版本	修订内容	修订日期	修订人
A/4	依据备案整改要求修订	2025.08.29	孟宪龙

批准 _____

审核 _____

制订 孟宪龙

发布日期	修订日期	实施日期
2019.11.15	2025.08.29	2025.08.29

1 适用范围

1.1本规则用于中标通国际认证（深圳）有限公司（以下简称“中标通”）规范依据ISO/IEC 27001:2022《信息安全 网络安全和隐私保护 信息安全管理体系 要求》标准开展信息安全管理体系（以下简称“ISMS”）认证活动。

1.2 本规则依据认证认可相关法律法规，结合相关技术标准，对 ISMS 认证实施过程作出具体规定，明确中标通对认证过程的管理责任，保证 ISMS 认证活动的规范有效。

1.3 本规则是中标通在 ISMS 认证活动中的基本要求，中标通在该项认证活动中应当遵守本规则。

2 对认证机构的基本要求

2.1 获得国家认监委批准、取得从事 ISMS 认证的资质。

2.2 认证能力、内部管理和工作体系符合 GB/T 27021/ISO/IEC 17021-1《合格评定 管理体系审核认证机构要求》及 ISO/IEC 27006-1:2024《信息安全 网络安全和隐私保护 信息安全管理体系审核和认证机构要求 第一部分 通用》。

2.3 建立内部制约、监督和责任机制，实现培训（包括相关增值服务）、审核和作出认证决定等工作环节相互分开，符合认证公正性要求。

2.4 不得将申请认证的组织（以下简称申请组织）是否获得认证与参与认证审核的审核员及其他人员的薪酬挂钩。

3 对认证审核人员的基本要求

3.1 认证审核员应当取得国家认监委确定的认证人员注册机构颁发的 ISMS 审核员注册资格。

3.2 认证人员应当遵守与从业相关的法律法规，对认证审核活动及相关认证审核记录和认证审核报告的真实性承担相应的法律责任。

4 认证依据

ISMS认证依据：ISO/IEC 27001:2022《信息安全 网络安全和隐私保护 信息安全管理体系 要求》。

5 初次认证程序

5.1 受理认证申请

（4）考虑申请认证的活动范围及场所、员工人数及体系覆盖人数、完成审核所需时间和其他影响认证活动的因素（语言、安全条件、对公正性的威胁等）。

5.1.4.2 满足以下条件的，中标通可以受理认证申请：

a）申请组织已具备受理条件（见5.1.2、5.1.3）；

b）中标通具备实施认证的能力；

c）双方就认证事宜达成一致。

5.1.4.3 对被执法监管部门责令停业整顿或在全国企业信用信息公示系统中被列入“严重违法企业名单”的申请组织，中标通不应受理其认证申请。

5.1.4.4 在申请评审后，认证机构应接受或拒绝认证申请。经评审出现不满足 5.1.4.2 或出现 5.1.4.3 等应拒绝认证申请的情况时，应记录拒绝申请的原因并明确告知客户拒绝的原因。

5.1.5 签订认证合同

在实施认证审核前，中标通应与申请组织订立具有法律效力的书面认证合同，合同应至少包含以下内容：

（1）申请组织获得认证后持续有效运行 ISMS 的承诺。

（2）申请组织对遵守认证认可相关法律法规，协助认证监管部门的监督检查，对有关事项的询问和调查如实提供相关材料和信息的承诺。

（3）申请组织承诺获得认证后发生以下情况时，应及时向中标通通报：

① 客户及相关方有重大投诉。

② 被信息安全管理监管部门认定不合格。

③ 发生信息安全事故。

④ 相关情况发生变更，包括：法律地位、生产经营状况、组织状态或所有权变更；取得的行政许可资格、强制性认证或其他资质证书变更；法定代表人、最高管理者变更；生产经营或服务的工作场所变更；ISMS 覆盖的活动范围变更；ISMS 和重要过程的重大变更等。

