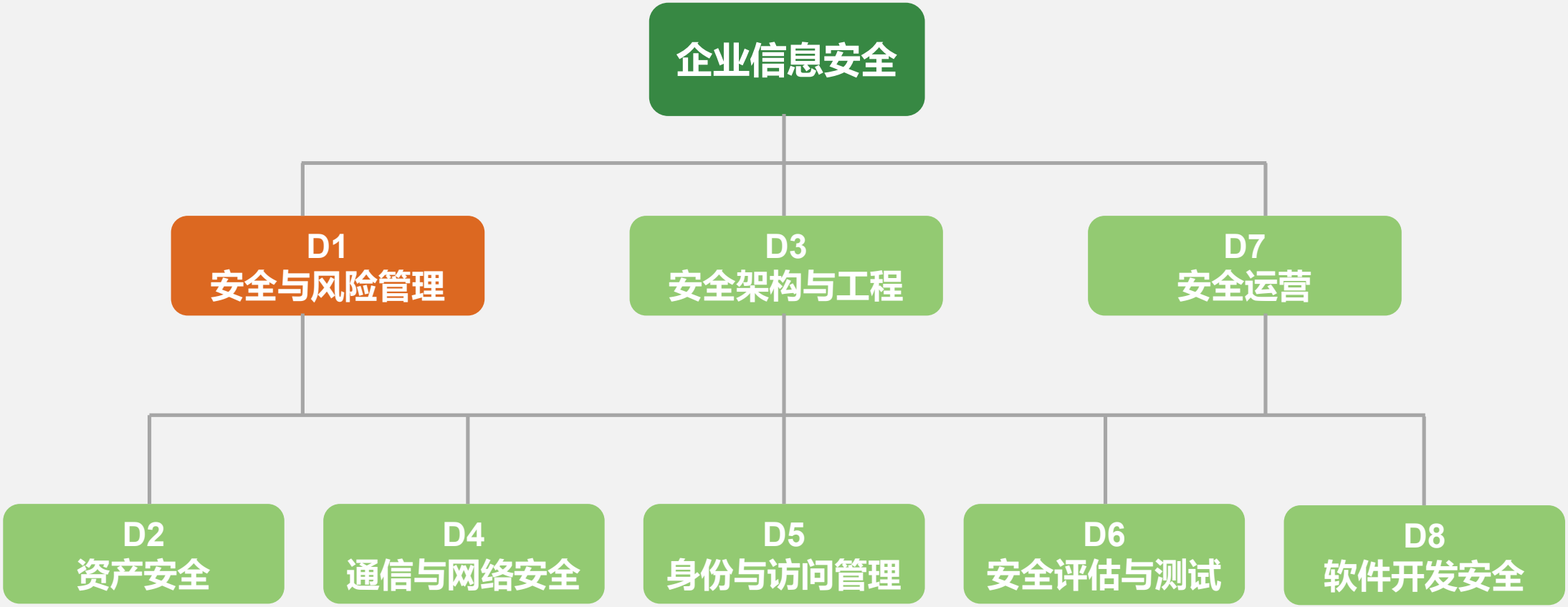

铭学在线课堂-CISSP认证
D1-安全和风险管理
铭记初心，实现自我

知识架构



CBK学习目标

- 理解信息安全的基本要素，以及延伸到安全治理与合规领域的相关概念
- 了解相关法律法规、道德规范
- 掌握和理解如何构建统一的安全策略和程序
- 理解业务连续性计划相关概念
- 理解风险管理的相关概念，以及在此基础上展开的威胁建模、如何将风险管理整合到企业相关活动中

本章知识架构

本节内容

1.1 理解和应用机密性、完整性和可用性的概念

- A、信息安全的定义
- B、信息安全的核心原则
- C、其它相关安全概念

信息安全的定义

- 业务视角：采取措施保护信息资产，使之不因偶然或者恶意侵犯而遭受破坏、更改及泄露，保证信息系统能够连续、可靠、正常地运行，使安全事件对业务造成的影响减到最小，确保组织业务运行的连续性。
- 安全视角：安全的核心目标是为关键资产提供可用性、完整性和机密性（AIC 三元组）保护

