考核指标，每个销售人员必须对每一项销售业务从签订合同到回收资金全过程负责，使销售人员明确风险意识，加强货款的回收。

3、强化应收账款的会计核算

企业应加强应收账款的会计核算，对于已经发生的赊销业务要及时登记，并按照客户设置相应的明细记录账，制定专人管理，并根据客户的业务情况，定期向债务人函证应收款项，进行应收账款的核对，对应收账款的可收回性进行评价。但公司无论怎样严格使用信用政策和信用条件，只要存在赊销行为，坏账损失的风险总是不可避免的。在市场经济条件下无风险和有风险机会并存，但控制的立足点应放在有风险上。

(作者单位：南开大学国际商学院)

责任编辑 季建辉

浅议网络环境下会计信息系统灾难风险控制

□ 孙良文 赛音娜

网络环境下会计信息系统实现了会计资源的共享和会计信息的实时处理，实现了财务与业务的高度集成，使企业越来越依赖于系统来支持日常的生产经营活动，以至于一旦会计信息系统处理过程中断或发生灾难性事故，企业将蒙受重大的损失。灾难风险控制的实质就是要保证在灾难性的事件发生时，会计信息系统能够正常工作或将灾难所造成的损失降到最低。

一、预防会计信息系统灾难发生的控制措施

建立健全企业会计信息系统良好的内部控制体系，能够在很大程度上避免企业的灾难损失，特别是预防许多由于蓄意破坏或者误操作所引起的灾难。

1、系统环境安全控制。环境安全控制尽量减少因外界因素所引起的计算机及网络故障的发生率，保障机器正常运行。具体控制措施主要有机房的选址、设施和工作环境要符合系统安全标准的要求；制定防火、防水和防盗等安全措施；配备稳压、不间断电源等系统保护设备；磁性介质档案的保管要有防高温、防磁措施；系统要安装相应的防病毒软件及防火墙等。

2、系统接触控制。系统接触控制就是要保证只有经过授权的人才能接触到系统软硬件设备及数据文档资料。主要措施包括：合理分配网络系统用户权限及密码和软件用户权限；设置外部(主要指关联方、供应链上的用户)访问区域；确保后台数据库不被直接访问；实行上机操作人员登记制度，并建立机内操作日志。同时，还应采用物理设备鉴别、兼容性测试等入侵检测技术和身份识别技术来防止非授权人员对系统的接触。

3、系统后备控制。对会计信息系统的软硬件系统、应用程序和数据文件均应有后备。按后备运行系统的准备程度，可将其分为冷备份、温备份和热备份三大类。冷备份指后备运行系统未安装或未配置成与作业系统相同或相似的运行环境，应用系统数据没有及时装入备份系统。一旦发生灾难，需安装配置所需的运行环境，恢复备份的应用数据，恢复系统运行。温备份指后备运行系统已安装配置成与作业系统相同或相似的系统和网络运行环境，安装了应用系统业务定期备份数据。一旦发生灾难，直接使用定期备份数据，恢复系统运行。热备份指后备运行系统处于联机状态，作业系统通过高速通信线路将数据实时传送到备份系统，保持备份系统与作业系统数据的同步，一旦发生灾难，不用追补或只需追补很少的孤立数据，备份系统可快速接替作业系统，恢复运行。

4、个人计算机和前端客户机控制。当前大多数的内部控制措施重视会计信息系统的服务器及网络设施的控制，往往忽视了对个人计算机(尤其是经常进入系统的移动计算机)和前端客户机进行控制。这些措施主要有：控制个人计算机对系统数据的存取，减少个人从公司窃取信息的可能，禁止拷贝公司的软件到自己的计算机，禁止未经系统授权对系统资源的使用等。

5、互联网和电子商务控制。互联网和电子商务应用的开放性，使非法入侵、非法截取数据等安全问题难以防范。针对这一控制的主要措施有传统的口令控制、加密技术和验证过程控制。另外还要采用防火墙技术，细分数据包并加密传输的隧道技术，运用公共或私人密钥的电子信封技术、数字签名技术等防止企业内部或外部非授权用户访问，保证互联网上数据的安全传递。

二、会计信息系统灾难恢复计划

企业应建立灾难恢复计划，在灾难事件发生后，保证会计数据处理系统能够尽快恢复正常运行。一个好的灾难恢复计划应该包含下列内容：

1、紧急响应小组。一个灾难恢复计划需要成立一个紧急响应小组，并指定一名负责人，对计划的所有阶段负责，在国外由首席信息官(CIO)或首席安全官(CSO)担任。该负

责人在紧急情况下，按恢复计划分配任务给小组成员，这些任务包含紧急情况下安装新的设备、操作计算机、安装软件、建立数据通讯设备、恢复关键记录等。

2、后备软、硬件系统与数据文件恢复。后备系统有冷备份、温备份和热备份。冷备份完成恢复可能需要数天的时间，温备份可能需要几个小时的时间，而热备份可以在几分钟内完成恢复工作。实际上，要采用哪种后备方式，基于公司的成本效益分析。对于冷备份后备系统，可以直接购买备用系统；对于温备份和热备份这些高成本的后备系统，一般情况下，公司可以通过专门提供灾难恢复服务的供应商得到解决，如Comdisco、IBM和Sungard等。

