信息安全管理
先锋论坛

跟我学信息安全管理

03、信息安全管理实操-ISMS体系构建　程武阳

信息安全管理专家委员会发布
2016年6月

信息安全管理论坛（http://www.iso27001cn.com）成立于2014年9月，为国内目前最专业的信息安全管理学习和实践交流平台。是学习信息安全管理方法、分享实战经验、提升实践水平的好地方！

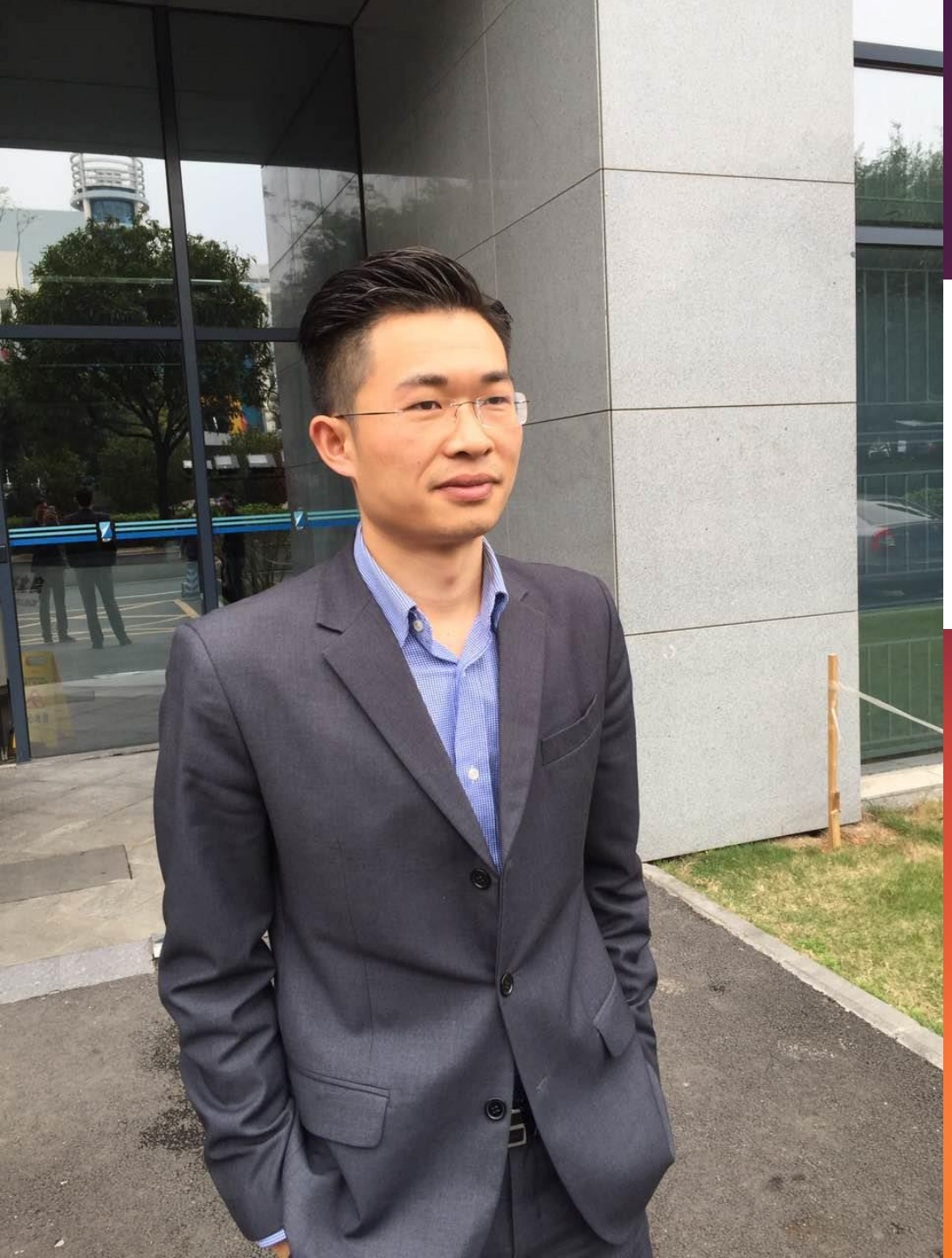
关于我们

我们提供

- 最全的信息安全管理资料
- 信安经理高薪工作机会推荐
- 每周专家讲堂（ 每周四晚上8点半YY频道89519382 ）
- 物美价廉的ISO27001课程团购

- 信息安全管理学习实践QQ群 207723402
- 微信 IT管理精英圈 itilxf_(记得有下划线)

欢迎关注



信息安全体系构建

CESI

Adam cheng（程武阳）

2016年6月

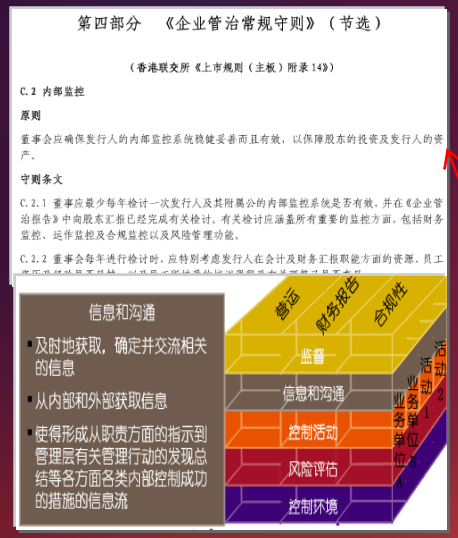
内容

1. 单位经营环境面临的信息安全风险
2. 单位信息安全现状分析
3. 单位信息安全体系模型及核心能力建设
   - 信息安全组织
   - 信息安全责任
   - 信息安全运营

