上海财经大学
SHANGHAI UNIVERSITY OF FINANCE AND ECONOMICS

会计信息系统安全风险管理

饶艳超 上海财经大学会计学院

raoyanchao@qq.com

- 学习目标
  - 熟悉会计信息系统面临的各类风险
  - 掌握分析识别系统面临的各类安全问题
  - 掌握系统安全需求分析方法
  - 掌握风险评估方法和技术
  - 熟悉并应用系统安全控制目标和控制措施的选择
  - 了解灾难恢复和业务持续计划的重要性
  - 掌握制定灾难恢复和业务持续计划的方法，并能有效管理相关计划

会计信息系统的安全问题

- 会计信息系统面临的风险类型
- 信息安全相关问题
- 信息安全管理控制规范

会计信息系统面临的风险类型

- （1）自然灾害和政治灾难
  - 火灾、水灾、地质灾害等自然灾害
  - 恐怖活动、战争等政治灾害
  - 2006年12月26日台湾地震导致国际海底光缆中断
- （2）软件错误和设备故障
  - 软件程序的BUG、电力中断、通信线路中断等
  - 例：用友软件操作过程中遇见的问题

会计信息系统面临的风险类型

- （3）无意识的破坏行为
  - 员工安全意识缺乏导致的系统及信息破坏
  - 会计无意中删除了重要的账户资料
- （4）有意识的破坏行为
  - 恶意软件、非授权访问和修改、偷窃、消息路径错误和重定向
  - 担任世界最大衍生交易市场领导角色的法国第二大银行兴业银行，2008年1月24日爆出该行历史上最大违规操作丑闻，30多岁的交易员热罗姆·盖维耶尔通过了银行“5道安全关”获得使用巨额资金的权限，在未经授权情况下大量购买欧洲股指期货，最终给银行造成49亿欧元（约合71.4亿美元）损失。

业务过程风险的类型

- 战略风险：指做了错误的事情。
- 操作风险：指做了正确的事情，但用的是错误的方法。
- 财务风险：指面临财务资源的损失、浪费或偷窃。
- 法律法规风险：指是否面临违背法律法规的风险。
- 信息风险：如是否存在错误的或不相关的信息、不可靠的系统和不正确的报告。

信息安全相关问题

- 信息是一种资产，和其他重要的业务资产一样，对企业而言具有价值，需要保护。
- 信息安全是指防止信息资源的非授权泄露、更改、破坏，或使用非法系统辨识、控制和否认，以确保信息的机密性（confidentiality）、完整性（integrity）、可用性（availability）、真实性（authenticity）及有效性（utility）。

信息安全相关问题

- 信息安全一般可以通过实体安全、运行安全、管理安全等方面来加以控制实现。
- 信息安全主要通过采用计算机软硬件技术、网络技术、密钥技术等安全技术和各种组织管理措施，来保护信息在其生命周期内的产生、传输、交换、处理和存储的各个环节中，信息的机密性、完整性、真实性、可用性等不被破坏。

信息安全相关问题

- 机密性是指确保只有被授予特定权限的人才能访问到信息。
  - 公开信息
  - 敏感信息
- 完整性是指保证信息及其处理方法的正确性和完整性。
  - 在使用、传输、存储信息的过程中不发生篡改信息、丢失信息、错误信息等现象。
  - 信息处理方法正确，错误的操作，有可能造成重要文件的丢失和毁损，甚至造成整个系统的瘫痪。
- 可用性是确保授权用户在需要的时候确实可以访问系统获得所需信息。
  - 通信线路中断、网络拥堵都会造成信息在一段时间内不可用，影响正常的业务运营。

信息安全相关问题

- 信息安全包括信息系统的安全和信息的安全，并以信息安全为最终目标。
- 实现信息安全必须从管理和技术两方面着手，技术层面和管理层面的良好配合，是企业实现信息安全的有效途径。
  - 信息安全不仅仅是技术问题，在很大程度上更多的表现为管理问题。
  - 据安永分析，在整个系统安全工作中，管理所占的比重应该达到70%，而技术应占30%。
  - 在信息安全实务工作中，人们的注意力通常集中在计算机及其技术的使用、安装、配置以及预防工具滥用等方面，容易忽视使用工具的人。

信息安全相关问题

- 常用的信息安全技术
  - 密码技术——密码编码、密码分析、认证、鉴别、数字签名、密钥管理、密钥托管等
  - 防病毒技术——专用的防病毒软件和硬件。
  - 防火墙技术——计算机防火墙、网络防火墙，结合采用过滤技术、代理技术、电路网关技术。
  - 入侵检测技术——检测计算中网络中违反安全策略的技术。
  - 虚拟专用网VPN技术——集成了见别人争、访问控制和密码变换的安全隧道技术。
  - 信息伪装技术——将秘密信息隐藏与另一非机密文件内容之中，不同于传统的加密技术，不仅隐藏了信息的内容，还隐藏了信息的存在。
- 单一的信息安全技术往往不能解决问题，必须综合运用多种信息安全技术，实现信息安全。

信息安全相关问题

- 信息安全管理是企业用于指导和管理各种控制信息安全风险的、一组相互协调的活动，有效的信息安全管理要尽量做到在有限的成本下，保证安全“滴水不漏”。
- 信息安全管理一般包括制定信息安全政策、风险评估、控制目标和方式的选择、制定规范的操作流程、对员工进行安全意识培训等一系列工作，通过在安全方针策略、组织安全、资产分类与控制、人员安全、物理与环境安全、通信与运营安全、访问控制、系统开发与维护、业务持续性管理、符合法律法规要求等十个领域内建立管理控制措施，为企业建立一张完备的信息安全“保护网”，保证企业信息资产的安全与业务的连续性。

