IT审计与信息安全审计

张文祺

风险控制服务部

经理

微信：TSSWENQI

电话：18910179945

简介

- 张文祺先生拥有多年IT管理及IT信息安全管理咨询经验，为银行业、能源业、电信高科技行业以及生产制造企业提供了IT项目管理咨询建设、IT服务管理流程平台建设、ERP平台建设、ISO20000与ISO27001认证、云计算运维管理建设、信息安全咨询、业务连续性咨询，并在2012年承担了ISO20000:2011版核心章节翻译工作。张先生作为特聘讲师，曾为多家公司提供ISO20000、ITIL、ISO27001、信息安全管理CISP、PMP项目管理、信息系统项目管理师等培训。
- 张先生以IT服务管理、IT信息安全管理作为基础，为客户提供相关咨询服务，分析并设计客户在新技术环境下组织架构，管理流程，风险控制服务，为客户建立了云计算环境下的运维管理体系，具体项目经验包括：

专业资格：

- IT治理框架(COBIT)、
- 项目管理专家（PMP）、Prince2 practitioner项目管理专家、
- ITIL专家认证（ITILv3 Expert）
- ISO20000主任审计员、ISO27001主任审计员、
- 注册信息系统审计师（CISA）、注册信息系统安全专家（CISSP）
- 注册信息安全讲师（CISI）

信息安全列为国家战略

国家互联网信息办公室副主任庄荣文在国新办介绍《“十三五”国家信息化规划》表示，规划确定了6大主攻方向、10大任务、16项工程、12项优先行动和6大政策措施。

信息安全列为国家战略

四大重点工作

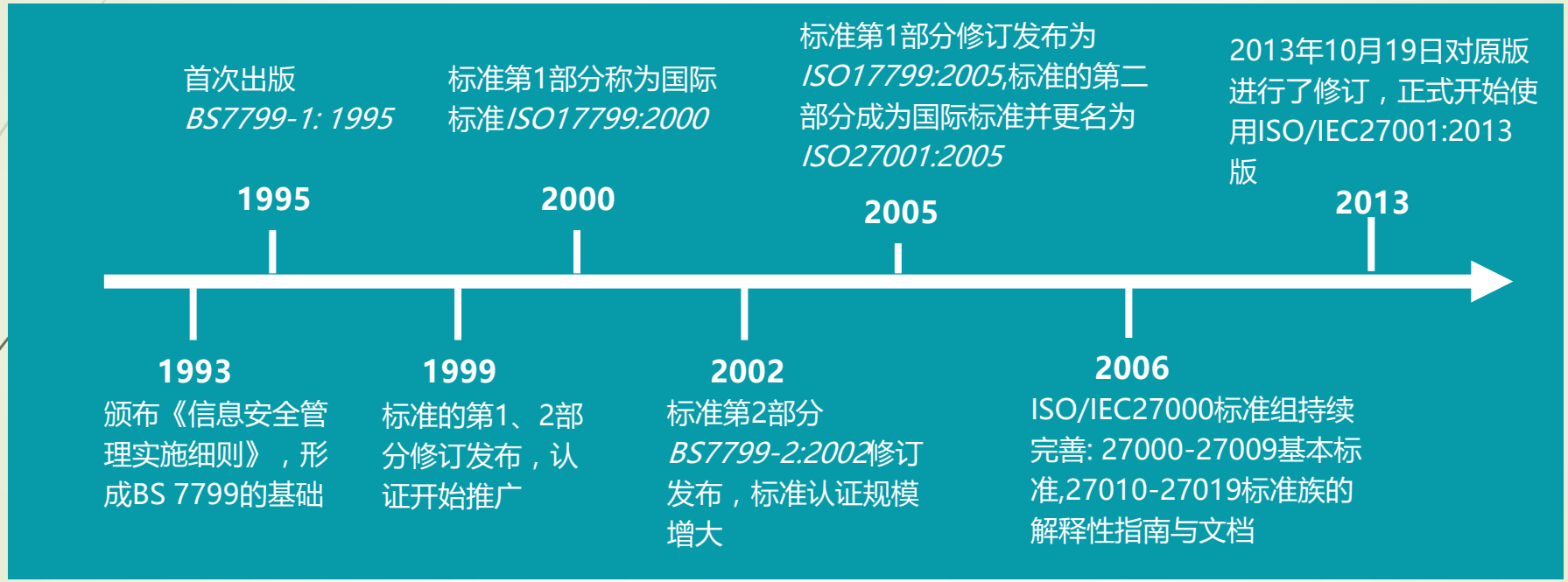
- 要打破信息壁垒和“孤岛”，构建统一高效、互联互通、安全可靠的国家数据资源体系
- 要加快高速宽带网络建设，打通入户“最后一公里”
- 要构建网络和信息安全监测预警、应急处置等保障体系
- 要开展5G关键技术研发和产业化、北斗系统建设应用、网络扶贫、普惠性在线教育等12项优先行动

