信息安全管理
先锋论坛

信息安全策略与实践

欢迎加入QQ群信息安全管理_ISO27001 群号207723402

程武阳

2016年7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

授课专家

唐龙

资深IT管理咨询顾问及讲师，十四年工作经验，服务的客户领域涉及电信、金融、政府、制造、能源等多个行业，服务的企业总数超过100多家。广州大学客座讲师，运行中心服务成熟度（国标）编委。

项目经验：咨询顾问、近三年部分项目

伊之密精密机械 安全评估　　中国移动南方基地 能力提升项目

华星光电 ITIL流程落地项目　　广州地铁ITIL流程落地+ISO20000体系认证

河北移动 访问控制下的配置项信息的变更控制项目　中国人保 DRP咨询

深圳招商银行 ITIL 项目　　深圳招商银行 DRP项目

深圳招商银行 应用关联关系梳理项目　深圳航空　ISO 27001认证

全国福利彩票 27001体系并认证　　深圳博众　27001体系并认证

广州工商行政管理局 ITIL流程优化　　东莞供电局 ISO 27001内审、27001落地咨询项目

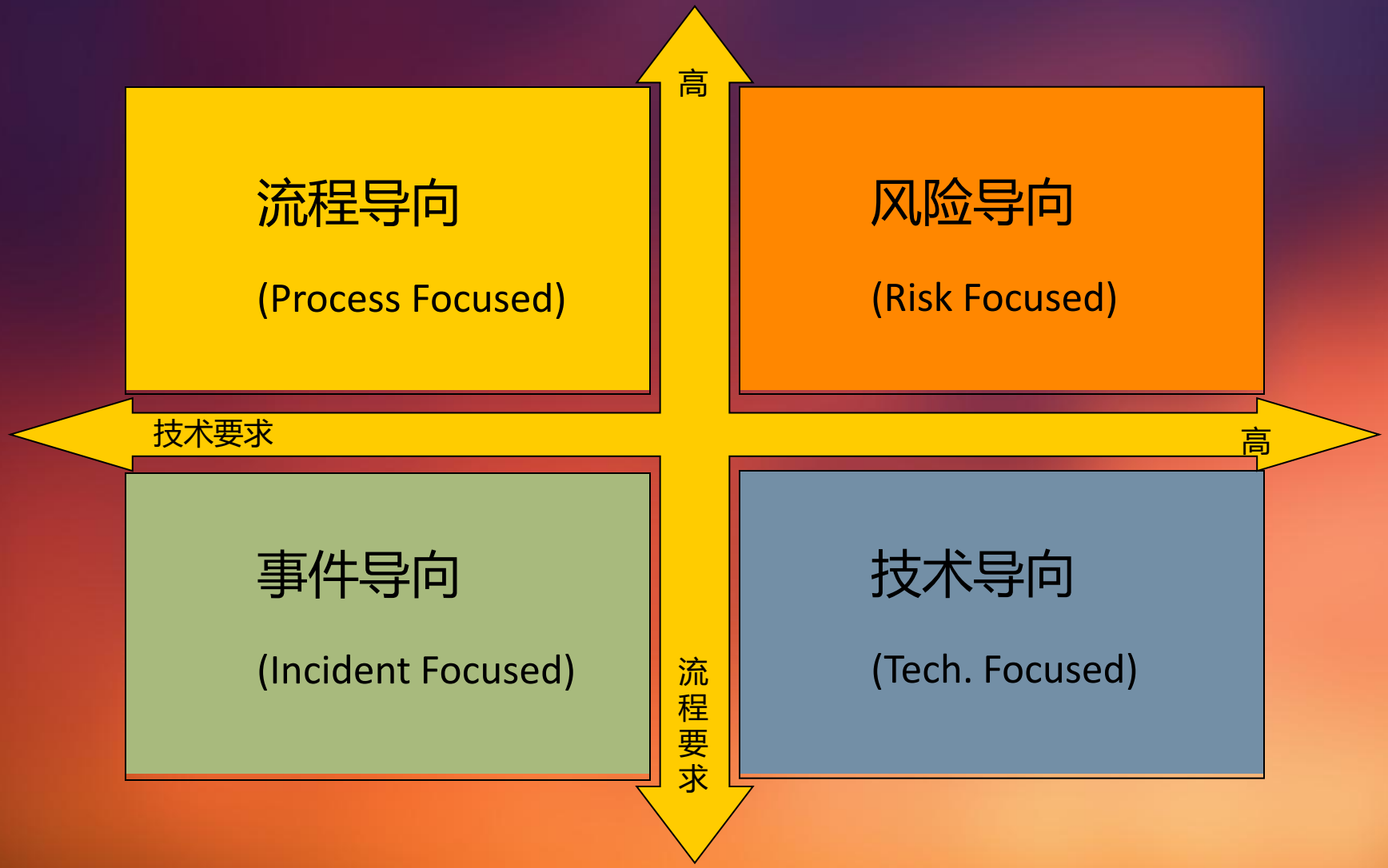
东莞供电局 ISO 20000内审

信息安全策略是重要的，但是…

客户最经常问的问题就是：

- **做什么？**
- **怎么做？**
- **何时做？**
- **谁来做 ？**

四种信息安全管理模式


高
流程导向
(Process Focused)
风险导向
(Risk Focused)
技术要求
高
事件导向
(Incident Focused)
技术导向
(Tech. Focused)
流程要求

信息安全最大的威胁

对信息安全最大的威胁不是来自攻击，而是来自信息安全管理者和使用者的大脑！

相比北美，国内企业缺乏内部安全策略和约束。75%的北美受访者表示企业有员工安全操作标准，中国只有38%的企业作出同样回答.