信息安全相关问题

- 信息安全国际标准
  - 互操作标准
    - 对称加密标准EDS,3DES,IDEA,AES;非对称加密标准RSA； VPN标准IPSec;传输层加密标准SSL；安全电子邮件标准S-MIME;安全电子交易标准SET;通用脆弱性描述标准CVE。
  - 技术与工程标准
    - ISO/IEC15408信息产品通用测评标准
    - SSE-CMM安全系统工程能力成熟度模型
    - TESEC美国信息安全桔皮书
  - 信息安全管理与控制标准
    - BS7799,ISO/IEC17799信息安全管理体系标准
    - COBIT信息和相关技术控制目标
    - ITIL基础架构库
    - ISO13335信息安全管理标准

信息安全相关问题

- 信息安全国家标准
  - GB17895-1999计算机信息系统安全保护等级划分准则
    - 将信息系统安全分为自主保护级、系统审计保护级、安全标记保护级、结构化保护级、访问验证保护级。
    - 主要的安全考核指标：身份认证、自主访问控制、数据完整性、审计等。
    - GA/T387-2002 计算机信息系统安全等级保护网络系统技术要求
    - GA/T388-2002 计算机信息系统安全等级保护操作系统技术要求
    - GA/T389-2002 计算机信息系统安全等级保护数据库管理系统技术要求
    - GA/T390-2002 计算机信息系统安全等级保护通用技术要求
    - GA/T391-2002 计算机信息系统安全等级保护管理要求
  - GB/T18336信息技术安全性评估准则

信息安全管理控制规范

- 信息安全组织之“基础设施”
- 信息安全组织之“第三方访问”
- 信息安全组织之“外包”

信息安全管理控制规范

- 资产的分类和控制之“资产的保管责任”
- 资产的分类和控制之“信息分类”

信息安全管理控制规范

- 人员安全之“工作说明及人力资源的安全”
- 人员安全之“用户培训”
- 人员安全之“安全事故及故障的响应”

信息安全管理控制规范

- 物理与环境安全之“安全区域”
- 物理与环境安全之“设备安全”
- 物理与环境安全之“一般控制”

信息安全管理控制规范

- 通信与运营安全之“作业程序及责任”
- 通信与运营安全之“系统规划及验收”
- 通信与运营安全之“对恶意软件的防范”
- 通信与运营安全之“日常事务处理”
- 通信与运营安全之“网络管理”
- 通信与运营安全之“存储媒体的处理与安全”
- 通信与运营安全之“信息及软件的交换”

信息安全管理控制规范

- 访问控制之“用户访问管理”
- 访问控制之“用户责任”
- 访问控制之“网络访问控制”
- 访问控制之“操作系统访问控制”
- 访问控制之“应用程序访问控制”
- 访问控制之“系统访问及使用的监控”
- 访问控制之“可移动式计算机运算及计算机远距工作”

信息安全管理控制规范

- 系统开发与维护之“系统的安全要求”
- 系统开发与维护之“应用系统中的安全”
- 系统开发与维护之“密码学的控制方法”
- 系统开发与维护之“系统文件的安全”

信息安全管理控制规范

- 业务持续性管理之“业务持续运作管理考虑”

信息安全管理控制规范

- 符合性之“法规要求的符合性”
- 符合性之“安全政策符合性及技术符合性的审查”
- 符合性之“系统审核的考虑”

会计信息系统的安全风险评估和管理

- 安全风险和安全需求
- 风险评估和管理
- 安全控制目标和控制措施的选择
- 影响安全控制措施选择的因素

安全风险

- 信息系统安全风险是指威胁利用系统的脆弱性，直接或间接造成资产损害的一种潜在的影响。
- 通过确定资产价值和相关威胁与脆弱性的水平，可以得出风险的度量值。

安全风险

- 威胁
  - 会带来负面影响的潜在事件。
- 脆弱性
  - 所谓脆弱性就是资产的弱点，这些弱点会被威胁利用造成安全事件发生，从而对资产造成伤害。
  - 脆弱性本身并不会引起损害，只是为威胁提供了影响资产的条件。
    - 缺乏物理保护或保护不当
    - 口令选择或使用不当
    - 与外部网络的连接没有保护
    - 没有保护的存档文件
    - 不足够的安全培训

安全风险

- 资产
  - 数据与文档（数据库、数据文件用户手册、运行与支持程序、业务持续性计划、应急安排）；
  - 合同、指南等企业文件；
  - 软件资产（应用软件、系统软件、开发工具和实用程序）；
  - 物理资产（计算机、通讯设备、磁性介质、供电设备、家具、办公场所等）；
  - 人员（员工、客户）
  - 企业形象与声誉
  - 服务（计算和通讯服务、照明和电力等其他技术服务）

安全风险

- 为了明确对资产的保护，有必要对资产进行估价。
- 资产估价要考虑其对业务的重要性和一定条件下的潜在价值。
- 资产价值常常是以安全事件发生时所产生的潜在业务影响来衡量，安全事件会导致资产机密性、完整性和可用性的损失，从而导致企业资金、市场份额、企业形象的损失。
- 采用精确的方式给资产赋值是比较困难的事情。
- 经过资产的识别和估价后，企业应根据资产价值的大小，进一步确定要保护的关键资产。

安全需求

- 信息安全体系要求组织满足三种安全需求
  - 安全风险如果出现将会导致业务损失，评估出组织面临的风险，并控制这种风险的需求。
  - 组织、贸易伙伴、签约客户和服务提供商需要遵守的法规及合同的要求。
  - 组织制定出的、支持业务运作与处理并适合组织信息系统的业务规则、业务目标的要求。
- 只有这些安全需求被定义之后，才能明确的表达信息安全的机密性、完整性和可用性，指导对安全控制方法的选择。

