# 奥邦检验认证集团有限公司企业标准

CTS_ABG 67032-2024

# 网络空间安全管理体系 要求

Information Security technology -
Cyberspace security management systems - Requirements

2024-06-28 发布　　2024-06-28 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。

本文件规定了网络空间安全管理体系的要求，旨在指导组织建立、实施、维护和持续改进网络空间安全管理体系，覆盖物理环境、网络架构、数据安全、应用防护等全领域安全控制，适用于各行业网络空间安全管理及认证活动。

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 06 月 28 日批准发布。

本文件自 2024 年 06 月 28 日起实施。

本文件由奥邦检验认证集团有限公司负责解释。

# 网络空间安全管理体系 要求

## 1 范围

本文件规定了组织建立、实施、维护和持续改进网络空间安全管理体系的要求，包括网络空间安全风险的识别、评估、处置，以及物理安全、网络安全、数据安全、应用安全等全维度控制措施。

本文件适用于所有类型和规模的组织，无论其所处行业或业务领域，可作为组织实现网络空间安全合规与能力提升的依据，也可用于第三方认证。

## 2 规范性引用文件

下列文件的内容通过文中的引用而构成本文件的规范性条款。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（包括所有的修改单）适用于本文件。

GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》

《中华人民共和国网络安全法》

《中华人民共和国数据安全法》

《中华人民共和国个人信息保护法》

## 3 术语和定义

GB/T 22239-2019 及下列术语和定义适用于本文件。

**3.1 网络空间安全**：指对网络基础设施、信息系统、数据资源及应用程序等进行保护，防范非法访问、攻击、篡改、泄露等风险，保障网络空间的保密性、完整性和可用性。

**3.2 等级保护对象**：指需实施安全等级保护的网络设施、信息系统、云计算平台、物联网、工业控制系统等。

**3.3 边界防护**：指在网络区域边界部署安全控制措施，防止未经授权的访问和数据传输。

**3.4 安全基线**：指为保障网络空间安全而制定的最基本安全配置和控制要求。

**3.5 应急响应**：指针对网络安全事件制定的预防、检测、处置和恢复流程。

## 4 组织环境

### 4.1 理解组织及其环境

组织应识别影响网络空间安全管理体系的内外部因素：

- **内部因素**：组织规模、业务模式、网络架构复杂度、现有安全设施、人员安全意识等；
- **外部因素**：法律法规要求（如等级保护、数据安全合规）、行业标准、供应链安全、网络威胁态势等。

组织应定期评审这些因素的变化，确保体系适应性。

### 4.2 理解相关方的需求和期望

组织应识别与网络空间安全相关的相关方，包括：

- 监管机构（要求合规性报告、等级测评）；
- 客户（要求数据保密性、服务连续性）；
- 合作伙伴（要求接口安全、数据共享合规）；
- 员工（要求安全操作规范、权限管理）。

组织应将相关方需求转化为体系的具体要求，并明确合规义务。

### 4.3 确定体系范围

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**。