



## FAQ – ISO 27001 信息安全管理

我们的专家就 ISO 27001 信息安全认证的常见问题进行了解答。希望了解更多 ISO 27001 的信息？请随时与我们联系！

### 1. ISO 27001 的目的是什么？

ISO 27001 旨在为信息保护提供统一和集中控制的管理体系。此外，通过有效监控 IT 安全风险，可降低各类业务流程所面临的威胁。

### 2. ISMS 指什么？

信息安全管理（ISMS）是综合了技术和人为因素的系统方法。它能根据您所规定的保护需求，帮助企业建立持续优化和监管流程。ISO 27001 说明了 ISMS 的详细实施要求和文件要求。

### 3. ISO 27001 认证对我的公司有什么好处？

- 防止企业遭受网络攻击
- 防止数据丢失，从而杜绝财务和声誉损失
- 确保符合法律要求
- 减少黑客攻击，最大程度地降低黑客访问敏感信息的能力

ISO 27001 认证的其他优势包括：

- 确保 IT 系统和程序的可用性
- 信息的保密性
- 竞争优势
- 发现和消除薄弱环节
- 最大程度降低 IT 风险和潜在损害
- IT 风险控制
- 确保满足合规要求
- 成本降低

#### 4. ISO 27001 认证需要评估哪些内容？

- 信息安全指南
- 人力资源安全
- 资产管理
- 物理和环境安全
- 访问控制
- 密码
- 运行安全
- 通信安全
- 系统获取、开发和维护
- 供应商关系
- 信息安全事件管理
- 业务连续性管理的信息安全方面
- 符合性

#### 5. ISO 27001 信息安全认证过程是怎样的？

我们的专家将按照以下步骤对贵公司进行检验和认证：

##### 1. 预审核（可选）

我们的审核员首先了解贵公司现场的当前状态。

##### 2. 认证审核（一阶段）

我们使用审计协议评估和记录贵公司的管理体系文件。我们确定并评估贵公司经营场所，并检查您是否符合法律和官方规定等。

##### 3. 认证审核（二阶段）

您展示信息管理体系的实际应用。审核员检查证据的适宜性和有效性。审核结束后，您将在总结会议中获得审核结果。

#### 4. 出具证书

如果满足所有标准要求，贵公司将获得 ISO 27001 证书。证书证明贵公司管理体系的符合性和有效性。此外，贵公司将同时录入到我们的线上证书数据库 Certipedia。

#### 5. 监督审核

我们的年度监督审核将帮助您持续优化 IT 流程。

#### 6. 再认证

三年认证有效期满前再认证，贵公司可持续改进流程。通过长期改进，您将向客户证明贵公司对信息安全的承诺。

#### 6. ISO 27001 证书的有效期多长？

证书的有效期为三年。通过年度监督审核和在三年期满前再认证，可确保贵公司持续改进流程。

#### 7. 企业如何获得信息安全？

企业需要根据最低标准采取网络安全措施。

此外，还需满足有关技术和组织规定，确保数据的可用性、完整性、保密性。如遇黑客攻击，必须立即报告。

我们的专业人员乐意为您解答任何疑问。请随时和我们联系！

### 在线联系方式

为安全而菜，菌品质而生  
Here for safety. Born for quality.

德国莱茵TÜV大中华区  
TÜV Rheinland Greater China

服务热线 Hotline  
4008831300/8009993668  
+852 21921022 (中国香港 Hongkong)  
service-gc@tuv.com

[www.tuv.com](http://www.tuv.com)

关注我们的微信：

TUV 莱茵

TUV 莱茵管理体系服务



 **TÜVRheinland®**  
Precisely Right.