主要内容

第一部分 理论上怎么说？

第二部分 实际中怎么做？

第三部分 风险预测与风险评估

第四部分 安全策略的制定与实施

信息系统 - 概念

- **信息系统：实现系统中各实体间数据的传输、交换、转移，并使各实体通过高速信息交换相互协作，提高工作效率的解决方案。**
  - **信息系统存在于任何一个社会组织中，它渗透到组织中的每一个部分，就像人体组织的神经系统，分布在人体组织中的每一个部分。**
  - **信息系统是为管理服务的，信息系统不同于组织中的其他系统，它不是从事某一具体工作，而是起关系全局并使系统中各子系统协调一致的作用。**
  - **信息系统主要由信息资源、硬件系统和软件系统三部分组成，各部分相互作用以达到提供信息的目的。**

信息系统安全 - 安全管理

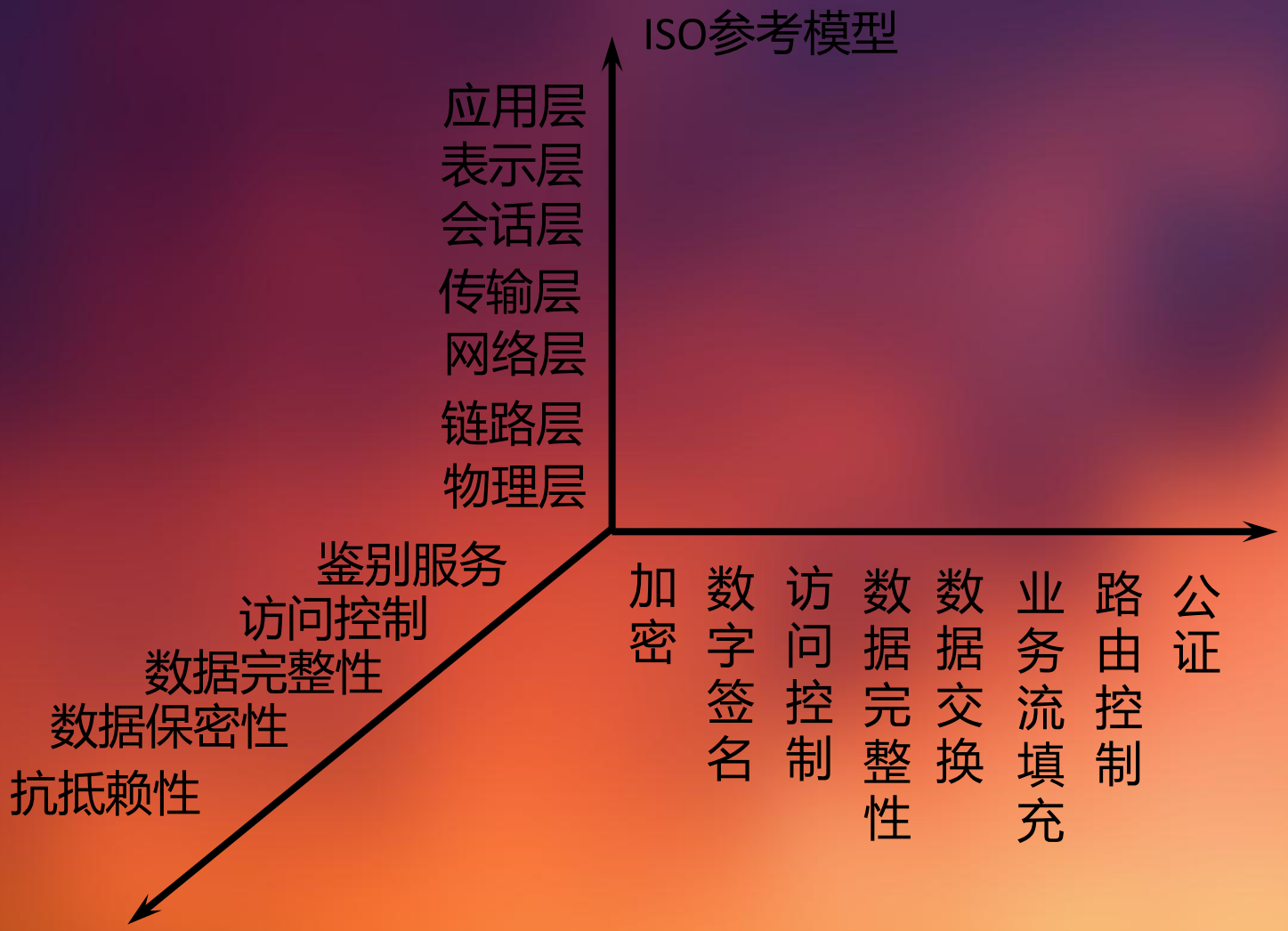
- 安全管理是企业信息安全的核心，是指针对于企业的信息安全而制订并审查实施过程的一整套解决方案；
- 安全管理包括***风险管理***、***安全策略***和***安全教育***，这三个组成部分构成了整个企业安全规划体系的基础。

风险管理识别企业的资产，评估威胁这些资产的风险，评估假定这些风险成为现实时企业所承受的灾难和损失。安全策略是指在一个特定的环境里，为保证提供一定级别的安全保护所必须遵守的规则，安全策略具有确定性、完整性和有效性。 根据安全策略的内容，对所有涉及的人员还要进行安全教育。

信息系统安全-安全策略

- 信息安全策略（Information Security Policy ）也称做信息安全方针，它是在一个组织内指导如何对包括敏感信息在内的资产进行管理、保护和分配的规则和指示。
- 阐述的不同层次来看，信息安全策略可以分为三类：
  - 总体方针
  - 特定问题策略
  - 特定系统策略

信息安全系统-ISO7498-2安全体系结构



信息安全系统-ISO7498-2安全体系结构

- 国际标准化组织(ISO)于1989年对OSI开放系统互联环境的安全性进行了深入研究，在此基础上提出了OSI安全体系结构，作为研究设计计算机网络系统以及评估和改进现有系统的理论依据，这个体系就是ISO 7498-2：1989(Information processing systems--Open Systems Interconnection--Basic Reference--Part 2:Security Architecture)，该标准被我国等同采用，即《信息处理系统--开放系统互连--墓本参考模型--第二部分：安全体系结构GB/T 9387.2--1995》。

