多变环境下的企业安全合规与审计机制

问题讨论

Powertime 时代新威

北京

2016.07.14

自我介绍

王新杰

- 全国信息安全标准化技术委员会（TC260）第二届委员
- 全国金融标准化技术委员会(TC180)第三届专家委员
- 中国合格评定认可委员会ISMS/ITSMS评审技术专家
- 全国信息技术标准化技术委员会ITSS工作组成员
- 国际信息安全标准化组织ISO/IEC JTC1/SC27注册专家
- 国际信息系统安全认证联盟(ISC)²中国顾问
- 亚洲信息安全论坛（RAISE Forum）成员

联系方式：wangxinjie@powertime.cn 13701275907

主要内容

1. 问题
2. 问题
3. 问题
4. ……

听众调查

序号	听众来自	比例
1	安全企业（包括产品和服务）	
2	非安全企业	

多变环境？

生产工具

生产资料

营业模式

IT环境

……

人在变

“变”是当下世界唯一不变的主题！

合什么规？

网络安全法

等保

27001

27017

29101

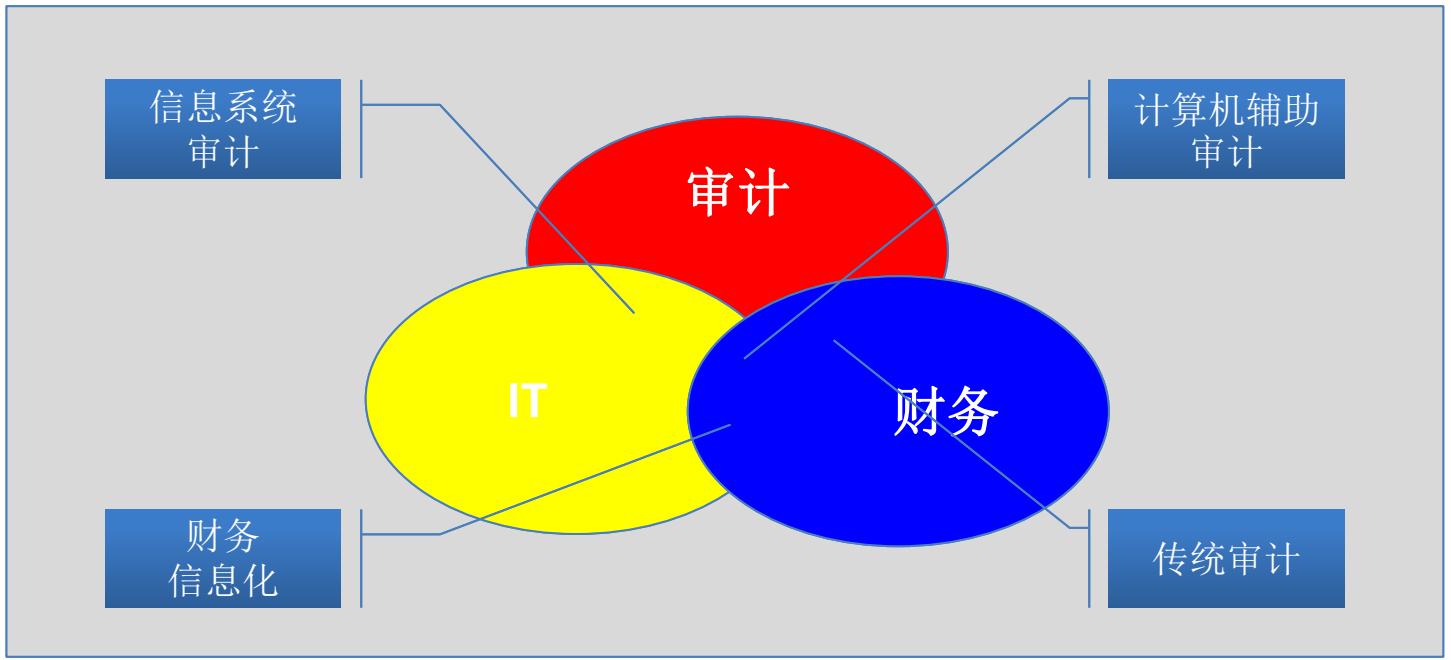
22301

PCI DSS

监管要求

……

审计？



又一个交叉领域：“IT”+“审计”