部署十大任务

- 构建现代信息技术和产业生态体系
- 建设泛在先进的信息基础设施体系
- 建立统一开放的大数据体系
- 构筑融合创新的信息经济体系
- 支持善治高效的国家治理体系构建
- 形成普惠便捷的信息惠民体系
- 打造网信军民深度融合发展体系
- 拓展网信企业全球化发展服务体系
- 完善网络空间治理体系
- 健全网络安全保障体系

ISO27001信息安全管理体系发展概况

“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"。



- ISO27001: ISMS要求,组织自评估和第三方认证的依据。
- ISO27002: 即ISO/IEC 17799:2005,信息安全管理实践规则
- ISO27003: 信息安全管理体系实施指南
- ISO27004: 信息安全管理测量
- ISO27005: 信息安全风险管理
- ISO27006: 信息安全管理体系审核认证机构要求
- ISO27007: 信息安全管理体系审核员指南

审计缺乏和审计不到位带来诸多隐患

2016年重大宕机事件

汇丰银行

影响评级：★★★

时间：2016.1.6

原因：未公开

持续时间：24小时 +

影响范围：1700万名个人及商业客户

新闻来源：金评媒
http://www.jpm.cn/article-5578-1.htm

2016年重大宕机事件

亦庄数据中心断电

影响评级：★★★★

时间：2016.4.22

原因：停电

持续时间：7小时

影响范围：某村镇银行和多家金融机构托管在该机房的所有设备宕机，服务全部中断

新闻来源：云头条 http://www.yuntoutiao.com/dongtai/6020.html

2016年重大宕机事件

全日空公司国内航线无法办理登机

影响评级：★★★★

时间：2016.3.22

原因：未公开

持续时间：1天

影响范围：国内多地机场航班延迟

新闻来源：中国新闻网 http://www.chinanews.com/gj/2016/03-22/7806495.shtml

2016年重大宕机事件

美国达美航空计算机系统宕机

影响评级：★★★★

时间：2016.8.8

原因：停电

持续时间：6小时

影响范围：451趟航班被取消

新闻来源：科技新报
http://technews.cn/2016/08/16/corporate-it-spending/

2016年重大宕机事件

Salesforce大范围宕机并丢失数据

影响评级：★★★

时间：2016.5.12

原因：停电

持续时间：20小时

影响范围：北美的14个站点切且丢失了4小时的数据

新闻来源：今日头条
http://www.toutiao.com/i6283708317688660481/

2016年重大宕机事件

美国东海岸网站集体宕机

影响评级：★★★★★

时间：2016.10.22

原因：物联网设备漏洞，被利用进行的DDOS攻击

持续时间：7小时

影响范围：Twitter、Tumblr、Netflix、亚马逊、Shopify、Reddit、Airbnb、PayPal和Yelp等诸多人气网站无法提供服务

新闻来源：新浪科技
http://tech.sina.com.cn/i/2016-10-22/doc-ifxwztrt0100881.shtml

什么是审计

什么是审计（Audit ）

- 1972年美国会计学会的《基础审计概念的说明》中对审计的定义是：“审计是为了查明经济活动和经济现象的表现与所定标准之间的一致程序而客观地收集和评价有关证据，并将其结果传达给有利害关系使用者的有组织的过程”。
- 美国审计总局对审计下的定义是：“审计一语，包括审查会计记录、财务事项和财务报表，但就审计总局的全部工作来说，它还包括如下内容：
- ①查核各项工作是否遵守有关的法律和规章制度；
- ②查核各项工作是否经济和有效率；
- ③查核各项工作的结果，以便评价其是否已有效地达到了预期的结果（包括立法机构规定的目标）