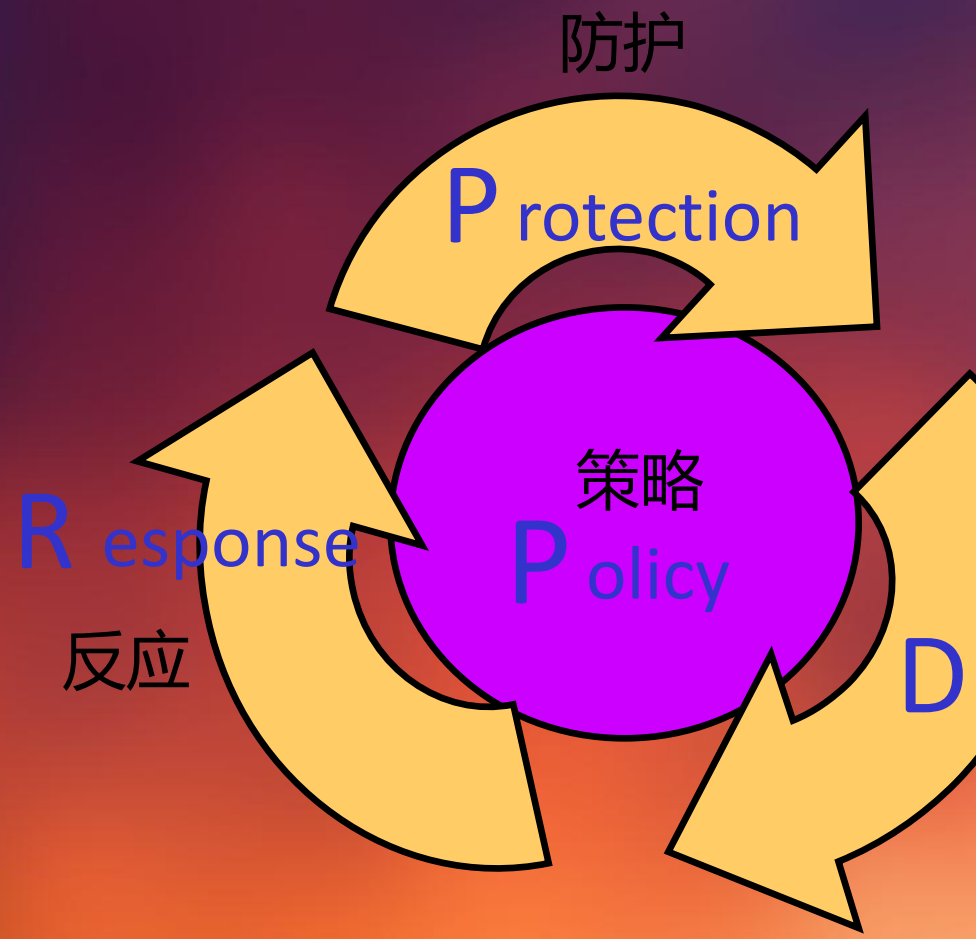
信息安全系统-ISO7498-2安全体系结构

- ISO7498-2安全体系结构由5类安全服务(Security Services)及用来支持安全服务的8种安全机制(Security Mechanisms)构成；
- 安全服务体现了安全体系所包含的主要功能及内容，是能够定位某类威胁的安全措施；
- 而安全机制则规定了与安全需求相对应的可以实现安全服务的技术手段，一种安全服务可以通过某种安全机制单独提供，也可以通过多种安全机制联合提供；而一种安全机制可以提供一种或者多种安全服务。

信息安全系统-ISO7498-2安全体系结构

- ISO7498－2安全体系结构针对的是基于OSI参考模型的网络通信系统，它所定义的安全服务也只是解决网络通信安全性的技术措施，其他信息安全相关领域，包括系统安全、物理安全、人员安全等方面都没有涉及。此外，ISO7498－2体系关注的是静态的防护技术，它并没有考虑到信息安全动态性和生命周期性的发展特点，缺乏检测、响应和恢复这些重要的环节，因而无法满足更复杂更全面的信息保障的要求。

安全防护的P2DR模型



安全防护的P2DR模型

- ISO7498是以防护为主的静态安全模型，随着以漏洞扫描和入侵检测(IDS)为代表的动态检测技术及产品的发展，人们对动态安全模型的研究也逐渐深入成型，P2DR模型就是动态安全模型的典型代表。
- 20世纪九十年代末，ISS联合众多厂商组成ANS联盟，试图以此为基础建立一个可量化、可数学证明、基于时间的、并以PDR为核心的安全模型标准，这个模型就是自适应网络安全模型ANSM(Adaptive Network Security model)。

