鹰企认证服务（上海）有限公司
Ench Inspection & Certification （Shanghai）Co., Ltd.

信息安全管理体系认证规则

编 制 / 日 期： 寻爱凌/2025.6.17

审 核 / 日 期： 钱晔/2025.6.17

批 准 / 日 期： 钱晔/2025.6.17

1 适用范围

为规范鹰企认证服务（上海）有限公司（以下简称“公司”或“鹰企认证”）对信息安全管理体系认证的要求，特制定本认证规则，并与鹰企认证程序等各级各类文件相对应，共同规范和指导鹰企认证的信息安全管理体系认证业务。

2 引用标准

本认证规则下的信息安全管理体系认证全过程活动以 ISO/IEC 27001:2022《网络安全技术 信息安全管理体系 要求》为认证依据。

CNAS-CC01《管理体系认证机构要求》

CNAS-GC01《认证证书管理实施指南》

CNAS-GC02《管理体系认证的结合审核管理实施指南》

CNAS-CC105 《确定管理体系审核时间》

CNAS-CC11 《多场所组织的管理体系审核与认证》

CNAS-CC12 《已认可的管理体系认证的转换》

认可机构发布的其它认可准则、规则及指南等

注：认证依据以国家或国际标准的现行有效版本为准。

3 定义与术语

3.1 同 ISO/IEC 27001:2022《网络安全技术 信息安全管理体系 要求》的术语。

3.2 现场审核

中心指派审核组到受审核组织所在地点进行的审核活动。

3.3 远程审核

应用信息和通信技术(ICT)，在受审核活动的实际场所以外任何地点实施的审核。

注 1:ICT 是应用技术来收集、存储、检索、处理、分析和发送信息，它包括软件和硬件，例如:智能手机、手持设备、笔记本电脑、台式电脑、无人机、摄像机、可穿戴技术、人工智能及其他。

注 2:远程审核可以是审核人员在受审核方某一场所对其他场所的人员、活动或过程进行的审核，也可以是审核人员不在受审核方场所对受审核方的人员、活动或过程进行的审核。

3.4 特殊审核

扩大认证范围或提前较短时间通知的审核。

3.5 审核类别和审核方式

审核类别分为初次认证审核（包括一阶段和二阶段审核）、监督审核、再认证审核和特殊审核。审核方式分为现场审核、远程审核。

3.6 审核人员、技术专家、审核组要求

审核人员必须取得认证注册资格，并得到中心的专业能力评价，以确定其能够胜任所安排的审核任务。技术专家必须得到中心的专业能力评价，以确定其能够胜任所安排的技术支持工作。审核组应由能够胜任所安排的审核任务的审核员组成。必要时可以补充技术专家以增强审核组的技术能力，技术专家应在审核员的监督下进行工作，可就受审核组织管理中技术充分性事宜为审核员提供建议，但技术专家不能作为审核员。

4 控制要求

4.1 认证申请的评审

收到《管理体系认证申请表》后，由业务员会同审核方案管理人员对认证申请进行以下内容的评审，以确定是否有能力满足申请方提出的要求：

1）所需要的基本信息都得到提供；

2） 申请组织的行业类别和与之相对应的业务过程特性和要求；

3） 国家对相应行业的管理要求；

4） 申请组织管理体系运行时间满三个月，已完成内部审核和管理评审；

5） 公司与申请组织之间任何已知的理解差异得到消除；

6） 公司有能力并能够实施所申请的认证活动；

7） 申请的认证范围、申请组织的运作场所、完成审核需要的时间和任何其他影响认证活动的因素；

8）核算并确定审核人日；

9）根据申请认证的活动范围及场所、从事活动的影响、员工人数、完成审核所需时间和其他影响认证活动的因素，综合确定是否有能力受理认证申请。

并将上述评审结果记录于《认证申请评审及审核方案策划表》中。

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，鹰企认证不受理其认证申请。

4.2 审核人天的确定

4.2.1 若申请认证组织在其控制的不同场所以同样的方式从事申请认证范围的活动时，应识别认证的管理体系所覆盖活动的复杂性和规模以及场所间的不同，作为确定抽样水平的基础。

4.2.2 单一场所的认证在确定审核人天时，现场审核时间、总时间应至少满足附件 1 所规定的要求。附件 1 所列的是以申请认证组织的员工人数为基点确定的审核员时间，根据申请认证组织的规模、评审范围、后勤、组织的复杂程度以及组织准备接受评审的情况，考虑到组织体系、过程和产品/服务方面所有的特征，对现场审核时间进行合理的调整，以便对组织实施有效的审核。如果因下列原因需要增加或减少现场审核时间，应在合同评审过程中作说明。

a）需要增加审核员时间的因素：

1）组织的工作在多于一处的建筑物或地点实施，审核时需要复杂的后勤安排，例如必须对一个单独的设计中心实施审核；

2）员工使用多于一种的语言（需要翻译或妨碍单个审核员独立工作）；

3）与人员数量相比，现场很大（例如无人作业车间面积广、森林）；

4）受法规管制的程度较高（例如食品、药品、航天、核能等领域）；

5）体系覆盖着高度复杂的过程或数量较多的互不相同的活动；

6）需要访问临时场所，以确认拟认证管理体系中的常设场所的活动。

b）允许减少审核员时间的因素：

1）组织的规模较小、信息安全特性不高、持续时间不长、业务复杂程度低、管理涵盖的范围较小、认证要求和其承担的风险较低以及所采取审核方式；

2）与人员数量相比，现场很小（例如仅有综合办公区）；

3）管理体系成熟；

4）把两个或多个兼容的管理体系整合起来的一体化体系实施结合审核；

5）对客户管理体系已有的了解（例如同一认证机构已依据另一标准认证了该客户）；

6）客户为认证所作的准备（例如已经获得另一个第三方合格评定制度的认证或承认）；

7）活动的复杂程度低，例如：

- 过程仅包含单一的一般性活动（例如仅包含服务）；
- 所有班次都实施相同的活动，且有适当证据表明所有班次的表现相同；

➢相当一部分员工从事相似的简单职能；

8）有一部分员工在组织的场所外工作，例如销售人员、司机、服务人员等，并且有可能通过记录审查来对其活动是否符合体系要求进行充分地审核；

9）低风险的产品或过程。

4.3.3 导致增加的因素可以和导致减少的因素相抵消。由上述因素引起的审核人日数的减少的总量不应超过规定审核人日数的 30%。整个审核时间中，现场审核时间不应少于总审核时间的 80%。通常情况下一阶段和二阶段现场审核时间比例为 3:7。第二阶段审核时间通常情况下不应少于 1 个审核人日，否则可能影响审核有效性。

