



信息安全管理体系认证规则

1 适用范围及认证依据

1.1 本规则用于规范本公司开展信息安全管理体系（简称 ISMS）的认证活动。

1.2 本规则依据认证认可相关法律法规，结合相关技术标准要求，对 ISMS 认证实施的全过程作出详细规定，是本公司开展 ISMS 认证活动的基础依据。

1.3 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》。

2 对认证机构的基本要求

2.1 获得国家认证认可监督管理委员会的批准，并取得从事信息安全管理体系认证的资质。

2.2 建立内部制约、监督和责任机制，确保从组织结构到认证活动的公正性。

2.3 鼓励认证机构寻求认可，证明其能力、内部管理和管理体系符合相关的技术要求

3 对认证审核人员的基本要求

3.1 认证审核员应具备相应的专业知识及教育、培训或工作经历，并取得 CCAA 认证人员 ISMS 领域的执业确认资格。

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

4 认证过程和要求

4.1 受理认证申请

4.1.1 应向申请组织至少公开以下信息：

- （1）可开展认证服务的范围，以及获得认可的情况；
- （2）对认证过程的申诉规定；
- （3）认证服务过程；
- （4）授予、拒绝、保持、更新、暂停、恢复或撤销认证或者扩大或缩小认证范围的过程；
- （5）本公司的机构名称和认证标志或徽标的使用；
- （6）公正性政策。

4.1.2 应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活动及活动的边界范围、信息资产和 SMS



范围复杂性的情况，组织结构、规模、ISMS 活动的基本信息等。

(2) 法律地位的证明性文件。若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（必要时）。

(3) 申请组织的管理体系范围所涉及的法律法规要求的资质复印件（适用 时，可包括行政许可证明、资质证书等）。

(4) 与申请认证有关的管理体系形成文件的信息（必要时）。

(5) 必要时，申请认证组织 ISMS 记录的保密性或敏感性声明

(6) 申请认证组织信息安全管理体系关于标准 ISO/IEC27001 的适用性申明（SoA）的现行版本，此适用性声明客户应就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作出说明。

4.1.3 应对申请组织提交的申请资料进行评审，以确定是否有能力受理认证申请。

被执法监管部门责令停业整顿、全国企业信用信息公示系统中被列入“严 重违法企业名单”的组织以及被市场监管部门认定为存在严重违法失信行为的组织，不应受理其认证申请。

4.1.4 对符合 4.1.2、4.1.3 要求的，可决定受理认证申请；对不符合上述要求的，应通知申请组织补充和完善，或者不受理认证申请。

4.1.5 签订认证合同

在实施认证审核前，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证书之后，发生以下情况时应及时通报认证机构：

a) 客户及相关方有重大投诉；

b) 被政府部门监管认定为不符合（不合格）、发生事故或被媒体曝光；

c) 相关情况发生变更，包括：法律地位、生产经营状况或所有权变更；取得的行政许可资格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；管理体系覆盖的范围变更等。

(4) 申请组织承诺获得认证证书之后，应该正确使用认证证书、认证标识 和标志，避免误导公众认为其产品或服务通过认证。



(5) 拟认证的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。

4.2 审核策划

4.2.1 审核时间

本公司有文件化的用于计算管理体系审核时间, 包括管理体系认证审核时间(即现场审核时间)的方法。应为每次管理体系审核计算审核时间, 并留有记录。ISMS 现场审核人日数的计算应按照 CNAS CC170《信息安全管理体系认证机构要求》附录所列的基础人日数进行核算。

4.2.2 审核组

4.2.2.1 本公司应根据组织申请认证的管理体系的范围, 选择具备相关能力的审核员组成审核组。审核组所具备的专业技术能力应能够覆盖组织的管理体系的范围。当审核组的专业技术能力不足时, 可以配备该专业的技术专家加入审核组。

4.2.2.2 技术专家主要负责提供审核组的技术支持, 不作为审核员独立实施审核, 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。

4.2.2.3 审核组可以有实习审核员。实习审核员应在审核员的指导完成审核, 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同组的审核员承担责任。

4.2.3 审核计划

4.2.3.1 本公司为每次审核制定审核计划(第一阶段非现场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、时间安排和场所, 审核组成员。

审核组配备的专业审核员、技术专家, 应标明其在审核组的专业技术代码。

4.2.3.2 本公司有文件化的用于计算管理体系的多场所审核时间, 包括管理体系认证审核时间(即现场审核时间)的方法。认证机构应为每次管理体系审核计算审核时间, 并留有记录。

4.2.3.3 为使现场审核活动能够观察到产品生产或服务的实际运行, 现场审核应安排在认证范围所覆盖产品的生产或服务的提供处于正常运行时进行。

4.2.3.4 在现场审核开始之前, 审核组应将审核计划提交给受审核方。如需要临时调整计划时, 审核组应及时将变更情况通知申请组织, 并与之协商一致。



4.3 实施审核

4.3.1 审核组应按照审核计划的安排完成审核工作。除特殊情况外, 审核过程中不得更换审核计划确定的审核员。

4.3.2 审核组应会同申请组织按照审核程序召开首、末次会议, 申请组织的管理层及与管理体系相关的职能部门负责人员应该参加会议。参会人员应签到, 审核组应保留首、末次会议签到表。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。

