



# 企业信息安全体系建设 交流讨论材料

2014年6月19日

马文杰

## **第一部分 企业面临的信息安全环境**

---

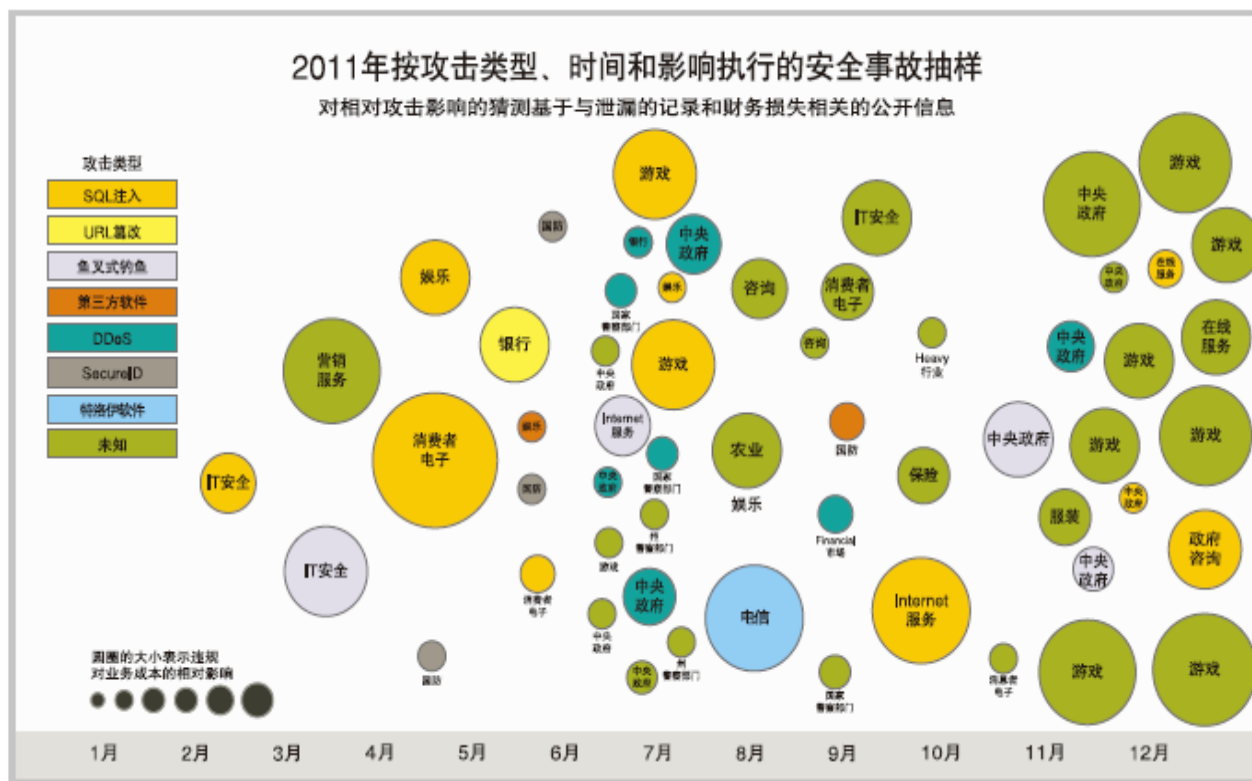
## **第二部分 企业信息安全的体系架构**

## **第三部分 企业信息安全体系的建设**

## **第四部分 企业信息安全管理实践**

# 超级互联的商业世界与极其复杂的IT环境

- **超级互联的商业世界**：激增的数字业务信息存储在消费者和企业所使用的虚拟云和社交平台、仪器、移动设备中，且可供访问。这就创造了一个极其复杂的 IT 环境——可能的攻击点几乎是无限的
- **高级持续性的安全威胁**：最有经验的对手现在正带来高级持续性威胁，他们通过密切的关注的不懈不懈来获取敏感业务信息的访问权限。这些攻击利用尖端的方法，可持续无限长的时间且具有专门的目标
- **传统IT防御的有效性**：如今，愈加多样的威胁侵蚀着传统 IT 防御（比如防火墙和防病毒软件）的有效性，甚至在许多情况下完全避开了这些控制
- **企业面临的安全挑战**：所有企业都迫切希望找到信任、透明度和隐私之间的绝佳平衡。企业实现这种更具挑战性的平衡而面临的三大压力：
  - 攻击面扩大
  - 攻击模式扩散且手法熟练
  - 威胁和解决方案异常复杂

