亿寰认证中心有限公司

信息安全管理体系认证实施规则

文件号：YH-GZ-ISMS

版本号：C/0 版

编写：技术部

审批：况　卉

发布日期：　2025.06.10

实施日期：　2025.06.10

目 录

1.适用范围..... 3
2.规范性引用文件..... 3
3.术语和定义..... 4
4.认证依据..... 4
5.认证机构基本要求..... 4
6.认证人员及审核组要求..... 4
7.认证信息公开..... 6
8.管理体系认证流程..... 6
9.认证程序和要求..... 8
10.暂停、撤销、注销认证或缩小认证范围.....15
11.认证证书要求..... 17
12.受理认证证书转换..... 18
13.申诉和投诉..... 18
14.认证记录的管理.....19
15.收费..... 19
16.其他..... 19
附录 A..... 20
附录 B..... 21
附录 C..... 22

1.适用范围

本文件适用于亿寰认证中心有限公司（以下简称“YHRZ”）开展信息安全管理体系认证活动。

2.规范性引用文件

中华人民共和国认证认可条例（2023 年 7 月 20 日中华人民共和国国务院令第 764 号修订）

认证机构管理办法（2020 年 10 月 23 日国家市场监督管理总局令第 31 号修订）

认证证书和认证标志管理办法（2022 年 9 月 29 日国家市场监督管理总局令第 61 号第二次修订）

市场监管总局关于在全国范围内推进认证机构资质审批“证照分离”改革的公告（国家市场监督管理总局公告 2022 年第 28 号）

国家认监委关于加强认证规则管理的公告（认监委公告 2025 年第 9 号）

国家认监委秘书处关于印发《〈国家认监委关于加强认证规则管理的公告〉实施指南》的通知(认秘函〔2025〕12 号)

GB/T 27021.1/ISO/IEC 17021-1《合格评定 管理体系审核认证机构要求 第 1 部分：要求》

GB/T 25067/ISO/IEC 27006 《合格评定 信息安全管理体系认证机构要求》

GB/T 27000/ISO/IEC 17000 《合格评定 词汇和通用原则》

GB/T 27004/ISO/PAS 17004 《合格评定 信息公开 原则和要求》

GB/T 27007/ISO/IEC 17007 《合格评定 合格评定用规范性文件的编写指南》

GB/T 27060/ISO/IEC 17060 《合格评定良好操作规范》

GB/T 19011/ISO 19011 《管理体系审核指南》

GB/T 29246/ISO/IEC27000 《信息技术 安全技术 信息安全管理体系 概述和词汇》

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-SC170 《信息安全管理体系认证机构认可方案》

CNAS-CC11 《多场所组织的管理体系审核与认证》

CNAS-CC14 《信息和通信技术（ICT）在审核中应用》

CNAS-GC02 《管理体系认证结合审核应用指南》

CNAS-CC106 《CNAS-CC01 在一体化管理体系审核中的应用》

CNAS-R02 《公正性和保密规则》

CNAS-R03 《申诉、投诉和争议处理规则》

CCAA-101 《管理体系审核员注册准则》

ISO/IEC 27001《信息安全 网络安全和隐私保护 信息安全管理体系 要求》

3.术语和定义

GB/T 27000/ISO/IEC 17000、GB/T 29246/ISO/IEC27000、GB/T 19011/ISO 19011 界定的术语和定义适用于本文件。

4.认证依据

名称	编号	发布单位	发布/实施日期
《信息安全 网络安全 隐私保护 安全管理体系 要求》	ISO / IEC 27001:2022	国际标准化组织 ISO	2022-10-25 发布

