优化信息系统 提升管理水平

——财政部会计司解读《企业内部控制应用指引第 18 号——信息系统》

一、信息系统内部控制概述

《企业内部控制应用指引第 18 号———信息系统》中所指信息系统，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。信息系统内部控制的目标是促进企业有效实施内部控制，提高企业现代化管理水平，减少人为操纵因素；同时，增强信息系统的安全性、可靠性和合理性以及相关信息的保密性、完整性和可用性，为建立有效的信息与沟通机制提供支持保障。信息系统内部控制的主要对象是信息系统，由计算机硬件、软件、人员、信息流和运行规程等要素组成。

现代企业的运营越来越依赖于信息系统。比如航空公司的网上订票系统、银行的资金实时结算系统、携程旅行网的客户服务系统等，没有信息系统的支撑，业务开展就举步维艰、难以为继，企业经营就很可能陷入瘫痪状态。还有一些新兴产业和新兴企业，其商业模式完全依赖信息系统，比如各种网络公司（新浪、网易、百度）、各种电子商务公司（比如阿里巴巴、卓越公司），没有信息系统，这些企业可能失去生存之基。

同时应当看到，企业信息系统内部控制以及利用信息系统实施内部控制也面临诸多风险，至少应当关注下列方面：一是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；二是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；三是系统运行维护和安全措施不到位，可能导致信息泄漏或毁损，系统无法正常运行。

鉴于信息系统在实施内部控制和现代化管理中具有十分独特而重要的作用，加之信息系统本身的复杂性和高风险特征，《企业内部控制应当指引第 18 号——

信息系统》规定，企业负责人对信息系统建设工作负责。换言之，信息系统建设是“一把手”工程。只有企业负责人站在战略和全局的高度亲自组织领导信息系统建设工作，才能统一思想、提高认识、加强协调配合，从而推动信息系统建设在整合资源的前提下高效、协调推进。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，制定信息系统建设总体规划，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。

二、信息系统的开发

企业根据发展战略和业务需要进行信息系统建设，首先要确立系统建设目标，根据目标进行系统建设战略规划，再将规划细化为项目建设方案。企业开展信息系统建设，可以根据实际情况，采取自行开发、外购调试或业务外包等方式。选择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选择供应商或开发单位。选择自行开发信息系统的，信息系统归口管理部门应当组织企业内部相关业务部门进行需求分析，合理配置人员，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。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，增进开发单位与企业内部业务部门的日常沟通和协调，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检查验收，并组织系统上线运行。

（一）制定信息系统开发的战略规划

信息系统开发的战略规划是信息化建设的起点，战略规划是以企业发展战略为依据制定的企业信息化建设的全局性、长期性规划。制定信息系统战略规划的主要风险是：第一，缺乏战略规划或规划不合理，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。第二，没有将信息化与企业业务需求结合，降低了信息系统的应用价值。信息孤岛现象是不少企业信息系统建设中存在的普遍问题，根源在于这些企业往往忽视战略规划的重要性，缺乏整体观念和整合意识，常常

陷于头痛医头，脚痛医脚，这就导致有的企业财务管理信息系统、销售管理信息系统、生产管理信息系统、人力资源管理系统、办公自动化系统等各自为政、孤立存在的现象，削弱了信息系统的协同效用，甚至引发系统冲突。

主要控制措施：第一，企业必须制定信息系统开发的战略规划和中长期发展计划，并在每年制定经营计划的同时制定年度信息系统建设计划，促进经营管理活动与信息系统的协调统一。第二，企业在制定信息化战略过程中，要充分调动和发挥信息系统归口管理部门与业务部门的积极性，使各部门广泛参与，充分沟通，提高战略规划的科学性、前瞻性和适应性。第三，信息系统战略规划要与企业的组织架构、业务范围、地域分布、技术能力等相匹配，避免相互脱节。

（二）选择适当的信息系统开发方式

信息系统的开发建设是信息系统生命周期中技术难度最大的环节。在开发建设环节，要将企业的业务流程、内控措施、权限配置、预警指标、核算方法等固化到信息系统中，因此开发建设的好坏直接影响信息系统的成败。

