

IBM 信息科技服务部

# 信息安全与IT优化

田成

中国区经理，资深管理顾问，IT策略与架构咨询

2007.07

## 交流内容

---



### 1. 信息安全风险管理趋势和理念

### 2. 信息安全风险管理建设的方法和思路

### 3. 信息化系统优化

# 信息安全已成为国家经济和社会发展的的重要内容

黑客

网络犯罪

工业间谍

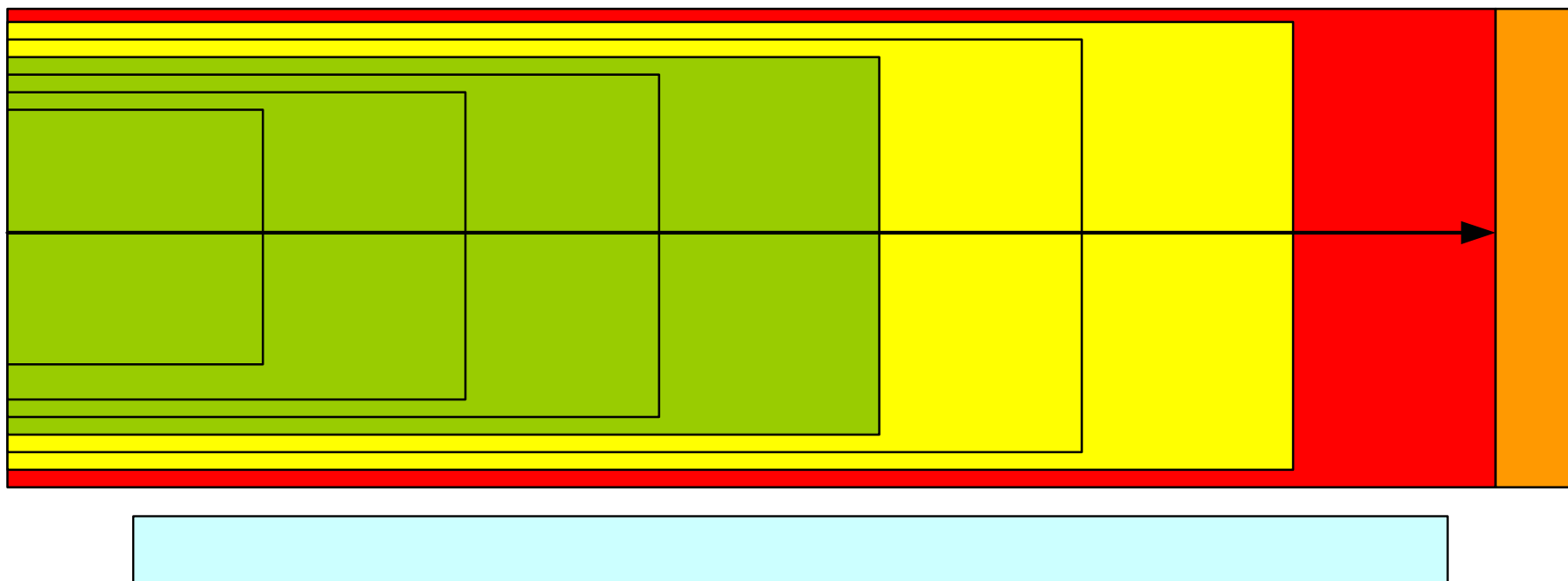
身份盗窃

拒绝服务

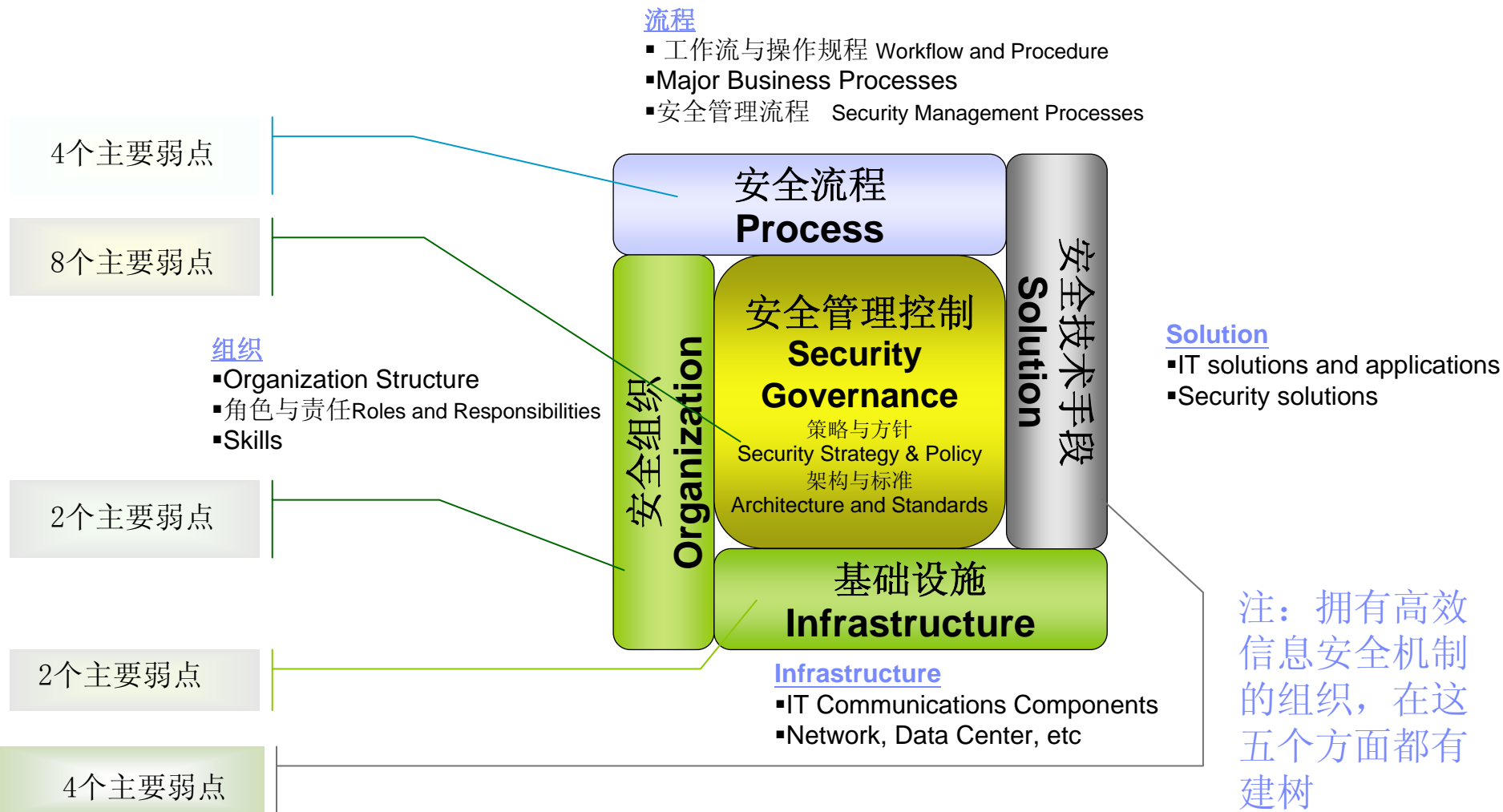
政府在《国民经济和社会发展第十一个五年规划纲要》中明确提出‘加强基础信息网络和国家重要信息系统的安全防护。推进信息安全产品产业化。发展咨询、测评、灾备等专业化信息安全服务。健全安全等级保护、风险评估和安全准入制度’等方针政策。

