认 证 规 则

信息安全管理体系认证实施规则

编 号：ZXB-ISMS-2025

受控状态：受 控

版本	编修	审核	批准	编写/修订日期	发布日期
A/0	崔海军	张京梅	郑宇兵	20250820	20250830
A/0	崔海军	张京梅	郑宇兵	20251222	20251222

管理体系手册编制/修订履历

版本	修订内容	编写日期/修订日期	发布日期
A/0	新编	20250820	20250830
A/0	统一版本号和依据文件中文名称	20251222	20251222

目录

一、适用范围

1.1 本规则用于规范众信标（北京）认证有限公司（以下简称：ZXB）依据 ISO/IEC 27001:2022 《信息技术 安全技术 信息安全管理体系 要求》标准开展的信息安全管理体系认证活动。

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，对信息安全管理体系认证实施过程作出具体规定，明确公司对认证过程的管理责任，保证信息安全管理体系认证活动的规范有效。

1.3 本规则是公司在信息安全管理体系认证活动中的基本要求，公司在该项认证活动中应当遵守本规则。除本文件规定的信息安全管理体系特定要求外，应遵循公司基本管理要求和各项管理制度。

二、认证依据（技术规范、强制性要求或标准）

ISO/IEC 27001:2022 《信息技术 安全技术 信息安全管理体系 要求》

三、认证人员要求

3.1 认证人员基本要求

认证人员应当遵守与从业相关的法律法规，对认证活动及作出的认证审核报告和认证结论的真实性承担相应的法律责任。

3.2 认证审核人员应具备 CCAA 注册的信息安全管理体系审核员资质要求。

四、认证程序

4.1 受理认证申请

4.1.1 申请组织应满足以下条件:

(1)取得法人资格(或其组成部分);

(2)取得相关法规规定的行政许可(适用时);

(3)已按认证标准建立 ISMS 体系,且运行满三个月，且至少已实施一次完整内审

和管理评审;

(4)未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”:

(5)遵守有关主管部门对信息安全管理的强制性要求,或相关要求(适用时)，两年内未发生信息安全事故或违反相关法规的情况(经审批可放宽至-年内);

(6)承诺遵守工信部联协[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(例如，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》)。;

(7)其他应具备的条件。

4.1.2 公司应当要求申请组织至少提交以下资料:

(1)认证申请书，申请书应包括申请认证的生产、经营或服务活动范围及活动情况的说明。

(2)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)。

(3)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。

(4)信息安全管理体系成文信息(适用时)，包括 1)体系范围，2)方针，3)目标，4)信息安全风险评估准则及报告，5)信息安全风险处置计划，6)残余风险评估报告(适用时)，7)适用的信息安全法律法规要求清单;8)网络拓扑结构图(适用时)，9)组织机构图或职责说明，10)覆盖申请范围的 1 个或多个适用性声明(SOA)

注:以上文件若包含在手册、程序文件中可不单独提供

(5)工信部安全审查备案(适用时);

(6)说明适用的关于认证机构的资质、信息安全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，以便判断公司是否具备对该客户实施认证活动的资格或条件。

4.1.3 公司应对申请组织提交的申请资料进行评审,根据申请认证的活动范围及场所、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。

4.1.4 对符合上述要求的，公司可决定受理认证申请;对不符合上述要求的，公司应通知申请组织补充和完善，或者不受理认证申请。

4.2 申请评审

4.2.1 申请评审

4.2.1.1 满足以下条件的，认证机构可以受理认证申请：

（1）认证委托人已具备受理条件；

（2）认证机构具备实施认证的能力；

（3）双方就认证事宜达成一致。

4.2.1.2 ZXB 收到申请材料后，由运营部完成评审，重点审查以下内容：

(1) 材料完整性：确认申请材料是否齐全、信息是否准确；

(2) 范围合理性：评估申请的认证范围是否明确、是否与组织业务匹配；

(3) 体系文件符合性：初步审查《信息安全管理手册》是否覆盖 ISO/IEC 27001:2022 《信息技术 安全技术 信息安全管理体系 要求》核心要素，程序文件是否具有可操作性；

若材料不完整或不符合要求，组织需进行补充完善；只有在申请材料通过评审后，认证机构才会受理组织的认证申请，并与组织沟通确定后续的认证安排。

4.2.1.3 对于新的认证委托人，仅在同时满足下列情况的前提 下，认证机构可实施认证转换，否则应按照初次认证开展认证活动：

（1）认证机构具有认证委托人申请认证的 ISMS 认证范围的认可资格；

（2）原认证证书处于有效期内，未被原认证机构实施暂停或撤销；

（3）原认证机构认证业务正常运行，不存在认可资格到期、被暂停或撤销的问题；

（4）认证机构应获得认证委托人初次认证审核报告或最近一次的再认证审核报告、监督审核报告、审核中发现的不符合及其纠正措施。

4.3 签订合同

在实施认证审核前,公司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信息安全管理体系的承诺。

(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重大变更时，应及时向公司通报。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;信息安全管理体系覆盖的活动范围变更;信息安全管理体系和重要过程的重大变更等;出现影响信息安全管理体系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,不利用信息安全管理体系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)拟认证的信息安全管理体系覆盖的生产或服务的活动范围。

(6)在认证审核实施过程及认证证书有效期内，公司和申请组织各自应当承担的责任、权利和义务。

(7)认证服务的费用、付费方式及违约条款。

4. 4 方案策划

4.4.1 ZXB 应针对每一认证委托人建立认证周期内的审核方案，以清晰地识别所需的审核活动。全认证周期审核方案（认证周期为 3 年），内容包括：审核阶段划分：初次认证（第一阶段 + 第二阶段）、监督审核（第 1 年 / 第 2 年各 1 次）、 再认证（第 3 年）；

4.4.2 审核时间:

组织有效人数应包括认证范围内组织的在册员工数量和非固定人员(组织认证范围内的兼职、承包商/分包商人员、施工人员等)。根据确定的组织有效人数，按照本规范附录 A 确定基础审核人日和风险等级。

4.4.2.1 为确保认证审核的完整有效，公司应根据申请组织信息安全管理体系覆盖的活动范围、特性、技术复杂程度、信息安全因素风险程度、认证要求和体系覆盖范围内的有效人数等情况，核算并拟定完成审核工作需要的时间。在特殊情况下，可以减少审核时间，但减少的时间不得超过所规定的审核时间的 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%。

4.4.2.2 多场所和抽样

当客户组织申请认证涉及多场所，且多场所不涉及中心职能时，可依据 CC11《多

场所组织的管理体系审核与认证》文件要求执行抽样。

4.4.3 审核组

4.4.3.1 公司应当根据信息安全管理体系覆盖的活动的专业技术领域选择具备相关能力的审核员组成审核组，必要时可以选择技术专家参加审核组。审核组中的审核员承担审核任务和责任。

4.4.3.2 技术专家主要负责提供认证审核的技术支持，不作为审核员实施审核，不计入审核时间，其在审核过程中的活动由审核组中的审核员承担责任。

4.4.3.3 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。

4.4.3.3 审核组成员不得与认证委托人存在利益关系。

4.5 审核计划

认证机构应依据审核方案制定每次现场审核的审核计划。审核计划至少包括：审核目的、审核准则、审核范围、风险程度、技术复杂程度、现场审核的日期、时间安排和场所、审核组成员及审核任务安排。其中，审核员应注明 ISMS 审核员注册号，专业领域审核员和技术专家应标明专业代码，兼职审核员和在职技术专家应注明工作单。