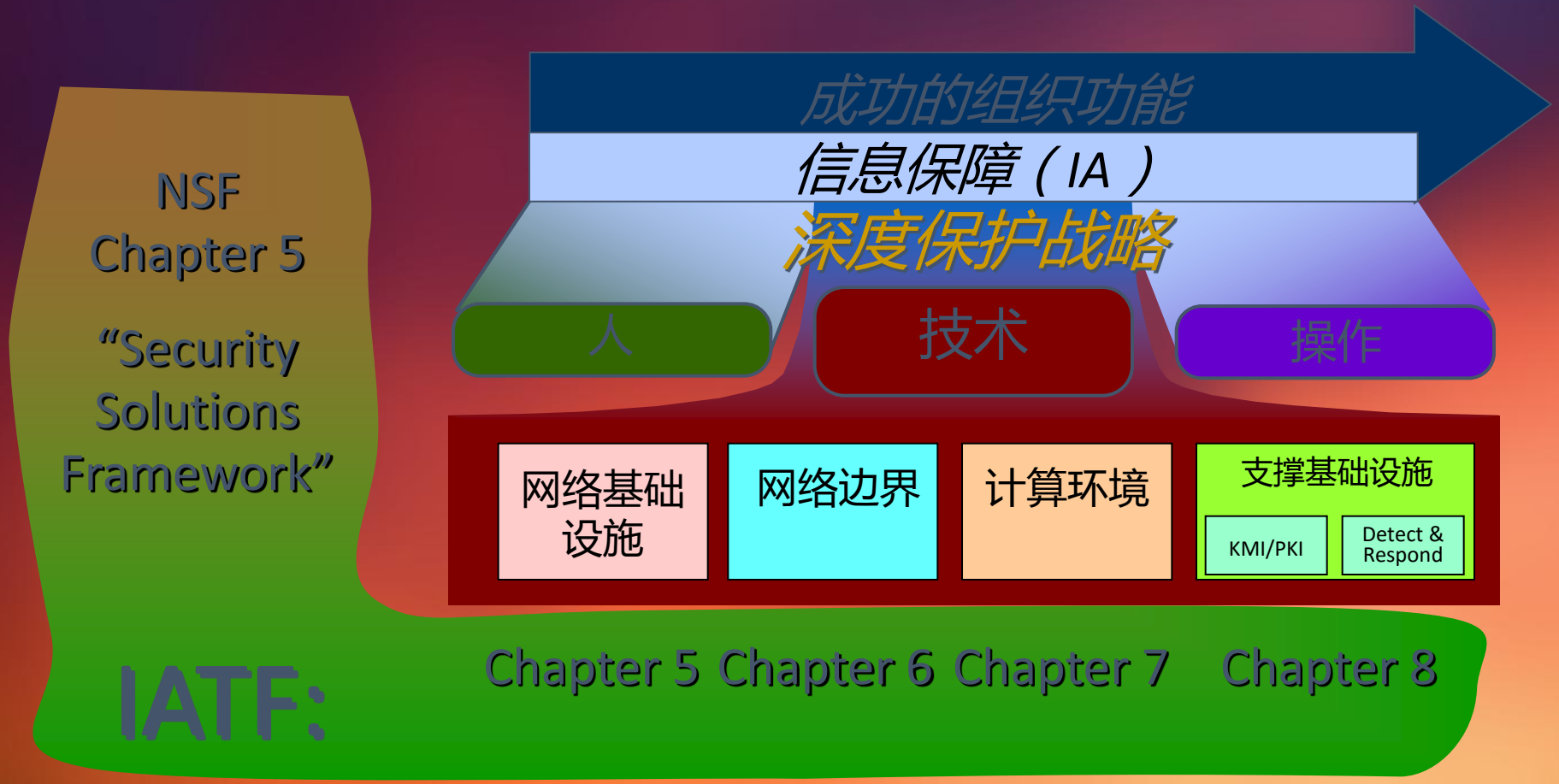
安全防护的P2DR模型

- 按照P2DR的观点，一个良好的完整的动态安全体系，不仅需要恰当的防护(比如操作系统访问控制、防火墙、加密等)，而且需要动态的检测机制(比如入侵检测、漏洞扫描等)。在发现问题时还需要及时作出响应，这样的一个体系需要在统一的、一致的安全策略的指导下进行实施，由此形成一个完备的、闭环的动态自适应安全体系。

- P2DR模型是建立在基于时间的安全理论基础之上的。该理论的基本思想是，信息安全相关的所有活动，无论是攻击行为、防护行为、检测行为还是响应行为，都要消耗时间，因而可以用时间尺度来衡量一个体系的能力和安全性。

信息保障技术框架(IATF)模型

Information Assurance Technical Framework ，IATF



IATF模型

- IATF是由美国国家安全局组织专家编写的一个全面描述信息安全保障体系的框架，它提出了信息保障时代信息基础设施的全套安全需求。IATF创造性的地方在于，它首次提出了信息保障依赖于人、操作和技术来共同实现组织职能/业务运作的思想，对技术/信息基础设施的管理也离不开这三个要素。IATF认为，稳健的信息保障状态意味着信息保障的策略、过程、技术和机制在整个组织的信息基础设施的所有层面上都能相以实施。

IATF模型

- 人，借助技术的支持，实施一系列的操作过程，最终实现信息保障目标，这就是IATF最核心的理念。在明确了信息保障的三项要素之后，IATF定义了实现信息保障目标的工程过程和信息系统各个方面的安全需求。在此基础上，对信息基础设施就可以做到多层防护，这样的防护被称为“深度保护战略Defense-in-Depth Strategy”。
- 在关于实现信息保障目标的过程和方法上，IATF 论述了系统工程、系统采购、风险管理、认证和鉴定以及生命周期支持等过程，对这些与信息系统安全工程(ISSE）活动相关的方法学作了说明。这就为我们指出了一条较为清晰的建设信息保障体系的路子。

IATF模型

- 为了明确需求，IATF定义了四个主要的技术焦点领域：保卫网络和基础设施，保卫边界，保卫计算环境和为基础设施提供支持，这四个领域构成了完整的信息保障体系所涉及的范围。在每个领域范围内，IATF都描述了其特有的安全需求和相应的可供选择的技术措施。
- 无论是对信息保障体系的获得者，还是对具体的实施者或者最终的测评者，这些都有很好的指导价值。

主要内容

第一部分 理论上怎么说？

第二部分 实际中怎么做？

第三部分 风险预测与风险评估

第四部分 安全策略的制定与实施

信息安全策略

“信息资源保护项目的成功依赖于所采用的策略，也依赖于管理层对自动系统中信息的保护态度。作为策略的制定者，应当定好基调，强调信息安全在机构中所产生的重要作用。制定者的主要责任就是为机构制定信息资源安全策略以达到下述目标：减少风险，遵从法律和规则，确保机构运作的连续性、信息完整性和机密性。”

——1989年，美国国家标准与技术研究院（NIST）在《Special Publication SP500-169》的《信息资源保护执行指南》

信息安全策略

“从信息安全领域中实际发生的每件事来看，信息安全策略的核心地位变得越来越明显。例如，除非有一套条款清晰的信息安全策略，否则系统管理员将不能安全地安装防火墙。这些策略规定了所允许的信息传输服务类型、怎样鉴定用户身份以及怎样记录与安全有关的事件。如果没有制定信息安全策略，就不能有效地开展信息安全培训和意识提升工作，因为策略提供了培训和意识培养材料中所要使用的基本内容。”

