

解决方案：立足萨班斯法案电信安全解决方案 PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/202/2021_2022__E8_A7_A3_E5_86_B3_E6_96_B9_E6_c40_202195.htm 萨班斯(SOX)法案内控审计要求的出台，提升了IT控制在企业内部控制中的重要性，对电信运营商IT设施的安全性提出了更高的要求，如何改进IT控制和完善IT治理，是电信运营商的CIO们面临的新挑战。潜心关注电信行业安全并不断创新的启明星辰信息技术有限公司结合多年在安全领域的丰富经验与最佳实践，推出了针对电信运营商SOX内控的系列安全解决方案，从宏观到微观，包括ISO27001安全认证咨询服务解决方案、安全域解决方案、4A(账号、认证、授权、审计)统一安全管理平台解决方案、以及面向业务保障的安全服务体系解决方案。

一、ISO27001安全认证咨询服务解决方案 近年来，国家出台了一系列信息安全的法律法规，信息产业部已将安全与业务准入挂钩，与此同时，海外政府、资本市场提出的新监管要求(如：SOX法案)的强制执行都要求运营商进一步遵守安全内控要求。放眼电信市场，各大运营商的“转型”都在寻找新的蓝海，IT与电信迅速融为一体成为ICT，而IT为传统通信产业注入无限活力的同时，也引发了大量安全问题，能否解决这些安全问题，已成为运营商与竞争对手拉开差距的关键，并已成为新的业务增长点。在此背景下，各大运营商需要建立完善的信息安全管理体系(ISMS)，通过国际权威机构的安全认证，并不断巩固完善，旨在赢得国内外客户的信任与国际资本市场的青睐，为企业的持续健康发展保驾护航。相关国际标准与法案 来源：www.examda.com 作为建立信息安全管理

体系(ISMS)的重要规范，BS7799标准被ISO组织采纳后，衍生为ISO 17799《信息安全管理体系实施细则》和ISO 27001《信息安全管理体系规范》。ISO 17799是建立并实施信息安全管理体系的指导性标准，ISO 27001是对信息安全管理体系进行审核的依据性标准。获得ISO 27001认证是企业拥有完善的信息安全管理体系的象征。萨班斯(SOX)法案是另一部更加具有国际性影响的规章，始创于2002年，由美国证券交易委员会(SEC)提交，是一部旨在消除企业财务欺诈行为和弊端的历史性法案，它要求在美国上市的所有企业必须通过该法案审核。ISO 17799/27001与定义信息治理过程的COBIT标准和COSO框架共同健全了萨班斯法案中与安全和内控审计相关的404条款。启明星辰安全认证、咨询服务解决方案 启明星辰公司积极参照ISO 17799/27001和COBIT为客户提供安全认证、咨询服务，最终达到符合SOX法案的要求。同时我们也意识到，安全认证的真正目的不仅仅是为了获得证书，更重要的是建立切实的网络和业务安全体系，帮助运营商争取更多的用户，特别是高端的国际型用户与投资，在此基础上，将SOX内控审计落实到具体的运营工作中、塑造卓越的运维队伍、驱动更大的经济效益。应该看到，安全管理具有宏观、中观和微观三重层次，ISO 27001在宏观安全管理体系规划方面有很好的定义，但中观调整、特别是微观实现方面实际上是留待各实施机构根据各自情况自行解决，换句话说，ISO 27001偏重从宏观角度提供理论指导。执行ISO 27001、符合ISO 27001，必须结合运营商的主业、从中观和微观角度加以落实。启明星辰公司为运营商提供立体的ISO 27001防御体系，涉及宏观规划和监控、中观整合加固、微观技术实现

，每个层面上又纵深提供评估服务、应急服务、技术培训和
技术支撑，真正做到将ISO 27001认证落实到安全运维人员每
天可执行的技术、工具、平台、流程、规章等各个层次。收
益 启明星辰公司承诺所提供的安全认证、咨询服务针对运营
商的不同系统量体裁衣，协助运营商除获得认证证书之外，
落实并巩固安全认证成果，包括：|制定切实可操作的安全规
范与安全策略.|实施网络安全优化方案. 来源

：www.examda.com |对系统进行深层次的安全评估并提交安
全加固建议.|提供电信级应急响应服务.|提供专业的安全管
理和安全技术培训.|实施全面的安全监控 来源

：www.examda.com二、安全域解决方案 划分安全域的原则 安
全域是指同一环境内有相同的安全保护需求、相互信任、并
具有相同的安全访问控制和边界控制策略的网络或系统。启
明星辰公司采用“同构性简化”的安全域划分方法，将复杂
的大网络进行简化后设计防护体系，以便进行有效的安全管
理。启明星辰公司安全域划分遵循以下原则：1、业务保障
原则. 2、结构简化原则. 3、立体协防原则。 来源

：www.examda.com 以某运营商系统为例，我们通过对该系统
进行数据流分析、网络结构分析，结合考虑现有的安全隐患
，从资产价值、脆弱性、安全隐患三者间的关系出发，得到
了整体的安全防护体系和各个业务系统自身的安全防护体系
，为进一步管理整合后的安全域做好了准备。基于安全域划
分的最佳实践，该运营商的各个系统被分别划入不同的安全
域，再根据每个安全域内部的特定安全需求进一步划分安全
子域，包括：核心交换区、核心生产区、日常办公区、接口
区、安全管理区、内部系统接入区、外部系统接入区。

100Test 下载频道开通，各类考试题目直接下载。详细请访问
www.100test.com