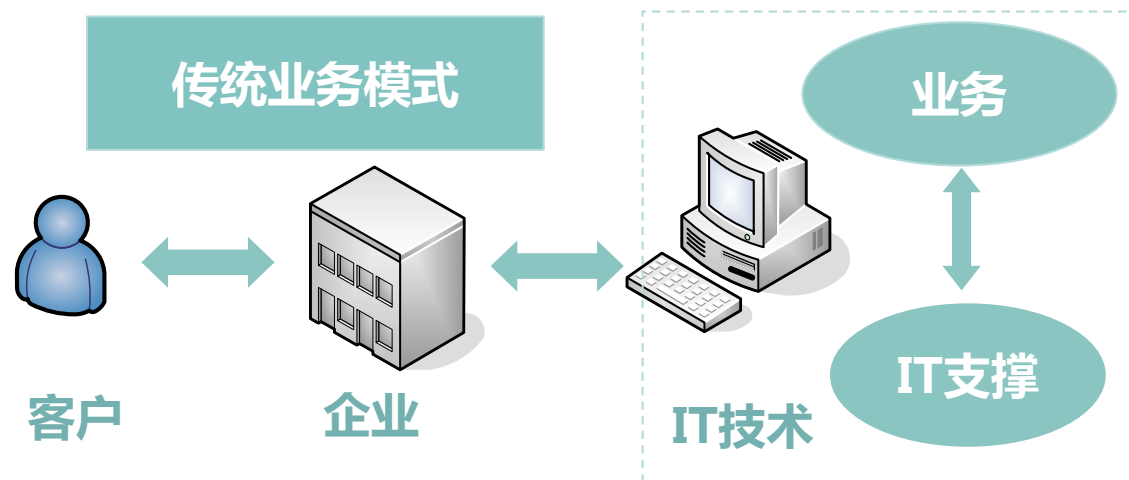


\* 根据思科2014年安全报告，IBM安全报告

# 业务模式的变革增加了企业信息安全压力

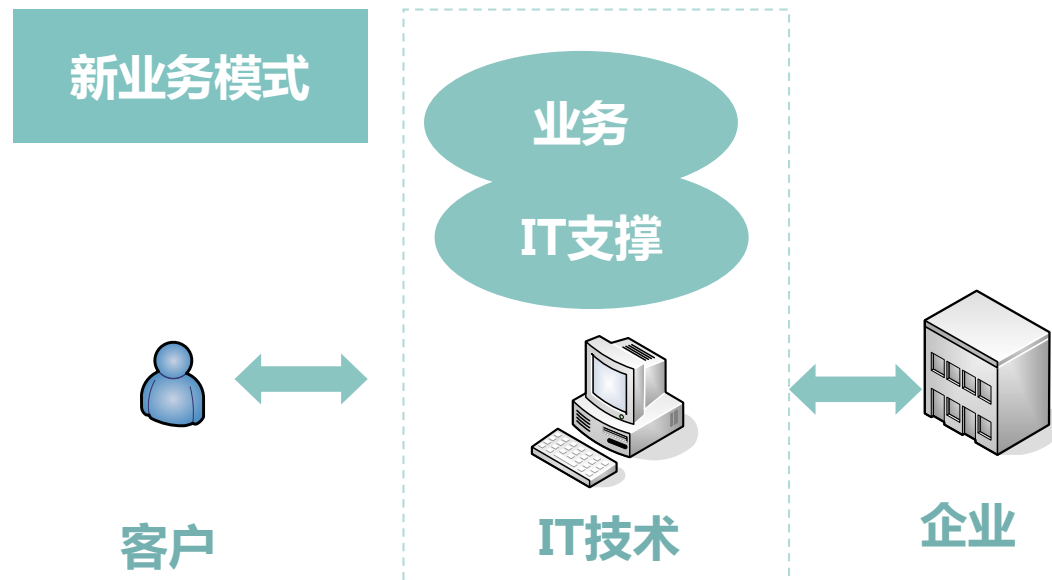
## 传统的企业运作模式

- ❖ 信息安全仅作为后台数据的保障
- ❖ 基本与业务无关的信息安全需求



## 新的企业运作模式

- ❖ 因客户和IT直接连线导致IT 和业务流程的汇合
- ❖ 安全不是单独的解决方案



## 新的安全考虑

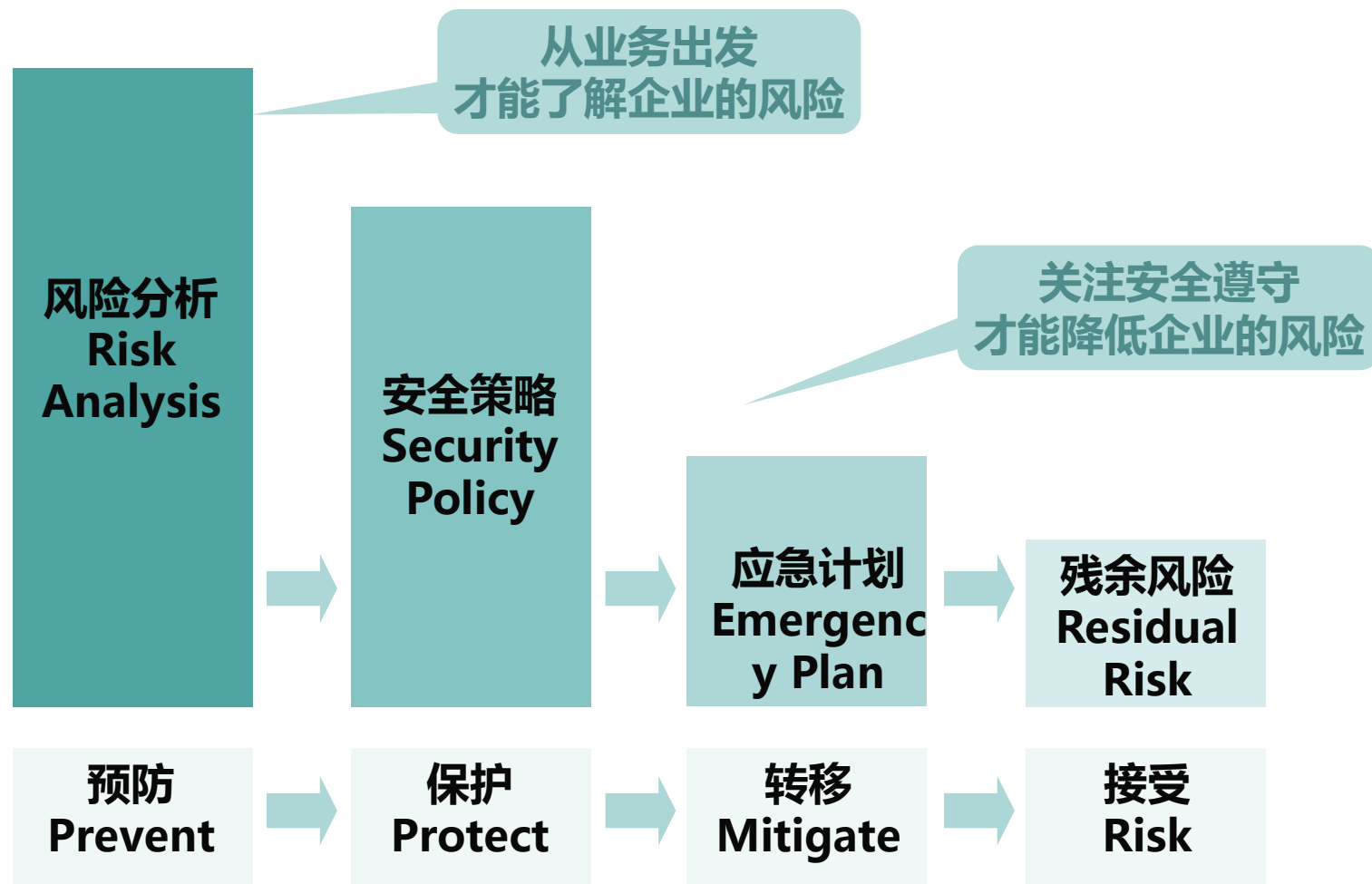
- ❖ 安全是一个企业整体需求
- ❖ 风险评估和企业连续战略都是今天董事会上讨论的话题
- ❖ 企业对受过安全培训的人员需求越来越高

# 企业的信息安全需求与风险管理视角

企业的信息安全需求来自以下方面：

- 法律法规与合同条约的要求
- 组织原则目标和规定
- 风险评估的结果

风险评估是信息安全管理的基础



**第一部分 企业面临的信息安全环境**

**第二部分 企业信息安全的基本框架**

---

**第三部分 企业信息安全体系的建设**

**第四部分 企业信息安全新领域挑战**

# 企业信息安全框架的基本层面

- **视角**：企业信息安全需要从全方位的视角去管理，而不是通过单一系统或程序来实现
- **框架**：合适的信息安全框架有利于指导安全体系的建设
- **层次**：从体系框架的角度，分为三层：
  - 安全治理、风险管理与合规
  - 安全运维
  - 基础安全服务与架构





# 安全治理、风险管理与合规

- 安全治理、风险管理与合规是企业安全框架的最顶层，是业务驱动安全的出发点
- 通过对企业业务和运营风险的评估，确定其战略和治理框架，风险管理框架，定义合规和策略遵从，确立信息安全文档管理体系
- 信息安全治理不同于信息安全管理，是在宏观层面的战略角度上，对信息安全战略上的过程、结构与联系进行梳理与监控，以确保组织信息系统的安全运营管理能够沿着正确方向演进

## 战略与治理框架

- 为组织的信息安全定义战略框架
- 指明具体安全管理工作的目标和职责范围
- 安全意识培养 – 宣传教育

## 风险管理

- 对象确立
- 风险评估
- 风险处理
- 审核批准
- 监控审查
- 沟通咨询

## 合规与策略遵从

- 加强对规范策略了解
- 确立企业需要合规的具体内容和实现方式
- 合规性建设，从管理与技术面落实规范与策略要求
- 合规性审计，提供综合性评述



# 相关标准规范：ISO27002与ISMS信息安全管理体系

ISO27002是一个完整的信息安全控制模型，包含了11个主题，可以为企业带来：

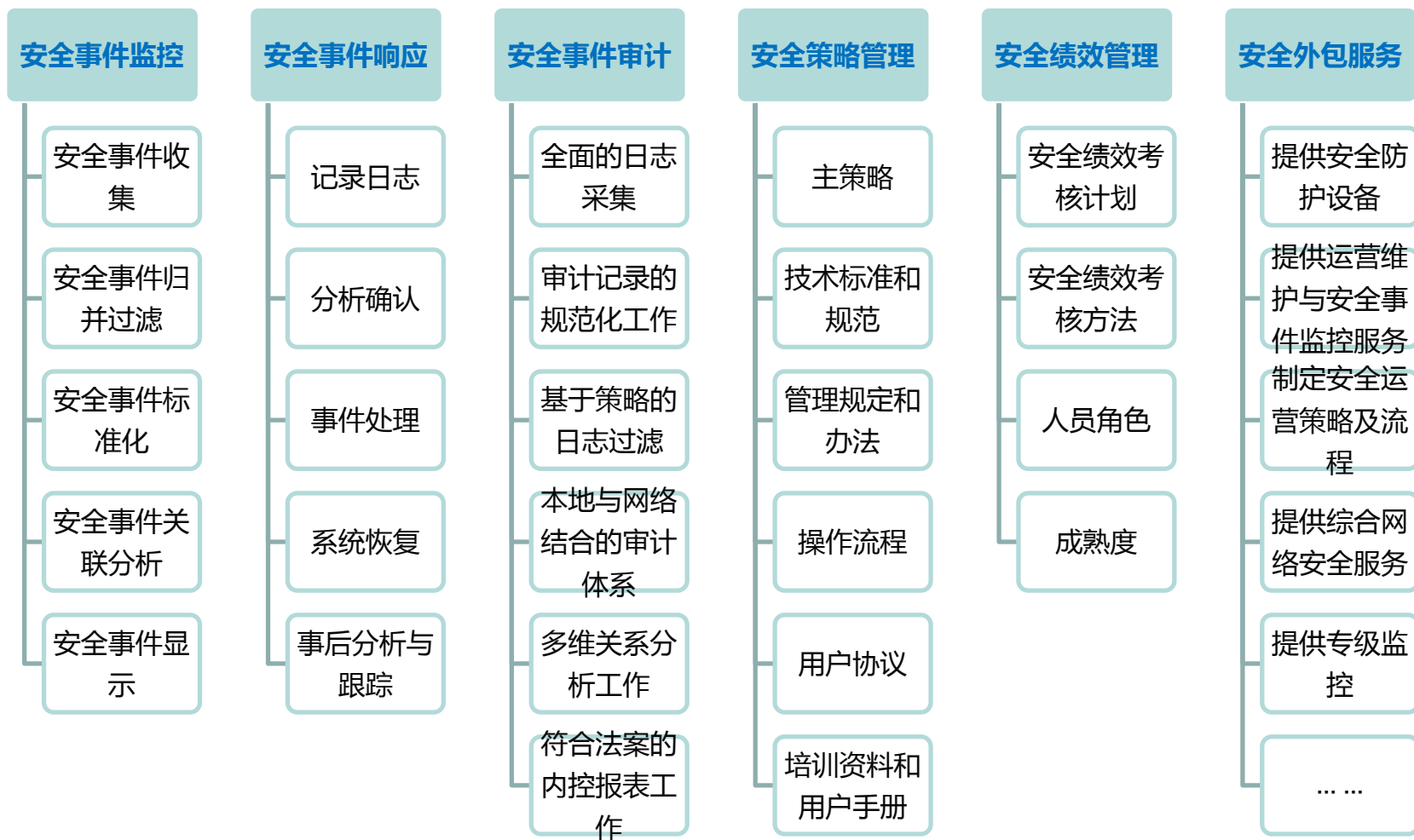
- 受业界广泛认同的方法论
- 按业界最佳实践方针开展信息安全评估、实施、维护和管理
- 为定义策略、标准、流程提供框架指南