4.3.3 对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。

4.3.4 发生下列情况时, 审核组应向认证公司报告, 经同意后终止审核。

- (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。

4.4 初次认证审核

ISMS 的初次认证审核应分为两个阶段实施: 一阶段审核和二阶段审核。

4.4.1 一阶段审核

4.4.1.1 一阶段审核应收集信息、了解组织的情况, 确定申请组织是否具备条件接受二阶段审核。

一阶段审核至少覆盖以下内容:

- (1) 评审组织的文件化信息, 确认其与组织实际情况的一致性。
- (2) 确认组织是否实施了内部审核与管理评审、管理体系是否运行并且超过 3 个月。
- (3) 确认申请组织管理体系覆盖的范围及体系覆盖范围内的有效人数、过程和场所, 以及遵守适用的法律法规及强制性标准的情况。
- (4) 确定是否具备二阶段审核条件及二阶段审核重点。

对管理体系文件不符合现场实际、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。

4.4.1.2 一阶段审核应在受审核方的生产经营或服务现场进行, 除非满足下列条件之一, 并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, 可不进行一阶段现场审核:

- (1) 申请组织已获本认证机构颁发的其他有效认证证书。
- (2) 有充足的理由证明申请组织的生产经营或服务的技术特征明显、过程简单、风险较



低, 已获取到受审核方合规性证明文件。

(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同领域有效的 管理体系认证证书。

应记录未在受审核方现场开展一阶段审核的原因。

4.4.1.3 本公司应将受审核方是否具备二阶段审核条件的书面结论告知客户, 包括所识别的引起关注的、在第二阶段可能被判定为不符合的问题。

4.4.2 二阶段审核

二阶段审核应在受审核方的现场进行, 评价受审核方管理体系的实施情况, 包括有效性。第二阶段审核应至少覆盖以下内容:

- (1) 最高管理者的领导力和对信息安全方针与信息安全目标的承诺;
- (2) ISO/IEC 27001 中所列的文件要求;
- (3) 评估与信息安全有关的风险, 以及评估可产生一致的、有效的、在重复评估时可比较的结果;
- (4) 基于风险评估和风险处置过程, 确定控制目标和控制;
- (5) 信息安全绩效和 ISMS 有效性, 以及根据信息安全目标对其进行评审;
- (6) 所确定的控制、适用性声明、风险评估与风险处置过程的结果、信息安全方针与目标, 它们相互之间的一致性;
- (7) 控制的实施 (详见 CNAS-CC170 附录 D), 考虑了外部环境、内部环境与相关的风险, 以及组织对信息安全过程和控制的监视、测量与分析, 以确定控制是否得以实施、有效并达到其所规定的目标;
- (8) 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信息安全方针与目标。

4.5 监督审核

4.5.1 本公司应对持有其颁发的管理体系认证证书的组织 (以下称获证组织) 进行有效跟踪, 监督获证组织持续运行管理体系并符合认证要求。

4.5.2 监督审核应确认获证组织的管理体系的持续符合性和有效性, 监督审核应至少覆盖以下内容:

- (1) 信息安全风险评估与控制的维护、ISMS 内部审核、管理评审和纠正措施等管理体系要素的保持;
- (2) 根据 ISMS 标准 ISO/IEC 27001 和认证所需的其他文件的要求, 与来自外部各方沟



通;

- (3) 文件化管理体系的变更;
- (4) 发生变更的区域;
- (5) 所选择的 ISO/IEC 27001 的要求;
- (6) ISMS 在实现针对客户信息安全方针所确定的目标方面的有效性;
- (7) 对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;
- (8) 所确定的控制的变更, 及其引起的 SoA 的变更;
- (9) 控制的实施和有效性 (根据审核方案来审查)。
- (10) 适宜时, 其他被选择的区域。

4.5.3 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。

4.5.4 监督审核应在获证组织现场进行。但由于市场、季节性等原因, 在每次监督审核时难以覆盖所有产品和服务的, 在认证证书有效期内的监督审核需覆盖认证范围内的所有产品和服务。

4.6 再认证审核

4.6.1 获证组织在认证证书期满前申请继续持有认证证书的, 认证机构应实施再认证审核, 并决定是否延续认证证书。

4.6.2 对获证组织管理体系无重大变更的, 再认证审核可省略一阶段审核。

对获证组织管理体系的运作环境有变更的, 应要求获证组织重新提交申请资料。应对获证组织的变更进行评审, 有重大变更时, 可考虑实施一阶段审核。

4.6.3 获证组织继续满足认证要求的, 认证公司应作出延续的再认证决定, 并换发认证证书。

4.6.4 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认证证书的, 新认证证书的终止日期可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。