开发建设主要有自行开发、外购调试、业务外包等方式。各种开发方式有各自的优缺点和适用条件，企业应根据自身实际情况合理选择。

1．自行开发

自行开发是企业依托自身力量完成整个开发过程。其优点是开发人员熟悉企业情况，可以较好地满足本企业的需求，尤其是具有特殊性的业务需求。通过自行开发，还可以培养锻炼自己的开发队伍，便于后期的运行和维护。其缺点是开发周期较长、技术水平和规范程度较难保证，成功率相对较低。因此，自行开发方式的适用条件通常是企业自身技术力量雄厚，而且市场上没有能够满足企业需求的成熟的商品化软件和解决方案。比如百度的搜索引擎系统就偏重于自行开发。

2．外购调试

外购调式的基本做法是企业购买成熟的商品化软件，通过参数配置和二次开发满足企业需求。其优点是开发建设周期短；成功率较高；成熟的商品化软件质

量稳定，可靠性高；专业的软件提供商实施经验丰富。其缺点是难以满足企业的特殊需求；系统的后期升级进度受制于商品化软件供应商产品更新换代的速度，企业自主权不强，较为被动。外购调试方式的适用条件通常是企业的特殊需求较少，市场上已有成熟的商品化软件和系统实施方案。比如大部分企业的财务管理系统、ERP 系统、人力资源管理系统等多采用外购调试方式。

3．业务外包

信息系统的业务外包是指委托其他单位开发信息系统，基本做法是企业将信息系统开发项目外包出去，由专业公司或科研机构负责开发、安装实施，由企业直接使用。其优点是企业可以充分利用专业公司的专业优势，量体裁衣，构建全面、高效满足企业需求的个性化系统；企业不必培养、维持庞大的开发队伍，相应节约了人力资源成本。其缺点是沟通成本高，系统开发方难以深刻理解企业需求，可能导致开发出的信息系统与企业的期望产生较大偏差；同时，由于外包信息系统与系统开发方的专业技能、职业道德和敬业精神存在密切关系，也要求企业必须加大对外包项目的监督力度。业务外包方式的适用条件通常是市场上没有能够满足企业需求的成熟的商品化软件和解决方案，企业自身技术力量薄弱或出于成本效益原则考虑不愿意维持庞大的开发队伍。

（三）自行开发方式的关键控制点和主要控制措施

虽然信息系统的开发方式有自行开发、外购调试、业务外包等多种方式，但基本流程大体相似，通常包含项目计划、需求分析、系统设计、编程和测试、上线等环节。

1．项目计划环节

战略规划通常将完整的信息系统分成若干子系统，并分阶段建设不同的子系统。比如，制造企业可以将信息系统划分为财务管理系统、人力资源管理系统、MRP 系统（销售、采购、库存、生产）、计算机辅助设计和制造系统、客户关

系系统、电子商务系统等若干子系统。项目就是指本阶段需要建设的相对独立的一个或多个子系统。

项目计划通常包括项目范围说明、项目进度计划、项目质量计划、项目资源计划、项目沟通计划、风险对策计划、项目采购计划、需求变更控制、配置管理计划等内容。项目计划不是完全静止、一成不变的，在项目启动阶段，可以先制定一个较为原则的项目计划，确定项目主要内容和重大事项，然后根据项目的大小和性质以及项目进展情况进行调整、充实和完善。项目计划环节的主要风险是：信息系统建设缺乏项目计划或者计划不当，导致项目进度滞后、费用超支、质量低下。

主要控制措施：第一，企业应当根据信息系统建设整体规划提出分阶段项目的建设方案，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。第二，企业可以采用标准的项目管理软件（比如 Office Project）制定项目计划，并加以跟踪。在关键环节进行阶段性评审，以保证过程可控。第三，项目关键环节编制的文档应参照《GB8567－88 计算机软件产品开发文件编制指南》等相关国家标准和行业标准进行，以提高项目计划编制水平。

2．需求分析环节

需求分析的目的是明确信息系统需要实现哪些功能。该项工作是系统分析人员和用户单位的管理人员、业务人员在深入调查的基础上，详细描述业务活动涉及的各项工作以及用户的各种需求，从而建立未来目标系统的逻辑模型。这一环节的主要风险是：第一，需求本身不合理，对信息系统提出的功能、性能、安全性等方面的要求不符合业务处理和控制的需要。第二，技术上不可行、经济上成本效益倒挂，或与国家有关法规制度存在冲突。第三，需求文档表述不准确、不完整，未能真实全面地表达企业需求，存在表述缺失、表述不一致甚至表述错误等问题。