什么是审计（Audit ）

- 日本著名审计学者三泽一教授在《审计基础理论》一书中为审计所下的定义是：“审计是具有公正不伪立场的第三者就一定的对象的必须查明的事项进行批评性的调查行为，还包含报告调查结果”。
- 《中华人民共和国审计法实施条例》第2条对审计所下的定义是:”审计是审计机关依法独立检查被审计单位的会计凭证、会计账簿、会计报表以及其他与财政收支、财务收支有关的资料和资产，监督财政收支、财务收支真实、合法和效益的行为”。

审计的基础特性

- 独立性：审计独立性审计师不受那些削弱或纵是有合理的估计仍会削弱审计师做出无偏审计决策能力的压力及其他因素的影响。其对审计工作来讲至关重要。因为涉及市场经济的利益公平，独立性被职业界视为审计的灵魂。

审计的基础特性

- 以证据为基础

什么是信息系统审计

- 信息系统审计与控制（Information System Audit and Control ）
- IT审计（IT audit）
- IT审计就是信息系统审计，也称IT监查，是独立于信息系统本身、信息系统相关开发、使用人员的第三方－IT审计师采用客观的标准对信息系统的策划、开发、使用维护等相关活动和产物进行完整地、有效地检查和评估。
- 信息系统审计是一个通过收集和评价审计证据，对信息系统是否能够保护资产的安全、维护数据的完整、使被审计单位的目标得以有效地实现、使组织的资源得到高效地使用等方面作出判断的过程。

信息系统审计的意义

- 21世纪是信息化的时代，生产、交易和管理都离不开信息流和对信息流的管制。信息系统对生产经营和管理的影响越来越重大，管理人员在面对传统经营风险和财务风险的同时，必须随时面对信息风险对企业生存和发展的挑战。 信息系统必须随时置于专家的监控之下。
- 对信息系统的监控三个目的：机密性、完整性、可用性。

信息系统审计的意义

- 信息安全的基本目标
- 信息安全通常强调所谓AIC三元组的目标，即保密性、完整性和可用性（如图所示）。AIC概念的阐述源自信息技术安全评估标准（Information Technology Security Evaluation Criteria，ITSEC），它也是信息安全的基本要素和安全建设所应遵循的基本原则。

