第5章　信息系统一般控制审计

本章主要介绍信息系统的一般控制及其审计，着重阐述一般控制的内容和审计程序。一般控制主要包括基础设施控制、系统访问控制、信息系统硬件控制、信息系统软件控制、信息系统安全控制、灾难恢复与业务持续性控制等。通过一般控制审计案例，介绍一般控制审计技术方法、一般控制审计重点内容及审计事项。

5.1　信息系统一般控制

信息系统一般控制作为内部控制的一个方面，是指对整个计算机信息系统及环境要素实施的，对系统所有的应用或功能模块具有普遍影响的控制措施。信息系统一般控制是应用于一个单位信息系统全部或较大范围的内部控制，其基本目标为保证数据安全、保护信息系统应用程序、防止系统被非法侵入、保证在意外中断情况下的继续运行等。有效的一般控制是保证应用控制有效的重要因素，提供应用系统运行和应用控制实施的环境。如果一般控制薄弱，将严重地削弱相关应用控制的可靠性。

审计人员应当采用合适的方法、合理的技术手段针对被审计信息系统的系统环境、访问控制、基础架构、数据保护及灾难恢复等方面的控制进行检查与测试，以评估信息系统一般控制的效力，也可以为数据审计提供审计线索和依据。

审计人员制定信息系统审计计划时，应当将注意力集中在那些直接影响信息系统的一般控制上，确定关键审计领域、重要审计事项及关键控制活动。在确定重要审计事项和关键控制活动时，审计人员既要考虑与审计目标直接有关的应用程序，也要考虑系统的架构，因为它们对于评估信息系统一般控制是否有效实施十分关键，审计人员还要考虑获取审计证据的方式，通过证据判断该审计事项的控制活动是否有效。

信息系统一般控制关注基础设施控制、逻辑的和物理的访问控制、配置管理、职责分离及灾难恢复与业务持续性等关键审计领域。

（1）基础设施控制。基础设施是保障信息系统工作所必需的设施与条件，信息系统的一般控制要针对基础设施，设计必要的控制措施，以保障信息系统安全、可靠运行。基础设施控制重点是信息系统环境及信息系统软、硬件的采购、配置、运行与管理。

（2）系统访问控制。限制或监控对计算机资源（数据、程序、设备和设施）的访问，防范计算机资源被未经授权的修改、丢失及泄露。

（3）系统配置管理。防止未经授权更改信息系统资源配置（如软件程序和硬件配置），有效保证系统配置合理，运行安全。

（4）职责分离。制定相关制度，成立相应的机构，确保信息系统关键岗位的有效隔离和对不相容岗位的分工控制，有效消除职务舞弊风险。

（5）灾难恢复与业务持续性。当出现紧急事件时，保护相关信息系统的关键数据，保证

关键的业务迅速恢复并持续运行。

5.1.1　信息基础设施控制

1. 信息系统环境控制

信息系统环境风险可能来源于自然灾害，常见的自然灾害有闪电、地震、火山爆发、暴雨、台风、龙卷风、洪水；也可能来自电力故障、设备故障、温度、湿度、静电、接地、恐怖袭击等方面。其中对信息系统影响最大的就是计算机和支持系统的电力故障，根据故障的持续时间和严重性，这类故障分为电力完全中断、电压不足、电压不稳及电磁干扰四种情况。

针对信息系统环境风险，采用的控制设施和控制技术包括：

1）安装与使用报警控制面板

信息系统物理环境必须设置报警控制面板，保证负责防火的部门员工随时可以访问；面板必须安装在保护盒中，使用单独的电源或专用电源供电，保障在特殊情况下能正常运行。

2）水灾探测器

水灾探测器是用来预防信息系统的相关设备遭受水患，对于无人看管的信息处理设备来说，安装水灾探测器尤为重要。

3）火灾控制

火灾是信息系统环境风险中产生威胁频率最高的风险之一，大部分的信息系统环境都需要充分考虑防范火灾的需要，设置有火灾控制系统或设备。

信息处理设施的环境中，墙壁、地板及天花板必须为防火材料，必须具备阻隔火灾、避免扩散的功能。所有供电线路应安装在防火线槽内，而防火线槽通常放置于计算机机房的防火地板下。另外，在信息处理设施中的常用办公设施（垃圾桶、窗帘、办公桌、文件柜等），都应当具备防火能力。

对于火灾的防范，最常见的控制设施是手控式火灾警报器及手提式灭火器，对于信息处理设施的环境来说，设置有效的火灾自动灭火系统是相当重要的。完整的自动灭火系统包括烟雾探测装置和自动灭火装置。

烟雾探测装置必须装置在整个设施的天花板上及计算机机房高架地板下，探测器启动警报时必须产生足够的警报声响，且能连接至监控室。在天花板上及高架地板下的探测器的位置必须加上记号，以利识别及维护。在自动灭火系统中，烟雾探测器报警时应启动自动灭火装置。