1、法律法规遵从

近年来，单位通过制定战略，进一步清晰了未来五年发展规划，在打造核心能力的基础上，逐步建立差异化竞争优势和可持续发展的商业模式。随着战略落地、流程再造、核心系统建设和品牌建设，单位将不断提升综合竞争力，不断提升资产质量，提高风险管理水平，将借助单位集团的品牌和产业优势，坚持创新发展，建立专业专长，走差异化发展之路，为客户提供高品质服务，成为客户首选成长伙伴，成为一流特色企业。

单位法律法规遵从提出对信息安全的要求— 法律风险

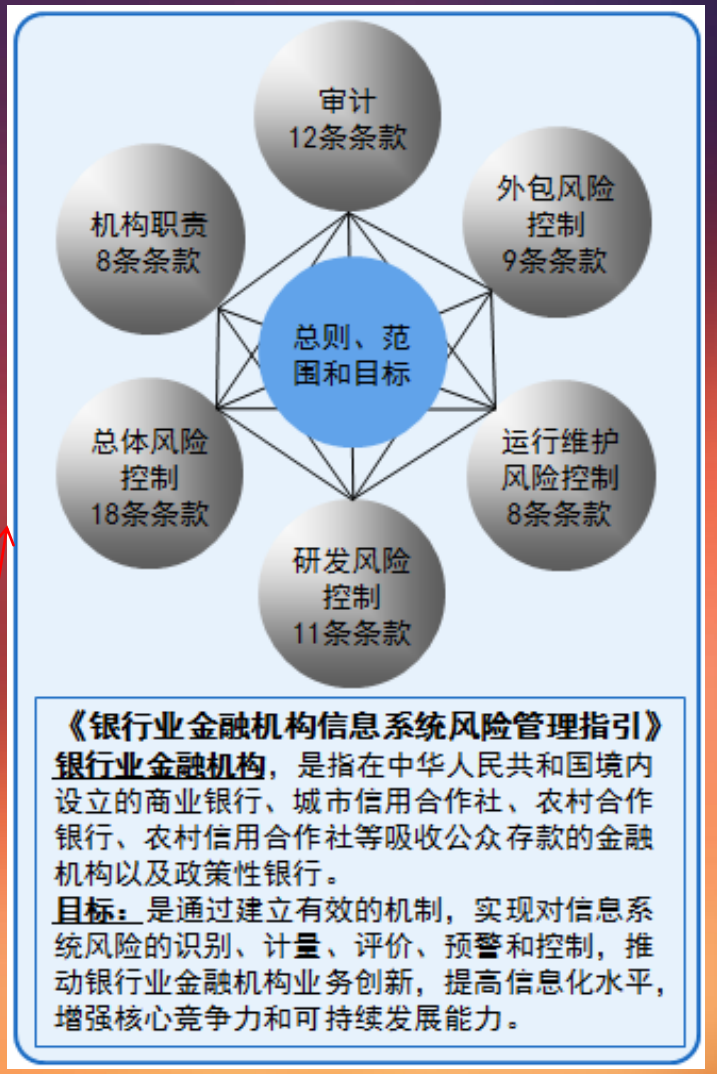


当前和未来单位银行可能遇到的安全合规举例：

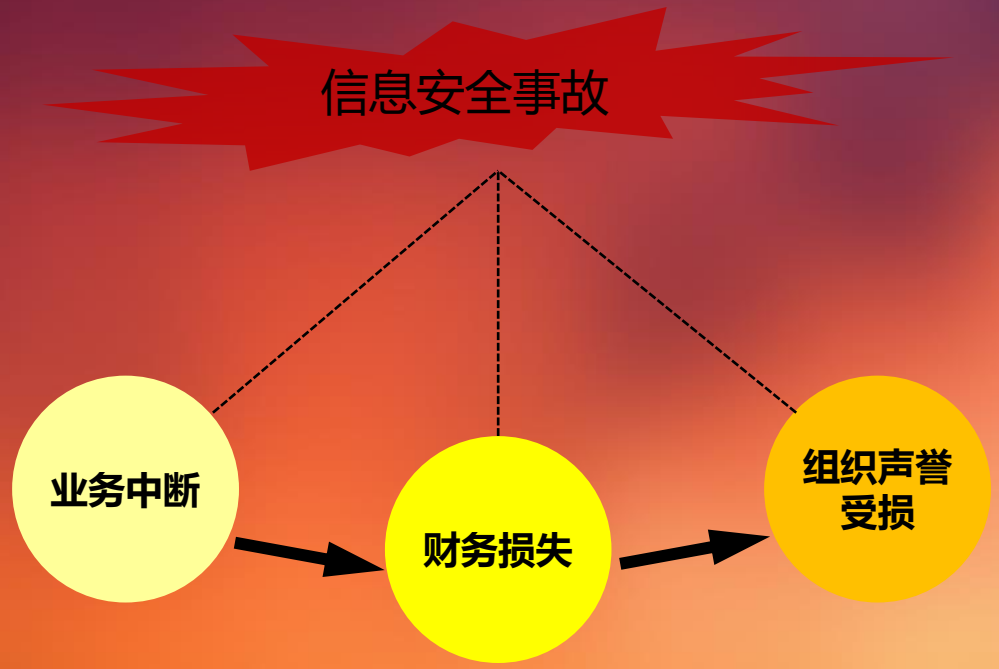
1.在国外上市的内控安全需求
- 美国SOX法案；
- 日本J-SOX法案；
- 香港上市公司内控与风险管理条例要求；
- 国际反虚假财务报告委员会下属的COSO委员会报告提出的内部控制框架