4.4 多场所申请组织审核时间的确定

4.4.1 如果满足多场所抽样审核的条件，抽样审核应满足附件 1 的要求。如果不能满足多场所抽样审核的条件，则在初次审核及后续的再认证审核中应对所有场所进行完整的审核，在后续的监督审核中可以对这些场所进行抽样审核。

4.4.2 确定审核时间时宜综合考虑客户管理体系覆盖的区域、活动、产品和服务的所有属性，合理调整审核时间，同时能够证明审核时间的增加或减少对于有效审核是合理的。

4.5 认证审核的安排

认证审核由第一阶段审核（包括文件和资料审核、现场审核）、第二阶段审核（现场审核）。通常情况下要求第一阶段审核活动应在申请认证组织的场所进行，若受审核方属产品、服务实现过程比较简单，且规模很小，经审核方案管理人员评审，在第二阶段现场审核能充分保证审核的深度和有效性的前提下，第一阶段审核可不安排现场访问。

4.5.1 审核方案管理及审核实施

4.5.1.1 对整个认证周期制定审核方案，以清晰地识别所需的审核活动，这些审核活动用以证实客户的管理体系符合认证所依据标准或其他规范性文件的要求。

4.5.1.2 审核方案应包括两阶段初次审核、第一年与第二年的监督审核和第三年在认证到期前进行的再认证审核。三年的认证周期从初次认证或再认证决定算起。审核方案的确定和任何后续调整应考虑客户组织的规模，其管理体系、产品和过程的范围与复杂程度，以及经过证实的管理体系有效性水平和以前审核的结果。

4.5.1.3 如果考虑客户已获得认证或接受的其他审核，则应收集充足的、可验证的信息，以证明对审核方案的任何调整的合理性，并予以记录。

4.5.1.4 信息安全管理体系的审核方案管理按《认证审核策划程序》执行；审核实施按《认

证审核实施程序》、《监督审核及再认证程序》执行。

4.5.2 审核组组成

4.5.2.1 有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）的过程。审核组由满足 ISO/IEC17021 对审核组长能力要求的审核员担任审核组长并负责领导审核组，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)审核目的、范围、准则和预计的审核时间；

b)是否是结合审核或联合审核；

c)实现审核目的所需的审核组整体能力；

d)认证要求（包括任何适用的法律、法规或合同要求）；

e)语言和文化；

f)审核组成员以前是否审核过该客户的管理体系。

4.5.2.2 当安排实习审核员进行审核见习时，参加见习的实习审核员的人数不应超过审核组中级别审核员的总数，并要指派一名审核员作为评价人员。评价人员应有能力接管实习审核员的作务，且对实习审核员的活动和审核发现最终负责；实习审核员不应当在没有指导和帮助的情况下进行审核。

4.5.3 文件审核

文件审核中应对申请认证组织提出的有关标准要求不适用的适宜性进行审查，并在现场审核期间进一步验证不适用的合理性。必要时，可采取沟通或现场核实等适宜的方式验证申请认证组织对法律法规和过程识别的充分性。

4.5.4 审核计划

4.5.4.1 组长严格按照审核策划结果及组长任命书要求安排审核计划；应确保为审核方案中确定的每次审核编制审核计划，以便为有关各方就审核活动的日程安排和实施达成一致提供依据；

4.5.4.2 除了满足本须知对审核计划的其它要求之外，还应在审核计划中注明远程审核 的审核员、审核时间、场所、部门、过程等必要内容；

4.5.4.3 对于多场所的认证审核，如果满足多场所抽样审核的条件，应依据附件 1 的要求进行抽样，策划审核方案，安排审核计划。如果不能满足多场所抽样审核的条件，则应针对所有场所策划审核方案，安排审核计划。

4.5.4.4 审核计划应明确对信息资产识别、信息安全风险识别及评价、针对高级风险削 减计划以及计划落实情况；审核计划应考虑所确定的信息安全控制。

4.5.4.5 针对远程审核，执行远程审核的要求见本须知远程审核；

4.5.4.6 确定审核目的、范围和准则

1） 审核目的应由认证机构确定。审核范围和准则包括任何更改应由认证机构在与客户商讨后确定。

2） 审核目的应说明审核要完成什么，并应包括下列内容：

a)确定客户管理体系或其部分与审核准则的符合性；

b)评价管理体系确保客户组织满足适用的法律、法规及合同要求的能力，（注：管理体系认证审核不是合规性审核）；

c)评价管理体系确保客户组织持续实现其规定目标的有效性；

d)适用时，识别管理体系的潜在改进区域。

3） 审核范围应说明审核的内容和界限，例如拟审核的实际位置、组织单元、活动及过程。当初次认证或复审过程包含一次以上审核（例如覆盖不同位置的审核）时，单次审核的范围可能并不覆盖整个认证范围，但整个审核所覆盖的范围应与认证文件中的范围一致。

4） 审核准则应被用作确定符合性的依据，并应包括：

---所确定的管理体系规范性文件的要求；

---所确定的由客户制定的管理体系的过程和文件。

4.5.4.7 编制审核计划

1） 审核计划应与审核目的和范围相适应。审核计划至少应包括或引用：

a)审核目的；

b)审核准则；

c)审核范围，包括识别拟审核的组织和职能单元或过程；

d)拟实施现场审核活动（适用时，包括对临时场所的访问）的日期和场所。审核计划应明确对信息资产识别、信息安全风险识别及评价、针对高级风险削减计划以及计划落实情况；审核计划应考虑所确定的信息安全控制。

e)现场审核活动预期的时间和持续时间；

f)审核组成员及与审核组同行的人员的角色和职责。

（注：审核计划的信息可以包含在一个以上的文件中。）

2） 审核组长和审核员所需的知识和技能可以通过技术专家和翻译人员补充，技术专家和翻译人员应在审核员的指导下工作，使用翻译人员时，翻译人员的选择要避免他们对审核产生不正当影响，技术专家的选择准则根据每次审核的审核组和审核范围的需要为基础确定。审核组内具备专业能力的审核员或技术专家介绍审核范围所覆盖的特定活动、 产品和服务的信息安全要求，控制技术，活动相关的规程和其潜在的信息安全风险以及有关适用的法律法规、标准。

3） 审核组长在与审核组商议后，应向每个审核组成员分配对特定过程、职能、场所、区域或活动实施审核的职责。所进行的分配应考虑到所需的能力、有效并高效地使用审核组以及审核员、实习审核员和技术专家的不同作用和职责。在审核进程中，为确保实现审核目的，可以改变工作分配。