现场审核应安排在认证委托人的生产或服务处于正常运行时进行。

现场审核开始前，应将审核计划提交给认证委托人并经其确认。如需要临时调整审核计划，应经双方协商一致后实施。

4.6 实施审核

4.6.1 文件审核

组长或组织相关审核员对受审核方的信息安全管理体系文件及必要的其它文件进行符合性评审，以确定审核的可行性，并确信能够实现审核目标。对评审中发现问题和评审结论应形成《文件评审报告》并提出明确的整改要求和时限。

4.6.2 第一阶段审核

4.6.2.1 第一阶段审核应至少覆盖以下内容:

(1)结合现场情况，确认申请组织实际情况与信息安全管理体系成文信息描述的一致性，特别是体系成文信息中描述的产品和服务、部门设置和职责与权限、

生产或服务过程等是否与申请组织的实际情况相一致。

(2)结合现场情况，审核申请组织理解和实施 ISO/IEC 27001:2022 《信息技术 安全技术 信息安全管理体系 要求》标准要求的情况，评价信息安全管理体系运行过程中是否实施了内部审核与管理评审，确认信息安全管理体系是否已运行并且超过 3 个月。

(3)确认申请组织建立的信息安全管理体系覆盖的活动内容和范围、体系覆盖范围内有效人数、过程和场所，遵守适用的法律法规及强制性标准的情况；核心信息处理设施，IT 部门的设计和开发维护部门，信息备份方法。

(4)结合信息安全管理体系覆盖产品和服务的特点识别对信息安全目标的实现具有重要影响的关键点，并结合其他因素，科学确定重要审核点。

(5)与申请组织讨论确定第二阶段审核安持。对信息安全管理体系成文信息不符合现场实际、相关体系运行尚未超过 3 个月或者无法证明超过 3 个月的，以及其他不具备二阶段审核条件的，不应实施二阶段审核。

4.6.2.2 在下列情况，第一阶段审核可以不在申请组织现场进行，但应记录未在现场进行的原因:

(1)申请组织已获本公司颁发的其他有效认证证书，公司已对申请组织信息安全管理体系有充分了解。

(2)公司有充足的理由证明申请组织的生产经营或服务过程过程简单且信息安全影响风险较低,通过对其提交文件和资料的审查可以达到第一阶段审核的目的和要求。

(3)申请组织获得了其他经认可机构认可的认证机构颁发的有效的信息安全管理体系认证证书,通过对其文件和资料的审查可以达到第一阶段审核的目的和要求。

除以上情况之外,第一阶段审核应在受审核方的生产经营或服务现场进行。

4.6.2.3 审核组应将第一阶段审核情况形成书面文件告知申请组织。对在第二阶段审核中可能被判定为不符合项的重要关键点，要及时提醒申请组织特别关注。

4.6.3 第二阶段审核

第二阶段审核应当在申请组织现场进行。重点是审核信息安全管理体系符合 ISO/IEC 27001:2022 《信息技术 安全技术 信息安全管理体系 要求》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)对信息安全管理体系覆盖的过程和活动的管理及控制情况，信息安全风险评估。

(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。

发生以下情况时，审核组应向公司报告，经公司同意后终止审核。

(1)受审核方对审核活动不子配合，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。

4.7 不符合项纠正和纠正措施及验证要求

4.7.1 不符合项分类

根据不符合的严重程度，分为 “严重不符合” 和 “一般不符合”：

严重不符合：存在以下情形之一，视为严重不符合：

a) 信息安全管理体系核心要素缺失；

b) 违反法律法规要求；

c) 多个一般不符合集中在同一要素；

d) 上次审核的一般不符合重复发生；

e) 信息安全相关重大事故未采取纠正措施。

一般不符合：孤立的、轻微的不符合，不影响体系整体有效性。

4.7.2 不符合项处置流程

(1) 开具报告：审核组需在现场审核结束前，向组织出具《不符合项报告》，明确不符合事实、判定依据、整改要求；

(2) 整改期限：严重不符合需在规定时间内内完成整改，一般不符合需在 30 个工作日内完成；

(3) 验证方式：

书面验证：组织提交整改材料，审核组长通过文件验证整改有效性；

现场验证：严重不符合或整改涉及复杂流程，需安排现场验证；

下次监督验证：轻微且不影响体系运行的一般不符合，可在下次监督审核中验证。

4.7.3 整改关闭

审核组长需在收到整改材料后完成验证，确认整改有效的；整改无效的，要求组织重新整改，逾期未完成的，不应当给予该受审核方推荐认证、保持认证或再认证。

4.8 审核报告

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。

(5)审核活动的实施日期和地点，包括固定现场和临时现场;对偏离审核计划情况的说明，包括对审核风险及影响审核结论的不确定性的客观陈述。

(6)叙述程序及各项要求的审核工作情况。

(7)识别出的不符合项。

(8)审核组对是否通过认证的意见建议。

五、复核、认证决定

5.1 复核

ZXB 技术部需在收到第二阶段审核报告及整改材料后将审核资料提交给认证机构的技术评定人员进行复核，复核内容包括：

(1) 审核过程合规性：审核计划是否执行，审核证据是否充分，不符合项判定是否准确；

(2) 整改有效性：不符合项整改材料是否完整，验证结论是否合理；

(3) 体系符合性：是否覆盖 ISO/IEC 27001:2022 《信息技术 安全技术 信息安全管理体系 要求》全部要求，是否符合相关法律法规；

(4) 认证范围合理性：确认认证范围与组织实际信息安全管理体系活动一致。

若复核发现问题，需要求审核组补充审核；若整改无效，需要求组织重新整改。

5.2 认证决定

5.2.1 决定主体

审核组成员不得参与对审核项目的认证决定。

5.2.2 决定条件

对于符合认证要求的申请人，应颁发认证证书。对于不符合认证要求的申请人，应以书面的形式明示其不能通过认证的原因。

通过认证：满足以下全部条件，颁发认证证书：

(1) 第二阶段审核报告结论为 “推荐认证”；

(2) 不符合项已全部整改并验证有效；

(3) 组织已履行认证合同义务；

(4) 信息安全管理活动符合相关法律法规要求。

不通过认证：存在以下情形之一，出具《不予认证通知》：

(1) 体系存在严重不符合，且整改无效；

(2) 审核证据表明体系未实际运行；

(3) 组织存在重大信息安全违规行为；

(4) 未履行认证合同义务。

5.2.3 决定通知与信息报送

ZXB 在颁发认证证书后 30 个工作日内按照规定的要求将相关信息报送国家认监委。证书信息可在：国家认证认可监督管理委员会官方网站（www.cnca.gov.cn）或众信标（北京）认证有限公司官方网站（www.zhongxinbiao.com/）上查询。

5.2.4 利益回避

ZXB 不得将组织是否通过认证与审核员薪酬挂钩，确保决定客观公正。

六、 监督审核

6.1 ZXB 应对获证组织进行有效跟踪，依据审核方案 对获证组织开展监督审核，并要求获证组织的最高管理者参与审核访谈，以确认获证组织 ISMS 与 ISO/IEC 27001:2022 《信息技术 安全技术 信息安全管理体系 要求》标准的持续符合性

和运行的有效性。

6.2 每次监督审核应尽可能覆盖认证范围内的典型产品/ 服务及有代表性的生产/服务过程，并确保在认证证书有效期内 的监督审核覆盖认证范围内的所有典型产品/服务、有代表性的 生产/服务过程。