2.在国内上市
- 财政部内控法案（2009年7月1日开始实行）；
- 交易所内控规范；

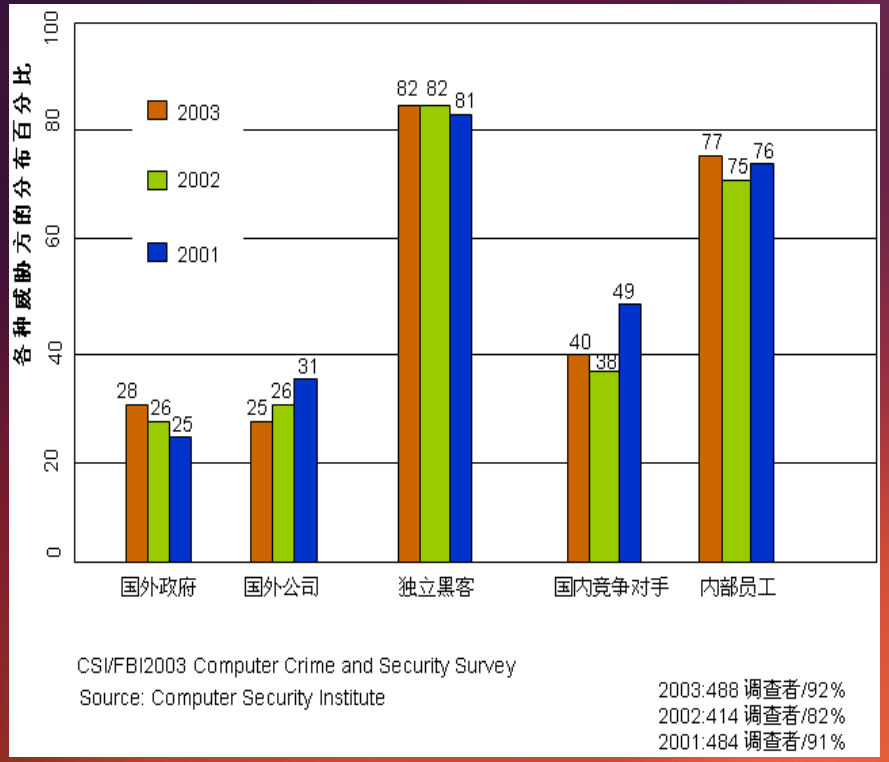
3.行业监管：
中央企业：国资委《中央企业全面风险管理指引》 ；
电信企业：工信部，通信管理局监管要求；
商业银行：银监会科技风险（313号文）；《银行业金融机构信息系统风险管理指引》
证券企业：证监会监管要求，行业协会（IT治理）；
4.公安部要求：等级保护，分级保护（要求国有企业开始定级）；
《信息安全技术、公共及商用服务信息系统个人信息保护指南》



2、业务运作的信息安全威胁



单位经营环境面临的信息安全威胁



- **独立黑客：**

  黑客攻击越来越频繁，直接影响企业正常的业务运作！

- **内部员工：**
  - 信息安全意识薄弱的员工误用、滥用等；
  - 越权访问，如：系统管理员，应用管理员越权访问数据；
  - 政治言论发表、非法站点的访问等；
  - 内部不稳定、情绪不满的员工。如：员工离职带走企业秘密，尤其是企业内部高层流动、集体流动等！