——Charles Cresson Wood的《Information Security Policies Made Easy》

信息安全策略的设计与制定

- 确定安全策略的结构；
- 风险评估/分析或审计；
- 制定信息安全策略的原则：
  - ❑先进的网络安全技术；
  - ❑严格的安全管理；
  - ❑严格的法律、法规规范。
- 确定安全策略的范围。

信息安全策略的设计与制定（续）

原则：

多层防护、管防结合；

风险分散、灵活配置；

优化管理、可扩展性；

主动、被动防御结合；

成熟产品、易于实施；

易于管理、易于维护；

难点：

确定优先次序；

内部策略；

所有权的确定；

编写本身的困难；

法律依据：

技术标准；

行业规范；

法律法规；

编写安全策略的几个简单原则

今天的好策略比明年的伟大策略要更好！

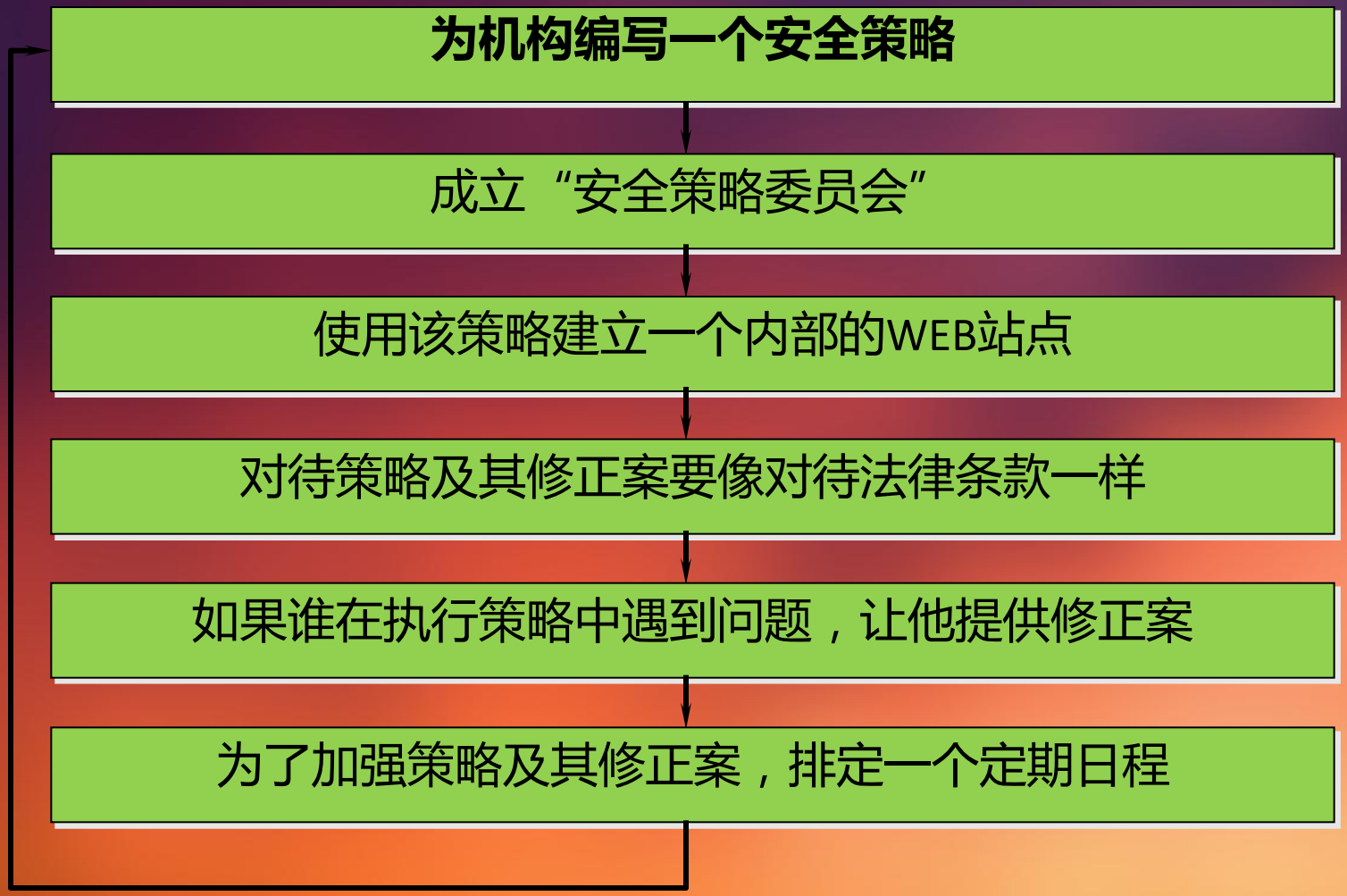
薄弱的但广为分发的策略比没有人阅读的强壮的策略要更好！

容易理解的简单策略要比没有人看的复杂策略要更好！

有微小错误的策略比根本没有细节的策略要更好！

连续更新的活跃的策略比时间上过期而发展的策略要更好！

一种编写策略可行的方法



主要内容

第一部分 理论上怎么说？

第二部分 实际中怎么做？

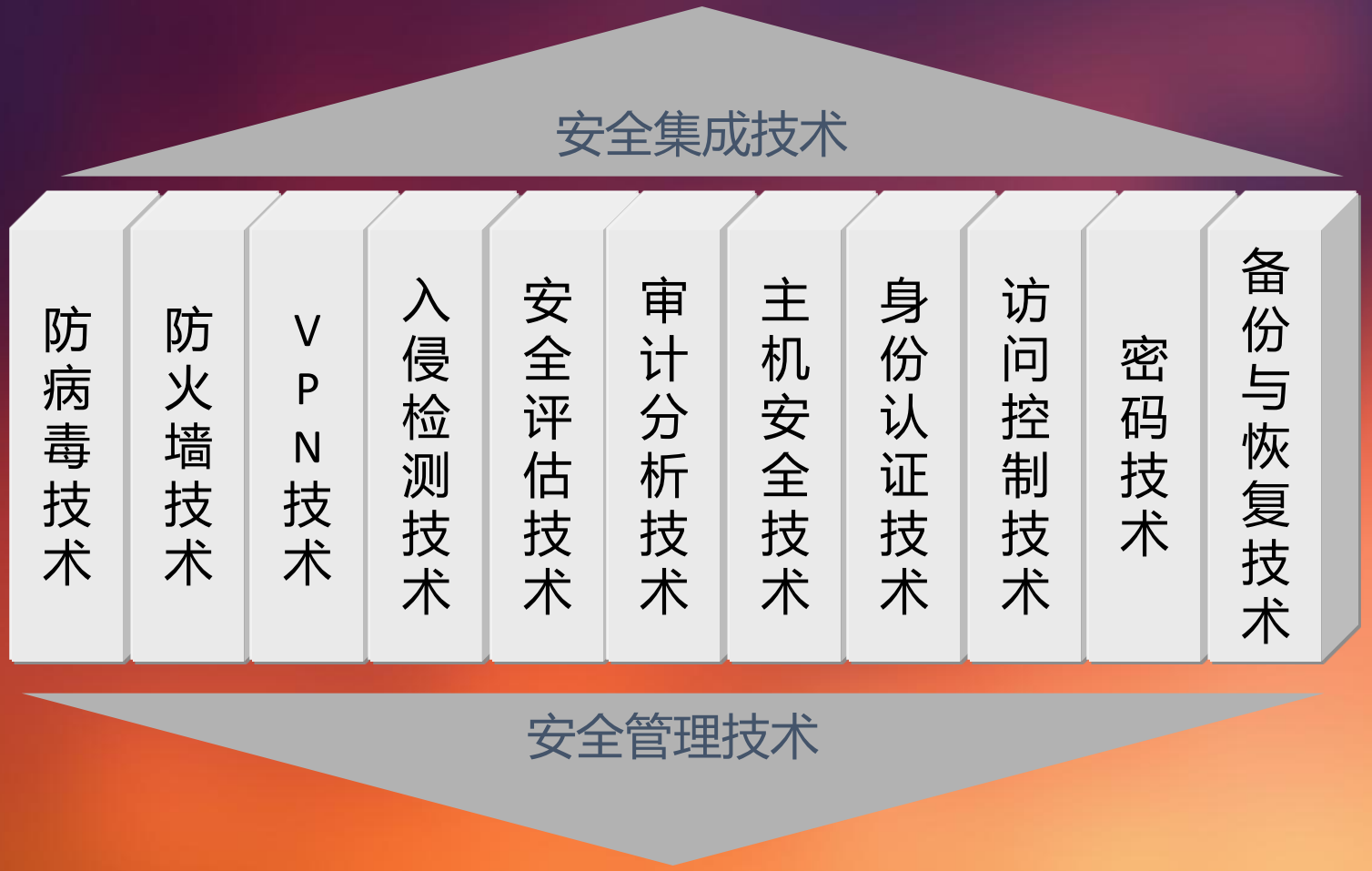