4.6.5 在当前认证证书终止日期前, 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的, 本公司不应予以再认证, 也不应延长原认证证书的有效期。

在证书到期后 6 个月内完成未尽的再认证活动的, 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。恢复认证的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。

4.7 不符合纠正的验证

4.7.1 对审核中发现的不符合（包括严重和轻微），应要求受审核方在规定的时限内进行原因分析、采取相应的纠正和纠正措施（轻微不符合可以是纠正措施计划）。对严重不符合所实施的纠正和纠正措施的验证，其时限应不超过审核结束后的 6 个月，并应在认证证书到期前完成。

4.7.2 对于组织未能在规定时限完成对不符合项所采取措施的情况，则不应给予该组织推荐认证、保持认证、或推荐再认证。

4.8 审核报告

4.8.1 审核组应对审核活动形成审核报告，并在商定的时间期限内提交。如果延迟，应向受审核方和审核方案管理人员通告原因。审核报告应注明日期，并经适当的评审和批准。经批准的审核报告应分发至审核程序和审核计划规定的接受人，至少包括受审核方。

审核报告应描述审核活动的主要内容，至少应包括：

- （1）受审核方的名称、注册地址和审核地址。
- （2）受审核方的审核范围及审核范围内的产品/服务/过程/活动和场所（包括固定场所和临时场所）。
- （3）审核委托方、审核的类型、准则和目的。
- （4）审核组组长、审核组成员及任何与审核组同行的人员。
- （5）对偏离审核计划情况及理由的说明。
- （6）对管理体系是否符合认证标准要求 and 有效运行情况进行正反两方面评价；重点评价以下方面：
 - a) 对目标及实现目标的措施实现情况。
 - b) 对合规性义务的识别、评价和遵守情况。
 - c) 对管理体系覆盖的过程和活动的管理及控制情况（重点评价关键过程 和活动）。
 - d) 受审核方的内部审核和管理评审是否有效。
- （7）开具的不符合项和识别出的需改进方面。
- （8）审核组对是否通过认证的推荐性意见。
- （9）监督审核和再认证审核报告还应描述受审核方对以前不符合采取的纠正措施有效性的验证情况、对认证文件和标志的使用情况、上次审核后发生的影响管理体系的重要变更控制情况等。



4.8.2 对终止审核的项目, 审核组应将已开展的工作情况形成报告, 认证公司应将终止审核的原因以适宜的方式告知受审核方。

4.9 认证决定

4.9.1 本公司应该在对审核报告、不符合项的纠正和/或纠正措施及其结果进行综合评价基础上, 作出认证决定。

4.9.2 认证决定人员应为本公司管理控制下的人员, 审核组成员不得参与对审核项目的认证决定。

4.9.3 在作出认证决定前应确认如下情形:

(1) 审核报告符合本规则第 4.7 条要求, 审核组提供的审核报告及其他信息能够满足作出认证决定所需要的信息。

(2) 对于严重不符合项, 已评审、接受并验证了纠正和/或纠正措施的有效性。

(3) 对其他一般不符合项已评审, 并接受了受审核方计划采取的纠正和/或纠正措施。

4.9.4 在满足 4.8.3 条要求的基础上, 本公司有充分的客观证据证明受审核方满足下列要求, 评定该受审核方符合认证要求, 向其颁发认证证书。

(1) 受审核方的管理体系符合标准要求且运行有效。

(2) 认证范围覆盖的活动、产品和服务符合相关法律法规要求, 不存在重大事故和其他严重违法行为。

4.9.5 若受审核方不能满足上述要求, 则评定该受审核方不符合认证要求。认证公司应以适宜的方式告知受审核方并说明其未通过认证的原因。

5 认证证书要求

5.1 认证证书基本内容要求

(1) 获证组织名称、地址应与其法律地位证明文件信息一致。

(2) 获证组织的管理体系所覆盖的业务范围; 若认证的管理体系覆盖多场所, 应表述覆盖的相关场所的名称和地址信息。

(3) 认证依据的标准、技术要求。

(4) 证书编号。

(5) 发证机构、发证日期和有效期。

(6) 证书查询方式。

(7) 认证证书中应包括适用性声明 (SOA) 的版本。

(8) ISMS 认证证书中引用特定行业标准的要求如下:



一是所引用的行业标准应为国家标准和国际标准，而不能是其他类别的标准

二是确保该引用要清晰地表述这些标准仅是组织适用性声明（SOA）中控制的来源，而不是依据这些标准实施认证。

5.2 认证证书管理要求

5.2.1 公司应当建立证书信息披露制度。除向申请组织、认证监管部门等执法监管部门提供认证证书信息外，还应当根据社会相关方的请求向其提供证书信息，接受社会监督。

5.2.2 公司应当建立认证证书管理制度，对不能符合认证要求的获得认证的组织和个人，应当暂停其使用直至撤销认证证书，并予以公布。

5.3 证书的暂停或撤销

公司应制定暂停、撤销认证证书或缩小认证范围的规定和管理制度。对认证证书的暂停和撤销处理应符合管理制度，不得随意暂停或撤销认证证书。

5.3.1 暂停证书

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

（1）管理体系持续或严重不满足认证要求。

（2）不承担、履行认证合同约定的责任和义务的。

（3）被有关执法监管部门责令停业整顿的。

（4）持有的与管理体系范围有关的行政许可证明、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的。

（5）获证组织不能按照规定的时间间隔接受监督。

（6）主动请求暂停的。

（7）其他应当暂停认证证书的。

5.3.1.2 认证证书暂停期原则上不得超过 6 个月。但被行政许可责令停业整顿；资质有效期到期，正在办理过程中的，暂停期可延至相关单位作出许可决定之日。

5.3.1.3 应以适当方式公开暂停认证证书的信息，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。

5.3.2 撤销证书

5.3.2.1 获证组织有以下情形之一的，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）被注销或撤销法律地位证明文件的。

（2）被国家市场监管部门认定存在严重违法失信行为的组织。



(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) 拒绝接受国家产品质量监督抽查的。

(5) 出现重大事故，经执法监管部门确认是获证组织责任造成的。

(6) 有其他严重违法违反法律法规行为的。

(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未予以纠正的（包括持有的与管理体系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) 没有运行管理体系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，或者认证公司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。

5.3.2.2 撤销认证证书后，应及时在相关媒体和网站上公布或声明撤销决定。

5.3.2.3 暂停或撤销认证证书应当在认证公司网站上公布相关信息，同时按规定程序和要求报国家认证认可监督管理委员会。

6 认证记录的管理

6.1 公司应当建立认证记录保持制度，对认证全过程做出完整记录，并保留相应认证资料。

6.2 记录应当真实、准确，以证实认证活动得到有效实施。归档留存时间应当与认证证书有效期一致。

6.3 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。

7 组织申、投诉处理

7.1 申请组织或获证组织对认证决定有异议时，认证公司应接受申诉并且及时进行处理，在 60 日内将处理结果形成书面通知送达申诉人。

7.2 若申诉人认为认证公司未遵守认证相关法律法规或本规则并导致自身合法权益受到严重侵害的，可以直接向所在地认证监管部门或国家认监委申诉。

7.3 任何组织或个人对认证公司、工作人员或者获证组织的投诉，认证公司应确认投诉是否与其负责的认证活动有关，并在经确认有关时予以受理。对于针对获证组织的有效投诉，认证公司还应在适当的时间将投诉告知该客户。

7.4 公司应当在受理当事人投诉之日起 60 日内办结，并将处理结果告知投诉人。



北京中水源禹认证有限公司

2023 年 11 月 06 日修订发布实施

国际标准

ISO/IEC
27001

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



目 录

前言	III
引言	IV
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 组织环境	2
4.1 理解组织及其环境	2
4.2 理解相关方的需求和期望	2
4.3 确定信息安全管理体范围	2
4.4 信息安全管理体	2
5 领导	2
5.1 领导和承诺	2
5.2 方针	3
5.3 组织的角色，责任和权限	3
6 规划	3
6.1 应对风险和机遇的措施	3
6.2 信息安全目标及其实现规划	5
6.3 变更的策划	5
7 支持	5
7.1 资源	5
7.2 能力	5
7.3 意识	6
7.4 沟通	6
7.5 文件化信息	6
8 运行	7
8.1 运行规划和控制	7
8.2 信息安全风险评估	7
8.3 信息安全风险处置	7
9 绩效评价	7
9.1 监视、测量、分析和评价	7
9.2 内部审核	8
9.3 管理评审	8
10 改进	9
10.1 持续改进	9
10.2 不符合及纠正措施	9
附录A	10
参考文献	17

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标准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。本标准根据 ISO/IEC 指令第 2 部分的编辑规则起草（见 www.iso.org/Directives 或 https://www.iec.ch/members_experts/refdocs）。

请注意，本标准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。标准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 <https://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写。

第三版取消并取代了第二版（ISO/IEC 27001:2013），该版本已进行了技术修订。它还包含了技术勘误表 ISO/IEC 27001:2013/Cor 1:2014 和 ISO/IEC 27001:2013/Cor 2:2015。

主要变化如下：

文本已与管理体系标准和 ISO/IEC 27002:2022 的协调结构保持一致。

关于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.html 和 www.iec.ch/national-committees。

引言

0.1 总则

本标准提供建立、实现、维护和持续改进信息安全管理体系的要求。采用信息安全管理体系是组织的一项战略性决策。组织信息安全管理体系的建立和实施受组织的需求和目标、安全要求、组织所采用的过程、规模和结构的影响。所有这些影响因素可能随时间发生变化。