自动灭火系统在探测到火灾引起的高温时可自行启动，系统必须能产生足够的警报声响，且连接至中央保安监控室。理想情况下，系统必须自动触发其他装置以封闭火场，包括关闭防火门、通知消防单位、关闭通风系统及关闭非必要电力措施，然后释放灭火材料。

自动灭火系统自动释放的灭火材料要根据不同的信息处理环境进行选择，最常见的灭火系统采用水作为灭火材料，但因为会损害设备而在信息系统环境中不常用。二氧化碳作为灭火材料，在无人值守的信息系统环境中也是一种常见选择，由于高浓度的二氧化碳会威胁到人的生命，因此许多国家都规定二氧化碳自动释放是违法的。在保障人员和设备安全的前提下，采用惰性气体作为自动释放灭火材料成为一种选择。

为确保防火探测系统符合建筑标准，负责消防的部门每年应当定期检测消防设施。消

防部门也必须知道计算机机房位置，以备火灾发生时，及时运来适当的设备扑救火灾。

4）电力供应相关风险的控制

针对短暂的电力中断的不同情况，可以采用不同的控制方法。例如，可以通过浪涌保护器加以保护；持续几秒到几十分钟的电力中断可以采取不间断电源（UPS）加以保护；持续几小时到几天的电力中断可以采用后备发电机供电。为了防止意外事件造成的电力中断，还可以采用来自不同电网的备份电力系统，当一套电力系统中断时，备份电力系统工作，不影响正常的电力供应。

在计算机机房发生火灾或要求紧急疏散时，必须立即切断计算机及周边设备的电力。

5）其他相关的控制

在信息处理场所中就餐、喝饮料及吸烟会增加污染、导致火灾、破坏敏感性设备（特别是液体洒在设备上时），所以必须禁止，例如，入口处贴上警示标语等。

紧急疏散计划必须强调人员安全，同时要兼顾信息处理设施的安全。在紧急情况下，如果时间允许，应当建立程序来控制关机。

2. 信息系统硬件控制

信息系统由计算机硬件、软件和操作计算机系统的人员组成。计算机硬件基础设施是信息系统的重要组成部分，是系统运行的重要保障。对于信息系统硬件设施的控制，是保证信息系统安全性的重要措施。对于硬件基础设施的内部控制及其审计，主要考虑硬件设施的获取、运行、维护、监控和能力管理等方面。

1）硬件设施的获取

招标是企业为确保系统硬件采购的成本、设备可用性与可靠性而采取的必要措施。根据信息系统需求选择计算机硬件环境，通常向设备供应商发布一个需求说明，并制定评估设备供应商建议的准则。这类需求以招标书或者需求建议书的形式送达供应商，必须尽可能全面说明所需设备的用途、任务和要求，并描述设备运行环境。

（1）招标书。为确保硬件获取的可用性与可靠性，从审计与控制角度分析，招标书或请求建议书应包括如下内容。

① 组织环境。按信息系统设施需求，组织的业务环境可以是集中式或分布式环境。

② 处理需求。定义组织的业务需求、计算机硬件负载与性能要求、计算机信息处理途径。

③ 硬件需求。说明招标所需要的硬件规格，包括 CPU 处理速度、外部设备、终端设备与数目、网络设备。

④ 系统软件。阐明系统软件环境及其需求，包括计算机操作系统、编译环境、数据库管理软件、通信软件及访问控制软件等。

⑤ 支持需求。说明对所采购硬件的技术支持需求，包括系统的维护、操作人员的培训及备份。

⑥ 适应需求。说明现有系统软硬件环境，对采购硬件的兼容性及对现有设备和装置的影响有明确定义。

⑦ 实施需求。招标书应规定设备的测试、实施与系统运转时间安排。

⑧ 约束条件。招标书在保证信息安全的基础上，可说明硬件采购的容量、现有员工及其操作水平，以及交付日期。

(2) 硬件设施的招标评标。根据招标书需求,硬件供应商提供投标书,企业应安排对投标书从技术和商务层面进行评估分析。在评标过程中,除了根据竞争性报价、成本/效益和系统需求选择供应商,还应考虑供应商的财务状况、维护支持能力,还应了解其他用户对供应商设备的使用情况与评价,通常参考的技术指标有以下几种。

① 好转时间——发生故障时,厂商从登录系统到解决问题所需的时间。

② 响应时间——系统响应一个特定的用户查询所需的时间。

③ 吞吐量——单位时间内系统的有效工作量,吞吐量的衡量指标可以是每秒执行的指令数或其他性能单位。对于数据传输,吞吐量为有效的传输速率,通常用 kb/s、Mb/s 或 Gb/s 表示。

④ 负载——执行必要工作的能力,或系统在给定时间区间内能完成的工作量。

⑤ 兼容性——供应商提供的新系统对现有应用的运行支持能力。

⑥ 容量——新系统处理并发网络应用请求的数目,以及系统能够为每个用户处理的数据量。

⑦ 利用率——新系统可用时间与故障时间之比。

通过评标,确定硬件设备供应商后,需形成正式的书面报告,阐明对投标方案的分析过程与结果,并基于成本效益原则说明评标结果。在评标结果获高层批准后,应与设备供应商签订正式的合同,合同中应包括审计权利条款,以确保组织利益。