- **竞争对手：**

  法制环境不健全，行业不正当竞争（如：窃取机密，破坏企业的业务服务）！

- **国外政府或机构：**

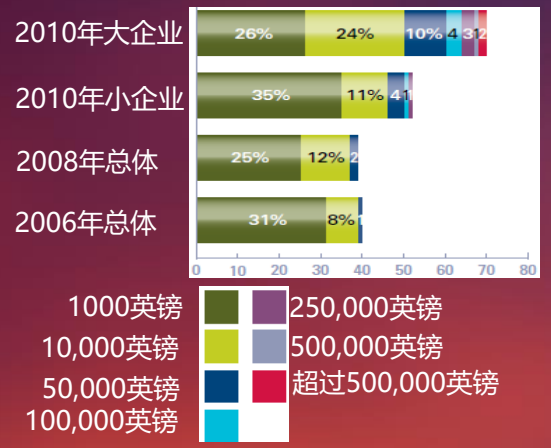
  法制环境不健全，行业不正当竞争（如：窃取机密，破坏企业的业务服务）！

信息安全事故影响分析— 业务风险、财务风险、市场风险

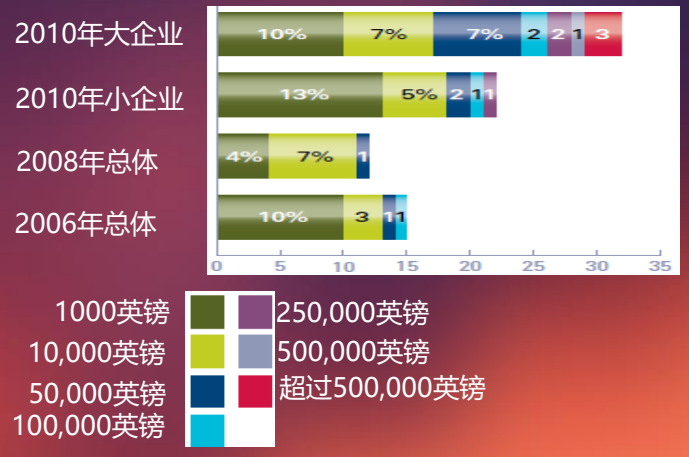
事件导致业务中断的程度

	没有	少于一天	一天到一周	一天到一月	超过一个月
非常严重中断					
中断					
小中断					
微小中断					

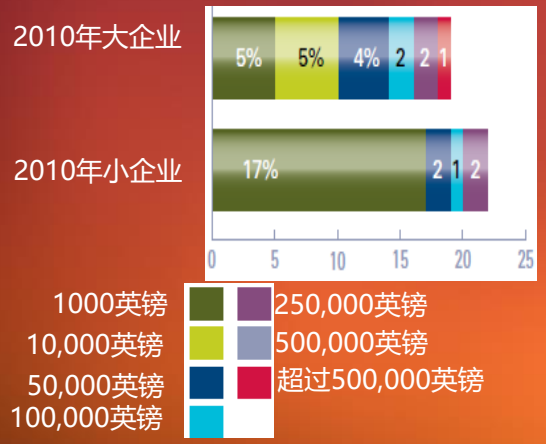
恢复事件花费的成本



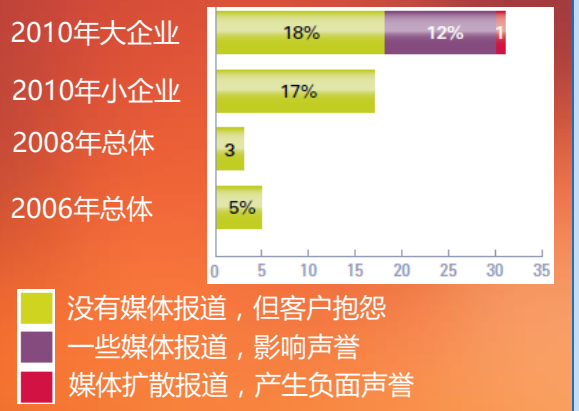
直接财务损失



间接财务损失



信息安全对企业声誉破坏

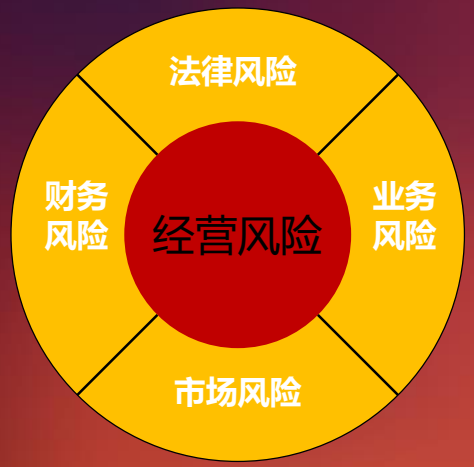


分析和结论：

•和2009年的情况相似，病毒和恶意软件是去年导致中断最主要原因，第二位的是系统失败和数据中断

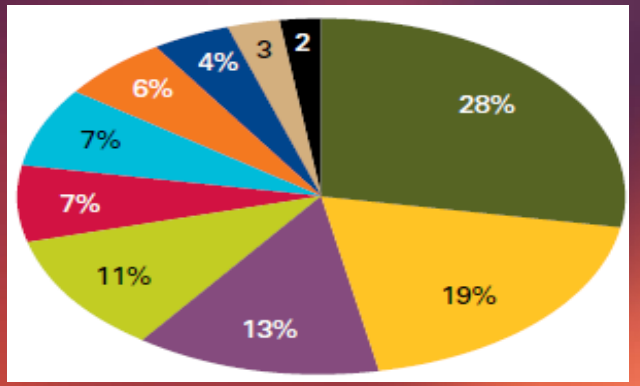
•大型企业业务中断平均是2-5天，平均每次中断恢复总成本是£200,000-£380,000，平均的直接财务损失是£25,000-£40,000，平均间接损失是£15,000-£20,000。被调查的最严重的间接损失高达£500,000。最大的损失是来自企业声誉的损失。尤其媒体对大型企业的安全事件非常关注，一旦发生事件，很容易被媒体进行宣传报道，造成恶劣的企业声誉影响，这是用财务成本无法估算的。

单位信息安全根本目标—对单位经营过程中面临的信息安全风险进行有效管控，保障单位经营业务的持续、可靠、正常运行，是单位信息安全的根本目标



业务风险管控

全球2010年信息安全主要业务驱动因素



1、保护客户信息
2、防止停机情况
3、法律和规则遵从
4、保护组织声誉
5、维护数据完整性
6、灾难中业务持续运行
7、保护知识产权
8、促进业务机会
9、提高效率/减少成本
10、保护其他资产不被偷窃

内容

1. 单位经营环境面临的信息安全风险
2. **单位信息安全现状分析**
3. 单位信息安全体系模型及核心能力建设
   - 信息安全组织
   - 信息安全责任
   - 信息安全运营

单位信息安全体系现状概述

基于国际信息安全体系最佳实践进行分析评估

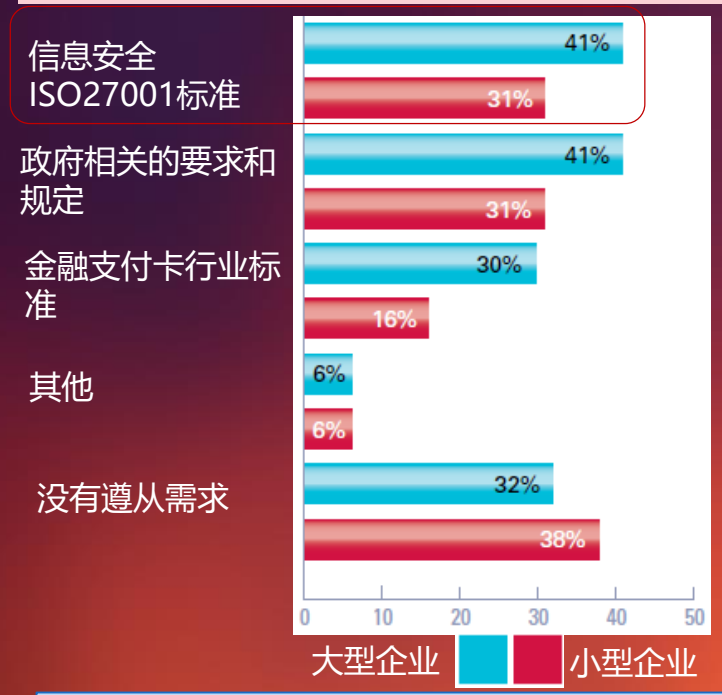
经过多年的建设，单位先后部署实施了多种安全产品，并配套建设了ISO27000安全体系，基本达到了控制重大**资产层面风险**的目标。