信息安全管理体系通过应用风险管理过程来保持信息的机密性、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的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到信息安全。期望的是，信息安全管理体系的实现程度要与组织的需求相符合。

本标准可被内部和外部各方用来评估组织的能力是否满足自身的信息安全要求。

本标准中所表述要求的顺序不反映各要求的重要性或暗示这些要求要予实现的顺序。列表项的枚举仅供参考使用。

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

0.2 与其他管理体系的兼容性

本标准应用ISO/IEC指令第1部分附录SL中定义的高层结构、相同的条款标题、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的管理体系的标准具有兼容性。

附件SL中定义的通用方法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的组织是有用的。

信息安全、网络安全和隐私保护

信息安全管理体系 要求

1 范围

本标准规定了在组织环境下建立、实现、维护和持续改进信息安全管理体系的要求。本标准还包括针对组织需求量身定制的信息安全风险评估和处理的要求。

本标准中规定的要求是通用的，旨在适用于所有组织，无论其类型、规模或性质如何。当组织声称符合本标准时，不能排除第4章到第10章中所规定的任何要求。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修订单）适用于本文件。

ISO/IEC 27000，信息技术-安全技术-信息安全管理体系 概述和词汇

3 术语和定义

ISO/IEC 27000中界定的术语和定义适用于本文件。

ISO和IEC为标准化使用维护术语数据库，具体网址如下：

- ISO在线浏览平台：<https://www.iso.org/obp>
- IEC电子百科：<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，影响其实现信息安全管理体预期结果能力的外部 and 内部事项。

注：对这些事项的确定，参见ISO31000:2018^[5]第5.4.1条中建立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) 信息安全管理体相关方；
- b) 这些相关方与信息安全相关的要求；
- c) 其中哪些要求将通过信息安全管理体来解决。

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范围

组织应确定信息安全管理体的边界及其适宜性，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

组织应按照本标准的要求，建立、实现、维护和持续改进信息安全管理体，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要求整合到组织过程中；
- c) 确保信息安全管理体所需资源可用；
- d) 沟通有效的信息安全管理及符合信息安全管理体要求的重要性；
- e) 确保信息安全管理体达到预期结果；
- f) 指导并支持相关人员为信息安全管理体的有效性做出贡献；
- 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：本标准中提及的“业务”可被广义地解释为指对组织存在的目的具有至关重要的活动。

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。

信息安全方针应：

- e) 形成文件化信息并可用；
- f) 在组织内得到沟通；
- g) 适当时，对相关方可用。

5.3 组织的角色，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。

最高管理人员应分配责任和权限，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绩效。

注：最高管理层也可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 应对风险和机遇的措施

6.1.1 总则

当规划信息安全管理体系时，组织应考虑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过程，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，以识别信息安全管理范围内与信息保密性、完整性和可用性损失相关的风险；
 - 2) 识别风险责任人。
- d) 分析信息安全风险：
 - 1) 评估6.1.2 c) 1)中所识别的风险发生后，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) 评价信息安全风险：
 - 1) 将风险分析结果与6.1.2a)中建立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) 在考虑风险评估结果的基础上，选择适合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6.1.3b)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包含了控制目标和控制的综合列表。本标准用户可在附录A的指导下，确保没有遗漏必要的控制。

注3：附录A所列的控制目标和控制并不是完备的，可能需要额外的控制目标和控制。

- d) 制定一个适用性声明，其中包含：

- 必要的控制 [见6.1.3 b)和c)]
- 纳入它们的理由；
- 是否实施了这些必要的控制；
- 排除任何附录A的控制的理由。

- 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^[5]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) 被监测；
- e) 得到沟通；
- f) 适当时更新；
- g) 可作为文件化信息并保持可用；

组织应保留有关信息安全目标的文件化信息。

在规划如何达到信息安全目标时，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，变更应按所策划的方式实施。

7 支持

7.1 资源

组织应确定并提供建立、实现、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) 确定在组织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，例如针对现有雇员提供培训、指导或重新分配；雇佣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的沟通需求，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​​系的有效性，组织所确定的必要的文件化信息；

注：不同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) 识别和描述（例如标题、日期、作者或引用编号）；
- b) 格式（例如语言、软件版本、图表）和介质（例如纸质的、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​​系及本标准所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(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，适用时，组织应强调以下活动：

- c) 分发，访问，检索和使用；
- d) 存储和保护，包括保持可读性；
- e) 控制变更（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所必需的外来的文件化信息，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计划、实施和控制满足要求所需的过程，并实施第6章中确定的措施：

- 为这些过程建立准则；
- 根据准则实施对过程的控制。

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。

组织应控制计划内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) 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；

注：所选的方法宜产生可比较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；
- 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。

组织应评价信息安全绩效以及信息安全管理体系的有效性。

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) 是否得到有效实现和维护。

9.2.2 内部审核方案

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

审核方案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，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；
- d) 保留文件化信息作为审核方案和审核结果的证据。

