北京恩格威认证中心有限公司

信息安全管理体系认证专项管理规则

文件编号：NGV-GZ-001-2016

发布日期：2016 年 9 月 30 日

修订日期：2016 年 9 月 30 日

实施日期：2016 年 9 月 30 日

目　　录

信息安全管理体系认证专项管理规则

1 适用范围

为规范信息安全管理体系认证活动，制定本文件。该文件适用于恩格威认证有限公司（以下简称：NGV）信息安全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-CC170：2015 信息安全管理体系认证机构要求

2.2 CNAS-SC170：2017 信息安全管理体系认证机构认可方案

2.3 GB/T 22080-2016/ISO/IEC 27001：2013《信息技术 安全技术 信息安全管理体系 要求》

2.4 GB/T 28450-2012 《信息安全技术 信息安全管理体系审核指南》

2.5 《管理体系认证受理管理规则》

2.6《管理体系认证证书转换管理规则》

2.7《管理体系认证项目管理规则》

2.8《管理体系认证审核时间确定规则》

2.9《管理体系认证通用审核管理规则》

2.10《多场所审核管理规则》

2.11《管理体系认证决定管理规则》

2.12《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《管理体系认证受理管理规则》的要求执行。证书转换按《管理体系认证证书转换管理规则》要求执行。

3.1.2 受理条件特殊要求

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

b) 接受申请时，项目管理人员应要求客户组织向其说明适用的关于 ISMS 认证机构的资质、诚信守法记录或认证人员身份背景的要求，以及适用的与保守国家秘密或维护国家安全有关的法律法规要求，并即时更新该说明，以便 NGV 判断是否具备对该客户组织实施认证活动的资格或条件。

3.1.3 申请方提交资料特殊要求

a) 申请组织按照《恩格威认证申请书》要求提交申请资料时，项目管理人员与申请人确认所提交的资料是否包含申请组织保密性或敏感性信息。在不影响申请评审和文件审核的前提下，申请组织可以对提交资料进行相应的处理，删除其中的保密性或敏感性信息。

b) 申请方按《恩格威认证申请书》中“基本资料”与“信息安全管理体系认证补充资料”中所列内容要求提交相关资料。

c) 如：影响审核时间的因素：服务器数量/PC 机数量、外包方数量、网络情况。

d) 不同 IT 平台数量、申请方使用的信息系统状况等。

e) 申请方按“信息安全管理体系认证补充资料”应提交信息安全管理体系文件：如：信息安全方针、目标，信息安全风险评价准则、信息安全管理体系适用性声明、风险处置计划等。

f) 适用时，客户组织应在递交认证申请时指明不完全包含在 ITSMS 范围内的服务活动。例如，与其他组织共同提供服务的情况。

3.2 受理申请评审特殊要求

3.2.1 项目管理人员按照《管理体系认证受理管理规则》或《管理体系认证证书转换管理规则》的规定进行评审并填写《申请评审表》，以确保行业类别、风险等级、ISMS 认证范围确认准确。证书转换按照《管理体系认证证书转换管理规则》进行评审，填写相应的记录。

3.2.2 初审项目评审应重点关注的特殊要求

1) 当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，根据所受到的影响采取相应的措施（例如终止审核、缩小审核和认证的

范围等)。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/检查任务书》予以记载。

如果客户组织事先没有禁止NGV接触某一信息，但NGV在认证过程中发现自己并不具备接触该信息的资格和条件，需立即向客户组织提出。

2) 识别申请组织的行业类别、风险等级和与之对应的信息安全管理过程特性和服务要求。(当认证范围覆盖的服务 / 活动有资质、许可证要求时，应核查其相关的证明资料)

3) 掌握国家对该行业的信息安全管理体系认证的管理要求。

4) 组织根据业务、组织、位置、资产和技术等方面的特性，确定 ISMS 的范围和边界，包括对任何范围删减的详细说明和正当性理由（见组织提供的《适用性声明》)；应注意 ISMS 标准中的 4、5、6、7、8、9、10 章不得删减（只能删减附录 A 的某些不适用的条款）

注：①范围中要求写到楼层，“位于 XXX 市 XX 大厦 X 层的 XX 公司为电力系统提供 XX 解决方案的信息安全管理活动。适用性声明　V1.0”;