主要控制措施：第一，信息系统归口管理部门应当组织企业内部各有关部门提出开发需求，加强系统分析人员和有关部门的管理人员、业务人员的交流，经综合分析提炼后形成合理的需求。第二，编制表述清晰、表达准确的需求文档。需求文档是业务人员和技术人员共同理解信息系统的桥梁，必须准确表述系统建设的目标、功能和要求。企业应当采用标准建模语言(例如 UML)，综合运用多种建模工具和表现手段，参照《GB8567－88 计算机软件产品开发文件编制指南》等相关标准，提高系统需求说明书的编写质量。第三，企业应当建立健全需求评审和需求变更控制流程。依据需求文档进行设计（含需求变更设计）前，应当评审其可行性，由需求提出人和编制人签字确认，并经业务部门与信息系统归口管理部门负责人审批。

3．系统设计环节

系统设计是根据系统需求分析阶段所确定的目标系统逻辑模型，设计出一个能在企业特定的计算机和网络环境中实现的方案，即建立信息系统的物理模型。系统设计包括总体设计和详细设计。总体设计的主要任务是：第一，设计系统的模块结构，合理划分子系统边界和接口。第二，选择系统实现的技术路线，确定系统的技术架构，明确系统重要组件的内容和行为特征，以及组件之间、组件与环境之间的接口关系。第三，数据库设计，包括主要的数据库表结构设计、存储设计、数据权限和加密设计等。第四，设计系统的网络拓扑结构、系统部署方式等。详细设计的主要任务包括：程序说明书编制、数据编码规范设计、输入输出界面设计等内容。系统设计环节的主要风险是：第一，设计方案不能完全满足用户需求，不能实现需求文档规定的目标。第二，设计方案未能有效控制建设开发成本，不能保证建设质量和进度。第三，设计方案不全面，导致后续变更频繁。第四，设计方案没有考虑信息系统建成后对企业内部控制的影响，导致系统运行后衍生新的风险。

主要控制措施：第一，系统设计负责部门应当就总体设计方案与业务部门进行沟通和讨论，说明方案对用户需求的覆盖情况；存在备选方案的，应当详细说明各方案在成本、建设时间和用户需求响应上的差异；信息系统归口管理部门和业务部门应当对选定的设计方案予以书面确认。第二，企业应参照《GB8567－88 计算机软件产品开发文件编制指南》等相关国家标准和行业标准，提高系统设计说明书的编写质量。第三，企业应建立设计评审制度和设计变更控制流程。第四，在系统设计时应当充分考虑信息系统建成后的控制环境，将生产经营管理业务流程、关键控制点和处理规程嵌入系统程序，实现手工环境下难以实现的控制功能，例如：对于某一财务软件，当输入支出凭证时，可以让计算机自动检查银行存款余额，防止透支。第五，应充分考虑信息系统环境下的新的控制风险，比如，要通过信息系统中的权限管理功能控制用户的操作权限，避免将不相容职务的处理权限授予同一用户。第六，应当针对不同的数据输入方式，强化对进入系统数据的检查和校验功能。比如，凭证的自动平衡校对。第七，系统设计时应当考虑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。第八，预留必要的后台操作通道，对于必需的后台操作，应当加强管理，建立规范的操作流程，确保足够的日志记录，保证对后台操作的可监控性。

4．编程和测试环节

编程阶段是将详细设计方案转换成某种计算机编程语言的过程。编程阶段完成之后，要进行测试，测试主要有以下目的：一是发现软件开发过程中的错误，分析错误的性质，确定错误的位置并予以纠正。二是通过某些系统测试，了解系统的响应时间、事务处理吞吐量、载荷能力、失效恢复能力以及系统实用性等指标，以便对整个系统做出综合评价。测试环节在系统开发中具有举足轻重的地位。

这一环节的主要风险是：第一，编程结果与设计不符。第二，各程序员编程风格差异大，程序可读性差，导致后期维护困难，维护成本高。第三，缺乏有效

的程序版本控制，导致重复修改或修改不一致等问题。第四，测试不充分。单个模块正常运行但多个模块集成运行时出错，开发环境下测试正常而生产环境下运行出错，开发人员自测正常而业务部门用户使用时出错，导致系统上线后可能出现严重问题。

主要控制措施：第一，项目组应建立并执行严格的代码复查评审制度。第二，项目组应建立并执行统一的编程规范，在标识符命名、程序注释等方面统一风格。第三，应使用版本控制软件系统（例如 CVS），保证所有开发人员基于相同的组件环境开展项目工作，协调开发人员对程序的修改。第四，应区分单元测试、组装测试（集成测试）、系统测试、验收测试等不同测试类型，建立严格的测试工作流程，提高最终用户在测试工作中的参与程度，改进测试用例的编写质量，加强测试分析，尽量采用自动测试工具提高测试工作的质量和效率。具备条件的企业，应当组织独立于开发建设项目组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。