诸多叫法

信息科技审计

信息科技风险审计

信息系统审计

IT审计

信息系统控制审计

专项审计名称

- ✓ 信息安全审计
- ✓ 数据中心审计
- ✓ 业务连续性审计
- ✓ 信息科技外包审计
- ✓ 数据质量审计
- ✓ 系统投产变更审计

今天的讨论，统一用“信息系统审计”这一术语

实践？

- 1960s，美国开始信息技术审计实践；
- 1977年，ISACA CobiT发布，至2013年已是5.0版；
- 2001年1月，GAO发布FISCAM，2009年2月发布第二版；
- 2002年7月25日，美国发布SOX法案，其中404条款提出内部控制要求；
- 至今，全球企业受美国SOX法案影响，纷纷开展信息系统审计；

国内实践


Powertime

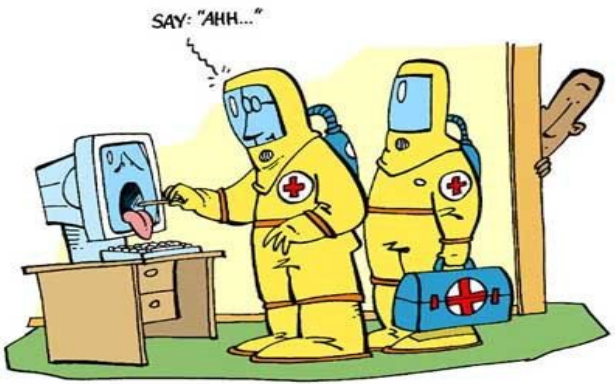
专业人员教育培训

注册信息安全审计师
CISP - Auditor

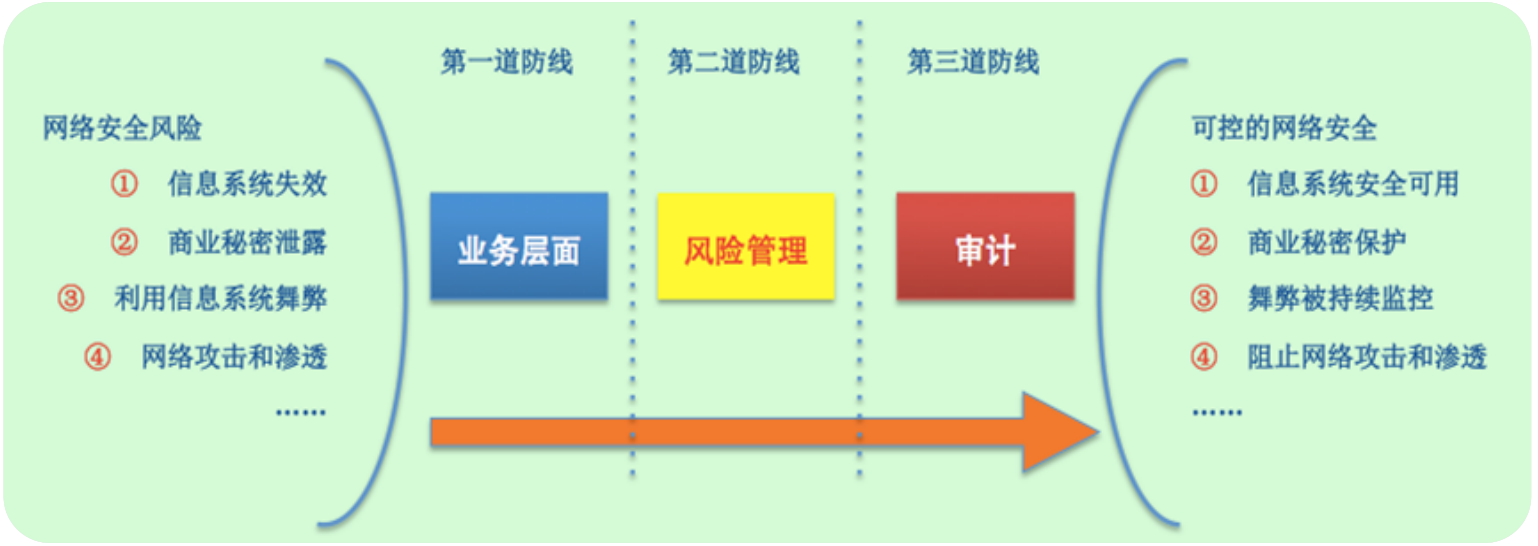
异同？

- 风险评估
- 安全测评
- 等保测评
- ISMS审核
