

11） 管理评审的实施情况；

5.3.2 第二阶段审核

5.3.2.1 二阶段审核应重点关注申请组织的下列方面：

(1) 符合ISO/IEC 20000-1：2011 要求的文件；

(2) 针对信息技术服务的管理职责；

(3) 所选择和实施的控制措施、过程的结果相互之间的一致性，以及它们与ITSMS 方针和目标之间的一致性；

(4) ITSMS 有效性的评审和信息技术服务控制措施有效性的测量，以及对照ITSMS 目标进行的报告和评审；

(5) 方案、过程、规程、记录、内部审核和对 ITSMS 有效性的评审，以确保其可被追溯至管理决定和ITSMS 方针与目标；

(6) 是否对法律法规符合性的保持和评价；

(7) ITSMS管理评审。

5.3.2.2 确认认证范围

a) 确定审核范围特别要关注受审核方的服务活动/过程发生在不同区域与地理位置。

b) 应了解受审核方的组织结构及每个组织单元的服务类别、服务技术及服务级别的差异。

c) 对临时服务的场所（包括移动场所），要注意服务活动不同阶段、服务类别、服务点的差异性，为确定具体的审核地理位置与区域提供输入信息；当确定仅对提供服务的场所实施认证审核时、或对临时/移动场所进行抽样审核时，应对其与总部的接口进行审核。

5.3.2.3 不合格的性质划分原则：

1）严重不符合

失败的实施或未遵守一个或多个标准适用的控制措施条款要求，因此产生关于对保护敏感信息的保密性、完整性和可用性测量的适当性的严重质疑，和/或一个无法接受的风险，可能未被组织的利害关系人觉察到。整个体系控制措施或程序的失效。

严重不符合项的部分范例如下：

a) 体系运行出现系统性失效。例如某一要素、某一关键过程重复出现的失效现象，又未能采取有效的纠正措施加以消除，形成系统性失效；

b) 体系运行区域性失效。例如某一部门或场所的全面失效现象，或者各层次、各部门中有关的要素失效，且没有纠正措施；缺乏业务持续性计划；

c) 造成严重的 IT 服务危害，或潜在危害严重后果；

d) 极高数量的不符合项集中在标准中某一要素或是部门；

e) 上次审核中发现的一般不符合重复发生；

f) 严重违背法律法规要求，后果较严重；

g) 相关方的严重投诉。

2）一般不符合

被观察到的一个单独失误，或隔离的意外事件。

一般不符合项的部分范例如下：

a) 对满足IT服务管理体系要素或体系文件要求而言，是个别的、偶然的、孤立的、性质轻微的不符合；

b） 对保证所审核范围的体系而言，是次要问题

5.3.2.4 审核报告：

审核报告应足够详细，以帮助和支持认证决定。审核报告应包括：

(1) 审核覆盖的区域（例如，认证要求和接受审核的场所，及每个场所审核的起止时间），也包括所采用的主要审核路线和所使用的审核方法；

(2) 审核过程的描述，IT服务活动识别、特别是重要/关键IT服务活动识别和管理的适当性。包括文审摘要；

(3) 受审核管理体系核心过程认证审核的说明；

(4) 法律法规和其他要求识别和管理的充分性和遵守法律法规满足客户要求的情况；

(5) 审核发现，关于组织的ITSMS与所有认证要求的符合性的说明。包括体系的实施情况，是否正确的实施和保持：包括方针、目标指标和管理要求的实施完成情况，重要IT服务活动是否都得到控制，各种程序文件和作业指导书的执行情况；