⑤ 出现影响 ISMS 运行的其他重要情况。

（4）申请组织承诺获得认证后正确使用认证证书、认证标志和有关信息，不利用 ISMS 认证证书和相关文字、符号误导公众认为其产品或服务通过认证。

5.2.2.2 中标通以附录 A 所规定的审核时间为基础，考虑认证覆盖范围内的有效人数、ISMS 审核时间计算因素，建立文件化的不同类型审核的审核时间（包括现场审核时间） 的确定方法。中标通应对每次审核的审核时间的确定过程应形成记录，尤其是减少审核时间的理由，减少的时间不得超过附录 A 所规定的审核时间的 30%，现场审核时间不得少于所确定的审核时间的 70%。审核时间计算方法详见附录 B。

5.2.2.3 ISMS 和其他管理体系结合审核时，中标通应根据申请组织体系的一体化程度、审核组一体化审核的能力适当减少审核，结合审核的总审核时间不得少于多个单独体系所需审核时间之和的 80%。确定减少结合审核人天数的计算方法详见附录 C。

5.2.3 多场所审核的策划

5.2.3.1 当申请组织为多场所组织时，具备以下资格条件时，可按照多场所策划审核：

1）组织应具有单一管理体系；

2）中心职能是组织的一部分且不应被分包给外部的组织；

3）中心职能应获得组织的授权以规定、建立并保持该单一管理体系；

4）组织的单一管理体系应服从集中的管理评审；

5）所有场所应服从组织的内部审核程序。

6）中心职能应有责任确保来自于所有场所的数据信息得到收集和分析，并且应能够证明其权威和能力，以便在需要时（包括但不限于下述情况）发起组织的变更：

（i）体系文件和体系变更；

（ii）管理评审；

（iii）投诉；

（iv）纠正措施的评价；

（v）内部审核的策划和对结果的评价；

（vi）与适用标准有关的法律法规要求。

注：中心职能是实施控制并得到组织最高管理者授权的，是对所有场所产生影响的。并没有要求中心职能仅处于某个单一场所。

5.2.3.2 拟抽样组织应满足的条件

5.2.3.2.1 所有场所的过程应实质上属于同一类活动、复杂程度和风险程度相似，并按

f）场所的管理体系和过程的复杂程度；

g)上次认证审核以来的变化；

h）管理体系的成熟度和组织的理解程度；

i）地域、文化、语言和法律法规方面的差异；

j）地理位置的分散程度；

k）还应考虑：

- 不同场所的信息系统的复杂程度；
- 工作实践的差的差异；
- 所实施的活动的差异；
- 控制的设计与运行的差异；
- 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；
- 场所的风险状况；
- 发生在特定场所的信息安全事件。

5.2.3.4.1.3 以下情况要全部审核：

a）有证据表明认证的风险性和复杂性很高；

b）各场所管理体系在实施上有较大的差异（厂房及设备设施、工艺、产品种类、周边环境、人员素质、信息安全资产、信息处理流程、信息技术应用等）；

c)各场所涉及的法律法规或当地行政机关的要求不相同；

d）ISMS 中每个具有重大风险的场所。

5.2.3.4.1.4 场所的选取不一定在审核过程开始前进行，也可以在对中心职能的审核完成时由认证审核组根据现场审核信息提议场所选取方案，并与认证机构方案策划人员沟通确认后调整方案。在任何情况下，认证机构都应将拟抽样的场所告知中心职能。认证机构可以提前较短的时间通知，但宜为迎审准备留出足够的时间。

