信息安全管理体系认证证书

证书编号：

统一社会信用代码：

建立的信息安全管理体系认证符合标准：

ISO IEC 27001:2022

注册地址：

审核地址：

认证范围：

组织 [具体活动] 相关的信息安全管理活动，适用性声明【编号/版本号】

首次发证日期：　　本次发证日期：　　有效期至：

本证书在国家规定的行政许可、资质许可有效期内有效。获证组织应按规定执行监督审核并经审核合格的情况下方可保持认证证书的有效性。本证书可通过以下方式查询：1. 本机构网站 （http:// www.bozrz.com）2. 中国国家认监委官方网站 （http://www.cnca.gov.cn）

签 发：_____

地址：浙江省杭州市钱塘区白杨街道东部创智大厦1幢1007室
电话：0571-86821236 邮箱：bang_zheng@yeah.net

国际标准

ISO/IEC
27001

第3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

Information security, cybersecurity and privacy protection —

Information security management systems —Requirements

ISO/IEC 27001

目 次

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 1
4.1 理解组织及其环境 1
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系的范围 2
4.4 信息安全管理体系 2
5 领导作用 2
5.1 领导作用和承诺 2
5.2 方针 3
5.3 组织的岗位、职责和权限 3
6 策划 3
6.1 应对风险和机遇的措施 3
6.1.1 总则 3
6.1.2 信息安全风险评估 4
6.1.3 信息安全风险应对 4
6.2 信息安全目标及其实现的策划 5
6.3 变更的策划 5
7 支持 5
7.1 资源 6
7.2 能力 6
7.3 意识 6
7.4 沟通 6
7.5 成文信息 6
7.5.1 总则 6
7.5.2 创建和更新 7
7.5.3 成文信息的控制 7
8 运行 7

8.1 运行的策划和控制 7
8.2 信息安全风险评估 7
8.3 信息安全风险应对 8
9 绩效评价 8
9.1 监视、测量、分析和评价 8
9.2 内部审核 8
9.2.1 总则 8
9.2.2 内部审核方案 8
9.3 管理评审 9
9.3.1 总则 9
9.3.2 管理评审输入 9
9.3.3 管理评审输出 9
10 改进 9
10.1 持续改进 9
10.2 不符合及纠正措施 10
附录 A （规范性附录）信息安全控制参考 11
参考文献 21

前　言

国际标准化组织(ISO)是由各国标准化团体(ISO 成员团体)组成的世界性的联合会。制定国际标准工作通常由 ISO 的技术委员会完成。各成员团体若对某技术委员会确定的项目感兴趣，均有权参加该委员会的工作。与 ISO 保持联系的各国际组织(官方的或非官方的)也可参加有关工作。ISO 与国际电工委员会(IEC)在电工技术标准化方面保持密切合作的关系。

制定本标准及其后续标准维护的程序在 ISO/IEC 指引 第 1 部分均有描述。应特别注意用于各不同类别 ISO 文件批准准则。本标准根据 ISO/IEC 导则第 2 部分的规则起草(见 www.iso.org/directives)。(见 www.iso. org/directives 或 www. iec. ch/members_experts/refdocs) 。

本标准中的某些内容有可能涉及一些专利权问题，对此应引起注意。ISO 不负责识别任何这样的专利权问题。在标准制定期间识别的专利权细节将出现在引言/或收到的 ISO 专利权声明清单中（www.iso.org/patents）。

本标准中使用的任何商品名称仅为方便用户而提供的信息， 不构成代言。

ISO 与合格评定相关的特定术语和表述含义的解释以及 ISO 遵循的世界贸易组织（WTO）贸易技术壁垒（TBT）原则关信息访问以下 URLL：www.iso.org/iso/foreword.html.。在 IEC 中， 请参见 www. iec. ch/understanding-standards

本标准由 ISO/IEC JTC 1 联合技术委员会， 信息技术 SC 27 小组委员会“信息安全、 网络安全和隐私保护”编写。

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

主要变化如下:

——文本已与管理体系标准的统一结构和 ISO/IEC 27002: 2022 保持一致。

关于本标准的任何反馈或问题都应直接向用户的国家标准机构提出。 这些机构的完整名单可以在 www. iso. org/members. html 和 www. iec. ch/national-committees 上找到。

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、保持和持续改进信息安全管理体系的要求。本标准还包括了根据组织需求所剪裁的信息安全风险评估和应对的要求。本标准规定的所有要求是通用的，适用于各种类型、不同规模或性质的组织。

当一个组织声称符合本标准时，不能删减 4 至 10 章所规定的任何要求。

2 规范性引用文件

下列文件对于本标准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标准。凡是不注日期的引用文件， 其最新版本（包括所有的修改单） 适用于本标准。