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 and 内部事项的变化；
- c) 与信息安全管理体系有关的相关方需求和期望的变化；

d) 有关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) 风险评估结果及风险处置计划的状态；

g) 持续改进的机会。

9.3.2 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的任何需求。

组织应保留文件化信息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

当发生不符合时，组织应：

a) 对不符合做出反应，适用时：

- 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，评价采取消除不符合原因的措施的需求，以防止不符合再发生，或在其他地方发生：

- 1) 评审不符合；
- 2) 确定不符合的原因；
- 3) 确定类似的不符合是否存在，或可能发生；

c) 实现任何需要的措施；

d) 评审任何所采取的纠正措施的有效性；

e) 必要时，对信息安全管理体进行变更。

纠正措施应与所遇到的不符合的影响相适合。

组织应保留文件化信息作为以下方面的证据：

f) 不符合的性质及所采取的任何后续措施；

g) 任何纠正措施的结果。

附录A

(规范性附录)

参考信息安全控制

表 A.1 所列的信息安全控制是直接源自并于 ISO/IEC 27002:2022^[1]第 5 章至第 8 章相对应，并在6.1.3 环境中被适用。

表A.1 信息安全控制

5	组织控制	
5.1	信息安全策略	<i>控制</i> 宜定义信息安全方针和特定主题策略，由管理层批准后发布，传达并让相关工作人员和相关方知悉，按计划的时间间隔以及在发生重大变更时对其进行评审。
5.2	信息安全角色和责任	<i>控制</i> 信息安全角色和责任宜根据组织需求进行定义和分配。
5.3	职责分离	<i>控制</i> 宜分离相互冲突的职责和责任范围。
5.4	管理责任	<i>控制</i> 管理层宜要求所有工作人员根据组织已建立的信息安全方针、特定主题策略和规程，履行信息安全责任。
5.5	与职能机构的联系	<i>控制</i> 组织宜建立并维护与相关职能机构的联系。
5.6	与特定相关方的联系	<i>控制</i> 组织宜建立并维护与特定相关方或其他专业安全论坛和专业协会的联系。
5.7	威胁情报	<i>控制</i> 宜收集并分析信息安全威胁相关的信息，以生成威胁情报。
5.8	项目管理中的信息安全	<i>控制</i> 宜将信息安全整合到项目管理中。
5.9	信息及其他相关资产的清单	<i>控制</i> 宜编制和维护信息及其他相关资产(包括资产拥有者)的清单。
5.10	信息及其他相关资产的可接受使用	<i>控制</i> 宜识别、文件化并实现信息及其他相关资产的可接受使用规则和处理规程。
5.11	资产归还	<i>控制</i> 适宜时，工作人员和其他相关方在任用、合同或协议变更及终止时，宜归还其拥有的所有组织资产

表 A.1（续）

5.12	信息分级	<i>控制</i> 宜根据组织基于保密性、完整性、可用性的信息安全需求以及相关方的要求，对信息进行分级。
5.13	信息标记	<i>控制</i> 宜按照组织采用的信息分级方案，制定并实施适当的信息标记规程
5.14	信息传输	<i>控制</i> 宜为组织内部以及组织与其他各方之间所有类型的传输设施，制定信息传输规则、规程或协议。
5.15	访问控制	<i>控制</i> 宜基于业务和信息安全要求，建立和实施信息及其他相关资产的物理和逻辑访问控制规则。
5.16	身份管理	<i>控制</i> 宜管理身份的全生存周期
5.17	鉴别信息	<i>控制</i> 宜通过管理过程控制鉴别信息的分配和管理，包括向工作人员提供鉴别信息的适当处理建议。
5.18	访问权	<i>控制</i> 宜根据组织访问控制的特定主题策略和规则来提供、评审、修改和删除信息及其他相关资产的访问权。
5.19	供应商关系中的信息安全	<i>控制</i> 宜定义并实施过程和规程，以管理与供应商产品或服务使用相关的信息安全风险。
5.20	在供应商协议中强调信息安全	<i>控制</i> 宜根据供应商关系的类型建立相关的信息安全要求，并与每个供应商达成一致。
5.21	管理信息通信技术供应链中的信息安全	<i>控制</i> 宜定义并实施过程和规程，以管理与 ICT 产品和服务供应链相关的信息安全风险。
5.22	供应商服务的监视、评审和变更管理	<i>控制</i> 组织宜定期监视、评审、评价和管理供应商信息安全实践和服务交付的变更。
5.23	云服务使用的信息安全	<i>控制</i> 宜根据组织的信息安全要求，建立云服务的获取、使用、管理和退出过程。
5.24	信息安全事件管理规划和准备	<i>控制</i> 组织宜通过定义、建立和传达信息安全事件管理过程、角色和责任，规划和准备管理信息安全事件。
5.25	信息安全事态的评估和决策	<i>控制</i> 组织宜评估信息安全事态，并决定是否将其归类为信息安全事件。
5.26	信息安全事件的响应	<i>控制</i> 宜按照文件化的规程响应信息安全事件。