第三部分 信息安全策略的规划

第四部分 安全策略的制定与实施

确定安全策略保护的对象

- 信息系统的硬件和软件；
- 信息系统的数据：
  - 数据处理
  - 个人数据
- 人员。

确定安全策略中所使用的主要技术



主要内容

第一部分 理论上怎么说？

第二部分 实际中怎么做？

第三部分 信息安全策略的规划

第四部分 安全策略的制定与实施

制定安全策略的考虑

- 物理层安全
- 系统层安全
- 网络层安全
- 应用层安全
- 管理层安全

1. 通信线路的安全
2. 物理设备的安全
3. 机房的安全

制定安全策略的考虑(续）

- 物理层安全
- 系统层安全
- 网络层安全
- 应用层安全
- 管理层安全

这一层次的安全问题来自于网络内使用的操作系统：WINDOW2000/NT\NETWARE、LINUX等，系统层的安全性问题表现在两方面：

- 操作系统本身的不安全
- 对操作系统的配置不合理

制定安全策略的考虑（续）

- 物理层安全
- 系统层安全
- 网络层安全
- 应用层安全
- 管理层安全

该层次的安全问题主要体现在网络信息的安全性，包括：

- 网络层身份认证；
- 网络资源的访问控制；
- 数据传输的保密及完整性；
- 远程接入的安全；
- 域名系统的安全；
- 路由系统的安全；
- 入侵检测的手段等。