我国的信息安全建设正从信息安全基础设施建设为重心的阶段转向统筹规划、协调互动的整体发展的新阶段

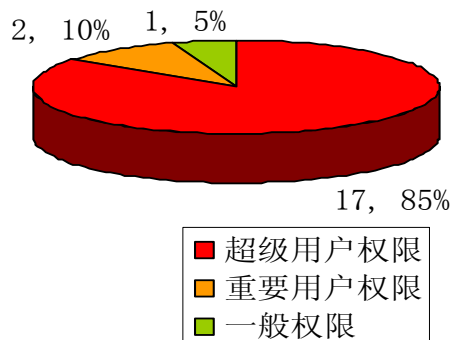
# 数据安全链分析



# 案例分析：为了评估安全机制的有效性，从五个不同的安全方面进行审计和分析



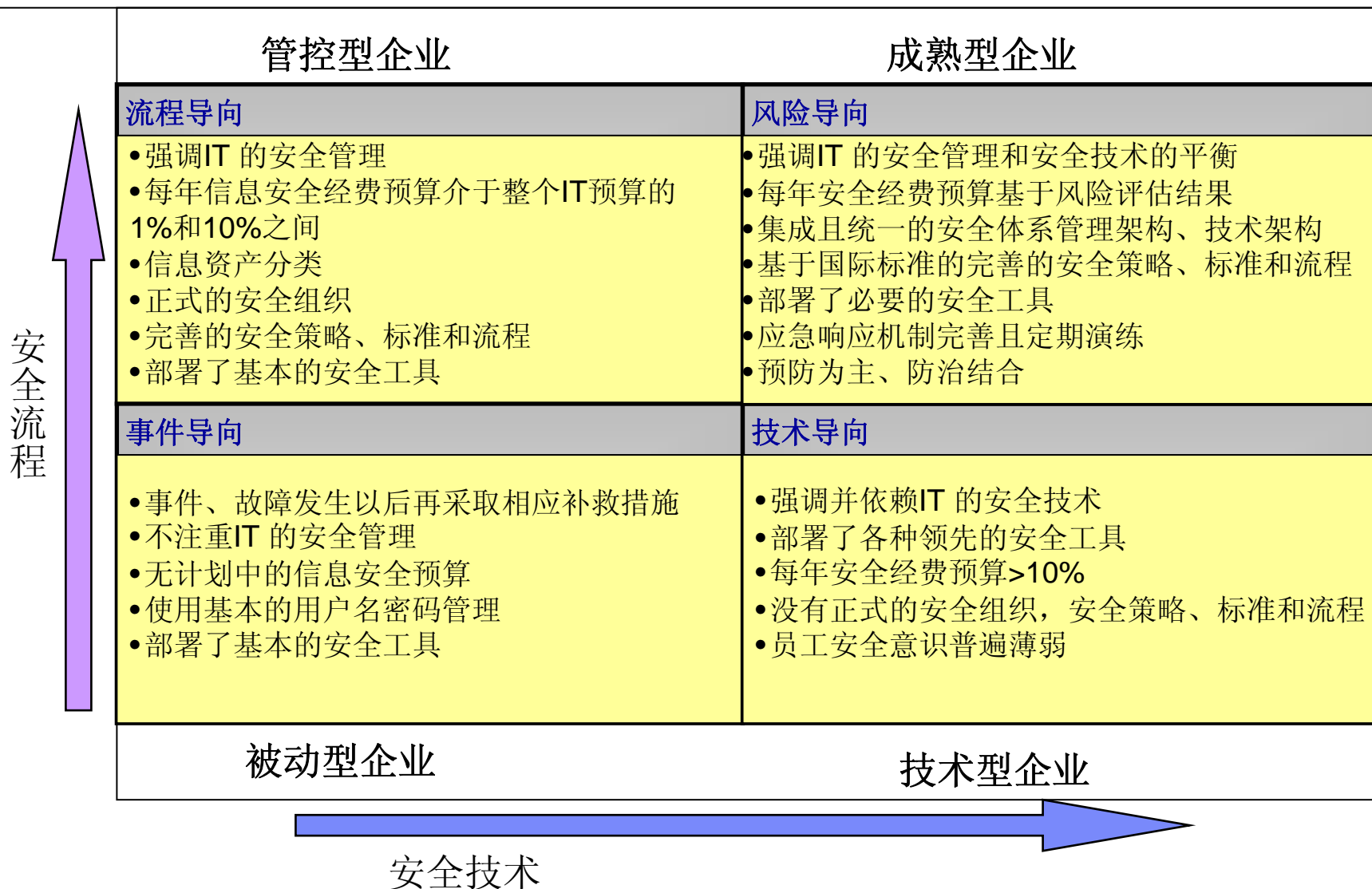