安全需求

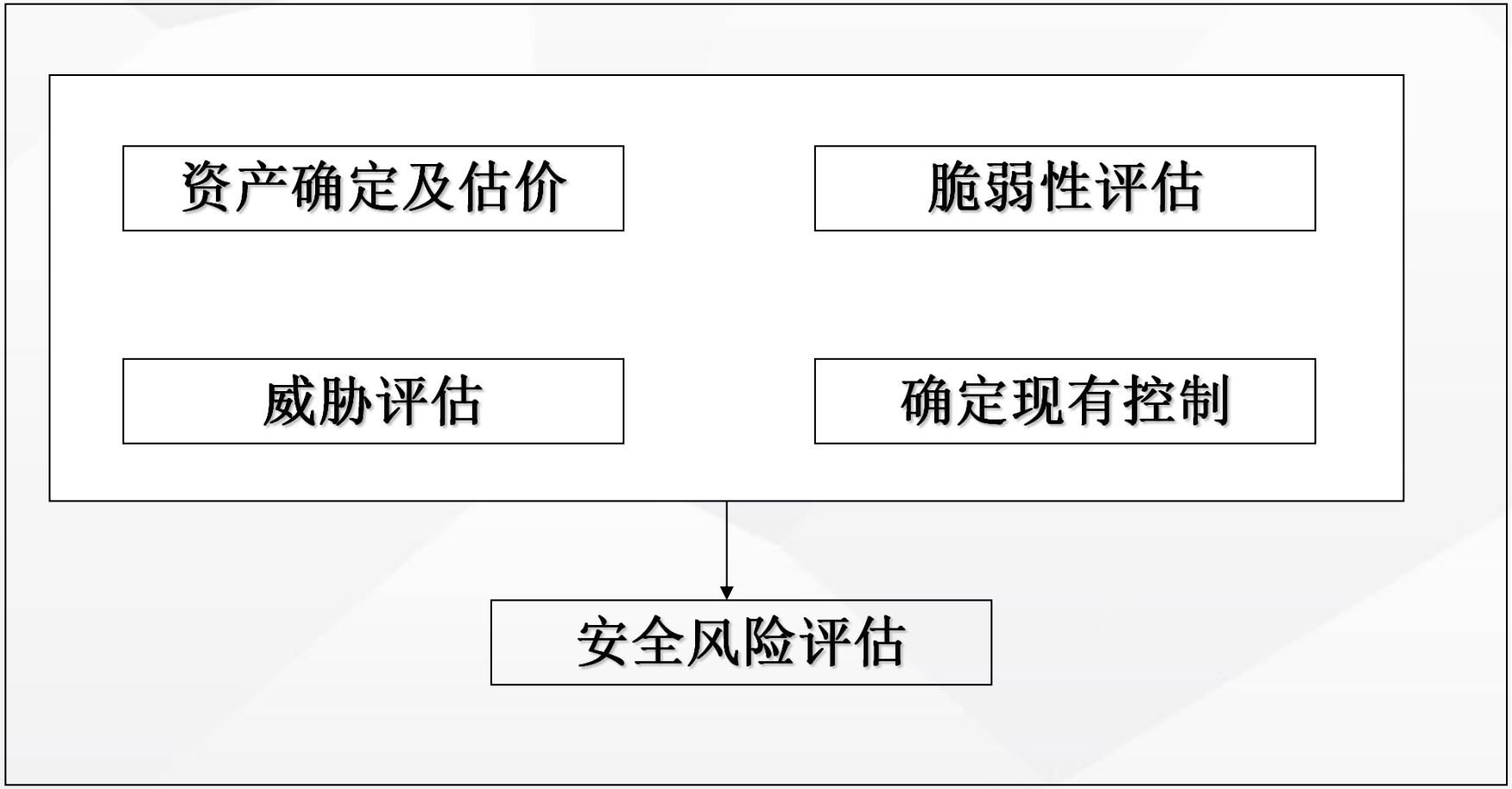
- 在确定由风险而产生的安全需求时，理解安全风险将会对组织产生什么样的影响是很重要的。
- 需要考虑的问题：
  - 组织中最重要的业务环节是什么？这些部分是如何使用与处理信息的？信息系统对这部分的重要性如何？
  - 组织什么样的重要决策要依靠性的的准确性、完整性、可用性或及时性？
  - 什么样的机密信息需要保护？
  - 安全事件对业务和组织的影响是什么？

安全需求

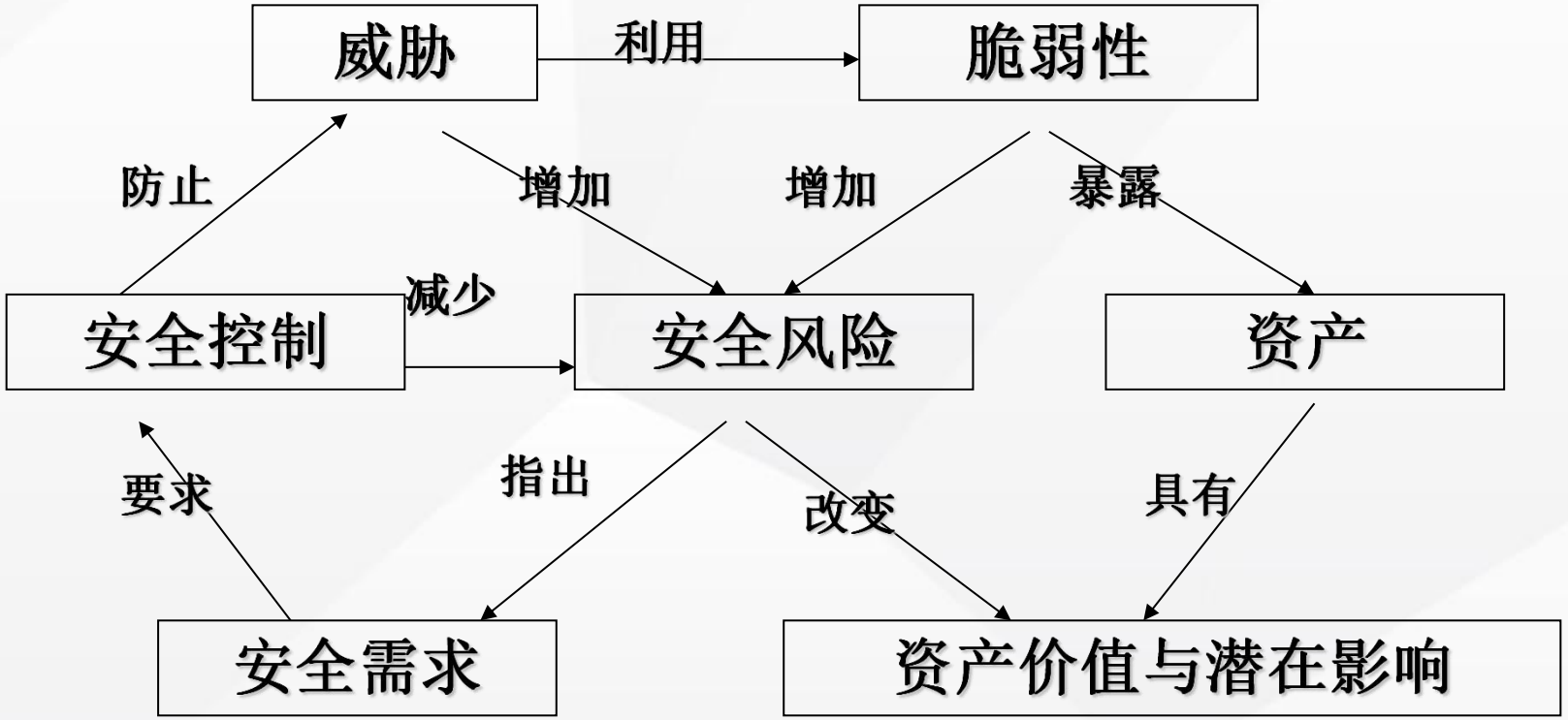
- 业务伙伴需要遵守的有关法律、法规、合同的要求应该在信息安全管理体系文件中详细描述，要保证实施安全控制不会损害任何法令、法规、商业合同的要求。
- 需要考虑的问题：
  - 专利软件的拷贝复制条件
  - 组织记录的保护要求
  - 数据的保护要求