4.5.4.8 确定审核时间

1） 认证机构应有形成文件的确定审核时间的程序，并针对每个客户确定策划和完成对其管理体系的完整有效审核所需的时间。认证机构应记录所确定的时间及其合理性。在确定审核时间时，认证机构应考虑（但不限于）以下方面：

a)相关管理体系标准的要求；

b)规模和复杂程度；

c)技术和法规环境；

d)管理体系范围内活动的分包情况；

e)以前审核的结果；

f)场所的数量和对多场所的考虑；

g)与组织的产品、过程或活动相关联的风险；

h)是否是结合审核、联合审核。

2） 未被指派为审核员的审核组成员（即技术专家、翻译人员、观察员和实习审核员）所花费的时间不应计入上面所确定的审核时间。

4.5.5 实施现场审核

鹰企认证有实施现场审核的过程。该过程应包括审核开始时的首次会议和审核结束时的末次会议。注：除了访问有形场所（如工厂）外，“现场” 还可以包括远程访问包含管理体系审核相关信息的电子化场所。

4.5.5.1 召开首次会议

与客户的管理层（适用时，还包括拟审核职能或过程的负责人员）召开正式的首次会议，并记录参加人员。首次会议通常应由审核组长主持，会议目的是简要解释将如何进行审核活动，并应包括下列要素。详略程度可与客户对审核过程的熟悉程度相一致：

a)介绍参会人员，包括简要介绍其角色；

b)确认认证范围；

c)确认审核计划（包括审核的类型、范围、目的和准则）及其任何变化，以及与客户的其他相关安排，例如末次会议的日期和时间，审核期间审核组与客户管理层的会议的日期和时间；

d)确认审核组与客户之间的正式沟通渠道；

e)确认审核组可获得所需的资源和设施；

f)确认与保密有关的事宜，澄清是否存在不能提供给审核组的包含保密性或敏感性信息的 ISMS 记录或限制条件；

g)确认适用于审核组的相关的工作安全、应急和安保程序；

h)确认可得到向导和观察员及其角色和身份；

i)报告的方法，包括审核发现的任何分级。如果审核组得出不对已识别的保密性或敏感性的记录进行核查就不能对 ISMS 进行充分审核的结论，就应告知客户，并只有获得适当的访问安排许可时才能进行认证审核；

j)说明可能提前终止审核的条件；

k)确认审核组长和审核组代表认证机构对审核负责，并应控制审核计划（包括审核活动和审核路径）的执行；

l)适用时，确认以往评审或审核的发现的状态；

m)基于抽样实施审核的方法和程序。为了得到充分地审核，告知哪些ISMS记录必须在审核中查核；

n)确认审核中使用的语言；

o)确认在审核中将告知客户审核进程及任何关注点；

p)让客户提问的机会。

4.5.5.2 审核中的沟通和限制条件

1） 在审核中，审核组应定期评估审核的进程，并沟通信息。审核组长应在需要时在审核

组成员之间重新分配工作，并定期将审核进程及任何关注告知客户。

2） 当可获得的审核证据显示审核目的无法实现，或显示存在紧急和重大的风险（例如安全风险）时，审核组长应向客户和鹰企认证报告这一情况，以确定适当的行动。该行动可以包括重新确认或修改审核计划，改变审核目的或审核范围， 或者终止审核。审核组长应向鹰企认证报告所采取行动的结果。

3） 如果在现场审核活动的进行中发现需要改变审核范围，审核组长应与客户审查该需要，并报告鹰企认证。

4）审核组应满足客户提出的保密性或敏感性的限制条件，否则不应在认证活动中接触组织的相关信息资产。如果审核组因为未获得组织的允许或无法满足适用的要求而不能接触相关信息资产，那么审核组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）并向机构业务运营管理部报告。

5）如果客户事先没有禁止CCSC及审核组接触某一信息资产，或未告知应满足的要求，但禁止CCSC及审核组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。如组织有要求，审核组成员应按照组织的保密要求与组织签署保密协议，或向 组织做出保密承诺。

6）审核组成员不宜在审核过程中以任何方式记录受审核组织的保密或敏感信息。审核组在离开受审核组织前，宜请受审核组织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组织的任何保密或敏感信息。

4.5.5.3 观察员和向导

4.5.5.3.1 观察员

鹰企认证与客户应在实施审核前就审核活动中观察员的到场及理由达成一致。审核组应确保观察员不影响或不干预审核过程或审核结果。（观察员可以是客户组织的成员、咨询人员、实施见证的认可机构人员、监管人员或其他有合理理由的人员。）

4.5.5.3.2 向导

每个审核员应由一名向导陪同，除非审核组长与客户另行达成一致。为审核组配备向导是为了方便审核。审核组应确保向导不影响或不干预审核过程或审核结果。

注：向导的职责可以包括：

a)为面谈建立联系或安排时间；

b)安排对现场或组织的特定部分的访问；

c)确保审核组成员知道并遵守关于现场安全和安保程序的规则；

d)代表客户观察审核；

e)应审核员请求提供澄清或信息。

4.5.5.4 收集和验证信息

1）在审核中应通过适当的抽样来收集与审核目的、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。

信息收集方法应包括（但不限于）：

a)面谈；

b)对过程和活动进行观察；

c)审查文件和记录。

2）审核过程中，除采用管理体系审核的证据收集的一般方法和技巧外，信息安全管理体系还应通过如下方式获得审核证据：

a)对控制措施直接测试（或重新实施）：技术类的控制措施的绩效证据可以通过系统测试（见下面），或者通过使用专门的审核和（或）报告工具，进行收集。

（1） “系统测试”意味着对系统的直接评审（例如，系统设置或配置的评审）。对于审核员的提问，可以在系统控制台回答，也可以通过对测试工具的结果的评价来回答。

（2） 如果客户组织使用了基于计算机的工具，这种工具又恰是审核员所熟悉的， 那么可以使用该工具以支持审核，或者核查客户组织（或其的分包方）所完成的评价结果。

b) 执行远程审核：审核员除了按照本须知的要求做好审核记录之外，远程审核的记 录可以包括下载的电子文档或图片等。

4.5.5.5 确定和记录审核发现

4.5.5.5.1 审核发现应简述符合性，详细描述不符合以及为其提供支持的审核证据，并予以记录和报告，以便为认证决定或保持认证提供充分的信息。

4.5.5.5.2 可以识别和记录改进机会，但是属于不符合的审核发现不应作为改进机会予以记录。

4.5.5.5.3 关于不符合的审核发现应对照审核准则的具体要求予以记录，包含对不符合的清晰陈述，并详细标识不符合所基于的客观证据。应与客户讨论不符合，以确保证据准确