②范围中要求写上适用性声明及版本号;

③核对范围与适用性声明的一致性。

举例：如范围:“xxx 电力信息管理系统的设计和开发的信息安全管理活动。适用性声明 V1.0”,提供的《适用性声明 V1.0》中删减了 A14 系统获取、开发和维护，这是不可以的。

5) 解决了 NGV 与申请组织之间任何已知的理解差异，并做相应记录;

6) 根据申请组织的具体情况分析确定拟实施审核和认证所需的能力，NGV 有能力实施认证活动。

7) 对于信息安全管理体系，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。

8) 根据以上信息制定或组织相关人员制定认证项目审核方案，对特殊项目（指较多现场、多种/类产品、较多审核目的、同时涉及扩项/扩地址等复杂要求的认证项目）填写《特殊项目审核实施方案》，由合同评审人员、客户（适当时)、项目管理人员、或技术专家共同确定。

9） 保持了决定实施审核的理由的记录。

10）与客户签订认证服务合同书。并将该客户的报价单作为合同附件。或将报价单与认证服务合同书一同存档保留。作为认可有要求时的备查资料。

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） 申请认证覆盖的信息安全服务类别的变化；

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） 适用性声明及版本的变化；

7） 信息安全服务点的变化；

8） 资质、许可证的有效性。

其受理过程同初次认证受理过程。

4 认证项目管理特殊要求

按照 NGV《管理体系认证项目管理规则》执行，参考采用 GB/T 28450：2012 《信息安全技术 信息安全管理体系审核指南》，其为 ISMS 审核方案管理、审核实施提供了指南。

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《管理体系认证项目管理规则》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，由审核组长组织在现场确认，必要时根据审核组在现场确认的结果调整审核方案。

当受审核方组织由于信息技术/安全等原因在申请认证时无法提供足够的信息时，可考虑通过第一阶段审核在受审核方的现场补充对上述信息的确认。

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 审核时间的策划特殊要求

NGV 针对每个申请 ISMS 认证组织的初次审核（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《管理体系认证审核时间确定规则》进行。

对于扩项等特殊审核时间的策划，参照《管理体系认证审核时间确定规则》。

计算有效人数---确定基准审核时间---根据增减因素进行调整计算---根据多场所（含临时场所）策划抽样时间----结合审核（一体化）审核时间计算。

ISMS 可以和其他管理体系进行结合审核或一体化审核。策划结合审核时间时，考虑一体化的程度。

ISMS 体系审核时间增减因素：与业务和组织（非 IT）相关因数和与 IT 环境相关的因数。两种因数分别计算，并将计算结果代入《因数对审核时间的影响表》中，得出可调整的百分比。

需要调整审核时间时，策划人员应在方案策划表中记录增减的理由。

关于审核时间的计算方法等详见《管理体系认证审核时间确定规则》相关章节。

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安全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。

根据申请评审时已识别的特定的申请组织的具体情况，分析对其实施审核和认证所需的能力，委派具备相应能力的审核组实施审核。当了解到特定的获证组织的 ISMS 已发生变化时（特别是在监督审核、再认证审核方案策划时），审核方案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，确保审核的有效性。

举例：如申请方 XX 科技有限公司，认证范围：“xxx 电力信息管理系统的设计和开发的信息安全管理活动。适用性声明 V1.0”。

评审确认的专业类别：04.08，风险级别：二级。拟派审核组中至少有一名审核员应具有 04.08 专业。对于风险级别为二级，应派出具有技术领域为 A1、A2 的审核员。在审核员无此专业类别或技术领域时，应补充相应专业或技术领域的专家，对审核组提供技术支持。

注：对应风险级别为一级的组织，选派具有 A1 技术领域或具有评审确认的该专业中类的审核员，不能选派技术领域为 A2、A3 的审核员。反过来，对于具有三级风险的组织，

可以选派具有A1、A2、A3或具有评审确认的该专业中类的审核员（A1技术领域级别最高，可以向下兼容，依次类推）。

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2天且不多于60天的要求进行策划。

4.1.4.1.2 一阶段审核应在申请客户组织的现场进行，审核应策划以下的内容：

(1) 评价申请客户的运作场所和与重要信息资产有关的现场，如：提供过程中对资产的保密性、完整性及可用性要求，重要资产清单中所列资产的物理位置，现场观察在服务和活动过程中和ISMS直接相关的重要场所：