ISMS信息安全管理体系框架

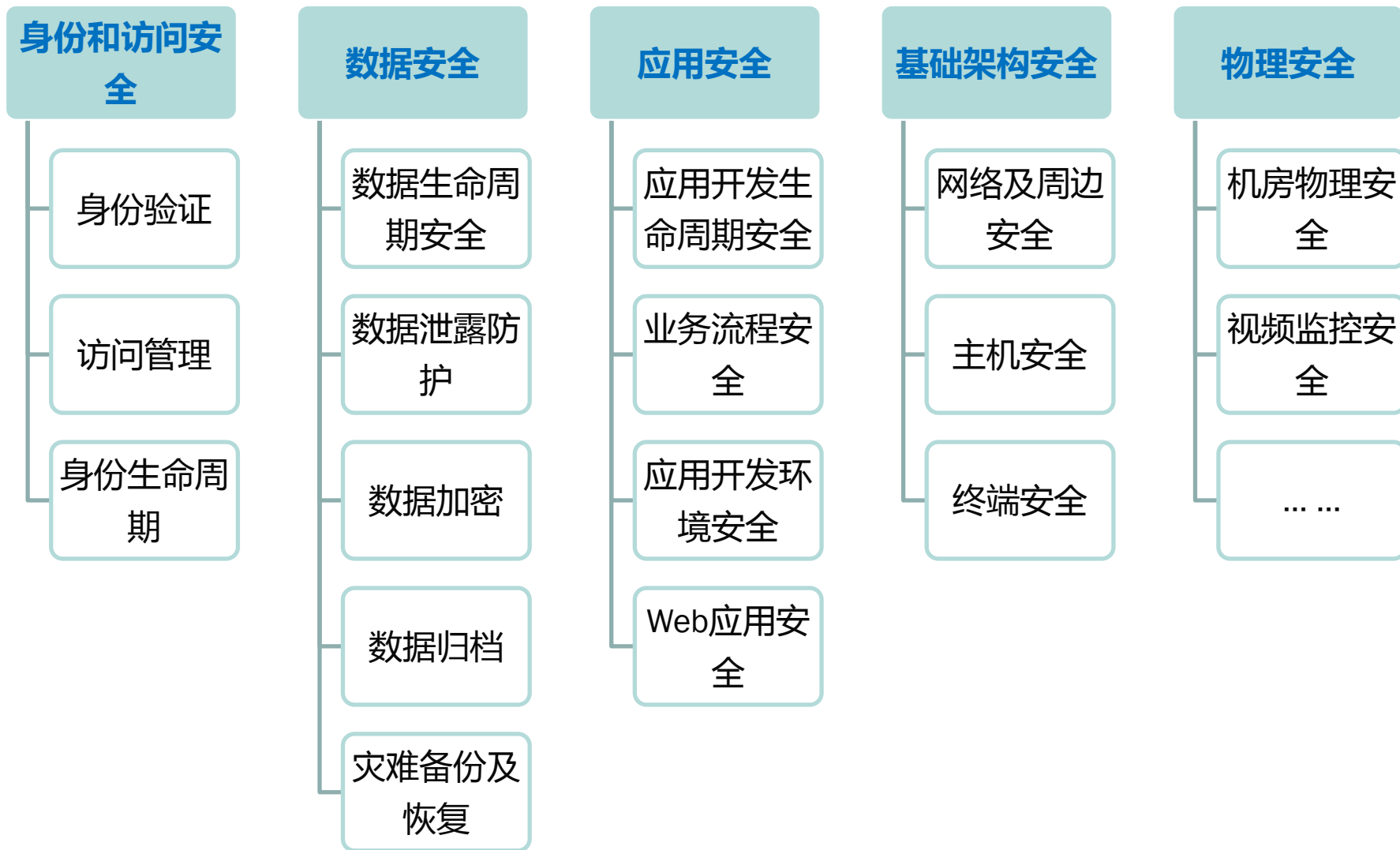
# 信息安全运维

- 安全运维是指在安全策略的指导下，安全组织利用安全技术来达成安全保护的过程
- 安全运维与IT运维相辅相成、互为依托、共享信息和资源
- 安全运维与安全组织紧密联系，融合在业务管理和IT管理体系中