6.3 监督审核应重点关注获证组织的变更以及 ISMS 绩效的持续改进，监督审核的内容至少包括：

（1）内部审核和管理评审；

（2）对上次审核确定的不符合采取的纠正措施及效果；

（3）ISMS 在实现获证组织目标和 ISMS 预期结果方面的有效性；

（4）为持续改进而策划的活动的进展；

（5）持续的运作控制；

（6）任何变更；

（7）认证证书、认证标志的使用和（或）任何其他对认证 信息的引用；

（8）ISMS 相关投诉的处理；

（9）上次审核后发生的信息安全事故的调查与处理。

6.4 监督审核的时间应根据获证组织当前有效人数和 ISMS 风险类型确定，不少于依据附录 A 所确定的初次认证审核时间的 1/3。

七、再认证审核

7.1 认证证书期满前，获证组织申请继续持有认证证书的， 认证机构应依据审核方案实施再认证审核，以判断获证组织的 ISMS 作为一个整体与 ISO/IEC 27001:2022 《信息技术 安全技术 信息安全管理体系 要求》持续符合性和运行的有效性。

7.2 再认证审核应在获证组织现场进行，并应在认证证书到期前完成。再认证审核的内容至少应包括：

（1）结合其内部信息安全和外部信息安全的变化情况，确认获证组织 ISMS 有效性及认证范围的持续相关性和适宜性；

（2）ISMS 绩效持续改进的证实；

（3）ISMS 在实现获证组织目标和 ISMS 预期结果方面的有效性。

7.3 再认证审核策划时应考虑获证组织最近一个认证周期内的 ISMS 绩效，包括调阅以往的监督审核报告。

7.4 再认证审核的审核时间应按要求，根据获证组织当前有效人数和 ISMS 风险类型情况来确定，不少于依据附录 A 所确定的初次认证审核时间的 2/3。

7.5 特殊审核

7.5.1 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。

7.5.2 提前较短时间通知的审核为调查投诉、信息安全事故，对变更做出回应或对被暂停的客户进行追踪，可能需要在提前较短时间或不通知获证组织的情况下进行审核，此时：

（1）认证机构应说明并使获证组织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，认证机构应在指派审核组时给予更多的关注。

7.5.3 获证组织认证范围内抽查中被查出不合格时，自市场监管部门发出通报起 30 日内，认证机构应对该组织实施提前较短时间通知的审核。

八、认证证书状态管理规定、要求

信息安全管理体系认证证书的 “批准、拒绝、保持、扩大、缩小、暂停、恢复、撤销” 全生命周期管理。

8.1 批准认证资格

8.1.1 批准条件

(1) 申请材料真实、完整；

(2) 体系符合 ISO/IEC 27001:2022《信息技术 安全技术 信息安全管理体系 要求》要求，审核结论为 “推荐认证”；

(3) 认证范围在组织法律地位及资质范围内；

(4) 不符合项已整改并验证有效；

(5) 组织已签订认证合同并缴纳费用。

8.1.2 批准流程

ZXB 认证决定委员会审议通过后，由法定代表人或授权人签发证书，经 ZXB 评定，认为认证客户在认证范围内已满足批准认证资格的条件，同意批准再认证注册。

8.2 拒绝认证

(1) 体系不符合标准核心要求，审核结论为 “不推荐认证”；

(2) 申请材料伪造；

(3) 组织存在重大信息安全违规行为；

(4) 未履行认证合同义务。

ZXB 需出具《不予认证注册通知》，说明理由，送达组织。

8.3 保持认证资格

8.3.1 保持条件

(1) 按时接受监督审核，结论为 “证书继续有效”；

(2) 体系持续符合标准要求，信息安全管理活动合规；

(3) 及时通报重大变更；

(4) 按规定使用证书和标志，无违规行为；

(5) 履行认证合同义务。

8.3.2 保持流程

每次监督审核通过后，ZXB 出具监督审核标识，确认证书持续有效。

8.4 扩大认证范围

8.4.1 扩大条件

(1) 组织已保持认证资格 1 年以上；

(2) 新增范围符合法律资质要求；

(3) 新增范围的体系文件已编制，且运行至少 1 个月；

(4) 已缴纳扩大范围的认证费用。

8.4.2 扩大流程

(1) 组织提交《扩大认证范围申请书》及新增范围的体系文件、运行记录；

(2) ZXB 开展文件审核 + 现场审核；

(3) 审核通过后，ZXB 换发证书。

8.5 缩小认证范围

8.5.1 缩小条件

(1) 组织停止某类管理活动；

(2) 某类管理活动不再符合标准要求；

(3) 缩小范围不得为规避审核风险。

8.5.2 缩小流程

(1) 组织提交《缩小认证范围申请书》，说明理由；

(2) ZXB 验证缩小理由的真实性；

(3) 验证通过后，ZXB 收回原证书，换发新证书。

8.6 暂停证书

8.6.1 暂停情形

组织存在以下情形之一，ZXB 在调查核实后 5 个工作日内暂停证书：

(1) 体系持续或严重不符合要求；

(2) 未履行认证合同义务；

(3) 被监管机构责令停业整顿；

(4) 资质文件过期；

(5) 主动申请暂停。

8.6.2 暂停期限

一般暂停期限最长 6 个月；

资质文件过期导致的暂停，期限可至新资质文件下发之日。

8.6.3 暂停通知

ZXB 需出具《证书暂停通知》，明确暂停起始时间、期限，声明 “暂停期间不得使用证书及标志”。

8.7 恢复认证资格

8.7.1 恢复条件

(1) 暂停原因已消除；

(2) 暂停期间未使用证书及标志；

(3) 已提交《恢复认证资格申请书》及整改材料。

8.7.2 恢复流程

(1) ZXB 审核整改材料，必要时开展现场验证；

(2) 验证通过后，ZXB 出具《恢复证书使用通知》，公告恢复信息；

(3) 暂停期限届满未恢复的，证书自动撤销。

8.8 撤销证书

8.8.1 撤销情形

组织存在以下情形之一，ZXB 在调查核实后 5 个工作日内撤销证书：

(1) 法律地位被注销；

(2) 提供虚假材料；

(3) 发生重大信息安全事故，且确认是体系失效导致；

(4) 暂停期限届满未恢复；

(5) 违规使用证书。

8.8.2 撤销流程

(1) ZXB 出具《证书撤销通知》，说明理由；

(2) 收回原证书；无法收回的，在 ZXB 官网及国家认监委官网公告撤销；

(3) 撤销信息需报送国家认监委。

8.9 信息公示

ZXB 需在官网实时公示证书状态（正常 / 暂停 / 撤销），接受社会监督。

九、认证证书及认证标志的要求

9.1 认证证书内容

证书需至少包含以下信息：

(1) 获证组织名称、地址；

(2) 认证范围；

(3) 认证依据（ISO/IEC 27001:2022 《信息技术 安全技术 信息安全管理体系 要求》）；

(4) 证书编号；

(5) ZXB 名称及标志；

(6) 证书签发日期、有效期（3 年）；

(7) 认可标识及认可注册号（适用时）；

(8) 查询方式（ZXB 在颁发认证证书后 30 个工作日内按照规定的要求将相关信息

报送国家认监委。证书信息可在：国家认证认可监督管理委员会官方网站（www.cnca.gov.cn）或众信标（北京）认证有限公司官方网站（www.zhongxinbiao.com/）上查询。）。