C onfidentiality

I ntegrity

A vailability

信息系统审计的意义

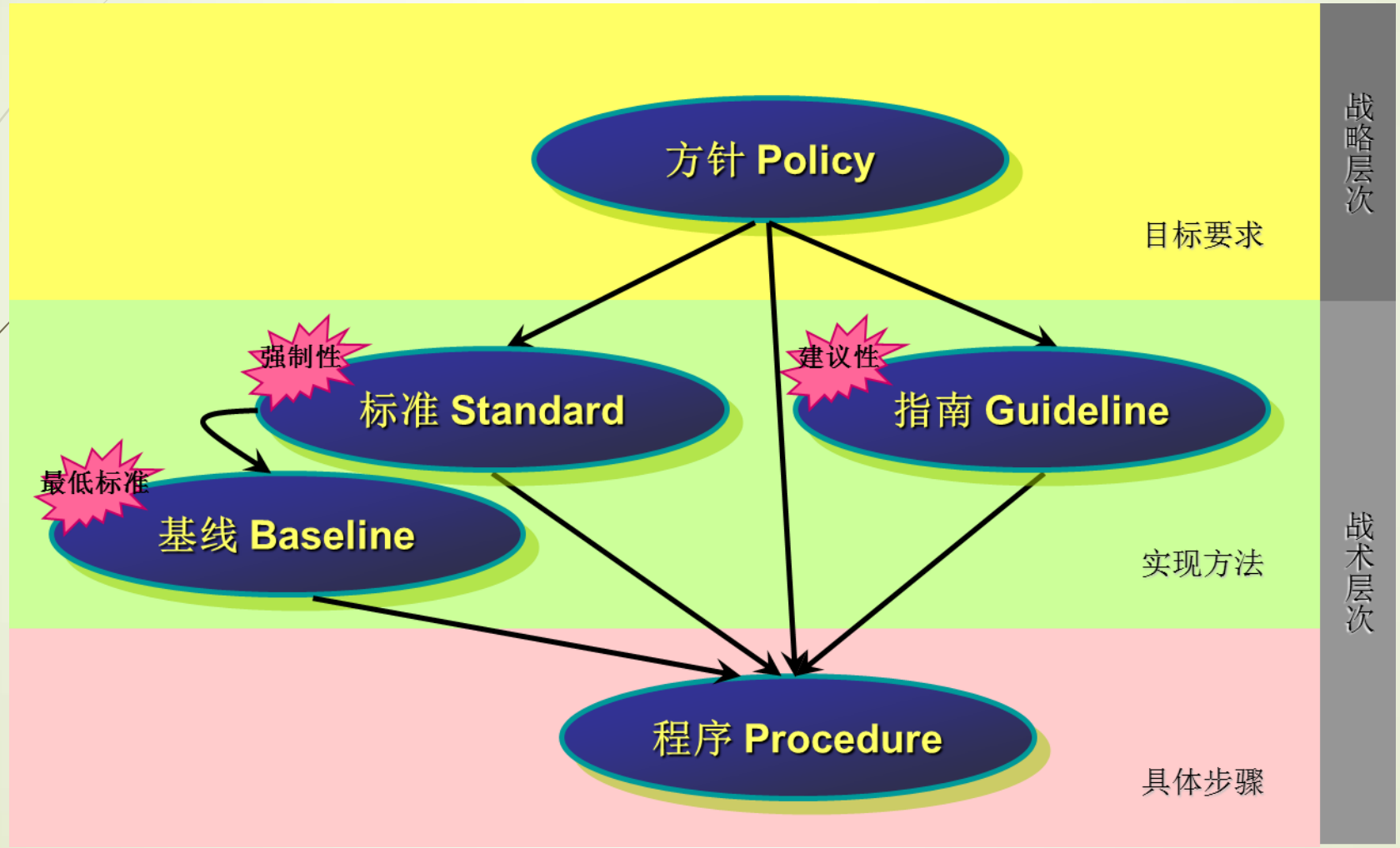
- （1）可用性（Availability）：确保授权用户或实体对信息及资源的正常使用不会被异常拒绝，允许其可靠而及时地访问信息及资源。
- （2）完整性（Integrity）：确保信息在存储、使用、传输过程中不会被非授权用户篡改，同时还要防止授权用户对系统及信息进行不恰当的篡改，保持信息内、外部表示的一致性。
- （3）保密性（Confidentiality）：确保信息在存储、使用、传输过程中不会泄漏给非授权用户或实体。

安全策略

安全策略具有层次性

- **方针**——处于策略链的最高层次，它是由组织的高级管理层发布的、关于信息安全最一般性的声明。方针应该代表着高级管理层对信息安全承担责任的一种承诺，一旦发布，要求组织成员必须遵守。方针的实施要依靠标准、指南和程序。
- **标准**——标准规定了在组织范围内强制执行的对特定技术和方法的使用。标准起着驱动方针的作用，标准可以用来建立方针执行的强制机制。
- **指南**——类似于标准，也是关于加强系统安全的方法，但它是建议性的。指南比标准更灵活，考虑到了不同信息系统的特点。指南也可用来规定标准的的开发方式，或者保证对一般性安全原则的遵守。彩虹系列、CC、BS7799等，都可以看作是此类。
- **基线**——基线建立的是满足方针要求的最低级别的安全需要。在建立信息安全整体框架之前，基线是需要考虑的最低标准。标准的开发通常都是以基线为基础的，基线可以看作是抽象的简单化的标准。大多数基线都是很具体的，或者与系统相关，或者是陈述某种配置。
- **程序**——是执行特定任务的详细步骤。位于策略链的最低层次，是实现方针、标准和指南的详细步骤。

安全策略的层次模型


方针 Policy
目标要求
强制性
标准 Standard
建议性
指南 Guideline
最低标准
基线 Baseline
实现方法
程序 Procedure
具体步骤
战略层次
战术层次