5.2.3.4.2 样本量

对多个相似场所可抽样审核，抽样数量应不少于按以下方法计算的结果：

（1）初次认证审核：$Y=\sqrt{x}$

（2）监督审核 ：$Y=0.6\sqrt{x}$

（3）再认证审核 ：$Y=0.8\sqrt{x}$

- 出现对受审核方的重大投诉，且系受审核方责任的
- 发生了信息安全、信息技术服务等事故的；
- 媒体负面曝光且系受审核方责任的；

b）出于对信息安全及安全保密的需要，不适宜选择远程审核方式；

c）暂停恢复审核；

d）上次认证审核方式已是完全的远程审核方式；

e）其他不适宜远程审核的活动/过程或场所，如易燃易爆场所、无网络信号或不具备 ICT 技术实施条件的关键活动或场所等。

5.2.5.3 审核中采用远程审核方式的，远程审核时间不得超过现场审核时间的 30%，并应在审核计划、审核记录及审核报告中予以注明。

5.2.6 审核计划

5.2.6.1 中标通应为每次审核制定书面的审核计划（第一阶段审核不要求正式的审核计划）。审核计划至少包括以下内容：审核目的，审核准则，审核范围，现场审核的日期和场所，现场审核持续时间，审核组成员（其中：审核员应标明认证人员注册号;技术专家应标明专业代码、工作单位及专业技术职称）。

5.2.6.2 为使现场审核活动能够观察到产品生产或服务活动情况，现场审核应安排在认证范围覆盖的产品生产或服务活动正常运行时进行。

5.2.6.3 在审核活动开始前，审核组应将审核计划交申请组织确认，遇特殊情况临时变更计划时，应及时将变更情况通知申请组织，并协商一致。

5.3 实施审核

5.3.1 审核组应当按照审核计划的安排完成审核工作。除不可预见的特殊情况外，审核过程中不得更换审核计划确定的审核员。

5.3.2 审核组应当会同申请组织按照程序顺序召开首、末次会议，申请组织的最高管理者及与 ISMS 相关的职能部门负责人员应该参加会议。参会人员应签到，审核组应当保留首、末次会议签到表。审核组应按国家认 监委的要求完成首、末次会议现场审核的网络签到。申请组织要求时，审核组成员应向申请组织出示身份证明文件。

5.3.3 审核过程及环节

5.3.3.5第二阶段审核应当在申请组织现场进行。重点是审核ISMS符合ISO/IEC 27001标准要求和有效运行情况，应至少覆盖以下内容：

（1）在第一阶段审核中识别的重要审核点的过程控制的有效性。

（2）为实现信息安全方针而在相关职能、层次和过程上建立信息安全目标是否具体适用、可测量并得到沟通、监视。

（3）对ISMS覆盖的过程和活动的管理及控制情况。

（4）申请组织实际工作记录是否真实。对于审核发现的真实性存疑的证据应予以记录并在做出审核结论及认证决定时予以考虑。

（5）申请组织的内部审核和管理评审是否有效。

5.3.4 在审核中应通过适当的抽样来获取与审核目的、范围和准则相关的信息（包括与职能、活动和过程之间的接口有关的信息），并对这些信息进行验证，使之成为审核证据。信息获取方法应包括（但不限于）：

（1）面谈；

（2）对过程和活动观察；

（3）审查文件和记录。

5.3.5发生以下情况时，审核组应向中标通报告，经中标通同意后终止审核：

（1）受审核方对审核活动不予配合，审核活动无法进行；

（2）受审核方实际情况与申请材料有重大不一致；

（3）其他导致审核程序无法完成的情况。

5.4 审核报告

5.4.1 审核组应对审核活动形成书面审核报告，由审核组组长签字。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：