9.2 认证证书有效期

证书有效期最长 3 年，自签发之日起计算；

再认证通过后，新证书有效期自原证书到期日起计算。

9.3 认证标志要求

a)获证客户在传播媒介(如互联网、宣传册或广告)或其他文件中引用认证状态时，应符合 ZXB 的要求。

b）使用 ZXB 的认证标志，需向 ZXB 提出申请。在使用时，其图案必须按照 ZXB 提供的 图案的比例放大或缩小，并且做到颜色一致。未经 ZXB 许可不得使用认证标志；

c) 不得在任何资料中有关于其认证资格的误导性说明； d）不得以误导性方式使用认证文件或其任何部分；

e) 不得利用管理体系认证证书和相关文字、符号，暗示或误导公众认为认证证书覆盖 范围外的管理体系、产品或服务、过程、活动和场所获得 ZXB 的认证；

f) 宣传认证结果时不得损害 ZXB 的声誉和（或）使认证制度声誉受损，失去公众信任；g) 不得擅自更改证书内容；

h) 不得伪造、涂改、出借、出租、转让、倒卖、部分出示、部分复印证书；

i) 获证客户应妥善保管好认证证书，以免丢失、损坏；

j) 获证客户的管理体系若发生重大变化时，应及时报告 ZXB ，接受 ZXB 的调查或监督 检查。对经监督检查不合格者，不得继续使用认证证书；

k) 在认证范围被缩小时，应及时修改所有的广告宣传材料；

l) 认证证书被暂停期间，相应的认证领域的管理体系认证暂时无效。认证客户应停止 使用认证证书和认证标志，直到造成暂停的问题得到解决。如果客户在规定的时限内未能解 决造成暂停的问题，ZXB 将撤销或缩小相应领域的认证范围；

m) 证书被 ZXB 撤销，获证客户应按 ZXB 的要求将证书交还给 ZXB ，并同时使用所有引 用认证资格的广告材料。停止在文件、网站、广告和宣传资料中或广告宣传等商业活动，以 及在工作场所、销售场所展示认证证书；

n）不应允许其标志被获证客户用于实验室检测、校准或检验的报告或证书；

o) 标志不应用于产品或产品包装之上，或以任何其它可解释为表示产品符合性的方式 使用；注：产品包装的判别标准是其可从产品上移除且不会导致产品分裂、破裂或损坏。

p）认证证书和认证标志的使用应符合规定；

q）认证标志使用时可以等比例放大或缩小，但不允许变形、变色；

r）证书持有人应对认证证书和认证标志的使用和展示进行有效的控制。

十、信息通报

获证组织需建立《信息安全管理体系信息通报程序》，及时向 ZXB 通报以下信息：

10.1 组织运营信息

法律地位变更、所有权变更；

经营状况重大变化；

行政许可 / 资质变更。

10.2 信息安全管理信息

信息安全类别重大变更；

信息安全管理体系重大变更；

重大信息安全事故；

客户或相关方重大投诉；

国家监督检查结果。

10.3 通报方式

需以书面形式发送至 ZXB 运营部，必要时需提供佐证材料。

十一、受理申诉和投诉

11.1 申诉（组织对认证决定有异议）

组织需在收到《认证决定通知书》后 15 个工作日内，向 ZXB 提交《申诉申请书》，说明异议理由并提供证据；

ZXB 需在收到申诉后 60 日内完成调查，出具《申诉处理结果通知书》；

组织对申诉结果仍有异议的，可向国家认监委或相关认可机构投诉。

11.2 投诉（外部相关方对认证活动有异议）客户、监管机构等相关方可向 ZXB 投诉；

ZXB 需在收到投诉后 5 个工作日内受理，30 日内完成调查，出具《投诉处理结果通知书》；投诉情况属实的，ZXB 需采取纠正措施。

十二、记录管理

12.1 ZXB 应当建立认证纪录保持制度，记录认证活动全过程并妥善保存。

12.2 记录应当真实准确以正式认证活动得到有效实施。保存时间至少应当与认证证书有效期一致。

12.3 记录可以用纸质或电子文档的方式加以保存。

附录 A-信息安全管理体系认证审核时间表

表 1-1 审核时间表

雇员总数量	ISMS 初次审核 审核时间（审核人日）	增加或减少的因素	总审核时间
1 ~ 10	5	见本附录 1.2	
11 ~ 25	7	见本附录 1.2	
26 ~ 45	8.5	见本附录 1.2	
46 ~ 65	10	见本附录 1.2	
66 ~ 85	11	见本附录 1.2	
86 ~ 125	12	见本附录 1.2	
126 ~ 175	13	见本附录 1.2	
176 ~ 275	14	见本附录 1.2	
276 ~ 425	15	见本附录 1.2	
426 ~ 625	16.5	见本附录 1.2	

626 ~ 875	17.5	见本附录 1-2,1-3,1-4,1-5	
876 ~ 1175	18.5	见本附录 1-2,1-3,1-4,1-5	
1176 ~ 1550	19.5	见本附录 1-2,1-3,1-4,1-5	
1551 ~ 2025	21	见本附录 1-2,1-3,1-4,1-5	
2026 ~ 2675	22	见本附录 1-2,1-3,1-4,1-5	
2676 ~ 3450	23	见本附录 1-2,1-3,1-4,1-5	
3451 ~ 4350	24	见本附录 1-2,1-3,1-4,1-5	
4351 ~ 5450	25	见本附录 1-2,1-3,1-4,1-5	
5451 ~ 6800	26	见本附录 1-2,1-3,1-4,1-5	
6801 ~ 8500	27	见本附录 1-2,1-3,1-4,1-5	
8501 ~ 10700	28	见本附录 1-2,1-3,1-4,1-5	
＞ 10700	沿用 以上规律	见本附录 1-2,1-3,1-4,1-5	

对上述表 1-1 及 ISMS 审核时间说明：

A.1 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 1-1 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。

A.2 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”减少到表表 1-1 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%是一个基于 ISMS 审核经验所考虑的系数。

A.3 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。

A.4 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。

A.5 信息安全管理体系调整审核时间的因素不能孤立的使用表 1-1，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 8.5.3 条款的、与 ISMS 相关的变更的数量和程度。A.6 如上述 a）-h）所列举的，表 1-2 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获得一个符合的审核时间计算方案。

表 1-2 审核时间计算因数的分类

对工作量的影响 / 因数（见 A.5）	减少工作量	正常工作量	增加工作量

对工作量 因数　　的影响 （见 A.5）	减少工作量	正常工作量	增加工作量
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； 2-3 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，灵活的过程执行。
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	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	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

对工作量 因数　　的影响 （见 A.5）	减少工作量	正常工作量	增加工作量
平台的数量、隔离网络的数量]；	据库、网络等）；		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 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； 若干个数据心；

对工作量 因数　　的影响 （见 A.5）	减少工作量	正常工作量	增加工作量
h）对于监督或再认证审核：符合 GB／T 27021.1-2017　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；

7)审核时间计算的示例

以下示例阐述了认证机构如何使用 A.5 中 a）-h）所列举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 1-3 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 1-4 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 1-5 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 5-1）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。

表 1-3 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. 一般的过程，涉及一般的且重复性的任务；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. 一般的但不重复的过程，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 涉及复杂性高的过程，或数量相对较大的活动，或独特的活动）。
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 是新且没有建立。
a：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、形象和政府运行能力的风险，从而可能对国家造成非常重大的负面影响。	

表 1-4 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 1-5 因数对 ISMS 审核时间的影响

IT 复杂性	低	中	高
业务复杂性	（3-4）	（5-6）	（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 %

示例 1：

受审核的组织有 700 人，因此根据**表 1-1**，其初次认证审核需要 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。根据表 1-3 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，但大量地使用外包。该组织没有内部的或外包的开发活动。根据表1-4，可以得出与IT环境相关的因子为1+3+1=5。利用表1-5，可以得出该审核时间无需调整。

示例2：

还是示例1中的这个组织，但其已有多个管理体系且已较好地建立了ISMS。根据表1-3，与业务和组织相关的因子将变为：1+1+1=3。根据表1-5，将得出需要减少5%~10%的审核时间，即：审核时间将减少1到1.5人天，变为16到16.5人天。