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

3 术语和定义

本标准采用 ISO/IEC 27000-2018 中所确立的术语和定义。

ISO和IEC设有用于标准化的术语数据库，地址如下：

——ISO 在线浏览平台：http://www.iso.org/obp

——IEC 电力维基百科：https://www.electropedia.org/

4 组织环境

4.1 理解组织及其环境

组织应确定与其宗旨相关并影响其实现信息安全管理体系预期结果的能力的各种外部和内部因素。

杭州邦证认证有限公司

Hangzhou Bangzheng Certification Co., Ltd

信息安全管理体系认证实施规则

文件编号：	BZ-MC-R-105
版　　本：	A/3
编　　制：	
审　　核：	
批　　准：	
控制状态：	受控

2025-08-08 发布　　2025-11-26 实施

文件修订记录表

序号	发布日期	实施日期	修订内容摘要	版次	批准
1	2023-01-16	2023-01-18	新做成	A/0	
2	2025-5-14	2025-5-14	补充 附录 E“信息安全管理体系（ISMS）审核有效人数计算操作指引”	A/1	
3	2025-08-08	2025-08-08	**1 新增：**0 前言 **2 修改：**1 适用范围 **3 补充：**2 规范性引用文件 GB/T 27007 合格评定 合格评定用规范性文件的编写指南 GB/T 27060 合格评定 良好操作规范 **4 补充：**3 原则要求和管理要求 **5 修改：**12 获证组织的信息报告 12.3 信息报送 颁证后 30 日内向国家认监委报送认证信息； 在认证证书有效期间，获证组织发生与信息安全管理体系有关的重大变化时（如获证组织发生重大事故/行政处罚），本机构应及时做出暂停或撤销证书的措施并及时报告国家认监委。 12.4 监管配合 备案规则作为市场监管检查依据，违规行为按《认证认可条例》处罚。 **6 完善：** 联系信息与公开渠道	A/2	
4	2025-11-26	2025-11-26	**补充：**在前言中补充，本规则文本可通过本机构官方网站获取（官方网站：www.bozrz.com）。	A/3	

0 前言

本规则依据《中华人民共和国认证认可条例》、《认证机构管理办法》及《国家认监委关于加强认证规则管理的公告》（2025 年第 9 号）制定。

由杭州邦证认证有限公司（批准号：CNCA-R-2021-885）发布实施。认证机构对本规则的合法性、合规性、科学性负责，并承担主体责任。补充：在前言中补充，本规则文本可通过本机构官方网站获取（官方网站：www.bozrz.com）。

信息安全管理体系审核范围的模式为：组织［具体活动］相关的信息安全管理活动，适用性声明【编号/版本号】。

1 适用范围

1.1 本规则适用于本机构开展的信息安全管理体系认证活动。

1.2 认证对象为建立并运行信息安全管理体系的组织，覆盖组织信息安全管理体系的策划、运行、监控及持续改进全过程。

1.3 本规则依据 ISO/IEC 27001-2022《信息安全、网络安全和隐私保护 信息安全管理体系 要求》标准开展信息安全管理体系认证活动。

2 规范性引用文件

下列文件中的条款通过本文件的引用而成为本文件的条款。未注明日期的， 引用文件的最新版本(包括有效版本) 适用。

CNAS-CC01 《管理体系本机构要求》

GB/T 27000 《合格评定词汇和通用原则》

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

GB/T 27007 《合格评定 合格评定用规范性文件的编写指南》

GB/T 27060 《合格评定 良好操作规范》

CNAS-RC05 《多场所本机构认可规则》；

CNAS-RC07 《具有境外场所的本机构认可规则》；

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》；

CNAS-CC14　《计算机辅助审核技术在获得认可的管理体系认证中的使用》；

CNAS-CC106　《CNAS-CC01 在一体化管理体系审核中的应用》；

CNAS-SC170　《信息安全管理体系本机构认可方案》（ 2023 第二次修订版）

GB/T 30270　《信息技术 安全技术 信息技术安全性评估方法》

GB/T 22081　《信息技术　安全技术　信息安全控制实践指南》

GB/T 29246 《信息技术　安全技术　信息安全管理体系　概述和词汇》

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》

3 原则要求和管理要求

3.1 原则要求

认证机构承诺遵守以下原则：

符合国家法律法规、部门规章及强制性标准；

不涉及国家安全、政治组织、民族宗教等敏感领域；

认证规则名称不含“中国”“国家”“领跑”等禁用词；

认证依据明确，不与国家标准冲突，且鼓励高于行业标准要求；

确保公正性，禁止混淆产品、服务、管理体系认证规则。

3.2 管理要求

3.2.1 认证规则全生命周期管理

建立以下制度并留存记录：

立项论证：评估项目合规性及认证依据适宜性；

规范编制：依据 GB/T 27007、GB/T 27060 编写规则；

符合性自查：发布前自查原则符合性，形成报告；

验收审查：聘请外部专家验收，形成结论性意见；

实施效果评估：每两年评估规则有效性（资源、获证组织绩效等）；

动态维护：跟踪法规/标准更新，及时修订或注销规则。

3.2.2 境外使用声明