CNAS-SC170

信息安全管理体系认证机构认可方案

Accreditation Scheme for ISMS Certification Bodies

中国合格评定国家认可委员会

2017 年 01 月 01 日 发布　　2023 年 02 月 24 日第二次修订　　2020 年 11 月 30 日 实施

目 次

前 言

本文件由中国合格评定国家认可委员会（CNAS）制定。

本文件是CNAS对信息安全管理体系（ISMS）认证机构提出的特定要求和指南，并与相关认可规则和认可准则共同用于CNAS对ISMS认证机构的认可。

本文件中，用术语“应”表示相应条款是强制性的，用术语“宜”表示建议。

本文件代替了 CNAS-SC170:2015。

信息安全管理体系认证机构认可方案

1 范围

1.1 为确保 CNAS 对实施 ISO/IEC 27001 认证的信息安全管理体系（以下称为“ISMS”）认证机构实施评审和认可的一致性，指导申请和获得认可的 ISMS 认证机构理解和实施认可规范要求，特制定本文件。

1.2 本文件包括对信息安全管理体系认证机构认可规范的补充说明和指南，适用于 CNAS 对 ISMS 认证机构的认可。

本文件 R 部分和 C 部分分别是对相关认可规则和认可准则的补充和说明。本文件 G 部分是对相关认可准则的应用指南。

2 规范性引用文件

下列文件中的条款通过本文件的引用而成为本文件的条款。以下引用的文件，注明日期的，仅引用的版本适用；未注明日期的，引用文件的最新版本（包括任何修订）适用。

CNAS-RC01《认证机构认可规则》

CNAS-CC01《管理体系认证机构要求》

CNAS-CC170《信息安全管理体系认证机构要求》

CNAS-CC11《基于抽样的多场所认证》

CNAS-CC12《已认可的管理体系认证的转换》

ISO/IEC 27007 《信息技术 安全技术 信息安全管理体系审核指南》

3 术语和定义

GB/T 19000、GB/T 27000 和 CNAS-CC01 中的术语和定义以及下列术语和定义适用于本文件。

3.1 认证业务范围：认证机构的 ISMS 认证活动涉及的行业领域

注：认证业务范围的分类与分级见附录 A，包括“政务”、“公共”、“商务”、“产品的生产”四个大类，每个大类包含若干中类，每个中类被赋予“一”、“二”或“三”级别（认可风险水平由高至低）。附录 A 介绍了认证业务范围分类与分级的相关考虑。

注：对于 ISMS，技术领域与信息安全控制措施所涉及的信息安全技术、信息技术及业务活动的类别有关。

3.2 专业能力：能够应用特定技术领域的知识实现预期结果的本领

4 ISMS 认证机构认可规范的构成

4.1 CNAS-RC01《认证机构认可规则》是 ISMS 认证机构认可活动的基本程序规则。

CNAS-CC01《管理体系认证机构要求》是 ISMS 认证机构的基本认可准则。

CNAS-CC170《信息安全管理体系认证机构要求》是 ISMS 认证机构的专用认可准则。

4.2 其他适用的认可规则包括：

a) CNAS-R01《认可标识使用和认可状态声明规则》；

b) CNAS-R02《公正性和保密规则》；

c) CNAS-R03《申诉、投诉和争议处理规则》；

d) CNAS-RC02《认证机构认可资格处理规则》；

e) CNAS-RC03《认证机构信息通报规则》；

f) CNAS-RC04《认证机构认可收费管理规则》；

g) CNAS-RC05《多场所认证机构认可规则》；

h) CNAS-RC07《具有境外场所的认证机构认可规则》。

4.3 其他适用的认可准则包括：

a) CNAS-CC11《基于抽样的多场所认证》；

b) CNAS-CC12《已认可的管理体系认证的转换》；

c) CNAS-CC14《信息和通信技术（ICT）在审核中应用》；

d) CNAS-CC106《CNAS-CC01 在一体化管理体系审核中的应用》。

R 部分

R.1 认可申请

申请方应提供 CNAS-RC01 条款 5.1.2 规定的申请文件以及下列文件和信息：

1） 已审核过的客户（对应到附录 A 的相应中类）；

2） 自申请时间起 6 个月内计划实施的审核（对应到附录 A 的相应中类）；

3） 本机构确保客户符合工信部联协[2010]394 号文《关于加强信息安全管理体系认证安全管理的通知》的要求以及有关主管部门/监管部门对信息安全管理体系认证的管理要求的措施；

4） 需要时，CNAS 要求的其他信息。

R.2 预访问

必要时，CNAS 可在受理申请过程中安排预访问，以了解申请方是否已满足认可申请条件以及是否基本具备接受认可评审的条件。

R.3 初次认可的见证评审

CNAS 结合申请方 ISMS 认证活动的范围、规模和风险水平确定初次认可的见证评

审安排。

R.4 认证业务范围的认可

R.4.1 CNAS 按附录 A 的大类进行认可，必要时可将认可范围限定到中类。CNAS 认可某一大类的基本要求是认证机构的能力分析和评价系统覆盖了该大类，且系统运行基本有效。为此，认证机构应满足以下条件：

a) 对该大类和认证活动涉及到的中类进行了适宜、有效的能力需求分析；

b) 根据该大类和相关中类的能力需求分析，以适宜、有效的方式确定了能力分析和评价系统的相关组成部分（例如技术领域、能力准则等）；

c) 能力分析和评价系统在与相关中类有关的认证活动中有效地发挥了作用。

CNAS 按申请认可的每个大类评价认证机构是否满足以上条件。如果认证机构在一个大类中的多个中类实施了认证，CNAS 可采用抽样的方式优先选取风险级别高的中类进行评价，并实施见证评审。

R.4.2 CNAS 对 ISMS 认证机构认证业务范围的认可不包括中华人民共和国境内（不含香港、澳门特别行政区，台湾地区）的各级政府机关、政府信息系统运行单位和涉密信息系统建设使用单位，并在认可证书附件中做相应说明。