(6) 审核结果，包括正面的和负面的；

(7) 已识别的任何不符合的详细情况，包括支持它们的客观证据和这些不符合所涉及的认证准则的要求（界定严重不符合和一般不符合）；

(8) 受审核方IT服务管理体系实施的持续适宜性和有效性，包括服务改进等；

(9) 受审核方的IT服务管理体系符合标准的情况；

(10) 对ITSMS内部审核和管理评审的信任程度的评价；

(11) 最终确定的审核范围；

(12) 审核组的推荐意见；

(13) 分歧及其说明（适用时）；

(14) NGV的 审批意见

(15) （审核实施与计划的偏离情况）等。

5.4 监督审核特殊要求

在证书有效期，监督审核可以不覆盖标准的全部要求，如在覆盖范围内有新的服务点增加也应纳入本次监督的审核范围中。应重点审核服务活动及SLA的实现情况，重点事件过程的控制，对服务提供的范围审核应覆盖标准所涉及的“十三”个管理过程，如4.1、4.3、4.4、5、6.1、6.2、6.3、7.2、7.3、8.2、9.2等条款并形成有效的证据链。

1） 对各部门、相同的现场的抽样须三年内全部覆盖。信息技术服务管理体系的推进部门每次都应进行审核。如果获证组织上的分布于几个不同的场所，每监督审核可针对不

同的现场进行抽样，但应确保在三年中覆盖全部现场，其中每年对其总部至少应进行一次审核。

2) 每次监督审核应涉及主要IT服务管理体系要素，三年内的不同次监督审核对各个要素审查的深度和广度可各有侧重，应注意对上次现场审核遗留问题的验证。

3) 监督审核必审条款：ISO/IEC 20000-1：2011标准中的4.1；4.2；4.5.1；4.5.4；4.5.5；5；6.1；6.2；6.3；6.6；7.1；7.2；8.1；9.2；条款必须核查。标准其他条款在3年监督审核时至少应审核1次。

4) 较之初次审核，监督审核的要求不仅不应放松，反而应适度从严，如发现与上次审核相同的问题，应考虑不符合性质的升级。

5.5 再认证审核特殊要求

每次再认证时至少应获取以下信息：

1) 文件化体系，包括获证客户机构的变化、体系文件、服务类别、服务目录、服务级别协议、服务点、供应商、顾客的变化，更改涉及区域的运行有效性、符合性；

2) 资质、行政许可等的持续适宜性，特别是涉及保密信息的项目，当保密资质撤销后，证书应及时进行相应处理。

服务级别管理、服务报告、服务连续性与可用性管理、信息技术服务的预算与核算、信息安全管理、业务关系管理、供方管理、事件管理、问题管理、配置管理、变更管理、发布管理等过程是否得到有效管理。

5.6 非常规审核的特殊要求

a) 扩大认证范围的审核

要改变区域和服务类别的扩大认证范围的审核，应做一阶段审核；

扩项时的必查条款：

1) 仅场所方面扩项时，必须核查标准6.6条款，其他条款根据该场所内涉的服务内容确定；

2) 仅人员方面扩项时，必须核查标准4.4、6.5条款，其他条款根据人员涉及的服务活动确定；

3) 仅业务种类扩项时，一般情况下按初次认证，应覆盖标准全部条款。

4) 若扩项时涉及上述 1）～3）中的 2 项或全部时，须进行叠加并综合考虑。

b) 变更地址：按照涉及地址变更的要求执行；

c) 变更名称：提供新法人执照、变更申请、体系变更申请表、更名后的方针文件、证书

制作单、注册审定批准表。项目部将资料审核后上报 NGV 审定部门。

结合监督按照监督资料提供、填写和审查，但须将扩项内容在审核计划、审核报告中体现。

5.7 远程审核特殊要求

如果拟使用远程审核技术（例如，交互式基于 web 的协作、web 会议、电话会议和/或组织过程的电子验证），可以考虑将其作为审核时间的一部分。不允许远程审核活动占据大于 30%的现场审核时间。