3、定期测试和修订。模拟一个灾难，在模拟过程中每一个灾难恢复成员都应完成计划规定的恢复任务。灾难恢复计划必须被完整地通过测试，否则恢复计划是不完善的。灾难恢复计划一年中至少应该被测试两次。许多计划由于没有初始的测试，当灾难发生时，很难达到预期的目标。另外，恢复计划必须不断地被更新和校订，以保证它适应当前的计算机及网络应用需求、设备配置和人员分配的变化。

4、建立健全灾难恢复管理制度。公司根据自己的需要，还应该制定一系列的灾难恢复管理制度，这些灾难管理制度主要有：灾难报告制度、灾难恢复审批制度、灾难通知程序、灾难恢复处理流程、数据的恢复方式、业务部门的认可程序、备份系统日常运行管理制度、备份系统替代运行状态下的运行制度、数据一致性认可程序、信息系统复原后的回切处理流程等。

(作者单位：内蒙古财经学院会计系
内蒙古财税职业学院)

责任编辑 王教育

企业粉饰信用的识别

□ 陈江光

粉饰信用是指企业采取各种手段，对反映企业信用的各种指标、信息资料进行掩饰、美化的行为。这种粉饰会计信息的行为其形式是多种多样的。从内容来看，主要表现在粉饰企业反映其偿债能力的各种静态指标，粉饰企业的盈利能力，粉饰作为担保的标的物或是担保企业等方面。从手段来看，主要表现在改变会计方法及计算、计价的口径，违反会计制度，变造会计信息，虚构、虚计业务，账、表不相符合，对将来情况进行主观的、带有倾向性的，甚至是欺骗性的估计等方面。虽然其形式和手段多样，但目的都是为了获取银行的信任和好感，"改善"各种财务指标，以获取信贷资金。无论是什么样的情况，对发放贷款的银行来说都是非常危险的。因为这些粉饰行为都是一种主观上的故意，如果不能正确地识别，银行的信贷资产就存在着较一般贷款更大的风险。

一般情况下，企业的信用粉饰行为多表现为"异动"，即各种财务指标突然地、非正常地变化；"异常"，即贷款企业所表现的各种财务指标较之人们对它的预期、参照企业等存在比较大的差别；"不合逻辑"，即贷款企业的各种指标之间由于人为编造、掩饰等原因，破坏了企业各种指标之间、各种会计资料之间应有的勾稽关系。对于"异动"、"异常"、"不合逻辑"的审核，应通过以下方式进行：一是对比贷款企业的历史资料，审核企业的财务指标有无"异动"情况。二是对比相同、相似行业不同企业的相关资料，判断贷款企业是否存在"异常"情况。三是对比设定"理想"贷款企业的财务指标。银行应根据不同地区、不同行业的具体情况，设定财务指标的一般标准，作为对贷款企业财务状况的判断标准。四是对比贷款企业提供给其他有关部门、机构的资料，以确定其真实性。五是检查企业各种指标之间、各种会计资料之间的勾稽关系。六是检查企业近期的大宗交易，查看有无虚假交易以及其他的非正常交易。七是严格界定企业担保物的所有权和抵押资格，在现时市场条件下确定其价值。要注意贷款企业对其价值的计算确定是否有依据。

简单来说，对于一般的信用粉饰采用对比分析的方法，就可以发现存在的问题。但对于贷款数额较大，或是有违约记录，内部管理混乱，信誉较差的企业，就应该在全面检查企业账目的基础上，根据客观事实做出正确的评价。

此外，按现行会计制度计算的各种财务指标也可能对企业信用状况的判断产生误导。现行会计模式提供的财务信息客观上存在的缺陷主要表现在：一是流动比率等财务指标的设置和计算缺乏稳健，有失准确。二是会计核算体系是建立在历史成本基础上的，在对企业进行信用评价时，根据历史成本的会计信息作出的各种决策，必然会存在很多缺陷。三是现行会计制度是以权责发生制为基础的。因此，企业的净收益和实际的偿债能力之间是不能划等号的，只有实际可以用来还债的净收益，才能视为企业未来的偿债能力。金融企业在审核贷款企业的财务状况时，对于这种情况也必须予以关注。

(作者单位：山东省财政厅)

责任编辑 闵 超