R.4.3 认证机构应确保运用能力分析和评价系统为该大类的每次认证活动配备所需的全部能力，同时确保客户符合工信部联协[2010]394 号文《关于加强信息安全管理体系认证安全管理的通知》的要求以及有关主管部门/监管部门对信息安全管理体系认证的管理要求。只有在满足这些条件之后，认证机构才可实施认证活动和颁发带有 CNAS 认可标识的认证证书。此外，对于一级风险的中类，认证机构还应在该大类中某个一级风险的中类已通过了 CNAS 的见证评审之后，才可以在认证证书上施加 CNAS 认可标识。

R.4.4 CNAS 在认可某一大类后，将在后续监督中对认证机构在该大类下自我评价和配备认证能力的情况进行评审（包括在见证时优先选取风险等级高的中类），并依据相关认可规范对发现的不符合进行处理（包括依据 CNAS-RC02 暂停或撤销部分或全部认可范围）。

R.5 其他

R.5.1 CNAS 对 ISMS 认证机构认可标识的管理遵循 CNAS-R01《认可标识使用和认可状态声明规则》的相关要求。

R.5.2 CNAS-RC03 条款 5.2 中“获证组织发生重大事故/事件”是指获得 ISMS 认证的组织发生具有下列影响的信息安全破坏：

a) 已经或可能严重损害国家安全、社会秩序、公共利益或获证组织及其相关方的合法权益；或者

b) 可能损害颁证机构或 CNAS 的公信力、声誉，或使颁证机构或 CNAS 承担连带责任。

发生上述情况时，颁证机构应及时采取相应措施并向 CNAS 通报相关情况。

R.5.3 如果 CNAS 可能需要在评审中接触认证机构的客户的相关信息资产，认证机构应向相关组织询问是否同意 CNAS 接触这些信息资产。如果组织同意，认证机构应识别 CNAS 接触这些信息资产时须满足的所有要求，并告知 CNAS。如果组织不同意或 CNAS 无法满足相关要求，CNAS 将根据评审所受的影响采取相应的措施。

C 部分

C.1 认证协议（CNAS-CC01 条款 5.1.2）

认证协议应就控制审核和认证活动引发的客户信息安全风险做出规定，包括明确认证机构和客户及其有关人员的责任与义务。

C.2 风险评估和责任安排（CNAS-CC01 条款 5.3.1）

认证机构应对其审核和认证活动可能给客户的信息安全带来的风险以及认证机构可能承担的责任进行评估，并做出充分的安排（例如购买职业责任保险或设立储备金）。

C.3 ISMS 认证证书（CNAS-CC01 条款 8.2.2、CNAS-CC170 条款 8.2.1）

C.3.1 认证机构宜在 ISMS 认证证书中从客户的业务、组织结构、位置和技术特点等方面清晰地界定认证所覆盖的 ISMS 范围。如果由于客户的信息安全的原因不能在认证证书上明示上述全部与客户 ISMS 范围相关的信息时，通过在认证证书上引用客户的适用性声明的方式是一种可以采取的间接方式。

C.4 保密（CNAS-CC01 条款 8.4、CNAS-CC170 条款 8.4.1）

C.4.1 在认证审核前，认证机构应要求客户识别并向认证机构告知其 ISMS 范围内的哪些信息资产不允许认证机构接触，或者认证机构在接触相关信息资产时应满足哪些要求，包括法律要求、相关方的要求和客户自身的要求。认证机构应满足所有这些要求，否则不应在认证活动中接触客户的相关信息资产。

如果认证机构因为未获得客户的允许或无法满足适用的要求而不能接触相关信息资产，那么认证机构应对审核和认证所受到的影响进行评估并采取相应的措施（例如终止审核、缩小审核和认证的范围等）。

如果客户事先没有禁止认证机构接触某一信息资产，或未告知认证机构应满足的要求，但认证机构在认证过程中发现自己并不具备接触该信息资产的资格和条件，应立即向客户提出。

C.4.2 认证机构应与其 ISMS 认证相关人员签订在法律上具有强制实施力的协议，以确保认证相关人员对审核和认证过程中接触到的客户的保密或敏感信息予以保密。认证机构还宜要求直接接触客户信息的认证人员（例如审核组成员）按照客户的保密要求与客户签署保密协议，或向客户做出保密承诺。

C.4.3 认证机构宜对其 ISMS 认证人员进行保密意识教育，并进行保密方面的法律法

规、标准、规章制度、知识技能的培训。

C.4.4 审核组成员不宜在审核过程中以任何方式记录受审核客户的保密或敏感信息。审核组在离开受审核客户前，宜请受审核客户检查和确认审核组携带的文件、资料和设备中未夹带受审核客户的任何保密或敏感信息。

C.4.5 认证机构应为包含客户保密或敏感信息的文件、资料和其他物品的制作、收发、传递、使用、复制、摘抄、保存和销毁建立保密程序。

C.5 ISMS 的变化（CNAS-CC01 条款 8.5.3）

认证机构应要求客户即时报告其业务、组织结构、位置和技术特点等方面可能导致其 ISMS 范围和边界变化的情况，以及与其 ISMS 相关的法律法规的变化情况。

C.6 认证申请（CNAS-CC01 条款 9.1.2）

C.6.1 认证机构应确保客户符合工信部联协[2010]394 号文《关于加强信息安全管理体系认证安全管理的通知》的要求，以及有关主管部门/监管部门对信息安全管理体系认证的管理要求（如工信部 2011 年第 21 号公告《工业和信息化部加强政府部门信息技术外包服务安全管理》等）。

C.6.2 认证机构宜要求客户向其说明适用的关于认证机构的资质、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，以便认证机构判断其是否具备对该客户实施认证活动的资格或条件。

