ISO27001 快速实施工具软件

ISO27001 Easy Tool

白皮书

科飞咨询

www.cofly.com

sd@cofly.com

目 录

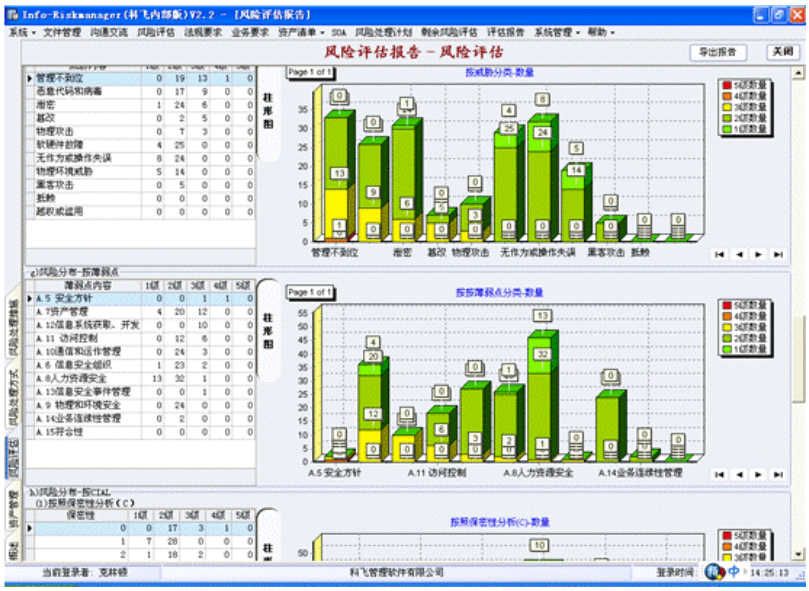
ISO27001 Easy Tool

介 绍

科飞管理咨询公司

一. 用途

ISO27001 Easy Tool 能够协助各类机构高效、快速、规范、全面的按照 ISO27001 标准要求建立、实施和运行信息安全管理体系，获得第三方认证证书。



二. 适用范围

ISO27001 Easy Tool 适用于各类机构，包括电力、通信、金融、证券、生产制造业、研究院所、IT 服务、软件及软件外包、政府机关等，用最快的速度、最低的成本，按照 ISO27001 要求建立信息安全管理体系。

从事 ISO27001 咨询机构也可借助 ISO27001 Easy Tool，简化咨询流程，减少咨询人员的占用时间，缩短咨询周期。

教学机构也可利用 ISO27001 Easy Tool 指导学员学习 ISMS 的建立过程，实际演练风险评估过程。

三. 应用效果

使用 ISO27001 Easy Tool, 可以达到如下效果：

- 能够显著的提高建立 ISO27001 信息安全管理体系的效率；
- 大幅度缩短建立信息安全管理体系的时间；
- 减少贯标项目参与人员的工作量；
- 监控信息安全管理体系建立过程的进度；
- 节省 ISO27001 的建立和实施费用（内部资源占用费用和咨询费用）；
- 保证信息安全管理体系建立的完整性和效果；
- 完全符合 ISO27001、ISO27002 和 ISO27005 标准的要求；
- 方便认证机构的现场审核；
- 便于对 ISMS 进行持续改进和维护；
- 有助于保证 ISMS 资料，特别是风险评估数据的保密性。

四. 软件特点

ISO27001 Easy Tool 内置实施 ISO27001 所必须的信息安全管理知识、文件模版、数据模型和参考数据，具有过程完整、使用方便、符合标准的特点，如下：

- 内置 ISO27001 信息安全管理体系范围和方针模版；
- 内置 ISO27001 项目启动所必需的通知、职责分配等文件和记录；
- 内置 ISO27001 和 ISO27002 标准；
- 内置完整的信息安全风险评估数学模型；
- 内置风险处置、选择风险控制措施和风险处理计划管理流程；
- 内置信息安全事件报告、响应和处理流程；
- 内置全面的资产、风险分析工具；
- 内置信息安全管理组织模版；
- 内置 ISO27001 所必须的全部 ISMS 文件模版；
- 内置 ISO27001 所必须的全部 ISMS 记录模版；
- 内置常用的、与信息安全相关的法律法规和标准；