# 基础安全服务与架构

- 基础安全服务与架构定义了企业信息安全框架中的五个核心的基础技术架构和相关服务
- 基础安全服务于架构是安全运维和管理的对象，其功能由各自的子系统提供保证



# 目录

---

**第一部分 企业面临的信息安全环境**

**第二部分 企业信息安全的基本框架**

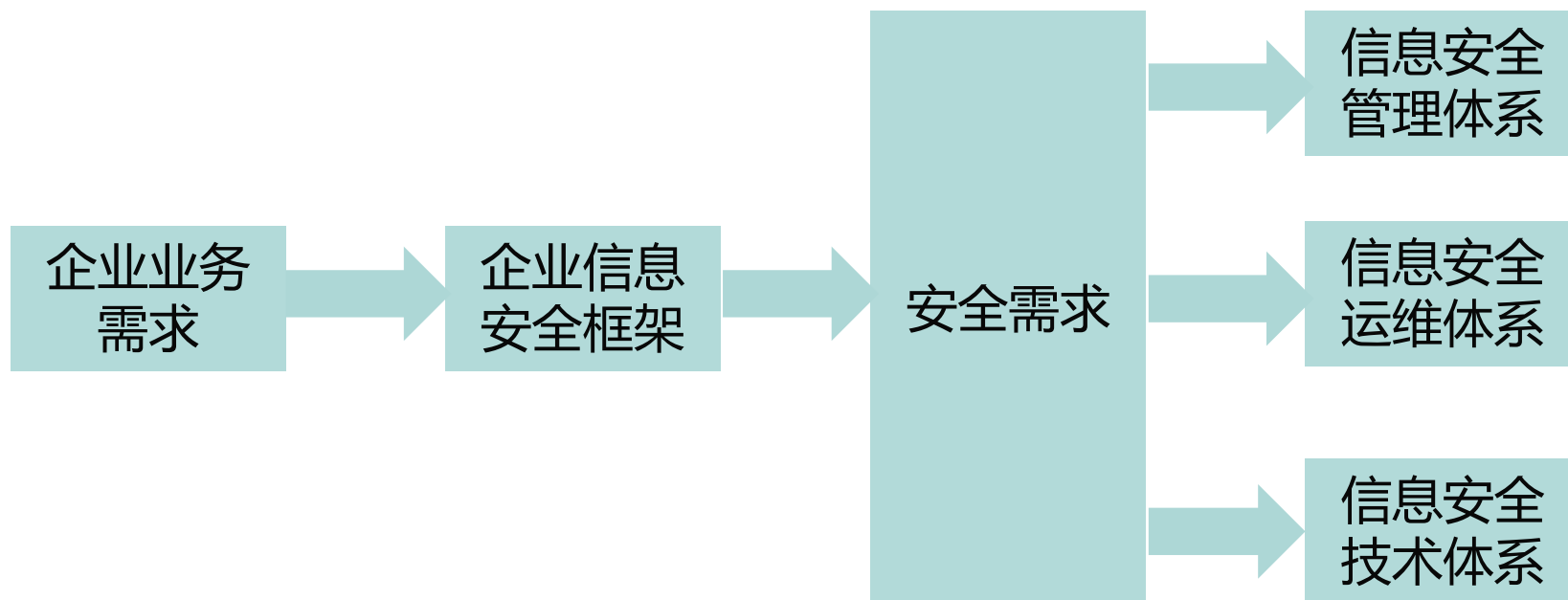
**第三部分 企业信息安全体系的建设**

---

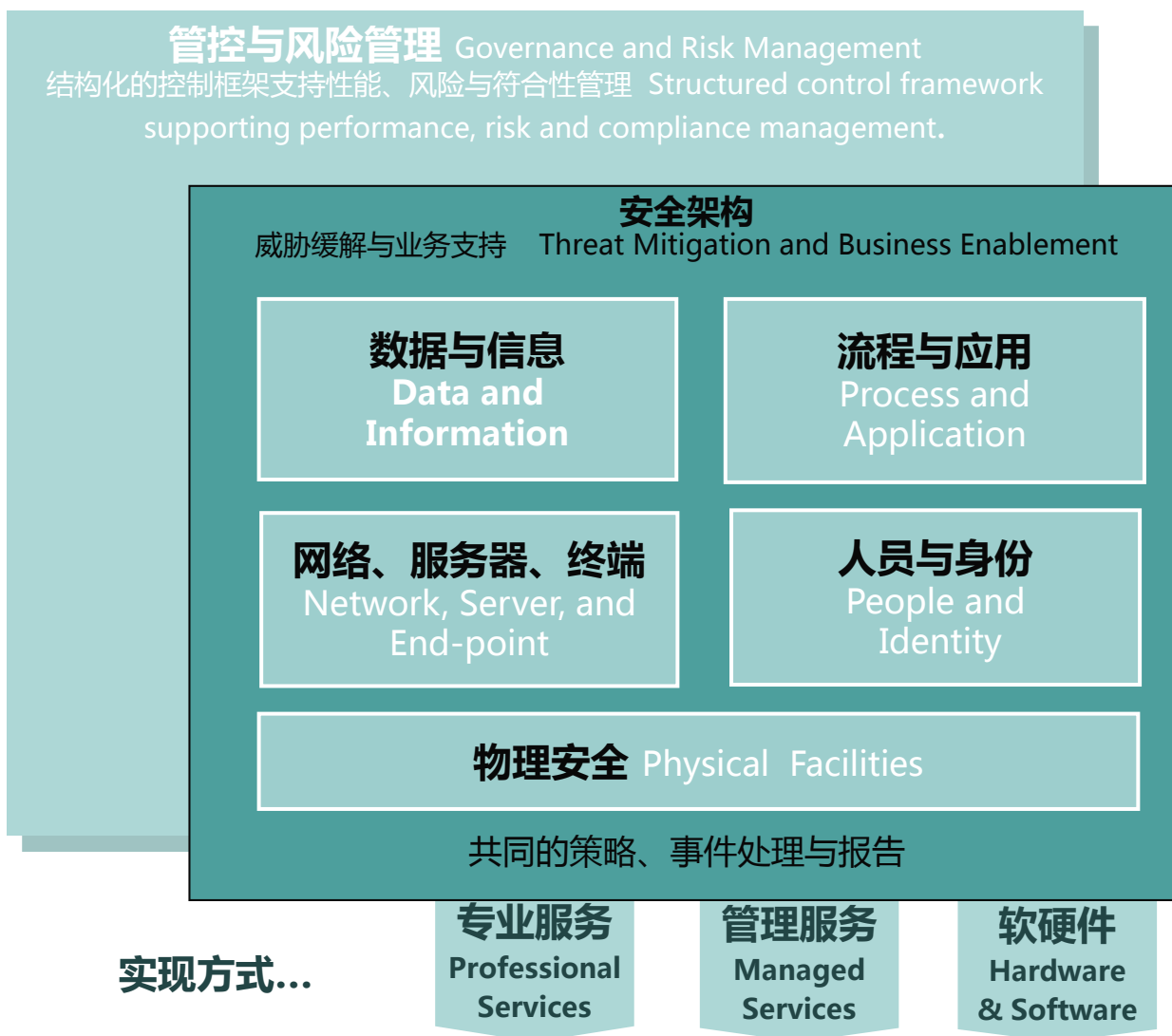
**第四部分 企业信息安全新领域挑战**

# 企业信息安全体系总体建设方法

- 企业信息安全框架参考和吸取了行业经验与实践，可作为建设的参照
- 从企业需求出发，参照企业信息安全框架，通过评估和风险分析等方法，定义企业安全需求
- 根据企业安全需求，定义企业信息安全建设的内容与方向



# 企业参照安全框架模型来帮助信息安全体系的建立



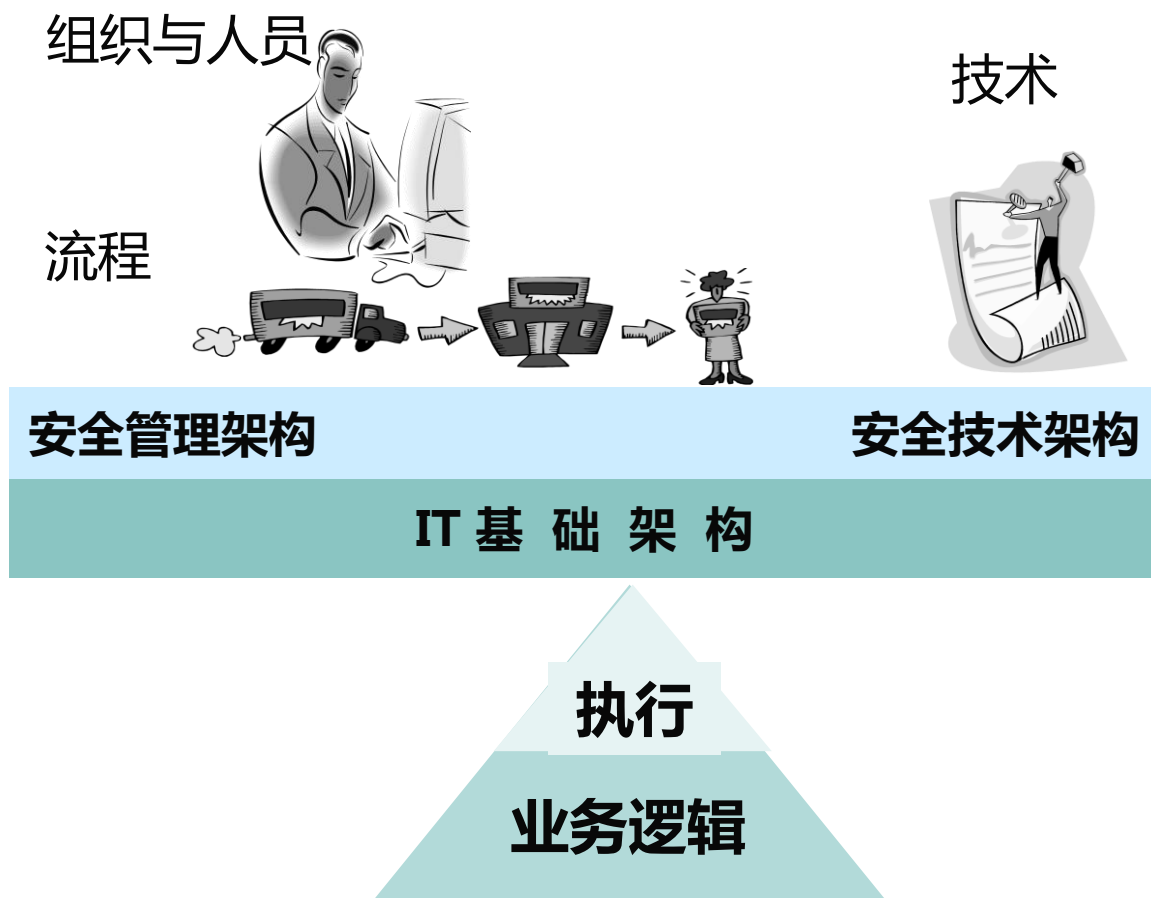
- **管理上**：管控与风险管理是安全的基础，它包括策略定义、遵从与合规、以及与审计相关的活动