5. 认证机构基本要求

5.1 YHRZ 应获得国家认监委批准、取得从事信息安全管理体系认证的资质。

5.2 YHRZ 的认证能力、内部管理和工作体系应符合 CNAS-CC01《管理体系认证机构要求》。

5.3 YHRZ 应建立内部制约、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。

5.4 YHRZ 不将申请认证的组织（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。

6. 认证人员及审核组要求

6.1 认证审核员应当取得中国认证认可协会（CCAA）的信息安全管理体系审核员注册资格。

6.2 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。

6.3 参与认证活动的人员应当满足 CNAS-CC170《信息安全管理体系认证机构要求》所述的人员能力要求并满足表 1 中规定要求：

表 1 认证人员应当具备的能力

岗位	能力要求
认证规则和认证方案制定人员	具有相应领域的专业知识和工作经验；熟悉认证依据标准或规范性文件；熟悉认证认可相关标准及认证程序要求；熟悉相应领域有关法律、法规、技术标准及其他要求。
认证申请评审人员	熟悉认证依据标准或规范性文件；熟悉相应认证领域划分并能正确判断认证委托人委托的认证领域和专业；熟悉本机构相应领域专业资源配备情况。
认证审核方案管理人员	熟悉认证依据标准或规范性文件；熟悉认证认可相关标准及认证程序要求；能够识别各认证领域的专业特点；能够根据认证客户的业务/产品/过程/组织结构的知识和信息识别其对审核方案，特别是对审核组的能力要求；熟悉本机构相应领域专业资源配备情况。
认证审核人员	审核员 具有 CCAA 信息安全管理体系注册资格；满足 CCAA 注册准则规定的资格经历、个人素质和审核原则、知识和技能、行为规范要求。 具有与认证领域相关的专业知识和实践经验，熟悉行业相关法律法规要求；理解和掌握认证依据标准或规范性文件；熟悉认证认可相关标准及认证审核原则、实践和技巧；了解企业管理和组织运作相关知识，了解认证机构认证管理过程要求，完全能够按照认证机构的程序和过程开展工作。 技术专家： 具有与认证领域相关的专业知识和实践经验，熟悉行业相关法律法规要求；了解企业管理和组织运作相关知识，了解认证机构认证管理过程要求，完全能够按照认证机构的程序和过程开展工作。
认证决定或复核人员	具有与认证领域相关的专业知识；熟悉认证认可相关标准及认证审核原则、实践和技巧；了解认证机构认证管理过程要求。
认证人员能力的评价人员	熟悉认证认可相关标准及认证程序要求；能够识别各认证领域的专业特点；熟悉认证流程及认证过程各阶段的专业管理要求；掌握专业能力评定要求；熟悉各类认证人员的能力准则，能正确选择对认证人员能力评价的方法，并能基于已有的证据准确判定受评价人员的能力与准则的符合性。

6.4 参与认证活动的人员应经过 YHRZ 的能力评价，以确定其能够胜任所安排的审核任务。

6.5 认证审核人员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和翻译以增强审核组的能力。技术专家和翻译应在审核员的指导下进行工作，可就申请组织（客户）或获证组织中充分性事宜为审核员提供建议，但技术专家和翻译不能作为审核员。