制定安全策略的考虑（续）

- 物理层安全
- 系统层安全
- 网络层安全
- 应用层安全
- 管理层安全

该层次的安全考虑所采用的应用软件和数据的安全性，包括：

- 数据库软件；
- WEB服务；
- 电子邮件系统等；
- 此外还包括病毒对系统的威胁。

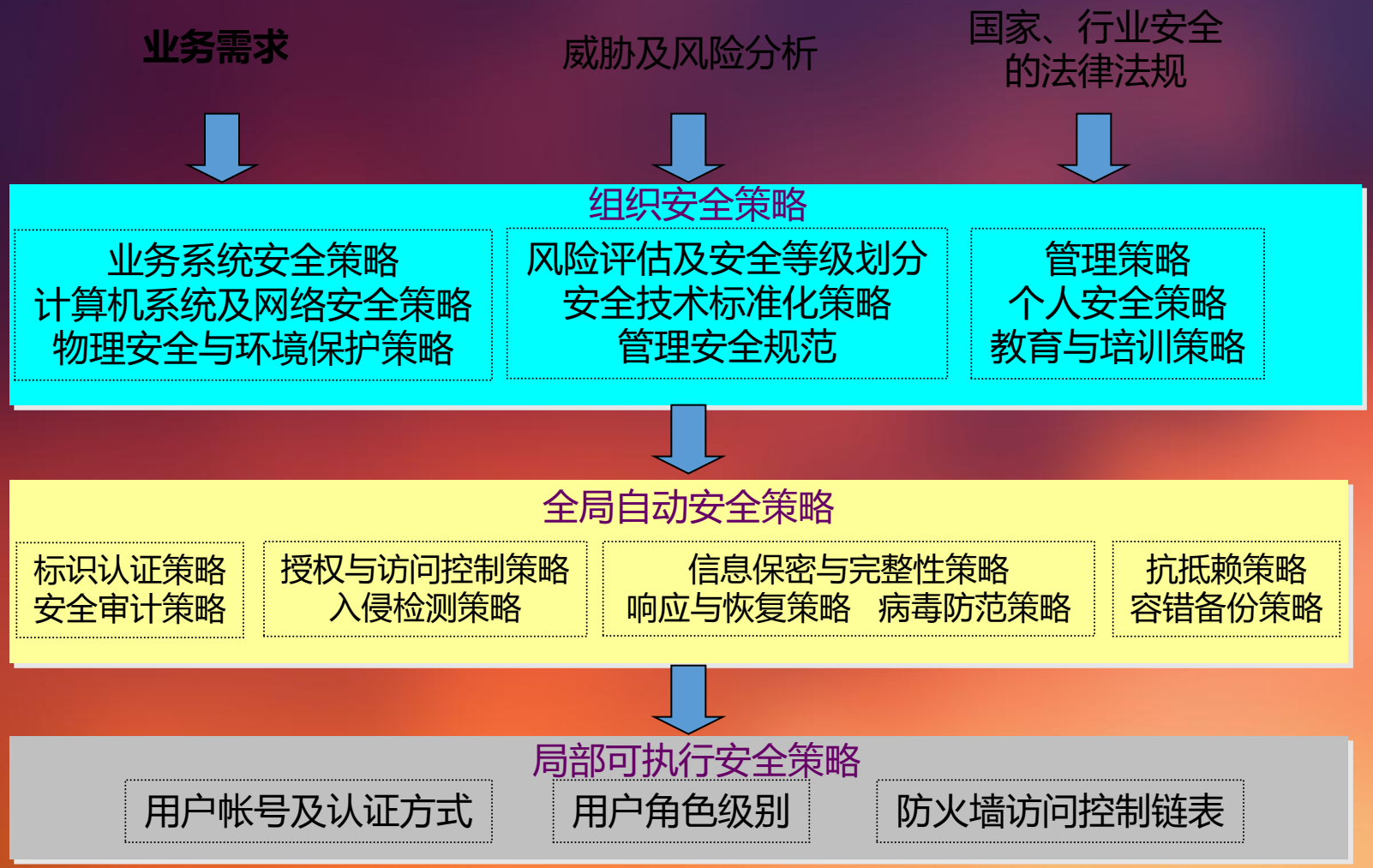
制定安全策略的考虑（续）

- 物理层安全
- 系统层安全
- 网络层安全
- 应用层安全
- 管理层安全

安全管理包括：

- 安全技术和设备的管理；
- 安全管理制度；
- 部门与人员的组织规则等。

安全策略的制定


业务需求
威胁及风险分析
国家、行业安全的法律法规
组织安全策略
业务系统安全策略
计算机系统及网络安全策略
物理安全与环境保护策略
风险评估及安全等级划分
安全技术标准化策略
管理安全规范
管理策略
个人安全策略
教育与培训策略
全局自动安全策略
标识认证策略
安全审计策略
授权与访问控制策略
入侵检测策略
信息保密与完整性策略
响应与恢复策略
病毒防范策略
抗抵赖策略
容错备份策略
局部可执行安全策略
用户帐号及认证方式
用户角色级别
防火墙访问控制链表

安全策略的具体组成

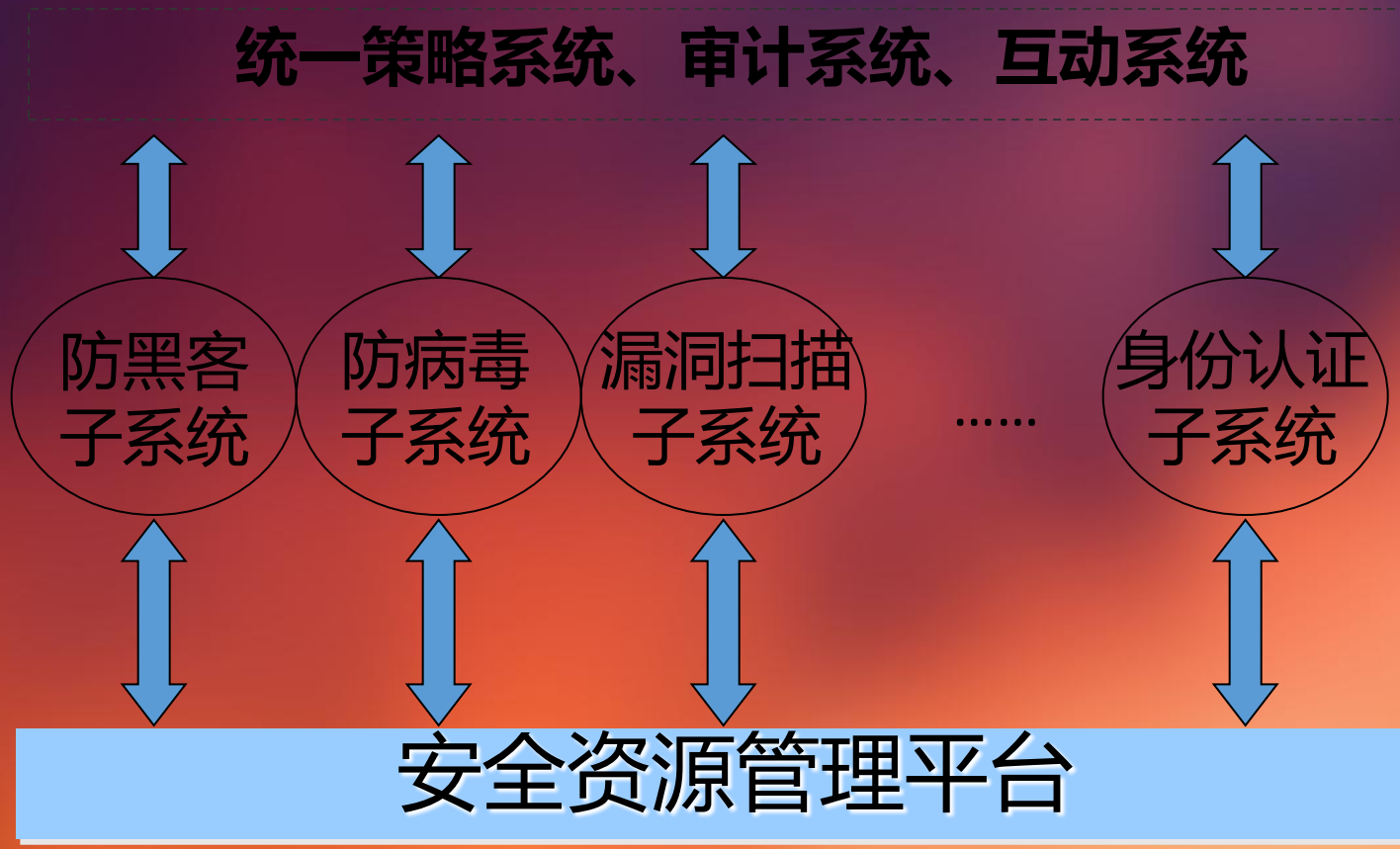
环境安全策略	数据访问控制安全策略	数据加密与数据备份策略
病毒防护策略	系统安全策略	身份认证与授权策略
互联网安全策略	紧急响应、事故处理、灾难恢复策略	口令管理策略
安全教育策略	维护策略	复查审计策略