- **技术上**：威胁缓解与业务支持包括5大类安全功能，构成了安全技术架构

- **安全管理与技术**：通过专业服务、管理服务、软硬件部署三种形式来提供

# 企业信息安全体系建设是人员、流程与技术的整合

越来越多的企业认识到：必须整合企业组织与人员、管理体系与流程、技术手段三方面因素，设计一致完整的安全架构、并持续实施才能获得理想的安全管控效果



## 若干误区：

- 网络安全和信息安全概念的混淆
- 重视技术，轻视管理
- 重视产品功能，轻视人为因素
- 重视对外安全，轻视内部安全
- 静态不变观念
- 缺乏整体性信息安全体系的考虑

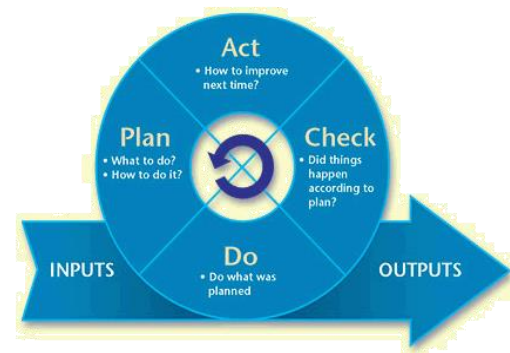
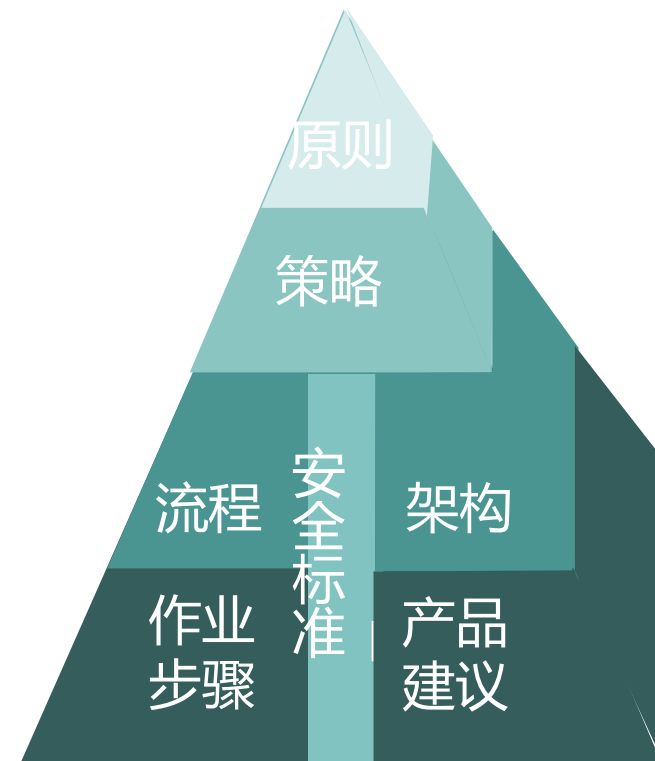


# 企业信息安全管理架构应包含的内容

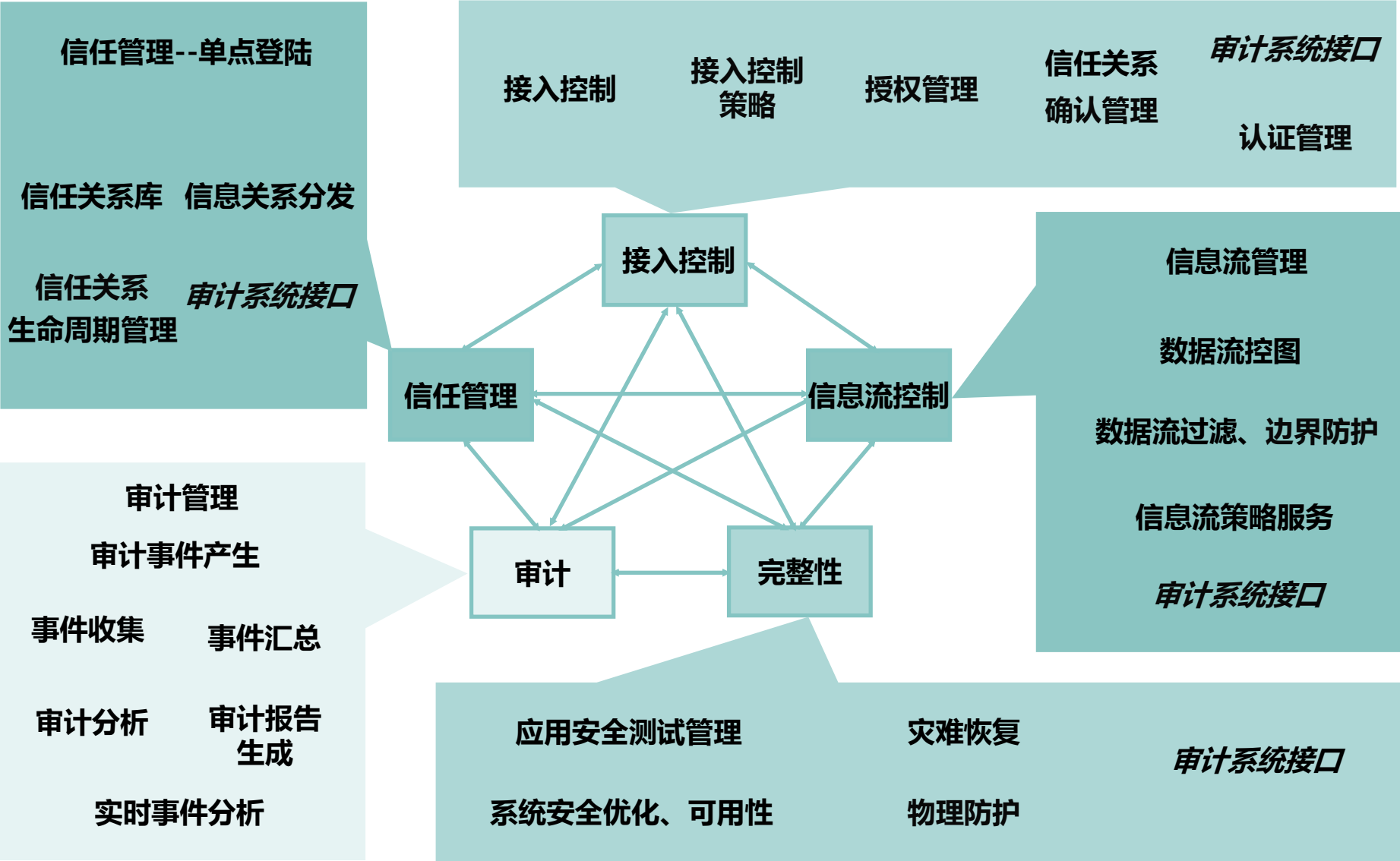
## ■ 企业信息安全金字塔描述了企业安全架构的构成

- 安全原则：描述信息安全的业务需求价值
- 安全政策：描述信息安全的目地、方向、愿景及责任
- 安全标准：信息安全实施规则，包括技术、方法及其它细节
- 安全流程：于跨单位实施政策标准的活动、工作及程序
- 安全步骤：描述个人在流程上的详细工作
- 安全架构：信息安全技术如何结合的细节
- 安全产品：信息安全解决方案所选的产品及工具

