ICS 35.020
L70

DB37

山　东　省　地　方　标　准

DB 37/T 3303—2018

信息安全技术 内控安全管理技术规范

2018－06－12 发布　　2018－07－12 实施

山东省质量技术监督局　发布

前　言

本标准按照GB/T 1.1-2009给出的规则起草。

本标准由潍坊市质量技术监督局提出并归口。

本标准起草单位：潍坊市智慧潍坊建设办公室、山东省计算中心（国家超级计算济南中心）、山东瑞宁信息技术股份有限公司、山东省经济和信息化发展研究院、山东华国信息安全技术有限公司、山东信息协会、山东电子商会、山东正中信息技术股份有限公司。

本标准主要起草人：胡延年、李刚、汉京宁、毕建秀、周鸣乐、朱秀美、朱珊珊、李旺、冯正乾、李波、李敏、王超逸、李强、张玉瑞、张建成、徐兵、刘波、戚元华、王玮、刘一鸣、王丽君。

本标准为首次发布。

信息安全技术 内控安全管理技术规范

1 范围

本标准规定了信息安全技术中用于内控安全管理的相关技术内容。

本标准适用于提供内控安全管理服务的机构及有内控安全管理需求的用户。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 22239-2008 信息安全技术信息系统安全等级保护基本要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

内控安全管理 internal security management

对组织内部IT系统的管理和维护人员（包括第三方IT外包服务人员）的运维行为进行的安全风险管理。

3.2

应用发布机制 application publishing mechanism

将某些应用系统所需的客户端运维软件集中安装、部署到特定系统，实现应用软件的集中管控。

3.3

管理员 Administrators

具有对IT系统管理职能的人员。根据职责不同分为运维管理员和密码管理员。运维管理员负责对IT系统运维权限的划分与操作员的管理；密码管理员负责IT系统账号密码的管理。

3.4

审计员 Auditor

负责对操作员、管理员的操作行为监督审计的人员的统称。

3.5

操作员 Operator

负责对IT系统运维的工作人员的统称。

4 缩略语

下列缩略语适用于本文件。

AD 活动目录（Active Directory）
FTP 文件传输协议（File Transfer Protocol）
HTTP 超文本传输协议（HyperText Transfer Protocol）
HTTPS 安全超文本传输协议（Hyper Text Transfer Protocol over Secure Socket Layer）
ID 标识符（IDentifier）
IP 网络协议（Internet Protocol）
IT 信息技术（Information Technology）
ITIL 信息技术基础架构库(Information Technology Infrastructure Library)
ITSS 信息技术服务标准(Information TechnologyService Standards)
KPI 关键绩效指标（Key Performance Indicator）
LDAP 轻量目录访问协议（Lightweight Directory Access Protocol）
Radius 远程用户认证系统（Remote Authentication Dial In User Service）
RDP 远程桌面协议（Remote Desktop Protocol）
SFTP 安全文件传输协议（Secure File Transfer Protocol）
SSH 安全外壳协议（Secure Shell）
SSL 安全套接层(Secure Sockets Layer)
SSO 单点登录（Single Sign On）
TELNET 远程通信协议（Telecommunications Network）
VNC 虚拟网络控制台（Virtual Network Console）

5 内控安全管理参考模型

5.1 内控安全管理参考模型如图 1 所示，模型中涉及人员、IT 系统、流程制度三个要素，人员是指维护和管理 IT 系统的人员，包括第三方外包维护人员。IT 系统包括但不限于主机、数据库、网络、中间件、应用程序等各类 IT 资源。流程制度是组织内部为规范 IT 运维行为、保证运维安全所制订的一系列流程化管理制度或工具。

5.2 内控安全管理是将人员对 IT 系统的运维过程结合组织自身的流程制度进行集中管控。包括对人员的管控和对 IT 系统的管控两个方面。对人员的管控采用三权分立原则。对 IT 系统的管控采用集中、统一的方式。