7.认证信息公开

YHRZ 应向申请认证的社会组织(以下称申请组织)至少公开以下信息：

1) 可开展认证业务的范围，以及获得认可的情况；

2) 认证依据；

3) 认证实施程序；

4) 认证证书样式；

5) 认证证书、认证标志及相关的使用规定；

6) 认证证书状态管理规定、要求

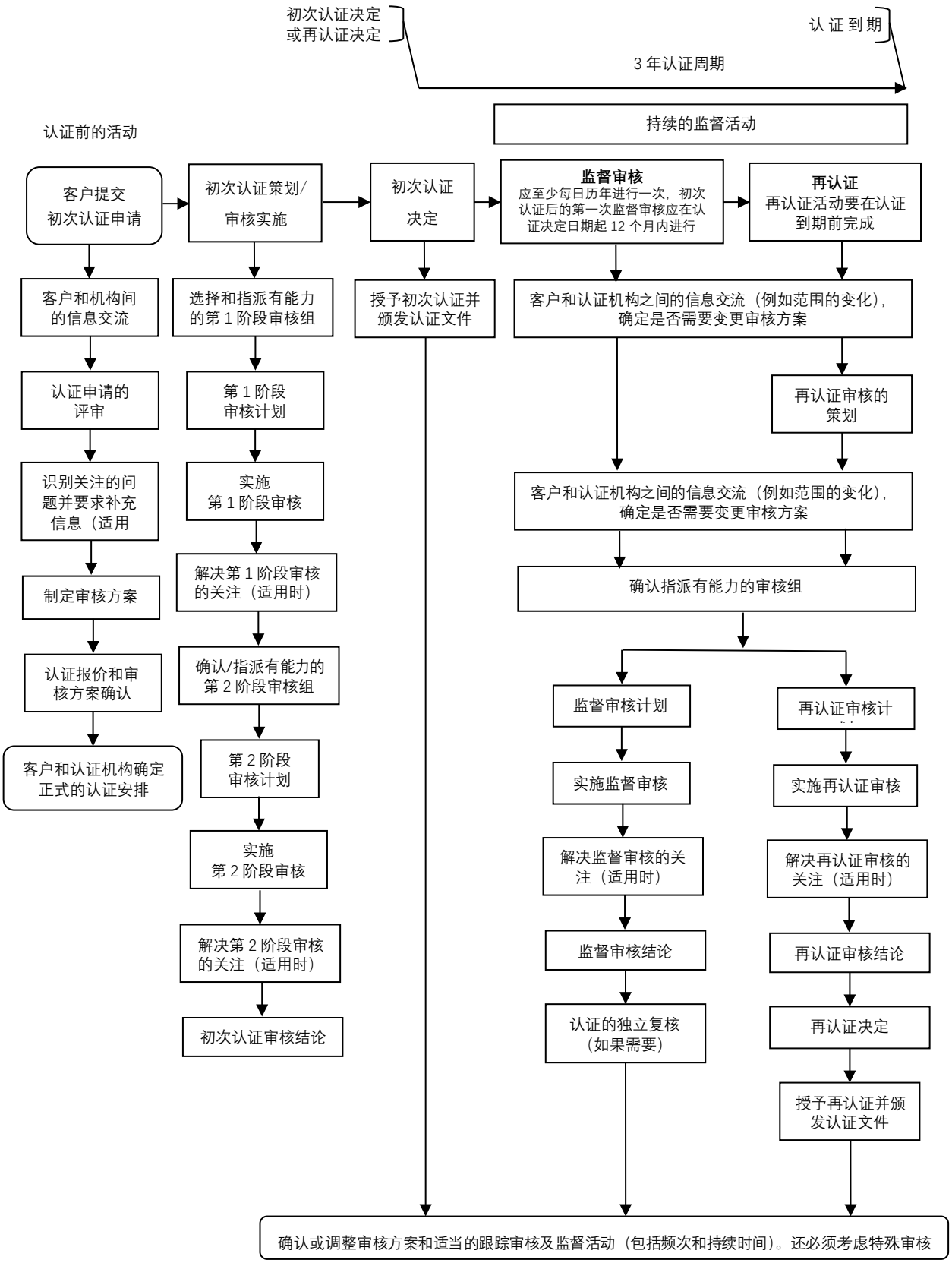
7) 对认证过程的申诉、投诉规定；

8）认证收费标准。

8.管理体系认证流程

认证审核分为初次认证审核，监督审核和再认证审核。为满足认证的需要，YHRZ 可以实施特殊审核，特殊审核采取现场审核方式进行。管理体系认证典型流程如下图 1：

图 1 管理体系认证典型流程



9.认证程序和要求

9.1 认证申请

YHRZ 应要求申请组织的授权代表至少提供以下必要的信息：

1)法律地位资格证明(营业执照、事业单位法人证书或社会团体法人登记证书等)；

2)取得相关法规规定的行政许可文件、资质证书、强制性认证证书等（适用时)；

3)从事的业务活动符合中华人民共和国相关法律、法规、信息安全标准和有关规范的要求；

4)对信息安全管理体系认证范围涉及的业务活动的描述；

5)已按认证依据和相关要求建立和实施了文件化的信息安全管理体系；

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。

上述必要信息应使 YHRZ 能够确定：

1)申请组织的行业类别；

2)申请认证的范围；

3)申请组织的一般特征，包括其名称、物理场所的地址、为内部或外部顾客的业务过程提供支持的说明、过程和运作的重要方面以及任何相关的法律义务；

4)申请组织与申请认证的领域相关的一般信息，包括其活动，人力与技术资源，以及适用时，其在一个较大实体中的职能和关系；

5)申请组织采用的所有影响符合性的外包过程的信息；

6)接受与信息安全管理体系有关的咨询的情况。

申请组织按上述信息提供如下材料（包括但不限于)：

a 认证申请书;

b 法律地位的证明文件的复印件。若信息安全管理体系覆盖多场所活动，应附每个场所的法律地位证明文件的复印件（适用时）;

c 信息安全管理体系覆盖的活动所涉及法律法规要求的行政许可证明、资质证书、强制性认证证书等的复印件；;

d 信息安全管理体系适用性声明（SoA)；

e 适用的法律法规标准清单;