●信息安全管理管理体系推进部门；

●核心信息处理设施的放置场所，如核心机房等；

●IT部门，如信息系统的设计、开发及维护部门等。

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。

(2) 审查申请客户理解和实施信息安全管理体系标准要求的情况，包括信息安全方针、目标、适用性声明及版本；

(3) 了解组织环境下所进行的ISMS设计，风险评估和处置（包括所确定的控制）、关注风险评估的规程是否健全。

(4) 确认受审核方的ISMS范围和边界的界定是否清晰和充分。

(5) 审查申请客户是否系统而充分的识别与所提供的信息安全服务相关的法律法规和其他要求及其遵守情况；

(6) 审查第二阶段审核所需资源的配置情况；

(7) 结合申请客户信息安全管理体系方针和目标，了解其审核准备的状态，为策划第二阶段的审核提供重点；

(8) 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安全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安全管理体

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安全活动是相适应的。

审核组应要求申请客户证实其对信息安全管理过程的风险分析和组织运作实施了适当的信息安全控制措施。

4.1.4.1.4 信息安全管理体系文件与其他管理体系文件的整合

只要信息安全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安全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、信息技术服务管理体系等）相结合。

4.1.4.1.5 管理体系结合审核

信息安全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安全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安全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 监督审核频次策划特殊要求

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。

在满足认可要求的基础上，根据获证组织信息安全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。当获证组织信息安全管理体系发生重大变更，或发生重大泄密问题、服务质量事故、客户投诉等情况时，应视情况可增加监督的频次。由于获证组织业务运作的时间(季节)特点如有限时段（例如：临时服务场所）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安全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）适用性声明及版本的变化情况；

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）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 应作出保持其信息安全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 再认证审核策划特殊要求

4.1.4.4.1 再认证应考虑信息安全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 当获证客户的信息安全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，以提供对信息安全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。

4.1.4.6 选择和指派审核组特殊要求

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安全管理体系认证注册资格。审核组由取得资格的人员组成，其中至少一名专职审核员。

根据实现审核目标所需的能力来选择和任命审核组（包括审核组长），并使客户知晓。应确保他们是经过 NGV 的审核能力和专业能力评定、有能力完成本次审核任务的人员。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。决定审核组的规模和组成时，应考虑下列因素：

a) 应具备了拟认证范围所涉及的信息技术和信息安全技术知识、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、涉及有关覆盖过程及其管理、信息安全审计、配置管理等过程涉及使用的特定软件工具。熟悉特定行业典型的信息资产及其类型、典型信息安全特性等。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。

b) 审核组应由取得信息安全管理体系认证注册资格的审核员组成，其中至少有一名专职审核员。必要时可以补充技术专家以增强审核组的技术能力。确保审核组整体上具备被审核领域足够的认识和经验。

c) 审核组能识别相应专业受审核方管理体系中的关键活动（如信息安全管理体系中的主要威胁、重大风险，并有能力将受审核方 ISMS 中的安全事件迹象追溯到 ISMS 的相应要素等），并对关键活动控制的有效性能做出恰当的评价。对组织关键部门或活动进行审核时，应有相应专业资格的审核员实施审核或在技术专家的支持下实施；

d) 熟悉有关和（或）相关的 ISMS 标准、行业先进经验、（ISMS）安全策略和规程，并能验证受审核方管理体系确已明确承诺遵守相应法规及有关强制性规定要求，及确保符合这些规定要求的证据；

e) 熟悉信息资产及其风险的识别、风险评价、风险控制等知识；

f) ISMS 有效性的评审和控制措施有效性测量方面的知识，业务连续性的相关知识等；

g) 当审核组审核一个主要依赖电子化过程与文件的组织的管理体系时，审核组需具备相应的电子化文件的审核能力，如远程审核工具运用、计算机辅助审核技术（如采用电话会议，网络会议，基于网络的交互式通讯以及远程访问相应管理体系文件和（或）管理体系过程）的能力。