单位信息安全评估参照标杆—— 国际主流信息安全管理模式趋势

目前四种信息安全管理模式：

单位信息安全评估参照标杆—— ISO27001是信息安全标准方面企业遵从的主流标准

企业需要遵从哪些信息安全标准



企业控制外部服务商安全采取的行为

分析和结论：

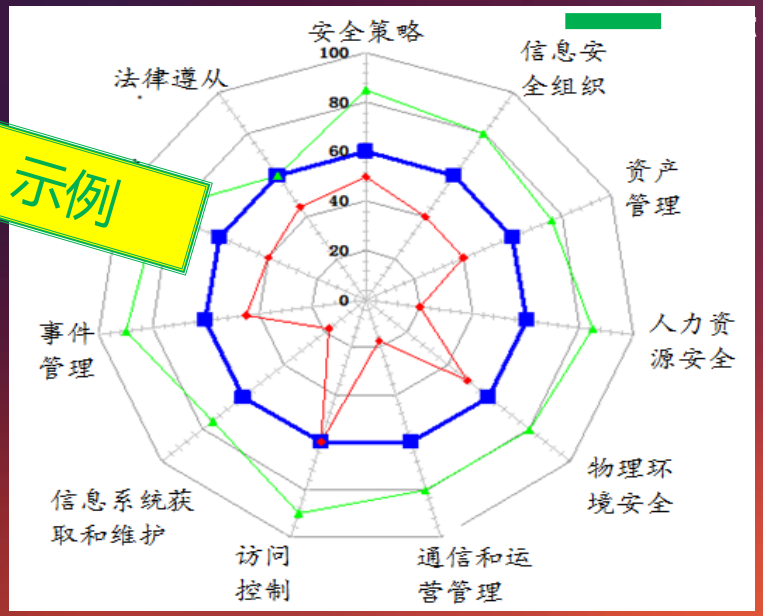
ISO27001已经成为信息安全标准方面企业遵从的主流标准！目前ISO27001可以含盖很多法律遵从所提出的需求。在中国，而商业银行大量借鉴ISO27001来贯彻信息安全风险管控措施、提高其信息安全管理水平和并最终降低其业务风险。

单位银行作为众多大中型企业的资金中转站，其本身也可能面临其众多客户的信息安全考量。借鉴ISO27001和ITIL等主流标准，大力加强信息安全风险管控能力，势在必行。

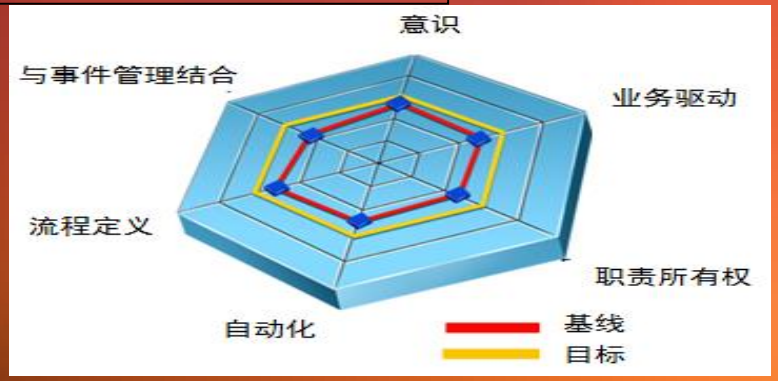
同时大多数银行企业甚至包括政府都采取了服务外包的方式，对于外包服务商的安全保障需求最近也非常重视，上图是大多数企业约束服务商安全方面的方法，单位银行可以借鉴上面的方式，对外包服务的信息安全进行管理和控制！

单位信息安全评估模型— 以ISO27001的十一个控制域成熟度雷达展现

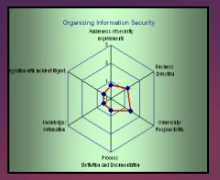
信息安全十一个域的成熟度



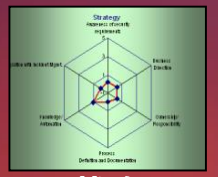
信息安全6个维度的成熟度




风险评估成熟度


组织信息安全

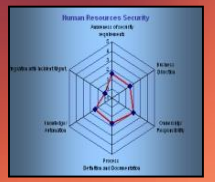

安全管理报告和度量

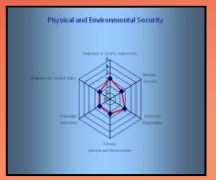

战略

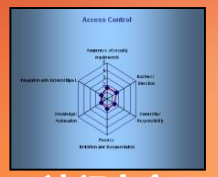

资产管理

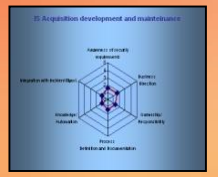

安全策略

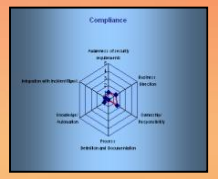

运营管理安全


人力资源安全


物理和环境安全


访问安全


开发和维护安全


法律遵从

内容

1. 单位经营环境面临的信息安全风险
2. 单位信息安全现状分析
3. **单位信息安全体系模型及核心能力建设**
   - 信息安全组织
   - 信息安全责任
   - 信息安全运营

单位信息安全体系建设总体思路

- 基于信息安全管理国际标准ISO27001，同时考虑国内的管理和法制环境
- 综合顾问的管理和技术经验，结合单位现有的信息安全管理措施
- 以单位信息安全现状为基础，充分考虑单位银行所存在的业务信息安全风险