(3) 硬件获取过程的控制与审计。硬件获取过程控制与审计时,关注硬件的获取是否基于业务需求,确保硬件获取符合企业的业务目标。通过审核企业的业务和招标书内容可以检查硬件需求是否在招标书中明确定义并反映了业务需求。此外,还应该检查硬件采购是否有适当的评标过程,在充分分析多个供应商的基础上,依据评标准则进行严格的比较,确定采购方案。

2) 硬件设施的维护与监控

信息系统的硬件维护需求随系统复杂性和运行负载的不同而不同。应制定明确的维护计划,最大限度地满足供应商要求的维护规格。硬件维护的执行过程应形成文件,明确要求日常维护的硬件资源信息、维护日程表、维护成本,并记录可提供特殊设备维护的服务商信息。文件还应明确维护记录的保存,对维护执行历史,包括计划内的、计划外的、已执行的和例外的维护都要求有相应的审计轨迹。文件应要求管理层监视、标识和记录所有与供应商维护规格的偏离。在对该硬件维护过程进行审计时,应该确定已形成正式的维护计划并得到管理层的批准;确定已标出超出预算的或额外的开销,这些超额开销意味着没有遵守维护程序,或可能发生的硬件变更,此时应进行及时的调查并采取后续措施。

信息系统审计还要检查硬件监控过程,确保硬件的可用性与可靠性,通过分析硬件使用的相关报告监控硬件的使用。可参考的报告有以下几种。

(1) 硬件错误报告——标识出 CPU、输入/输出、电源和存储故障。管理层应检查该报告以确定系统的工作状态,检测故障并启动纠错程序。

(2) 可用性报告——指出系统工作正常的时间段。如果有过多的死机时间意味着硬件设施不完备、操作系统维护过度、缺乏预防性维护、环境设施(如电源和空调)不充分或缺乏有效的操作员培训。

(3) 利用率报告——记录硬件设施的使用情况。一般通过监控软件捕获处理器、通道

和存储介质的有效利用状况。一般来说,大型计算机的平均利用率应为 85%～95%,偶尔可达到 100%或低于 70%。管理层利用该报告分析和预测当前处理资源的需求趋势,以便及时增减资源。如果利用率经常超过 95%,管理层就应该考虑对用户和应用模式进行审查以求释放空间,升级计算机硬件,或调研是否能通过杜绝不必要的处理或将非关键的处理移至较为空闲的时间以减轻系统的压力。如果利用率经常低于 85%,就有必要确认硬件是否已经超出了处理需求。

3) 硬件设施的能力管理

能力管理是对计算机资源的计划和监控,其目标是根据业务的变化动态地增减资源,以确保可用资源的有效利用。能力计划应由用户和信息系统管理部门共同参与完成,并至少每年进行审查和修改。

能力计划应包括被经验所证实的预测,并同时考虑现有业务的潜在增长和未来业务的扩充,重点应考虑 CPU 的利用、计算机存储的利用、远程通信和广域网带宽的利用、I/O 通道的利用、用户的数目、新的技术的运用和服务水平协议等。

对硬件能力管理的审计应当清楚上述需求的数量和分布具有灵活性,某个类别的特定资源可能会对其他类别的需求产生影响。例如,相对于普通终端,"智能"终端可以减少处理器的处理时间和通信带宽,因此,上述信息与正在使用或计划使用的系统部件的类型和质量密切相关。

4) 对硬件基础设施控制的审计

在对硬件基础设施的采购、运行、维护、监控和能力管理等方面的控制进行审计时,应重点检查和审核其控制的相关文档,必要时也可采用会谈等方法了解控制的有效性。

审查硬件获取计划可以了解信息系统环境设施是否足以适应当前的硬件,审核硬件获取计划是否和信息系统计划同步,并且考虑了现有设备及新设备的技术退化,还需要检查软硬件规格、安装要求及交货时间等说明的准确性。

审查硬件的能力管理程序和性能评估程序,可以确定是否对硬件和系统软件的性能和能力进行连续的审查;判断信息系统管理层的硬件性能监控计划中使用的标准是否基于历史数据和分析结果。

信息系统审计人员还需要审查变更管理控制,确定信息系统变更控制的存在性与有效性。

3. 信息系统软件控制

1) 信息系统软件组成

软件包括系统软件和应用软件,是信息系统审计需要关注的关键区域。系统软件是指控制和协调计算机及外部设备,支持应用软件开发和运行的系统,包括操作系统、数据库管理系统、通信软件、数据管理软件、作业调度软件、程序库管理系统和系统工具软件等,这些系统软件为业务系统的正确运行提供系统级的保障;应用软件是为满足用户不同领域、不同问题的应用需求而提供软件,它拓宽计算机系统的应用领域,放大硬件的功能,ERP 等企业应用系统属于应用软件。

(1) 操作系统。操作系统是系统软件中最重要的部件,它包含用户、处理器和应用程序间的接口,也是计算机中各种用户共享资源(如处理器、内存、辅存和 I/O 设备)的管理者和控制者。操作系统因其所管理的资源、管理的广泛性和采用的管理技术的不同而不同。计