安全需求

- 与业务运营相关的安全需求也应在安全体系中详细描述。
- 需要考虑的问题：
  - 如何支持组织获得竞争优势？
  - 如何帮助提高现金流和盈利能力？
  - 安全控制是否妨碍业务的正常运行？



安全风险评估过程


威胁
利用
脆弱性
防止
增加
增加
暴露
减少
安全控制
安全风险
资产
要求
指出
改变
具有
安全需求
资产价值与潜在影响

- 资产确定及估价
  - 先确定安全管理体系的范围，以便确定资产的评审边界。
  - 评估资产最简单的方式是列出组织业务过程中、安全体系范围内所有具有价值的资产，然后对资产赋予一定的价值，这种价值应该反映资产对业务运营的重要性，并以对业务的潜在影响程度表现出来。
    - 资产价值越大，由于泄漏、修改、损害、不可用等安全事件对组织业务的潜在影响就越大。
    - 资产的价值有资产的所有者和相关用户来确定。
  - 在对资产赋值时，一方面要考虑资产的购买成本，另一方面也要考虑当这种资产的机密性、完整性、可用性受到损害时，对业务运营的负面影响程度。

- 资产确定及估价
  - 在信息安全管理中对资产赋值时，一般并不采用资产的账面价值，比较实用的做法是以定性分级的方式建立资产的相对价值，以相对价值来作为确定重要资产的依据和为这种资产的保护投入多少资源的依据。
  - 定性分级表参考：

分级类型	定性分级程度
相对较粗的分级	低、中、高
详细分级	可忽略、低、中、高、非常高
更详细的分级	（低）0、1、2、……10（高）

- 资产确定及估价
  - 在确定资产的机密性、完整性、可用性受到损害，对业务运营的负面影响程度时，可以参考以下因素：
    - 违反法令、法规；
    - 对业务绩效的影响；
    - 对组织声誉和形象的损害；
    - 对个人信息的侵害；
    - 对个人安全的威胁；
    - 对法律实施的负面影响；
    - 对业务机密性的破坏；
    - 对公共秩序的破坏；
    - 资金损失；
    - 业务活动中断；
    - 对环境安全的破坏；

- 资产确定及估价
  - 组织可以制定符合自己需要的资产评估价值级别；
  - 价值级别的选择应该与企业选择的价值标准一致；
  - 一般来说，组织应该按照实际需要和使用的价值标准，考虑使用一个能综合满足定量和定性要求的方式。
  - 组织还要决定什么样的损害程度为“低”，什么样的损害程度为“高”。

- 威胁评估
  - 与威胁有关的信息可从安全管理人员和业务流程处收集。
    - 人力资源部的员工、设备计划与管理人员、信息技术专家、组织中对安全负责的人员
  - 一项资产可能面临多个威胁，同样一个威胁可能对不同资产造成影响。
  - 威胁来源可与安全控制规范中定义的领域相对照来识别确定

- 威胁评估
  - **威胁来源：参见ISO/IEC13335第三部分《信息安全管理方针》中列出的威胁来源**

维护错误	恶意软件	用户身份伪装	消息路径错误或重定向	滥用资源
非授权人员访问	运行支持人员的错误	电力波动	软件故障	否定服务
人员短缺	盗窃	流量分析	流量过载	传输错误
以非授权方式使用软件	存储介质的非授权使用	非授权使用网络设施	硬件	……

- 威胁评估
  - 组织识别出威胁的原因、威胁的目标以后，有必要评估威胁发生的可能性。
    - 威胁的原因（谁造成了威胁？）
    - 威胁的目标（威胁会影响组织信息系统的什么要素？）

- 威胁评估
  - 需要考虑的因素：
    - 威胁发生的频度——根据经验和统计规律，估计出威胁多长时间发生一次
    - 有预谋的威胁——研究攻击者的动机，需具备的能力、所需的资源、组织资产吸引力的大小和脆弱性的程度
    - 意外事故产生的威胁——研究地理因素，如是否靠近石油化工企业、是否处于极端天气频发地带、环境因素是否容易引发人为错误和设备故障等等。