安全策略不同层次不同作用

- 方针作为最高级别的管理层陈述，它说明了需要保护的对象和目标(What)
- 标准和指南规定了用来保护特定对象的技术和方法
- 程序则是对执行保护任务时具体步骤的细节描述（How）。
- 例如，某个公司在其安全方针中声明：所有的机密信息必须得到加密保护。这种声明是很宽泛而模糊的，这时候，一个强制性的标准进一步指出：所有保存在数据库中的客户信息必须采用DES算法进行加密，数据的传输必须使用IPSec这一VPN技术。具体执行安全策略时，相应的程序会详细解释怎样实施DES及IPSec技术。对于某些意外的情况，比如数据传输过程中遭受的窃取或破坏，相应的处理方法就可以通过指南来描述。

重要的角色

- 用户 (User)
- 高级管理者 (Senior management)
- 安全官 (Security Officer)
- 信息系统安全专家 (Information systems security professionals)
- 数据属主 (Data owners)
- 保管者 (Custodian)
- 灾难恢复/应急计划人员 (BCP and DRP Planners)
- 安全管理员 (Security Administrators)
- 网络/系统管理员(Network/Systems Administrators)
- 信息系统审计师 (Information systems auditor)
- 帮助台 (Help desk)

三道防线

第一道防线：所有业务部门及职能部门。其中，风险管理职能部及内部审计职能部门是第一道防线的核心。各部门一线员工是企业的窗口，也是最先与风险源接触的群体，在日常业务中负有及时识别、上报与初步管理风险的职责，是事前控制风险的关键。

第二道防线：风险管理委员会及风险管理职能部门。这两个机构不直接参与企业任何经营业务，而主要负责企业风险管理工作的统筹组织、协调与规划，并对第一道防线的风险管理工作、内部控制开展情况进行实时监控，同时承担重大风险的核心管理与组织职责，是事中控制风险的关键。

第三道防线：内部审计委员会及内部审计职能部门。这两个机构也不直接参与企业任何经营业务，主要负责对第一及第二道防线部门的工作进行事后稽核、审计和监察等，对企业内部控制度进行查漏补缺、对企业主要业务流程的合规性、合理性和风险可控性进行审计、对经营管理者进行经济责任审计、对企业信息系统有效性进行审计、对企业财务报表进行审计等，是事后控制风险的关键，也是最后一道防线。

内部控制目标

- 内部控制由控制环境、控制风险、控制活动、信息与沟通以及监控组成，是一个覆盖整个经济实体的系统 。
- 控制类型
- 内部会计控制：会计运营，如资产保护和财务记录的可靠性；
- 运营控制：日常运营、职能和活动，确保运营满足业务目标的要求；
- 管理控制：关注职能部门的运营效率、运营控制是否符合管理层政策，是以保证运营控制的效率和对组织政策的符合程度为目标的控制

内部控制目标

- 内部控制的目标是实施控制活动（程序）想要达到的结果和目的。
- 示例
  - 保护IT资产
  - 符合公司政策和法规的要求
  - 授权和认证
  - 机密性
  - 数据准确性和完整性
  - 处理的可靠性
  - IT服务的可用性
  - 运营效率和经济性
  - IT及相关系统的变更管理

IS控制目标

- 保护资产
- 确保操作系统环境（包括网络管理和运行）的完整性
- 保护敏感及关键的应用系统环境，包括财务及管理信息（信息目标）和客户数据的完整性
  - 输入授权
  - 输入确认
  - 交易处理的准确性和完整性
  - 信息处理活动的整体可靠性
  - 输出的准确性
  - 数据库的完整性、可用性和机密性

IS控制目标

- 确保对IS资源（包括基础设施支撑）用户的恰当识别和验证
- 确保运行的效率和效果（运行目标）
- 符合用户需求、组织政策和规程，并遵从法律、法规的要求（符合性目标）
- 制定有效的业务连续性计划（BCP）和灾难恢复计划（DRP），确保IT服务的可用性
- 制定事件响应计划，确保系统的完整性和可靠性

一般控制

- 内部会计控制：主要针对会计操作，关注资产保护和财务记录的可靠性；
- 运营控制：关注日常运营、职能和活动，确保运营满足业务目标的要求；
- 管理控制：关注职能部门的运营效率、运营控制是否符合管理层政策，是以保证运营控制的效率和对组织政策的符合程度为目标的控制
- 确保恰当使用信息和技术资产的组织安全政策和规程
- 在设计和使用充分的文档与记录方面的总体政策，以确保交易的正确记录
- 确保充分保护资产和设施的访问及使用的安全保护流程和实务
- 数据中心和IT资源的物理、逻辑安全政策