## ■ ISO27001要求企业建立起PDCA的模型，确保信息安全的持续发展。



# 企业信息安全技术架构应包括的内容



# 企业信息安全管理体系的建设

- 信息安全管理体系是信息安全保障体系的重要组成部分
- 信息安全管理体系框架从企业管理的层面出发，按照多层防护的思想，为实现信息安全战略而搭建

安全政策，标准- 管理规定

安全意识培养 - 宣传教育

安全组织 - 管理控制

审计 - 监督

风险评估 - 发现问题

# 企业信息安全运维体系的建设

包含的内容	达到的效果
<div><div></div></div> <ul style="list-style-type: none"><li><input type="checkbox"/> 威胁分析与预警</li><li><input type="checkbox"/> 安全状态和时间的监控</li><li><input type="checkbox"/> 安全事件或事故的响应</li><li><input type="checkbox"/> 基于安全管控目标的操作行为与日志审计系统</li></ul>	<div><div></div></div> <ul style="list-style-type: none"><li><input type="checkbox"/> 统一的管理模式</li><li><input type="checkbox"/> 规范化的管理流程</li><li><input type="checkbox"/> 自动化的管理操作</li><li><input type="checkbox"/> 高级的维护管理</li><li><input type="checkbox"/> 量化的评估标准</li><li><input type="checkbox"/> 科学的考核体系</li><li><input type="checkbox"/> 防患于未然</li></ul>

# 企业信息安全技术体系的建设

- 合适的安全技术解决方案，不但需要理解安全管理的要求，同时也为安全运维管理提供易于操作的平台
- 企业安全技术体系的建立原则是要建设与管理体制对应的企业的安全架构设计
- 解决方案设计与具体的安全技术的应用上，要考虑当前企业应用系统能够中常见的安全弱点

## 安全技术规划的原则



- ☐ 整体安全性的规划
- ☐ 功能整合以统一管控
- ☐ 考虑同时进行项目的影响
- ☐ 从负面影响最小措施入手
- ☐ 具有未来扩充性

## 信息安全架构的对应



- ☐ 接入控制
- ☐ 信任管理
- ☐ 信息流控制
- ☐ 审计
- ☐ 完整性

## 安全技术体系的建设



- ☐ 物理安全技术
- ☐ 基础架构安全
- ☐ 应用安全技术
- ☐ 数据安全技术
- ☐ 身份和访问管理

# 企业信息安全框架的应用

- 为应对企业信息安全建设的需求，企业信息安全的各个层次可以对应到相应的安全服务
- 在技术体系的建立过程中，可对应提供技术架构的参考



# 目录

---

**第一部分 企业面临的信息安全环境**

**第二部分 企业信息安全的基本框架**

**第三部分 企业信息安全体系的建设**

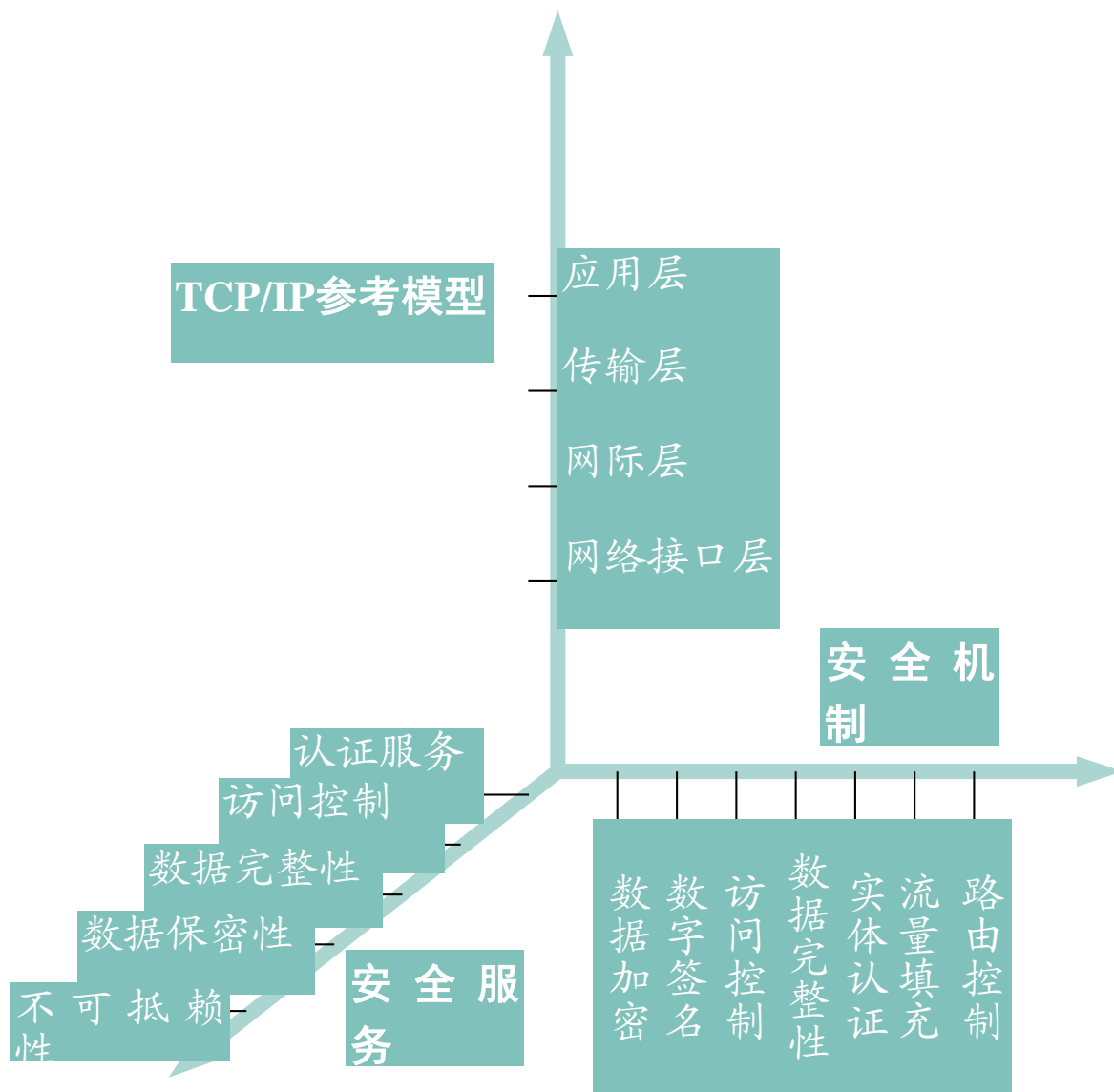
**第四部分 企业信息安全管理实践**

---



# 企业信息安全体系的实践：确保有效的信息安全须做到五点

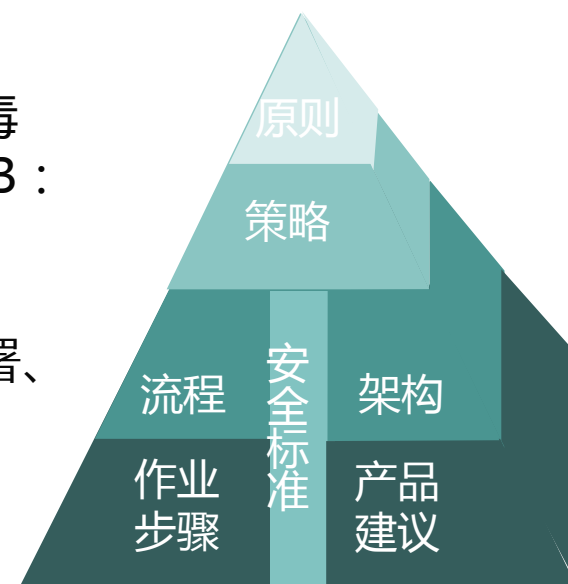
- **安全性风险和薄弱环节的评估及管理**：分析系统所面临的威胁，制定并实施正确的应对策略，治理和组织能力用以管理各种风险，并确保符合监管规范的要求。
- **技术和网络基础设施的保护**：保证端点的安全性和完整性，提供流量管理和配置管理。
- **企业持续性经营和灾难恢复**：确保能够从严重的技术故障和/或安全漏洞中迅速恢复，并做到从一开始就主动预防故障的发生。
- **身份认证和访问权限管理**：为安全、有效地访问关键应用和资源提供支持，包括用户管理、供应和访问权限，以及增强用户的安全意识，改进政策和培训。
- **保护企业应用**：具备端到端的能力以保障应用层面的安全——此方法集技术、控制、流程和管理于一体。



# 企业信息安全管理实践：IT安全和使用标准及运营的制定

## 基础是建立企业的信息安全架构模型

1. 参考企业的安全政策，企业IT安全准则，和信息安全分类与控制
2. 制定终端安全标准：员工电脑的安全和使用标准；相关的执行流程、组织架构等
3. 根据企业的安全架构设计，进行桌面安全产品的功能定位、确定选择标准并进行测试。
4. 分两类进行产品的布置，并完成相应的作业指南：A. 基本类：防毒软件、补丁工具、个人防火墙。企业身份管理平台与资产管理工具；B：符合与审计类：同步或提前布置符合与审计工具
5. 在实际的工作中，对第2步的规范、管理流程，进行修订。包括部署、执行、检查、培训、通知、符合与审计流程及相应的角色定位
6. 定期根据执行情况进行相应的改进与变更，包括对基本类产品的更换与日常支持，开发并部署一些符合与审计的工具。