注：远程场所的电子审核被视为远程审核，即使电子审核在组织的物理场所进行。

5.8 现场审核活动特殊要求

5.8.1 当发现多服务点数量、类别等与任务通知和审核策划安排的不一致，且导致了审核组的专业能力或原定的人日数不能满足审核需求；现场确认委托服务相关资质证明有效性时，发现有问题且直接影响认证范围；客户申请填报的信息与实际有较大的差别且影响了审核的实施，如：审核范围、专业类别的判别、审核组专业能力、受审管理体系覆盖的实际人数等，导致原审核策划不能完成预期的审核；体系实际运行不足三个月、现场不能按预期的策划获取能够评价管理体系的客观证据等变更情况，审核组长应及时与项目管理人员沟通，获得解决办法。

5.8.2 审核时，对每个业务种类抽样要求：

a) 初次认证（再认证）审核时，业务种类不能抽样，每个业务种类过程亦不可以抽样；

b) 监督审核时，业务种类不能抽样，过程可以抽样。

5.9 认证决定特殊要求

5.9.1 总则

认证决定工作执行 NGV《管理体系认证决定管理规则》的要求，并同时满足以下要求：

根据申请评审时已识别的对特定的申请组织实施认证所需的能力，委派具备相应能力的认证决定人员完成认证评定。当了解到特定的获证组织的ITSMS已发生变化时（特别是在监督审核、再认证审核方案策划时），并已对原有的能力分析评价后进行更新，应按更新后的能力需求委派具备相应能力的认证决定人员完成认证评定，确保认证决定的有效性。

5.9.2 业务范围和边界的界定

ITSMS 认证范围宜基于服务方对其 ITSMS 范围的描述界定。ISO/IEC 20000-3 通过下列参数描述其 ITSMS 的范围：

提供服务的组织单元，例如单个部门、一组部门或所有部门；

所提供的服务，例如单个服务，一组服务或所有服务；或金融服务、零售服务、电子邮件服务

服务提供者交付服务的物理场所，例如单一办公场所、一组办公场所、区域的、全国的或全球的；

顾客及其地点，例如一个顾客、多个顾客、外部顾客或内部顾客；

服务提供所使用的技术。

5.9.3 组织 ITSMS 范围和边界的综合描述

范围和边界是相互渗透、紧密联系的。综合以上几方面的范围和边界后，组织 ITSMS 的范围和边界可从以下方面进行描述：

“位于 xxx 地理位置的 xx 楼 xx 层 XX 公司范围内的向外（或内）部客户提供 xxx 业务的服务相关的信息技术服务管理活动”。

例如：位于北京市海淀区 X 楼 12 层的 XX 公司范围内向外部客户提供网络运行维护、应用系统运行维护服务相关的信息技术服务管理活动。

例如：位于北京市海淀区 X 楼 12 层的 XX 公司的 IT 部门向内部客户提供网络运行维护、桌面支持服务相关的信息技术服务管理活动。

注：可行的服务类别：网络运维、服务器运维、基础设施运维、数据库运维、业务信息系统运维、应用软件运维、信息系统开发服务、软件开发服务、软件测试服务、桌面运维……

5.10 认证证书格式特殊要求

执行 NGV《管理体系认证证书内容表达规则及技术内容说明》。

5.11 暂停、撤销后恢复、或缩小范围审核特殊要求

对获证组织注册资格保持、暂停、撤销或缩小认证范围的管理执行 NGV《管理体系认证的批准、拒绝、保持、扩大、缩小、暂停、恢复和撤销的条件和管理规则》的要求。

5.11.1 发生以下情况（但不限于）时，NGV 应暂停获证客户的信息技术服务管理体系认证资格：

1）获证客户信息技术服务管理体系持续第或严重地不满足认证要求，包括对信息技术服务管理体系有效性要求。

2）获证客户不允许按要求的频次实施监督或再认证审核。

3）获证客户不接受或不配合认证认可监督管理部门的监督管理。

4）获证客户主动请求暂停。

5.11.1.1 认证资格暂停期最长不超过 6 个月。

5.11.1.2 在暂停认证期间，获证客户的信息技术服务管理体系认证证书暂时无效。

5.11.1.3 如果获证客户未能在 NGV 规定的时限内解决造成暂停认证的问题，NGV 将撤销其信息技术服务管理体系认证证书或缩小其相应的认证范围。

5.11.1.4 如果获证客户在认证范围的某些部分持续地或严重地不满足认证要求，NGV 将缩小其信息技术服务管理体系认证范围，以排除不满足的部分。认证范围的缩小应与认证标准的要求一致。