安全核心原则：CIA

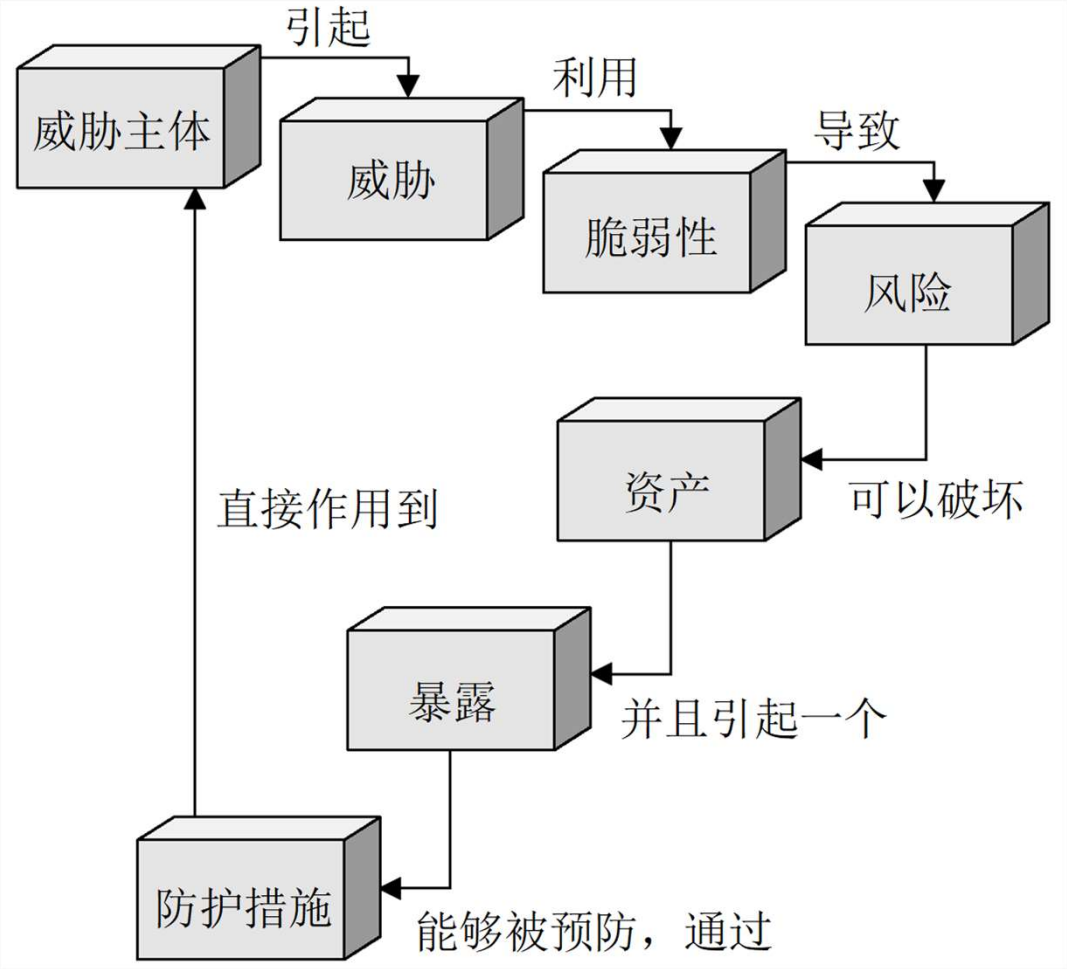
这三方面同等的重要，但需要平衡。

其它相关安全概念

- 帕克里安（Parkerian Hexad）六元组架构：
  - ✓机密性（Confidentiality）
  - ✓完整性（Integrity）
  - ✓可用性（Availability）
  - ✓真实性（Authenticity）
  - ✓实用性（Utility）
  - ✓拥有或控制（Possession or control）

其它相关安全概念

- 描述安全问题方面的概念：
  - ✓脆弱性（vulnerability）
  - ✓威胁（threat）
  - ✓风险（risk）
  - ✓暴露（exposure）
- 描述安全控制方面的概念
  - ✓按类型分：行政类、技术类、物理类
  - ✓按功能分：预防性、检测性、纠正性、威慑性
    恢复性、补偿性、指引性



本节内容

1.2 评估和应用安全治理原则

- A、信息安全治理的定义
- B、信息安全治理的重要性
- C、通过制定和实施信息安全规划达到安全目标
- D、组织中角色、责任和评价
- E、开发、文档化和实施安全策略、标准、指南、基线和措施
- F、制定和执行人员安全管理

信息安全治理的定义

- 信息安全治理
  - ✓一套信息安全解决方案和相互紧密联系的管理方法
  - ✓一个框架：定义目标、协调、实施和监督涉及所有安全相关方面。
- 管理 VS. 治理
- 企业治理 VS. IT治理 VS. 安全治理
- 保障业务的持续运行和向更好的方向发展

信息安全治理的重要性

- 信息安全必须存在并支撑着组织的业务架构和目标
- 管理层
- 安全专家

企业管理层在安全治理方面关注什么？

设定策略和战略的方向

提供安全活动资源

指派管理责任

设定优先级

支持必须的改变

定义与风险评估相关文化

从内外部审计获取保障

坚持安全投资被度量和听取项目有效性的汇报

安全专业人员在安全治理方面关注什么？

安全专业人员要认识到	安全专业人员要做哪些工作	开展这些工作的同时
• 组织的愿景、任务和目标 • 组织在其生命周期中的安全问题 • 安全角色和责任 • 信息安全策略 • 法律、法规和道德	• 建立完整、有效的安全规划 • 开发和执行信息安全策略 • 建立业务连续性和灾难恢复计划 • 人员安全管理 • 信息安全风险管理	• 需要和管理层建立联系，以确保安全目标的实现。

安全管理计划

为什么?

安全管理计划能确保安全**策略**的适当创建、实现和实施

如何做?

安全管理计划是由**许多实体构成的框架**，包括逻辑、管理和物理的保护机制、流程、业务过程和人

1.公司安全的使命和目标

2.安全体系总体**模型**

3.安全现状

4.关键举措和重点工作

5.实施策略选择

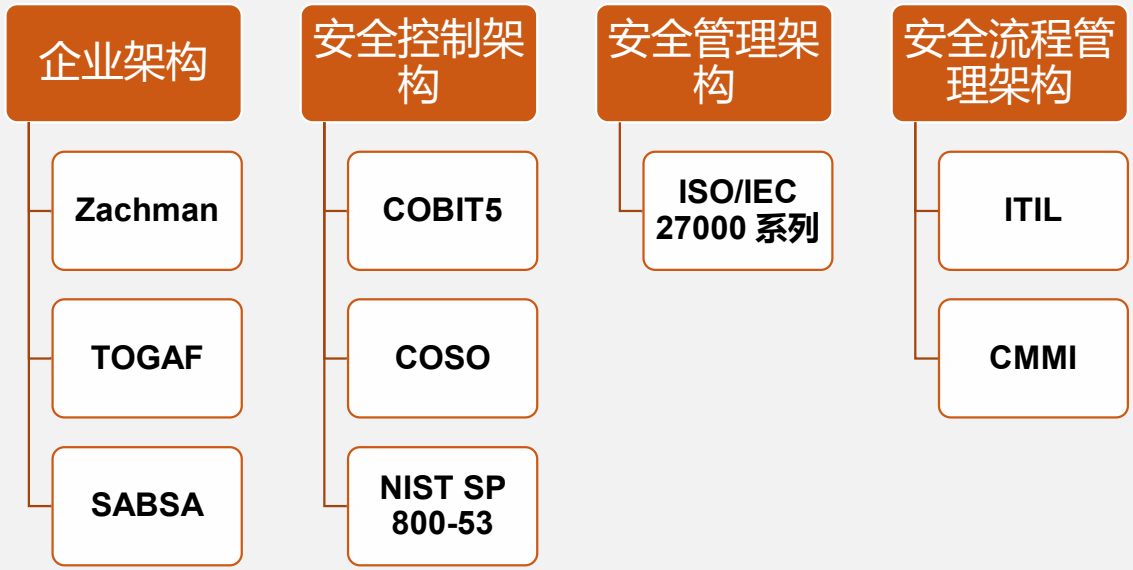
6.工作计划

7.建设实施

8.安全运营和持续改进

安全框架

- 企业架构
  - ✓ Zachman
  - ✓ TOGAF
  - ✓ SABSA
- 安全控制架构
  - ✓ COBIT5
  - ✓ COSO
  - ✓ NIST SP 800-53
- 安全管理架构
  - ✓ ISO/IEC 27000 系列
- 安全流程管理架构
  - ✓ ITIL
  - ✓ CMMI



