

图书基本信息

书名：<<全球信息系统审计指南（上下册）>>

13位ISBN编号：9787511900777

10位ISBN编号：7511900771

出版时间：1970-1

出版时间：中国时代经济

作者：王光远 编

页数：586

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

## 前言

本书中IIA所使用的“技术审计”，其实质就是信息系统审计。

20世纪60年代IBM出版《Audit Encounters Electronic Data Processing》一书，首次提出计算机审计概念，随着计算机技术的不断普及和发展，其审计的内涵和外延也不断拓展，进入21世纪，信息系统审计框架逐渐形成。

原本，信息系统审计与组织内部的管理审计是沿着技术和管理两条路线并行发展的，但因计算机应用技术逐步发展到信息技术和网络技术，并从早期的辅助应用演进为与企业的经营活动相融合，于是，相对独立的信息技术就从纯技术层面走向与财务管理、会计核算、组织营运等活动相融合的技术经济综合体。

计算机技术的应用与发展，改变了企业、机关等组织的作业环境和作业条件，使现代企业运营对于信息技术与网络依赖与日俱增。

在遵从SOX法案的过程中，尤其是在规范企业管理方面，信息系统起着极为重要的作用，因此，信息系统审计与内部管理审计相融合成为历史的必然。

2005年，IT治理协会第三次修订了“信息及相关法律控制目标（Control Objectives for Information and Related Technology）”框架（简称COBIT4.0），它与COSO和SOX紧密结合，将IT治理和IT控制纳入组织治理和组织内部控制范畴，该框架的颁布，加速了信息系统审计与内部管理审计的结合。

## 内容概要

《全球信息系统审计指南（套装上下册）》中IIA所使用的“技术审计”，其实质就是信息系统审计。

20世纪60年代IBM出版《Audit Encounters Electronic Data Processing》一书，首次提出计算机审计概念，随着计算机技术的不断普及和发展，其审计的内涵和外延也不断拓展，进入21世纪，信息系统审计框架逐渐形成。

## 书籍目录

译序1 信息技术控制1.1 主席的信1.2 执行摘要1.2.1 IT控制的介绍1.2.2 理解IT控制1.2.3 IT控制的重要性1.2.4 IT的角色和职责1.2.5 分析风险1.2.6 监督和技术1.2.7 IT控制评估1.3 介绍1.4 评估IT控制——概述1.5 理解IT控制1.5.1 控制分类1.5.2 治理管理技术1.5.3 IT控制——期望目标1.5.4 信息安全1.5.5 IT控制框架1.6 IT‘控制的重要性1.7 组织中IT的角色1.7.1 董事会理事机构1.7.2 管理1.7.3 审计1.8 分析风险1.8.1 风险决定的反应1.8.2 决定IT控制充分性的风险因素1.8.3 风险缓解策略1.8.4 考虑控制的特性1.8.5 基线IT控制1.9 监控(Monitoring)与技术(Techniques)1.9.1 选择一个控制框架1.9.2 监督IT控制1.10 评估1.10.1 可以使用哪些审计方法1.10.2 测试IT控制和持续鉴证1.10.3 审计委员会 / 管理层 / 审计接口1.11 结论1.12 附录A——信息安全计划要素1.13 附录B——法律和条例的遵守以及相关执行情况的指导1.14 附录C——内部审计人员IT知识的三个类别1.15 附录D——遵守框架1.16 用COSO评估IT控制1.16.1 内部控制定义1.16.2 COSO内部控制整体框架1.17 ITGI的信息和相关技术控制目标CobiT1.18 审计委员会考虑到IT控制度量1.18.1 董事会 / 董事的度量1.18.2 管理层的度量1.19 CAE的检查表1.20 参考文献1.20.1 治理1.20.2 管理1.20.3 技术问题1.20.4 IT审计1.21 词汇表1.22 关于全球技术审计指南GTAG计划的合作方1.23 合作者和全球项目组1.23.1 IT控制咨询理事会1.23.2 合作组织1.23.3 项目审评小组1.23.4 国际分支机构1.23.5 其他国际组织1.23.6 国际先进技术委员会1.23.7 撰写组1.23.8 总部员工产品组2 变更和补丁管理控制：组织成功的关键2.1 执行摘要2.1.1 为什么控制变更和补丁管理中一定要有首席审计执行官2.1.2 快速识别不良的变更管理2.1.3 理解怎样有效管理IT变更2.1.4 降低IT变更风险的五大步骤2.1.5 内部审计人员的作用2.2 介绍2.2.1 为什么IT变更和补丁管理重要2.2.2 IT变更和补丁管理如何帮助控制IT风险和成本2.2.3 什么可行和什么不可行2.2.4 如何确定IT变更和补丁管理是否正常发挥作用2.2.5 内部审计人员应该做什么2.2.6 C10和CAE之间的启发性对话2.3 为什么应该关注组织变更管理的方法2.3.1 变更产生风险：为什么必须把补丁作为一种变更2.3.2 我们已经有了变更管理流程——差别在哪里2.3.3 稳健的变更管理流程如何发挥作用2.4 定义IT变更管理2.4.1 什么是变更管理的范围2.4.2 无效的变更管理看起来是怎样的2.4.3 有效的变更管理看起来是怎样的2.4.4 变更管理度量和指标2.4.5 把补丁管理整合到变更管理中2.4.6 指南的原则：如何决定是否需要实施变更、何时变更、如何变更2.5 我应该就变更和补丁管理提什么问题...3 连续审计：对保证、监控和风险评估的意义4 IT审计管理5 管理和审计隐私风险6 IT薄弱的管理与审计7 信息技术外包8 应用控制审计9 身份和访问管理10 业务持续性管理11 制订IT审计计划12 IT审计项目