# 案例分析：渗透测试的初步结果



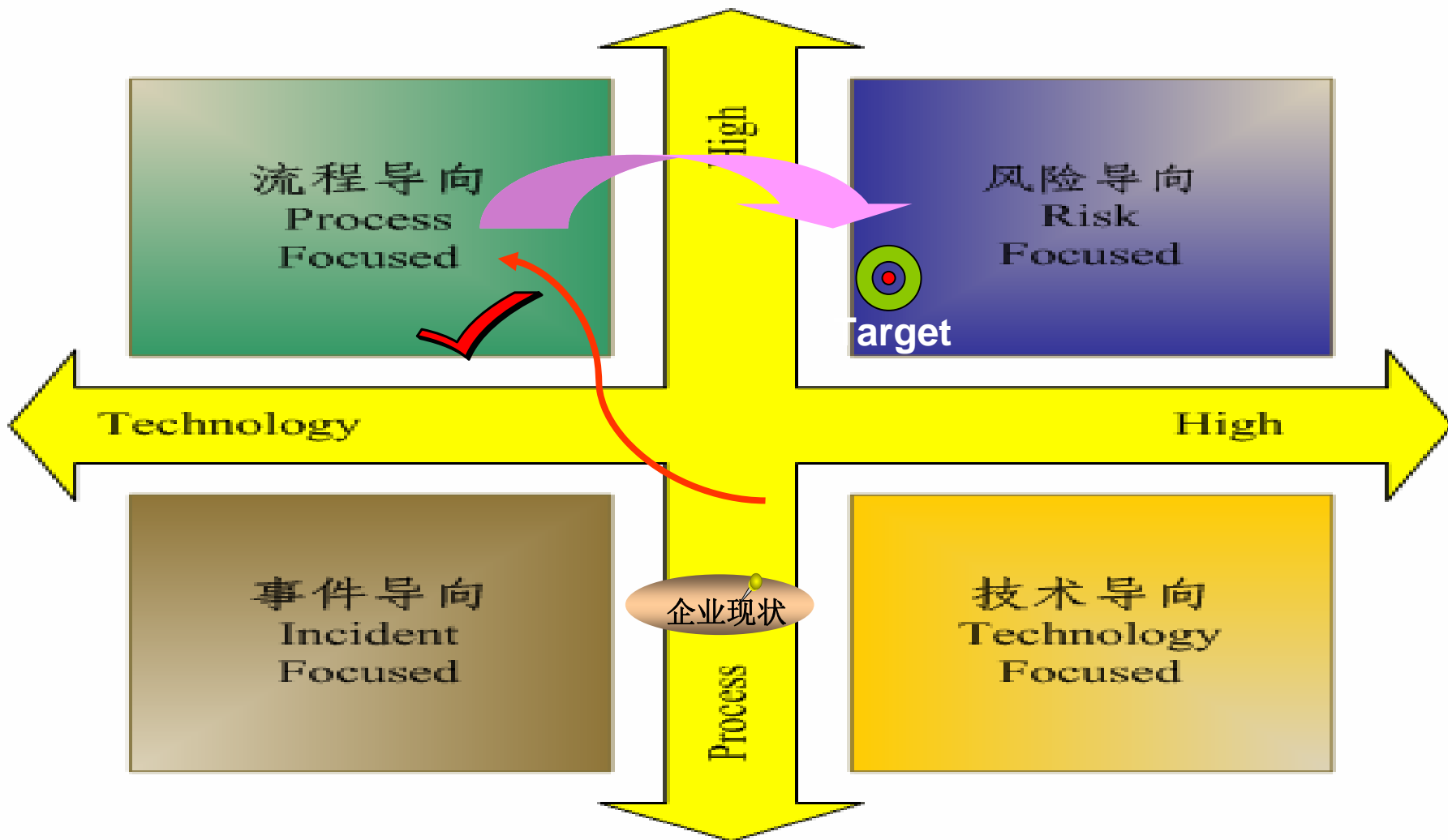
- 基本上所有的核心应用主机都能被入侵，并能获得基本上所有的机密业务数据
- 只是时间问题，入侵者完全就能了解所有的应用及数据含义
- 85%，获得主机超级用户Root的权限
- 10%，获得重要帐号权限（oracle），以及Root的未隐藏密码的Passwd文件
- 5%，获得帐号权限（patrol），如果时间充足，可以利用来进行进一步权限提升