国际标准

ISO/IEC 27001 标准

第三版
2022-10

信息安全 网络安全和隐私保护 信息安全管理体系要求

参考号ISO/IEC 27001:2022（E）

受版权保护的文档

ISO版权办公室
CP 401•Ch.de Blandonnet 8
Ch-1214 Vernier，日内瓦电
话：+41 22 749 01 11
电子邮件：copyright@iso.org
网址：www.iso.org

在瑞士出版

内容页

目录

前言

ISO（国际标准化组织）和IEC（国际电工委员会）构成了全球标准化的专门体系。作为ISO或IEC成员的国家机构通过各自组织为处理特定技术活动领域而设立的技术委员会参与国际标准的制定。ISO和IEC技术委员会在共同感兴趣的领域进行合作。与ISO和IEC保持联系的其他国际组织，包括政府组织和非政府组织也参与了这项工作。

ISO/IEC指令第1部分描述了用于编制本文件的程序及其进一步维护的程序。特别是，应注意不同类型文件所需的不同批准标准。本文件根据ISO/IEC指令第2部分的编辑规则起草（见www.ISO.org/Directives或www.IEC.ch/members_experts/refdocs）。

请注意，本文件的某些要素可能是专利权的主题。ISO和IEC不对识别任何或所有此类专利权负责。文件开发过程中确定的任何专利权的详细信息将在引言和/或收到的ISO专利声明列表（见www.ISO.org/patents）或IEC专利声明列表中（见https:/patents.IEC.ch）。

本标准中使用的任何商品名称都是为方便用户而提供的信息，不构成背书。

有关标准的自愿性质的解释、与合格评定相关的ISO特定术语和表达的含义，以及ISO在技术性贸易壁垒（TBT）中遵守世界贸易组织（WTO）原则的信息，请参见www.ISO.org/ISO/foreword.html。在IEC中，请参阅www.IEC.ch/understanding-standards。

本标准由ISO/IEC JTC 1信息技术联合技术委员会SC 27信息安全、网络安全和隐私保护小组委员会编制。

本第三版取消并取代了已进行了技术修订的第二版（ISO/IEC 27001:2013），第三版还包含了技术勘误ISO/IEC 27001:2013/Cor 1:2014和ISO/IEC 2.7001:2013/Cor 2:2015。

主要变化如下：

该标准与管理体系标准和ISO/IEC 27002:2022的统一结构保持一致。

有关本标准的任何反馈或问题都应提交给用户的国家标准机构。这些机构的完整清单可在www.iso.org/members上找到。html和www.iec.ch/national-committees。

本标准由ISO/IEC JTC 1信息技术联合技术委员会SC 27信息安全、网络安全和隐私保护小组委员会编制。

引言

0.1 总则

本标准提供建立、实施、维护和持续改进信息安全管理体系的要求。采用信息安全管理系统是组织的一项战略决策。组织信息安全管理体系的建立和实施受组织的需要和目标、安全要求、组织的过程、规模和结构的影响。所有这些影响因素都可能随着时间发生变化。

信息安全管理体系通过应用风险管理过程来保持信息的保密性、完整性和可用性，并为相关方树立风险得到充分管理的信心。

重要的是，信息安全管理体系是组织过程和整体管理结构的一部分并集成在其中，并且在过程、信息系统和控制的设计中要考虑信息安全。期望的是，信息安全管理体系实现的程度与组织的需要相符合。

本标准可供内部和外部各方用于评估组织的能力是否满足自身的信息安全要求。

本标准中所提出要求的顺序不反映各要求的重要性或暗示这些要求予以实现的顺序。条款编号仅为方便引用。

ISO/IEC 27000描述了信息安全管理体系的概述和词汇，引用了信息安全安全管理体系标准族（包括ISO/IEC 27003[2]、ISO/IEC 27004[3]和ISO/IEC 27005[4]），以及相关术语和定义。

0.2 与其他管理体系标准的兼容性

本标准应用ISO/IEC合并导则附录SL中定义的高层结构、相同条款标题、相同文本、通用术语和核心定义，因此维护了与其他采用附录SL的其他管理体系的标准具有兼容性。

附录SL中定义的通用途径对于选择运行单一管理体系来满足两个或更多管理体系标准要求组织是有用的。

信息安全 网络安全和隐私保护 信息安全管理系统 -要求

1 范围

本国际标准规定了在组织的环境下建立、实施、维护和持续改进信息安全管理体系的要求。本国际标准还包括根据组织需求定制的信息安全风险评估和处理要求。本国际标准所列的要求是通用的，适用于各种类型、规模和特性的组织。组织声称符合本标准时，对于第4章到第10章规定的要求不能删减。

2 规范性引用文件

以下文件的全部或部分在本文件中进行引用。这些文件对于本标准的应用是必不可少的。凡是注明日期的引用文件，仅引用的版本适用。凡是不注明日期的引用文件，其最新版本的参考文件（包括所有的修改单）适用于本标准。