当为特定认证审核选择审核组时，应确保每次委派时审核组的能力是适宜的，审核组应：

h) 对拟认证 ISMS 范围内的特定活动具备适当的技术知识，以及相关时，对这些活动的相关规程和其潜在信息安全风险具备适当的技术知识（技术专家可以履行此项职责）；

i） 理解客户，足以基于客户 ISMS 范围和组织环境对 ISMS（该体系管理着客户活动、产品和服务的信息安全）进行可靠的认证审核；

j） 适当地理解适用于客户 ISMS 的法律法规要求。

注：适当地理解法规要求不意味着要有深厚的法律背景。

4.1.4.7 多场所审核策划特殊要求

多地点抽样时，应关注现场业务活动的差异性。

4.1.4.7.1 当客户拥有满足以下 a)至 c)的多个场所时，则使用基于抽样的方法进行多场所认证审核：

所有场所在同一 ISMS 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 ISMS 中每个有重大信息安全风险的场所；

b）无论在其中心职能机构（总部）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。

4.1.4.7.2 抽样按照 NGV《多场所审核管理规则》的通用要求，以及考虑以下特殊要求：

a)在初次的合同评审和项目策划时，最大程度地识别场所之间的差异，以便确定适宜的抽样水平；

b）结合以下因素，策划抽取具有代表性的场所：

1） 总部及其他场所的内部审核的结果；

2） 管理评审的结果；

3） 场所规模的差异；

4） 各场所业务目的的差异；

5） 不同场所的信息系统的复杂程度；

6） 工作实践的差异；

7） 所实施的活动的差异；

8） 控制的设计与运行的差异

9） 与关键的信息系统或处理敏感信息的信息系统之间的潜在交互；

10） 任何不同的法律要求；

11） 地域和文化因素；

12） 场所的风险状况；

13） 发生在特定场所的信息安全事件。

c）从客户ISMS范围内的所有场所中选择具有代表性的样本，该选择应基于一个可体现上述b)中所列因素的判定，同时也考虑随机因素；

d）在授予认证之前，审定确认审核了ISMS中每个具有重大风险的场所；

e）根据上述要求策划审核方案，且审核方案要在三年内覆盖ISMS认证范围内的代表性样本；

f)无论是总部还是单个场所发现不符合，纠正措施规程的实施适用于包括在认证范围内的总部和所有场所。

审核应关注客户总部为确保一个ISMS运用于所有场所并在运行层面上实施统一管理所进行的活动。审核应关注上述所有事项。

4.2 审核任务下达特殊要求

4.2.1 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。第一阶段与第二阶段现场审核间隔应不少于 2 个工作日且不多于 60 个工作日。第一阶段审核应进入受审核方的现场进行审核。

5 审核实施特殊要求

审核按照审核计划执行。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。

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时，由审核组长完成受审核方的文审及准备，包括：

a. 查阅并熟悉 ISMS 标准条款的要求；

b. 阅读受审核方提交的 ISMS 方针文件、ISMS 的范围、风险评估方法的描述、风险评估报告、风险处理计划、适用性声明、支持 ISMS 的过程和控制措施及其它 ISMS 标准要求的信息，了解受审核方信息安全管理体系覆盖范围内信息安全事项、风险评估、风险管理、业务领域及与信息安全管理体系适用的法律法规要求；

c. 按分工编制检查表，检查表应体现受审核方文件要求和/或具有专业特点的检查项目，审核组长审定。

5.1.2 文件评审要求

1） 信息安全管理体系文审重点：

a） 标准中所要求的建立文件化的 ISMS 是否完整；

b） ISMS 文件层次、结构及相互关系是否清晰；

c） 是否明确 ISMS 各个职能与层次的组织机构与职责；

d） 风险评估的方法是否合理？如何进行风险评估与风险管理？及其有效性及充分性；

e） 适用性声明中控制措施的选择及删减理由描述是否充分合理；

f） 方针和目标、风险处置计划、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；

g） 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。

5.2 审核计划要求

5.2.1 制定审核计划总体上应：

a） 审核范围与合同评审及审核任务通知书中范围一致；

b） 审核计划覆盖审核任务书中的审核时间、人日数、审核员；

c） 审核的条款按照专业类别及技术领域能力安排审核员：

d） ISMS 审核计划应考虑所确定的信息安全控制措施。

1） 如下条款及主控部门需具备专业类别的审核员实施审核：6、8、A.8(主业务部门的)、A18.2.1。

2） 如下条款需相应技术领域能力的审核员实施审核：A9.4、A10.1、A12.2、A12.6、A13、A14.2、A17.1、A18.2.3。涉及信息安全技术管理部门、技术实施部门、管理体系推进部门， 如：计算机管理部门、网管、系统维护部。