## 章节摘录

插图：缓解关键的薄弱点通常情况下，缓解关键薄弱点的最有效的途径是让IT安全职员运用现有的事件或故障测试系统。

这个系统是标准IT操作程序的一部分，它能够确保相关人员及时修复发现的薄弱点。

创建一个减轻薄弱点的程序确定最关键的薄弱点能够显著消除风险。

这应该是一个非常快速的执行过程，因为往往这样的薄弱点不会太多。

但当你试图一次修护成百上千的薄弱点时，很多不同的挑战就会接踵而至。

此时，最有效的方法就是去创建一个包含有一位项目经理，一套交付过程和一个截止期限的IT项目来修复这些薄弱点。

那么这个项目就必须获得整合组织基础设施管理流程的授权并安装必要的补丁。

因此，想要不断重复并有效率地实施薄弱点管理，其最有效的途径便是实施一套依据组织基础设施管理流程而精心设计的薄弱点管理项目。

依此类推，我们同样可以考虑建立一个软件应用公司的开发团队。

通过建立应用程序的生命周期来开发高质量的软件，并且开发团队也意识到一项产品如果要不断发展，那就必须不断开发产品的新特征。

他们采纳这些特征，依据其商业价值和作用将其分级；随后开发、测试，最后推出该产品。

他们通过运用能让股东们认同他们的动机、角色和职责的保证过程来做到这一切。

例如，一个开发团队可能会要求来自IT职员的额外的基础设施来支持某一项业务应用。

当然，这样的结果自然会影响到IT的成本、数据传递或配置，但是却有利于达到组织的目标和期望。

成功执行一个有效的薄弱点管理项目有赖于与IT管理团队相类似的IT安全团队的介入。

项目的成功也取决于指定一套薄弱点管理过程并将它传达给IT管理团队，这就如同将另一项计划的工作加到了原本的工作领域上。

包括数据传递、职责和薄弱点的确认在内的这些项目细节都成为日益庞大的IT运作过程的组成部分。

编辑推荐

《全球信息系统审计指南(套装上下册)》：内部审计前沿报告书系。

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>