- 脆弱性评估
  - 脆弱性评估是指在评审范围内，确定以下各资产的弱点：
    - 物理环境；
    - 人员管理、业务管理、行政管理过程与控制
    - 硬件、软件和通讯设施；
  - 这些方面的脆弱性很容易被威胁利用，从而造成对资产和业务的损害。
  - 脆弱性分级：
    - 高度可能，很可能，可能，不太可能，不可能
  - 与每一种威胁相关的脆弱性都应该评估出来

- 脆弱性评估
  - 脆弱性及其可能利用该脆弱性的威胁示例：

脆弱性	威胁	脆弱性	威胁
员工缺编	人员短缺	外部人员的行动没有受到监督	盗窃
不完备的安全培训	运行支持人员错误	缺乏安全意识	用户错误
软件文档不完全	运行支持人员错误	缺乏监控机制	非授权使用软件
缺乏正确使用媒介与通讯信息的政策	以非授权的形式使用网络设施	不完备的招聘程序	蓄意破坏
存储介质缺乏维护或错误安装	维护错误	过于复杂的用户界面	运行支持人员错误
缺乏审计轨迹	非授权使用软件	缺乏身份验证机制	用户身份伪装
未退出工作站离开	非授权使用软件	未对软件充分测试	非授权使用软件
口令管理不善	用户身份伪装	规格说明书不完整	软件故障
不受控制的下载	恶意病毒	访问权限未正确分配	非授权使用软件

- 现有的安全控制
  - 应用现有的安全控制措施，可以减少重复工作，降低安全控制成本。
  - 在应用现有控制之前，一定要检查这些控制措施是否有效，根据检查的结果来决定保留、去除或是替换。
  - 通过风险评估过程确定的控制措施要与现有控制兼容，以免在实施过程中出现冲突。（如银行卡挂失要求与挂失安排）

- 风险分析技术
  - 风险分析：就是要对风险的辨识，估计和评价做出全面的，综合的分析，其主要组成为：
  - （1）风险的辨识，也就是那里有风险，后果如何，参数变化？
  - （2）风险评估，也就是概率大小及分布，后果大小？
  - 进行风险分析必须考虑以下几个方面的要素
    - 业务过程面临的威胁和易受攻击性
    - 对业务过程的影响
    - 威胁发生的可能性
    - 业务过程风险的类型

- 风险管理目标
  - 接受风险：不做任何事情，不引入控制措施
  - 避免风险：通过放弃某一业务活动或主动从风险区域撤离来规避风险。
  - 转移风险：在无法规避风险，减少风险成本很困难或成本很高时，将风险转移给第三方，如保险、外包。
  - 降低风险：通过选择控制目标与控制措施来降低评估确定的风险。
    - 减少威胁
    - 降低脆弱性
    - 降低负面影响
    - 检测意外事件
    - 从意外事件中恢复

- 风险分析矩阵

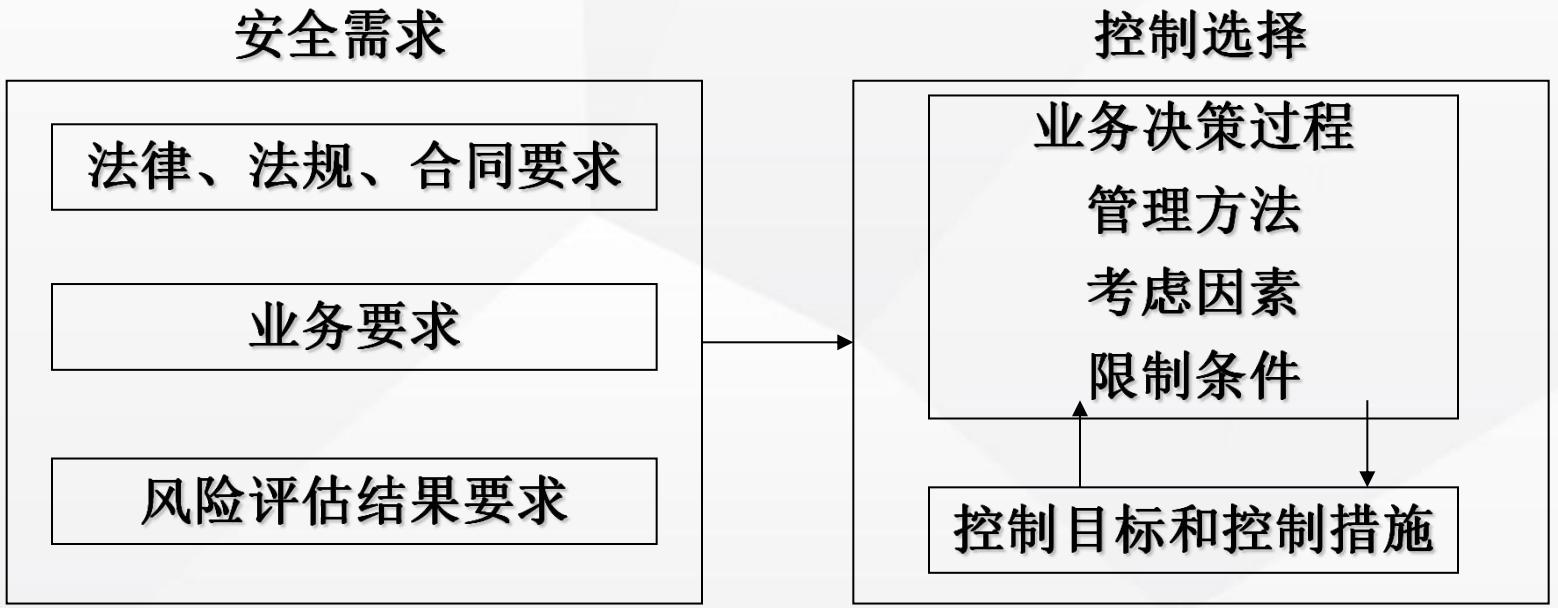
	完整性	保密性	可用性
无意识的行为（错误和遗漏）	重要或不重要	保密或不保密	必要或不必要
有意识的行为（欺骗和滥用）	重要或不重要	保密或不保密	必要或不必要
	数据破坏或修改	数据泄露	对数据的非法接近、使用