f 保密和敏感信息声明；

g 信息安全管理体系成文信息（适用时)。

9.2 申请评审

YHRZ 的认证申请评审人员应根据认证依据、程序等要求，在三个工作日内对申请组织提交的认证申请书及其相关资料进行评审并保存评审记录，做出评审结论，以确保：

1)识别申请组织的行业类别和与之相应的生产/服务提供过程的信息安全要求；

2)掌握国家对相应行业的信息安全管理体系认证的管理要求；

3)申请组织及其管理体系的信息充分，可以进行审核；

4)认证要求已有明确说明并形成文件，且已提供给申请组织；

5)解决了 YHRZ 与申请组织之间任何已知的理解差异；

6)YHRZ 有能力并能够实施认证活动；所属业务范围分类见《YHRZ 认证业务代码分类及认证业务范围》。

7)考虑了申请的认证范围、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)保持了决定实施审核的理由的记录。；

9) 当评审结论为不受理时，以书面形式通知申请人。评审结论为受理时，与申请组织签订认证合同。

9.3 建立审核方案

经申请评审，对可以接受后，YHRZ 应针对申请组织建立审核方案，并由专职人员负责管理审核方案。

9.3.1 确定审核组

YHRZ 应根据申请组织（客户）的规模和业务复杂程度组建审核组，指派审核组长。审核组组建原则见本文件第 6 章。

1）认证审核人员必须取得信息安全管理体系认证注册资格。

2）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。必要时可以补充技术专家以增强审核组的技术能力。

3）具有信息安全、信息安全法规等方面的特定知识的技术专家可以成为审核组成员。技术专家应在审核员的监督下进行工作，可就受审核方管理体系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）审核组可以有实习审核员，其要在审核员的指导下参与审核，不计入审核时间，不单独出具记录等审核文件，其在审核过程中的活动由审核组中的审核员承担责任。

9.3.2 确定审核人日

YHRZ 应根据申请组织的规模、特性、业务复杂程度、信息安全管理体系涵盖的范围、认证要求和其承担的风险等因素核算并确定审核人日，以确保审核的充分性和有效性。审核人日基准参考附录 A，在适当的情况下，可以减少审核时间，但减少的时间不得超过 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%。

9.3.3 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地被识别，可以允许申请组织将信息安全管理体系文件与其他管理体系文件(例如，质量管理体系、环境管理体系，职业健康安全管理体系等)相结合。

9.3.4 管理体系结合审核

当申请组织在运行信息安全管理体系的同时还运行了其他管理体系，若其他管理体系在 YHRZ 的认证业务范围内，YHRZ 可以根据申请组织的需求，仅提供信息安全管理体系认证服务或结合信息安全管理体系认证提供其他管理体系认证服务，但 YHRZ 需确保在结合审核的情形下，对诸如审核范围的界定、审核时间的确定、审核方案的策划等进行有效的管理。结合审核的审核时间人日数，不得少于多个单独体系所需审核时间之和的 80%。

对于结合审核，审核活动满足信息安全管理体系认证所有要求为前提，审核的质量不应由于结合审核而受到负面影响。在审核报告中，应清晰体现所有与体系有关的重要要素的描述并易于识别。

9.3.5 审核方案内容

审核方案应包括在规定的期限内有效和高效地组织和实施审核所需的信息和资源，应包括以下内容：

1) 审核方案的目标；

2) 审核的范围与程度、数量、类型、持续时间、地点、日程安排；

3) 审核准则；

4) 审核方法；

5) 审核组的选择；

6) 所需的资源；

7) 其它事宜。

9.3.6 审核方案记录与变更

认证审核方案管理人员应收集审核前收集的信息、现场审核和认证决定的信息，特别是形成的结论和变化的信息，记录到审核方案中。并确定审核方案是否需要进行变更，如需要则更新相应项目内容。

9.4 初次认证审核

初次认证审核分第一阶段和第二阶段进行。第一、二阶段审核的时间隔不宜超过 6 个月，超过该期限将调整审核方案。

9.4.1 审核计划

9.4.1.1 YHRZ 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 。

9.4.1.2 如果信息安全管理体系覆盖范围包括在多个场所进行相同或相近的活动，且这些场所都处于申请组织授权和控制下，YHRZ 可以在审核中对这些场所进行抽样，但应根据相关要求实施抽样以确保对所抽样本进行的审核对信息安全管理体系包含的所有场所具有代表性。如果不同场所的活动存在明显差异、或不同场所间存在可能对信息安全管理有显著影响的区域性因素，则不能采用抽样审核的方法，应当逐一到各现场进行审核。