IS控制

- 战略和方针
- 全面的组织和管理
- IT资源的访问，包括数据和程序
- 系统开发方法和变更控制
- 运行规程
- 系统编程及技术支持职能
- 质量保证（QA）流程
- 物理访问控制
- 业务连续性计划（BCP）、灾难恢复计划（DRP）
- 网络和通讯
- 数据库管理
- 对内、外部攻击的检查和保护机制

实施信息系统审计

- 一般原则
- 审计计划
- 信息技术风险评估
- 审计内容
- 审计方法
- 审计报告和后续工作

信息系统审计的一般原则

- 信息系统审计可作为独立的审计项目组织实施、或作为综合性内部审计项目的组成部分实施。
- 信息系统审计划分为以下阶段：
  - 审计计划阶段
  - 审计实施阶段
  - 审计报告
  - 后续工作阶段
- 审计人员应采用以风险为导向的审计方法进行信息系统审计，风险评估应贯穿审计的计划、实施、报告与后续工作各个阶段 。

审计计划

- 内部审计人员在执行信息系统审计之前，需要确定审计目标并初步评估审计风险，估算完成信息系统审计或专项审计所需的资源，确定重点审计领域及审计活动的优先次序，明确审计组成员的职责，并以此制定信息系统审计计划。
- 信息系统审计作为综合性内部审计项目的一部分时，审计人员在审计计划阶段还应综合考虑相关内部审计的审计目标及要求。

审计计划

- 制定信息系统审计计划时，应遵循其他相关内部审计具体准则规定的因素，同时针对信息系统审计的特殊性，审计人员还应充分考虑以下因素：
  - （一）高度依赖信息技术、信息系统的关键业务流程及相关的组织战略目标；
  - （二）信息技术管理的组织架构；
  - （三） 信息系统框架和信息系统的长期发展规划及近期发展计划；
  - （四）信息系统及其支持的业务流程的变更情况；
  - （五）信息系统的复杂程度；
  - （六） 以前年度信息系统内、外部审计等相关的审计发现及后续审计情况。

信息技术风险评估

- 进行信息系统审计时，审计人员应当识别组织所面临的与信息技术相关的内、外部风险
- 信息技术风险是指组织在信息处理和信息技术运用过程中产生的、可能影响组织目标实现的各种不确定因素。信息技术风险包括组织层面的信息技术风险、一般性控制层面的信息技术风险及业务流程层面的信息技术风险等。

信息技术风险评估

- 审计人员在识别、评估组织层面、一般性控制层面的信息技术风险时需要关注以下几方面：
  - （一）业务关注度，即组织的信息技术战略与组织整体发展战略规划的契合度以及信息技术（包括硬件及软件环境）对业务和用户需求的支持度；
  - （二）信息资产的重要性；
  - （三） 对信息技术的依赖程度；
  - （四）对信息技术部门人员的依赖程度；
  - （五） 对外部信息技术服务的依赖程度；
  - （六）信息系统及其运行环境的安全性、可靠性；
  - （七）信息技术变更；
  - （八）法律规范环境；
  - （九） 其他。

信息技术风险评估

- 业务流程层面的信息技术风险受行业背景、业务流程的复杂程度、上述组织层面及一般性控制层面的控制有效性等因素的影响而存在差异。一般而言，审计人员应了解业务流程并关注以下几方面信息技术风险：
- （一）数据输入；
- （二）数据处理；
- （三）数据输出。

信息技术风险评估

- 审计人员应充分考虑风险评估的结果，以合理确定信息系统审计的内容及范围，并对组织的信息技术内部控制的设计有效性和执行有效性进行测试。

信息系统审计的内容

- 信息系统审计通常包括对组织层面信息技术控制、信息技术一般性控制及业务流程层面相关应用控制的审计。
- 信息技术内部控制的各个层面都包括人工控制、自动控制和人工、自动相结合的控制形式