构建安全资源管理平台

- **建立在一个强有力的认证系统和信息加密系统之上，具有以下特点：**
  - **从地域上，对各关键路径上的监测系统，对包括从桌面机到服务器各关键系统的安全状态进行监控；**

- 覆盖多个层面：防黑客、病毒、私密系统、认证系统；
- 从时间上掌握最近一个时段的网段状况分析数据，支持实时方面更准确地分析和判断；
- 进行统一的安全策略管理及实施：木桶原理及国家计算机系统保护等级制度。

构建安全资源管理平台（续）



安全策略实例分析：口令管理策略

网络服务器密码口令的管理

- **服务器的口令和密码，由部门负责人和系统管理员商议确定，必须两人同时在场设定。**
- **服务器的口令须部门负责人在场时要由系统管理员记录封存。**
- **密码及口令要定期更换（视网络具体情况），更换后系统管理员要销毁原记录，将新密码或口令记录封存。**
- **如发现密码及口令有泄密迹象，系统管理员要立刻报告部门负责人，有关部门负责人报告安全部门，同时要尽量保护好现场并记录，需接到上一级主管部门批示后再更换密码和口令。**

安全策略实例分析：口令管理策略

用户密码及口令的管理

- **对于要求设定密码和口令的用户，由用户方指定负责人与系统管理员商定密码及口令，由系统管理员登记并请用户负责人确认（签字或电话通知），之后系统管理员设定密码及口令，并保存用户档案。**
- **当用户由于责任人更换或忘记密码、口令时要求查询密码、口令或要求更换密码及口令的情况下，需向网络服务管理部门提交申请单，有部门负责人或系统管理员核实后，对用户档案做更新记载。**
- **如果网络提供用户自我更新密码及口令的功能，用户应自己定期更换密码及口令，并设专人负责保密和维护工作。**

安全策略实例分析：口令管理策略

- 所有活动账号都必须有口令保护。
- 生成账号时，系统管理员应分配给合法用户一个唯一的口令，用户在第一次登录时应更改口令。
- 口令必须至少要含有8个字符。
- 口令必须同时含有字母和非字母字符。
- 必须定期用监控工具检查口令的强度和NG长度是否合格。
- 口令不能和用户名或者登录名相同。
- 口令必须至少60天更改一次。
- 禁止重用口令。
- 必须保存至少12个历史口令。
- 口令不能通过明文电子邮件传输。
- 所有供应商的默认口令必须更改。
- 用户应在不同的系统中使用不同的口令。
- 当怀疑口令泄漏时必须予以更改。
- 应该控制登录尝试的频率

组织机构管理策略

对象	特征	权限	管理手段	监督机制
组织机构	一级管理组织			
	二级管理组织			
	三级管理组织			
	四级管理组织			

人员管理策略

对象	特征	权限	管理手段	监督机制
人员管理	安全官员			
	安全咨询专家			
	系统管理员			
	专项管理员			
	操作员			
	一般人员			
	内部其他人员			
	外部人员			

设备管理策略

对象	特征	权限	管理手段	监督机制
设备管理	国际通信系统			
	国内通信系统			
	内部网			
	计算机系统			
	各种专用服务器			
	各种专用网络设备			
	各种专用业务设备			
	其他设备			

独立服务器系统管理策略

对象	特征	权限	管理手段、产品	监督机制
系统管理	硬件设备			
	系统版本			
	用户管理			
	口令管理			
	弱点漏洞管理			
	日志、监控、预警			
	敏感数据管理			
	身份认证机制			

安全性分析和评估管理策略

对象	特征	分析策略	管理手段、产品	监督响应机制
弱点漏洞管理	服务器—1			
	服务器—n			
	路由器—1			
	路由器—n			
	交换机—1			
	交换机—n			
	防火墙—1			
	防火墙—n			

监控、预警、响应管理策略

对象	特征	分析策略	管理手段、产品	监督响应机制
监控预警响应管理	服务器—1			
	服务器—n			
	路由器—1			
	路由器—n			
	交换机—1			
	交换机—n			
	防火墙—1			
	防火墙—n			

安全产品采购开发管理策略

对象	特征	分析策略	管理手段、产品	监督响应机制
产品采购开发管理	服务器			
	路由器			
	交换机			
	防火墙			
	应用系统			
	安全分析工具			
	预警响应系统			
	加密算法			

Thank you