ISO/IEC 27000，信息技术-安全技术-信息安全管理体系-术语和定义

3 术语和定义

ISO/IEC 27000中的术语和定义适用本标准。

ISO和IEC在以下地址维护用于标准化的术语数据库：

— ISO在线浏览平台：位于 https://www.iso.org/obp

— IEC Electropedia：位于 https://www.electropedia.org/

4 组织环境

4.1 理解组织及其环境

组织应确定与其意图相关的、且影响其实现信息安全管理体系预期结果能力的外部和内部事项。

注：确定这些事项是指确定ISO 31000:2018 第5.4.1条款谈及用以建立组织的外部和内部环境的内容。

4.2 理解相关方的需求和期望

组织应确定：

a) 信息安全管理体系的相关方；

b) 这些相关方与信息安全相关的要求；

c) 哪些要求可以通过信息安全管理体系解决。

注：相关方的要求可包括法律、法规要求和合同义务。

4.3 确定信息安全管理体系范围

组织应确定信息安全管理体系的边界及其适用性，以建立其范围。

在确定范围时，组织应考虑：

a) 4.1中提到的外部和内部事项；

b) 4.2中提到的要求；

c) 组织实施的活动之间的及其与其他组织实施的活动之间的接口和依赖关系。

该范围应形成文件化信息并可用。

4.4 信息安全管理体系

组织应按照本保准的要求，建立、实施、维护和持续改进信息安全管理体系，包括所需的过程及其相互作用。

5 领导

5.1 领导和承诺

最高管理层应通过以下活动，证实对信息安全管理体系的领导和承诺：

a) 确保建立了信息安全策略和信息安全目标，并与组织战略方向一致；

b) 确保将信息安全管理体系要求整合到组织过程中；

c) 确保信息安全管理体系所需资源可用；

d) 沟通有效的信息安全管理及符合信息安全管理体系要求的重要性；

e) 确保信息安全管理体系达到预期的结果；

f) 指导和支持相关人员为信息安全管理体系的有效性做出贡献；

g) 促进持续改进；

h) 支持其他相关管理角色，以证实他们的领导按角色应用于其责任范围。

注：本文件中提及的“业务”可广义解释为组织存在的目的核心活动。

5.2 方针

最高管理层应建立信息安全方针，该方针应：

a) 与组织意图相适宜；

b) 包括信息安全目标（见6.2）或为设定信息安全目标提供框架；

c) 包括对满足适用的信息安全相关要求的承诺；

d) 包括对持续改进信息安全管理体系的承诺。

信息安全的方针应：

e) 形成文件化信息并可用；

f) 在组织内部得到沟通；

g) 适当时，对相关方可用。

5.3 组织角色、责任和权限

最高管理层应确保与信息安全相关角色的责任和权限得到分配和沟通。

最高管理者应分配以下责任和权限，以：

a) 确保信息安全管理体系符合本标准的要求；

b) 向最高管理层报告信息安全管理体系的绩效。

注：最高管理层也可以为组织内报告信息安全管理体系绩效，分配责任和权限。

6 规划

6.1 应对风险和机会的措施

6.1.1 总则

当规划信息安全管理体系时，应考虑4.1中提到的事项和4.2中提到的要求，并确定需要应对的风险和机遇，以：

a) 确保信息安全管理体系可达到预期结果；

b) 预防或减少不不良影响；

c) 达到持续改进。

组织应规划：

d) 应对这些风险和机遇的措施；

e) 如何

1) 将这些措施整合到信息安全管理体系过程中，并予以实现；

2) 评价这些措施的有效性。

6.1.2 信息安全风险评估

组织应定义并应用信息安全风险评估流程，以：

a) 建立并维护信息安全风险准则，包括：

1) 风险接受准则；

2) 信息安全风险评估实施准则；

b) 确保反复的信息安全风险评估产生一致的、有效的和可比较的结果；

c) 识别信息安全风险：

1) 应用信息安全风险评估过程，以识别与信息安全管理体系范围内与信息保密性、完整性和可用性损失有关的风险；

2) 识别风险责任人；

d) 分析信息安全风险：

1) 评估如果6.1.2 c）1）中的风险发生后，可能导致的潜在后果；

2) 评估6.1.2 c）1）中所识别的风险实际发生的可能性；

3) 确定风险级别；

e) 评估信息安全风险：

1) 将风险分析结果与6.1.2a）中规定的风险准则进行比较；

2) 为风险处置排序已分析风险的优先级。

组织应保留有关信息安全风险评估过程的文件化信息。

6.1.3 信息安全风险处置

组织应定义并应用信息安全风险处置过程，以：

a) 在考虑到风险评估结果的基础上，选择合适的信息安全风险处置选项；

b) 确定实现已选的信息安全风险处置选项所必需的所有控制；

注1：当需要时，组织可设计控制，或识别来自任何来源的控制。

c) 将上述6.1.3 b）确定的控制与附录A中的控制进行比较，并验证没有忽略必要的控制；

注2：附录A列出了可能的信息安全控制的列表。本标准的用户可在附录A的指导下，确保没有遗漏必要的控制。

注3：附录A所列的信息安全控制并非完备的，如有必要，可包括其他信息安全控制。

d) 制定一个适用性声明，包含：

— 必要的控制【见6.1.3 b）和c）】；

— 及其选择的合理性说明；

— 无论该控制是否已经实现；

— 以及附录A控制删减的合理性说明。

e) 制定正式的信息安全风险处置计划；

f) 获得风险责任人对信息安全风险处置计划以及对信息安全残余风险的接受的批准。

组织应保留有关信息安全风险处置过程的文件化信息。

注4：本标准中的信息安全风险评估和处置过程与ISO 31000中给出的原则和通用指南相匹配。

6.2 信息安全目标及其实现规划

组织应在相关职能和层级上建立信息安全目标。信息安全目标应：

a) 与信息安全方针一致；

b) 可测量（如可行）；

c) 考虑适用的信息安全要求，以及风险评估和风险处置的结果；

d) 受到监控；

e) 得到沟通；

f) 适当时更新；

g) 作为文件化信息可用。

组织应保留有关信息安全目标的文件化信息。在规划如何实现其信息安全目标时，组织应确定：

h) 要做什么；

i) 需要什么资源；

j) 由谁负责；

k) 什么时候完成；

l) 如何评价结果。

6.3 变更的策划

当组织确定需要对信息安全管理体系进行变更时，应以策划的方式进行变更。

7 支持

7.1 资源

组织应确定并提供建立、实施、维护和持续改进信息安全管理体系所需的资源。

7.2 能力

组织应：

a) 确定在其控制下从事会影响组织信息安全绩效的工作人员的必要能力；

b) 确保上述人员人员在适当的教育、培训或经验的基础上能够胜任其工作；

c) 适用时，采取措施以获得必要的能力，并评估所采取措施的有效性；

d) 保留适当的文件化信息作为能力的证据。

注：适用的措施可包括，例如针对现有员工提供培训、指导或重新分配；雇用或签约有能力的人员。

7.3 意识

在组织控制下工作的人员应了解：

a) 信息安全方针；

b) 其对信息安全管理体系有效性的贡献，包括改进信息安全绩效带来的益处；

c) 不符合信息安全管理体系要求带来的影响。

7.4 沟通

组织应确定与信息安全管理体系相关的内部和外部沟通需求，包括：

a) 沟通什么；

b) 何时沟通；

c) 与谁沟通；

d) 如何沟通。

7.5 文件化信息

7.5.1 总则

组织的信息安全管理体系应包括：

a) 本标准要求的文件化信息；

b) 为信息安全管理体系有效性，组织所确定的必要的文件化信息。

注：不同的组织有关信息安全管理体系文件化信息的详略程度可以是不同的，这是由于,：

1) 组织的规模及其活动、过程、产品和服务的类型；

2) 过程及其相互作用的复杂性；

3) 人员的能力。

7.5.2 创建和更新

创建和更新文件化信息时，组织应确保适当的：

a) 标识和描述（例如标题、日期、作者或引用号）；

b) 格式（例如语言、软件版本、图表）和介质（例如纸制的、电子的）；

c) 对适宜性和充分性的评审和批准。

7.5.3 文件化信息的控制

信息安全管理体系和本标准要求的文件化信息应得到控制，以确保：

a) 在需要的地点和时间，是可用的和适宜使用的；

b) 得到充分的保护（例如，避免保密性损失、不恰当使用、完整性损失等）。

为控制文件化信息，组织应强调以下活动：

c) 分发、访问、检索和使用；

d) 储存和保护，包括保持可读性；

e) 变更控制（例如版本控制）；

f) 保留和处理。

组织确定的为规划和运行信息安全管理体系所必需的外来文件化信息，应得到适当的识别并予以控制。

注：访问隐含着仅允许浏览文件化信息,或允许和授权浏览及更改文件化信息等决定。

8 运行

8.1 运行规划和控制

组织应通过以下方式规划、实现和控制满足要求所需的过程，并实现第6章中确定的活动：