5.11.2 应根据暂停时间长短，在恢复审核时，由项目部适当增加人日数，并在审核任务单中明示告知审核组长。

另外，如果发现受审核组织不允许接触信息资产或无法满足受审核组织关于接触信息资产的相关要求时，CWM 在评估其对审核和认证的影响后可缩小认证范围或暂停或撤销注册资格。

5.11.3 在任何组织提出请求时，NGV 应正确说明获证客户的信息技术服务管理体系认证被暂停、撤销或缩小的情况。

5.12 对获证客户正确宣传认证结果的控制特殊要求

NGV 制作证书遵循 NGV《管理体系认证证书内容表达规则及技术内容说明》。在认证证书被暂停期间或撤消后，应收回相应的授权。

5.13 对获证客户的信息通报要求及响应的特殊要求

为确保获证客户的信息技术服务管理体系持续有效，NGV 要求获证客户填写《获证组织认证信息变更沟通单》，及时向 NGV 通报以下信息：

1）业务、地点、组织结构变化等情况的信息（及时通报）；

2）顾客投诉的相关信息（每三个月通报一次）；

3）认证客户的体系文件、服务目录信息的变化；

4）有严重信息技术服务事故的信息（及时通报）；

5）其他重要信息。（视情况）

附录 A　《信息技术服务管理体系审核技术要求》

A1　审核计划中的专业条款及必查条款安排

A1.1 完整审核（初审和再认证）

2005 版:
专业人员应实施对：5，6.3 ，6.5， 9.1 临时现场专业审核
认证范围内业务种类：全部覆盖
体系范围内部门：全部覆盖
每类业务过程均应覆盖：第 6、8、9 章

2011 版:
专业人员应实施对：5、6.3、6.5、9.1、9.2、软件维护 9.3；
认证范围内产品或行业：全部覆盖
体系范围内部门：全部覆盖
每类业务过程均应覆盖：第 6、8、9 章

A1.2 监督审核

证书有效期内，历次监督的叠加应覆盖获证组织所申请的管理体系标准要求的全部条款和管理体系范围内的所有部门；

2005 版:
必查部门：高层、体系主控部门、IT 服务实施部门、服务实施场所
必查条款： 3.1、4.3、4.4、5、6.1、6.2、6.3、7.2、7.3、8.2、9.2
证书有效期内，历次监督审核范围的叠加应覆盖获证组织所申请的管理体系标准要求的全部条款和管理体系范围内的所有部门；
认证范围的产品或行业：认证业务种类不能抽样，过程可以抽样。

2011 版:
必查部门：高层、体系主控部门、IT 服务实施部门、服务实施场所
必查条款：4.1；4.2；4.5.1；4.5.4；4.5.5；5；6.1；6.2；6.3；6.6；7.1；7.2；8.1；9.2；9.3
监督审核时，业务种类必须全部覆盖，其中每类业务过程必查条款：6.1，8.1，其他条款的安排应满足必查条款的要求。

A1.3 专项转版审核

1. 应覆盖所有认证范围内的产品；
2. 部门：
－高层、体系主控部门必查；
－可结合企业部门设置及职责进行安排，其必查条款如下：
4.1－管理职责；4.2－由其它方运行过程的治理；4.3.1－建立和维护文件；4.4.1－资源提供；4.5.1－定

义范围；4.5.3 f)和 g)－实施和运行服务管理体系；4.5.4－监视和评审服务管理体系；4.5.5－维护和改进服务管理体系；5.1－总要求；
6.1－服务级别管理；6.5－容量管理；9.1－配置管理；9.2-变更管理；9.3－发布与部署管理。
（除内审、管评外，其他条款可重点关注其变化的内容）