5．上线环节

系统上线是将开发出的系统（可执行的程序和关联的数据）部署到实际运行的计算机环境中，使信息系统按照既定的用户需求来运转，切实发挥信息系统的作用。这一环节的主要风险是：第一，缺乏完整可行的上线计划，导致系统上线混乱无序。第二，人员培训不足，不能正确使用系统，导致业务处理错误，或者未能充分利用系统功能，导致开发成本浪费。第三，初始数据准备设置不合格，导致新旧系统数据不一致、业务处理错误。

主要控制措施：第一，企业应当制定信息系统上线计划，并经归口管理部门和用户部门审核批准。上线计划一般包括人员培训、数据准备、进度安排、应急预案等内容。第二，系统上线涉及新旧系统切换的，企业应当在上线计划中明确应急预案，保证新系统失效时能够顺利切换回旧系统。第三，系统上线涉及数据

迁移的，企业应当制定详细的数据迁移计划，并对迁移结果进行测试。用户部门应当参与数据迁移过程，对迁移前后的数据予以书面确认。

（四）其他开发方式的关键控制点和主要控制措施

下面介绍其他开发方式（业务外包、外购调试）的关键控制点和主要控制措施。

在业务外包、外购调试方式下，企业对系统设计、编程、测试环节的参与程度明显低于自行开发方式，因此可以适当简化相应的风险控制措施，但同时也因开发方式的差异产生一些新的风险，需要采取有针对性的控制措施。

1．业务外包方式的关键控制点和主要控制措施

（1）选择外包服务商

这一环节的主要风险是：由于企业与外包服务商之间本质上是一种委托—代理关系,合作双方的信息不对称容易诱发道德风险，外包服务商可能会实施损害企业利益的自利行为,如偷工减料、放松管理、信息泄密等。

主要控制措施：第一，企业在选择外包服务商时要充分考虑服务商的市场信誉、资质条件、财务状况、服务能力、对本企业业务的熟悉程度、既往承包服务成功案例等因素,对外包服务商进行严格筛选。第二，企业可以借助外包业界基准来判断外包服务商的综合实力。第三，企业要严格外包服务审批及管控流程,对信息系统外包业务，原则上应采用公开招标等形式选择外包服务商，并实行集体决策审批。

（2）签订外包合同

这一环节的主要风险是：由于合同条款不准确、不完善，可能导致企业的正当权益无法得到有效保障。

主要控制措施：第一，企业在与外包服务商签约之前,应针对外包可能出现的各种风险损失,恰当拟定合同条款,对涉及的工作目标、合作范畴、责任划分、所有权归属、付款方式、违约赔偿及合约期限等问题做出详细说明,并由法律部

门或法律顾问审查把关。第二，开发过程中涉及商业秘密、敏感数据的，企业应当与外包服务商签订详细的“保密协定”，以保证数据安全。第三，在合同中约定付款事宜时,应当选择分期付款方式，尾款应当在系统运行一段时间并经评估验收后再支付。第四，应在合同条款中明确要求外包服务商保持专业技术服务团队的稳定性。

（3）持续跟踪评价外包服务商的服务过程

这一环节的主要风险是：企业缺乏外包服务跟踪评价机制或跟踪评价不到位，可能导致外包服务质量水平不能满足企业信息系统开发需求。

主要控制措施：第一，企业应当规范外包服务评价工作流程，明确相关部门的职责权限，建立外包服务质量考核评价指标体系，定期对外包服务商进行考评,并公布服务周期的评估结果,实现外包服务水平的跟踪评价。第二，必要时，可以引入监理机制，降低外包服务风险。

2．外购调试方式的关键控制点和主要控制措施

在外购调试方式下，一方面，企业面临与委托开发方式类似的问题，企业要选择软件产品的供应商和服务供应商、签订合约、跟踪服务质量，因此，企业可采用与委托开发方式类似的控制措施；另一方面，外购调试方式也有其特殊之处，企业需要有针对性的强化某些控制措施。