	应用	主机
综合XXX (13)	BBB	xxBBBh1
	xx运营帐务	xxdfh1
	xx帐务	xxgfh1
	xx营业	xxgfh2
	xx运营帐务分拣分发	xxdiyh1
	xx运营帐务接口	xxinkh1
	xx运营帐务应用	xxyzh_test
	xx运营帐务离线	yyyxt1
	xx数据库	jff1
	xx数据库	jff2
	xx应用	jff3
	xx应用	jff4
	xx网关	jff5
xx网关	jff6	
业务XXX (3)	xx集中计费	xx-CK-h3
	xx集中计费	xx-CK-h4
	xx集中计费	xxhzmh1

# 四种常见的信息安全风险管理模式



国内大多数单位和企业的信息安全风险管理方式处于事件与技术导向之间，可以以首先以“流程导向”为中短期目标，长远来说以“风险导向”为最终目标



## 国内信息安全风险管理趋势概述


- ◆ 2003年，27号文，强调“要重视信息安全风险评估工作”
- ◆ 2004年，完成风险评估研究报告与标准草案
- ◆ 2005年，开展风险评估试点工作
- ◆ 2006年1月，出台5号文，提出开展信息安全风险评估工作的意见
- ◆ 2006年8月-9月，开展风险评估检查工作
- ◆ 2006年10月，总书记批示“加快专控队伍建设”，“风险评估工作要制度化”
- ◆ 从2007年起，对”8+2“系统开始实行制度化的风险评估

- ◆ 公安部主力推动“等级保护”工作；
- ◆ 保密局对涉密网络和信息系统提出相应风险管控要求；
- ◆ 发改委、科技部、信息产业部等持续在科研和产业化投入方面予以支持
- ◆ 国防科工委加强安全风险管理的体制、机制和建制工作；
- ◆ 信息安全标准化工作重点支持风险评估/管理；
- ◆ 各相关部门在积极开展风险管理方面的政策制定、技术研究和评估实践

## 交流内容

---

1. 信息安全风险管理趋势和理念

 2. 信息安全风险管理建设的方法和思路

3. 信息化系统优化

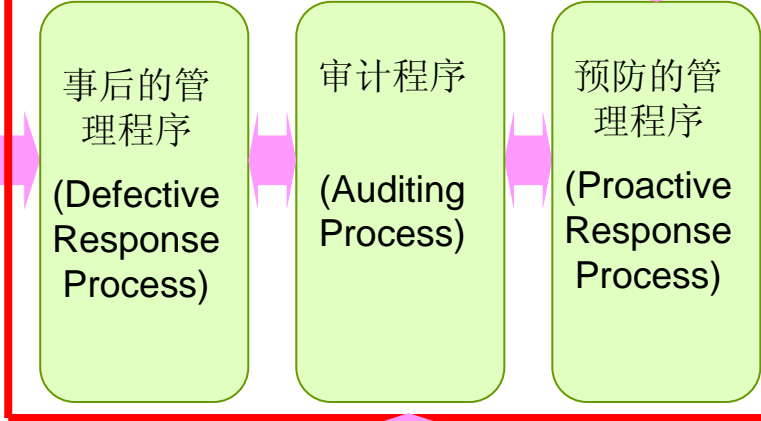
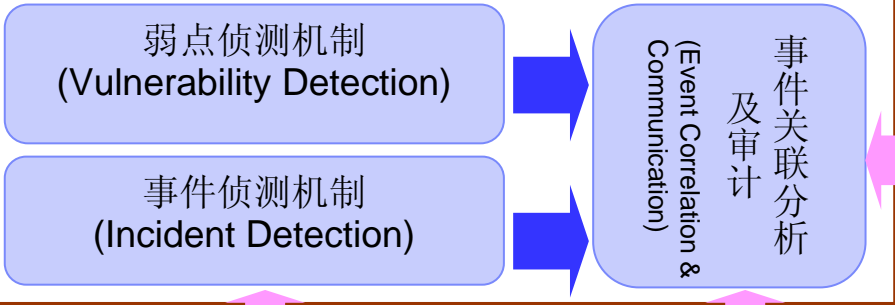
# IBM建议从”风险导向”(Risk Focused)的角度来规划企业的信息安全管理架构蓝图

企业经营策略/业务管理需求 (Business Strategy / Requirement)