5.2.2 应关注初次审核、监督审核、再注册及特殊项目审核时的要求。

5.2.3 多地点抽样时，应关注现场业务活动的差异性，考虑使用基于抽样的方法进行多场所认证审核，计划策划原则参见 4.1.4.7 多场所审核策划特殊要求。

5.2.4 区域的表述应具体到单元（楼层，门牌号），不应笼统进行描述。

5.2.5 网络支持审核技术

如适宜，审核计划应识别在审核中使用的网络支持的审核技术。

注：网络支持的审核技术可包括：例如，电话会议、网络会议、基于网络的交互式通信和远程电子访问 ISMS 文件和（或）ISMS 过程。对这些技术的关注，将提高审核的有效性和效率，并支持审核过程的完整性。

5.3 初次审核特殊要求

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 NGV 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，信息安全服务的流程和特点、活动的现场分布情况，提供过程中对资产的保密性、完整性及可用性要求，重要资产清单中所列资产的物理位置。

应关注在服务和活动过程中和 ISMS 直接相关的重要场所：

- 信息安全管理管理体系推进部门；
- 核心信息处理设施的放置场所，如核心机房等；
- IT 部门，如信息系统的设计、开发及维护部门；
- 与重要信息资产有关的现场。

b） 获取有关 ISMS 设计文件，包括 GB/T 22080-2016/ISO/IEC 27001：2013 所要求的文件。

c） 充分了解组织环境下所进行的 ISMS 设计，风险评估和处置（包括所确定的控制）、关注风险评估的规程是否健全。信息安全方针、目标、适用性声明。以及客户的审核准备情况。并让客户知晓第二阶段可以要求对更进一步的信息和记录做详细检查。

d） 确认受审核方的 ISMS 范围和边界的界定是否清晰和充分。

e） 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） 组织机构和安全职责的合理性；

4） 风险评估、风险管理方法策划的合理性及充分性；

5） 适用于组织的 ISMS 法律、法规及合同要求的识别、获取和遵守情况；

6） 目标、指标策划的合理性；

7） 组织内审与管理评审的实施状况；

8） ISMS 确认的二阶段审核的范围；

9） 体系能否进入二阶段审核的结论。

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GB/T 22080-2016 /ISO/IEC 27001：2013要求的文件；

(2) 确认客户遵守自身的方针、策略和规程；

(3) 最高管理者的领导力和对信息安全方针、目标的承诺；

(4) 评估与信息安全有关的风险，以及评估可产生一致的、有效的、在重复评估时可比较的结果；

(5) 基于风险评估和风险处置过程，确定控制目标和控制；

(6) 信息安全绩效和ISMS有效性，以及根据信息安全目标对其进行评审；

(7) 所制确定的控制、适用性声明、风险评估和风险处置过程的、信息安全方针 、信息安全目标之间的一致性；

(8) 控制的实施（控制措施），考虑了外部环境、内部环境与相关的风险，以及组织对信息安全过程及控制措施的监视、测量与分析，以确定控制是否得以实施，有效并达到其所规定的目标；

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

(10) 审核ISMS中每个具有重大风险的场所。

5.3.2.2 确认认证范围

审核组确认受审核方在其 ISMS 范围内满足了 GB/T 22080-2016/ISO/IEC27001:2013 中 4.3 的要求。

审核组按照 ISMS 标准 GB/T 22080-2016/ISO/IEC 27001:2013 的要求，确认受审核方的信息安全风险评估和风险处置与客户组织的活动及活动的边界相一致，并确认这些都在受审核方的 ISMS 范围和适用性声明中得到体现。

审核组确认与不完全属于 ISMS 范围内的服务或活动的接口已在接受认证的 ISMS 中得到说明，并已包括在受审核方的信息安全风险评估中，例如，与其他机构共享设施的情况（信息技术系统、数据库和通讯系统等）。