算机的类型、应用目标及其支持的连接设备和网络等均会影响操作系统的需求、特征和复杂性。大型计算机需要处理大量合并和分布交易，要求其操作系统能根据应用的输入和输出，极可靠地管理广泛的资源和无数的并发操作。小型计算机需要处理大量终端用户的数据和程序，或对批处理和交互处理进行混合处理，要求其操作系统能分配和隔离内存，实现多用户共享磁盘空间和 CPU 时间，并管理终端连接，如 UNIX 操作系统。网络环境中的计算机作为具有特定功能的服务器（如 DBMS、目录/文件存储、应用系统等），其操作系统也应具备和多个用户的数据和程序打交道的能力，以便通过网络为客户机工作站提供服务，如 Windows 操作系统。

（2）数据库管理系统。数据库管理系统（Database Management System，DBMS）是一种操纵和管理数据库的系统软件，用于建立、使用和维护数据库。它对数据库进行统一的管理和控制，以保证数据库的安全性和完整性。用户通过 DBMS 访问数据库中的数据，数据库管理员也通过 DBMS 进行数据库的维护工作。DBMS 提供数据定义语言（Data Definition Language，DDL）与数据操作语言（Data Manipulation Language，DML），供用户定义数据库的模式结构与权限约束，实现对数据的增加、删除等操作。常见的 DBMS 有 SQL Server、Access、Oracle 等。

2）软件获取与实施

信息技术的快速发展使得软件的功能也在不断提升，软件可以改进业务流程，以更有效的方式为业务和客户提供应用服务。管理层应保证使用的软件具有最新的版本，保证组织的竞争能力。非最新版本的软件可能逐渐过时，并不再被供应商提供技术支持；可能不具备最新的应用程序所要求的技术特征；同时开放互连系统的特征也使得非最新版本的系统更易于受到安全威胁。

管理层应制定短期和长期的计划，以便及时将操作系统及相关的系统软件迁移到更新、更有效率和效益的版本上。软件的获取同硬件一样，需要相应的招标与评标过程，充分考虑成本与效益，所以从审计角度，软件的获取过程也要得到相应的控制。

由于软件自身的特点及其与硬件的附着性，信息系统软件的采购、实施与通常的硬件同时进行。信息系统审计可以将其作为同一个审计对象加以评估，这也符合信息系统软硬件的集成性的特点。在这种情况下，信息系统审计要特别考虑系统软件采购中的业务和技术因素，包括业务需求、功能需求和技术需求规格，与现有系统的兼容性、安全性需求，对现有雇员的要求，操作人员的培训和聘用需求，对系统性能和网络的影响，组织未来发展的需要。

软件的实施需要制定使用的标准配置，包括功能特征、配置选项和控制方法。从信息系统审计角度，需要对软件在非生产环境下进行测试，在其投入正式运行前需完成相应的认证和使用授权等。

3）软件的变更控制

变更控制程序用来保证变更已经得到授权，管理层和相关人员清楚并参与变更过程，确保变更不会破坏现有处理流程。变更控制程序应保证变更已经得到适当的评估，保证有适当的备份/恢复程序，一旦变更安装失败，能使其影响最小化。

变更控制程序还应通知所有可能受变更影响的相关人员，并保证这些人员已经对变更在各自领域可能产生的影响做了适当的评估。变更后系统投入实际运行前，应确保所有测试结果已进行记录、审查并得到相关领域技术专家的认可。

4）软件的版权与许可

软件版权是国家立法予以保护，非授权软件是导致感染计算机病毒、木马，造成业务损失的不可忽视的因素，也使组织面临诉讼风险。为预防或检测对软件版权的侵犯，管理层或审计部门需要制定相应的政策与管理手段，保证信息系统部门建立了标准的计算机软件许可策略。

（1）审查用于防范非授权使用和复制软件的策略和程序文件。在某些情况下，企业会要求用户签署一个协议，保证不在没有软件许可协议并得到批准的情况下复制软件。

（2）审查所有软件列表。将该列表和网络内各种服务器中所安装的软件相比较。

（3）建立对软件安装的集中控制和自动分发（包括取消用户安装软件的能力）机制。

（4）定期扫描计算机，确保计算机中没有安装非授权的软件。

和软件供应商签署基于访问网的用户数目站点许可协议，防止在同一网络中的多台计算机非法复制软件。在考虑成本效益的情况下，企业可以选择并发许可协议，允许一定数目的用户同时访问网络中的软件，还可以帮助网络管理员确定软件的使用率，可以判断是否需要购买更多的许可。

5）数据库安全控制

数据库安全就是保证数据库信息的保密性、完整性、一致性和可用性。保密性指保护数据库中的数据不被泄露和未授权的获取；完整性指保护数据库中的数据不被破坏和删除；一致性指确保数据库中的数据满足实体完整性、参照完整性和用户定义完整性要求；可用性指确保数据库中的数据不因人为的和自然的原因对授权用户不可用。