重要的安全角色和责任

高级管理者

安全专家

数据所有者

数据监管者

用户

审计人员

应尽关注和应尽职责

应尽职责

（Due Diligence）

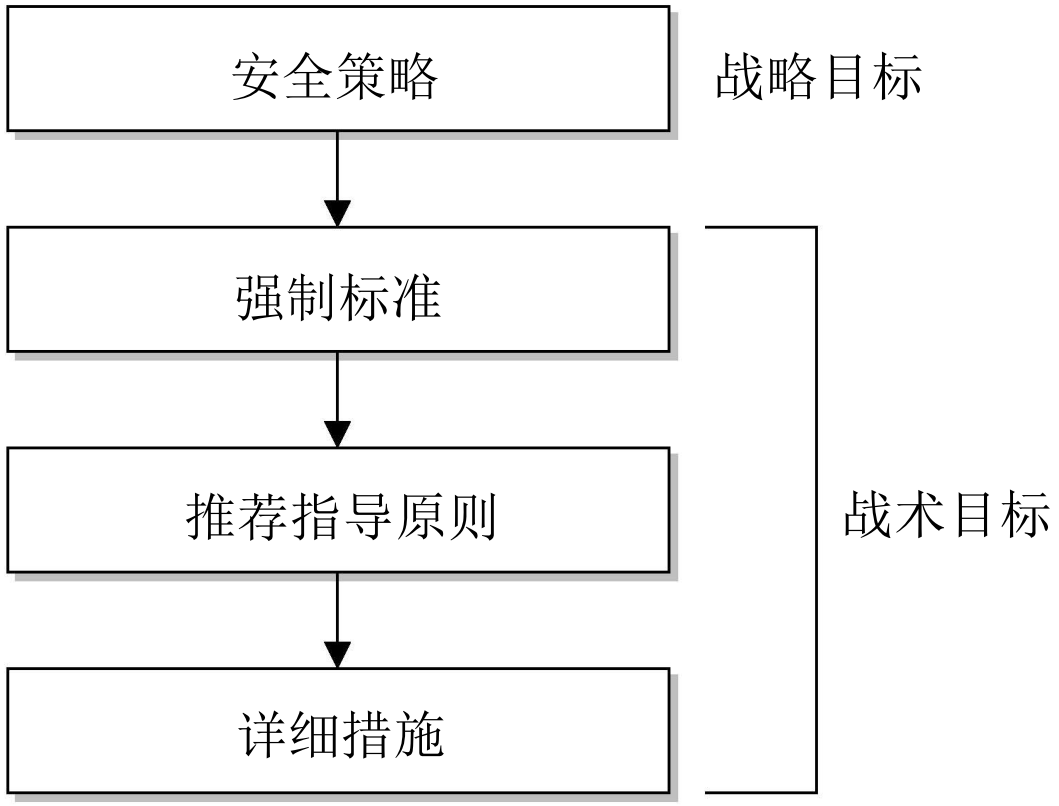
应尽关注

（Due Care）

安全策略概述

安全策略的分层

- 战略目标
  - ✓安全策略|安全方针
- 战术目标
  - ✓标准
  - ✓基线
  - ✓指南
  - ✓详细措施



人员安全管理---入职

- 背景检查（Background Check）
  - ✓入职
  - ✓转入重要岗位
- 保密协议

人员安全管理---在职

- ✓职责分离（Separation of duties）
- ✓工作轮换（Job rotation）
- ✓强制度假（Mandatory vacation）
- ✓须知原则（Need to Know）
- ✓最小特权原则（The Principle Of Least ）
- ✓保密协议（Non Disclosure Agreement）
- ✓非竞争协议（Non Compete Agreement）
- ✓监控（Monitoring）

人员安全---解雇

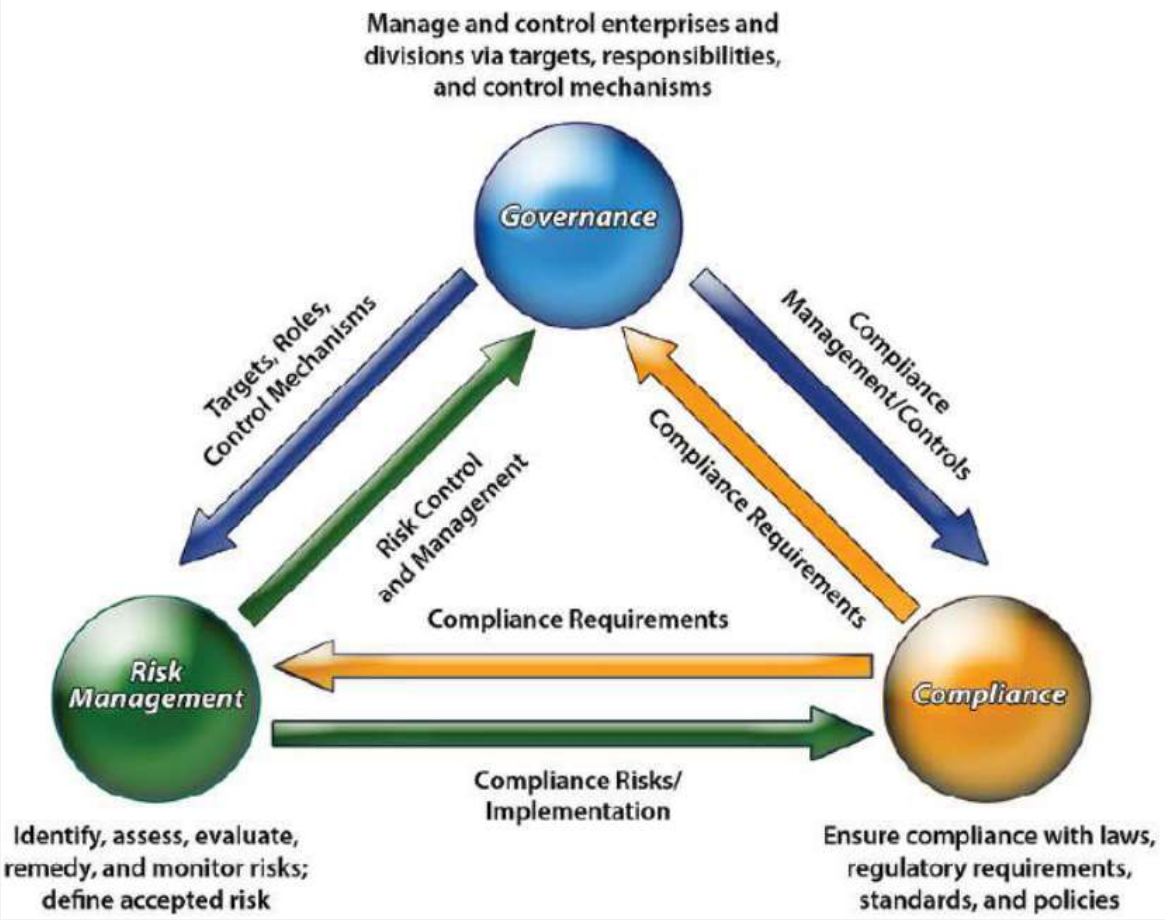
- 公司应当制订一组特定的措施来管理每种解雇事件，例如：
  - ✓ 被解聘员工必须在一名经理或保安的监督下立即离开公司。
  - ✓被解聘员工必须上交所有身份徽章或钥匙，要求完成离职谈话，并返还公司的供应品。
  - ✓公司应立即禁用或修改被解聘员工的账户和密码。