A1.4 其他要求

1. 再认证+转版的审核，应满足 A1.1 的审核要求，同时要重点关注新标准在企业的落实、实施情况；
2. 监督+转版的审核，应同时满足A1.2 和 A1.3 的要求。

A1.5 非常规审核

2005 版:
1、 仅场所方面扩项时，必须核查标准 6.6 条款，其他条款根据该场所内涉及的服务内容确定；
2、 仅人员方面扩项时，必须核查标准 3.3、6.5 条款，其他条款根据人员所涉及的服务活动确定；
3、 仅业务种类扩项时，一般情况下按初次认证，应覆盖标准全部条款；
4、 若扩项时涉及上述 1-3 中的 2 项或全部时，须进行叠加并综合考虑。

2011 版:
1、 仅场所方面扩项时，必须核查标准 6.6 条款，其他条款根据该场所内涉及的服务内容确定；
2、 仅人员方面扩项时，必须核查标准 4.4、6.5 条款，其他条款根据人员所涉及的服务活动确定；
3、 仅业务种类扩项时，一般情况下按初次认证，应覆盖标准全部条款。
4、 若扩项时涉及上述 1-3 中的 2 项或全部时，须进行叠加并综合考虑。

A2 第一阶段审核

第一阶段审核主要侧重于组织的策划过程，在制定审核计划是应按照下面要求进行策划，主要内容为：

●通过现场观察，了解组织的基本概况，包括受审核方的组织机构及职能，服务的流程和特点，服务的活动现场分布情况，服务提供过程中提供商，关键/特殊活动控制点设置情况等；
●通过收集有关 IT 服务方针、目标指标、重要 IT 服务管理活动过程，特别是关键特殊服务活动控制点以及为实现 IT 服务方针、目标指标、满足法律、法规要求、顾客要求等所制定的 IT 服务管理控制措施和管理程序等信息。了解受审核方 IT 服务管理体系的整体情况；
●对受审核方识别及评价重要 IT 服务管理活动过程，特别是关键/特殊 IT 服务活动控制点的程序的合理性、适用性以及控制措施的有效性作出初步评价；
●评价受审核方识别顾客信息、法律、法规程序的有效性，以及组织遵守法律、法规及标准的情况和满足顾客要求的情况；
●审核组织的 IT 服务管理体系内审程序、内审计划和各项内审记录，对受审核方的内审程序和内审实施的有效性时行评价；评价管理评审实施的情况及有效性，评价组织自我完善和持续改进机制；
●相关人员的 IT 服务意识是否具备；
●体系文件的建立是否完备，在办公室文件审查的基础上，在现场对程序及作业书进行补充审查，考察其完整性、协调性、可操作性及合理性；
●评价组织对外包方的识别管理情况；
●现场调查过程中，应关润在生产、服务和活动过程中控制点的场所：
服务点
关键过程
相关基础设施（环境、施施、设备、工具）
临时现场

分现场
特殊的人员要求
重要的分供方等

A3 第二阶段审核

第二阶段审核主要是判断受审核方的 IT 服务管理体系是否符合标准要求，能否有效实施组织的 IT 服务方针和目标指标；判断受审核方是否遵守了 IT 服务管理体系的各项控制程序，实施了对重要质量因素的控制，审核员现场实施审核时，应注意收集受审核方 IT 服务管理体系运行中的客观证据：

- IT 服务方针是否已得到贯彻实施；
- IT 服务目标、指标是否正在按规定的管理要求和计划进行；
- 重要的管理程序和相关要求是否已被严格遵守或执行；
- 体系中规定的日常监测和必要的外检是否已执行；
- 内审和管理评审等是否已按规定实施。

