信息安全作业 14

190110429-何为

1. 如何理解信息安全管理的内涵?

答:

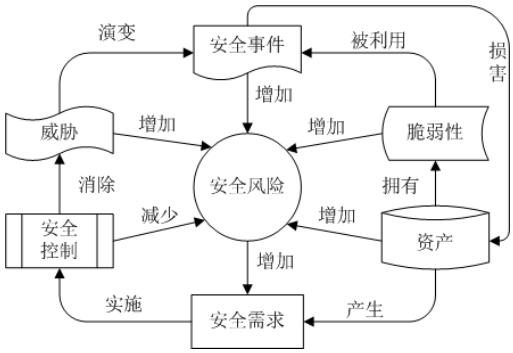
信息安全管理是一个十分复杂的综合管理体系，规章制度、法律法规和道德规范是管理的基础，标准规范是信息系统实施和安全运行的保证，风险管理是建设信息安全管理体系的重要手段。

由此形成信息安全管理体系（ISMS），它是一个系统化、过程化的管理体系，风险评估管理、标准规范管理以及制度法规管理 3 个方面直接影响到整个信息安全管理体系是否能够有效实行。

2. 各信息安全风险因素之间的关系是怎样的?

答:

信息安全中存在的风险因素之间相互作用、相互影响。在信息安全管理过程中，安全风险随各因素的变化呈现动态调整演变趋势，威胁、脆弱性、安全事件及资产等风险因素的增加均会扩大安全风险，只有安全控制的实施才能有效地减少安全风险。



3. 风险评估的主要任务有哪些?

答:

（1） 识别组织面临的各种风险，了解总体的安全状况;

（2） 分析计算风险概率，预估可能带来的负面影响;

（3） 评价组织承受风险的能力，确定各项安全建设的优先等级;

（4） 推荐风险控制策略，为安全需求提供依据。

4. 实施风险控制主要包括那些步骤?

答:

具体 7 个步骤如下:

（1） 对实施控制措施的优先级进行排序，分配资源时，对标有不可接受的高等级的风险项应该给予较高的优先级;

（2） 评估所建议的安全选项，风险评估结论中建议的控制措施对于具体的单位及其信息系统可能不是最适合或最可行的，因此要对所建议的控制措施的可行性和有效性进行分析，选择出最适当的控制措施;

（3） 进行成本效益分析，为决策管理层提供风险控制措施的成本效益分析报告;

（4） 在成本效益分析的基础上，确定将实施的成本有效性最好的安全措施;

（5） 遴选出那些拥有合适的专长和技能，可实现所选控制措施的人员（内部人员或外部合同商），并赋以相应责任；

（6） 制定控制措施的实现计划，计划内容主要包括风险评估报告给出的风险、风险级别以及所建议的安全措施，实施控制的优先级队列、预期安全控制列表、实现预期安全控制时所需的资源、负责人员清单、开始日期、完成日期以及维护要求等；

（7） 分析计算出残余风险，风险控制可以降低风险级别，但不会根除风险，因此安全措施实施后仍然存在的残余风险。

5. CC 标准与 BS 7799 标准有什么区别？

答：

（1） 所属标准不同：

CC 标准属于技术与工程标准，而 BS 7799 是信息安全管理与控制标准的代表。

（2） 主要思想不同：

CC 标准提倡安全工程的思想，通过信息安全产品的开发、评价、使用全过程的各个环节的综合考虑来确保产品的安全性。

BS7799 旨在具体有效指导信息安全具体实现，最终目的是建立适合企业所需的信息安全管理体系。

（3） 内容方面不同：

CC 标准包括“简介和一般模型”、“安全功能要求”、“安全保证要求”三部分。涵盖安全需求的定义；需求定义的用法；安全可信度级别；安全产品的开发和产品安全性评价等几个方面。

BS7799 是英国标准协会（British Standards Institute，BSI）针对信息安全管理而制定的一个标准，共分为两个部分，其中 BS7799-1 是《信息安全管理实施细则》，另一部分 BS7799-2 是《信息安全管理体系规范》（即 ISO/IEC 27001）。