信息系统审计的内容

- 信息技术一般性控制是指与网络、操作系统、数据库、应用系统及其相关人员有关的信息技术政策和措施，以确保信息系统持续稳定的运行，支持应用控制的有效性。对信息技术一般性控制的审计应考虑以下控制活动：
  - （一）信息安全管理
    - 组织的信息安全管理政策，物理访问及针对网络、操作系统、数据库、应用系统的身份认证和逻辑访问管理机制，系统设置的职责分离控制等；
  - （二）系统变更管理
    - 组织的应用系统及相关系统基础架构的变更、参数设置变更的授权与审批，变更测试，变更移植到生产环境的流程控制等；
  - （三）系统开发和采购管理
    - 组织的应用系统及相关系统基础架构的开发和采购的授权审批，系统开发的方法论，开发环境、测试环境、生产环境严格分离情况，系统的测试、审核、移植到生产环境等环节；
  - （四）系统运行管理
    - 组织的信息技术资产管理、系统容量管理、系统物理环境控制，系统和数据备份及恢复管理，问题管理和系统的日常运行管理等。

信息系统审计的内容

- 业务流程层面应用控制是指在业务流程层面为了合理保证应用系统准确、完整、及时完成业务数据的生成、记录、处理、报告等功能而设计、执行的信息技术控制。对业务流程层面应用控制的审计应考虑以下与数据输入、数据处理以及数据输出环节相关的控制活动：
  - （一）授权与批准；
  - （二） 系统配置控制；
  - （三） 异常情况报告和差错报告；
  - （四） 接口/转换控制；
  - （五） 一致性核对；
  - （六） 职责分离；
  - （七） 系统访问权限；
  - （八） 系统计算；
  - （九） 其他。

信息系统审计的方法

- 审计人员在进行审计与信息技术相关内部控制及流程中可以单独或综合应用下列的审计方法来获取充分、适当的审计证据以评估信息技术内部控制的设计有效性和执行有效性：
  - （一）询问相关的控制人员；
  - （二）观察特定控制的运用；
  - （三） 审阅文件和报告；
  - （四）根据信息系统的特性，进行穿行测试，追踪交易在信息系统中的处理过程；
  - （五）验证系统控制和计算逻辑；
  - （六）登录信息系统进行系统查询；
  - （七）利用计算机辅助审计工具和技术；
  - （八） 保证独立性、客观性及职业技能的质量控制前提下，利用其他专业机构的审计结果或组织对信息技术内部控制的自我评估结果；
  - （九）其他

信息系统审计的方法

- 信息系统审计人员可以根据需要利用计算机辅助审计工具和技术进行数据的验证、关键系统控制/计算的逻辑的验证、审计样本选取等；审计人员在充分考虑安全的前提下，可以利用可靠的信息安全侦测工具进行渗透性测试等。
- 审计人员在对信息技术内部控制进行评估时，应获得充分、可靠及相关的审计证据以支持审计结论完成审计目标，并应充分考虑系统自动控制的控制效果的一致性及可靠性的特点，在选取审计样本时可根据情况适当减少样本量。在系统未发生变更的情况下，可考虑适当降低审计频率。

信息系统审计的方法

- 审计人员在审计过程中进行风险评估，并在此基础上依据信息技术内部控制评估的结果重新评估审计风险，并根据剩余风险来进一步设计审计程序。
- 审计工作底稿应以正式的书面或电子形式进行记录，其中应包含审计程序、审计发现和审计结论以及支持审计结论的审计工作细节及审计证据。审计过程中获取的电子数据应建立严格的电子数据归档措施，并对敏感数据进行严格的保密管理。

审计报告与后续工作

- 在审计实施结束后，审计人员应以充分、可靠及相关的审计证据为依据形成审计结论与建议，出具审计报告，形成审计结果，追踪审计建议的落实并执行相应后续审计程序。
- 当信息系统审计作为综合性内部审计项目的一部分时，审计人员应及时与其它相关内部审计人员沟通信息系统内部审计的发现，并考虑依据审计结果调整其他相关审计的范围、时间及性质。