C.7 认证审核相关要求（CNAS-CC01 条款 9.3 至条款 9.9）

C.7.1 初次认证第一阶段审核（CNAS-CC01 条款 9.3.1.2）

ISMS 初次认证审核的第一阶段审核宜包括在客户现场实施的审核活动，现场审核时间不宜少于 1 个审核人日。当客户由于信息安全的原因在申请评审阶段不能提供给认证机构足够的信息时，认证机构应通过第一阶段审核在客户的现场补充对上述信息的确认，并完成申请评审任务。这种情况下，认证机构应增加第一阶段现场审核时间。

C.7.2 对 ISMS 认证审核的指南

ISO/IEC 27007《信息技术 安全技术 信息安全管理体系审核指南》为 ISMS 审核方案管理、审核实施等内容提供了指南，认证机构可参考采用。

C.8 认证机构的管理体系（CNAS-CC01 条款 10.1、CANS-CC170 条款 10.1.1）

认证机构宜在其方针、政策、目标和承诺上体现自身的信息安全意识和追求，并在管理体系建立和实施中予以体现。

认证机构宜将认证机构的信息安全绩效，以及为其 ISMS 认证活动所采取的、与客户信息安全相关的措施的绩效作为管理评审的关注点之一。

G 部分

G.1 ISMS 认证机构能力分析和评价系统指南

G.1.1 概述

G.1.1.1 能力要求

G.1.1.1.1 能力是应用知识和技能实现预期结果的本领。ISMS 认证人员的能力要求应包括：

a) 所需的知识/技能。表 G.1（参照 CNAS-CC01 附录 A 的表 A.1）列举了承担申请评审、认证决定、审核三种职能的人员应掌握的知识和技能的类型；

b) 应用知识/技能所要实现的结果。它与人员所承担的职能有关，例如：ISMS 审核员需要考虑客户的整体信息安全风险，分析和判断客户的控制措施的充分性、适宜性和有效性，然后追溯到客户 ISMS 的符合性和有效性。

认证机构宜参考表 G.1 定义其他人员宜掌握的知识和技能。

注：其他人员包括认证机构的管理人员、行政支持性人员、相关委员会的成员以及技术专家等。

表 G.1 承担三种 ISMS 认证职能的人员所需知识和技能列表

承担认证职能 / 知识和技能	实施申请评审以确定所需的审核组能力、选择审核组成员和确定审核时间	复核审核报告和做出认证决定	审核和领导审核组
业务管理实践的知识			√
审核原则、实践和技巧的知识		√	√
ISMS 标准和规范的知识	√	√	√
认证机构过程的知识	√	√	√
客户的业务领域的知识	√	√	√
客户的产品、过程和组织的知识	√	√	√
与客户组织中的各个层级相适应的语言技能			√
作记录和撰写报告的技能			√
表达技能			√
面谈技能			√
审核管理技能			√

G.1.1.1.2 认证机构宜在能力要求中进一步定义表 G.1 中每类知识/技能的具体内容。

由于承担不同职能的人员需要具有的知识/技能水平可能不同（如表 G.1 所示），承担同种职能的人员在不同的认证活动风险和复杂性水平下需要具有的知识/技能水平也可能不同，因此能力要求宜体现出各种职能在各种认证活动风险和复杂性水平下

宜具有的知识/技能水平。相应的，认证机构宜定义：

a）认证活动风险和复杂性的确定方法和水平分级；

b）知识/技能的水平分级。知识/技能的水平宜从知识/技能的广度和深度、知识/技能的熟练程度等方面来体现。

G.1.1.2 专业能力和技术领域

G.1.1.2.1 ISMS 认证人员应用表 G.1 中的“技术领域”的知识，实现预期结果的本领是认证人员的专业能力。

技术领域是以 ISMS 相关过程的共性为特征的领域。ISMS 相关过程包括分析和评价业务活动中信息资产面临的信息安全风险，即风险评估；然后选择和实施保护信息资产的安全控制措施，以消除信息安全风险或把风险降至可接受的水平，即风险处置；以及风险评估和风险处置的持续改进。这些过程是信息安全技术和信息技术在客户业务活动中的应用，因此归纳过程的共性和划分技术领域宜基于信息安全技术、信息技术和客户业务活动的种类，并考虑信息安全技术和信息技术在客户业务活动中的应用特点。技术领域的一种划分方法是：

a）通用信息安全技术领域；

b）通用信息技术领域；

c）业务应用技术领域。

G.1.1.2.2 通用信息安全技术领域和通用信息技术领域

G.1.1.2.2.1 通用信息安全技术领域和通用信息技术领域是考虑到信息安全技术和信息技术具有通用性，不同种类业务活动中所应用的信息安全技术和信息技术很多是相同或相近的，与之相关的知识构成了 ISMS 认证人员专业能力的基础。因此，认证机构可将通用的信息安全技术知识和信息技术知识分别作为两个技术领域，即通用信息安全技术领域和通用信息技术领域。

G.1.1.2.2.2 认证机构宜确定通用信息安全技术领域和通用信息技术领域的具体分类方式，以确保专业能力分析和评价的系统性和充分性。本文件附录 B 提供了通用信息安全技术领域和通用信息技术领域的参考分类，认证机构可根据认证业务范围专业能力需求分析结果对其进行调整或补充，以形成本机构的分类。本文件附录 B 还对通用信息安全技术领域和通用信息技术领域的知识点及其应用提供了指南，可供认证机构在分析通用信息安全技术领域和通用信息技术领域的知识以及相应的专业能力时参考。

G.1.1.2.3 业务应用技术领域和认证业务范围

G.1.1.2.3.1 业务应用技术领域是考虑到 ISMS 是为了控制客户业务活动中的信息安全风险，为客户的业务活动提供保障。ISMS 认证人员需要适当掌握与客户业务活动相关的知识，例如流程、资产、风险、安全要求、控制措施以及信息安全技术和信息技术在业务活动中的特定应用等方面的知识，以便能够分析和判断客户信息安全控制措施的充分性、有效性和适宜性，进而追溯到客户 ISMS 的符合性和有效性。认证