- 安全审查

……



机制？

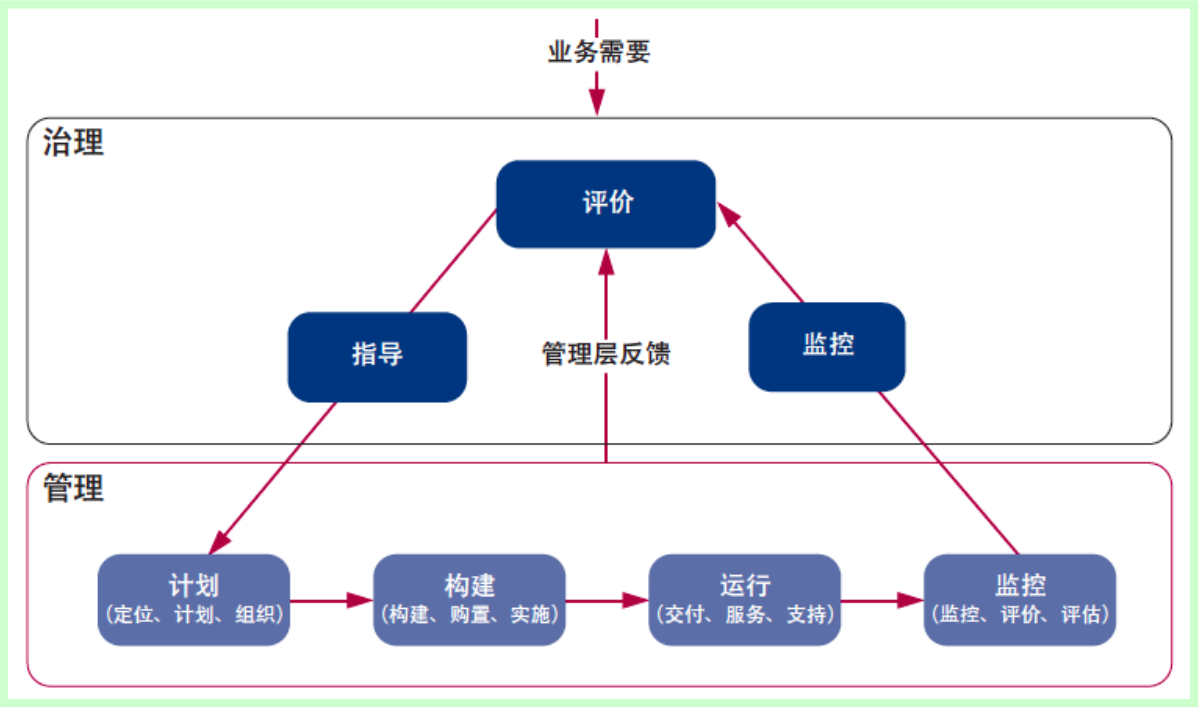

第一道防线
第二道防线
第三道防线
网络安全风险
① 信息系统失效
② 商业秘密泄露
③ 利用信息系统舞弊
④ 网络攻击和渗透
……
业务层面
风险管理
审计
可控的网络安全
① 信息系统安全可用
② 商业秘密保护
③ 舞弊被持续监控
④ 阻止网络攻击和渗透
……

输入　　输出

企业：区别对待？

谁来保护小微企业信息安全！

治理？


业务需要
治理
评价
指导
管理层反馈
监控
管理
计划
(定位、计划、组织)
构建
(构建、购置、实施)
运行
(交付、服务、支持)
监控
(监控、评价、评估)

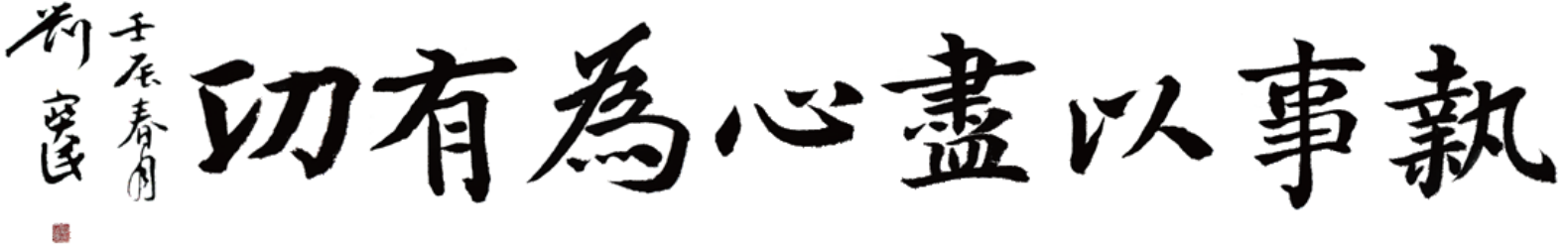
“君子务本”

企业信息安全要务什么“本”！

企业信息系统审计机制建设的探索者

Powertime
时代新威

王新杰，wangxinjie@powertime.cn，13701275907



Best Efforts in Everything We Do.