9.4.1.3 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。

9.4.1.4 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。

9.4.2 第一阶段审核

第一阶段审核应在申请组织的现场进行，审核内容包括：

1）评价申请组织的场所和现场的具体情况，并与申请组织的人员进行讨论，以确定第二阶段审核的准备情况；

2）审查申请组织理解和实施标准要求的情况，特别是对信息安全管理体系的关键绩效或重要因素、过程、目标和运作的识别情况；

3）收集并审查关于申请组织的信息安全管理体系范围、已完成的风险评估、过程和场所的必要信息，以及相关的法律法规要求和遵守情况（如：申请组织运作相关的法律因素和识别的风险等）；

4）审查第二阶段审核所需资源的配置情况，并与申请组织商定第二阶段审核的细节；

5）结合可能的重要因素充分了解客户的信息安全管理体系和现场运作，以便为策划第二阶段审核提供关注点；

6）评价申请组织是否策划和实施了内部审核与管理评审，以及信息安全管理体系的实施程度能否证明申请组织已为第二阶段审核做好准备。

YHRZ 应将第一阶段审核发现形成文件并告知申请组织，包括识别任何引起关注的、在第二阶段审核中可能被判定为不符合的问题。

9.4.3 第二阶段审核

第二阶段审核应在具备实施认证审核的条件下在申请组织的场所进行。如果第一阶段审核提出影响实施第二阶段审核的问题，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，并判断是否推荐认证注册。应重点关注申请组织是否充分识别了信息安全管理过程的重要性，并证实与申请组织的信息安全活动是相适应的。应至少覆盖以下内容：

1）与适用的规范性文件的所有要求的符合情况及证据；

2）依据关键绩效目标和指标，对绩效进行的监视、测量、报告和评审；

3）组织的信息安全管理体系以及在遵守法律法规方面的绩效；

4）运作控制；

5）内部审核和管理评审；

6）针对申请组织方针的管理职责；

7）规范性要求、方针、绩效目标和指标、适用的法律要求、职责、人员能力、运作、程序、绩效数据和内部审核结果之间的联系。

9.4.4 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。

如果现场审核发现不符合项应开具不符合项报告，且获得受审核组织认同。

现场审核结束后，审核组长完成审核报告编制工作，并与申请组织（客户）进行沟通，确保双方对报告的理解上没有歧义。

现场审核结束，审核组应形成是否推荐认证注册的结论；审核组可以根据审核前收集的信息和现场审核的结果对申请组织（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要求进行评价，并判断是否推荐认证注册。

不符合项分为：一般不符合项、严重不符合项。一般不符合关闭期限通常在 90 个工作日内，严重不符合项不超过 6 个月。无论何种情况，未能在第二阶段结束后 6 个月内验证对不符合实施的纠正和纠正措施，则应拒绝其认证注册，或者重新实施第二阶段审核。

9.4.5 认证决定

YHRZ 应指派认证决定或复核人员，对申请组织（客户）的认证申请实施认证决定，以决定：

a） 同意认证注册，颁发认证证书；

b） 补充认证决定所需的信息，包括但不限于申请材料、审核材料，再行决定；

c） 不同意认证注册。

认证决定或复核人员实施认证决定时应该以认证过程中收集的信息和其他相关信息为基础，以充分的证据证实申请组织建立信息安全管理体系的管理评审和内部审核的方案已经得到有效实施并且将得到保持，才可决定申请组织通过认证。

注 1：参加审核的人员不能再作为认证决定或复核人员实施认证决定。

注 2：申请组织（客户）获得认证注册资格后变更为获证组织。

注 3：审核材料符合要求后，在 10 个工作日内做出认证决定。对经评定合格的申请组织，认证机构应颁发认证证书，准予使用认证标志和认证证书，认证标志和认证证书的使用应符合认证机构的文件要求。评定合格组织的名单将在认证机构的网站上公布。

对经评定不合格的申请组织，YHRZ 应做出不予以认证注册的决定，并将不能注册的原因书面通知申请组织。

9.5 监督审核

9.5.1 监督频次

YHRZ 应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，或发生重大问题、产品或服务质量事故、客户投诉等情况时，YHRZ 视情况可增加监督的频次。

第一次监督审核的最长时间间隔不超过 12 个月，第二次监督审核的最长时间间隔不超过 15 个月。由于获证组织业务运作的时间(季节)特点及其内部审核安排等原因，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两次监督审核涉及的条款之和必须覆盖认证标准的所有条款并覆盖全部认证范围。