表 A.1（续）

5.27	从信息安全事件中学习	<i>控制</i> 宜使用从信息安全事件中得到的知识来加强和改进信息安全控制。
5.28	证据收集	<i>控制</i> 组织宜建立并实施包括识别、收集、获取和保存信息安全事态相关证据的规程。
5.29	中断期间的信息安全	<i>控制</i> 组织宜制定在中断期间将信息安全维持在适当级别的计划。
5.30	业务连续性的信息通信技术就绪	<i>控制</i> 宜根据业务连续性目标和 ICT 连续性要求，计划、实施、维护和测试 ICT 的就绪。
5.31	法律、法规、规章和合同要求	<i>控制</i> 宜识别、文件化和保持更新与信息安全相关的法律、法规、规章和合同要求，以及组织满足这些要求的方法。
5.32	知识产权	<i>控制</i> 组织宜实现适当的规程来保护知识产权。
5.33	记录的保护	<i>控制</i> 宜保护记录不被丢失、破坏、篡改、未经授权的访问和未经授权的发布。
5.34	隐私和个人可识别信息保护	<i>控制</i> 组织宜根据适用的法律、法规和合同要求，识别并满足有关隐私保护和 PII 保护的要求。
5.35	信息安全的独立评审	<i>控制</i> 组织管理信息安全的方法及其实现，包括人员、过程和技术，宜在计划的时间间隔内或发生重大变化时进行独立评审。
5.36	符合信息安全策略、规则 and 标准	<i>控制</i> 宜定期评审组织的信息安全策略、主题策略、规则和标准的符合情况。
5.37	文件化的操作程序	<i>控制</i> 信息处理设施的操作规程宜形成文件，并对有需要的工作人员可用。
6	人员控制	
6.1	审查	<i>控制</i> 在加入组织前，宜对所有拟录用工作人员的候选人进行背景审查，并在入职后持续进行，同时考虑适用的法律、法规和道德规范，与业务要求、访问信息的级别和感知到的风险相适宜。
6.2	任用条款和条件	<i>控制</i> 宜在任用合同协议中规定工作人员和组织对信息安全的责任。

表 A.1（续）

6.3	信息安全意识、教育和培训	<i>控制</i> 组织的工作人员和相关方，宜按其工作职能，接受适当的信息安全意识、教育和培训，及定期更新的组织信息安全方针、特定主题策略和规程。
6.4	违规处理过程	<i>控制</i> 宜有正式的、且已被传达的违规处理过程，以对违反信息安全方针的工作人员和其他相关方采取措施。
6.5	任用终止或变更后的责任	<i>控制</i> 宜确定任用终止或变更后仍有效的信息安全责任及其义务，传达至相关工作人员和其他相关方并执行。
6.6	保密或不泄露协议	<i>控制</i> 宜识别、文件化、定期评审反映组织信息保护需求的保密或不泄露协议，并与工作人员和其他相关方签署。
6.7	远程工作	<i>控制</i> 宜在工作人员远程工作时实施安全措施，以保护在组织场所外所访问的、处理的或存储的信息。
6.8	信息安全事态的报告	<i>控制</i> 组织宜提供机制，使工作人员通过适当渠道及时报告观察到的或可疑的信息安全事态。
7	物理控制	
7.1	物理安全边界	<i>控制</i> 宜定义并使用安全边界来保护包含信息及其他相关资产的区域。
7.2	物理入口	<i>控制</i> 安全区域宜由适当的入口控制和访问点保护。
7.3	办公室、房间和设施的安全保护	<i>控制</i> 宜对办公室、房间和设施的物理安全进行设计，并予以实施。
7.4	物理安全监视	<i>控制</i> 宜持续监视场所，以防止发生未经授权的物理访问。
7.5	物理和环境威胁防范	<i>控制</i> 宜对物理和环境威胁的防范进行设计并予以实施，例如：自然灾害和其它对基础设施有意或无意的物理威胁。
7.6	在安全区域工作	<i>控制</i> 宜设计并实现在安全区域工作的安全措施。
7.7	清理桌面和屏幕	<i>控制</i> 宜定义并适当地执行纸质和可移动存储媒体的桌面清理规则和信息处理设施的屏幕清理规则。
7.8	设备安置和保护	<i>控制</i> 宜安全地安置并保护设备。