认证范围举例说明：

位于北京市海淀区 XXX 大街 X 大厦 X 层的 X 公司电力行业应用软件系统运维服务相关的信息安全管理活动。适用性声明：V 1.0

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) 没有安全方针；

b) 没有安全事件管理系统；

c) 缺乏业务持续性计划；

d) 没有正式的系统来管理和更新 ISMS 文件；

e) 体系、控制措施，或程序的完全失效；

f) 极高数量的不符合项集中在标准中某一要素或是部门；

g) 未经批准的实行 ISMS 的变更；

h) 严重违背法律法规要求，后果较严重；

i) 相关方的严重投诉；

j) 上次发现的一般不符合重复发生等。

2. 一般不符合

在一个隔离的环境中有一些适用控制措施的要求没有被满足，因此产生一些关于对敏感信息的保密性、完整性和可用性测量的适当的质疑。和/或表示一个轻微的风险，可能将被组织的利害关系人觉察到。

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) 观察到的未遵守清空桌面和屏幕策略；

b) 在某种场合中访客离开场所时未登记；

现场发现某天未按照备份策略进行备份。

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，还应提供以下信息或对这些信息的引用：

(1) 审核说明，其中包括了文件评审摘要；

(2) 对客户信息安全风险分析进行认证审核的说明；

(3) 与审核计划的偏离（如：某一预定的活动上花费更多或更少的时间；

(4) ISMS范围；

(5) 所采用的主要审核路线和所使用的审核方法；

(6) 形成的观察结果，包括正面的（例如，值得注意的特征）和负面的（例如，潜在的不符合）；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）；

(7) 对客户ISMS与认证要求的符合性的评价意见、对不符合的清楚说明、所引用的适用性声明的版本，以及适用时，与客户以往认证审核结果的任何有用的对照。

完成的问卷、检查清单等可以构成完整的审核报告的一部分。如果使用这些方法，这些文件应作为支持认证决定的证据提供给NGV审定部门。在审核过程中，有关被评价的样本的信息应包含在审核报告。

对ISMS内部审核和管理评审的信任程度的评价；

关于ISMS要求和信息安全控制的实施与有效性的、最重要的观察（正面、负面）摘要；

审核组的推荐意见。

5.4 监督审核特殊要求

监督审核方案关注以下内容：

1） ISMS 管理体系保持要素，如：信息安全风险评估与控制维护、内审、管理评审、和纠正措施。

2） 根据 ISMS 标准 GB/T 22080-2016/ISO/IEC 27001：2013 和认证所需的其他文件要求，与来自外部各方沟通；

3） 文件化管理体系的变更；

4） 发生变更的区域；

5） 所选择的 GB/T 22080-2016/ISO/IEC 27001：2013 的要求；

6） 适宜时，其他所选则的区域。

每一次监督至少审查以下方面：

a) 监督审核可采用抽样的方式进行。对各部门、相同的现场的抽样须三年内全部覆盖。ISMS 的推进部门及重要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，其中每年对其总部的审核应至少一次。

b) 每次监督审核必查标准附录 A 条款：A6.1,A.8.1、A.10.1、A.11.1、A.16.1、 A.17.1、A.18.1 为监督必审；

A.9、A.12、A.13、A.14 每次要抽查，三年覆盖此 4 个条款的全部内容。

主业务部门、主实施部门、体系推进部门必须审核；其他条款三年覆盖一遍。

c) 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，应考虑不符合项性质的升级。

d) ISMS 在实现客户信息安全方针的目标方面的有效性；

e) 与相关信息安全法律法规的符合性进行定期评价与评审的规程的运行情况；

f) 所确定的控制的变更，及其引起的 SoA 的变更；

g) 控制的实施和有效性（根据审核方案来审查）。

h) NGV 针对与信息安全问题相关的风险及其对客户的影响来调整监督方案，并说明监督方案的合理性。

i) 在监督审核过程中，NGV 检查客户提交给认证机构的申诉和投诉记录，并且在发现任何不符合或不满足认证要求时，还应检查客户是否对其自身的 ISMS 和规程进行了调查并采取了适当的纠正措施。

