**关于开展IT审计工作的请示**

公司领导：

为进一步提高公司信息系统权限管理水平，加强对系统运维人员的监督与管控，申请选聘第三方专业咨询机构开展中化信息公司层面信息化专项审计，系统性提高对重要信息系统非授权操作的监督检查。具体情况汇报请示如下：

**一、审计范围**

本次审计覆盖中化信息重要信息系统清单中包含的核心系统

1. **审计内容**

本次重点进行权限管理体系方面的审计主要从数据权限、访问控制、身份鉴别以及日志审计四个方面展开，重点检查运维人员权限与岗位职责是否匹配、权限申请流程是否健全等权限管理体系方面。在日志方面，重点检查2023年度系统操作日志中的非授权操作。

1. 数据权限
   1. 数据权限授权审批流程建设落实情况，是否明确用户账号分配、开通、使用、变更、注销等安全保障要求，是否对数据权限申请和变更进行审核，是否严格控制管理员权限账号数量；
   2. 系统管理员、安全管理员、安全审计员等人员角色分离设置和权限管理情况；
   3. 系统权限分配表建设及更新情况，用户账号实际权限是否满足最少够用、职权分离原则；
   4. 是否存在与权限申请审批结果不一致的情况；
   5. 是否存在多余、重复、过期的账户和角色；
   6. 是否存在共享账户和角色权限冲突的情况；
   7. 是否存在离职人员账号未及时回收、沉默账号、权限违规变更等安全问题；
   8. 数据批量复制、下载、导出、修改、删除等数据敏感操作是否采取多人审批授权或操作监督，并进行日志审计。
2. 访问控制
   1. 建立与数据类别级别相适应的访问控制机制情况，是否限定用户可访问数据范围；
   2. 是否在数据访问前设置身份认证等措施，防止数据的非授权访问；
   3. 数据访问权限与访问者的身份关联情况；
   4. 数据访问权限申请、审批机制的建设落实情况；
   5. 是否以满足业务实际需要的最小化权限原则进行授权。

身份鉴别