9.5.2 信息收集

在进行监督审核之前，YHRZ 需要收集获证组织的信息安全管理体系的相关信息，以确定获证组织的信息安全管理体系相关信息是否发生变化。信息确认文件，包括但不限于：

a 基本信息，包括组织名称、地址、联系人等信息的变化情况；

b 组织信息，包括范围、组织架构、人员数量等信息的变化情况；

c 信息安全管理体系相关信息，关键文件化信息的变化情况。

9.5.3 信息评审

审核组应对获证组织的信息确认文件进行评审，以确定：

1） 获证组织的信息安全管理体系变化情况，尤其是覆盖范围的变化；

2） 是否需要修订审核方案。

9.5.4 监督审核实施

审核组按照审核计划的安排对获证组织进行审核，由于监督审核并不要求覆盖认证标准的所有方面，因此在监督审核的策划过程中，如果获证组织的认证范围信息有变化，应对变化的方面进行关注，必要时重新确认审核范围。

监督审核应包括，但不限于以下内容：

1)体系保持和变化情况；

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)生产和服务的变化情况；

6)对上次审核时提出的不符合所采取纠正措施的审查；

7)标志的使用和（或）任何其他对认证资格的引用；

8)适当时，其它选定的范围。

9.5.5 监督审核结果评价

对于监督审核合格的获证组织，YHRZ 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、撤销或注销相应的认证资格。

9.6 再认证

认证证书有效期满前，YHRZ 根据获证组织的申请对获证组织实施再认证，以保证信息安全管理体系认证证书持续有效。

9.6.1 再认证审核的策划

9.6.1.1 YHRZ 应策划和实施再认证审核，以评价获证组织是否持续满足信息安全管理体系标准和相关的认证规范性文件的所有要求。

9.6.1.2 再认证审核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。

9.6.1.3 当获证组织、获证组织的信息安全管理体系或其运作环境有重大变更时，YHRZ 应对变更的影响进行评价，确认再认证审核活动是否需要有单独的第一阶段审核。

9.6.1.4 对于多场所认证或依据多个管理体系标准进行的认证，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。

9.6.2 再认证程序应与信息安全管理体系认证审核的要求和指南保持一致。

9.6.3 YHRZ 应根据再认证审核的结果，以及认证周期内的体系评价结果和认证使用方的投诉，作出是否更新认证的决定。

9.7 特殊审核

9.7.1 扩大或变更认证范围

对于已授予的认证，YHRZ 应对获证组织扩大或变更（含标准转换）认证范围的申请进行评审，策划并实施必要的审核活动，并在该审核活动中验证获证组织的信息安全管理体系的适宜性和有效性，以作出是否可予扩大或变更的决定。扩大或变更认证范围的审核活动可单独进行，也可和对获证组织的监督审核或再认证一起进行。

9.7.2 调查投诉、变更回应、被暂停认证资格追踪

YHRZ 在调查投诉、对变更做出回应或对被暂停认证资格的获证组织进行追踪时，可能需要在提前较短时间通知获证组织后对其进行审核。此时：

1） 应向获证组织说明并使其提前了解将在何种条件下进行此类审核；

2） 由于获证组织缺乏对审核组成员的任命表示反对的机会，YHRZ 应在指派审核组时给予更多的关注。

10.暂停、撤销、注销认证或缩小认证范围

YHRZ 建立并保持暂停、撤销、注销认证或缩小信息安全管理体系认证范围的程序，并规定 YHRZ 的后续措施。

10.1 获证组织有以下情形之一的，YHRZ 应在调查核实后的 5 个工作日内暂停其认证证书：

1)获证组织的信息安全管理体系持续地或严重地不满足认证要求，包括对信息安全管理体系有效性的要求；

2)组织不承担、履行认证合同约定的责任和义务（如：不按要求的频次实施监督或再认证审核）；

3)获证组织不接受或不配合认证认可监督管理部门的监督管理（包括对有关事项的询问和调查提供了虚假材料或信息的）；

4)获证组织主动请求暂停。

5）持有的行政许可证明、资质证书、强制性认证证书等过期失效，重新提交的申请已被受理但尚未换证。

6）其他原因需要暂停证书。

10.2 认证资格暂停期最长不超过 6 个月。但属于 10.1 第（5）项情形的暂停期可至相关单位作出许可决定之日。

10.3 在暂停认证期间，获证组织的认证证书暂时无效，暂停信息通过“认证认可信息统一上报平台”上报，可通过“全国认证认可信息公共服务平台”公开获取。YHRZ 以书面通知获证组织相关事宜，在暂停认证期间获证组织应避免继续宣传信息安全管理体系认证资格。

