企业内部控制应用指引第18号——信息系统

第一章 总则

第一条 为了促进企业有效实施内部控制，提高企业现代化管理水平，减少人为因素，根据有关法律法规和《企业内部控制基本规范》，制定本指引。

第二条 本指引所称信息系统，是指企业利用计算机和通信技术，对内部控制进行集成、转化和提升所形成的信息化管理平台。

第三条 企业利用信息系统实施内部控制至少应当关注下列风险:

（一）信息系统缺乏或规划不合理，可能造成信息孤岛或重复建设，导致企业经营管理效率低下。

（二）系统开发不符合内部控制要求，授权管理不当，可能导致无法利用信息技术实施有效控制。

（三）系统运行维护和安全措施不到位，可能导致信息泄漏或损，系统无法正常运行。

第四条 企业应当重视信息系统在内部控制中的作用，根据内部控制要求，结合组织架构、业务范围、地域分布、技术能力等因素，制定信息系统建设整体规划，加大投入力度，有序组织信息系统开发、运行与维护，优化管理流程，防范经营风险，全面提升企业现代化管理水平。

企业应当指定专门机构对信息系统建设实施归口管理，明确相关位的职责权限，建立有效工作机制。企业可委托专业机构从事信息系统的开发、运行和维护工作。

企业负责人对信息系统建设工作负责。

第二章 信息系统的开发

第五条 企业应当根据信息系统建设整体规划提出项目建设方案，明确建设目标、人员配备、职责分工、经费保障和进度安排等相关内容，按照规定的权限和程序审批后实施。

企业信息系统归口管理部门应当组织内部各单位提出开发需求和关键控制点，规范开发流程，明确系统设计、编程、安装调试、验收、上线等全过程的管理要求，严格按照建设方案、开发流程和相关要求组织开发工作。

企业开发信息系统，可以采取自行开发、外购调试、业务外包等方式。选定外购调试或业务外包方式的，应当采用公开招标等形式择优确定供应商或开发单位。

第六条 企业开发信息系统，应当将生产经营管理业务流程、关键控制点和处理规则嵌入系统程序，实现手工环境下难以实现的控制功能。

企业在系统开发过程中，应当按照不同业务的控制要求，通过信息系统中的权限管理功能控制用户的操作权限，避免将不相容职责的处理权限授予同一用户。

企业应当针对不同数据的输入方式，考虑对进入系统数据的

检查和校验功能。对于必需的后台操作，应当加强管理，建立规范的流程制度，对操作情况进行监控或者审计。

企业应当在信息系统中设置操作日志功能，确保操作的可审计性。对异常的或者违背内部控制要求的交易和数据，应当设计由系统自动报告并设置跟踪处理机制。

第七条 企业信息系统归口管理部门应当加强信息系统开发全过程的跟踪管理，组织开发单位与内部各单位的日常沟通和协调，督促开发单位按照建设方案、计划进度和质量要求完成编程工作，对配备的硬件设备和系统软件进行检查验收，组织系统上线运行等

第八条 企业应当组织独立于开发单位的专业机构对开发完成的信息系统进行验收测试，确保在功能、性能、控制要求和安全性等方面符合开发需求。

第九条 企业应当切实做好信息系统上线的各项准备工作，培训业务操作和系统管理人员，制定科学的上线计划和新旧系统转换方案，考虑应急预案，确保新旧系统顺利切换和平稳衔接。系统上线涉及数据迁移的，还应制定详细的数据迁移计划。

第三章 信息系统的运行与维护

第十条 企业应当加强信息系统运行与维护的管理，制定信息系统工作程序、信息管理制度以及各模块子系统的具体操作规范，及时跟踪、发现和解决系统运行中存在的问题，确保信息系统按照规定的程序、制度和操作规范持续稳定运行。

企业应当建立信息系统变更管理流程，信息系统变更应当严格遵照管理流程进行操作。信息系统操作人员不得擅自进行系统软件的删除、修改等操作；不得擅自升级、改变系统软件版本；不得擅自改变软件系统环境配置。

第十一条 企业应当根据业务性质、重要性程度、涉密情况等确定信息系统的安全等级，建立不同等级信息的授权使用制度，采用相应技术手段保证信息系统运行安全有序。

企业应当建立信息系统安全保密和泄密责任追究制度。委托专业机构进行系统运行与维护管理的，应当审查该机构的资质，并与其签订服务合同和保密协议。

企业应当采取安装安全软件等措施防范信息系统受到病毒等恶意软件的感染和破坏。

第十二条 企业应当建立用户管理制度，加强对重要业务系统的访问权限管理，定期审阅系统账号，避免授权不当或存在非授权账号，禁止不相容职务用户账号的交叉操作。

第十三条 企业应当综合利用防火墙、路由器等网络设备，漏洞扫描、入侵检测等软件技术以及远程访问安全策略等手段，加强网络安全，防范来自网络的攻击和非法侵入。

企业对于通过网络传输的涉密或关键数据，应当采取加密措施，确保信息传递的保密性、准确性和完整性。

第十四条 企业应当建立系统数据定期备份制度，明确备份范围、频度、方法、责任人、存放地点、有效性检查等内容。

第十五条 企业应当加强服务器等关键信息设备的管理，建立良好的物理环境，指定专人负责检查，及时处理异常情况。未经授权，任何人不得接触关键信息设备。