白皮书 2026

从合规要求到竞争优势：

ISO/IEC 27001在企业价值创造中的应用

目录

01 摘要

02 引言：不断变化的网络安全环境

03 什么是ISO 27001?——不仅仅是一项认证

04 ISO 27001框架：分阶段实施方法
- 4.1 规划阶段：建立ISMS
- 4.2 实施阶段：运行ISMS
- 4.3 检查阶段：监控与评估
- 4.4 改进阶段：维护与持续改进

05 认证路径：理解审核过程

06 案例研究：强化安全与信任

07 结论

引言：
不断变化的网络安全环境

数字边界正在逐渐消失。随着云计算、远程办公以及高级威胁攻击者的出现，传统固定的网络边界日益失效，“城堡与护城河”的安全模型正在被取代。

数据泄露可能导致巨额经济处罚、业务中断以及不可挽回的声誉损害。企业已无法再依赖被动式、清单式的网络安全管理方法。对一种具备韧性、适应性强且经过实践验证的信息安全风险管理框架的需求，从未像现在这样迫切。

在当今时代，信息已成为企业的核心生命线。然而，数字化转型与网络威胁的持续升级并存。保护信息这一关键资产，不仅依赖技术手段，更需要一种系统化、整体性的管理方法——即管理体系方法。

本白皮书重点介绍国际标准ISO/IEC 27001（信息安全管理体系，ISMS），并阐述该框架如何：

- 强化企业安全防护能力
- 创造实际业务价值
- 提升合规性
- 建立客户与合作伙伴的信任

什么是ISO 27001？
——不仅仅是一项认证

ISO 27001并不是软件，也不是简单的打勾式核查清单。它是一项国际公认的标准，用于建立、实施、维护并持续改进信息安全管理体系（ISMS）。

由经认可的认证机构颁发的ISO 27001认证，是证明您的信息安全管理体系（ISMS）已有效实施和运行，并符合全球最佳实践的权威体现。

ISO 27001的价值逻辑：

业务风险	ISO 27001应对措施	业务收益
数据泄露	风险评估与风险处置	提升防护能力
合规失效	安全控制与制度建设	满足法规要求
运营中断	持续监控机制	客户信任与业务增长

ISO 27001的核心特征：

系统性（Systematic）
ISMS是由政策、程序、流程和控制措施组成的系统性框架，用于管理组织敏感信息的风险

基于风险（Risk-based）
核心在于针对组织特定环境、目标与威胁环境实施信息安全风险评估与处理

整体性（Holistic）
涵盖人员、流程与技术，实现组织范围内统一的安全管理

ISO 27001框架：
分阶段实施方法

1 规划（Plan）：建立ISMS

- 确定范围：
明确ISMS适用范围（全组织/特定业务单元）

- 组织环境与领导作用：
确保管理层支持并识别内外部环境

- 设定目标：
将信息安全目标纳入整体业务目标

- 定义风险评估方法：
明确风险阈值、风险偏好及风险接受准则

2 实施（Do）：运行ISMS

- 风险评估与处置：
识别您的信息资产在保密性、完整性和可用性方面所面临的风险，对其进行分析，并根据附录A中的要求实施相应的控制措施。

- 控制实施，包括
  - 技术控制（如加密、访问控制）
  - 物理控制（如访问限制）
  - 组织与人员控制（如职责划分、安全意识培训）

- 文档体系建设，包括：
  - 适用性声明（SoA）
  - 风险处理计划（RTP）
  - 信息安全方针

- 员工意识：确保员工理解其在ISMS中的职责

3 检查（Check）：监控与评估

- 绩效评估：
通过KPI衡量控制措施效果

- 内部审核：
定期开展ISMS内部审核，验证符合性与有效性

- 管理评审：
管理层定期评估体系适宜性、充分性与有效性

4 改进（Act）：持续优化

- 纠正措施：
针对问题采取改进行动

- 持续改进：
基于检查结果优化体系，应对变化环境

认证路径：
理解审核过程

ISO 27001认证由经认可的认证机构通过两阶段审核完成：

- **第一阶段审核**（文件审核 / 准备情况评估）审核员对信息安全管理体系（ISMS）的文件进行审查，确保其符合标准要求，并核实关键要素的存在。

- **第二阶段审核**（现场审核）审核员将前往企业现场，核查信息安全管理体系（ISMS）是否已得到适当实施，并在实际运行中有效执行。审核通过后（包括对审核结果的独立评审），将颁发有效期为三年的认证证书。此后通过年度监督审核，以确保体系持续符合相关要求。

成功获得ISO 27001认证的关键步骤

1 认证审核（初次审核）

- 文件审核：确认信息安全管理体系（ISMS）符合标准要求
- 现场审核：验证体系有效实施与运行

2 审核报告

- 出具审核结果
- 评价体系符合性与成熟度

3 认证证书（有效期3年）

- 获得ISO 27001认证证书
- 可用于对外展示与市场竞争

核心价值：提升客户信任与市场认可度

4 第一次监督审核

- 验证体系持续有效运行

核心价值：确保不是“一次性合规”，而是持续管理

5 第二次监督审核

- 再次验证体系稳定性与执行效果

核心价值：强化管理成熟度与执行能力

6 再认证

- 重新进行审核以延续认证（再3年）

核心价值：持续维护企业信息安全能力与品牌信誉

案例研究：
强化Innovatech Manufacturing的安全与信任

Innovatech Manufacturing是一家中型精密制造企业，由于远程办公、全球供应链及敏感设计数据的存在，面临日益严峻的数据保护挑战。

频繁的小规模安全事件与审核问题暴露出其安全体系的不足，并影响客户信任与合规表现。

实施路径（PDCA）：

- **Plan:** 识别关键信息资产与风险，并获得管理层支持
- **Do:** 在IT系统、生产流程及员工操作中实施控制措施，并开展培训
- **Check:** 通过内部审核与KPI监控评估效果
- **Act:** 持续改进并强化体系

实施成果：

- 12个月内获得ISO 27001认证
- 客户信任显著提升，获得汽车及航空领域新订单
- 安全事件减少60%，避免潜在业务中断与经济损失
- 建立企业级安全文化

结论：
对于安全韧性与信任能力的投资

ISO 27001不仅仅是合规要求，更是对企业长期发展的一项战略投资。它为企业提供清晰、结构化的方法，用于应对21世纪最重要的业务风险之一——信息安全风险。

通过实施ISO 27001：

- 不仅实现数据保护
- 更建立信任基础
- 提升运营成熟度
- 增强企业在不确定数字环境中的长期竞争力

想要了解更多信息？

联系我们

DEKRA

DEKRA德凯亚太区
服务热线：400 688 1925
邮箱：info@dekra.com.cn
网址：www.dekra.com.cn