（1）申请组织的名称和地址

（2）申请组织活动范围和场所。

（3）审核的类型、准则和目的。

（4）审核组组长、审核组成员及其个人注册信息。

（2）反映以下问题的不符合项，中标通已评审、接受并验证了纠正和纠正措施的有效性：

①在持续改进 ISMS 的有效性方面存在缺陷，实现信息安全目标有重大疑问；

②制定的信息安全目标不可测量、或测量方法不明确；

③对实现信息安全目标具有重要影响的关键点的监视和测量未有效运行，或者对这些关键点的报告或评审记录不完整或无效；

④其他严重不符合项。

（3）中标通对其他一般不符合项已评审，并接受了申请组织计划采取的纠正和纠正措施。

5.6.4 在满足 5.6.3 条要求的基础上，中标通有充分的客观证据证明申请组织满足下列要求的，评定该申请组织符合认证要求，向其颁发认证证书：

（1）申请组织的 ISMS 符合标准要求且运行有效；

（2）认证范围覆盖的产品和服务符合相关法律法规要求；

（3）申请组织按照认证合同规定履行了相关义务。

5.6.5 申请组织不能满足上述要求或者存在以下情况的，评定该申请组织不符合认证要求，以书面形式告知申请组织并说明其未通过认证的原因：

（1）受审核方的 ISMS 有重大缺陷，不符合 ISO/IEC 27001:2022 标准的要求。

（2）发现受审核方存在重大信息安全问题或有其他与产品和服务信息安全相关严重违法违规行为。

6 监督审核程序

6.1 中标通应对持有其颁发的 ISMS 认证证书的组织（以下称获证组织）进行有效跟踪，监督获证组织持续运行 ISMS 并符合认证要求。

6.2 为确保达到 6.1 条要求，中标通应根据获证组织的产品和服务的信息安全复杂程度或其他特性，确定对获证组织的监督审核的频次。

6.2.1 作为最低要求，初次认证后的第一次监督审核应在认证证书签发日起 12 个月内进行。此后，监督审核应至少每个日历年（应进行再认证的年份除外）进行一次，且两次监督审核的时间间隔不得超过 15 个月。

6.9 中标通根据监督审核报告及其他相关信息，作出继续保持或暂停、撤销认证证书的决定。

7 再认证程序

7.1 认证证书期满前，若获证组织申请继续持有认证证书，中标通应当实施再认证审核，并决定是否延续认证证书。

7.2 中标通应按 5.2.4 条和 5.3.1 条要求组成审核组。按照 5.2.6 条要求并结合历次监督审核情况，制定再认证审核计划交审核组实施。

在 ISMS 及获证组织的内部和外部信息安全无重大变更时，再认证审核可省略第一阶段审核，但审核时间应不低于按 5.2.2 条计算人天数的 2/3。

7.3 对再认证审核中发现的严重不符合项，中标通应规定时限要求获证组织实施纠正与纠正措施，并在原认证证书到期前完成对纠正与纠正措施的验证。

7.4 中标通按照 5.6 条要求作出再认证决定。获证组织继续满足认证要求并履行认证合同义务的，向其换发认证证书。

7.5 如果在当前认证证书的终止日期前完成了再认证活动并决定换发证证书，新认证证书的终止日期可以基于当前认证证书的终止日期。新认证证书上的颁证日期应不早于再认证决定日期。

如果在当前认证证书终止日期前，中标通未能完成再认证审核或对严重不符合项实施的纠正和纠正措施未能进行验证，则不应予以再认证，也不应延长原认证证书的有效期。

在当前认证证书到期后，如果中标通能够在 6 个月内完成未尽的再认证活动，则可以恢复认证，否则应至少进行一次第二阶段审核才能恢复认证。认证证书的生效日期应不早于再认证决定日期，终止日期应基于上一个认证周期。