且不符合得到理解。但是应避免提示不符合的原因或解决方法。

4.5.5.5.4 审核组长应尝试解决审核组与客户之间关于审核证据或审核发现的任何分歧意见，未解决的分歧点应予以记录。

4.5.5.6 准备审核结论

在末次会议前，审核组应：

a)对照审核目的审查审核发现和审核中收集的任何其他适用的信息；

b)考虑审核过程中内在的不确定性，就审核结论达成一致；

c)确定任何必要的跟踪活动；

d)确认审核方案的适宜性，或识别任何所需要的修改（例如范围、审核时间或日期、监督频次、能力）。

4.5.5.7 召开末次会议

4.5.5.7.1 应与客户的管理层（适用时，还包括所审核的职能或过程的负责人员）召开正式的末次会议，并记录参加人员。末次会议通常应由审核组长主持，会议目的是提出审核结论，包括关于认证的推荐性意见。不符合应以使其被理解的方式提出，并应就回应的时间表达成一致。（“被理解”不一定意味着客户已经接受了不符合。）

4.5.5.7.2 末次会议还应包括下列要素。详略程度应与客户对审核过程的熟悉程度一致：

a)向客户说明所收集的审核证据基于对信息的抽样，因而会有一定的不确定性；

b)进行报告的方法和时间表，包括审核发现的任何分级；

c)认证机构处理不符合（包括与客户认证状态有关的任何结果）的过程；

d)客户为审核中发现的任何不符合的纠正和纠正措施提出计划的时间表；

e)认证机构在审核后的活动；

f)说明投诉处理过程和申诉过程。

4.5.5.7.3 客户应有机会提出问题。审核组与客户之间关于审核发现或结论的任何分歧意见应得到讨论并尽可能获得解决。任何未解决的分歧意见应予以记录并提交鹰企认证。

4.5.5.8 审核报告

鹰企认证为每次审核提供书面报告。审核组可以识别改进机会，但不应提出具体解决办法的建议。鹰企认证享有对审核报告的所有权。

审核组长应确保审核报告的编制，并应对审核报告的内容负责。审核报告应提供对审核的准确、简明和清晰的记录，以便为认证决定提供充分的信息， 并应包括或引用下列内容：

a)注明认证机构；

b)客户的名称和地址及其管理者代表；

c)审核的类型（例如初次、监督或再认证审核）；

d)审核准则；

e)审核目的；

f)审核范围，特别是标识出所审核的组织或职能单元或过程，以及审核时间；

g)注明审核组长、审核组成员及任何与审核组同行的人员；

h)（现场或非现场）审核活动的实施日期和地点；

i)与审核类型的要求一致的审核证据、审核发现和审核结论，涉及到老鹰认证标志的分级认证推荐结论应有审核组分级评价表；

j)已识别出的任何未解决的问题。

4.5.5.9 不符合的原因分析

对于审核中发现的不符合，鹰企认证要求获证组织在规定期限内分析原因，并说明为消除不符合已采取或拟采取的具体纠正和纠正措施。

4.5.5.10 纠正和纠正措施有效性的验证

鹰企认证审查获证组织提交的纠正和纠正措施，以确定其是否可被接受；验证所采取的任何纠正和纠正措施的有效性。所取得的为不符合的解决提供支持的证据应予以记录，对不符合的解决进行审查和验证的证据应予以记录，将审查和验证的结果告知获证组织。

注：可以通过审查客户提供的文件，或在必要时实施现场验证来验证纠正和纠正措施的有效性。

4.5.6 补充审核

如果需要进行全面或部分的补充审核，或需要形成文件的证据（在将来的监督审核中予以确认），以验证纠正和纠正措施的有效性，则鹰企认证告知受审核的组织。

4.5.7 认证决定

鹰企认证确保做出合格评定的人员不是实施审核的人员。

鹰企认证在做出决定前确认：

1)审核组提供的信息足以确定认证要求的满足情况和认证范围；

2)对于所有反映以下问题的不符合，机构已评审、接受并证实了纠正和纠正措施的有效性：

a)未能满足管理体系标准的一项或多项要求；或

b)使人对客户管理体系实现预期结果的能力产生重大怀疑的情况；

3)对于任何其他不符合，鹰企认证评审并接受了客户计划采取的纠正和纠正措施。

4.6 初次认证

4.6.1 第一阶段审核

4.6.1.1 第一阶段审核的目的：

1）收集组织基本情况信息，包括：组织机构职能、现场分布、产品及生产过程、适用标准和法规、行业地位等，评价组织管理体系基础，确定审核范围；

2）确定组织是否已按约定标准要求策划建立并运行了信息安全管理体系，是否为接受第二阶段审核做好准备；

3）了解组织关键绩效和关键生产/服务过程运行，确定第二阶段审核重点、审核日期和资源需求。

4.6.1.2 第一阶段审核内容：

a） 文件的符合性、适宜性和充分性；

b）适用法律、法规的识别情况及在相关文件中落实法律、法规的情况；

c）与申请组织就认证范围再次确认，了解申请组织为接受第二阶段审核的准备情 况，并商定第二阶段的审核安排；

d） 确认客户组织 ISMS 范围和边界的界定是否清晰和充分。

e）申请组织内部审核和管理评审的实施情况。

4.6.1.3 确定审核范围

1）确定审核范围时，审核组应确保根据客户组织的业务、组织、位置、资产和技术的特点清晰地确定其 ISMS 的范围和边界。审核组应确保按照 ISMS 标准GB/T22080 (IDT ISO27001)的要求，客户组织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，并应在适用性声明中得到体现。

2）确定审核范围时，审核组应确定客户组织的信息安全风险评估中包括了与不完全属于 ISMS 范围内的服务或活动的接口，界定不完全属于 ISMS 范围内的服务或活动的接口关系。

3）组织 ISMS 范围和边界的界定：组织 ISMS 的范围和边界宜从业务、组织、技术、物理和资产五个方面来定义。

a） 业务范围和边界的界定

（1)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。

（2)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。

b） 组织范围和边界的界定

（1)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。

（2)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。

（3)在界定组织范围和边界时，客户组织宜考虑以下因素：

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 PDCA 管理所涉及的所有职能和部门均已纳入管理体系范围。如某客户组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宜纳入到其 ISMS 范围；

② 信息安全管理委员会/管理机构宜包括与 ISMS 直接相关的管理人员；

③ 对 ISMS 负责的管理层人员宜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 的角色不是高层管理人员，则有必要让一名来自最高管理层组织高层的发起人来作为信息安全利益的代表，并在组织的最高层作为 ISMS 的代言人；

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。

（4)基于以上考虑，在界定组织的边界时，宜识别 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，这些依赖关系宜清晰地形成文件。

c） 确定物理范围和边界

（1)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。

（2)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。

（3)在考虑以上因素的基础上，物理范围和边界的描述一般宜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。

（4)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。

（5)公司在确定客户组织审核范围时宜考虑其临时场所和异地备份地点的情况。对临时场所一般宜到现场进行审核，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。