- 能够自动生成 ISO27001 风险评估所要求的全部文件、记录；
- 能够自动生成《风险评估报告》；
- 能够自动生成《风险处理计划》；
- 能够自动生成《风险处理计划检查记录》；
- 能够自动生成《适用性声明(SOA)》；
- 能够对各部门参与风险评估、文件制定的过程进行管理；
- 能够完成文件和记录管理功能；
- 能够完成事件管理功能；
- 能够识别、管理法律法规中的信息安全要求；
- 能够识别、管理企业自身对信息安全要求。

五. 功能介绍

ISO27001 Easy Tool 的功能：

1. ISO27001 基本知识

包含 ISO27001 相关的基本知识，可用于员工的信息安全意识和知识培训，满足

ISO27001 4.2.2 和 5.2.2 中的培训要求，具体内容包括：

- 信息安全相关的术语和定义；
- 信息安全管理的基本知识；
- 信息安全管理体系的建立与实施；
- 信息安全管理体系认证认可；
- 信息安全风险管理与风险评估；
- 风险评估软件工具 Info-Riskmanager；
- 我国信息安全法律法规和标准化；
- 信息安全管理的其他可供参考的标准。

2. 标准及理解

- 包含完整的 ISO/IEC 27001 和 ISO/IEC 27002 中英文标准，并附带标准的理解和使用指南。
- 为了方便学习，本部分内容以标准的章节条款为单元，采用中文标准和英文标准对照的方式编排，在每个章节的中英文对照后面，是标准的理解和使用指南。编排格式如下：

中文标准
英文标准
理解
指南

3. 文件管理

- 可以对 ISMS 建立过程的全部文件进行管理，包括：信息安全范围、方针、目标、组织机构、手册、程序文件、记录等。
- 利用文件管理功能，企业可以进行文件发布和更新，员工可以利用文件管理功能查阅、学习企业发布的文件。
- 程序中内置 ISO27001 所要求的全部文件模版和记录模版，数量达到 187 个，用户可以利用这些模版，结合企业自身的特点和实际情况，快速生成适宜的、符合

ISO27001 标准要求的 ISMS 文件和记录，并利用文件管理功能进行发布。

内置的文件符合 ISO27001 的 4.3.1 中的文件要求。

4. 沟通交流

- 在 ISMS 建设过程中，在上下级之间、部门之间需要有大量的沟通工作，包括：信息安全方针、范围的发布；信息安全组织机构设置及职责；风险评估方法；实施计划安排；进展状况反馈；问题与解答；内部审核计划及审核结果反馈；纠正与预防措施的落实等等，利用软件的沟通交流功能，可以方便的就 ISMS 建立过程中的各类问题进行沟通，保证 ISMS 建设工作的顺利进行；
- 能够自动形成并导出与信息安全组织和信息安全体系文件相关的沟通信息。

本功能符合 ISO27001 的 4.24 和 5.1 中相关的规定和 ISO27005“风险沟通”的相关要求。

5. 风险评估

信息安全风险评估是 ISO27001 信息安全管理体系的核心和基础，**ISO27001 Easy Tool** 的风险评估模块，能够实现完整的风险评估和风险管理功能，包括：

A、 资产管理

- 分类识别全部资产；
- 按照资产自身价值、CIAL(保密性、完整性、可用性、合规性)重要程度，自动评估资产的重要度；
- 预置风险评估准则，自动判定重要资产；
- 能够自动形成并导出《资产清单》和《重要资产清单》。

B、风险识别

- 对重要的资产识别所面临的威胁；
- 识别可以为威胁所利用的薄弱点；
- 评估威胁利用薄弱点发生信息安全事件的可能性；
- 根据事件发生后对 CIAL 的影响，自动评估事件对信息系统和业务的影响程度；
- 分析现有控制措施及有效性。