8 特殊审核程序

8.1 扩大认证范围

对于已授予的认证，认证机构应对扩大认证范围的申请进行评审，并确定任何必要的审核活动，以做出是否可予扩大的决定。

这类审核活动可以结合监督审核同时进行。

8.2 提前较短时间通知的审核

9.1.3 中标通应以适当方式公开暂停认证资格的信息，明确暂停的起始日期和暂停期限，并声明在暂停期间获证组织不得以任何方式使用认证证书、认证标识或引用认证信息。

9.2 认证资格的撤销

9.2.1 获证组织有以下情形之一的，中标通应在获得相关信息并调查核实后 5 个工作日内撤销其认证资格，并保留相应证据：

（1）被注销或撤销法律地位证明文件的；

（2）被列入信用严重失信企业名单；

（3）拒绝配合认证监管部门实施的监督检查，或者对有关事项的询问和调查提供了虚假材料或信息的；

（4）拒绝接受信息安全监督抽查的；

（5）出现重大信息安全事故，经执法监管部门确认是获证组织违规造成的；

（6）有其他严重违反法律法规行为，受到相关行政部门处罚的；

（7）暂停认证证书的期限已满但导致暂停的问题未得到解决或纠正的（包括持有的与 ISMS 范围有关的行政许可证明、资质证书等已经过期失效但申请未获批准）；

（8）没有运行 ISMS 或者已不具备运行条件的；

（9）不按相关规定正确引用和宣传获得的认证信息，造成严重影响或后果，或者中标通已要求其纠正但超过 2 个月仍未纠正的；

（10）其他应当撤销认证证书的。

9.2.2 撤销认证证书后，中标通应及时收回撤销的认证证书。若无法收回，中标通应及时在相关媒体和网站上公布或声明撤销决定。

9.3 认证资格的注销

获证组织主动申请不再保持认证资格时，中标通应注销其认证资格，并保留相应证据。

9.4 认证资格的恢复

暂停期间，如获证组织采取有效的纠正措施，造成暂停的原因已消除的，中标通应恢复其认证资格，并保留相应证据。

9.5 中标通应当在公司网站上公布认证证书暂停、撤销、注销的信息，同时按规定程序和要求报国家认监委。

10.2.1 中标通应及时向认证决定符合要求的组织出具认证证书，认证证书的签发日期不应早于做出认证决定日期。

10.2.2 ISMS 认证证书的有效期最长为 3 年，初次认证证书有效期的起算日期为认证决定日期，再认证证书有效期的起算日期不得晚于最近一次有效认证证书的截止日期。

10.2.3 对每张 ISMS 认证证书应赋予一个认证证书编号，认证证书编号应遵循一定的规律，具体详见附录 F。

10.2.4 认证证书在中华人民共和国境内使用的，证书使用的语言至少应包括中文。

10.2.5 认证证书的信息应真实、准确，不产生误导，并至少包含以下内容：

（1）获证组织名称、统一社会信用代码、注册地址、经营地址/审核地址。若认证的 ISMS 覆盖多场所，表述覆盖的相关场所的名称和地址信息；

注：认证证书中可不包括临时场所，当在认证证书上展示临时场所时， 应注明这些场所为临时场所。

（2）获证组织 ISMS 覆盖的业务范围（认证范围），包含适用性声明；

（3）认证依据的认证标准 ISO/IEC 27001 所采用的当时有效版本的完整标准号；

（4）证书编号（或唯一识别代码）；

（5）首次颁证日期、本次颁证日期、证书有效日期、换证日期（换证时适用）。证书应注明:“在本认证证书有效期内获证组织必须定期接受监督审核并经审核合格此证书方继续有效”的提示信息；

（6）发证机构名称、发证机构地址、签发人等信息；

（7）中标通徽标；

（8）相关的认可标识、认可注册号（获得相关认可时适用）；

（9）证书二维码；

（10）证书信息及证书状态的查询途径。

10.3 认证标志

10.3.1 中标通暂无 ISMS 认证标志。若制定使用 ISMS 认证标志，须符合《认证证书和认证标志管理办法》中认证标志管理规定。认证标志的式样、文字和名称，不得违反法律、行政法规的规定，不得与国家推行的或其他机构自制定并公布的认证标志相同或者相近似，