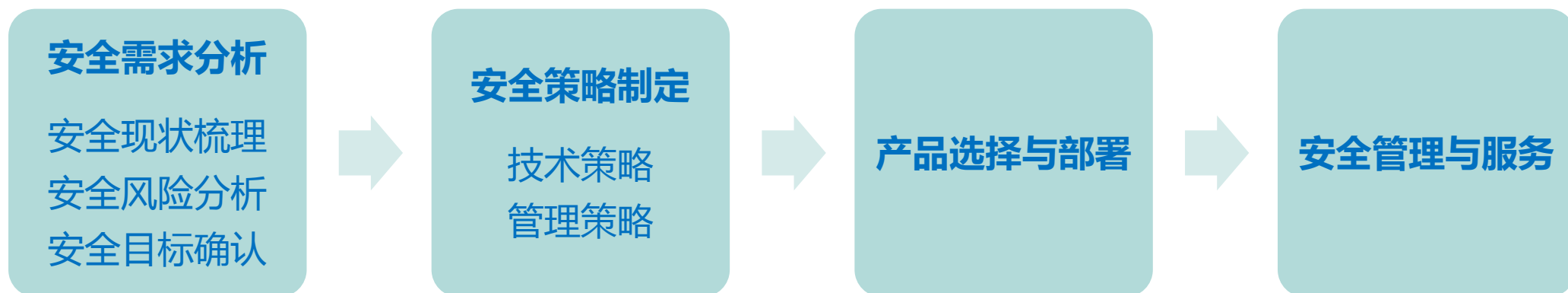


# 企业信息安全安全管理实践：培训是安全实践中的重要环节

■ 在企业的安全培训中的“保障IT安全的服务实施”应该包括基本的安全主题

课程主题	受众
安全概述	学习本课程的所有人
员工的安全责任	所有员工
内部系统的安全标准	支持业务或为和外部企业提供企业间服务的多用户系统、应用、中间件和网络基础设施的所有者和系统管理员
安全与外包客户	负责管理信息科技服务实施的全球服务实施中心
事件管理	所有服务实施人员
用户ID管理	在内部或外部客户中负责下列任何系统、服务器或应用的人员： <ul style="list-style-type: none"><li>• 建立员工帐号                      更新员工帐号                      删除员工帐号</li><li>• 维护员工帐号                      重建员工帐号密码</li></ul>
脆弱性管理	使用“不符合事件追踪系统”负责保证设备遵从内部系统的安全标准的系统管理员和如其他人员
不符合事件追踪系统	业务线管理者、安全管理员或任何其他由业务线管理者安排的人员；任何负责网络或服务以保证与业务线管理和安全管理相关业务执行的人员

# 企业信息安全技术实践：根据风险评估与业务发展的安全需求分析



为确保公司的整个网络系统能够安全稳定的运行，需要对重要服务器、重要子网进行安全保护，对传输的数据进行加密，用户的身份进行鉴别等，主要须解决以下方面的安全问题：

- **平台安全**：包括网站服务器、邮件服务器、Intranet服务器和内部服务器等。
- **网络安全**：防备来自Internet的攻击，如：病毒、木马和黑客等
- **用户安全**：包括公司员工、网站访客和网络会员的身份认定等
- **数据安全**：数据的灾备，总部与分支机构之间、内部网用户到服务器、移动用户和家庭用户到服务器等的数据传输等
- **管理安全**：如研发中心有公司产品源代码等重要的资料需特别的管理措施

# 企业信息安全技术实践：策略制定遵循一定的原则，并分门别类

## 策略制定的原则

- 适应性原则：在一种情况下实施的安全策略到另一环境下就未必适合
- 动态性原则：用户在不断增加，网络规模在不断扩大，网络技术本身的发展变化也很快
- 简单性原则：安全的网络是相对简单的网络
- 系统性原则：应全面考虑各类用户、各种设备、各种情况，有计划有准备地采取相应的策略
- 最小特权原则：每个用户并不需要使用所有的服务；不是所有用户都需要去修改系统中的每一个文件；每一个用户并不需要都知道系统的根口令等

## 安全策略的分类

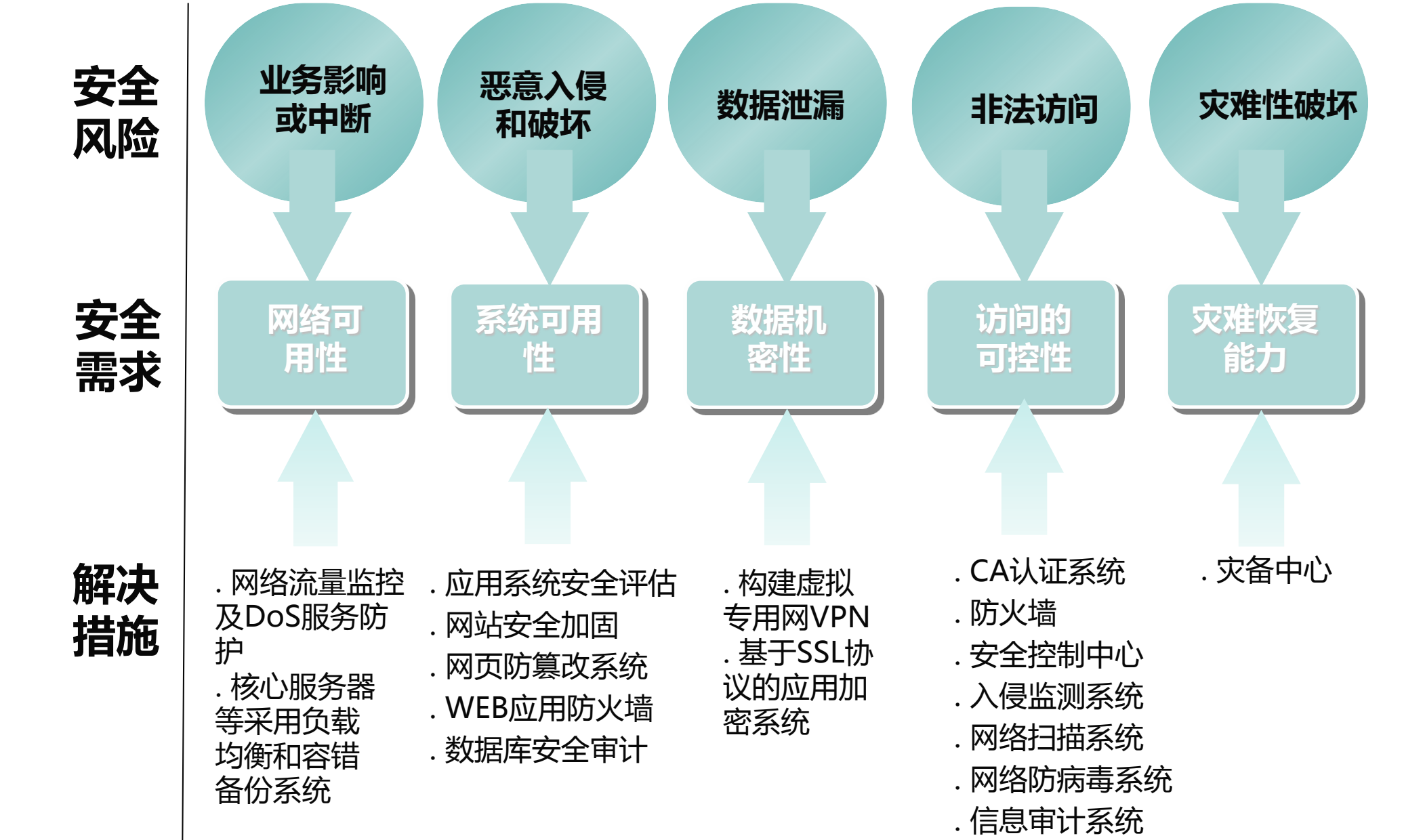
- 物理安全策略：如机房环境、门禁系统、设备锁、数据备份、CMOS安全设置等。
- 访问控制策略：为公司总部内部网与Internet网之间、公司总部与分支机构之间、Internet用户与公司网络之间等需要进行互连的网络制定访问控制规则。
- 安全配置及更新策略：对操作系统、应用系统、安全产品等进行升级更新、设置用户访问权限及信任关系等。
- 管理员和用户策略：制定机房出入管理制度、实行安全责任制等。
- 安全管理策略：安全规则设置、安全审计、日志分析、漏洞检测及修补等。
- 密码安全策略：密码复杂度、密码更改周期、密码有效期等
- 紧急事件策略：针对攻击和入侵可能导致的结果制定应急处理流程和灾难恢复计划。