- 控制矩阵

控制计划建议	业务过程的控制目标				信息过程的控制目标				
	操作有效性		操作效率	资源安全	汇款通知单输入			应收账款主数据	
	合理合法收取款项	子目标2	X笔收款/天	款项安全入帐	输入有效	输入完整	输入准确	更新完整	更新准确
当前的控制措施									
措施1(P1)：三张单据核对	X			X					

安全控制目标和控制措施的选择

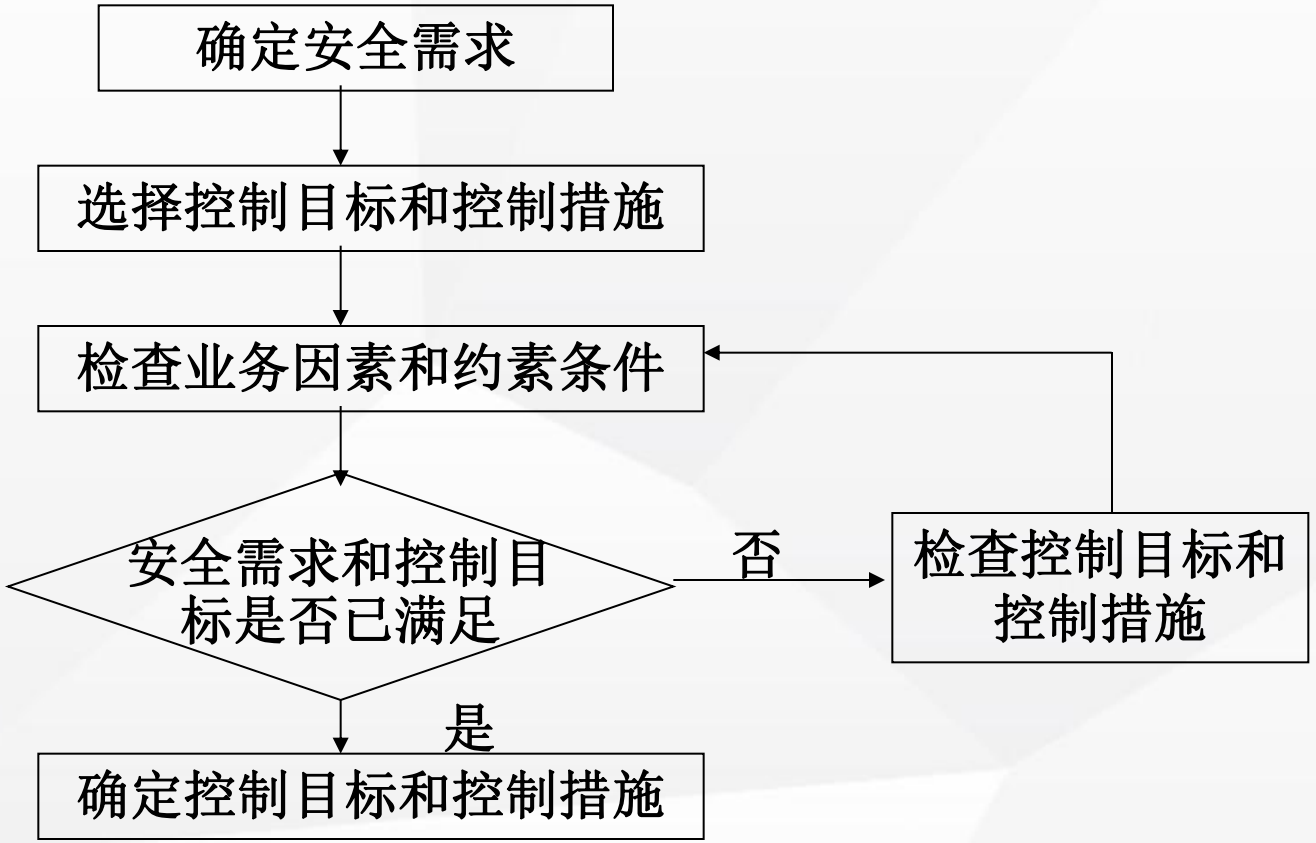
- 对控制目标和控制措施的选择应当由安全需求来驱动，选择控制措施应当最好能满足安全需求，并考虑安全需求的不到满足时的后果。



安全需求与控制选择

安全控制目标和控制措施的选择

- 选择控制的过程



选择控制的过程

安全控制目标和控制措施的选择

- 选择控制的原则
  - 对控制目标和控制措施的选择应当由安全需求来驱动，选择控制措施应当最好能满足安全需求，并考虑安全需求的不到满足时的后果。
  - 应当在安全与投入之间保持平衡，保证组织的盈利能力、高效性和竞争能力。
  - 在选择控制时并没有一套标准与通用的办法，选择的过程往往不是很直接，可能要涉及一系列的决策步骤、咨询、讨论过程，最后的结果要很好的满足组织对业务目标、资产保护、投资预算的要求。

安全控制目标和控制措施的选择

- 影响选择控制的因素和条件
  - 选择控制需要考虑的因素
    - 成本
      - 控制的成本必须小于要保护的资产的价值
    - 可用性
      - 主要是技术上和操作上的可用性
        - 如电子商务交易的风险是财务信息被篡改，加密？不加密？加密安全，但如果法律规定不允许加密，措施则不可用。

安全控制目标和控制措施的选择

- 影响选择控制的因素和条件
  - 选择控制需要考虑的因素
    - 实施与维护
      - 实施和维护的简易性、成本和时间因素必须要考虑
  - 可以采用检查列表的方式，列出系统所需要的最小安全保证、成本、可用性、安全因素等内容，逐项检查筛选。

