



信息安全管理体系（ISMS）

什么是信息安全管理体系以及您为什么需要它？

信息安全管理体系是企业内部用于持续控制和改进信息安全的一个方法、规则和制度的集合。

信息安全管理体系的基本目标是在公司处理的信息中识别相关风险并有针对性地处理这些风险。

建立信息安全管理体系有诸多好处，可做到：

- 符合法规及合同要求
- 向第三方证明组织的信息安全
- 识别、评估及处理现有风险
- 通过制定应对风险的措施提高经济效益

关注信息

信息安全管理体系的重点关注对象是对企业至关重要的信息，外加该信息所必需的一切资源。信息往往是指信息技术，因为信息技术通常是基本的支持流程。然而，诸如文档信息、人员以及建筑安全等其他领域也应纳入信息的考量范围。

基于贵公司的目标和价值观，信息安全管理体系会识别和评估贵公司的重要信息资产在保密性、可用性和完整性方面的价值。

基于风险的方法及公认的标准

信息安全管理体系根据选择的风险评估准则来识别、评估和处理现有风险。风险管理为选择和执行适当的管控措施建立了一个有效、直观、可再现的基础框架。除此之外，您还可以有针对性地选择风险接受、风险规避或者风险转移。

作为我们风险管理流程的一部分，所采取的行动通常源自于公认的标准，尤其是遵守信息技术 - 信息安全 - 信息安全控制使用规则（ISO/IEC 27002:2013）、德国联邦安全信息技术局制定的基本信息技术保护标准，或者行业通用标准。这些标准对风险管理流程提供补充，并为贵公司达到理想的信息安全水平提供了坚实的基础。

成功的关键

综合性方法是信息安全管理体系成功的关键，因为信息安全管理体系旨在保护价值链中每一个环节的重要信息。为了达到理想的安全水平，信息安全管理体系会与现有的组织结构及其流程相互作用。除了信息技术，信息安全管理体系主要处理以下几种问题：

- | | | |
|--------|--------|-----------|
| ▪ 公司组织 | ▪ 人员安全 | ▪ 物理安全 |
| ▪ 访问控制 | ▪ 事件管理 | ▪ 业务连续性计划 |

持续优化流程

建立和运行信息安全管理体系并非一劳永逸的过程，而是一个不断重复的过程。这个过程需要完成所有常规活动，比如风险管理、内部审核及管理评审。除此之外，信息安全管理体系的流程、规则及结果要进行持续的严格评估，并且在必要时进行调整以实现改进。

适合自身且高绩效

信息安全管理体系拥有的结构化体系使复杂且通常高成本的措施不至于孤立地执行，而是在符合现有风险和经济可行性的背景下实施。这将产生协同效应，并且有助于降低策划、实施和正在运行的成本。

实践表明，对比相互矛盾的，以及在多数情况下相互重叠的定制解决方案，集中化的解决方案通常可以在更少的资源下实施，并且可以提供更高级别的安全性和更高的可靠性。

综合管理体系运作

信息安全管理体系无需作为一个孤立的体系进行策划和实施。它可以与现有管理体系（如：质量管理体系，业务连续性管理体系）进行整合或者以现有的管理体系为基础。这种方法能够利用协同效应、避免冗余并且可持续性地增加雇员的接受度。

认证证明

符合国家或者国际标准（如：ISO/IEC 27001:2013 和 IT - Grundsicherheits standards）的信息安全体系可由一个经官方认可的组织为其颁发认证证书。

拥有认证证书后，贵公司便可向第三方，如，政府部门、审核员、客户和合作伙伴提供信息安全方面的证明。

TÜV 莱茵集团服务范围

- 现有信息安全管理体系分析
- 信息安全管理体系的策划和实施
- 信息安全管理体系的持续运维
- 风险评估
- 设计并实施意识宣传
- 为信息安全管理者进行指导

为安全而莱，茵品质而生
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)
888@tuv.com

关注我们的微信：

TUV 莱茵

TUV 莱茵管理体系服务



 **TÜVRheinland®**
Precisely Right.

www.tuv.com