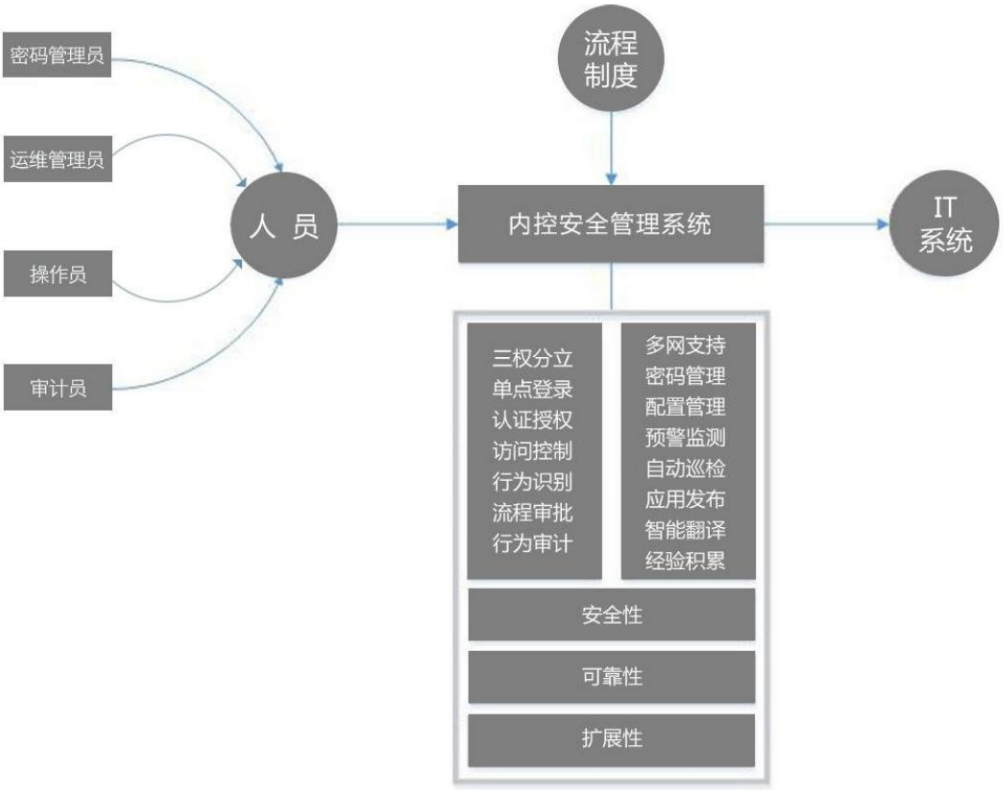

图1　内控安全管理参考模型

6　集中管控

6.1　三权分立

根据GB/T 22239-2008基本要求，信息系统管理应满足三权分立原则,分为管理员、操作员、审计员三类角色，每人分配一个唯一的身份ID。

6.2　身份 ID 集中管理

内控安全管理系统应支持人员身份ID的集中管理,支持分部门、分组管理人员，管理员负责操作员身份ID的创建和维护，操作员权限应与管理员、审计员的权限分开。

6.3　登录管理

6.3.1　单点登录

内控安全管理系统作为统一运维入口，操作员通过唯一身份ID认证后，能够直接访问要运维的IT系统，无需再次输入账号密码。

6.3.2　身份认证

登录内控安全管理系统时，应对人员身份ID进行认证，支持单种认证方式或多种认证方式的组合，认证方式包含但不限于：

a)　静态密码；

b)　动态密码；

c) 数字证书；
d) AD 域认证；
e) LDAP 认证；
f) 虹膜认证。

6.4 IT 系统授权

6.4.1 IT 系统授权应由管理员统一负责。

6.4.2 授权管理包括授权主体、授权客体和授权关系三个元素，内控安全管理系统应设置授权策略，包括：

a) 授权主体：
   1) 人员身份 ID、人员身份 ID 组或者二者的组合；
   2) 管理员为临时授权所创建的临时人员身份 ID。
b) 授权客体：IT 系统、IT 系统组、访问权限或者三者的组合；
c) 授权关系支持任意授权主体对任意授权客体的授权，在授权时效上支持有固定时效的长期授权和一次性临时授权；
d) 授权策略：
   1) 时间策略（包括时间周期、时间段，可精确到秒）；
   2) IP 策略（包括单个 IP 地址、IP 地址段和多个 IP 地址段的组合）；
   3) 命令策略（包括指令、指令参数和执行频次三个维度）。
e) 对 IT 系统的临时操作或关键操作要获得管理员的审批后才可运维。

6.5 行为管理

6.5.1 越权处置

内控安全管理系统应支持对越权访问的处置，处置方式包括阻断、告警或阻断同时告警。

6.5.2 行为识别

内控安全管理系统应对操作员的运维行为进行实时识别，对SSH、TELNET、FTP、SFTP等协议操作进行精确识别，对RDP、VNC等图形操作协议的识别应能鉴别操作步骤和目的，并能将操作行为转为文本日志，便于检索和控制。

6.5.3 行为控制

内控安全管理系统应对操作员的访问行为进行控制，对高危或非法操作实时阻断。

6.5.4 告警通知

内控安全管理系统包含以下告警通知：
a) 对 IT 系统的非正常状态告警；
b) 对违反安全策略的行为告警；
c) 对安全事件告警；
d) 告警方式可采取电子邮件、短信、移动 APP。

6.6 IT 系统账号集中管理

内控安全管理系统应支持IT系统账号的集中管理，IT系统账号包括被管辖的网络、主机、数据库、中间件等账号，IT系统账号应由密码管理员统一管理，操作员、审计员不应具有IT系统账号的管理权限。IT系统账号应采用加密方式集中存储在内控安全管理系统中。