机构可将与特定种类业务活动相关的这些知识归为一个技术领域，即业务应用技术领域。

G.1.1.2.3.2 本文件附录 A 的认证业务范围分类为认证机构确定业务应用技术领域分类提供了框架（参见附录 A 相关说明）。认证机构宜根据认证业务范围专业能力需求分析的结果，通过认证业务范围中类的进一步细分和（或）合并来确定本机构业务应用技术领域的分类。

注：认证业务范围中类进一步细分后得到的类别，可以与其他中类或其他中类里的细分类别合并。

G.1.1.2.4 技术领域知识的水平

在能力评价时，认证机构宜确定认证人员技术领域知识的水平，作为选择和使用认证人员的依据。认证机构可以对认证人员的通用信息安全技术领域知识的整体水平和通用信息技术领域知识的整体水平进行评价，但每个业务应用技术领域的知识水平宜分别进行评价。

表 G.2 给出了从事申请评审、认证决定、审核和领导审核组四种职能的人员在不同的认证活动风险和复杂性水平下，在认证活动涉及的技术领域宜具有的知识水平。由于风险和复杂性水平、知识水平可以有不同的分级方式，表 G.2 仅用“*”的数量表示了相对水平，“*”数量越多，相对水平越高。

表 G.2 四种 ISMS 认证人员技术领域知识的水平

技术领域知识水平 / 职能 / 风险和复杂性水平	实施申请评审以确定所需的审核组能力、选择审核组成员和确定审核时间	复核审核报告和做出认证决定	审核	领导审核组
*	*	*	**	**
**	*	*	**	**
***	**	**	***	***

G.1.2 能力分析和评价系统

认证机构应按照认可规范的所有适用要求建立覆盖所有 ISMS 认证人员的能力分析和评价系统。在专业能力方面，该系统宜包括以下过程（见图 G.1），以确保为每个客户配备有效审核和认证所需的专业能力：

a) 认证业务范围专业能力需求分析：认证机构对本机构认证活动涉及的所有认证业务范围大类和中类进行专业能力需求分析（参见 G.1.3.1）。

b) 技术领域的分类和专业能力要求的确定和调整：认证机构对从本机构涉及的所有认证业务范围大类和中类分析出的知识进行归纳，形成本机构技术领域分类（参见 G.1.1.2），然后基于每个技术领域的知识确定该技术领域对每类认证人员的专业能力要求，必要时编制特定技术领域的审核指导文件。当认证业务范围类别增加时，或者当特定客户的专业能力需求分析或者来自审核

过程的相关反馈显示有必要时，调整和完善技术领域的分类和专业能力要求。

c）特定客户专业能力需求分析：在申请评审中，根据特定客户的具体情况和本机构技术领域的分类与专业能力要求，分析和确定对该客户实施审核和认证所涉及的技术领域类别以及相应的专业能力，以便为选择和使用认证人员以及改进技术领域分类和专业能力要求提供输入，并在后续的审核方案管理中根据客户情况的变化予以必要调整（参见 G.1.3.2）。

d）能力评价：在认证活动管理和实施的相应阶段，采用适宜的能力评价方法，依据专业能力要求，对拟使用的人员实施能力评价，以确定其是否具备所需的专业能力（参见 G.1.4）。下列情况时宜对人员能力进行补充评价：

1）技术领域分类和（或）专业能力要求得到了更新；

2）通过能力的持续监视获得了相关反馈；

3）对人员能力进行了提升。

e）能力提升和补充：当能力评价结果显示相关人员的能力不满足专业能力要求时，通过适当方式（例如培训）提升其能力，或通过其他途径（例如技术专家）补足所需的能力。

f）选择和使用对特定客户实施审核和认证的人员：根据特定客户涉及的技术领域类别和专业能力，从经评价可供使用的人员中选择具备相应能力的人员，用于对该客户实施审核和认证。