本节内容

1.3 法律、合规和道德

- A、GRC概述
- B、知识产权和许可
- C、隐私相关法律
- D、(ISC)2 道德规范

GRC概述



三种主要的法律类别

- 在我们的法律系统中有三种主要的法律类别发挥着作用
- 每一种法律都涵盖了许多不同的环境，并且在不同的类别下对于违法的处罚方式也不相同
  - ✓刑法
  - ✓民法
  - ✓行政法

知识产权

版权

商标

专利

商业秘密

许可证

隐私相关法律

欧盟《通用数据保护条例》

GDPR

经济合作与发展组织

OECD

(ISC)2 道德准则

- (ISC)2道德规范准则：
  - ✓保护社会、公共利益、必要的公共信任和信心、以及基础设施。
  - ✓行为得体、诚实、公正、负责和遵守法律。
  - ✓为委托人提供尽职的和胜任的服务工作。
  - ✓发展和保护职业声誉。

本章知识架构

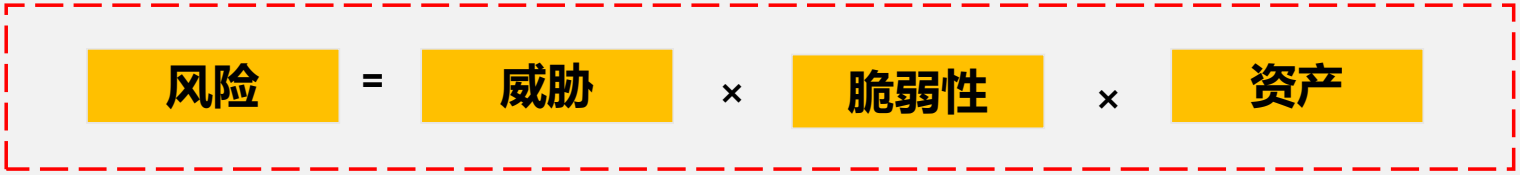
本节内容

2.1 风险和风险管理

- A、风险概述
- B、风险相关术语
- C、风险管理概述和重要性
- D、风险管理策略和团队、职责
- E、风险管理框架和步骤

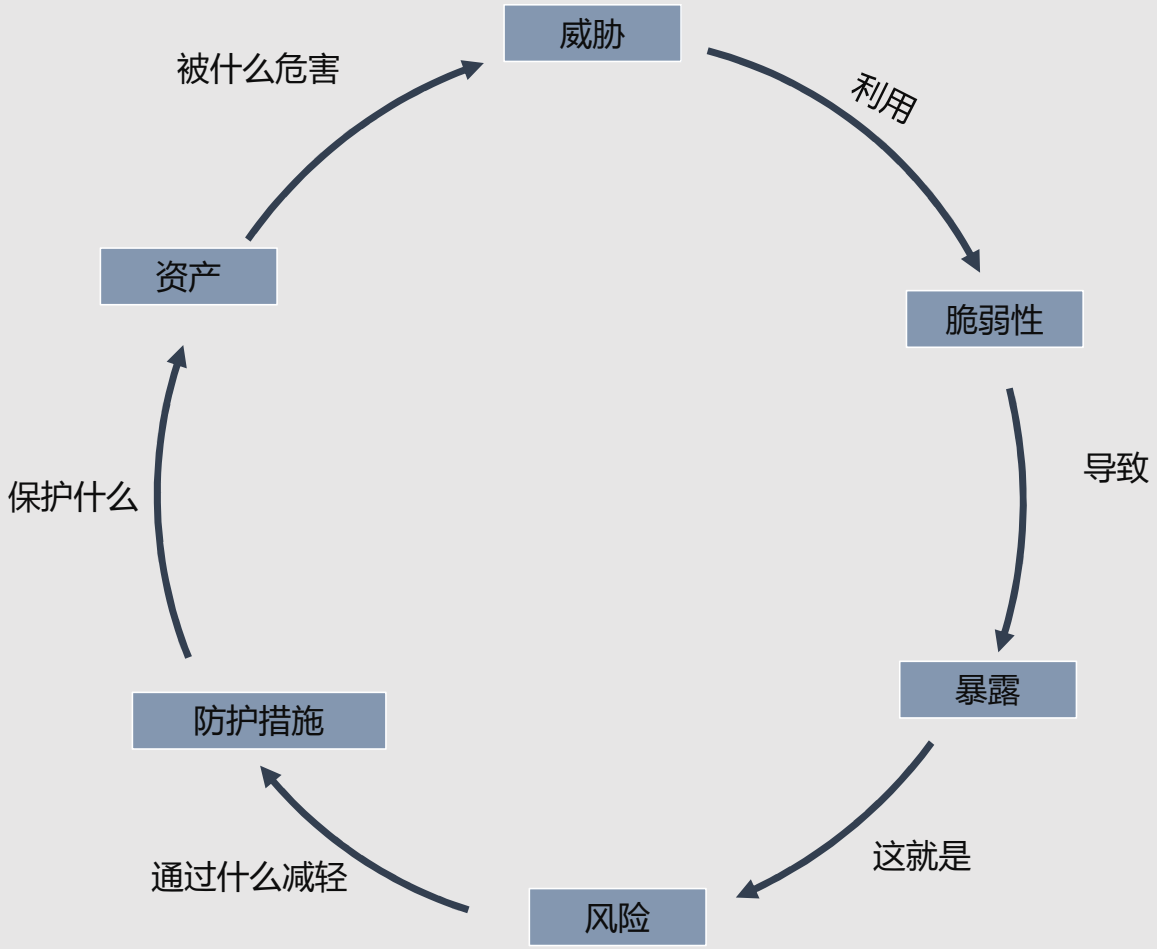
风险概述

- 风险（Risk）在信息安全领域就是指信息资产遭受损坏并给企业带来负面影响的潜在可能性。
- 三层风险管理：组织层面、业务流程层面、信息系统层面
- 风险最常见的定义是：