14.2 记录应当真实准确以证实认证活动得到有效实施。记录资料应当使用中文，保存时间为认证证书有效期届满或者被注销、撤销之日起2年以上。

14.3 以电子文档方式保存记录的，应采用不可编辑的电子文档格式。

14.4 所有具有相关人员签字的书面记录，可以制作成电子文档保存使用，但是原件必须妥善保存，保存时间至少应当与认证证书有效期一致。

15 认证依据变更

15.1 本规则内容提及 ISO/IEC27001 标准时均指认证活动发生时该标准的有效版本。认证活动及认证证书中描述该标准号时，应采用当时有效版本的完整标准号。

15.2 当认证依据有变更时，若国家市场监管部门有统一制订发布的关于 ISMS 认证标准转版要求的，应按国家市场监管部门要求执行，若国家市场监管部门没有统一制订发布认证标准转版要求的，可按照国际标准的转版要求执行，确保组织能够及时获得新版标准认证。

16 信息报送

16.1 中标通应至少在审核实施前3天，将审核计划上报国家认监委相关网站，并应在上报认证证书信息的同时，上报管理体系审核结果信息。

16.2 在颁发认证证书后，应在次月10日前，将认证结果相关信息报送国家认监委。

17 其他

17.1 本规则所提及的各类证明文件的复印件应是在原件上复印的，并经审核员确认是与原件一致。

17.2 中标通可开展 ISMS 及相关技术标准的宣贯培训，促使组织的全体员工正确理解和执行 ISMS 标准。

18 附则

18.1 本规则包含的术语具有如下含义：

18.1.1 申请组织：申请认证并接受认证审核、尚没获得认证的组织；

18.1.2 获证组织：管理体系已获认证的组织。

18.1.3 ISMS 认证业务范围：以 ISMS 相关过程及预期结果的共性为特征的领域。

注：认证业务范围类别与信息安全管理体系范围内的产品、过程和服务有关，认证业务范围也被称作“技术领域”、“行业”等。

附录 A：

ISMS 认证审核时间要求

表 A—ISMS 认证基础审核时间表

有效人数	审核时间 第 1 阶段+第 2 阶段（天）	有效人数	审核时间 第 1 阶段+第 2 阶段（天）
1-10	5	876-1175	18.5
11-15	6	1176-1550	19.5
16-25	7	1551-2025	21
26-45	8.5	2026-2675	22
46-65	10	2676-3450	23
66-85	11	3451-4350	24
86-125	12	4351-5450	25
126-175	13	5451-6800	26
176-275	14	6801-8500	27
276-425	15	8501-10700	28
426-625	16.5	＞10700	遵循上述递进规律
626-875	17.5		

注：1.有效人数包括认证范围内所有班次在组织控制下工作的总人数。在组织控制下工作的人员包括认证范围内所有需要按照 ISMS 要求工作的人员（无论他们是否是组织成员）。

2. 与在组织控制下工作的全职人员相比，在组织控制之下工作的兼职人员与工作时间成比例地贡献了在组织控制范围内工作的人数。该决定应取决于与全职员工相比的工作小时数。

3. 当在认证范围内在组织控制下工作的人员中有很高比例从事某些相同的活动时，应根据与任务相关的活动风险减少执行相同活动的人数。执行每项相同活动的人数的平方根可用于确定用于审计持续时间计算的有效人数，四舍五入到下一个完整人数。该数字应为允许的最大减少人数。

可以减少作为计算基础的执行某些相同活动人数的因素示例包括：

——具有只读权限以执行其职责的信息人员；

——在 ISMS 范围内的无法访问组织信息处理设施的人员；

——执行活动时实施严格限制以限制信息泄露的人，例如禁止个人物品和设备进入工作区域的措

或承认）；

e）高度成熟的管理体系。

宜考虑上述因素，并根据这些因素对审核时间做出调整。这些因素可证实一次有效审核所需更多或更少的审核时间的合理性。增加时间的因素可被减少时间的因素冲抵。在任何情况下，对审核时间表中的时间的调整，应保持足够的证据和记录来证实其变化的合理性。

