**信息系统安全控制**

**内部审计方案**

# **审计目标**

评估关键信息系统安全控制的有效性。

# **审计标准**

本次审计依据目前国际上通用的信息系统审计的标准COBIT（Control Objectives for Information and related Technology），该标准由信息系统审计与控制协会在1996年公布，是一个在国际上公认的、权威的安全与信息技术管理和控制的标准，目前已经更新至5.0版。它在商业风险、控制需要和技术问题之间架起了一座桥梁，以满足管理的多方面需要。该标准体系已在世界一百多个国家的重要组织与企业中运用，指导这些组织有效利用信息资源，有效地管理与信息相关的风险。

# **审计范围**

1. **审计期间**

2017年1月1日至2017年12月31日。

1. **关键信息系统**

信天游管理系统、邮件系统、VPN系统。

1. **关键数据**

业务数据、财务数据、邮件、访问日志。

# **审计内容**

1. 系统层面

系统层面安全审计对象包括系统安全技术、计算机病毒防治、远程访问安全。在对设备层面审计重点是对各种系统生成的日志、操作日志进行审计。

具体审计内容如下：

|  |  |  |  |
| --- | --- | --- | --- |
| 审计对象 | 审计内容 | 具体审计项 | 审计方法 |
| 系统安全技术 |  操作系统安全性 |  查看操作系统安全日志文件   查看管理员操作日志文件   查看文件访问记录   对用户权限分配情况进行抽查，重点关注各管理员权限的划分情况   进行系统漏洞扫描 | 利用集中日志管理系统完成日志信息的收集和处理；如果系统中没有集中日志管理系统选择人工收集。 |
| 计算机病毒防治 |  防病毒系统的安装情况   防病毒系统运行情况   系统病毒数据库更新情况   用户病毒数据库更新情况 |  抽查计算机用户的PC机是否安装了系统统一规定防病毒程序，并检查程序的内部设定   抽查计算机用户PC机上的病毒数据库版本   随机测试防病毒系统功能   查看防病毒系统的运行日志文件   检查防病毒系统的病毒数据库的版本 | 人工收集和审计 |
| 远程访问安全 |  远程访问身份验证   远程访问权限分配   远程访问通讯加密   远程访问性能   远程访问服务器和系统的安全性 |  查看远程访问安全日志文件   查看远程访问控制设定   查看远程访问服务器的性能日志文件   对远程访问服务器进行漏洞扫描   对传送的数据实行“电子侦听”测试 | 人工收集和审计 |

1. 应用层面

应用层面审计重点是对应用系统生命周期管理的审计，包括：应用软件开发安全、应用系统运行安全、数据库安全、数据备份和恢复等方面。

具体审计内容如下：

|  |  |  |  |
| --- | --- | --- | --- |
| 审计对象 | 审计内容 | 具体审计项 | 审计方法 |
| 软件开发安全 | 软件开发环境  软件测试规定和执行情况  软件开发文档管理规定和执行情况  测试系统的升级 | 查看软件开发规范、关键数据的加密算法  查看软件开发环境设计和实施方案  抽查软件开发项目文档和有关技术文档  抽查软件测试记录  查看软件开发系统的备份记录  查看测试系统升级（升级到生产系统）计划和有关实施文档 | 人工收集及审计 |
| 应用系统运行安全 |  业务主机安全性   业务主机备份和恢复 |  查看业务主机安全日志文件   查看业务主机管理员操作日志文件   查看文件访问记录   查看数据备份策略、记录   进行主机漏洞扫描   检查所有用户的权限分配情况 | 利用集中日志管理系统完成日志信息的收集和处理；  其他采用人工收集和审计。 |
| 数据库安全 |  数据库用户设定和权限分配   数据库访问身份验证   数据库完整性   数据库访问性能 |  查看数据库安全日志文件   查看数据库性能日志文件   查看数据库用户和用户组设定以及相应的权限设定   运行数据库健康测试工具，检查数据库内数据和数据关系的完整性 | 利用集中日志管理系统完成日志信息的收集和处理；  其他采用人工收集和审计。 |
| 数据备份和恢复 |  数据备份和恢复计划和执行情况   备份应用程序 |  查看备份应用程序的运行日志文件   查看备份介质记录   查看备份介质管理记录   查看备份和恢复操作记录 | 人工审计 |

1. 业务层面

业务层面的安全重点是对账号集中审计管理以及对关键业务操作行为的审计。

|  |  |  |  |
| --- | --- | --- | --- |
| 审计对象 | 审计内容 | 具体审计项 | 审计方法 |
| 账号管理 | 对账号分配情况的审计  账号创建情况审计  账号变更情况审计 | 账号的创建时间、创建人，从账号的创建时间、创建人信息审计；  账号的变更时间、变更人、变更内容审计；  账号冻结、解冻时间、操作人员审计；  将从账号分配给从账号的分配时间、分配者，主、附属账号的有限期等。 | 通过集中账号管理系统收集账号的审计数据  如果没有集中账号管理系统采用人工审计 |
| 账号授权 | 对账号授权过程审计。  对账号当前使用权限审计 | 包括账号的访问权限，查询资源的授权访问者，权限的分配时间、分配者等；  账号权限变更时间、变更人员、变更内容审计；  账号当前对应的权限是否与该账号所进行操作的对应的权限一致。 | 通过集中账号管理系统收集账号的审计数据  如果没有集中账号管理系统采用人工审计 |
| 登陆行为 | 成功登陆  失败登陆  登陆顺序 | 包括什么人用什么账号在什么时间登录了什么系统，什么时间登出等；  账号失败登陆使用的账号、频率、时间等；  同一个账号在一段周期（可设置）内登陆业务系统的顺序。 | 通过集中账号管理系统收集账号的审计数据  如果没有集中账号管理系统采用人工审计 |
| 业务操作 | 网络管理行为审计 | 对在维护工作中使用FTP/Telnet的各种操作进行审计，获得全部操作记录和结果；  实现ftp/telnet命令级细粒度访问策略审计；  对ftp/telnet的操作执行回放，还原操作内容。 | 必须通过业务行为审计手段收集网络管理行为数据，结合人工操作进行审计。 |
| 数据库操作审计   | 记录与登录者身份不符合的SQL命令、应用操作命令或流程；  基于对指定的数据库对象（如数据库、表、视图、存储过程等）和指定操作（如创建、修改、添加、删除等）进行审计；  基于自定义的关键字进行访问控制和审计；  通过审计输出界面，对SQL命令的截获、分析和还原，审计关键操作的结果；  实现对主流数据库的审计。 |
| 关键操作审计 | 对于系统配置数据的删除操作进行审计；  通过制定数据库关键字段、关键操作进行审计；  根据操作时序顺序对操作行为进行审计；  对于关键操作关联操作账号的权限范围进行审计； |
| 互联网访问行为（此项审计限于严格控制与互联网访问的系统中） | 互联网访问行为审计 | 邮件收发、Webmail发送审计；  VPN维护行为审计；  即时通讯、文件下载等行为审计 | 必须通过业务行为审计手段收集网络管理行为数据，结合人工操作进行审计。 |

# **时间预算**

。

# **人员安排**

。