C、 风险评价

- 根据风险识别的结果，自动计算风险值，确定风险等级；
- 内置风险评价准则，根据风险准则，自动判断是否属于高风险。

D、 风险处理计划及控制计划

- 针对风险评估的结果，选择风险处理方式；
- 对应风险处理方式，选择风险控制目标及措施；
- 将控制措施落实到具体的责任部门和责任人，限定完成时限；
- 能够自动形成并导出《风险处理计划》和《风险处理计划检查记录》；
- 能够自动形成并导出《风险评估报告》；
- 根据风险处理计划检查情况，评估处理措施的有效性，自动计算剩余风险，并根据风险接受准则，判断是否接受；
- 能够自动形成并导出《剩余风险评估报告》。

E、连续进行风险评估

- 能不限次数的对同一资产，连续进行风险评估。

F、查询统计

- 按照不同的要求，对资产和风险进行查询分析；
- 能够自动监测、查询、统计风险评估过程中的错误和遗漏，保证评估信息、评估过程的完整性。

风险评估的功能符合 ISO27001 的 4.2.1,ISO27002 第 4 章,以及 ISO27005 的规定。

6. 事件管理

- 能够完成事态（Event）报告、事态分析、事件（Incident）确认、事件分类、事件分级、事件响应、事件调查、改进总结等功能。

符合 ISO27001 的 4.2.2，4.2.3，8.2.2，8.2.3，以及 ISO27002 第十三章的规定。

7. 法规要求

满足法律法规、上级规定、以及与相关方签订的合约中的信息安全要求是建立 ISMS，设定信息安全可接受水平的必要条件，利用 ISO27001 Easy Tool 的法规要求功能，可以方便的识别法律法规、确定法律法规中的信息安全要求、根据要求建

立风险控制计划。

符合 ISO27001 的 4.2.1 中的相关规定。

8. 业务要求

在与组织战略和风险管理相一致的环境下，建立和保持 ISMS 是任何机构必须考虑的重要因素，利用 ISO27001 Easy Tool 的业务要求功能，可以方便的对机构自身的信息安全方向、政策和要求进行管理，并通过风险控制计划加以落实。

符合 ISO27001 的 4.2.1 中的相关规定。

9. 剩余风险评估

风险处理计划实施后，评定风险降低的程度，判断剩余风险是否可接受。如剩余风险仍不可接受，可继续增加新的控制措施。

符合 ISO27001 的 4.2.1 的规定。

10. 自动生成资产清单

自动生成资产清单、重要资产清单。可按资产的全部属性进行查找、筛选和排序。允许将结果导出 Excel 文件。

符合 ISO27001 的 4.2.1 的规定。

11. 自动生成风险控制计划

自动生成风险处理计划清单。可按资产、风险等级、处理方式、处理措施、资产所有者、措施实施责任部门、计划时间、关联业务或系统等方式查看、分析风险处理计划。可按资产的属性、风险评估的过程参数或结果对风险处理计划进行查找、筛选和排序。允许将结果导出 Excel 文件。

符合 ISO27001 的 4.2.1 的规定。

12. 自动生成 SOA

《适用性声明（SoA）》是 ISO27001 标准要求的必须具备的文件之一，利用 ISO27001 Easy Tool 可以方便的自动生成 SoA，并且能够随着选择控制措施的变化，自动更

新 SoA 内容。

符合 ISO27001 的 4.2.1 的规定。

13. 自动生成风险评估报告

自动生成风险评估报告，系统性的对资产、风险、风险处理方法、风险处理措施和剩余风险进行全面统计和分析。通过风险评估报告，可以概括性的了解一个组织的信息资产构成和分布、风险分布趋势、风险控制措施概况，便于决策者从宏观分析信息安全风险，采取相应的风险管理方法。允许将结果导出 Word 文件。

符合 ISO27001 的 4.2.3，7.2，8.1 的规定。

14. 系统管理

可以对 **ISO27001 Easy Tool** 的基础参数进行个性化调整设置；增减用户并设置用户的使用权限。

六. 使用要求

1. 软件要求

服务器端	Windows 2000 Server SP4, SQL Server 2000
客户端	Windows98/2000 Professional/XP（建议使用 Win 2000 或 xp）

2. 硬件要求

服务器端	CPU（P4 以上）、内存（512 M 以上）、硬盘（不少于 80G）
客户端	CPU（P4 以上）、内存（不低于 256M）

3. IP 地址要求

如果需要从外部通过互联网使用软件，公司必须有一个固定 IP 地址。