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

d） 确定资产范围和边界

（1)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。

（2)在确定客户组织的资产范围和边界时，宜考虑以下因素：

资产范围宜包括软件资产、硬件资产、数据资产、文件资产、人员资产及服务资产等方面；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。

e） 确定技术范围和边界

（1)技术范围和边界主要是指客户组织所使用的信息与通信技术（ICT）和其它技术的范围和边界，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宜纳入组织 ISMS 范围。

（2)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）。

（3） 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。

（4)当上述内容不是由客户组织自行控制时，宜将对第三方的依从关系用文件清晰定义。

（5)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，宜提供排除的理由。

4）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：

a） 组织的关键特征(组织的职能部门、组织结构、服务、资产以及各资产的责任范围和边界等)；

b） 范围内的组织的过程；

c） 范围内的设备和网络的配置；

d） 范围内的信息资产列表；

e） 范围内的信息通信技术资产（例如服务器）列表；

f） 范围内的场所位置图，并指出组织 ISMS 的物理边界；

g） ISMS 范围内的角色和职责描述，以及其与组织结构的关系；

h） 对于 ISMS 范围的任何删减的细节和正当性理由。

4.6.1.3 ISMS 第一阶段审核报告

第一阶段审核结果应形成书面报告。ISMS 第一阶段审核报告还应关注：

a）第一阶段审核组长应在第一阶段审核报告中明确引用的适用性声明的特定版 本，确认其采用程度和删减合理性，提出第二阶段审核组成员能力要求。

b）第一阶段审核报告中应说明不完全属于 ISMS 范围内的服务或活动的接口关系。

c）根据客户组织的业务、组织、位置、资产和技术的特点，确定第二阶段审核需进行远程审核的场所、部门、过程等必要内容；

d）如第一阶段采用了远程审核方式，报告中还应包括对本次远程审核完成的情况 及效果的说明，并对下次审核时的远程审核提出建议，可行时做出策划；

e）在第一阶段审核报告中明确提示在第二阶段的审核中，可能需要进一步提供信息和记录以供详细检查。

f）在二阶段之前，应评审一阶段审核报告，以确认第二阶段审核小组成员是否具备必要的能力。这一评审可以由能力适当的一阶段审核组长执行，必要时由不参与审核的认证人员进行独立评审。如发现问题，应及时与审核策划人员沟通，以进行必要调整。

4.6.1.4 对于文件审核发现的问题和第一阶段审核发现的问题，应要求受审核方纠正或采取纠正措施并将有关证据提交审核组，经审核组验证合格后才能进行第二阶段审核。

4.6.1.5 若审核组通过第一阶段的审核，认为原定的第二阶段审核时间难以保证审核的深度和充分性，审核组长应向审核委派人员提出第二阶段审核人天的调整意见。审核委派人员应会同审核方案管理人员根据审核组长建议的审核时间确认第二阶段审核所需人天数，并由业务员与客户进行沟通，增加第二阶段现场审核时间。

4.6.2 第二阶段审核

4.6.2.1 第二阶段审核目的：

1）证实受审核方实施了信息安全方针、目标，并遵守了相应的程序。

2）确认客户组织的 ISMS 符合规范性 ISMS 标准的所有要求，并正在实现客户组织依据方针所制定的目标。

3)通过在申请组织的现场进行系统、完整地审核，评价申请组织的信息安全管理体系是否满足所有适用的认证依据的要求，是否推荐认证注册。

4.6.2.2 第二阶段审核重点：

a） 确定客户组织的 ISMS 满足 GB/T 22080(IDT ISO27001)标准的要求以及客户组织的策略与目标。

b） 审核与信息安全有关的风险评估，及评估能产生可比较和可再现的结果；

c） 识别、检查和评价有关客户组织的与信息安全有关的资产威胁、脆弱性及影响的规程与执行情况，包括符合 ISMS 标准中所列要求的文件/规程；

d）评价基于风险评估与风险处置过程，对控制目标与控制措施的选择的适应性；控制措施的有效性分析、业务连续性管理；

e）ISMS 有效性的评审和信息安全控制措施有效性的测量，以及对照 ISMS 目标进行的报告和评审；

f） ISMS 内部审核和管理评审；

g）针对信息安全方针的管理职责；

h）所选择和实施的控制措施、适用性声明及风险评估和风险处置过程的结果相互之间的一致性，以及它们与 ISMS 方针和目标之间的一致性；

i） 控制措施的实施，考虑客户组织对控制措施的有效性的测量，以确定控制措施是否得以实施并在达到所声明的目标方面是有效的；

j） 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。

4.6.2.3 当审核中发现 ISMS 中的安全事件时，审核组应将客户组织 ISMS 中的安全事件现象追溯到 ISMS 的相应要素；

4.6.2.4 ISMS 审核的特定要点

a） 确定客户组织证实对信息安全威胁的分析与组织的运行是相应和充分的；注：客户组织负责确定它的与信息安全有关的重大风险的识别准则，并制定实施的规程。

b） 确定客户组织识别、检查和评价与信息安全有关的资产威胁、脆弱性和影响的规程以及应用的结果是否与客户组织的方针、目标和指标保持一致。

c） 确定用于重大风险分析的规程是否健全并正确实施。如果有关客户组织的与信息安全有关的资产威胁、脆弱性或影响被识别为重大时，则应纳入 ISMS 管理之中。

d） 法律和法规的符合性：法律法规符合性的保持和评价是客户组织的责任。审核组应通过检查和抽样的方式对 ISMS 在客户组织的合规性收集证据，为作出审核结论提供支持。审核组应验证客户组织所具有的管理体系使其达到符合有关信息安

全风险和影响的法律法规。

e）安排专业审核员负责专业部门/专业过程/专业条款的审核，如企业认证范围为“人工智能应用产品开发及相关过程的信息安全管理”，其人工智能产品开发部门的信息资产识别、运行安全等条款应安排专业审核员审核。

4.6.2.5 审核组组成

第二阶段审核组成员原则上与第一阶段审核组成员相同。若第二阶段审核组成员中有未参加第一阶段审核的，审核组长需要向其介绍第一阶段的审核结果及须进一步追踪的问题。

4.6.2.6 编制审核计划

审核组长负责以第一阶段审核的结果为依据制定第二阶段审核计划，若申请认证组织的生产经营有多班制如机房晚班运维，审核组长应在编制审核计划时考虑对风险处置控制措施中涉及到晚班作业的审核安排和抽样，并要求审核员对晚班作业控制进行审核。

4.6.2.7 审核报告

第二阶段的审核报告需对申请认证组织信息安全管理体系作出总体评价，并编制审核报告，评价内容有以下几方面：

—信息安全风险识别的充分性、评价合理性及其应对措施的针对性；

—客户组织对信息安全威胁的分析与组织的运行是相应和充分的；

—客户组织识别、检查和评价与信息安全有关的资产威胁、脆弱性和影响的规程与执行情况，包括符合 ISMS 标准中所列要求的文件/规程，以及其应用的结果是否与客户组织的方针、目标和指标保持一致；