A4 监督审核

每次监督审核均应特别关注以下内容：

1、 IT 服务管理体系在实现组织的 IT 服务方针、目标方面的持续有效性；
2、 重要 IT 服务活动的变化及控制；
3、 内审及内审结论的跟踪；
4、 组织有关法律法规的变化及符合性的定期评价工作是否有效，是否及时向认证机构通报了违法行为；
5、 为实现整体服务绩效的改进，依据组织的 IT 服务方针对 IT 服务管理体系加以不断改进面采取的措施、计划等的进展情况；
6、 与相关方的信息交流，包括有关接收、记录及反应程序以及执行情况；
7、 上次审核中发现的不符合所采取纠正措施的现场验证；
8、 体系文件的修改与调整；
9、 体系范围的变更；
10、 认证证书、标志和报告的使用和宣传情况；
11、 顾客的投诉
12、 内部运行及监测情况
13、 最高管理层
14、 选定的其它审核内容。

A5 审核报告

A5.1 一阶段审核报告

- 文件符合性结论；
- 体系建立和运行的基本情况；
- IT 服务管理范围、过程、场所得必要信息；
- 组织机构和职责的合理性；
- 关键/重要 IT 服务活动的识别、评价和基本控制情况；
- 适用于组织的法律、法规以及顾客要求的获取和遵守情况；
- 方针、目标、指标和 IT 服务管理措施建立的合理性；
- 与 IT 服务管理体系相关的信息交流及相应措施记录；
- 必要的监控机制建立；
- 内审的可信性及持续改进机制建立；
- 管理评审的实施情况；
- 全员基本意识；

●是否具备二阶段审核的条件的结论。

A5.2 二阶段审核报告

审核报告应准确、简明和清晰地描述审核活动的主要内容，至少包括以下内容：
●服务活动识别、特别是重要/关键 IT 服务活动识别和管理的适当性；
●法律法规和其他要求识别和管理的充分性和遵守法律法规满足客户要求的情况；
●体系的实施情况，是否正确的实施和保持：包括方针、目标指标和管理要求的实施完成情况，重要 IT 服务活动是否都得到控制，各种程序文件和作业指导书的执行情况；
●内审和管理评审是否按程序规定执行。能否实现自我发现、自我纠正、自我完善的运行机制；
●受审核方 IT 服务管理体系实施的持续适宜性和有效性，包括服务改进等;
●审核发现的不符合项概述，以及实施完成纠正措施的要求；
●不符合项纠正措施有效性验证情况；
●受审核方的 IT 服务管理体系符合标准的情况。
●是否偏离审核计划的情况；
●审核的推荐性结论。

A5.3 监督审核报告

1、 IT 服务管理体系是否得到正确的实施和保持；
2、 IT 服务管理体系是否确保持续适用性和有效性；
3、 重要 IT 服务活动是否得到有效地控制；
4、 组织是否持续遵守相关法律法规及其它要求，有无申投诉情况；
5、 不符合项是否破坏体系的完整性、有效性，是否得到纠正；
6、 是否推荐保持认证证书或暂停，撤销认证证书；
7、 对下一次监督审核应关注的要点及需要重点抽查的要素提出线索和建议。

附录：标准结构的变化

2011		2005	
章节	主要内容	章节	主要内容
1	范围	1	介绍
2	标准参考文献	2	术语和定义
3	术语及定义	3	管理体系要求
4	服务管理体系要求	4	策划与实施服务管理
4.1	管理职责	4.1	策划服务管理
4.2	相关方流程及治理	4.2	实施服务管理并提供服务
4.3	文档管理	4.3	监控、度量和评审
4.4	资源管理	4.4	持续改进
4.5	建立和改进服务管理体系		
5	设计和转换新的或变更的服务	5	策划和实施新的或变更的服务
6	服务交付过程	6	服务交付过程
7	关系过程	7	关系过程
8	解决过程	8	解决过程
9	控制过程	9	控制过程
9.1	配置管理	9.1	配置管理
9.2	变更管理	9.2	变更管理
9.3	发布与部署管理		
		10	发布与部署管理