d）在 ISMS 各部分的实施过程中，所应用的技术的水平和多样性[例如，不同 IT 平台的数量、隔离网络的数量]；	●高标准化、低多样性的环境（很少的 IT 平台、服务器、操作系统、数据库、网络等）；	●标准化且多样性的 IT 平台、服务器、操作系统、数据库和网络；	●高多样性或复杂的 IT 环境（例如，很多不同的网段、服务器或数据库的类型、关键应用的数量）
e）ISMS 范围内所使用的外包和第三方安排的程度；	●没有外包且对供应商的依赖较小，或； ●对外包协议进行了明确的规定、良好的管理与监视； ●外包方获得了 ISMS 认证； ●可获得相关的独立担保报告。	●多个管理不充分的外包协议；	●高度依赖外包或供应商，它们对重要业务活动有很大影响；或， ●对外部的数量或程度不清楚； ●多个未得到管理的外包协议；
f）信息系统开发的程度；	●没有内部的系统开发 ●使用标准化的软件平台	●使用标准化的、具有复杂配置/参数化的平台； ●（高度）定制软件； ●若干开发活动（内部的或外包的）	●大量的内部软件开发活动，有若干针对重大业务目的的、持续进行的项目。
g）场所的数量和灾难恢复场所的数量；	●较低的可用性要求，且没有或有一个可选的灾难恢复场所；	●中等或高的可用性要求，且没有或有一个可选的灾难恢复场所；	●高可用性要求，例如 7×24 服务； ●若干个可选的灾难恢复场所； ●若干个数据中心；
h）对于监督或再认证审核：符合 CNAS-CC01-2015 8.5.3 条款的、与 ISMS 相关的变更的数量和程度。	●自上次再认证审核后未发生变化；	●ISMS 的范围或 SoA 有微小的变化，例如，一些策略、文件发生变化； ●以上因素有微小变化；	●ISMS 的范围或 SoA 有重大变化，例如，新的过程，新的业务单元，风险评估管理方法、策略，文件、风险处置。 ●以上因素有重大变化；

B.3 审核时间计算步骤

审核时间计算根据审核时间计算因数分类，按照参考公式计算，具体步骤如下。

第一步：确定与业务和组织相关的（非IT）因数，识别下表中每个类别的适宜分值，并对结果值求和。

	很大影响。
信息系统的开发	1.没有或非常有限的内部系统应用开发； 2.有一些服务于某些重要业务目的的、内部的或外包的系统/应用开发； 3.有大量服务于重要业务目的、内部的或外包的系统/应用开发。

第三步：基于以上第一步、第二步的结果，通过选择下表中的适宜条目，识别这些因数对审核时间的影响。

表B.4—因数对审核时间的影响表

IT复杂性 / 业务复杂性	低（3-4）	中（5-6）	高（7-9）
高（7-9）	+5%～+20%	+10%～+50%	+20%～+100%
中（5-6）	-5%～-10%	0%	+10%～+50%
低（3-4）	—10%～-30%	-5%～-10%	+5%～+20%

第四步：最终计算。将基础审核时间乘以第三步中得出的系数，确定最终审核时间。当利用多场所抽样时，要根据执行多场所抽样计划所需的工作量增加所计算出的审核人天。

审核时间计算示例：

示例1：受审核组织有700人，因此根据基础审核时间表A.1标准，初次认证审核需要17.5人天。该组织不属于关键业务领域，从事高度标准化和重复性的任务且刚建立ISMS。根据与业务和组织（非IT）相关的因数表，可以得出与业务和组织相关的因子为1+1+3=5。该组织具有非常少的IT平台和数据库，但大量的使用外包，该组织没有内部的或外包括的开发活动，根据与IT环境相关的因数表，可以得出与IT环境相关的因子为1+3+1=5。根据因数对审核时间的影响表，可以得出审核时间无需调整。