-基于风险评估与风险处置过程，对控制目标与控制措施的选择的适应性；控制措施的有效性分析、业务连续性管理；

-ISMS 有效性的评审和信息安全控制措施有效性的测量以及对照 ISMS 目标进行的报告和评审；

—组织满足有关信息安全风险和影响的法律法规要求的能力；

—内部审核和管理评审的有效性，包括不合格、纠正措施及持续改善的实施；

—组织风险预防和持续改进评价。

4.7 管理体系的一体化审核

a）ISMS 审核可以和其他管理体系的审核相结合。这种结合只有在证实审核满足 ISMS

认证所有要求时才有可能。

b） 审核中，所有对 ISMS 重要的要素应清晰地体现并易于识别。审核的质量不应由于多体系或一体化审核受到负面影响。

4.8 转换证书

4.8.1 转换证书审核中，审核组应通过现场收集客观证据，对被审核方已获证的信息安全管理体系的保持情况，与认证要求的符合程度作出评价，并向鹰企认证提出是否推荐转换证书的意见。

4.8.2 当以现场审核的方式确认是否进行证书转换时，除覆盖规定的必审条款（如信息安全风险评估、信息安全风险处置、管理评审、内部审核、不合格与纠正措施）外，还必须重点关注以下方面的条款：8.1 控制变更和由外部提供的过程、产品或服务。对于产品和服务实现的最终实现的部门或场所也必须抽样（如成品车间、服务场所等）。

为控制认证风险，审核组长在审核现场应核实申请转换组织产品/服务资质文件（如强制性产品认证、工业产品生产许可证等），关注与信息安全有关的强制性标准与法规的符合情况，收集相关产品/服务信息安全技术规范或标准与法规目录清单，核对产品/服务实际信息安全与法规标准的符合性，同时应收集有效的信息安全监测报告的复印件。若采用直接转换的方式转换证书，则应在转换证书申请受理时，要求被审核方提交上述资料。

4.9 监督审核

4.9.1. 监督审核的目的是验证已被认证的 ISMS 的持续实施、考虑由于客户组织运作的变化所 造成的管理体系变化，以及确认与认证要求的持续符合。

4.9.2. 监督审核人天数的确定

运营部根据获证组织适用标准、组织规模、体系覆盖人数及体系变更情况以及 ISO/IEC17021、CNAS-CC170 的规定确定监督审核人天数，具体按附件 1 执行。

4.9.3 审核组组成

监督审核应由具备审核组长能力的审核员担任审核组长,审核组成员中至少要有一名专业审核员或技术专家。当安排实习审核员进行见习审核时，参加见习审核的实习审核员的人数不应超过审核组内级别审核员的总数。实习审核员不能在没有指导和帮助的情况下进行审核。

4.9.3 监督审核的实施

4.9.3.1 监督审核包括：

a） ISMS 内部审核、管理评审和纠正措施等管理体系保持要素；

b） 根据 ISMS 标准 GB/T 22080(idt ISO27001)和认证所需的其他文件的要求，来自外部各方的沟通；

c） 形成文件的管理体系的变更；

d） 变更涉及的区域；

e） 所选择的 GB/T22080(idt ISO27001)要素；

f） 适宜时，其他被选择的区域。

4.9.3.2 监督审核至少应对以下方面进行审核：

a) ISMS 在实现客户信息安全方针的目标方面的有效性；

b) 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；

c) 所确定的控制的变更及其引起的适用性声明（SoA）的变更；

d) 控制的实施和有效性（根据审核方案来审查）；

e) 每次监督审核都应对 ISMS 范围内的业务部门（如有多个业务部门时可抽样，但每次监督审核都应审核业务类部门）、网络实施运维部门、体系主控部门和管理层进行审核；对其他部门可采用抽样的方式进行，但在一个认证周期内的两次监督审核应全部覆盖。

f) 每次监督审核必查标准附录A 的以下条款：5.1，5.8，5.9，5.15，5.22，5.31，8.6，8.9，8.13，8.31，8.32；其他条款在一个认证周期内的两次监督审核应全部覆盖。

g) 监督审核时，业务种类不能抽样，但过程可以抽样。例如， 业务种类A抽查了设计过程的信息安全管理，业务种类B抽查了运维过程的信息安全管理。

h) 针对上次审核中已识别的不符合采取的措施。

4.10 证书变更

信息安全管理体系的证书变更按《证书变更工作程序》执行。适用时还应满足以下要求。

如获证组织证书变更内容涉及对标准条款的不适用情况，则应在证书变更申请评审时，初步评审其适宜性，并由审核组在证书变更现场审核中验证并评价不适用的合理性。

4.10.1 文件审核

如获证组织的信息安全管理体系文件发生了重大变化，审核组应进行文件审核。

当以监督审核的方式进行扩大获证组织审核范围的证书变更审核时，除按正常的监督

方式进行审核抽样，并覆盖规定的必审条款（如信息安全方针和目标、内部审核、管理评审、信息安全风险评估、信息安全风险处置、监视、测量、分析和评价、不符合与纠正措施） 外，对于拟扩大的审核范围部门，还必须重点关注以下方面的条款：6.1.2 信息安全风险评估、6.1.3 信息安全风险处置、8.1 运行规划和控制、8.2 信息安全风险评估、8.3 信息安全风险处置，对于核心资产相关部门或场所也必须审核。

如获证组织在认证证书有效期内申请增加认可标志，如加发带 CNAS 标志证书，运营部应评审其专业范围是否属于鹰企认证在相应认可机构的认可业务范围，若是，报运营部经理批准后予以加发。若超出鹰企认证在相应认可机构现有的认可业务范围时，运营部应提出受理意见，报总经理审批。

4.11 再认证审核

信息安全管理体系的再认证审核工作按 《监督审核及再认证程序》执行，同时应满足以下要求。

4.11.1 再认证评审和再认证审核人天数的确定

运营部客服通过收集获证组织信息安全管理体系保持的状况，组织规模、审核范围、信息安全风险等级等体系变更情况，会同审核方案管理人员进行再认证审核的评审。按 ISO/IEC17021、CNAS-CC170 的有关要求，确定再认证审核人天数，具体按附件 1 确定。

4.11.2 再认证审核组

信息安全管理体系再认证审核组的要求与认证审核时相同，按上述条款执行。

4.11.3 文件审核

再认证审核组应进行文件审核，如获证组织的信息安全管理体系发生了重大变化，必要时，可以建议安排一次远程审核，具体可参照初次认证审核一阶段现场审核的要求进行。

4.11.4 再认证现场审核的实施

适用时，在再认证的现场审核中，应再次对申请标准要求的变更策划的合理性进行评价。

为控制认证风险，审核组长在审核现场应核实申请转换组织产品/服务资质文件（如强制性许可证等），关注信息安全风险相关强制性标准与法规的符合情况，收集信息安全相关标准与法规目录清单，核对信息安全风险应对措施与法规标准的符合性，同时应评估组织开展信息安全风险监测评价的有效性。