单位信息安全体系模型—基于经营风险管控的信息安全体系

最佳实践

参照国内外信息安全管理最佳实践

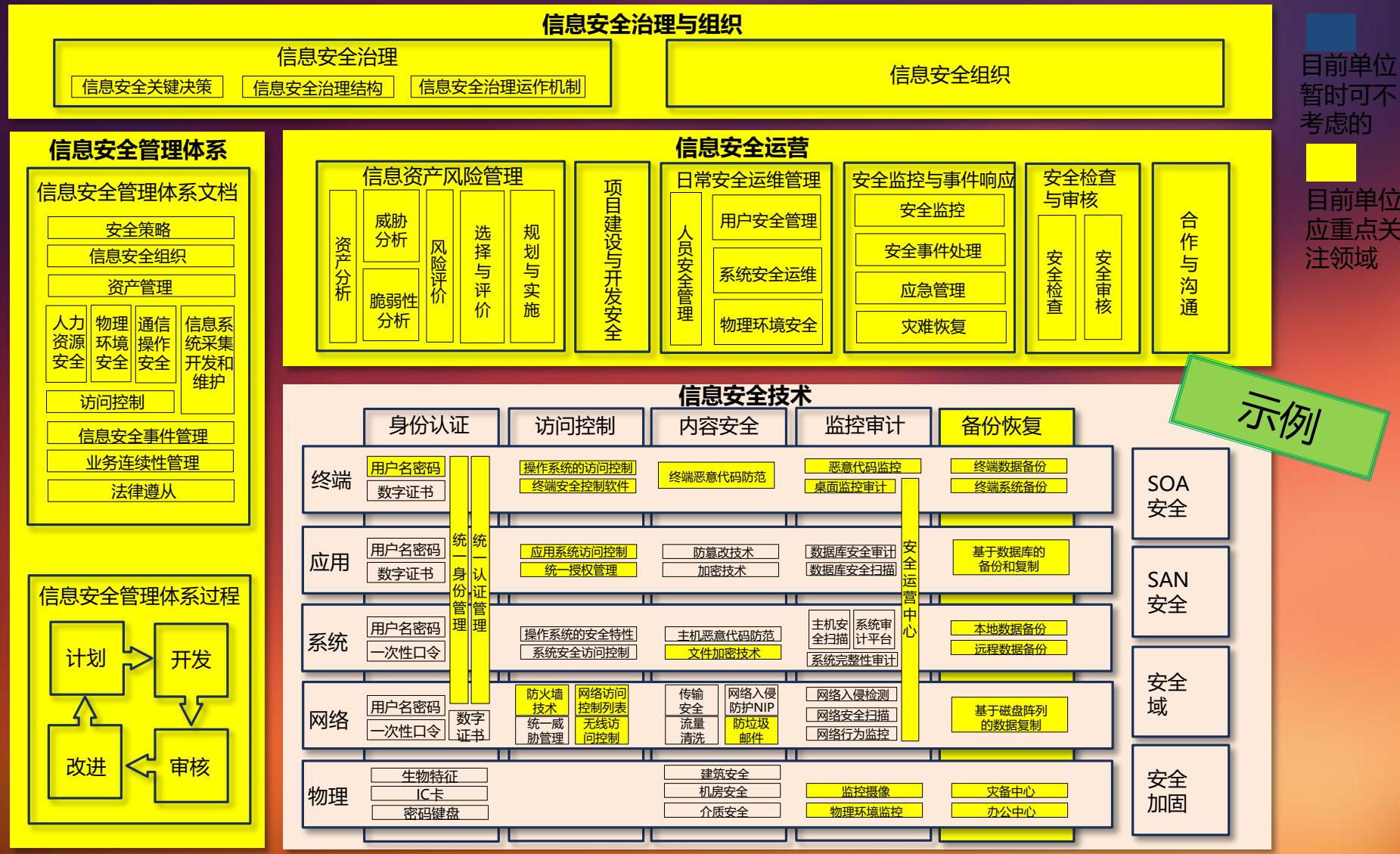
信息安全体系

四个相互联系的构成要素

经营风险

以单位经营风险管控为目标

单位信息安全体系蓝图—结合等级保护和ISO27001管理体系进行考虑，全面的信息安全蓝图



单位信息安全下一步提升重点— 升级信息安全体系，营造安全的信息环境，保障经营业务持续、有效运行，助力差异化特色银行新跨越战略的达成。

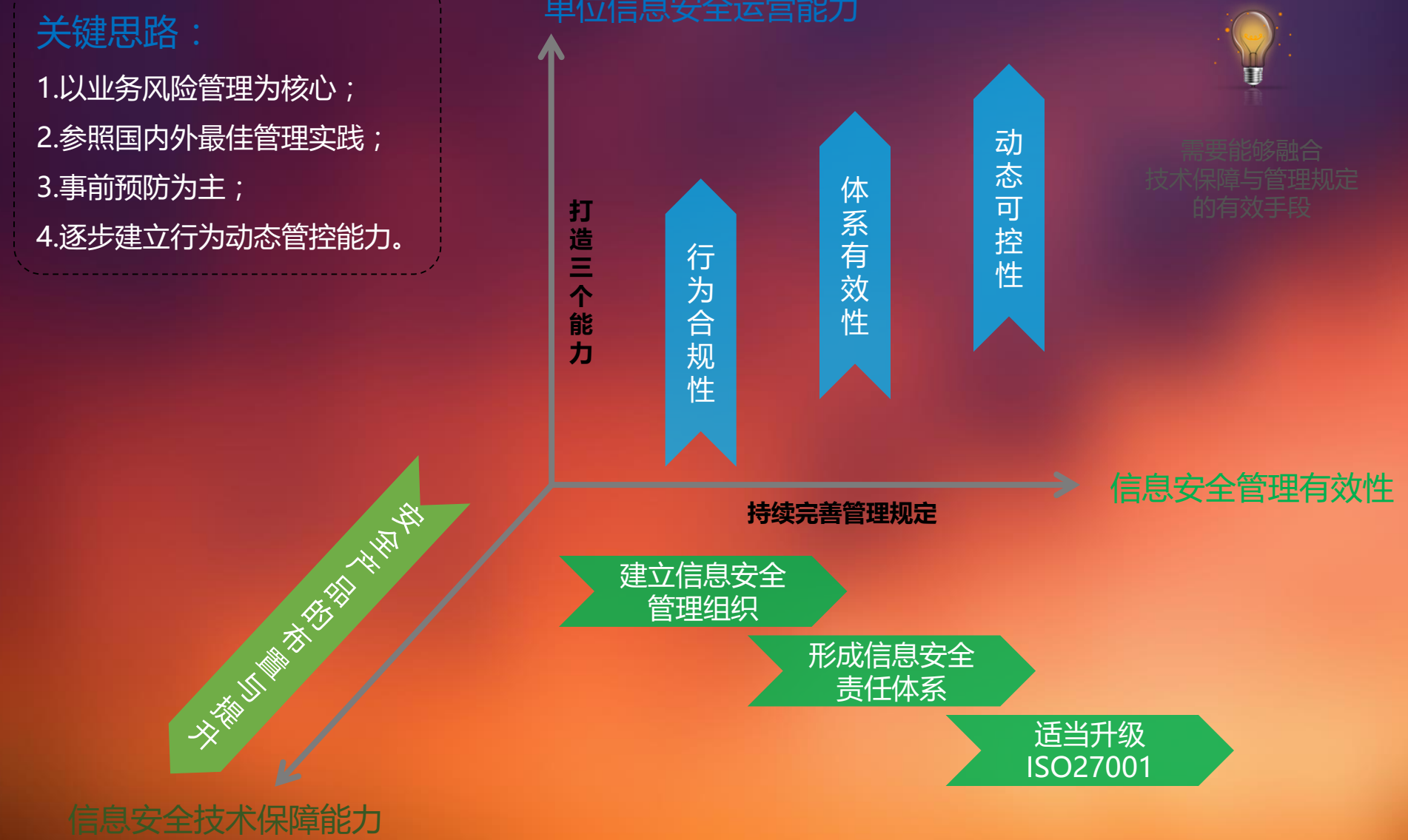
关键思路：

1.以业务风险管理为核心；

2.参照国内外最佳管理实践；

3.事前预防为主；

4.逐步建立行为动态管控能力。



内容

1. 单位经营环境面临的信息安全风险
2. 单位信息安全现状分析
3. **单位信息安全体系模型及核心能力建设**
   - **信息安全组织**
   - 信息安全责任
   - 信息安全运营

核心能力建设— 单位信息安全管理组织建设

国际主流管理模式

风险导向（主动）

- 信息安全由CSO直接负责
- 首先建立和优化信息安全体系
- 由业务和IT共管
- 有与风险平衡的安全预算
- 基于风险而整合的基础设施
- 使用主动性安全技术

最佳实践

ISO27001

信息安全方针
信息安全组织
资产管理
人力资源安全
物理和环境安全
通讯和运营管理
信息系统获得、开发和维护
信息安全事件管理
业务连续性管理
法律法规遵从

商业银行信息科技风险管理指引

设立一个由来自高级管理层、信息科技部门和主要业务部门的代表组成的专门信息科技管理委员会，负责监督各项职责的落实，定期向董事会和高级管理层汇报信息科技战略规划的执行、信息科技预算和实际支出、信息科技的整体状况。

确保银行所有员工充分理解和遵守经其批准的信息科技风险管理制度和流程，并安排相关培训。 ■

单位信息安全管理组织

落实IT、风险管理部门和各级业务信息安全管理责任制，督导、检查各业务单元的信息安全管理工作。