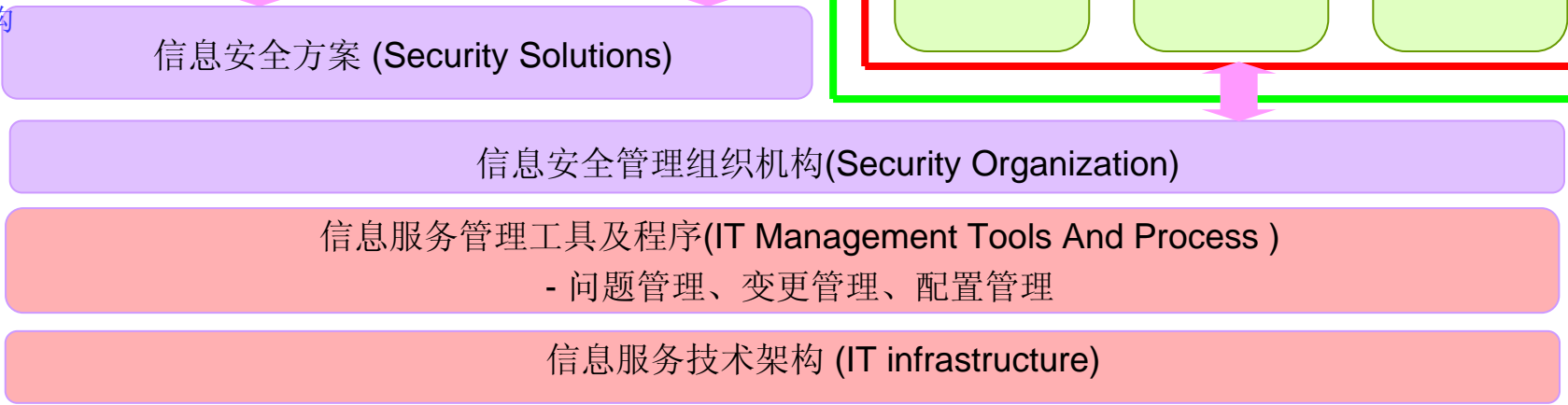
安全管理制度 → Process

信息安全管理体系统 ( Information Security Management System )  
- 信息安全政策、标准、及信息安全资产建立

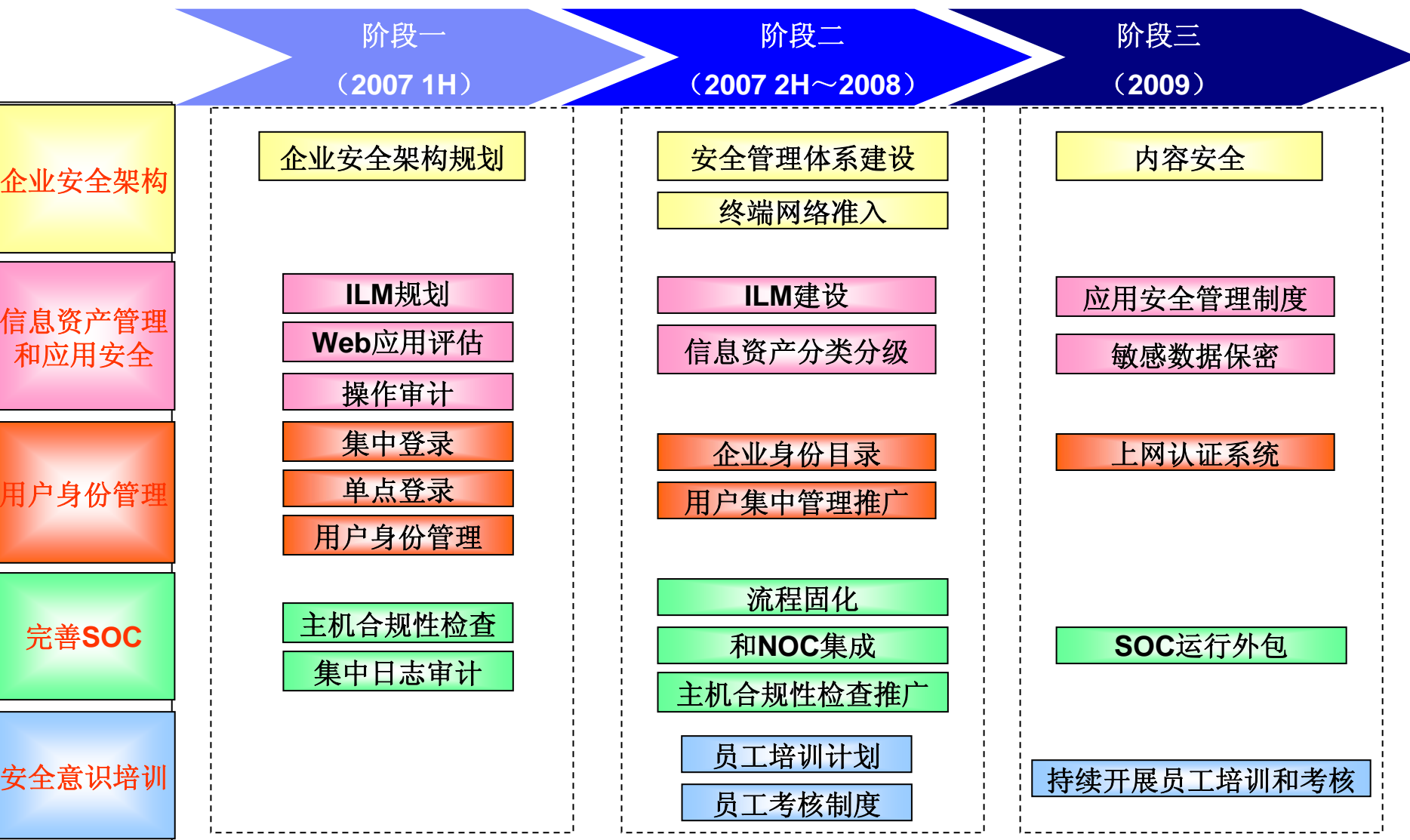
安全监控机制 → Operation



技术与架构支持 → Enabler




# 安全建设长期规划举例



## 交流内容

---

1. 信息安全风险管理趋势和理念
2. 信息安全风险管理建设的方法和思路

 3. 信息化系统的优化

## 全球CIO们在关心的问题

- 使IT能够及时地支持不断变化的业务需求
  - 改善IT资源的利用率、有效性、生产力
  - 降低IT运营的复杂度，控制IT支出
  - 在提高IT项目实施速度的同时控制风险
  - 提高IT系统的可靠性和安全性
- 
- 全球CIO们面临着为业务提供价值的同时更好地利用现有IT资源的挑战
  - 全球的CIO们在寻找优化IT投资的方法



# 当前IT所面临的挑战

目前多达**40%**的IT运营中断来源于操作员的人为错误.