g）能力的持续监视：对人员专业能力的运用、保持和发展情况进行持续监视，以便为人员能力补充评价提供输入。

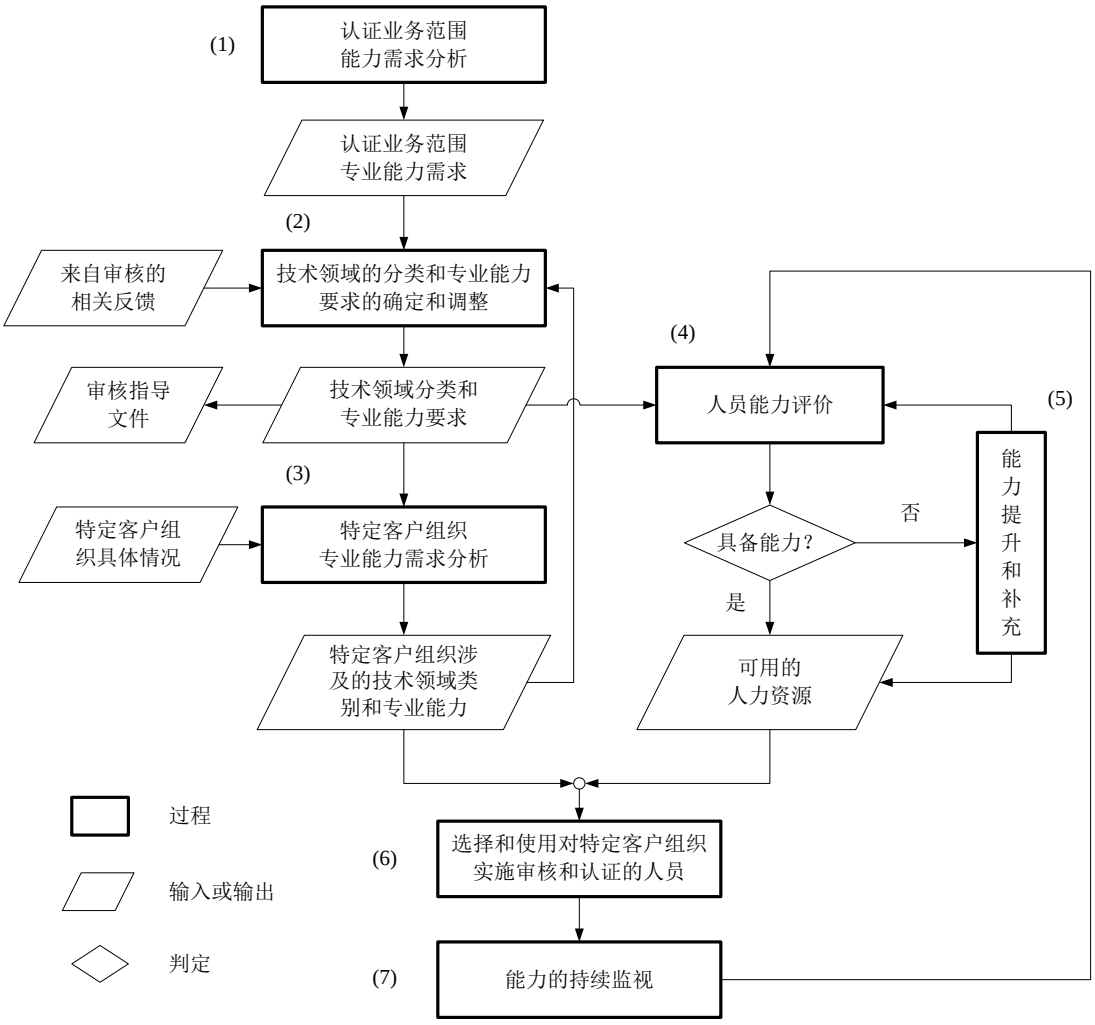

图 G.1 ISMS 认证人员专业能力的分析和评价

G.1.3 能力需求分析

G.1.3.1 认证业务范围专业能力需求分析

G.1.3.1.1 作为 ISMS 认证人员专业能力分析和评价的起点，认证机构宜对本机构认证活动涉及的认证业务范围大类和中类进行专业能力需求分析。

认证业务范围专业能力需求分析是为了初步识别实施涉及某个大类或中类的认证活动所需的专业知识，以便为归纳技术领域分类和确定专业能力要求，搭建能力分析和评价系统的框架，以及后续的针对特定客户实施专业能力分析奠定基础。因此，认证业务范围大类和中类的专业能力需求分析可基于该类别的典型的、有代表性的情况，而不必穷尽该类别涉及的所有情况。

G.1.3.1.2 实施认证活动需要了解 ISMS 建立与实施中涉及的知识，而信息安全风险评估和处置是建立与实施 ISMS 的基础。因此，认证业务范围大类或中类的能力需求分析可采用信息安全风险评估和处置的思路（见图 G.2），分析该类别 ISMS 建立与实施的典型情况及相应的知识，包括：

a) 分析典型的业务流程和信息处理流程；
b) 基于典型的业务流程和信息处理流程，分析典型资产（包括硬件、软件、网络、业务系统、人员和数据资料等）和典型信息安全风险（包括脆弱性和威胁）；
c) 基于典型信息处理流程和典型资产，分析信息技术在该类别中的典型应用；
d) 基于业务活动要求、法规要求和合同/相关方要求分析典型信息安全要求；
e) 基于典型资产和典型信息安全要求，分析典型信息资产的典型信息安全特性，例如保密性、可用性、完整性、、真实性、不可抵赖性、可追溯性等；
f) 基于典型信息安全风险和典型信息资产的典型信息安全特性，分析典型控制措施；
g) 基于典型控制措施，分析信息安全技术在该类别中的典型应用。

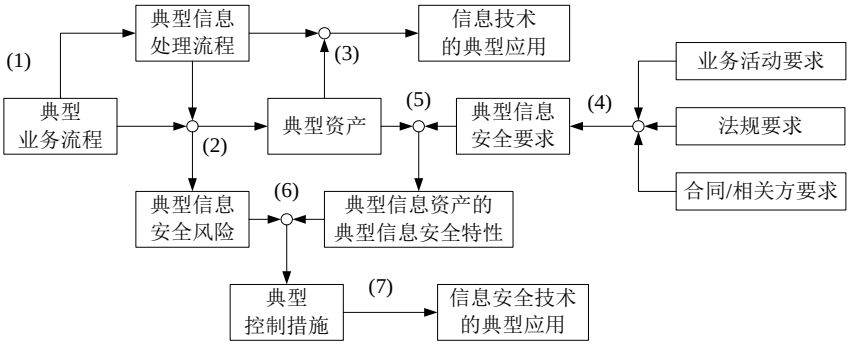

图 G.2 ISMS 认证业务范围能力需求分析思路

G.1.3.2 特定客户能力需求分析

G.1.3.2.1 认证机构在对特定客户实施申请评审时，宜根据该客户的具体情况以及本机构技术领域的分类和专业能力要求，分析和确定对该客户实施审核和认证所涉及的技术领域类别和相应的专业能力（即能力需求），并从经评价可用的人力资源中选择具备这些专业能力的人员，对该客户实施审核和认证。

认证机构在授予客户初次认证后，宜在审核方案管理中关注客户发生的任何可能影响其能力需求的变化，并及时根据此类变化对客户的能力需求和配备的认证人员进行必要的调整。

G.1.3.2.2 由于技术领域的分类和专业能力要求主要在认证业务范围能力需求分析的基础上确定，而后者基于相关业务范围类别的典型情况，不一定考虑到所有可能的情况，因此对特定客户进行能力需求分析时宜注意识别该客户是否存在认证业务范围能力需求分析时未考虑到的情况。如果存在，宜基于所识别的情况进行补充分析（可采用图 G.2 的分析思路），并根据补充分析的结果对现有的技术领域的分类和（或）专业能力要求进行调整和完善，然后相应地对相关认证人员的能力进行补充评价，并

