奥邦检验认证集团有限公司企业标准

CTS_ABG 67002-2024

信息安全控制管理体系 要求

Information technology - Security techniques -
Information security control management systems - Requirements

2024-10-28 发布　　2024-10-28 实施

奥邦检验认证集团有限公司发布

目录

前言

本文件按照 GB/T1.1—2020《标准化工作导则第 1 部分：标准化文件的结构和起草规则》的规定起草。

本文件规定了信息安全控制管理体系认证的要求，旨在指导组织建立、实施、维护和持续改进信息安全控制管理体系及相关认证活动，通过系统化的控制措施保障信息资产的保密性、完整性和可用性。

本文件由奥邦检验认证集团有限公司技术部提出并起草。

本文件主要起草人：袁海、邵优良。

本文件由奥邦检验认证集团有限公司 2024 年 10 月 28 日批准发布。

本文件自 2025 年 01 月 01 日起实施。

本文件由奥邦检验认证集团有限公司负责解释。

信息安全控制管理体系 要求

1 范围

本文件规定了在组织范围内建立、实施、维护和持续改进信息安全控制管理体系的要求，包括针对组织信息安全风险特征定制的控制措施策划与实施要求。本文件的要求具有通用性，适用于所有类型、规模和性质的组织，无论其所处行业或业务领域。

2 规范性引用文件

以下文件在正文中的引用方式使其部分或全部内容构成本文件的要求。对于注明日期的引用文件，仅引用的版本适用；对于未注明日期的引用文件，引用文件的最新版本（包括任何修订）适用。

GB/T 22081-2024/ISO/IEC 27002:2022《网络安全技术 信息安全控制》

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

3 术语和定义

在本文件中，GB/T 22081-2024/ISO/IEC 27002:2022 和 ISO/IEC 27001:2022 中给出的术语和定义适用。

4 组织环境

4.1 理解组织及其环境

组织应识别与信息安全控制管理相关的外部和内部问题，这些问题可能影响其实现信息安全控制管理体系预期结果的能力。

- 外部问题包括：法律法规变化、行业安全标准更新、供应链安全风险、网络威胁演变等；
- 内部问题包括：组织架构调整、业务流程变更、技术架构升级、人员安全意识水平等。

4.2 理解相关方的需求和期望

组织应确定：

- 与信息安全控制管理体系相关的相关方（如客户、员工、供应商、监管机构、股东等）；
- 相关方的信息安全要求（如客户对数据加密的要求、监管机构对日志留存的规定、供应商对访问控制的需求等）；
- 需通过信息安全控制管理体系满足的相关要求。

注：相关方的要求可包括法律义务、合同条款、行业准则、道德规范等。

4.3 确定信息安全控制管理体系的范围

如需获取全文，请联系奥邦检验认证集团客户服务部门：

1）通过邮件提出申请。请发送到邮箱：17312273399@163.com

2）也可通过客服电话咨询 025-85307007。