风险相关术语

- 资产
- 资产价值
- 威胁
- 脆弱性
- 暴露
- 防护措施
- 攻击
- 破坏



风险管理概述和重要性

- 风险管理（Risk Management）：
  - ✓**识别风险**
  - ✓**评估风险**
  - ✓采取措施将风险**减少到和维持可接受水平**
- 风险管理的整个过程被用来制定和实施信息安全策略
- 风险管理是信息安全管理的核心内容

风险管理策略和团队、职责

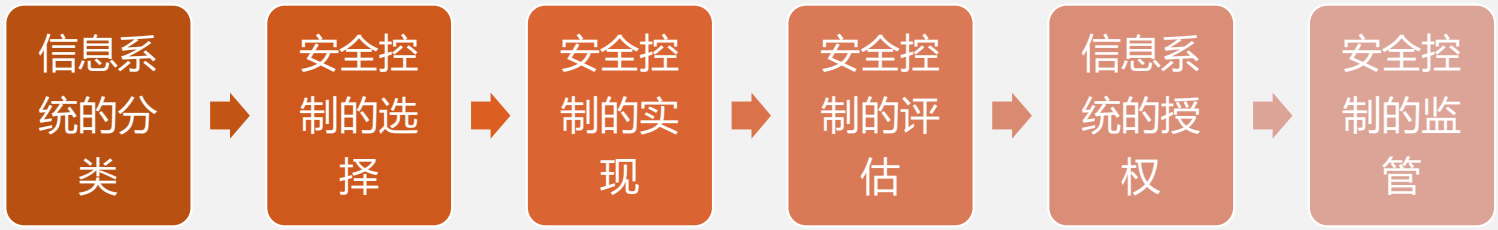
- 信息安全风险管理（Information System Risk Management，ISRM）策略包括以下内容：
  - ✓ISRM团队的目标
  - ✓公司可接受的风险级别及其定义
  - ✓风险识别的形式化过程
  - ✓ISRM策略与组织的战略规划过程之间的联系
  - ✓ISRM的职责以及履行这些职责的角色
  - ✓风险和内部控制之间的映射关系
  - ✓为响应风险分析而改变员工行为和资源分配的方式
  - ✓风险与业绩目标和预算之间的映射关系
  - ✓监控控制效率的主要指标

风险管理策略和团队、职责

- ISRM团队成员并非由专门从事风险管理工作的员工组成，但一般一个组织可能只有一名员工负责ISRM，或者拥有一个协同合作的ISRM 团队
- ISRM 团队的总体目标在于以最低预算确保公司安全，主要的工作内容和职责包括：
  - ✓创建一个高级管理层支持的、明确的风险接受级别
  - ✓记录风险评估过程与措施
  - ✓识别和缓解风险的措施
  - ✓恰当使用由高级管理层分配的资源与资金。
  - ✓对所有与信息资产有关的员工进行安全意识培训
  - ✓……

风险管理框架和步骤

- 风险管理框架（Risk Management Framework）是有关如何评估、解决和监控风险的指南或方法
- NIST风险管理框架SP 800-37概述了以下应用于RMF流程的六步骤