7 行为审计

7.1 审计范围

7.1.1 审计管理由审计员统一负责。

7.1.2 审计范围包括对 IT 系统的访问和操作行为、内控安全管理系统自身的安全日志记录。

7.1.3 IT 系统的审计信息包括：

——操作系统的操作行为数据；

——网络设备及其他 IT 系统的操作行为数据；

——数据库、中间件等应用系统的操作行为数据。

7.1.4 内控安全管理系统的审计信息包括：

——账号管理数据；

——访问授权数据；

——登录数据；

——平台自身管理数据。

7.2 审计分析

内控安全管理系统应提供审计分析规则管理接口，审计员可自定义分析规则，应精确审计到人、时间、IP地址、IT系统、账户、指令、参数等关联关系，并定位人员身份ID。

7.3 审计信息分类

内控安全管理系统应支持对审计信息进行分类、多维度的处理，应至少包括：

——运维会话审计；

——全文检索审计；

——行为识别审计；

——实时审计。

7.4 审计信息分级

内控安全管理系统应支持根据审计信息的严重程度进行审计分级，可分为：严重、警告、一般。

7.5 审计信息过滤

内控安全管理系统应支持对审计信息进行过滤，包括：

——源、目的 IP 地址；

——时间；

——人员身份 ID/IT 系统账号；

——操作类型/操作名称；

——其他。

7.6 审计信息查询

内控安全管理系统应支持审计信息查询、审计报表生成、审计报表处理，报表包括不限于：

——审计报表；

——趋势报表；

——KPI 报表；

——知识报表。

7.7 审计预警

7.7.1 出现非法登录或操作时，内控安全管理系统可通过多种方式向审计员发送预警。

7.7.2 提供精准的审计预警规则管理功能，可根据系统特点和数据来源，对源 IP、目的 IP、时间范围、人员名、IT 系统名、操作命令等关键字段进行设置，产生预警规则。

7.7.3 根据预警规则，对接收到审计信息进行分析和处理，发现符合预警规则的审计信息，则自动生成预警信息。

7.7.4 预警信息的参数包括但不限于预警 ID、预警类型、预警级别、预警内容和生成时间。

7.7.5 预警信息的级别可分为严重、警告和一般。

7.7.6 预警信息的类型包括但不限于越权操作、敏感数据访问。

7.7.7 预警信息可通过多种方式通知审计员，比如：图形化界面显示、手机短信、电子邮件等。

7.8 分级审计

内控安全管理系统应支持分级审计功能，设置审计总中心和审计分中心，审计总中心对审计分中心下发数据采集策略，收集审计分中心上传的审计记录，进行集中统计分析，实现总中心对分中心的审计。

7.9 智能翻译

内控安全管理系统宜具有智能翻译功能，将操作员的英文操作指令等专业技术术语翻译成通俗的业务术语，便于非技术类审计员理解。

8 经验积累

内控安全管理系统可设置经验积累功能，将操作员的运维经验进行积累并分享，以提高操作员的技术水平。

9 IT 系统管理

9.1 多网支持

内控安全管理系统在安全范围内应支持跨多个相互隔离网络的运维管理功能，相互隔离网络的集中运维不应对原有网络造成影响，支持多个不同网络的IT系统同时集中运维。

9.2 应用发布

内控安全管理系统应支持应用发布功能。

9.3 账户密码管理

9.3.1 账户密码策略管理

密码策略应由密码管理员配置，密码策略管理应实现以下功能：

——密码强度管理，对人员身份 ID、IT 系统账号的强度进行管理，包括密码安全设置及修改、组成规则及校验策略等；

——密码有效期管理，能安全使用和更新，具备密码有效期验证、提醒以及过期或输错次数锁定、管理员激活等功能；

——密码存储管理，提供离线电子介质和非电子介质双介质保存，如电子密函、密码信封；

——密码更新管理，使用密码链条技术，确保每次密码变更安全可靠。

9.3.2 密码自动变更

9.3.2.1 根据 IT 系统账号的密码变更周期和密码生成策略，自动对 IT 系统账号进行密码变更。

9.3.2.2 在密码变更过程中，内控安全管理系统突然崩溃的极端情况下，应提供密码应急恢复机制，使用无源接触式硬件，在离线情况下，解密获取明文密码。

9.4 配置管理

IT系统的配置文件可定期、自动备份，包括：

a) 配置文件历史查询；

b) 配置文件自动备份；

c) 配置文件人工还原；

d) 配置文件自动比较。

9.5 预警监测

内控安全管理系统应能自动监测IT系统的中央处理器利用率、内存占用率、系统进程、表空间、磁盘剩余空间等信息，当达到阀值时以电子邮件、短信方式通知操作员，在故障发生前，及时消除故障隐患。

9.6 自动巡检

内控安全管理系统应支持根据巡检模板对IT系统进行自动巡检，模板格式、巡检参数可定制，巡检后的报告以电子图标格式发给操作员。

9.7 远程运维

在突发紧急运维情况下，内控安全管理系统应能通过远程操作协助操作员解决问题，应实时监控并记录远程协助过程，便于事后审计。

10 基础支持

10.1 可靠性

内控安全管理系统本身应支持双机冗余部署，支持日志文件与系统配置文件双同步，支持IT系统密码变更密函丢失情况下的密码找回。

10.2 安全性

内控安全管理系统自身应具备安全性：

a) 敏感信息加密传输；

b) 操作系统加密成只读镜像；

c) 系统与日志独立加密，双介质存储。

10.3 扩展性

内控安全管理系统应能提供扩展接口，与用户的IT运维流程系统（符合ITSS或者ITIL标准）对接，将用户的运维安全管理制度转化为实际可技术实现的运维管理策略。