审核策划

- 管理层授意
  - 管理承诺
  - 明确内审要求和目标
  - 规定职责权限
  - 主持管理评审
  - 提供必要的资源

审核策划

- 建立内审程序
  - 目的：回答为什么编写此程序。
  - 范围：本程序适用于哪些部门、区域、过程和活动。
  - 术语和定义：本程序中出现的具有特定含义的词汇或专业术语。
  - 职责：主管部门/人，分主管部门/人，配合部门/人。
  - 控制程序和要求：回答5W1H（What？Why？Where？Who？When？How？）。
  - 相关文件：对其他相关控制程序的全文或部分引用。
  - 相关记录：与此程序相关的记录文件的全文或部分引用

审核策划

审核小组组长

协助管理者选择审核组其他成员；
制定审核计划；
组织审核活动，控制协调进度，保证按计划完成审核任务；
组织召开审核会议；
代表审核小组与受审核方管理层接触；
提交审核报告。

审核小组成员

熟悉必要的文件和程序；
根据要求编制检查列表；
传达和阐明审核要求；
配合支持审核组长的工作，有效完成审核任务；
将观察结果形成文件，并报告审核结果；
跟踪验证纠正措施的有效性；
收存和保护与审核有关的文件

	审核组长	审核员
资格	必须是信息安全管理体系内审员（有权威资质），并由信息安全管理经理指定	必须参加过信息安全管理体系审核员培训并考核合格，由管理层任命
业务范围	应与被审核部门无直接责任关系，但对被审核部门的业务有一定了解	其专业最好与被审核部门业务相适应，但也不强求一致，应与被审核的工作无直接责任关系
知识经验	应有较多的审核经验	对被审核部门业务知识有一定了解，但不强调是此方面专家
组织协调	应有组织管理整个审核工作的能力	有协调配合和团结合作的精神，应该被受审核部门接受

审核准备

- 制定审核计划
  - 目的：申明组织实施内部审核的目标。
  - 时间安排：审核时间通常要避免与组织重要业务活动发生冲突，审核频次与体系稳定性及组织信息系统风险状况有关，但至少应该一年一次，且能覆盖所有安全管理区域。对于发生重大信息安全事件等特殊情况，还应追加审核。
  - 审核类型：年度计划的方式可以采用分散/滚动方式，也可以采用集中的方式。前者一般是在通过第三方审核认证后被采用的，特点是持续时间长、多频次审核等；
  - 后者是在某计划时间内集中安排的审核，可以针对全部适用过程和部门，也可以针对某些特定过程或部门，通常适用于新建信息安全管理体系运行后，或者体系有重大变化，发生重大事故，或外部审核之前。
  - 其他考虑因素：范围、审核组织、审核要求、特殊情况等。

审核准备

- 准备检查列表
  - 明确与审核目标有关的抽样问题；
  - 使审核程序规范化，减少审核工作的随意性和盲目性；
  - 保证审核目标始终明确，突出重点，避免在审核过程中因迷失方向而浪费时间；
  - 更好地控制审核进度；
  - 检查列表、审核计划和审核报告一起，都作为审核记录而存档。

审核准备

- 实施文件审核
  - 文件审核通常包括两个阶段，一个是文件初审，一个是现场审核时的文件审查
  - 信息安全方针和目标声明；
  - 信息安全管理手册；
  - 风险评估报告；
  - 风险处理计划；
  - 组织为确保其信息安全过程有效策划、操作和控制所需的程序文件和作业指导文件，包括文件控制程序、记录控制程序、管理评审程序、内审程序、纠正与预防措施控制程序等；
  - 信息安全管理体系所要求的记录；
  - 实施安全控制措施的摘要，即适用性声明（Statement of Applicability，SoA）；
  - 体系文件清单。

审核实施

- 现场审核
  - 坚持以“客观证据”为依据的原则；
  - 坚持标准与实际核对的原则；
  - 坚持独立、公正的原则；
  - 坚持“三要三不要”原则：要讲客观证据，不要凭感情、凭感觉、凭印象用事；要追溯到实际做得怎样，不要停留在文件、口头上；要按审核计划如期进行，不要“不查出问题非好汉”。

温馨提示

•ITIL先锋论坛专家直播讲堂，每周四晚上8:30指定QQ大群

•专家讲堂视频&PPT合集，请猛击链接

•看预告&PPT更新，请关注右边二维码

•找培训，请看下图：

谢谢