— 建立过程准则；

— 根据准则实施过程控制

组织应保持文件化信息达到必要的程度，以确信这些过程按计划得到执行。

组织应控制计划的变更并评审非预期变更的后果，必要时采取措施减轻任何负面影响。

组织应确保外部提供的与信息安全管理体系相关的过程、产品或服务得到控制。

8.2 信息安全风险评估

组织应考虑6.1.2 a）中所建立的准则，按计划的时间间隔，或当重大变更提出或发生时，执行信息安全风险评估。

组织应保留信息安全风险评估结果的文件化信息。

8.3 信息安全风险处置

组织应实现信息安全风险处置计划。

组织应保留信息安全风险处置结果的文件化信息。

9 绩效评价

9.1 监视、测量、分析和评价

组织应确定：

a) 需要被监视和测量的内容，包括信息安全过程和控制；

b) 适用的监视、测量、分析和评价的方法，以确保得到有效的结果。所选的方法宜产生可比较的和可再现的有效结果；

c) 何时应执行监视和测量；

d) 谁应监视和测量；

e) 何时应分析和评价监视和测量的结果进行；

f) 谁应分析和评价这些结果。

组织应保留适当的文件化信息作为监视和测量结果的证据。

9.2 内部审核

9.2.1 总则

组织应按计划的时间间隔进行内部审核，以提供信息，确定信息安全管理体系：

a) 是否符合

1) 组织自身对其信息安全管理体系的要求；

2) 本标准的要求；

b) 是否得到有效实施和维护。

9.2.2 内部审核方案

组织应计划、建立、实施和维护审核方案（一个或多个），包括审核频次、方法、责任、规划要求和报告。

在制定内部审核方案时，组织应考虑相关过程的重要性和以往审核的结果。

组织应：

a) 定义每次审核的审核准则和范围；

b) 选择审核员并实施审核，以确保审核过程的客观性和公正性；

c) 确保将审核结果报告至相关管理层；

保留文件化信息作为审核方和审核结果的证据。

9.3 管理评审

9.3.1 总则

最高管理层应按计划的时间间隔评审组织的信息安全管理体系，以确保其持续的适宜性、充分性和有效性。

9.3.2 管理评审输入

管理评审应考虑：

a) 以往管理评审提出的措施的状态；

b) 与信息安全管理体系相关的外部和内部项事的变化；

c) 与信息安全管理体系相关的相关方需求和期望的变化；

d) 信息安全绩效的反馈，包括以下方面的趋势：

   1) 不符合和纠正措施；

   2) 监视和测量结果；

   3) 审核结果；

   4) 信息安全目标完成情况；

e) 相关方反馈；

f) 风险评估结果和风险处置计划的状态；

g) 持续改进的机会。

9.3.3 管理评审输出

管理评审的输出应包括与持续改进机会相关的决定以及变更信息安全管理体系的任任何需求。

组组应保留文件化信息应作为管理评审结果的证据。

10 改进

10.1 持续改进

组织应持续改进信息安全管理体系的适宜性、充分性和有效性。

10.2 不符合及纠正措施

当发生不合格时，组织应：

a) 对不符合做出反应，适当时：
   1) 采取措施，以控制并予以纠正；
   2) 处理后果；
b) 通过以下活动，评价采取消除不合格原因的措施的需求，以防止不合格再发生，或在其他地方发生：
   1) 评审不符合；
   2) 确定不合格的原因；
   3) 确定类似的不合格是否存在，或可能发生；
c) 实施任何需要的措施；
d) 评审任何所采取的纠正措施的有效性；
e) 必要时，对信息安全管理系统进行更改。纠正措施应与所遇到的不合格的影响相适应。组组应保留文件化信息作为以下方面的证据：

f) 不符合的性质及随后采取的任何后续措施，
g) 任何纠正措施的结果。

附件A
（规范性附录）

信息安全控制参考

表A.1中列出的信息安全控制直接来源于ISO/IEC 27002:2022第5章至第8章中列出的控制，并与之一致，并在6.1.3（信息安全风险处置）环境中被使用。

表A.1-信息安全控制

5	**组织控制**	
5.1	信息安全的策略集	**控制** 信息安全策略和特定主题的策略应由管理层定义、批准、发布、传达给相关人员和相关相关方，如果发生重大变化，应按计划的时间间隔进行审查。
5.2	信息安全角色和责任	**控制** 应根据组织需要定义和分配信息安全角色和职责。
5.3	职责的分离	**控制** 相互冲突的职责和相互冲突的责任范围应分离。
5.4	管理职责	**控制** 管理层应要求所有人员按照组织制定的信息安全策略、特定主题的策略和程序应用信息安全。
5.5	与职能机构的联系	**控制** 应维护相关职能机构的适当联系。
5.6	与特定相关方的联系	**控制** 应维护与特定相关方、其他专业安全论坛和专业协会的适当联系。
5.7	威胁情报	**控制** 应收集、分析与信息安全威胁有关的信息，以产生威胁情报。
5.8	项目管理中的信息安全	**控制** 信息安全应融入项目管理中。
5.9	信息和其他相关资产清单	**控制** 应编制和维护信息和其他相关资产清单，清单中应包含所有者。
5.10	信息和其他相关资产的可接受使用	**控制** 应确定、记录和实施信息和其他相关资产的可接受使用规则和处理程序
5.11	资产归还	**控制** 员工和其他相关方在任用、合同或协议终止时，应归还其占用的所有组织资产。

表A.1（续）

5.12	信息的分类	**控制** 信息应根据组织的信息安全需求，基于保密性、完整性、可用性和相关利益方要求进行分类。
5.13	信息标记	**控制** 应按照组织采用的信息分级方案，制定并实现一组适当的信息标记规程。
5.14	信息传输	**控制** 对于组织内部以及组织与其他方之间的所有类型的传输设施，应制定信息传输规则、程序或协议。
5.15	访问控制	**控制** 应根据业务和信息安全要求制定和实施控制信息和其他相关资产的物理和逻辑访问的规则。
5.16	身份管理	**控制** 应管理身份的整个生命周期。
5.17	身份验证信息	**控制** 身份验证信息的分配和管理应通过一个管理过程进行控制，包括建议人员对认证信息进行适当的处理。
5.18	访问权限	**控制** 信息和其他相关资产的访问权限应按照组织特定主题策略和访问控制规则进行设置、评审、修改和删除。
5.19	供应商关系中的信息安全	**控制** 应定义和实施流程和程序，以管理与使用供应商产品或服务相关的信息安全风险。
5.20	在供应商协议中强调信息安全	**控制** 应基于供应商关系的类型，与每个供应商建立相关信息安全要求并达成一致。
5.21	ICT 供应链的信息安全管理	**控制** 应定义和实施流程和程序，以管理与ICT产品和服务供应链相关的信息安全风险。
5.22	供应商服务的监控、审查和变更管理	**控制** 组织应定期监控、审查、评估和管理供应商信息安全惯例和服务交付的变化。
5.23	使用云服务的信息安全	**控制** 应按照组织的信息安全要求，建立从云服务获取、使用、管理和退出的流程。
5.24	信息安全事件管理规策划和准备	**控制** 组织应通过定义、建立和沟通信息安全事件管理流程、角色和责任，为信息安全事件的管理做好计划和准备。

表A.1（续）

5.25	信息安全事件的评估和决策	**控制** 组织应评估信息安全事件，并决定是否将其归类为信息安全事件。
5.26	应对信息安全事件响应	控制 信息安全事件应按照文件记录的程序进行响应。
5.27	从信息安全事件中学习	**控制** 从信息安全事件中获得的知识应用于加强和改进信息安全控制。
5.28	收集证据	**控制** 组织应建立并实施与信息安全事件相关证据的识别、收集、采集和维护程序。
5.29	中断期间的信息安全	**控制** 组织应规划如何在中断期间将信息安全维持在适当水平。
5.30	信通技术（ICT）为业务连续性做好准备	**控制** 应根据业务连续性目标和 ICT 连续性要求来规划、实施、维护和测试 ICT 准备情况
5.31	法律、法规、监管和合同要求	**控制** 应确定、记录和保持需求的更新与信息安全相关的法律、法规、监管和合同要求以及组织满足这些要求的方法。
5.32	知识产权	**控制** 组织应实施保护知识产权的适当程序。
5.33	记录的保护	**控制** 应保护记录免受损失、破坏、伪造、未经授权的访问和未经授权的泄露。
5.34	隐私和个人可识别信息保护	**控制** 组织应根据适用法律法规和合同要求，确定并满足有关隐私保护和PII保护的要求。
5.35	信息安全独立审查	**控制** 组织管理信息安全及其实施，包括人员、流程和技术，应按计划间隔或发生重大变化时进行独立审查。
5.36	信息安全策略、规程和 标准合规	**控制** 应定期检查对组织信息安全策略、特定主题策略、规则和标准的遵守情况。
5.37	文件化的操作规程	**控制** 信息处理设施的操作程序应记录在案，并提供给需要的人员。