本节内容

2.2 风险评估和处置

- A、风险评估定义
- B、风险评估团队
- C、风险评估流程
- D、定量和定性风险评估
- E、风险处置/响应

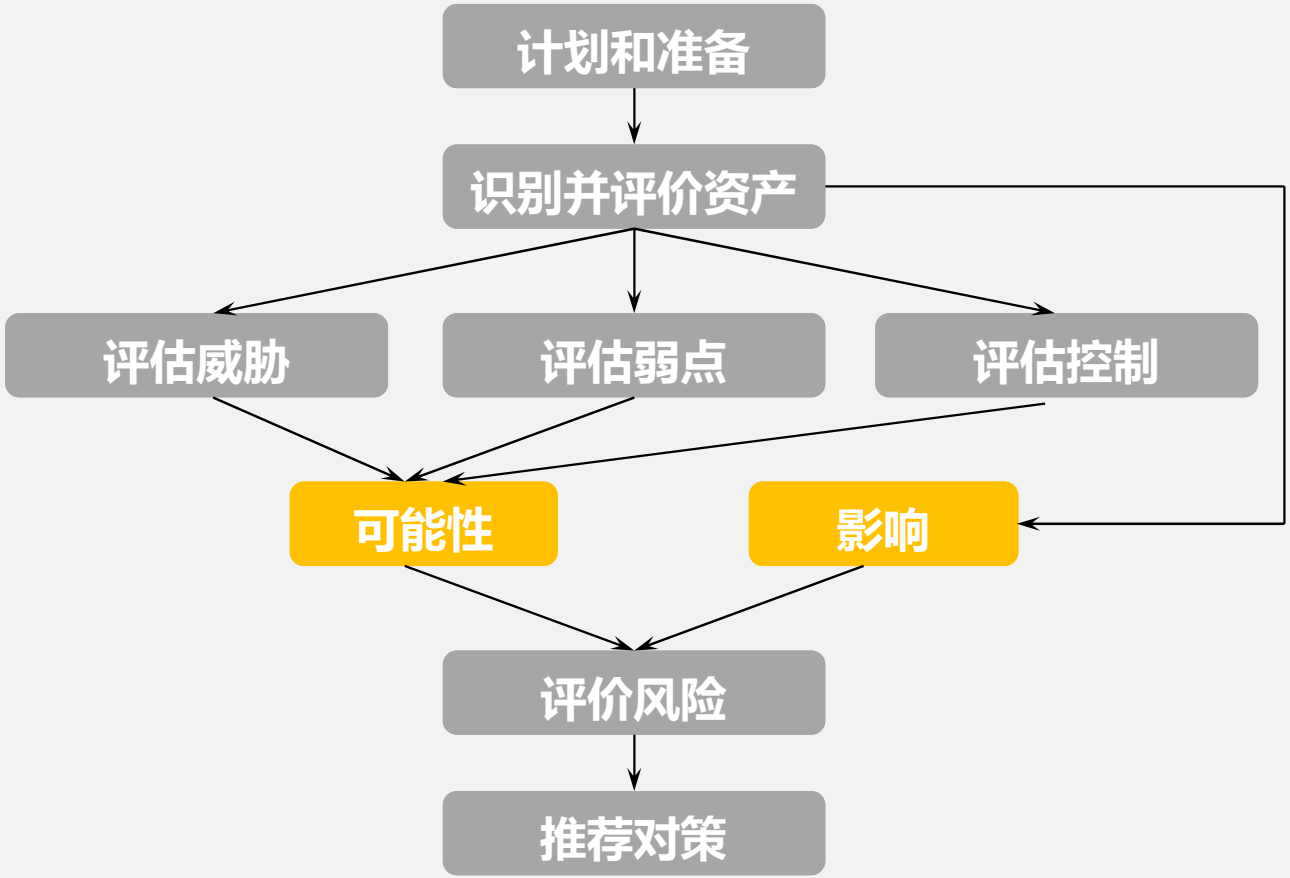
风险评估定义

- 风险评估（风险分析），实际上是一种风险管理工具，是一种能够识别脆弱性和威胁以及评估可能造成的损失，从而确定如何实现安全防护措施的方法
- 风险评估有4个主要目标：
  - ✓标识资产和它们对于组织的价值
  - ✓识别脆弱性和威胁
  - ✓量化潜在威胁的可能性及其对业务的影响
  - ✓在威胁的影响和对策的成本之间达到预算的平衡

风险评估团队

- 包括来自许多或全部部门的人员，以保证能够识别和处理所有的威胁
- 风险分析团队的成员：
  - ✓管理人员
  - ✓应用程序编程人员
  - ✓IT人员
  - ✓系统整合人员或运营部经理
  - ✓了解各自部门工作流程的人

风险评估流程



定量风险评估

- 定量分析使用风险计算来预测经济损失的程度以及每种威胁发生的可能性和影响：

SLE=资产价值 * EF

ALE=SLE * ARO

资产价值150000 * EF（25%）=37500

影响SLE：37500美元

可能性ARO：0.1

风险ALE=SLE * ARO=37500*0.1=3750

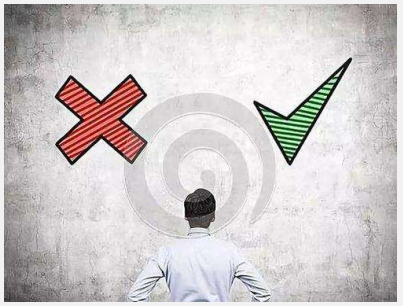
定性风险评估

- 定性方法将考查各种风险可能发生的场景，并基于不同的观点对各种威胁的严重程度和各种对策的有效性进行等级排列

可能性	后果				
	微不足道	很小	中等	很大	严重
几乎一定	中	高	高	天	天
很有可能	中	中	高	高	天
有可能	低	中	中	高	天
不太可能	低	中	中	中	高
几乎不可能	低	低	中	中	高

定量与定性的对比

- **定量方法的缺点**



✓计算更加复杂。管理层能够理解这些值是怎么计算出来的吗?