（1）软件产品选型和供应商选择

在外购调试方式下，软件供应商的选择和软件产品的选型是密切相关的。这一环节的主要风险是：第一，软件产品选型不当，产品在功能、性能、易用性等方面无法满足企业需求。第二，软件供应商选择不当，产品的支持服务能力不足，产品的后续升级缺乏保障。

主要控制措施：第一，企业应明确自身需求，对比分析市场上的成熟软件产品，合理选择软件产品的模块组合和版本。第二，企业在软件产品选型时应广泛

听取行业专家的意见。第三，企业在选择软件产品和服务供应商时，不仅要评价其现有产品的功能、性能，还要考察其服务支持能力和后续产品的升级能力。

（2）服务提供商选择

大型企业管理信息系统（例如 ERP 系统）的外购实施，不仅需要选择合适的软件供应商和软件产品，也需要选择合适的咨询公司等服务提供商，指导企业将通用软件产品与本企业的实际情况有机结合。这一环节的主要风险是：服务提供商选择不当，削弱了外购软件产品的功能发挥，导致无法有效满足用户需求。

主要控制措施：在选择服务提供商时，不仅要考核其对软件产品的熟悉、理解程度，也要考核其是否深刻理解企业所处行业的特点、是否理解企业的个性化需求、是否有过相同或相近的成功案例。

三、信息系统的运行与维护

信息系统的运行与维护主要包含三方面的内容：日常运行维护、系统变更和安全管理。

（一）日常运行维护的关键控制点和主要控制措施

日常运行维护的目标是保证系统正常运转，主要工作内容包括系统的日常操作、系统的日常巡检和维修、系统运行状态监控、异常事件的报告和处理等。这一环节的主要风险是：第一，没有建立规范的信息系统日常运行管理规范，计算机软硬件的内在隐患易于爆发，可能导致企业信息系统出错。第二，没有执行例行检查，导致一些人为恶意攻击会长期隐藏在系统中，可能造成严重损失。第三，企业信息系统数据未能定期备份，可能导致损坏后无法恢复，从而造成重大损失。

主要控制措施：第一，企业应制定信息系统使用操作程序、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。第二，切实做好系统运行记录，尤其是对于系统运行不正常或无法运行的情况，应将异常现象、发生时间和可能的原因作出详细记录。第三，企业要重视系统运行的日常维护，

在硬件方面，日常维护主要包括各种设备的保养与安全管理、故障的诊断与排除、易耗品的更换与安装等，这些工作应由专人负责。第四，配备专业人员负责处理信息系统运行中的突发事件，必要时应会同系统开发人员或软硬件供应商共同解决。

（二）系统变更的关键控制点和主要控制措施

系统变更主要包括硬件的升级扩容、软件的修改与升级等。系统变更是为了更好地满足企业需求，但同时应加强对变更申请、变更成本与进度的控制。这一环节的主要风险是：第一，企业没有建立严格的变更申请、审批、执行、测试流程，导致系统随意变更。第二，系统变更后的效果达不到预期目标。

主要控制措施：第一，企业应当建立标准流程来实施和记录系统变更，保证变更过程得到适当的授权与管理层的批准，并对变更进行测试。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软件的删除、修改等操作；不得擅自升级、改变软件版本；不得擅自改变软件系统的环境配置。第二，系统变更程序(如软件升级)需要遵循与新系统开发项目同样的验证和测试程序，必要时还应当进行额外测试。第三，企业应加强紧急变更的控制管理。第四，企业应加强对将变更移植到生产环境中的控制管理，包括系统访问授权控制、数据转换控制、用户培训等。

（三）安全管理的关键控制点和主要控制措施

安全管理的目标是保障信息系统安全，信息系统安全是指信息系统包含的所有硬件、软件和数据受到保护，不因偶然和恶意的原因而遭到破坏、更改和泄漏，信息系统能够连续正常运行。这一环节的主要风险是：第一，硬件设备分布物理范围广，设备种类繁多，安全管理难度大，可能导致设备生命周期短。第二，业务部门信息安全意识薄弱，对系统和信息安全缺乏有效的监管手段。少数员工可能恶意或非恶意滥用系统资源，造成系统运行效率降低。第三，对系统程序的缺陷或漏洞安全防护不够，导致遭受黑客攻击，造成信息泄露。第四，对各种计算

机病毒防范清理不力，导致系统运行不稳定甚至瘫痪。第五，缺乏对信息系统操作人员的严密监控，可能导致舞弊和利用计算机犯罪。

主要控制措施是：

第一，建立信息系统相关资产的管理制度，保证电子设备的安全。硬件和网络设备不仅是信息系统运行的基础载体，也是价值昂贵的固定资产。企业应在健全设备管理制度的基础上，建立专门的电子设备管控制度，对于关键信息设备（例如银行的核心数据库服务器），未经授权，不得接触。