核心能力建设一 单位信息安全管理组织建设，业务与IT共管的信息安全组织

参照标杆银行的信息安全组织体系，形成符合单位业务实际并能贯彻到基层的多层次信息安全组织责任体系，为有效落实行为合规、体系有效、资产安全提供了组织保障。

示例

单位银行信息安全委会

主任：副行长
成员：副行长、各业务单元、企管、风险管理、人力、信息部负责人
责任：负责整个银行信息安全的领导和决策工作

单位银行信息安全委员会秘书处

成员：信息部安全组、各功能部门、各业务单元信息部经理
责任： 负责单位银行的信息安全工作的协调，保障单位信息安全组织体系的日常运转。

各支行信息安全管理委员会

主任：支行主管领导
成员：支行信息安全负责人、支行各业务部门信息安全责任人
责任：负责在本支行推动、落实集单位银行的信息安全工作

总行各功能部门信息安全专员

成员：各功能部门信息安全负责人
责任：负责在本功能推动安全制度落实、安全培训、安全系统建设等工作。

核心文件

1.单位银行信息安全管理组织结构和人员责任管理办法
2.单位银行责任矩阵……

配套附件

1.单位银行人员信息安全职责说明
2.****年度单位银行信息安全指标
3……

内容

1. 单位经营环境面临的信息安全风险
2. 单位信息安全现状分析
3. **单位信息安全体系模型及核心能力建设**
   - 信息安全组织
   - **信息安全责任**
   - 信息安全运营

核心能力建设— 单位信息安全责任体系建设

1

业务目标

1、保护客户信息
2、防止停机情况
3、法律和规则遵从
4、保护组织声誉
5、维护数据完整性
6、灾难中业务持续运行
7、保护知识产权
8、促进业务机会
9、提高效率/减少成本
10、保护其他资产不被偷窃

参照

2

最佳实践

ISO27001

1. 信息安全方针
2. 信息安全组织
3. 资产管理
4. 人力资源安全
5. 物理和环境安全
6. 访问控制
7. 通讯和运营管理
8. 信息系统获得、开发和维护
9. 信息安全事件管理
10. 业务连续性管理
11. 法律法规遵从