表 A.1（续）

7.9	组织场所外的资产安全	<i>控制</i> 宜保护组织场所外的资产。
7.10	存储介质	<i>控制</i> 存储介质宜在其获取、使用、运输和处置的整个生存周期内，按照组织的分级方案和处理要求进行管理。
7.11	支持性设施	<i>控制</i> 宜保护信息处理设施使其免于由支持性设施的故障而引起的电源故障和其他中断。
7.12	布线安全	<i>控制</i> 宜保护传输电力、数据或支持信息服务的电缆免受窃听、干扰或损坏。
7.13	设备维护	<i>控制</i> 设备宜予以正确的维护，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	<i>控制</i> 宜对包含存储媒体的设备的所有部分进行核查，以确保在处置或重复使用之前，任何敏感数据和注册软件已被删除或安全的重写。
8	技术控制	
8.1	用户终端设备	<i>控制</i> 宜保护通过用户终端设备进行存储、处理或访问的信息。
8.2	特许访问权	<i>控制</i> 宜限制和管理特许访问权的分配和使用。
8.3	信息访问限制	<i>控制</i> 宜按照已建立的访问控制的特定主题策略，限制对信息及其他相关资产的访问。
8.4	源代码的访问	<i>控制</i> 宜适当对源代码、开发工具和软件库的读写访问进行管理。
8.5	安全鉴别	<i>控制</i> 宜根据信息访问限制和访问控制的特定主题策略实现安全的鉴别技术和规程。
8.6	容量管理	<i>控制</i> 宜根据当前和预期的容量需求，监视和调整资源的使用。
8.7	恶意软件防范	<i>控制</i> 宜实施恶意软件防范，并通过适当的用户意识教育予以支持。
8.8	技术脆弱性管理	<i>控制</i> 宜获取有关使用中的信息系统的技术脆弱性的信息，评价组织暴露于此类脆弱性的风险，并采取适当措施。
8.9	配置管理	<i>控制</i> 宜建立、记录、实施、监视和评审硬件、软件、服务和网络的配置，包括安全配置。

表 A.1 (续)

8.10	信息删除	<i>控制</i> 当不再需要时，宜删除存储在信息系统、设备或任何其他存储媒体中的信息。
8.11	数据脱敏	<i>控制</i> 宜根据组织关于访问控制的特定主题策略和其他相关的特定主题策略以及业务要求使用数据脱敏，并考虑到适用的法律法规。
8.12	数据防泄漏	<i>控制</i> 数据防泄露措施宜用于处理、存储或传输敏感信息的系统、网络 and 任何其他设备。
8.13	信息备份	<i>控制</i> 信息、软件和系统的备份副本宜按照商定的备份特定主题策略进行维护和定期测试。
8.14	信息处理设备的冗余	<i>控制</i> 信息处理设施宜具有足够的冗余以满足可用性要求。
8.15	日志	<i>控制</i> 宜生成、存储、保护和分析用于记录活动、异常、故障及其他相关事态的日志。
8.16	监视活动	<i>控制</i> 宜监视网络、系统和应用程序，以发现异常行为，并采取适当措施评价潜在的信息安全事件。
8.17	时钟同步	<i>控制</i> 组织使用的信息处理系统的时钟宜与批准的时间源同步。
8.18	特权实用程序的使用	<i>控制</i> 对于可能超越系统和应用控制的实用程序的使用宜予以限制并严格控制。
8.19	运行系统软件的安装	<i>控制</i> 宜实施规程和措施以安全地管理运行系统上的软件安装。
8.20	网络安全	<i>控制</i> 宜保护、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	<i>控制</i> 宜识别、实施和监视网络服务的安全机制、服务级别和服务要求。
8.22	网络隔离	<i>控制</i> 宜在组织的网络中隔离信息服务组、用户组和信息系统组。
8.23	网页过滤	<i>控制</i> 宜管理对外部网站的访问，以减少对恶意内容的暴露。
8.24	密码技术的使用	<i>控制</i> 宜定义并实现有效使用密码技术的规则，包括密钥管理。

表 A.1（续）

8.25	安全开发生命周期	<i>控制</i> 宜建立并应用软件和系统安全开发规则。
8.26	应用程序安全要求	<i>控制</i> 在开发或获取应用程序时，宜识别、规定和批准信息安全要求。
8.27	安全体系架构和工程原则	<i>控制</i> 宜建立、维护工程安全体系的原则并进行文档化，将其应用于所有信息系统开发活动。
8.28	安全编码	<i>控制</i> 软件开发中宜应用安全编码原则。
8.29	开发和验收中的安全测试	<i>控制</i> 宜在开发生存周期中定义和实施安全测试过程。
8.30	外包开发	<i>控制</i> 组织宜指导、监视和评审系统开发外包相关的活动。
8.31	开发、测试和生产环境的隔离	<i>控制</i> 宜隔离并保护开发、测试和生产环境。
8.32	变更管理	<i>控制</i> 信息处理设施和信息系统的变更宜遵从变更管理规程。
8.33	测试信息	<i>控制</i> 宜适当的选择、保护和管理测试信息。
8.34	在审计测试中保护信息系统	<i>控制</i> 宜规划涉及运行系统评估的审计测试和其他保障活动，并在测试人员和适合的管理人员之间达成一致。

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/IEC27003 信息技术-安全技术-信息安全管理体系-指南
- [3] ISO/IEC27004 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/IEC27005 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

中水源禹内部翻译稿