j) 特别是，监督报告应包括有关消除以往出现的不符合、SoA 版本和从上次审核之后发生的重大变更的信息。监督审核报告应至少完全覆盖本文件的 5．4 的要求。

5.5 再认证审核特殊要求

再认证的审核内容应结合初次认证注册审核第一阶段和第二阶段的审核内容，应考虑三年的审核的结果，评价信息安全管理体系绩效并至少包括 ISMS 文件的审核和所有认证范围的现场审核；还应检查组织投诉、申诉及其所采取的纠正措施记录，至少应确保组织：

a. ISMS 的所有要素之间统一协调；

b. 发生变更后，ISMS 运行良好；

c. ISMS 得到有效的保持。

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4.3、6.1、6.2、7.5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7.2、7.3、7.4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复审要求执行；

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、适用性声明、证书制作单、注册审定批准表。项目部将资料审核后上报审定。

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 当发现多信息安全服务点数量、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。

5.9.1.1 认证决定应基于审核报告中审核组对客户 ISMS 是否通过认证的建议。

通常情况下，对授予认证做出决定的人员或委员会不宜推翻审核组的负面建议。如果发生这种情况，NGV 应记录其作出推翻建议的决定的依据，并说明其合理性。 只有具备充分的证据证实管理评审和 ISMS 内部审核的安排已经实施，且是有效的并将得到保持，才可向客户授予认证。

5.9.2 业务范围和边界的界定

应根据其业务、组织、技术、物理和资产的特性充分、清晰地界定了其 ISMS 的范围和边界。受审核组织的信息安全风险评估和风险处置与其 ISMS 的范围和边界一致，并在其适用性声明中得到体现；与不完全属于客户组织 ISMS 范围内的服务或活动的接口已得到说明，并已包括在客户组织的信息安全风险评估中，例如：与其他供方共享设施的情况（信息技术系统、数据库和通讯系统等）。

5.9.2.1 业务范围和边界的界定

业务范围和边界主要包括关键业务及业务特性描述（业务、服务、资产和每一个资产的责任范围和边界等的说明）。一般从其从事的业务流程进行描述，如软件开发、系统集成等。如果客户组织只是选择其部分业务流程进入到ISMS 范围，则必须确保被选择的业务流程所涉及的所有资产均已在风险评估中予以考虑，对于ISMS 范围内的业务流程与范围之外的业务流程共用的资产和技术，要识别其可能产生的风险及相应的控制措施需求。

5.9.2.2 组织范围和边界的界定

组织范围和边界一般可以通过ISMS 范围内的职能部门、过程、组织结构来界定。对于没有纳入到组织ISMS 范围内的职能和部门，客户组织应提供将其排除在外的适当理由。在界定组织范围和边界时，可考虑以下因素：

(1) 在确定组织范围和边界时需考虑组织 ISMS 的PDCA 管理的完整性，确保组织ISMS的PDCA 管理所涉及的所有职能和部门均已纳入管理体系范围。如某客户织申请认证的业务范围是软件开发，则覆盖的组织范围和边界除了软件开发业务职能部门外，其它如涉及该业务的ISMS 策划部门、监控和持续改进职能部门也应纳入到其ISMS范围；

(2) 信息安全管理委员会/管理机构应包括与 ISMS直接相关的管理人员；

(3) 对 ISMS负责的管理层人员应是对所覆盖的所有职责领域负有最终责任的人员（即他们的角色通常是由其在组织中的控制力和职责的范围所决定的）；

(4) 如果负责管理 ISMS的不是最高管理者，则有必要让一名来自最高管理层的人员作为信息安全的代表，并代表最高层对ISMS进行管理；

(5) 组织范围和边界的界定方式需要使所有相关资产均被纳入风险评估的考虑之中以识别其风险控制需求。对于组织ISMS范围内的职能部门与体系范围外的职能部门共用的资产与技术，要识别其可能产生的风险及相应的控制措施需求。

基于以上考虑，在界定组织的边界时，应识别ISMS所影响的所有人员，并将其包括在组织的范围内。人员的识别可以与过程和（或）职能部门联系起来。如果组织范围内的某些过程被外包给第三方，则这些依赖关系应清晰地形成文件。