责任分解

3

业务目标	风控	内容及指标	责任主体	支持主体

形成责任制度文件

4

单位信息安全责任制度文件

单位信息安全责任体系建设— 责任矩阵说明

1.由业务目标进行分解

3.风险管控手段

5.支持部门应该承担的责任

序号	业务目标	风控点	内容及指标	责任主体	支持主体
1	保护客户信息	人员泄密风险	关键岗位人员背景调查	HR必须对关键岗位人员进行入职前背景调查	用人部门应该配合HR并主动提供相关信息。
			签署关键岗位保密协议	HR必须与关键岗位员工签署保密协议	用人部门提供必要的支持。
			培训员工的安全意识	全体员工必须积极参与集团组织的信息安全意识培训，提高安全意识	信息部门负责组织信息安全意识培训相关课程。
			管理员工行为	业务部门管理者必须行使管理职责，确保员工行为满足集团的信息安全政策	信息部负责提供相关技术支持手段，动态监控员工行为。
			员工离职控制	业务部门管理者必须执行员工离职流程控制，如：工作交接、归还资产、废除各类系统设施的访问权限等	离职流程涉及到的管理部门提供本环节的控制支持。
		业务系统的不当使用，可能造成客户信息泄露	业务系统授权合规	业务部门管理者负责根据员工的工作职责、涉及业务对业务系统授权进行审批	信息部负责提供业务系统授权审批机制，并定期为业务部门管理者提供业务系统授权清单，核对授权合规性。
			业务系统口令安全	全体员工必须保证口令的安全（如：设置强口令，定期更新口令等），避免口令丢失、盗用，从而造成业务系统的信息泄密	信息部负责提供相关技术支持手段，保障业务系统口令安全。
			业务系统使用合规	全体员工不能使用他人账号访问信息系统	
		存储设施泄密风险	客户信息分类	业务部门管理者负责对客户信息进行分类，明确保密要求	
			物理介质（如：纸质文件）保护	全体员工负责对各类存储了客户信息的物理介质（如：纸质文件）进行妥善保护，避免丢失、损坏或泄密	
			电子文档保护	全体员工必须使用集团统一的文档加密软件对客户信息文件进行加密处理	信息部负责提供并维护文档加密系统。
			安全销毁存储客户信息的介质	全体员工必须按要求安全销毁存储了客户信息的介质	信息部提供技术支持或提供必要的销毁手段。

示例

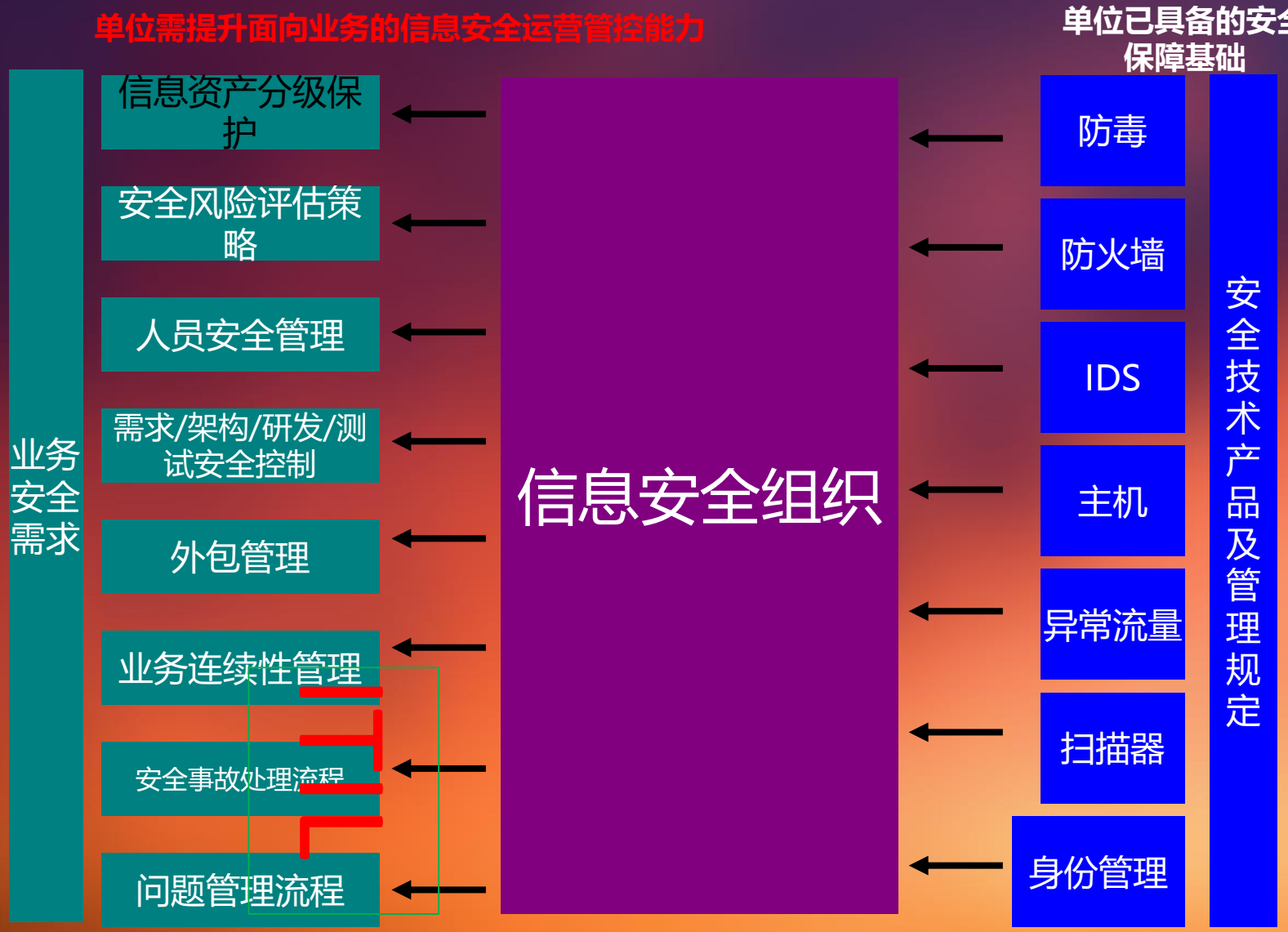
2.识别业务风险控制点

4.各业务部门应该承担的责任

内容

1. 单位经营环境面临的信息安全风险
2. 单位信息安全现状分析
3. **单位信息安全体系模型及核心能力建设**
   - 信息安全组织
   - 信息安全责任
   - **信息安全运营**

核心能力建设—安全运营管控能力体系



Thank you

宽恕

信息安全管理先锋论坛

特别鸣谢

北宙咨询 North Universe

Trendsetting Consulting

艾拓咨询 AituoXianfeng Consulting

特别鸣谢