安全控制目标和控制措施的选择

- 影响选择控制的因素和条件
  - 限制条件
    - 已存在的控制
    - 所有的控制目标和安全需求是否已经满足
    - 实施与维护控制

信息系统灾难恢复和业务持续计划

- 计划的重要性
- 如何制定计划
- 计划的测试
- 计划的管理和审计

相关背景材料

- 2005/5/26，在广东南海召开的“首届中国灾难恢复行业高层论坛”，被业界称为中国灾难恢复行业里程碑式的重要会议。
- 这一论坛由中国信息产业商会信息安全产业分会主办、国务院信息化办公室支持、广东省地税局和GDS公司协办，集合了来自政府、行业、厂商、专家等各方人士，他们就在中国开展灾难恢复业务将面临的主要挑战和实战方法，展开了深入而切实的讨论。同时，对于灾备建设中最重要的标准化问题，国务院信息化办公室借本次论坛对2005年4月份出台的指导文件《重要信息系统灾难恢复规划指南》，进行了宣讲和解释。
- 思考：究竟应当怎样对系统的灾难性故障进行迅速的响应和处置？如何制定适合自身实际的灾难恢复规划？

指南的主要亮点

- 何谓灾难？
  - 《指南》定义为：“由于人为或自然的原因，造成信息系统运行严重故障或瘫痪，使信息系统支持的业务功能停顿或服务水平不可接受、达到特定的时间的突发性事件，通常导致信息系统需要切换到备用场地运行。”
  - 由此可见，灾难不只指自然的原因，也包括人为的原因，对于信息系统的连续性运行来说，灾难的范围很宽泛。

指南的主要亮点

- 何为灾难恢复？何为灾难备份？二者有何不同？
  - 灾难恢复：“将信息系统从灾难造成的故障或瘫痪状态恢复到可正常运行状态，并将其支持的业务功能从灾难造成的不正常状态恢复到可接受状态，而设计的活动和流程”。
  - 灾难备份：“为了灾难恢复而对数据、数据处理系统、网络系统、基础设施、技术支持能力和运行管理能力进行备份的过程。”
  - 灾难恢复比灾难备份的外延要大。

指南的主要亮点

- 灾难恢复的等级划分
  - 参照国际相关标准，并结合国内实际情况，将灾难恢复应具有的技术和管理支持分为6个等级，每个等级都包括数据备份系统、备用数据处理系统、备用网络系统、备用基础设施、技术支持、运行维护支持及灾难恢复预案等7个要素。
  - 如要达到某个灾难恢复等级，应同时满足该等级中的7个要素的要求。

指南的主要亮点

- 《指南》的内容覆盖了灾难恢复工作的主要环节，以及每一个环节需要开展的各项具体工作，包括灾难恢复的管理，需求的确定，策略的制订和实现，预案的制订、落实和管理，预案框架等。

计划的重要性

- 信息和数据是企业最宝贵的资产，事关企业的经济运行命脉和商业信誉；
- 企业运作越依赖于IT架构，就对信息系统运作的稳定性和可靠性的要求越高。
- IT系统是否完善，是否能够提供全天候业务运作，是竞争力的一个最重要的前提。

计划的重要性

- 当企业越来越依赖于信息系统开展业务及落实管理时，面对随时都有可能发生的自然或人为的灾难，做好数据备份、系统恢复及业务连续性管理，也变得越来越紧迫和重要。
- 灾难恢复已经不只是信息技术部门关心的事，而是上升到企业高管需要给予高度关注的事。

定义

- 业务可持续计划是为了防止正常业务行为的中断而被建立的计划。
- 灾难恢复计划是在对灾难发生前后和期间内所采取的所有行动的综合说明，也包括能够确保运行继续的、以文件规定的、进过测试的应急程序。
- BCP强调使关键业务经得起不同的意外事件的影响
- DRP强调对于灾难的预防措施，以及在灾难发生时和灾难发生之后所应采取的行为和措施。

业务持续计划（BCP）过程

- 业务持续计划（BCP）过程包含：
  - 1.范围和计划的初始化；
  - 2.业务影响分析(BIA －Business Impact Assessment)；
  - 3.制订业务持续计划；
  - 4.业务持续计划的批准和执行；

灾难恢复（DRP）过程

- 灾难恢复计划（DRP）过程包含：
  - 建立灾难恢复计划；
  - 测试灾难恢复计划；
  - 灾难恢复计划程序

灾难恢复和业务持续计划测试

- 灾难恢复和业务持续计划最容易被忽视的方面就是计划测试。
- 测试十分重要，计划测试可以衡量人员的准备情况，发现计划中的纰漏和瓶颈状况。
- 干扰模拟测试在突击进行的情况下，测试效果最为显著。
- 在宣布模拟开始后，所有受其影响的处理状态均应加以记录，为以后的评估提供基准。
- 在经济允许的范围内，计划应尽可能充分地被检测，测试应该包括备份设备和备份支持材料。
- 测试过程中，应注意关键点计划的进展情况。
- 测试完成后，应编制计划执行报告，作为管理层决定是否修改计划或是安排额外的测试依据。