第二，企业应成立专门的信息系统安全管理机构，由企业主要领导负总责，对企业的信息安全作出总体规划和全方位严格管理，具体实施工作可由企业的信息主管部门负责。企业应强化全体员工的安全保密意识，特别要对重要岗位员工进行信息系统安全保密培训，并签署安全保密协议。企业应当建立信息系统安全保密制度和泄密责任追究制度。

第三，企业应当按照国家相关法律法规以及信息安全技术标准，制定信息系统安全实施细则。根据业务性质、重要程度、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。对于信息系统的使用者和不同安全等级信息之间的授权关系，应在系统开发建设阶段就形成方案并加以设计，在软件系统中预留这种对应关系的设置功能，以便根据使用者岗位职务的变迁进行调整。

第四，企业应当有效利用 IT 技术手段，对硬件配置调整、软件参数修改严加控制。例如，企业可利用操作系统、数据库系统、应用系统提供的安全机制，设置安全参数，保证系统访问安全；对于重要的计算机设备，企业应当利用技术手段防止员工擅自安装、卸载软件或者改变软件系统配置，并定期对上述情况进行检查。

第五，企业委托专业机构进行系统运行与维护管理的，应当严格审查其资质条件、市场声誉和信用状况等，并与其签订正式的服务合同和保密协议。

第六，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。企业应当特别注重加强对服务器等关键部位的防护；对于存在网络应用的企业，应当综合利用防火墙、路由器等网络设备，采用内容过滤、漏洞扫描、入侵检测等软件技术加强网络安全，严密防范来自互联网的黑客攻击和非法侵入。对于通过互联网传输的涉密或者关键业务数据，企业应当采取必要的技术手段确保信息传递的保密性、准确性、完整性。

第七，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。系统首次上线运行时应当完全备份，然后根据业务频率和数据重要性程度，定期做好增量备份。数据正本与备份应分别存放于不同地点，防止因火灾、水灾、地震等事故产生不利影响。企业可综合采用磁盘、磁带、光盘等备份存储介质。

第八，企业应当建立信息系统开发、运行与维护等环节的岗位责任制度和不相容职务分离制度，防范利用计算机舞弊和犯罪。一般而言，信息系统不相容职务涉及的人员可以分为三类：系统开发建设人员、系统管理和维护人员、系统操作使用人员。开发人员在运行阶段不能操作使用信息系统，否则就可能掌握其中的涉密数据，进行非法利用；系统管理和维护人员担任密码保管、授权、系统变更等关键任务，如果允许其使用信息系统，就可能较为容易地篡改数据，从而达到侵吞财产或滥用计算机信息的目的。此外，信息系统使用人员也需要区分不同岗位，包括业务数据录入、数据检查、业务批准等，在他们之间也应有必要的相互牵制。企业应建立用户管理制度，加强对重要业务系统的访问权限管理，避免将不相容职责授予同一用户。企业应当采用密码控制等技术手段进行用户身份识别。对于重要的业务系统，应当采用数字证书、生物识别等可靠性强的技术手段识别用户身份。对于发生岗位变化或离岗的用户，用户部门应当及时通知系统管理人员调整其在系统中的访问权限或者关闭账号。企业应当定期对系统中的账号

进行审阅，避免存在授权不当或非授权账号。对于超级用户，企业应当严格规定其使用条件和操作程序，并对其在系统中的操作全程进行监控或审计。

第九，企业应积极开展信息系统风险评估工作，定期对信息系统进行安全评估，及时发现系统安全问题并加以整改。

（四）系统终结的关键控制点和主要控制措施

系统终结是信息系统生命周期的最后一个阶段，在该阶段信息系统将停止运行。停止运行的原因通常有：企业破产或被兼并、原有信息系统被新的信息系统代替。这一环节的主要风险是，第一，因经营条件发生剧变，数据可能泄密。第二，信息档案的保管期限不够长。

主要控制措施：第一，要做好善后工作，不管因何种情况导致系统停止运行，都应将废弃系统中有价值或者涉密的信息进行销毁、转移。第二，严格按照国家有关法规制度和对电子档案的管理规定（比如审计准则对审计证据保管年限的要求），妥善保管相关信息档案。