表A.1（续）

6	**人员控制**	
6.1	审查	**控制** 在加入本组织之前，应考虑到适用的法律、法规和道德操守，对所有候选人员进行背景核查检查，并按业务要求、访问信息的分类和感知的风险进行。
6.2	任用条款和条件	**控制** 劳动合同协议应明确员工和组织在信息安全方面的责任。
6.3	信息安全意识、教育和培训	**控制** 组织和相关相关方人员应接受适当的信息安全意识、教育和培训，并定期更新与其工作职能相关的组织信息安全策略、特定主题的策略和程序。
6.4	违规处理过程	**控制** 应正式建立纪律程序并进行沟通，以对违反信息安全政策的人员和其他相关方采取行动
6.5	任用终止或变更的责任	**控制** 终止或变更雇佣关系后仍有效的信息安全责任和义务应明确、执行并传达给相关人员和其他相关方。
6.6	保密或不泄露协议	**控制** 应确定、记录、定期审查由人员和其他相关方签署、反映组织保护信息需求的保密协议或不披露协议。
6.7	远程工作	**控制** 当员工进行远程工作时，应实施安全措施，以保护在组织场所外访问、 处理或储存的信息。
6.8	报告信息安全事态	**控制** 组织应为人员提供一种机制，让员工通过适当的渠道及时报告已发现或怀疑的信息安全事件。
7	**物理控制**	
7.1	物理安全边界	**控制** 应定义并使用安全边界来保护包含信息和其他相关资产。
7.2	物理入口	**控制** 安全区域应通过适当的入口控制和接入点进行保护。
7.3	办公室、房间和设施的安全	**控制** 应为办公室、房间和设施设计并采取物理安全措施.。
7.4	物理安全监控	**控制** 应持续监控场所是否有未经授权的物理访问。

表A.1（续）

7.5	外部和环境威胁的安全防 护	**控制** 应设计和实施针对自然灾害和其他有意或无意的基础设施物理威胁等物理和环境威胁的保护措施。
7.6	在安全区域工作	**控制** 应设计实施在安全区域工作的安全措施。
7.7	清理桌面和屏幕	**控制** 应针对纸质和可移动存储介质，采取清理桌面规则，以及信息处理设施的屏幕清理规则。
7.8	设备选址和保护	**控制** 设备应安全放置并受到保护。
7.9	组织场所外的资产安全	**控制** 应保护组织场所外的资产。
7.10	存储介质	**控制** 存储介质应按照组织的分类方案和处理要求，在其获取、使用、运输和处置的整个生命周期内进行管理。
7.11	支持性设施	**控制** 应对信息处理设施进行保护，使其不受电源故障和支持性设施故障造成的其他中断的影响。
7.12	布缆安全	**控制** 应保护承载电力、数据或支持性信息服务的电缆，使其免受拦截、干扰或损坏。
7.13	设备维护	**控制** 应正确维护设备，以确保信息的可用性、完整性和保密性。
7.14	设备的安全处置或再利用	**控制** 应验证包含存储介质的设备项目，以确保任何敏感数据和许可软件在处置或重新使用前已被删除或安全覆盖。
8	**技术控制**	
8.1	用户终端设备	**控制** 应保护用户终端设备上存储、处理或可访问的信息。
8.2	特许访问权管理	**控制** 应限制和管理特权访问权的分配和使用。
8.3	信息访问限制	**控制** 应根据既定的特定主题访问控制策略限制对信息和其他相关资产的访问。
8.4	源代码的访问	**控制** 应适当管理对源代码、开发工具和软件库的读写访问。

表A.1（续）

8.5	安全的身份验证	**控制** 应根据信息访问限制和特定主题的访问控制策略实施安全认证技术和程序。
8.6	容量管理	**控制** 应根据当前和预期的能力要求对资源的使用进行监测和调整。
8.7	恶意软件防范	**控制** 应实施恶意软件的防范并通过适当的用户意识予以支持。
8.8	技术脆弱性管理	**控制** 应获得使用中的信息系统的技术脆弱性信息，应评估组织暴露于此类漏洞的风险，并采取适当措施。
8.9	配置管理	**控制** 应建立、记录、实施、监控和审查硬件、软件、服务和网络的配置，包括安全配置。
8.10	信息删除	**控制** 当不再需要时，应删除存储在信息系统、设备或任何其他存储介质中的信息。
8.11	数据屏蔽	**控制** 数据屏蔽应根据组织的特定主题访问控制策略和其他相关特定主题策略以及业务要求使用，并考虑适用的法律要求。
8.12	数据防泄漏	**控制** 数据泄漏防护措施应适用于处理、存储或传输敏感信息的系统、网络和任何其他设备。
8.13	信息备份	**控制** 信息、软件和系统的备份副本应按照商定的特定主题备份策略进行维护和定期测试。
8.14	信息处理设施的冗余	**控制** 信息处理设施的冗余度应足以满足可用性要求。
8.15	日志记录	**控制** 应生成、存储、保护和分析记录活动、异常、故障和其他相关事件的日志。
8.16	监测活动	**控制** 应监控网络、系统和应用程序的异常行为，并采取适当措施评估潜在的信息安全事件。
8.17	时钟同步	**控制** 组织使用的信息处理系统的时钟应与批准的时间源同步。

表A.1（续）

8.18	特权实用程序的使用	**控制** 对于可能超越系统和应用控制的实用程序的使用应予以限制并严格控制。
8.19	在操作系统上安装软件	**控制** 应实施操作系统软件安装的安全管理程序和措施。
8.20	网络安全	**控制** 应保护、管理和控制网络和网络设备，以保护系统和应用程序中的信息。
8.21	网络服务的安全	**控制** 应识别、实施和监控网络服务的安全机制、服务级别和服务要求。
8.22	网络隔离	**控制** 信息服务组、用户组和信息系统组应在组织网络中分离。
8.23	网站过滤	**控制** 应管理对外部网站的访问，以减少面临恶意内容的可能。
8.24	加密技术的使用	**控制** 应定义和实施有效的加密技术使用规则，包括密钥管理。
8.25	安全开发生命周期	**控制** 应制定并应用软件和系统的安全开发规则。
8.26	应用程序安全要求	**控制** 在开发或获取应用程序时，应确定、规定和批准信息安全要求。
8.27	安全系统架构和工程原则	**控制** 应建立、记录、维护工程安全系统的原则，并将其应用于任何信息系统开发活动。
8.28	安全编码	**控制** 软件开发应采用安全编码原则。
8.29	开发和验收中的安全测试	**控制** 应在开发生命周期中定义和实施安全测试过程。
8.30	外包开发	**控制** 组织应指导、监督和审查与外包系统开发相关的活动。
8.31	开发、测试和生产环境的分离	**控制** 开发、测试和生产环境应分离并加以保护。
8.32	变更管理	**控制** 信息处理设施和信息系统的变更应遵循变更管理程序。

8.33	测试信息	**控制** 测试信息应适当地选择、保护和管理。

表A.1（续）

8.34	在审计测试期间信息系统的保护	**控制** 涉及运行系统的审计测试和其他评估保证活动应在测试人员和适当的管理层之间得到规划和取得批准。

参考文献

[1] ISO/IEC 27002:2022，信息安全、网络安全和隐私保护 信息安全控制

[2] ISO/IEC 27003，信息技术-安全技术-信息安全管理体系-指南

[3] ISO/IEC 27004，信息技术-安全技术-信息安全管理
-监视、测量、分析和评价

[4] ISO/IEC 27005，信息安全、网络安全和隐私保护 信息安全风险管理指南

[5] ISO 31000:2018，风险管理 指南

ICS 03.100.70；35.030

价格基于19页