4.12 合格评定

信息安全管理体系的认证决定工作按《认证决定程序》执行。

4.13 批准、保持、暂停、撤销以及注销认证

认证的批准、保持、暂停、撤销和注销工作按《对授予保持扩大更新缩小暂停恢复及撤消认证的规定》执行。

4.14 认证证书与认证标志管理

认证证书与认证标志管理按 《认证认可标识（牌）使用及认证证书管理规定》执行；

4.15 认证情况通报

信息安全管理体系认证情况按照认证认可要求及时进行通报。

4.16 ISO27001 认证领域的能力分析系统

ISO27001 认证领域的能力分析系统按照《认证业务范围及能力分析评价系统管理程序》执行。

4.17 认证业务范围专业能力管理及扩大或缩小业务范围

认证范围专业能力管理及扩大或缩小业务范围管理按《认证业务范围及能力分析评价系统管理程序》执行。认证业务范围专业项目评定参见《管理体系认证机构认证业务范围分类指南》。

4.18 认证人员能力要求

鹰企认证对从事信息安全管理体系认证的各类人员在满足 ISO/IEC17021 要求的基础上，根据其承担的职责和鹰企认证对 ISO27001 认证业务范围内的分类管理要求和办法，确定其专业能力资格条件，并按《认证人员能力管理程序》和《信息安全认证人员能力要求及评价管理规定》的要求进行评价和聘用。

4.18.1 审核员注册要求及条件

4.18.1.1 审核员注册要求及条件参见 CCAA 的“信息安全管理体系审核员注册要求及条件”。

4.18.1.2 专业审核员的能力要求：

对于承担专业审核任务的专业审核员，在满足上述注册条件的基础上，还应满足以下条件：

a)具有专业技术领域的基本理论知识和一定的实践经验；

b)熟悉该专业适用的组织的设计、生产、安装和服务的过程；

c)能识别组织影响信息安全的关键活动，并对其控制的有效性进行评价；

d)熟悉相应专业的法律、法规、技术标准及其他要求；

e)适用时，具有特定行业的资格证书。

专业审核员的能力要求见《信息安全认证人员能力要求及评价管理规定》，学历教育、工作经历、审核员培训和审核经历仅仅是审核员获取审核能力的途径，审核员具有相应的经历并不等于一定具备所需的能力，因此，鹰企认证应按照能力分析和评价系统的规定，对满足上述条件的审核员实际所具有的能力进行评价和证实。审核员能力评价可以组合采用记录审查、意见反馈、面谈、考试、见证等方式评定确定其专业能力。

4.18.2 技术专家

技术专家的个人品质应符合 ISO/IEC17021 要求和 CCAA 的信息安全管理体系审核员注册的要求。技术专家的专业能力要求与专业审核员相同。

4.18.3 审核方案管理人员、认证决定人员的评聘

根据 CNAS-GC01:2017 《管理体系认证机构认证业务范围能力管理实施指南》和《信息安全认证人员能力要求及评价管理规定》关于审核方案管理人员、认证决定人员评定准则的要求进行聘用，并按照按具备的专业所属大类的专业能力进行委派。

5 附件 A ISO/IEC27001 信息安全管理体系审核时间表

附件 B 调整审核时间的因素

附件 C 审核时间计算方法

附件 A

ISO/IEC27001 信息安全管理体系审核时间表

（认证审核时间包含第一阶段与第二阶段）

在组织控制下工作的人员的数量	初次审核时间（审核人日）	增加或减少的因素	总审核时间	年度监督审核时间	再认证审核时间
1~10	5	见 B2		1.5	3
11~15	6	见 B2		2.0	4
16~25	7	见 B2		2.0	4.5
26~45	8.5	见 B2		2.5	5.5
46~65	10	见 B2		3.0	7
66~85	11	见 B2		4.0	7
86~125	12	见 B2		4.0	8
126~175	13	见 B2		4.0	9
176~275	14	见 B2		5.0	9
276~425	15	见 B2		5.0	10
426~625	16.5	见 B2		5.5	11
626~875	17.5	见 B2		5.5	12
876~1 175	18.5	见 B2		6.0	12
1 176~1 550	19.5	见 B2		6.5	13
1 551~2 025	21	见 B2		7.0	14
2 026~2 675	22	见 B2		7.0	15
2 676~3 450	23	见 B2		8.0	15
3 451~4 350	24	见 B2		8.0	16
4 351~5 450	25	见 B2		8.0	17
5 451~6 800	26	见 B2		9.0	17
6 801~8 500	27	见 B2		9.0	18
8 501~10 700	28	见 B2		1.5	3.5
>10 700	沿用以上规律	见 B2			

附件 B.调整审核时间的因素

B1.1 不能孤立地使用表附件 A。所安排的时间，还应考虑以下因素。这些因素与 ISMS 复杂程度相关，并因此与 ISMS 审核工作量相关：

a） ISMS 的复杂程度(例如，信息的关键程度、ISMS 的风险状况）；

b） ISMS 范围内所开展的业务的类型；

c） 以往已证实的 ISMS 绩效；

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]；

e） ISMS 范围内所使用的外包和第三方安排的程度；

f） 信息系统开发的程度；

g） 场所的数量和灾难恢复场所的数量；

h） 对于监督或再认证审核：符合 GB/T 27021.1—2017 中 8.5.3 要求的、与 ISMS 相关的变更的数量和程度。

B1.2 附录 C 提供了在计算审核时间时如何考虑这些不同因素的示例。

需要增加审核时间的其他因素，例如：

a） 复杂的后勤，在 ISMS 范围中涉及不止一处建筑物或地点；

b） 员工的语言超过一种(需要翻译或审核员个人无法独立工作)，提供的文件使用了一种以上的语言；

c） 为了确认管理体系认证范围内永久场所的活动，需要访问临时场所的活动；

d） 适用于 ISMS 的标准和法规数量很多。

B1.3 允许减少审核时间的因素，例如：

a） 没有风险或者低风险的产品/过程；

b） 过程只涉及单一的常规活动(例如，只有服务）；

c） 在组织控制下工作的雇员大部分是从事相同的任务；

d） 对组织已经有些了解(例如，如果组织获得了同一个认证机构的、另一个标准的认证）；

e） 客户的认证准备情况较好(例如，已经获得了另一个第三方认证方案的认证或承认）；

f） 高度成熟的管理体系。

当认证客户或获证组织在临时场所提供其产品或服务时，将对这类场所的评价纳入到认证审核和监督方案中是十分重要的。

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。

B.1.4 对审核时间偏离的限制

为了确保能够实施有效的审核并确保可靠和可比较的结果，对表 B.1 中审核时间的减少，不应超过 30%。

应确定偏离审核时间表的适当理由，并形成文件。

B.2 现场审核时间

策划和编制报告一起所用的时间，通常不宜使总的现场“审核时间”减少到表B.1中“总审核时间”的70%以下。当策划和/或编制报告需要增加时间时，这不应成为减少现场审核时间的理由。审核员 旅途时间未计在内，这应在表中所给出的审核时间的基础上另外增加。

