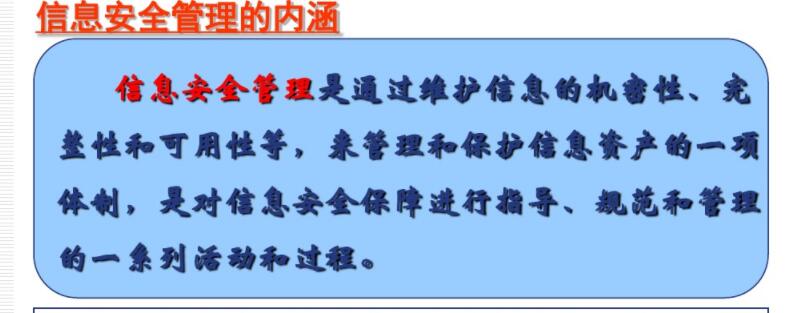
1. 如何理解信息安全管理的内涵



1. 各信息安全风险因素之间的关系

各因素之间相互影响、相互作用。

1. 风险评估的主要任务
2. 识别面临的风险，了解安全状况
3. 分析计算风险概率，了解可能带来的负面影响
4. 评价承受风险能力，确定各项安全建设的优先等级
5. 推荐风险控制策略，为安全需求提供依据
6. 实施风险控制主要的步骤
   1. 对不同安全措施优先级进行排序
   2. 评估并选择出最适当的安全选项
   3. 进行成本效益分析
   4. 选择合适的实现控制措施的人员
   5. 指定控制措施的实施计划
   6. 分析计算出残余风险
7. CC标准与BS7799标准
   1. CC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。 BS 7799则偏重于安全[管理](http://www.lwlm.com/Manages/)方面的要求。它不是一篇技术标准，而是管理标准。它处理的是对IT系统中非技术 内容 的检查。这些内容与人员、流程、物理安全以及一般意义上的安全管理有关。
   2. CC中虽对信息安全管理方面提出了一定的要求，但这些管理要求是孤立、相对静止的、不成体系的。同样，BS 7799也涉及极小部分的技术指标，但仅限于管理上必须的技术指标。
8. 我国有关信息安全的法律法规特点：
9. 信息安全法律法规体系初步形成
10. 与信息安全相关的司法和行政管理体系迅速完善
11. 目前法律规定中法律少而规章等偏多，缺乏信息安全的基本法。
12. 相关法律规定篇幅偏小，行为规范较简单。
13. 与信息安全相关的其他法律有待完善