✓没有可供利用的自动化工具，这个过程完全需要手动完成。

✓需要做大量基础性的工作，以收集与环境相关的详细信息。

✓没有相应的标准。每个供应商解释其评估过程和结果的方式各不相同。

- **定性方法的缺点**

✓评估方法及结果相对主观。

✓无法为成本/收益分析建立货币价值。

✓使用主观衡量很难跟踪风险管理目标。

✓没有相应的标准。每个供应商解释其评估过程和结果的方式各不相同。

风险处置/响应

- 风险评估结果
- 风险处置/响应的基本方式有下列4种：

转移　规避　缓解　接受

- 一个公司实现安全对策的原因是将整体风险降低到一个可接受的级别

威胁×脆弱性×资产价值=总风险

(威胁×脆弱性×资产价值)×控制间隙=剩余风险

总风险–对策=剩余风险

本节内容

2.3 理解和应用威胁建模的概念和方法

- A、威胁建模定义
- B、威胁建模方法
- C、确定和图解潜在攻击
- D、执行降低分析
- E、优先级和响应

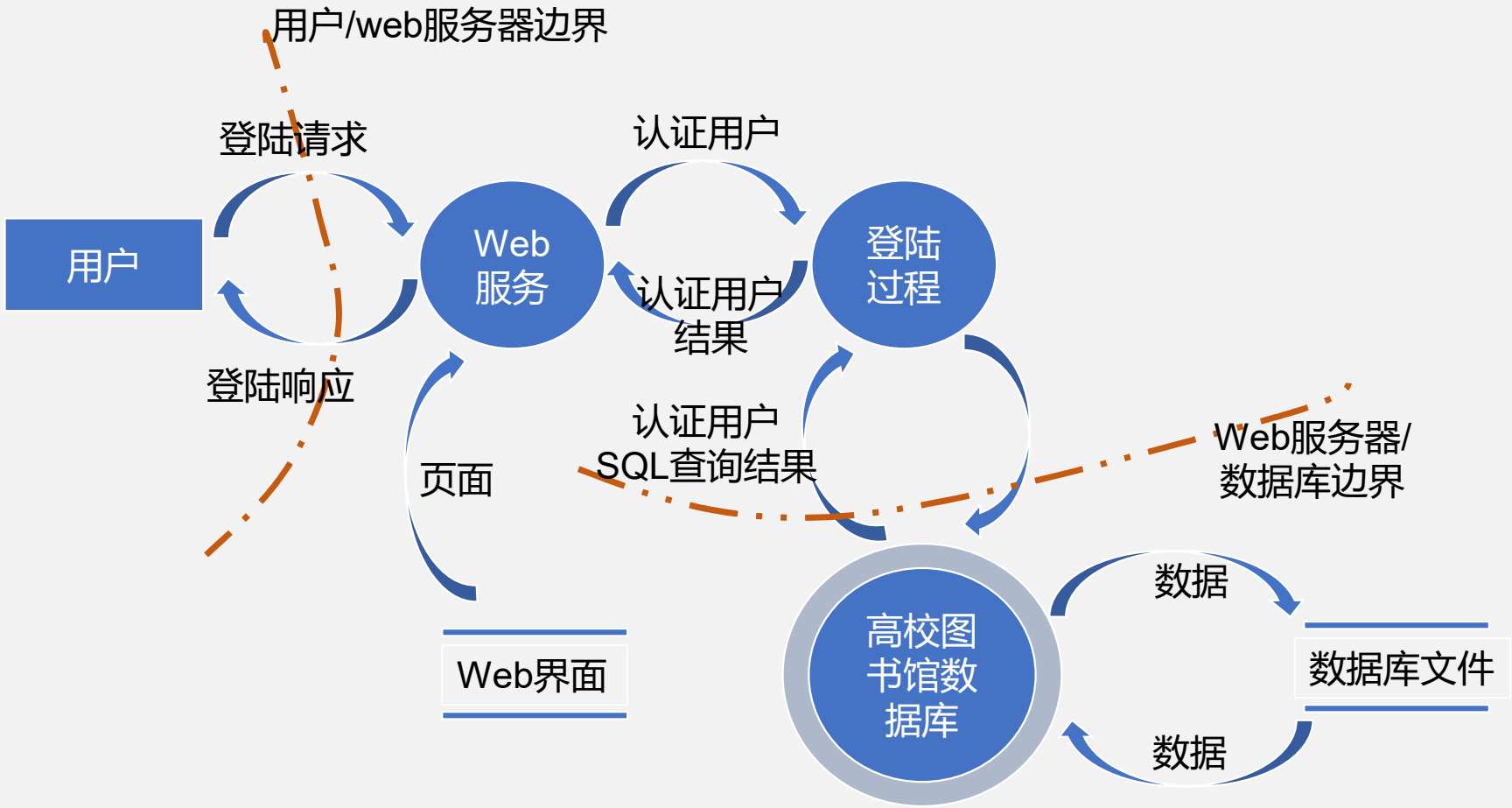
威胁建模定义

- 什么是威胁建模?
  - ✓潜在威胁被识别、分类和分析的安全流程
  - ✓目标：减少安全相关的设计和编码缺陷的数量、降低剩余缺陷的严重程度，最终减少风险
- 威胁建模的两种方法
  - ✓威胁建模的主动方法
  - ✓威胁建模的被动方法
- 威胁建模并不意味着是一个单独的事件

威胁建模定义

- 威胁建模有三种通用方法，安全专业人员需要理解这三种基本方法（approache）并将其应用到特定环境，其中：
  - ✓以攻击者为中心
  - ✓以资产为中心
  - ✓以系统（软件）为中心
- 有许多的威胁建模方法论（methodology），例如STRIDE、OCTAVE、NIST 800-154和 PASTA

确定和用图表示潜在攻击



消减分析

- 执行消减分析是为了分解应用程序、系统或环境
- 这个任务的目的是更好地理解产品逻辑及其与外部的交互元素

优先级和响应

- 概率×潜在损失的排名技术能产生一个代表风险严重性的编号
- 高/中/低的评级流程更加简单，每个威胁都会被标注为这三种优先级标签中的一种
- DREAD 评级系统，基于对每种威胁的5个主要问题的回答

潜在破坏 再现性 可利用性 受影响用户 可发现性

本节内容

2.4 将风险管理应用到供应链中

- A、供应链中的风险
- B、供应链风险管理

供应链中的风险

- 事实证明，攻击者对组织供应链的破坏，也会危害到组织自身的业务
- 常见的供应链中的风险有：
  - ✓知识产权方面的风险
  - ✓仿冒品方面的风险
  - ✓恶意代码
  - ✓未知谱系软件

供应链风险管理

- 供应链信息安全风险跨越了许多组织学科，包括采购，软件工程，软件保证和人员安全
- ISO 28000：2007，“供应链安全管理系统规范”，提供了管理供应链风险的广泛框架
- 将网络安全整合到供应链流程中的一些实践：
  - ✓现场评估
  - ✓公文交换和审核
  - ✓流程/策略审核
- 独立的第三方审计
- 合同、SLA

本节内容

2.5 创建和维护安全意识、培训和教育项目

- A、安全意识、培训、教育概述
- B、如何制定安全意识计划

安全意识概述

- 需要根据每个人在组织中的角色，在重点和深度上有所不同，其中：
  - ✓教育
  - ✓培训
  - ✓意识

如何制定安全意识计划

- 在风险级别的驱动下，该计划需要高级管理层的支持，同时要尊重组织的文化，利用可用资源以及满足组织对合规性的期望，主要步骤如下：
  - ✓现状评估
  - ✓需求评估
  - ✓战略和计划
  - ✓开发内容
  - ✓传递内容
  - ✓监控结果
  - ✓训练

本章知识架构

本节内容

3.1 业务连续计划概述

- A、业务连续管理概述
- B、业务连续性计划和灾难恢复计划
- C、业务连续计划过程和关键因素

业务连续性管理概述

- 为什么我们要做业务连续性
- DRP和BCP都面向计划开发，而业务连续性管理（BCM）是整体的管理过程，应该包括DRP和BCP
- BCM提供了一个框架，以整合恢复能力和有效应对的能力的方式，保护组织中主要利益相关者的利益
- BCM 的主要目的是允许该组织继续在不同条件下进行业务操作。

业务连续性与灾难恢复

- 什么是业务连续计划?
- 什么是灾难恢复计划?
- 业务连续性计划 VS. 灾难恢复计划

业务连续计划过程和关键因素

- **业务连续性计划过程包括以下四个主要步骤：**
  - ✓项目范围和计划编制阶段
  - ✓业务影响评估阶段
  - ✓连续性计划阶段
  - ✓批准和实现阶段

- **BCP的关键因素**
  - ✓BCP计划需要是一个活跃的实体，应当持续改进
  - ✓建立和维护当前连续性计划最关键的部分是管理层支持
  - ✓人员安全一直是最先考虑的

