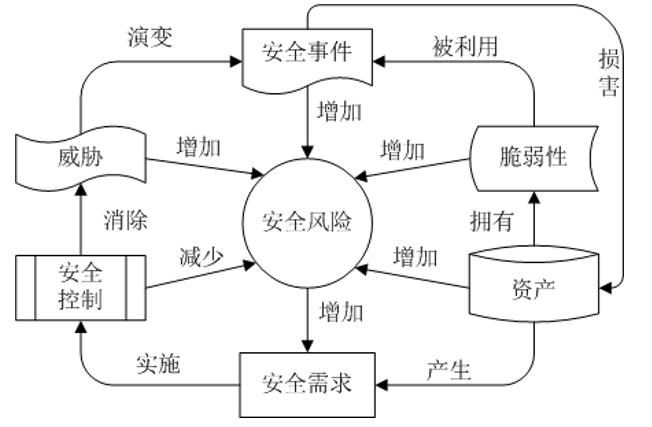
1.信息安全管理的内涵：体现预防控制为主的思想，强调遵守国家有关信息安全的法律法规，强调全过程的动态调整，从而确保整个安全体系在有效管理控制下，不断改进完善以适应新的安全需求

2.信息安全风险因素主要包括：威胁、脆弱性、资产、安全控制

风险因素之间相互作用、相互影响。安全风险随各因素的变化呈现动态调整演变趋势。

其相互关系可用下图表示：



3.风险评估的主要任务包括：

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以下步骤：

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，确定即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。其主要内容包括安全需求的定义，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。第一部分BS7799-1是《信息安全管理实施细则》，第二部分BS7799-2是《信息安全管理体系规范》。

CC标准侧重于对系统和产品的技术指标，旨在支持产品中IT安全特征的技术性评估。而BS7799则偏重于安全管理方面的要求。