注：70%是基于ISMS审核经验所得出的系数。

B.3 监督审核的审核时间

在初次认证审核周期，对一个组织的监督时间宜与初次审核时间成比例，每年用于监督审核的时间 总量大约是初次审核时间的1/3。宜时常评审所策划的监督审核时间，以考虑影响审核时间的变更。为审核ISMS的变更（例如，审核新的或发生变更的控制），应增加监督审核的时间。

B.4 再认证审核的审核时间

用于再认证审核的全部时间，应取决于9.4.3和GB/T 27021.1—2017中9.6.3所规定的、任何以往 审核的结果。再认证审核所需的时间，宜与同一组织的初次认证审核所用的时间成比例，宜至少是同一 组织初次认证审核时间的2/3。

B.5 多场所的审核时间

应针对每个场所计算每个场所(包括总部)的审核人天数。

可以考虑因部分审核与总部或分场所无关而减少审核时间。认证机构应记录这类减少的合理理由。

附录C 审核时间计算方法

C. 1 总则

本附录为推导出审核时间计算公式提供了进一步的指南。C. 2给出了一个对因数进行分类的示例,它可用作审核时间计算的基础。C. 3提供了一个审核时间计算的示例。

C.2 审核时间计算因数的分类

表C. 1给出了对主要的审核时间计算因数进行分类的示例。认证机构可以使用该分类来制定一个审核时间计算方案。

表C. 1 审核时间计算因数的分类

	对工作量的影响		
	减少工作量	正常工作量	增加工作量
附录B中因数（见B. 2）			
a) ISMS的复杂性： • 信息安全要求[保密性、完整性和可用性，(CIA)] • 关键资产的数量 • 过程和服务的数量	• 只有少量的敏感信息或保密信息，可用性要求低； • 很少的关键资产（根据CIA）； • 只有一个关键业务过程，该过程的接口和涉及的业务单元很少	• 较高的可用性要求或若干敏感/保密信息； • 若干关键资产； • 2个~3个简单的业务过程，这些过程的接口和涉及的业务单元很少	• 比较多的保密信息或敏感信息(例如，健康、个人可识别信息、保险、银行)，或可用性要求高； • 很多关键资产； • 超过2个复杂的过程，这些过程的接口和涉及的业务单元很多
b) ISMS范围内所开展的业务的类型	• 低风险的业务，没有法规要求	• 法规要求高	• 高风险的业务，有（仅有）有限的法规要求
c) 以往已证实的ISMS绩效	• 最近刚获得认证； • 没有获得认证，但ISMS已充分实施了多个审核与改进周期，包括文件化的内部审核，管理评审和有效的持续改进体系	• 最近刚通过监督审核； • 没有获得认证，但部分实施了ISMS:获得并实施了一些管理体系工具，一些持续改进过程是适宜的但未全部文件化	• 未获得认证且最近未接受审核； • ISMS是新的且没有完全建立(例如：缺少管理体系的特定控制机制，不成熟的持续改进过程，特别的流程执行)
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)

表 C. 1（续）

	对工作量的影响		
	减少工作量	正常工作量	增加工作量
附录 B 中因数（见 B2）			
e） 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； • 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、正在实施中的项目
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） 监督或再认证审核：符合 GB/T27021. 1—2017 中8. 5. 3、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 的范围或适用性声明有微小的变化，例如，一些策略、文件发生变化； • 以上因素有微小变化	• ISMS 的范围或适用性声明有重大变化，例如，新的过程、新的业务单元、区域、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

C.3 审核时间计算的示例

以下示例阐述了认证机构如何使用 B.2 中的因数来计算审核时间。该示例中的审核时间计算是按照以下方法进行的:

第一步: 确定与业务和组织相关的(非 IT)因数:识别表C.2中每个类别的适宜分值，并对结果求和;

第二步:确定与 IT 环境相关的因数:识别表 C.3 中每个类别的适宜分值，并对结果求和;

第三步:基于以上第一步和第二步的结果，通过选择表 C.4 中的适宜条目,识别这些因数对审核时间的影响;

第四步:最终计算将由审核时间表(表 B. 1)所确定审核人天数乘以第三步中得出的系数。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，这个结果是最终的审核人天数。

表 C.2 与业务和组织(非 IT)相关的因数

类别	分值
业务类型和法规要求	1) 组织所处的是一个非关键业务领域，且不受管制的领域[a]； 2) 组织的客户处于关键业务领域[a]； 3) 组织处于关键业务领域[a]
过程与任务	1) 标准过程，涉及标准的且重复的任务；大量在组织控制下工作的人员从事相同的任务； 很少的产品或服务； 2) 标准的但不重复的过程，涉及大量的产品或服务； 3) 复杂的过程，大量的产品和服务，许多业务单元包含在认证范围内(ISMS有复杂性高的过程，或相对较多的独特活动)
管理体系的建立水平	1) 已经很好地建立了 ISMS,和(或)存在其他管理体系； 2) 其他管理体系的要素，有些已经实施，有些没有实施； 3) 根本没有实施其他管理体系，ISMS是新的且没有建立
关键业务领域是可以影响关键公共服务的领域，这些公共服务将引起健康、安全、经济、形象和政府履职能力的风险，从而可能对国家造成非常重大的负面影响。	

表 C.3 与 IT环境相关的因数

类别	分值
IT基础设施的复杂程度	1) 很少的或高度标准化的 IT平台、服务器、操作系统、数据库、网络等； 2) 多个不同的 IT平台，服务器、操作系统、数据库、网络； 3) 很多不同的 IT平台、服务器、操作系统、数据库、网络
对外包和供应商(包括云服务)的依赖程度	1) 很少或不依赖外包或供应商； 2) 有些依赖外包或供应商，这些外包或供应商与某些重要业务活动相关，但不是与所有的重要业务活动相关； 3) 高度依赖外包或供应商，外包或供应商对重要业务活动有着很大影响
信息系统开发	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的、内部的或外包的系统/应用开发

表 C.4 因数对审核时间的影响

业务复杂性	IT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%

文件修改履历表

序号	修订说明	修订条款号	修订日期	实施日期	版次	编制	批准
1	新增		2025.06.17	2025.06.17	A/0	寻爱凌	钱晔