本节内容

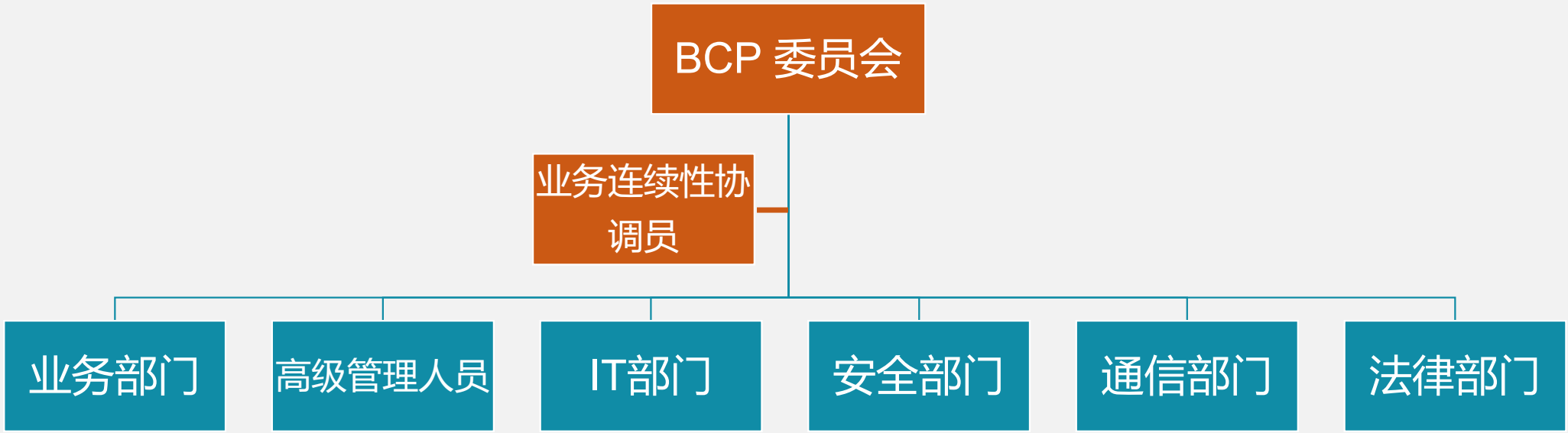
3.2 开发业务连续性计划项目

- A、项目范围和计划
- B、业务影响评估
- C、编制连续性计划
- D、批准和实现阶段

项目范围和计划

- 负责业务连续计划的人员首要职责之一是对业务组织进行分析，以识别与BCP流程具体有关的部门和个人。需要考虑：
  - ✓负责向客户提供核心服务业务的运营部门
  - ✓关键支持服务部门、设施和维护人员以及负责维护支持运营系统的其他团队
  - ✓负责物理安全的公司安全团队
  - ✓高级管理人员和对组织持续运营来说至关重要的其他人员

项目范围和计划



项目范围和计划

- 三个完全不同的BCP阶段所需的资源：
  - ✓BCP开发阶段
  - ✓BCP测试、培训和维护阶段
  - ✓BCP实现阶段
- BCP过程中消耗的最重要的资源之一是人力

项目范围和计划

- BCP项目的范围和目标方面都很清楚，但它并不是如此简单
- 应该了解公司业务的重点和方向
- 一个常见的异议
- 决定是否将组织的一个组成部分放到BCP范围以外以及如何放置通常会非常棘手

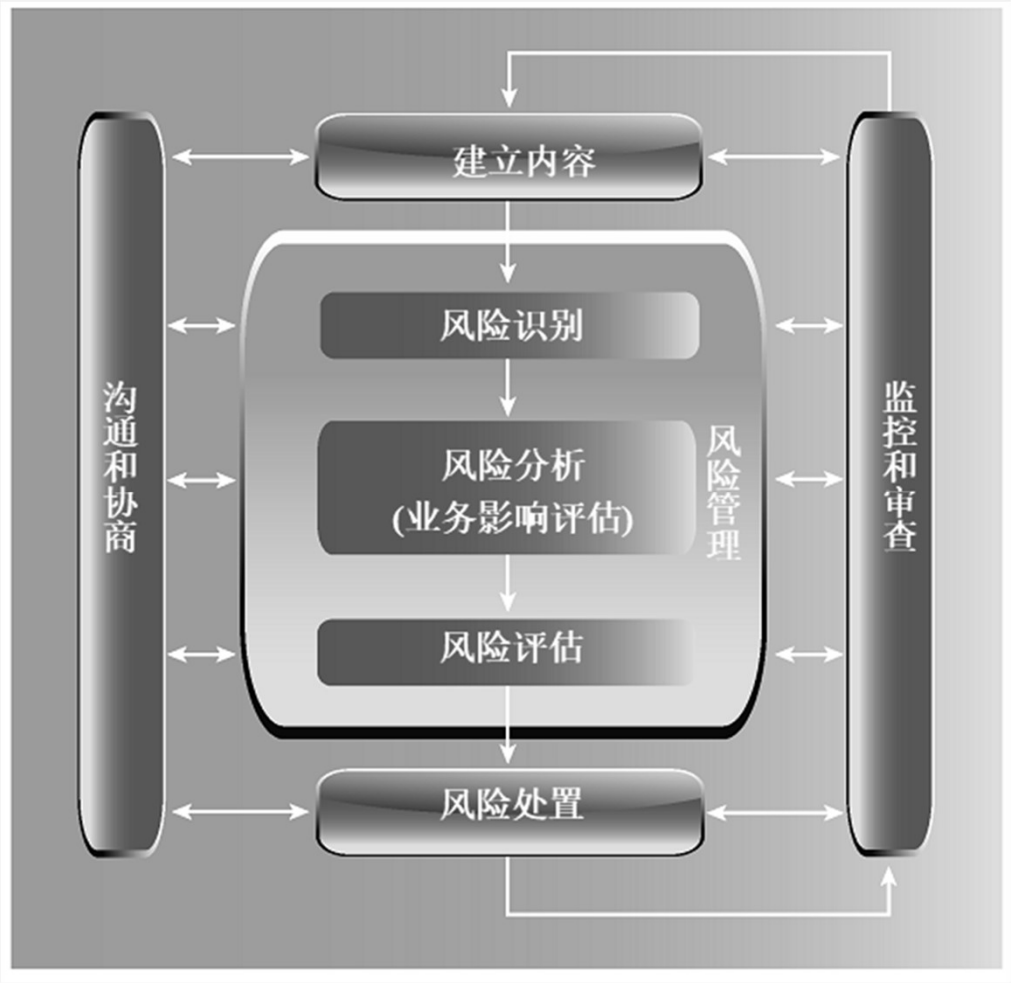
业务影响评估（BIA）

- BIA确定了能够决定组织持续发展的资源，以及对这些资源的威胁，并且还评估每种威胁实际出现的可能性以及出现的威胁对业务的影响。

定量决策	定性决策
• 数字和公式来作出评估决策	• 是非数值因素，通常以优先级类别（例如高、中、低）表示。

BIA 的步骤

使用标准的风险评估完成业务影响评估



编制连续性计划

- BCP开发的下一个阶段是编制连续性计划，这个阶段专注于连续性策略的开发和实现，包括的任务有：
  - ✓策略开发
  - ✓预备和处理

批准和实现阶段

- 一旦BCP团队完成连续性计划的编制工作，就应该当向最高管理层申请批准该计划。如果得以批准，就开始实施。主要包括的内容有：
  - ✓计划批准
  - ✓计划实施
  - ✓培训和教育
  - ✓BCP文档化


THANK YOU
感谢聆听
为客户提供优质学习服务