# 企业信息安全技术实践：产品贯彻策略，产品与管理有机结合

---

- 交换机：划分VLAN进行子网隔离、抵抗嗅探类程序和提高网络传输效率
- 防火墙：解决内外网隔离及服务器安全防范等问题，主要部署在网络的Internet接点和重要部门的子网与其它内部子网之间，其中个人防火墙系统安装在客户端。
- 虚拟私有网：解决网络间数据传输的安全保密，主要部署需要安全保密的线路两端的节点处，如：防火墙和客户端。
- 身份认证：解决用户身份鉴定问题，主要部署在专用认证服务器或需要认证的服务器系统中。
- 反病毒：防范病毒、木马、蠕虫等有害程序的感染与传播，主要部署在服务器系统和客户机系统。
- 入侵检测系统：安全监控和黑客入侵实时报警拦截，主要部署在需要保护的服务器主机和需要保护的子网。
- 灾备系统：.....
- .....

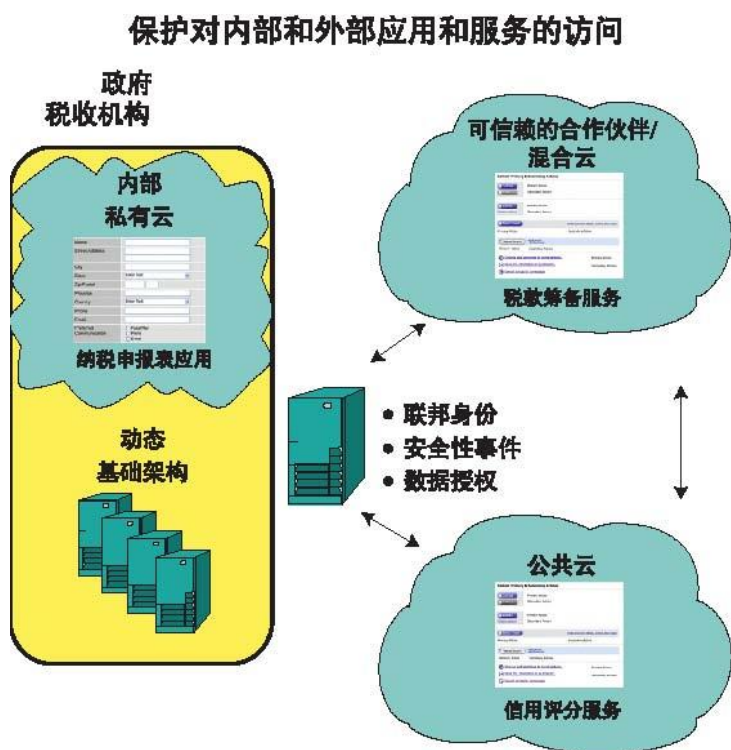
# 企业信息安全技术实践：企业典型信息安全风险及解决措施





# 技术发展与信息安全：云计算、SOA

- 安全总体原则适用于任何环境，不论是云计算还是SOA，如：身份验证，授权，机密性，完整性，审计和遵守
- 安全性、可靠性和经济性是“云”最大的关注点
- 基于SOA的企业关注身份识别及相关安全挑战



## 云计算的安全关注点

- ☐ 关键业务应用的可靠性
- ☐ 数据暴露给非授权用户访问的风险
- ☐ 法规要求将某些应用在云计算平台上的使用
- ☐ 云计算供应商必须提供防火墙与安全配置的管理方式
- ☐ 云计算降低了组织对资源的控制，需要足够的安全透明度

## SOA环境下的安全挑战

- ☐ 跨组织服务与服务的身份识别
- ☐ 基本事务需要不同组织间实时无缝对接
- ☐ 确保整合应用有足够的安全措施
- ☐ 对新旧技术混合而成系统和服务进行身份和安全管理
- ☐ 保护数据在整个生命周期中的安全
- ☐ 政府、行业、企业本身在合规方面的安全要求

# 技术发展与信息安全：大数据

- 激增的企业数据既带来了巨大的管理挑战，又带来了用于获取安全洞察的巨大机会。
- 前瞻性的组织正转向大数据平台，如基于Hadoop的平台，帮助解决各种高级安全挑战。这些平台提供的分析类型通常使用历史基线、统计和可视化功能来发现过去的欺诈或安全漏洞证据



数据的种类和数量正在推动实现新的大数据用例，帮助企业保持安全性

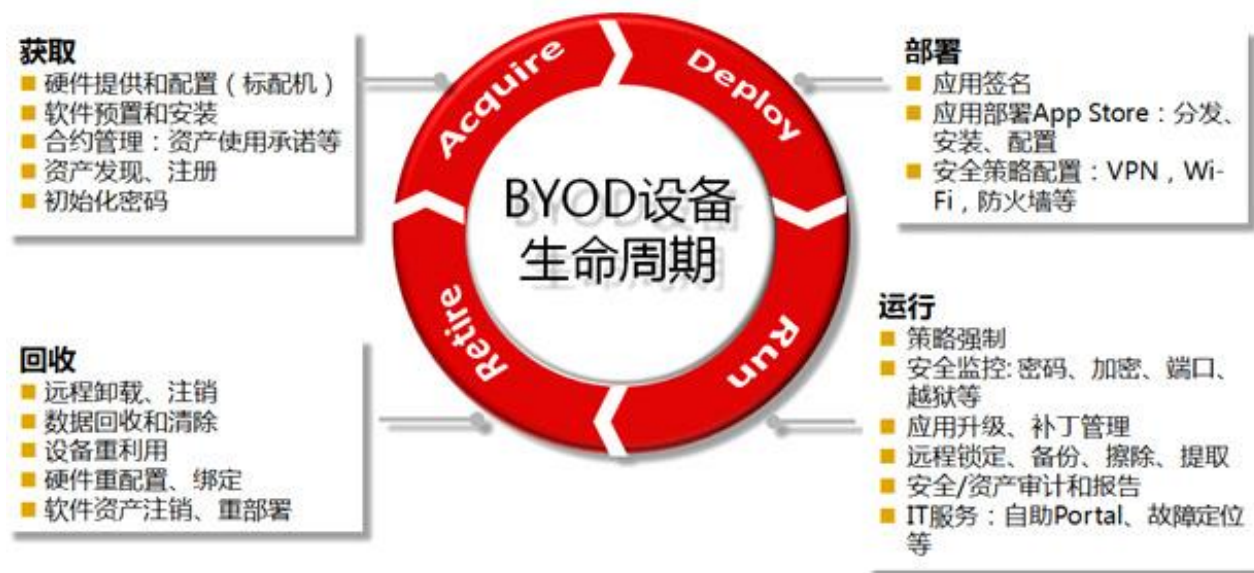
通过大数据分析捕获各种来源的数据，并使用现有规则以及客户定义的规则将这些数据缩小为一个可管理的攻击列表

# 技术发展与信息安全：移动设备BYOD与MDM

原本为个人消费者设计的智能手机和平板电脑正在不断被企业用于承载关键业务及核心应用，同时，BYOD的策略也被大量引入企业，传统的IT管理在针对不断涌现的新兴移动设备管理方面受到巨大的挑战

## BYOD策略需要涵盖以下内容：

- 可以访问哪一类设备，如安卓，iPad，MacBook，Wintel;需要什么版本的操作系统
- 你的用户群需要什么级别的访问权限
- 用户需要安装什么应用
- 最重要的一点，需要使用公共wifi网络的个人用户要安装VPN
- 最后，要让用户知道设置密码的重要性



- 利用Citrix XenMobile、MobileIron等产品对BYOD设备进行MDM管理
- 提供完整的移动设备生命周期管理；  
从设备注册、激活、使用、淘汰各个环节进行全面管理；  
实现用户及设备管理，配置管理，安全管理，资产管理等功能。

**谢 谢 ！**

联系方式：wenjie.ma@qq.com