数据库安全通常通过存取管理、安全管理和数据库加密来实现。存取管理就是一套防止未授权用户使用和访问数据库的方法、机制和过程，通过程序来控制数据的存取，防止非授权用户对共享数据库的访问。安全管理指采取安全管理机制实现数据库管理权限分配。

数据库系统提供的安全控制措施能满足一般的数据库应用，但对于一些重要部门或敏感领域的应用，仅有这些是难以完全保证数据的安全性的。因此有必要在存取管理、安全管理之上对数据库中存储的重要数据进行加密处理。数据库加密主要包括：库内加密（以一条记录或记录的一个属性值作为文件进行加密）、库外加密（整个数据库包括数据库结构和内容作为文件进行加密）、硬件加密等。

6）计算机病毒及其控制

计算机病毒是一种恶意计算机程序，它向被攻击的目标主机操作系统发出请求，向运行在操作系统中的其他程序复制自己，使得程序受到感染。有一种病毒变体称为蠕虫，蠕虫一般不会像病毒那样感染其他程序，它利用操作系统的漏洞，在计算机网络传播，占用网络资源，对联网环境下客户机/服务器系统造成了严重威胁。

浏览器和电子邮件已成为病毒和蠕虫传播的重要途径。有效的病毒防范方法一是要建立规范严谨的管理策略与程序，二是要采用一定的技术方法，如防病毒软件，来预防和检测计算机病毒。检测病毒的方法有两种，一种是检查计算机是否已感染病毒；另一种是用于监测异常指令的执行，可疑指令只有在得到用户确认后才能被执行。一旦发现病毒，扫描程序会报警，并将其从硬盘上清除或进行隔离。

防范病毒可以采用下面的技术手段：使用启动型病毒保护（内置的、基于固件的保护方法，如硬盘保护卡）可以保护计算机再重新启动后恢复到一个安全的状态；对于联网的工作

站可以采用无盘方式的远程启动；对计算机等设备可以采用基于硬件的口令，阻断病毒入侵的路径；写保护的 U 盘也可以防止病毒传播；对于计算机网络可以利用防火墙阻止不安全的协议进入。

7）信息系统软件的控制与审计

审计人员可通过与系统技术人员和相关负责人的会谈等过程，得到软件获取的审查和批准流程、软件实施的测试程序、测试结果的审查和批准程序、系统软件实施程序等软件相关文档。审计人员要检查软件选择程序，确定软件的选择是基于信息系统计划和业务计划，满足信息系统和业务需求；审查软件的获取可行性研究和选择流程，确定建议的系统目标和目的与招标书是否一致，是否对所有标书采用了相同的选择标准；审查在软件采购、实施过程中，是否特别注意审计成本/效益分析，确认软件采购充分考虑了成本控制；审查软件的安装控制，确保实施新系统的变更过程有相应控制；审查软件维护与变更控制，确保其有效性；审查软件安全控制，检查其安装、参数设置及相关的逻辑设置是否遵循相应的安全控制制度。

信息系统审计要特别检查系统文档，关注文档中有关安装控制语句、系统参数表、系统退出的触发事件及系统日志。对软件的审计要认真检查系统的授权文档，检查对系统访问授权的增加、删除或修改是否进行了记录。在审计过程中，要审查软件实施中的控制的充分性，主要测试的区域包括变更程序、授权程序、访问安全控制、文档规范化控制、系统测试控制、对生产环境的访问控制及相应的审计轨迹。

对于有数据库支持的信息系统来说，要检查数据库控制。检查系统对共享数据的访问是否恰当，检查系统数据结构是否恰当，确认利用了充分的变更程序来保证数据库管理软件的完整性，确认数据库管理系统的数据字典的完整性得到维护，还需要检查数据库管理系统的数据冗余度，确认凡存在数据冗余的地方均已在数据字典或其他文档中进行了适当的交叉引用。

审计数据库的管理应检查所有用户的安全级别和角色在数据库中的标识，确认所有用户或用户组的访问权限应有正当理由。确认数据库具有备份和恢复程序以确保数据库的可靠性和可用性。具备并发访问时保证数据一致性和完整性的机制和程序。

最后为保证数据的完整性和私密性，验证数据库与系统接口，审查数据导入导出程序。

5.1.2　信息系统访问控制

信息系统访问控制可以分为逻辑访问控制和物理访问控制。逻辑访问控制是通过一定的技术方法去控制用户可以利用什么样的信息，可以运行什么样的程序与事务，可以修改什么样的信息与数据。逻辑访问控制内置在应用系统、数据库系统和网络设施中。物理访问控制的目的是限制人员进出信息敏感区域，如机房设备区、数据中心等。物理访问控制措施包括胸牌、内存卡、门锁、从地板到天花板的防护墙、生物测定设备等。

1. 逻辑访问控制

逻辑访问控制是信息系统的主要控制措施之一，通过逻辑访问控制把安全风险降到组织可接受的范围内。信息系统审计人员应当理解逻辑访问措施在保护信息安全方面的作用，并分析与评价逻辑访问控制的有效性。