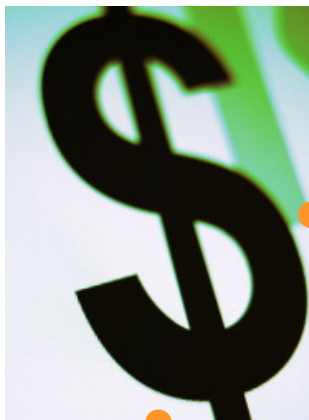


由于现有系统的多样性和复杂性，应用上线经常会延迟



尽管大多数服务器资源只达到**20%**或更少的使用率，在使用高峰期系统还会经历响应不及的问题.

近 **60%**的IT支出花在运维支持、系统管理维护上



IT资源的重复建设

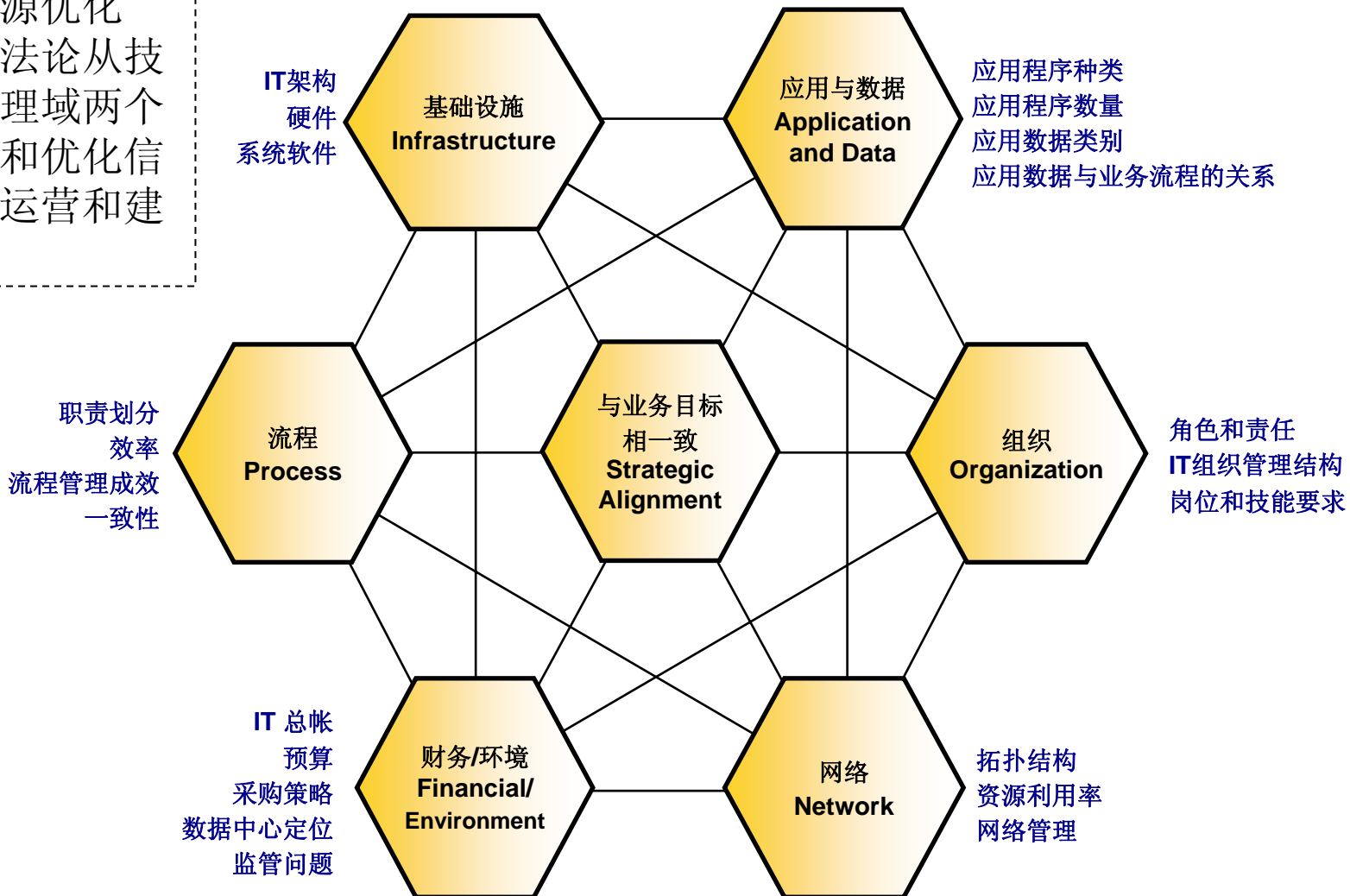
Sources: IBM and Industry Studies, Customer Interviews