示例2：仍然是示例1的组织，但其已有多个管理体系且已较好地建立了ISMS。根据与业务和组织（非IT）相关的因数表，可以得出与业务和组织相关的因子为1+1+1=3。根据因素对审核时间的影响表，可得出需要减少5%~10%的审核时间。即审核审核时减少1~1.5天，变为16到16.5人天。

（1）一套整合的文件，适宜时，包括适度融合的作业文件；

（2）考虑总体经营战略和计划的管理评审；

（3）对内部审核采用的一体化方法；

（4）对方针和目标采用的一体化方法；

（5）对体系过程采用的一体化方法；

（6）对改进机制（纠正和预防措施、测量和持续改进）采用的一体化方法；

（7）一体化的管理支持和管理职责。

注 2：图中横坐标为审核组承担结合审核能力的水平。可参考如下公式计算：

审核组结合审核能力水平=[(X1-1)+(X2-1)+(X3-1)+…+(Xn-1)]/[Z(Y-1)]×100%

式中 X1、X2…Xn 代表审核组中每位审核员有能力承担管理体系审核领域的数量；

式中 Z 为结合审核组中审核员的数量；

式中 Y 为结合审核所覆盖的整合管理体系的数量。

注 3：图中数值代表该区域可缩减的结合审核人天数占结合审核人天数起始点（T）的百分数。

注 4：结合审核人天数的起始点应为各单一管理体系的审核人天数之和。其中每个单一管理体系审核人日数(Sn)是针对单一管理体系考虑了增加或减少审核人天数因素后确定的时间值（注：这里不能把结合审核作为减少单一管理体系审核人天数的一个因素）。

C.3 结合审核时间确定

结合审核时间应为结合审核人天数的起始点减去按照 C.2 确定的减少量，无论如何，不宜使结合审核人日数少于起始点的 80%。

注：中标通可以在此基础上根据使组织产品（包括服务）满足信息资产安全管理要求和适用的法律法规要求所必需的过程的类别来进一步划分 ISMS 认证业务范围的类别。

表 D.2 ISMS 风险类型示例

风险等级	认证业务范围
一级风险	信息资产涉及范围非常广泛、保密要求高，信息安全管理失效导致的损失巨大、影响非常广泛，包括但不限于：国家机构；税务机关；海关；通信、广播电视；新闻出版（包括互联网内容的提供）；金融（例如银行、证券、期货、保险、资产管理等）；电子商务（以在线交易为主要特点，含网络游戏）；物流（包括邮政）；电力（包括发电和输、变、配电等）；铁路；民航；化工；航空航天；水利。
二级风险	信息资产涉及范围较广、有较高的保密要求，信息安全管理失效导致的损失大、影响广泛，包括但不限于：其他政务（例如政党、政协、社会团体等）；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）；医疗服务；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）；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）；冶金；采矿（含石油、天然气开采）；食品、药品、烟草。
三级风险	信息资产涉及范围有限、保密要求一般，信息安全管理失效导致的损失较小、影响一般，包括但不限于：教育；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）】； 咨询中介（例如法律、会计、审计、公证等）；旅游、宾馆、饭店；其他商务；农、林、牧、副、渔业；其他产品生产（包括一般工业产品、建设工程施工、工程技术服务等）。

信息科学、统计学、应用统计学、电气工程及其自动化、电子信息工程、电子科学与技术、通信工程、微电子科学与工程、光电信息科学与工程、信息工程、自动化、计算机科学与技术、软件工程、网络工程、信息安全、物联网工程、数字媒体技术、信息管理与信息系统、审计学、信息资源管理、电子商务、集成电路设计与集成系统、电子信息科学与技术、电信工程及管理、智能科学与技术、空间信息与数字技术、电子与计算机工程、密码学、人工智能等专业。

注：专业名称如有差异或发生变化，以教育部本科或研究生学科目录为准。

换证日期。

F.4　再认证完成后换发证书，按F.1规定重新赋予认证证书编号。

F.5　撤销证书后，原认证证书编号废止，不再它用。