逻辑访问控制中的身份识别与验证是证明用户身份的过程，用户向系统提交有效的身

份证明，系统验证这个身份证明后向用户授予访问系统的能力。身份识别与验证是多数系统的第一道防线，是防止非授权用户（或进程）进入系统的技术措施。身份识别与验证技术可以分为三类："只有你知道的事情"，如密码；"只有你拥有的东西"，如身份证、令牌卡；"只有你具有的特征"，如指纹、声音、虹膜。这三种技术可以单独使用，也可以结合起来使用。

（1）账号与口令。登录账号与口令的控制是逻辑访问控制的最基本的手段，登录账号用于识别用户，每位用户有唯一的登录账号，登录账号的命名格式应当标准化。口令也叫密码，用于用户身份的鉴定。在识别和鉴定的确认过程中，先证实是合法的用户名，然后强制使用人工输入个人密码以确认身份。口令还应该符合一定的规则，一般要求采用字母与数字混合，长度不低于 8 位，不使用常见的单词等。

（2）生物测定技术。生物测定技术是将人体的物理或行为特征作为访问限制基准，如指纹、虹膜、语音等。识别系统通过比对人体特征，只有人体特征相符时才准予通行，与账号口令访问控制方式相比，是一种更加安全可靠的控制方式。把生物测定技术用于访问控制，首先采集生物特征样本，然后把样本特征转换为一组唯一的数学编码，作为初始模板存储在数据库中，并与后续的多个采样进行对比，形成一个用于验证用户的最终标准模板。在用户进行访问控制时，设备获得用户生物特征的采样。与标准模板进行比对，通过统计数字进行判断是否匹配，并决定是否授予访问权。

（3）逻辑访问授权。逻辑访问控制在正确识别用户身份后，要通过授权过程赋予用户对系统逻辑访问的能力，决定访问资源，并把授权内容正式记录在案，以便于在系统中执行及日后的检查审核。

2. 物理访问控制

物理访问控制是用来保护组织使其免受非授权访问的一种措施，在物理访问控制的限制下，只有经过管理层授权的人员才能进行访问。通用的物理访问控制包括门禁系统（更高的安全控制力可以采用组合门锁或电子门锁、生物特征锁等）、摄像监控、出入陪同、访问日志登记、自动报警系统等。

组织需要针对不同的物理访问控制区域，选择合适的安保措施，利用有效的物理访问控制技术，保障物理访问的安全。

信息系统的逻辑访问控制和物理访问控制应当建立在"知所必需"（need-to-know）的基础上，按照最小授权原则（least-privilege）和职责分离原则（segregation of duty）来分配系统访问权限，只对必须使用资源的人赋予必要的授权，并把这些访问规则与访问授权通过正式书面文件记录下来，作为信息安全的重要文件加以妥善管理。

5.1.3 职责分离控制

职责分离是指遵循不相容职责相分离的原则，实现合理的组织分工。组织内部某些相互关联的职责，如果集中于一个人身上，就会增加发生差错和舞弊的可能性，或者增加了发生差错或舞弊以后进行掩饰的可能性。职责分离关注组织如何将交易授权、交易记录及资产保管等职责分配给不同员工，以防范同一员工在履行多项职责时可能发生的舞弊或错误。

对于信息系统来说，有效的职责分离应当在系统层面和应用程序层面执行，确保某个岗位不会控制业务流程的所有关键阶段。例如，应当严格限制程序员对业务操作，或者不允许

一个计算机程序员独立完成程序设计、测试和变更等关键环节，以减小舞弊风险。

职责分离控制的原则依据组织的规模及其面临的风险来确定。规模较大或舞弊风险较高的单位，应当设置更为严格的职责分离控制。信息系统审计人员应当关注重要的操作与编程活动之间的职责分离，如用户、程序员和数据中心员工等，还应当关注开发与生产、安全与审计、应付账款人员与应收账款人员、密码钥匙管理员与密码更改人员等关键人员岗位的分离情况。有效地实现职责分离，应关注以下几点。

(1) 制定职责分离的管理制度。信息系统的安全管理控制的主要目标是实现职责分离和有效的人员管理。在计算机信息处理环境中，业务处理环境发生了重大的变化，业务流程处理是基于信息系统平台来完成的，同一笔业务的授权、处理、复核、记录等工作可以通过计算机程序来实现，整个工作可以由一个人单独操作计算机完成。所以在计算机信息系统环境中，职责分离原则在业务处理层次被削弱。信息系统需要从组织结构和人员管理上来实现信息系统环境下各种职务之间的职责分离。职责分离的目的在于保证不同的人员承担不同的职责，人员之间可以互相监督和检查，从而防止错误和舞弊行为。

(2) 员工明确其岗位职责。在书面的岗位职责描述和关键岗位分离制度下，员工应当明确其岗位职责及行为准则，所有员工充分理解他们的职责，并且按照职位描述履行职责；被审计单位管理层应当提供足够的安全意识教育和培训，确保员工对职责分离原则的理解及在组织内部建立和实施职责分离制度，尤其在关键的业务操作和编程岗位，审计人员应当关注并检查相关控制。