在必要时进行能力的提升或补充，以确保具有充分的能力对特定客户实施审核和认证活动。

G.1.3.2.3 特定客户的能力需求分析由申请评审人员实施。由于申请评审人员的能力依据现有的专业能力要求评定，所以当特定客户能力需求分析的过程中有迹象显示该客户涉及的专业能力可能超出现有的专业能力要求时，认证机构宜及时确认申请评审人员的能力，并在必要时通过适宜方式补足对特定客户实施能力需求分析所需的能力。

G.1.4 能力评价

G.1.4.1 能力评价是获取被评价人能力的证据，并将能力的证据与能力要求进行比较，以确定被评价人是否满足能力要求的过程。能力评价宜保留能力证据、评价活动和评价结论的记录（包括音像资料）。

G.1.4.2 能力的证据宜与能力要求的内容相关，并且能够为评价结论提供支持。因此，认证机构宜通过适宜的评价方法获取充分的能力证据。评价方法的选择宜考虑：

a) 评价所依据的能力要求的内容（包括知识、技能、所要实现的结果）；
b) 评价的目的，例如：初次聘用、持续监视、扩大能力范围、能力要求更新后的补充评价等；
c) 已建立的对被评价人能力的了解和信心。

以下介绍了一些常用的评价方法。这些方法宜组合使用，以获得关于被评价人员能力的充分证据和全面评价；通常，仅采用其中某一种方法不足以对被评价人的能力做出全面评价。

a) 记录审查：对被评价人的教育、工作、培训、审核的相关记录进行审查，以获取其知识和技能的证据，获得对其能力的基本了解。记录审查的注意事项包括：
   1) 记录内容宜尽可能详细、充分，以便于识别被评价人所具有的知识和技能；
   2) 宜通过调查、面谈等方法对记录中的相关信息进行必要的验证、澄清和确认；
   3) 在通过记录审查获得对被评价人能力的基本了解后，宜进一步通过考试、见证等方法对其能力进行确认；
   4) 不宜直接根据被评价人的学历、工作年限、培训时间、审核次数/天数等经历认定其满足相关能力要求。
b) 意见反馈：通过被评价人的工作单位、同事或客户等方面反映的意见了解被评价人员的知识、技能、表现等情况。意见反馈宜作为其他评价方法的补充，不宜仅根据某方面的意见对被评价人的能力做出判断。
c) 面谈：面谈有助于详细了解被评价人的知识或技能，并可用于评估语言、沟通、人际管理方面的技能。依据能力要求对被评价人进行结构化面谈，并予以适当记录，可以获得其能力的直接证据。面试的示例：

- 人员招聘时进行面谈，以从人员的简历和过去的工作经历详细了解其知识和技能；
- 在绩效考评中进行面谈，了解人员知识和技能的具体情况；
- 在见证或审核报告的复核中与审核组成员进行面谈，以了解审核员的知识和技能、做出某项结论的理由或选择审核方法、审核路径的理由。

d) 考试：包括笔试、口试和实际操作考试。笔试可以为人员的知识提供良好的文件化证据。对于人员的技能也可通过适宜的笔试方法获取证据。口试可为人员的知识提供良好的证据，但在人员技能的评价上作用有限。实际操作考试的示例包括情景演练、案例分析、压力模拟、岗位实操考核等。

e) 见证：对人员实施工作任务的情况进行观察，可以用于认证机构的所有人员。见证可以为人员的能力提供直接证据。

ISO/IEC 27007《信息技术 安全技术 信息安全管理体系审核指南》为 ISMS 认证机构确定用以满足审核方案需求的审核员能力提供了指南，认证机构建立和实施能力分析评价系统时可参考采用。

附录 A（规范性附录）

ISMS 认证机构认证业务范围分类与分级

大类	中类	级别	描述	备注
01	政务			
	01.01	一	国家机构	包括人大、政府、法院、检察院等，不含税务机关和海关
	01.02	一	税务机关	
	01.03	一	海关	
	01.04	二	其他	例如政党，政协，社会团体等
02			公共	
	02.01	一	通信、广播电视	
	02.02	一	新闻出版	包括互联网内容的提供
	02.03	二	科研	涉及特别重大项目的应提升为一级
	02.04	二	社会保障	例如社会保险基金管理、慈善团体等。包括医疗保险
	02.05	二	医疗服务	
	02.06	三	教育	
	02.07	三	其他	例如市政公用事业（水的生产和供应、污水处理、燃气生产和供应、热力生产和供应、城市水陆交通设施的维护管理等）
03			商务	
	03.01	一	金融	例如银行、证券、期货、保险、资产管理等
	03.02	一	电子商务	以在线交易为主要特点，含网络游戏
	03.03	一	物流	包括邮政
	03.04	三	咨询中介	例如法律、会计、审计、公证等
	03.05	三	旅游、宾馆、饭店	
	03.06	三	其他	
04			产品的生产	产品包括软件、硬件、流程性材料和服务
	04.01	一	电力	包括发电和输、变、配电等
	04.02	一	铁路	
	04.03	一	民航	
	04.04	一	化工	
	04.05	一	航空航天	
	04.06	一	水利	
	04.07	二	交通运输	包括公路、水路、城市公共客运交通等，不含航空和铁路
	04.08	二	信息与通信技术	例如软、硬件生产及其服务，系统集成及其服务，数字版权保护等
	04.09	二	冶金	
	04.10	二	采矿	含石油、天然气开采
	04.11	二	食品、药品、烟草	
	04.12	三	农、林、牧、副、渔业	
	04.13	三	其他	

注 1：CNAS 提出 ISMS 认证机构认证业务范围分类是为了在规范的框架下对认证机构的能力实施评审，并相应地限定其认可范围，以促使 ISMS 认证活动规范、有序地发展，控制认可风险；同时给各认证机构开展能力分析和评价提供一致的框架。该分类并不意味着 CNAS 批准认证机构可以对每个类别中的任何组织实施认证活动。

注 2：CNAS 考虑到 ISMS 相关技术和知识与组织的业务活动具有相关性，组织相关方和业内专家，

通过讨论和划分 ISMS 认证组织业务活动的类型,提出了认证业务范围分类。该分类基于我国 ISMS 认证和认可活动当前的实践和经验，注意涵盖了我国信息安全等级保护的重点领域，例如：广播电视网、通信网、金融银行、电力、铁路、民航、石油化工等，同时兼顾了其他行业领域。