5.9.2.3 确定物理范围和边界

物理范围和边界一般根据组织业务运营实际使用并控制的地理位置，包括建筑物、场所或设施进行界定。

对于跨越物理边界的信息系统，客户组织在确定物理范围和边界时宜考虑以下因素：

(1) 远程设备；

(2) 通过顾客的信息系统以及第三方所提供的服务的接口；

(3) 适用时，适当的接口和服务级别。

考虑以上因素，物理范围和边界的描述一般可包括以下适用的方面：

(1) 结合职能部门或过程的物理位置以及组织对其的控制程度，对职能部门或流程进行描述；

(2) 在组织信息通信技术边界内的储存或包含信息通信技术硬件或 ISMS范围内的数据（如在备份磁带上）的专用设施。

如果这些内容不是由组织自己控制，则应将与第三方之间的依从关系形成文件。在确定客户组织审核范围时可考虑其临时场所和异地备份地点的情况。对临时场所一般可到现场进行审核，但如能同时满足以下条件则可考虑采用其它非现场方式取证：

(1) 客户组织的客户有充分合适的理由(例如：客户组织提供的系统集成或服务项目涉及客户机密信息或项目实施地址距离客户组织较远)；

(2) 客户组织已对临时现场风险进行评估并且该残余风险是可接受的，不是重大风险；

(3) 客户组织已经采取措施对临时现场信息安全风险进行监控或定期检查；

(4) 审核员确认通过上述方法客户组织的信息安全风险可以得到控制。

(5) 如果组织内有建筑物、场所或设施没有纳入到ISMS范围内的，客户组织应说明其排除在外的适当理由。

5.9.2.4 确定资产范围和边界

资产范围和边界的确定一般可根据确定的客户组织的业务、组织和物理边界进行确

定。在确定客户组织的资产范围和边界时，宜考虑以下因素：

(1) 资产范围包括：软件资产、硬件资产、数据资产、人员资产、服务资产、和其他资产（如客户关系）等方面；

(2) 客户组织 ISMS范围内的业务流程、组织与职能、物理范围内的所有资产均宜纳入组织信息安全风险评估范围。

5.9.2.5 确定技术范围和边界

技术范围和边界主要是指客户组织所使用的信息技术和信息安全技术的范围和边界，一般可以通过识别组织使用的信息系统的方法进行确定。组织为支持其业务运作而进行的存储、处理或传输关键信息的各类信息系统一般应纳入组织ISMS范围。组织信息系统可能跨越组织边界甚至国界，在这种情况下，确定组织信息系统的范围应考虑以下因素：

(1) 社会文化环境；

(2) 适用的法律法规及合同要求；

(3) 对关键职责的责任；

(4) 技术约束（如：可用的带宽、服务的可用性等）。

在考虑到以上因素后，适用时组织技术范围和边界的确定应包括以下描述：

(1) 组织负有管理职责的包含不同技术（例如无线、有线或数据/语音网络）的通信设施；

(2) 组织边界内的被组织控制和使用的软件；

(3) 网络、应用或生产系统所要求的信息通信技术硬件；

(4) 与信息通信技术硬件、网络和软件有关的角色和职责。

当上述内容不是由组织自行控制时，受审核组织应在文件中清晰界定对第三方的依从关系。对于任何由组织所管理的、但被排除在ISMS范围之外的信息通信技术，应提供排除的理由。

5.9.2.6 组织 ISMS 范围和边界的综合描述

以上五个方面的范围和边界是相互渗透、紧密联系的。综合以上五个方面的范围和边界后，组织 ISMS 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 名称提供 xxx 业务的信息安全管理活动。适用性声明 版本”。

5.9.3 在多场所客户的审核中，关注在授予认证之前，审定确认审核了 ISMS 中每个具有重大风险的场所；

无论是总部还是单个场所发现不符合，纠正措施规程的实施适用于包括在认证范围内

的总部和所有场所。

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 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。

5.11.2 在任何组织提出请求时，NGV 应正确说明获证客户的信息安全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安全管理体系持续有效，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；

2）顾客投诉的相关信息；

3）认证客户的体系文件、适用性声明及版本的变化；

4）有严重信息安全泄密事故的信息；

5）其他重要信息。（视情况）