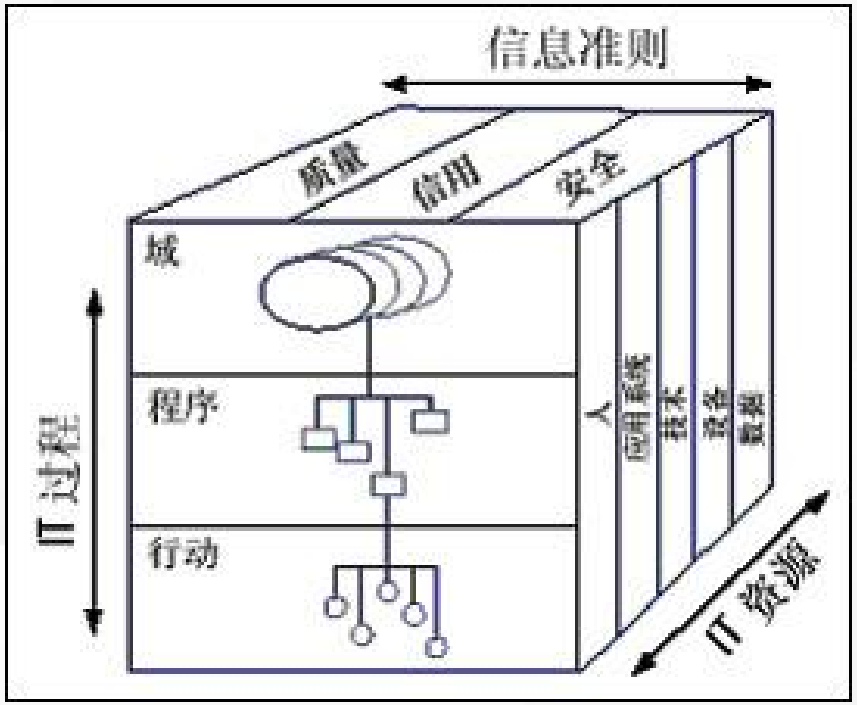
灾难恢复和业务持续计划测试

- 业务可持续计划是为了防止正常业务行为的中断而被建立的计划。
- 灾难恢复计划是在对灾难发生前后和期间内所采取的所有行动的综合说明，也包括能够确保运行继续的、以文件规定的、进过测试的应急程序。
- 尽管每个计划的细节针对不同公司的要求会有不同，但所有可行的计划都具有共同的特点。
  - 提供第二现场备份
  - 确认关键应用程序
  - 执行备份和非现场存储程序
  - 建立计划小组
  - 测试计划

灾难恢复和业务持续计划测试

- 计划的管理和审计
  - 计划的管理和审计目标是检查公司制定的灾难恢复和业务持续计划是否适应公司的要求，其实施是否可行、有效。
  - 审计程序包括
    - 第二现场备份审计
    - 关键应用程序清单审计
    - 备份关键应用程序审计
    - 备份关键数据文件审计
    - 备份相关支持材料、源文件和文档管理审计
    - 计划小组工作审计

- 信息系统控制标准
  - COBIT--Control Objectives for Information and related Technology，是一个由信息系统审计与控制学会ISACA（Information Systems Audit and Control Association）在1996年所公布的业界标准，目前已经更新至COBIT5，是国际上公认的最先进、最权威的安全与信息技术管理和控制的标准。



- COBIT
  - IT准则维集中反映了企业的战略目标，主要从质量、成本、时间、资源利用率、系统效率、保密性、完整性、可用性等方面来保证信息的安全性、可靠性、有效性。
  - IT资源维主要包括以人、应用系统、技术、设施及数据在内的信息相关的资源，这是IT治理过程的主要对象。
  - IT过程维则是在IT准则的指导下，对信息及相关资源进行规划与处理，从信息技术的规划与组织PO（Planning & Organization）、获取与实施AI（Acquisition & Implementation）、交付与支持DS（Delivery and Support）、监控Monitoring等四个方面确定了34个信息技术处理过程
  - COBIT标准的主要目的是为提供业界提供关于IT控制的一个清楚的政策和发展的良好的典范 。

- COBIT框架的组成部分
  - 管理指导方针（Management Guidelines）
  - 管理者摘要（Executive Summary）
  - 框架（Framework）
  - 审计指导方针（Audit Guidelines）
  - 控制目标（Control Objectives）
  - 应用工具集（Implementation Tool Set）

- 信息系统控制标准
  - BS7799
    - BS7799是英国标准协会（BSI）于1995年2月提出的《信息安全管理标准》，该标准分别于1995年5月和1999年重新进行了修订。
    - 标准主要包括2个部分：1.BS7799-1，信息安全管理的操作规则；2.BS7799-2，信息安全管理体系规范。
      - 第一部分主要是给负责开发的人员作为参考文档使用，从而在他们的机构内部实施和维护信息安全；
      - 第二部分详细说明了建立、实施和维护信息安全管理系统的要求，指出实施组织需遵循某一风险评估来鉴定最适宜的控制对象，并对自己的需求采取适当的控制。

- 信息系统控制标准
  - ISO/IEC17799
    - 英国标准协会（BSI）制订并于1999年修订的《信息安全管理标准》BS7799的一部分已经在2000末被采纳为国际标准，以标准号ISO/IEC17799发布，全名为《信息安全管理操作规则》。
    - 根据官方的报告，ISO/IEC17799的目的是“为信息安全管理提供建议，供那些在其机构中负有安全责任的人使用。它旨在为一个机构提供用来制定安全标准、实施有效的安全管理时的通用要素，并得以使跨机构的交易得到互信”。
    - 一个通用的信息安全管理指南，ISO/IEC17799 的目的并不是告诉你有关“怎么做”的细节，它不是一篇技术性的信息安全操作手册

- 信息系统控制标准
  - ITIL（Information Technology Infrastructure Library）——信息技术基础设施库——是英国商务部80年代后期提出和开发的一套书籍，这些书描述了一个用于管理IT服务的集成的、面向过程的和最佳实践框架。
  - 初衷是为了提高英国中央政府的IT服务管理水平，并适合公共的或私有的、大型的或小型的，和集中的或分散的所有组织。

- 信息系统控制标准
  - ITIL的内容
    - （1）服务水平管理（Service Level Management）
    - （2）可用性管理（Avaliablity Management）
    - （3）能力管理（Capacity Management）
    - （4）持续性计划（Contingency Planning）
    - （5）成本管理（Coat Management）
    - （6）帮助台（Helpdesk）
    - （7）问题管理（Problem Management）
    - （8）变动管理（Change Management）
    - （9）配置管理（Configuration Management）
    - （10）软件控制和分发（Software & Distribution）

- 阅读材料：网上银行系统的安全
  - 网上银行系统存在哪些安全问题？
  - 可以采取哪些有效的措施来应对这些问题？

上海财经大学

SHANGHAI UNIVERSITY OF FINANCE AND ECONOMICS

THANK YOU