(3) 关键岗位监控。有效的职责分离控制需要对关键岗位人员的活动进行正式的监督和审查，组织应该制定详细的操作手册，指导员工履行其职责。在信息系统的运行中，这些手册对计算机操作人员尤其重要。例如，计算机操作员手册应当提供系统启动和关闭的程序、紧急事件处理程序、系统工作状态汇报程序及操作员禁止从事的活动等方面的规定。操作手册还应该为每个应用程序的操作员提供更多的指导，例如，对职位设置、控制台和错误信息、工作检查点及系统故障后重启和恢复步骤的指导。操作手册应该明确规定禁止操作员撤销文档标记或设备错误信息。

监督和审查员工在计算机系统中的活动，能帮助确保这些活动按照规定的手续来进行，有效纠正错误，并且确保只有在得到授权的情况下才会使用计算机。为了实施有效的监督，计算机系统上的所有用户活动都应当记录在活动日志上作为审计轨迹。监督人员应该定期审查这些活动日志，寻找不相容的活动，调查任何异常情况。对计算机系统活动的定期审查能确保员工按照既定政策来履行职责，并且在操作流程改变时明确更新的需求。

加强职责分离控制机制，包括交易授权、资产保管、数据访问、授权单、用户授权表等。

(1) 交易授权是用户部门的职责。授权是将完成某项工作所必需的权力授给部属人员。管理层和审计师应当定期进行检查，以发现非授权交易记录。

(2) 资产保护。组织必须确定并适当分配资产保管责任。数据所有人通常指定为特定的用户部门，其职责应当书面说明。数据所有人负责确定能充分保证安全所需的授权水平，而管理层通常负责实施和加强安全体系。

(3) 数据访问。对数据访问的控制是通过在用户场所和计算机信息处理设施(IPF)综合采用物理层、系统层及应用层安全措施组成的。必须保护物理环境，以防止非授权人员访问与中央处理单元连接的各种物理设备(通过它们可以访问数据)，系统层和应用层安全则

可以预防非授权人员访问数据库。

(4) 授权单。用户部门管理人员必须向信息系统部门提交正式的授权单,明确其员工的访问权限,授权单必须经过管理层的明确批准。在大型公司或远程站点中,应当保留签字授权单,也应当把申请表和签字单进行核对,应当定期审查访问权限以确保它们与用户工作职责是匹配的。

(5) 用户授权表。信息系统部门应当使用授权单的数据来建立和维护用户授权表,明确谁有权更新、修改、删除和查看数据。用户授权表也是用户访问控制列表,必须通过额外的口令或数据加密加以保护,以防止非授权访问,应当采用控制日志记录所有用户的活动情况。管理层应定期对日志进行审查,并对所有例外事项进行调查。

管理层除了定期审查那些物理或逻辑访问控制之外的活动,职责分离的控制活动通常依靠监督和批准授权的文件来进行有效控制。

5.1.4 信息系统安全审计

随着信息技术的广泛应用,信息系统是否安全可靠对信息社会有着决定性的影响,信息系统安全问题成为信息化环境下的重要问题。企业实现信息化后,不仅要建立信息系统的安全管理控制体系,还要实施信息系统安全审计,以确保信息系统的各项安全管理控制措施合理、健全,并有效地发挥作用。

1. 信息系统面临的威胁

信息系统由于受到其自身的体系结构、设计思路及运行机制等限制,也隐含着许多不安全因素。常见的有:数据输入、输出、存取与备份,源程序及应用程序、数据库、操作系统等漏洞或缺陷,硬件和通信部分的漏洞、缺陷或者遗失,还有电磁辐射、环境保障系统、企业内部人的因素、软件非法复制、黑客与计算机病毒等,它们的具体表现如表 5-1 所示。

表 5-1 引发信息系统安全的各种因素

项 目	面临的风险
数据输入	数据容易被篡改或输入虚假数据
数据输出	经过处理的数据通过各种设备输出,有被泄露和被盗看的可能
数据存取与备份	可能被非法用户侵入系统恶意存取数据,也可能由于没有备份数据而使系统发生故障后难以恢复
系统开发与源程序	系统开发设计中由于人为和自然原因,可能留下各种隐患和缺陷。用编程语言书写的计算机处理程序,容易被修改和窃取,并且程序本身也可能存在漏洞
应用软件	软件的程序被修改或被破坏,会损坏系统的功能,进而导致系统瘫痪;软件文档的遗失也会给软件升级与维护带来困难
数据库	数据库存有大量的数据资源,如果遭到破坏或失窃,其损失将难以估计
操作系统	操作系统是支持系统运行、保障数据安全、协调处理业务和联机运行的关键部分,如果遭到攻击和破坏,将会造成系统运行的崩溃
硬件系统	计算机硬件本身具有被破坏、盗窃的可能。此外,组成计算机的电子设备和元件也存在偶然故障的可能,有时这种偶然故障可能是致命的
网络和通信	网络可以将不同地点的计算机信息系统连接在一起,这样就有可能导致未经许可的数据存取、滥用、发生错误的可能性不仅局限于单个计算机,而且在网络的每一点上都可能发生。信息和数据通过通信系统进行传输具有被窃听的危险