注 3：由于 ISMS 认证在世界范围内仍处于发展阶段，我国 ISMS 认证的数量以及涉及的业务活动类型都还有限，所以认证业务范围中组织业务活动类型的划分方式仍需随着我国 ISMS 认证的发展和经验的增加不断改进。因此认证机构不宜直接将认证业务范围分类作为业务应用技术领域分类，而需要以其为框架进一步分析和确定业务应用技术领域。

注 4：认证业务范围分级是为了使 CNAS 在确定认证业务范围的评审方式时考虑相关的风险，从而对认证机构业务活动的扩展进行控制，降低认可风险。这里的风险是指 CNAS 认可的风险，即 CNAS 认可的 ISMS 认证机构所认证的组织的信息安全发生问题时，连带使 CNAS 声誉受损或承担责任的风险。每个中类的级别主要考虑了在该中类信息安全对于国家安全、社会秩序、公共利益、组织及其相关方合法权益的重要性的典型情况。

附录 B（资料性附录）

通用信息安全技术领域和通用信息技术领域——参考分类、知识点及应用

注：以下的参考分类不是为了对信息安全技术和信息技术的学科门类进行精确的划分，而是给出一种相对合理且具有实用性的分类，以供 ISMS 认证机构在能力分析和评价中参考。

A 通用信息安全技术领域

分类	要素描述	知识点	能够应用知识点对下列方面进行分析和判断
A1 信息安全风险管理	A1.1 信息安全风险评估	• 常见的风险评估方法 • 典型资产的信息安全重要度 • 典型资产常见的脆弱性、威胁和风险	• 风险评估方法是否符合标准要求 • 风险评估的实施是否符合风险评估方法要求 • 风险评估报告的内容（重要资产、主要脆弱性和威胁、主要风险的分析与评价等）是否充分
	A1.2 信息安全风险处置	• 风险处置的基本要素和典型风险处置方法 • 典型资产常见脆弱性的控制措施 • 典型资产常见威胁的防范措施 • 典型信息安全风险的防范措施	• 风险处置计划是否充分和符合风险处置准则 • 控制措施是否适宜 • 残余风险的实际状况
	A1.3 脆弱性管理	• 典型的操作系统漏洞及获取方式 • 典型的应用系统漏洞 • 系统漏洞的管理方法与工具	• 脆弱性是否得到管理 • 脆弱性的报告机制是否完善 • 是否具有及时应对脆弱点的途径
A2 信息安全事件管理	A2.1 业务连续性管理	• 业务连续性管理的信息安全方面要求 • 业务连续性管理程序的要求 • 业务连续性计划、业务连续性演练方案制定方法 • 业务连续性演练分析、评价方法 • 典型的应急响应流程	• 关键业务的分析是否充分 • 业务连续性计划是否充分 • 业务连续性演练方案是否充分，执行是否有效 • 业务连续性演练分析是否充分、评价是否有效
	A2.2 备份与恢复	• 主流的灾备技术 • 典型的灾备设备 • 典型的灾备管理规范 • 典型的灾备方案和环境	• 灾备要求分析是否充分 • 灾备方案是否充分 • 日常灾备管理是否符合管理规范 • 灾备演练是否有效 • 灾备演练分析是否充分、评价是否有效

分类	要素描述	知识点	能够应用知识点对下列方面进行分析和判断
A3 物理和环境安全	A3.1 区域安全	• 安全区域的划分原则 • 安全区域的典型控制措施	• 安全区域划分是否合理 • 安全区域标识是否清晰 • 安全区域的控制是否有效
	A3.2 支持性设施与设备安全	• 典型的支持性设施与设备的作用与性能 • 典型的支持性设施与设备的维护与管理要求	• 支持性设施与设备的维护是否符合规范 • 支持性设施与设备的应急措施是否有效 • 支持性设施与设备的维护记录是否完整
A4 网络安全	A4.1 边界防护	• 网络环境与边界划分 • 典型的网络环境 • 典型的网络设备 • 典型的网络攻击手段 • 典型的边界防护技术	• 网络管理是否规范 • 网络区域划分是否满足风险控制要求 • 所采取的边界防护措施是否满足风险控制的要求 • 网络与边界防护设备维护是否符合规范 • 网络与边界防护应急措施是否有效 • 网络与边界防护设备的维护记录是否完整
	A4.2 主机安全	• 主流的计算环境 • 典型的操作系统 • 典型的系统安全问题 • 典型的系统安全加固技术	• 是否制定和执行了主机日志管理规范 • 主机安全加固是否满足风险控制要求 • 主机设备维护是否符合规范 • 主机设备应急措施是否有效 • 主机设备的维护记录是否完整
	A4.3 防范恶意和移动代码	• 恶意和移动代码的基本原理 • 流行的恶意代码 • 恶意代码的防护技术 • 移动代码的使用规范 • 主流的恶意代码检测、防护产品	• 是否制定和执行了恶意和移动代码管理规范 • 移动代码使用是否适宜 • 恶意代码防护措施是否满足信息风险控制的要求
A5 访问控制	A5.1 用户访问控制	• 用户鉴别技术及主流产品 • 典型的网络访问控制方式 • 典型的操作系统访问控制方式 • 典型的应用和信息（含数据库）访问控制	• 是否制定和执行了用户访问控制规范 • 访问控制的日志是否完整 • 访问控制日常检查是否有效
	A5.2 移动计算和远程工作	• 安全通讯协议 • 移动计算模式 • 远程工作模式 • 远程工作的典型问题	• 采取的安全通讯协议是否满足风险控制要求 • 是否制定和执行了移动计算与远程工作管理规范