10.4 如果获证组织在认证范围的某些部分持续地或严重地不满足认证要求，YHRZ 应缩小其信息安全管理体系认证范围，以排除不满足要求的部分。认证范围的缩小应与认证标准的要求一致。

10.5 获证组织有以下情形之一的，YHRZ 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证书：

1）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。

2）审核未通过；

3）被注销或撤销法律地位证明文件的

4）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 YHRZ 已要求其纠正但超过 2 个月仍未纠正的。

5）其他原因需要撤销证书。

10.6 发生以下情况(但不限于)时，YHRZ 应在获得相关信息并调查核实后 5 个工作日内注销获证组织的信息安全管理体系认证资格：

1）获证组织申请注销认证证书；

2）认证证书有效期届满，未申请延续使用；

3）因换发新证书而注销旧证书；

4）其他原因需要注销认证证书。

10.7 撤销或注销信息安全管理体系认证的信息通过“认证认可信息统一上报平台”上报，可通过“全国认证认可信息公共服务平台”公开获取，并在 YHRZ 网站上公布。YHRZ 将以书面通知获证组织有关撤销或注销认证证书的信息，要求获证组织立即停止使用任何引用信息安全管理体系认证资格的广告材料。

10.8 在任何组织提出请求时，YHRZ 应正确说明获证组织的认证证书被暂停、撤销、注销或缩小的情况。

11.认证证书

11.1 证书有效期

认证证书有效期为三年

11.2 证书内容

11.2.1 认证证书内容应以中文书写，至少包括以下方面：

1）认证证书名称，例如：信息安全管理体系认证证书；

2）证书编号；

3）获证组织名称，获证组织信息安全管理体系认证的每一场所的名称和可识别的物理位置；

4）符合本文件的认证依据；

5）与获证组织信息安全管理体系内所从事活动相适宜的认证范围，包括服务、过程等；

6）授予、扩大或更新认证的日期以及与再认证周期相一致的认证有效期。如：颁证日期：2023 年 12 月 1 日，有效期：2023 年 12 月 1 日至 2026 年 11 月 30 日；

7）YHRZ 的名称及其标志；

8）YHRZ 的印章和法定代表人代表或其授权人的签字；

9）认可标识及认可注册号(应为国家认监委确定的认可机构的标识，以申请认可为目的发出的证书可没有此内容)；

11.2.2 如果认证所覆盖业务的类别及其所涉及的过程和覆盖的场所较多，需在证书附件上加以注明。

11.3 证书编号

11.3.1 对同一个组织实施的同一个信息安全管理体系认证，赋予一个认证证书编号。

11.3.2 同一个组织的认证范围覆盖多个场所并需要颁发子证书时，在子认证证书编号后加上“-”和序号，如-1(-2，-3，…)。

11.3.3 有效期内换发证书，认证证书编号和认证的有效期保持不变，应注明换证日期。

11.3.4 再认证完成后换发证书，按规定重新赋予认证证书编号，第一次再认证为“R1”，第二次再认证为“R2”，依此类推。

11.3.5 撤销证书后，原认证证书编号废止，不再它用。

11.3.6 认证证书上的认证机构名称应与相应的认证机构批准书上的名称一致。

11.3.7 对获证组织正确宣传认证结果的控制

获证组织应当在广告、宣传等活动中正确使用认证证书和有关信息，不得利用管理体系认证证书和相关文字、符号，误导公众认为其产品、服务通过认证。

获证组织的信息安全管理体系发生重大变化时，获证组织应当向 YHRZ 申请变更，未变更或者经 YHRZ 调查发现不符合认证要求的，不得继续使用该认证证书。例如与下列方面有关的变更：