# IBM IT资源优化架构方法论简介

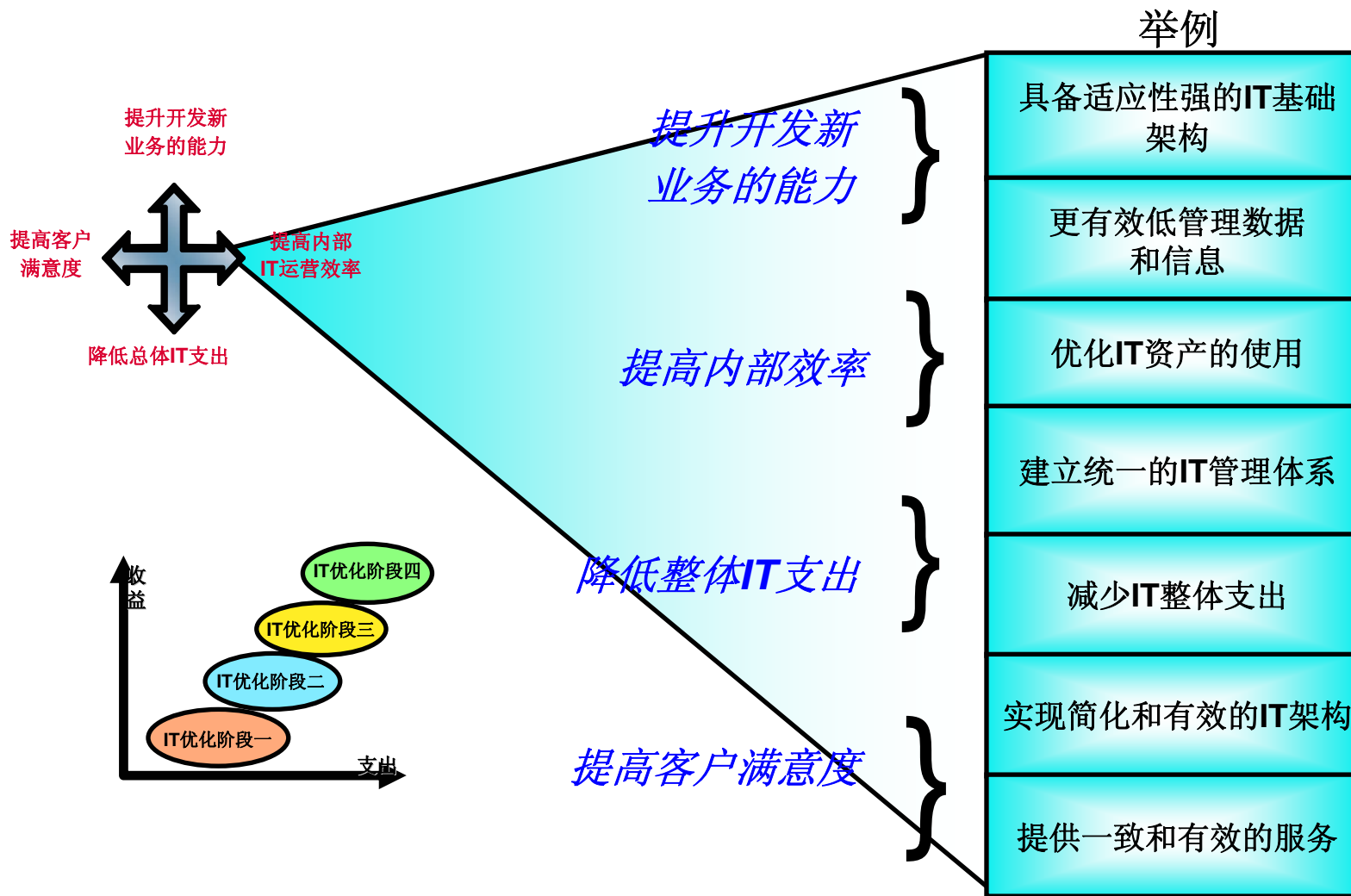


# IBM IT资源优化方法论 (ITRO) 简介

IBM IT资源优化 (ITRO) 方法论从技术域和管理域两个方面分析和优化信息系统的运营和建设:

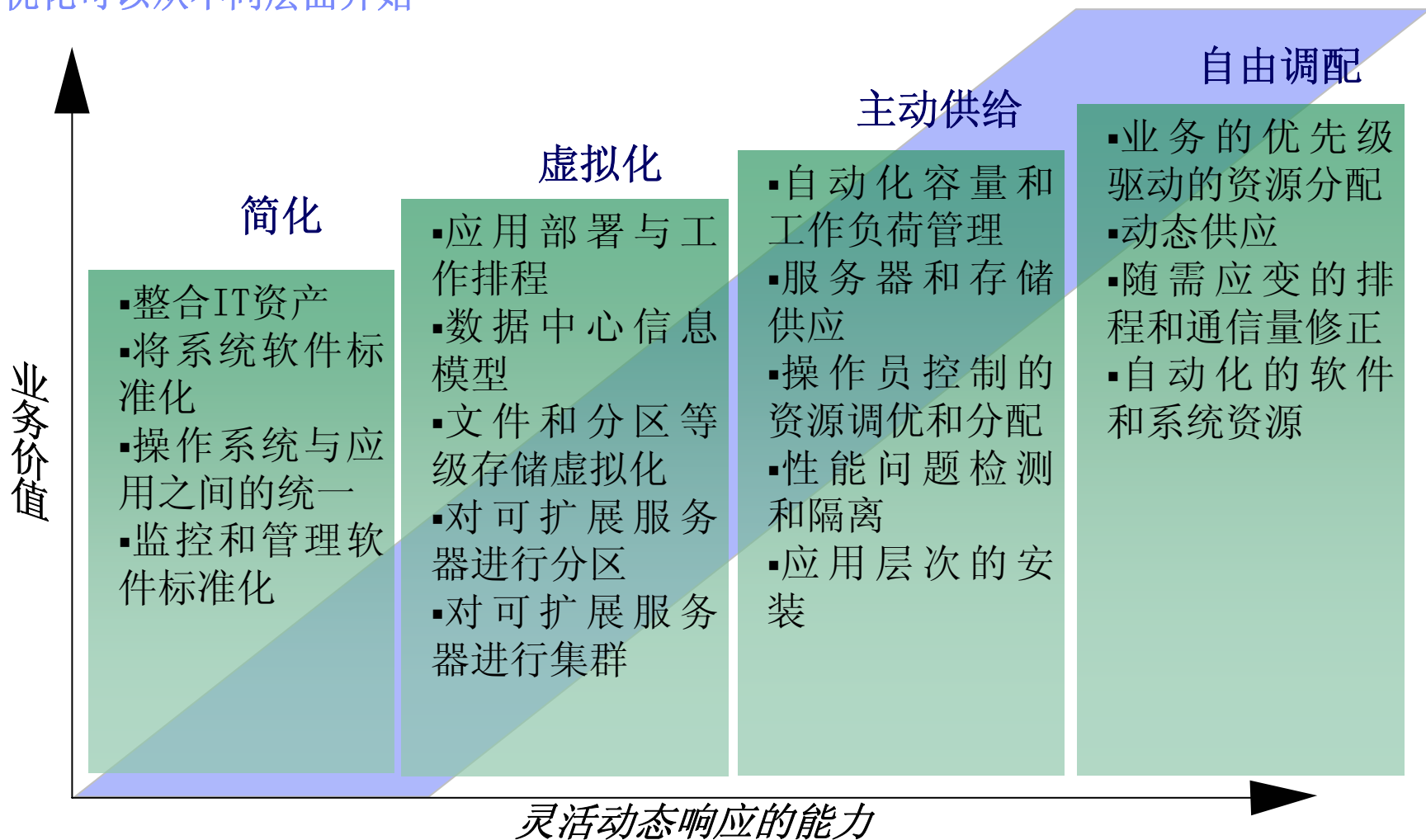


# IT优化的基础是将IT重要的价值组件分解为更为具体的需求



# IT资源优化的演进

IT优化可以从不同层面开始

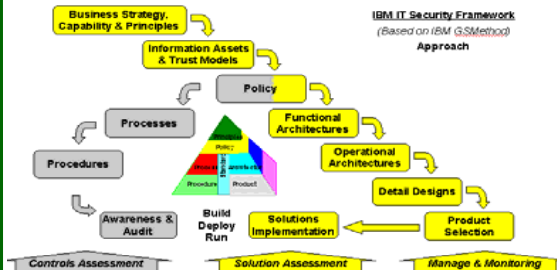


# IBM具有规范的咨询服务方法和丰富的知识库

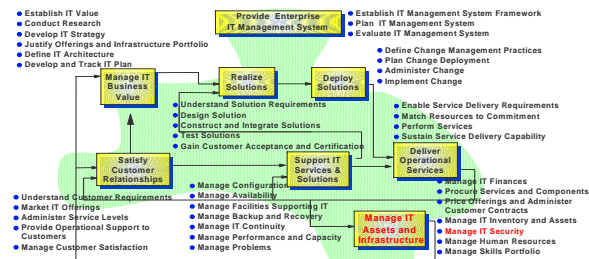
Methodology



IBM IGS Method



IBM Security Approach



IBM IT Process Model

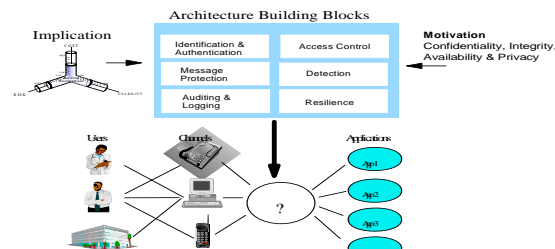
Model



ISO 17799-2002 Model



Security Life Cycle Model



Security Architecture Block

Reference



IBM Intelligence Capital DB

IBM Business Conduct Guidelines	Information Security Controls for Customer XYZ (GSD331)
Computer Security and Use Guidelines for IBM Employees (ITCS300)	Customer Service Center Security Policy
Security Standards for Providers of Network and Computing Services (ITCS204)	e-business Universal Server Farm Security Policies and Practices
Security Guidelines for Inter-Enterprise Services (ITCS302)	Data Privacy Security Standard

IBM Internal Reference

Appendices	
A1. OS/390 and MVS Platforms with RACF	O. DCAF
A2. OS/390 and MVS Platforms with CA-ACF2	P. DCE Servers
A3. OS/390 and MVS Platforms with CA-Top Secret	Q. DFS Servers
B1. Host VM with RACF	R. DCE/DFS Clients
B2. Host VM with ALERT/VM	S. Netfinity
B3. Host VM with VM Secure	T. Netview DM/2
C. OS/400 Platforms	U. Microsoft Windows NT Servers
D. Network Infrastructure	V. ADSM Servers
E. AIX Platforms	W. Web Servers
F. AFS Servers	X. Tandem
G. AFS Client Subsystems on AIX Servers	Y. DEC/VMS
H. OS/2 LAN Servers	Z. Tivoli
I. OS/2 Base Operating Systems	AA. HP/UX
J. Lotus Domino Servers	AB. Sun/Solaris
K. DB/2 & DB2/6000	AC. Digital/UNIX
L. CMVC	AD. Linux
M. Novell Netware	AE. Firewall
N. TCP/IP	AF. Sybase
N1. TCP/IP (AIX)	AG. Oracle
N2. TCP/IP (Linux)	AH. SAP
N3. TCP/IP (OS/400)	AI. Microsoft Exchange
N4. TCP/IP (OS/390)	AJ. Windows 2000
N5. TCP/IP (OS/2)	

# 谢谢！