分类	要素描述	知识点	能够应用知识点对下列方面进行分析和判断
A6 软件安全	A6.1 软件安全开发	• 软件安全设计与开发的过程管理 • 典型的应用软件安全问题 • 典型的应用软件安全控制措施	• 是否制定和执行了软件开发安全控制规范 • 软件开发设计中是否进行了安全需求分析并针对安全需求进行了专门设计 • 软件开发环境是否独立 • 开发文档管理是否规范
	A6.2 软件安全测试	• 典型的应用软件测试方法 • 主要的应用软件安全测试点和安全测试工具	• 测试记录管理是否规范 • 必要安全测试点是否完成测试 • 测试环境是否独立
	A6.3 软件获取与分发管理	• 软件分发管理技术 • 典型的软件获取方式 • 典型的软件分发方式及工具	• 是否制定和执行了软件获取与分发规范 • 软件开发、测试、验收的文档管理是否规范 • 软件分发控制是否有效
	A6.4 软件安全审计	• 软件安全审计技术 • 应用软件的关键安全审计点 • 典型的应用软件安全审计工具	• 是否制定和执行了软件安全审计规范 • 软件安全设计工具的使用是否得到控制 • 软件安全审计的记录是否完整
A7 密码技术	A7.1 密码原理密钥管理	• 密码基本原理 • 典型的密码算法 • 密钥管理技术 • 密码应用与密钥管理的相关要求	• 密码的应用是否符合法律法规要求 • 如果采用密码算法，是否达到风险控制要求 • 如果使用密钥，密钥管理是否符合相关要求
	A7.2 公钥体系（PKI）	• PKI 基本原理和典型应用 • RSA 和 ECC（两个典型算法） • CA 证书及其管理、CA 中心的管理要求	• 如果建立 CA 中心，是否符合法律法规要求 • 如果采用密码算法，密钥长度是否达到风险控制要求
A8 信息安全建设	A8.1 信息技术产品安全性	• 信息技术产品安全性评价 • 信息技术产品安全性保障 • 配置管理与安全配置	• 如果是信息技术产品开发者，是否制定和执行了相应的产品安全性保障规范 • 采用的信息技术产品是否经过了适宜的安全性评价 • 对信息技术产品是否采取了必要的配置管理措施 • 信息技术产品的安全配置是否满足信息安全风险控制的要求
	A8.2 信息安全工程	• 信息安全工程概念 • 信息安全工程管理手段	• 适用时，是否制定和执行了信息安全工程规范
	A8.3 信息安全产品	• 主流的信息安全产品 • 信息安全产品的管理要求	• 采用的信息安全产品是否满足信息安全风险控制的要求 • 采用的信息安全产品是否符合相关法律法规的要求 • 是否制定和执行了信息安全产品的配置管理规范 • 是否制定和执行了信息安全产品的日志管理规范

B 通用信息技术领域

分类	要素描述	知识点	能够应用知识点对下列方面进行分析和判断
B1 信息技术基础	B1.1 通讯技术基础（包括网络通讯和传统通讯技术）	• 网络通讯原理 • 传统通讯原理 • TCP/IP 协议族 • 典型的通讯环境 • 典型通讯问题	• 网络结构是否符合组织风险控制要求 • 路由策略管理是否规范 • 通讯外包服务管理是否规范 • 通讯设备的授权控制是否规范 • 通讯设备的日志分析是否有效 • 传统通讯环境下的新设备管理是否规范
	B1.2 计算机技术基础	• 计算机原理 • 操作系统 • 数据库原理	• 系统的容量管理是否有效 • 系统的脆弱性管理是否有效 • 系统的授权控制是否规范 • 系统的日志分析是否有效 • 系统的版本管理是否规范 • 数据库的配置管理是否适宜 • 数据库的用户管理与访问控制是否规范 • 数据库的备份策略与测试是否有效 • 数据库的备份信息管理是否规范 • 数据库脆弱性管理是否有效 • 数据库的日志分析是否有效
	B1.3 系统集成	• 系统集成的基本方法与项目管理方法 • 系统集成方案设计 • 典型的系统集成工程	• 项目的安全需求分析是否充分 • 项目的文档管理是否规范 • 项目实施的监理是否规范 • 项目验收是否规范 • 项目的后续服务保障是否落实
	B1.4 软件工程	• 软件工程基本思想 • 软件项目实施 • CMMi • 软件开发管理相关国家标准	• 软件开发安全需求分析是否充分 • 软件开发文档管理是否规范 • 软件开发文档是否完整 • 软件测试管理是否规范 • 软件验收是否规范 • 软件开发环境管理是否规范 • 软件脆弱性管理是否有效 • 软件版本控制是否规范

分类	要素描述	知识点	能够应用知识点对下列方面进行分析和判断
B2 信息技术应用	B2.1 通用支撑平台 （操作系统、数据库、中间件）	• 常用的操作系统 • 典型操作系统的适用环境 • 应用支撑平台分层 • 主流的应用支撑平台 • 主流数据库 • 操作系统、应用支撑平台和数据的主要安全问题	参照 B1.2，并考虑以下方面： • 配备的网络环境、系统环境和应用环境是否适宜 • 应用服务的版本管理是否规范 • 应用服务器的脆弱性管理是否有效 • 应用服务器的授权管理是否规范 • 应用服务器的日志分析是否充分
	B2.2 主流软件开发平台	• 主流软件开发平台 • 主要软件测试工具	参照 B1.4
	B2.3 IT服务管理	• IT 服务管理基本思想 • IT 服务管理流程 • 典型 IT 服务管理工具	• 外包管理是否规范 • 服务级别协议是否适宜 • 服务管理流程设置是否满足客户服务级别协议要求 • 对事件、问题、知识的管理是否规范
	B2.4 典型大众化应用	• 典型的大众化应用系统 （如 OA、网站、邮件系统、即时通讯系统、ERP 等）	• 应用系统的容量管理是否有效 • 应用系统的脆弱性管理是否有效 • 应用系统的授权控制是否规范 • 应用系统的日志分析是否充分 • 应用系统的版本管理是否规范 • 应用系统的基本安全防护是否有效