a）法律地位、经营状况、组织状态或所有权；

b）组织和管理层（如关键的管理、决策或技术人员）；

c）联系地址和场所；

d）获证信息安全管理体系覆盖的运作范围；

e）信息安全管理体系和过程的重大变更。

12.受理转换认证证书

12.1 YHRZ 应当履行社会责任，严禁以牟利为目的受理不符合 ISO/IEC 27001 标准、不能有效执行信息安全管理体系的组织申请认证证书的转换。

12.2 YHRZ 受理组织申请转换为本机构的认证证书，应该详细了解申请转换的原因，必要时进行现场审核。

12.3 被发证的认证机构撤销证书的，除非该组织进行彻底整改，导致暂停或撤销认证证书的情形已消除，否则不应受理其认证申请。

12.4 在转换合同签订前，通过“认证认可信息统一上报平台”提交转入备案申请，在接收到平台备案成功的反馈后，签订转换合同，实施转换。

13.申诉和投诉

13.1 申请认证客户或获证客户对认证决定有异议时，可在决定正式发布 10 日内向 YHRZ 提出申诉，YHRZ 自收到申诉之日起，在 60 日内进行处理，并将处理结果书面通知申诉人，具体参照 YHRZ 申诉投诉管理相关规定。

13.2 若申诉人认为 YHRZ 未遵守认证相关法律法规或本文件并导致自身合法权益受到严重侵害的，可以直接向认证监管部门投诉。

14.认证记录的管理

14.1 YHRZ 应当建立认证记录保持制度，记录认证活动全过程并妥善保存。

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，保存时间至少应当与认证证书有效期一致。

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.收费

认证费用按照 YHRZ 的相关认证收费标准收取。

16.其他

16.1 本文件内容提及应用的相关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标准号时，均应采用有效版本的完整标准号。

16.2 本文件所提及的各类证明文件的复印件应是在原件上复印的，并经审核员签字确认与原件一致。

16.3 YHRZ 可开展信息安全管理体系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信息安全管理体系标准。

附录 A：

信息安全管理体系认证审核时间表（仅适用于初次审核）

有效人数	审核时间 第 1 阶段＋第 2 阶段 （人天）	有效人数	审核时间 第 1 阶段＋第 2 阶段 （人天）
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：表中的人数宜视为连续变化的，而不是阶梯式。即如果画成曲线图，线段的起点宜来自表格上一栏值的值，并以表格每栏值为每段的终点。曲线的起点是人数为 1 时对应的人天。对非整数审核人日，宜将其调整为最接近的半人日数。

注 2：有效人数，由认证范围内所涉及的所有人员（包括倒班人员）组成。在认证范围内的人员，还应包括非永久雇员（例如合同工）和兼职人员。根据其所工作的小时数，可减少或增加兼职人数和部分工作包含在认证范围内的员工，并转化为等效的全职员工数量。当大量员工从事重复性的活动或任务时，允许减少认证范围内的员工数量。这种减少要有条理，要根据每个客户的情况进行一致地应用。

注 3：一个审核人日通常为 8 小时，是否可以包括午饭休息时间以当地法定要求为准。往返多审核场所之间所花费的时间不计入有效的管理体系认证审核时间。

注 4：审核时间的增减应记录合理的理由。

注 5：监督审核人日不少于初次审核确定的人日的 1/3，再认证审核人日不少于初次审核确定的人日的 2/3。

附录 B：

信息安全管理体系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	国家机关	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	包括互联网内容提供
	02.03	二	科研	涉及特别重大项目的应该提升为一级
	02.04	二	社会保障	例如社会保障基金管理、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，包括网络游戏
	03.03	一	物流	包括邮政
	03.04	三	咨询中介	例如法律、会计、公证、审计等
	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、输、变、配电
	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	

附录 C：

证书样式

信息安全管理体系认证证书

证书编号：**********

兹 证 明

**********公司

统一社会信用代码：**********

注册地址：**********

经营地址：**********

经现场评审符合

ISO/IEC 27001:2022
《信息安全 网络安全 隐私保护 安全管理体系 要求》

认证范围

****

发证日期：**年**月**日

有效期至：**年**月**日

证书签发人：

二维码

亿寰认证中心

YIHUAN CERTIFICATION CENTER CO.,LTD. 亿寰认证中心有限公司 证书专用章 4301041001019

本证书信息可在中国国家认证认可监督委员会官方网站（www.cnca.gov.cn）查询，
亦可登录亿寰认证中心有限公司官方网站（www.yihuaniso.com)查询或扫描二维码查询

亿寰认证中心有限公司

有效期三年内需两次现场监督审核，首次监督审核在初审后12个月内，此后监督审核至少每个日历年进行一次

湖南省长沙市岳麓区梅溪湖街道瞻星路56号中海湖润家园一期1栋2016-2028房