续表

项　　目	面临的风险
环境保障	信息系统需要一个良好的运行环境，周围环境的温度、湿度、清洁度及一些自然灾害等，都会对计算机硬件、软件造成影响
企业内部人员	低水平的安全管理、人员素质低下、偶然的操作失误或故障的违法犯罪行为等，都会成为影响信息系统安全的因素
黑客与病毒	一些非法的网络客户，出于各种动机，利用所掌握的信息技术会进入未经授权的信息系统，恶意的黑客可能导致严重的问题。病毒会在计算机系统之间进行传播，会在某个特定的时刻破坏计算机内的程序、数据甚至硬件，损坏系统，甚至使系统瘫痪

针对上述信息系统面临的风险，必须加强信息系统的安全管理，并对信息系统的各项安全管理措施是否健全、有效进行审查与评价。

2. 信息系统安全管理

在信息化社会中，一方面信息已成为人类重要资产，在政治、经济、军事、教育、科技、生活等方面发挥着重要作用，另一方面信息技术的迅猛发展带来的信息安全问题日益突出。由于信息具有易传播、易扩散、易毁损的特点，信息资产比传统的实物资产更加脆弱，更容易受到损害，使组织在业务运作过程中面临大量的风险。其风险来源于组织管理、信息系统、信息基础设施等方面的固有薄弱环节，以及大量存在于组织内、外的各种威胁，因此对信息系统需要加以严格管理和妥善保护，保证信息处理和传输过程是可靠的、有效的，保证重要的敏感信息是机密的、完整的和真实的。为达到这样的目标，必须采取一系列信息安全控制措施，使信息避免威胁，保障业务的连续性，最大限度地减少对业务的损失，最大限度地获取投资回报。

1）信息安全

信息安全一般包括实体安全、运行安全、信息资源安全和管理安全四个方面的内容。实体安全是指保护计算机设备、网络设施及其他通信与存储介质免遭地震、水灾、火灾、有害气体和其他环境事故（如电磁污染等）破坏的措施、过程。运行安全是指为保障系统功能的安全实现，提供一套安全措施（如风险分析、审计跟踪、备份与恢复、应急措施）来保护信息处理过程的安全。信息资源安全是指防止信息资源的非授权泄露、更改、破坏，或使信息被非法系统辨识、控制和否认。管理安全是指通过信息安全相关的法律法令和规章制度以及安全管理手段，确保系统安全生存和运营。

信息安全的目标是保证信息的机密性、完整性、可用性、真实性和有效性。信息的机密性是指确保只有那些被授予特定权限的人才能够访问到信息。信息的机密性依据信息被允许访问对象的多少而不同，所有人员都可以访问的信息为公开信息，需要限制访问的信息为敏感信息或秘密信息。根据信息的重要程度和保密要求将信息分为不同密级，例如，内部文件一般分为秘密、机密和绝密三个等级。信息的完整性是指要保证信息和处理方法的正确性。信息完整性一方面是指在使用、传输、存储信息的过程中不发生篡改信息、丢失信息、错误信息等现象；另一方面是指信息处理的方法的正确性，执行不正当的操作，有可能造成重要文件的丢失，甚至整个系统的瘫痪。信息的可用性是指确保那些已被授权的用户在他们需要的时候，确实可以访问得到所需要的信息。即信息及相关的信息资产在授权人需要的

时候，可以立即获得。通信线路中断故障、网络的拥堵会造成信息可用性的破坏。信息系统必须能适当地承受攻击并在失败时恢复。另外，还要保证信息的真实性和不可否认性，即组织之间或组织与合作伙伴间的商业交易和信息交换是可信赖的。

2）信息安全管理

信息安全管理是从管理、技术、人员、过程的角度来定义、建立、实施信息安全管理体系，指导安全实践活动，通过维护信息的机密性、完整性和可用性，来管理和保护组织所有的信息资产。信息安全管理一般包括制定合理的信息安全方针与策略、风险评估、控制目标与方式选择、制定规范的操作流程、对员工进行安全意识培训等一系列工作，来保证组织信息资产的安全与业务的连续性。

信息系统的安全管理是一项复杂的系统工程，它的实现不仅需要技术方面的支持，还需要法律、制度和人的素质因素的配合。因此，信息系统安全管理的模型如图 5-1 所示。从图中可以看出各层之间相互依赖，下层向上层提供支持，上层依赖于下层的完善，最终实现数据信息的安全。

有效的信息安全管理要尽量做到在有限的成本下，减少信息安全事故的发生，保障组织目标的实现。

第 7 层	数据信息安全
第 6 层	软件系统安全措施
第 5 层	通信网络安全措施
第 4 层	硬件系统安全措施
第 3 层	物理实体安全环境
第 2 层	管理细则和保护措施
第 1 层	法律、规范、道德、纪律

图 5-1 信息系统安全管理的层次模型

3. 信息系统安全审计

1）信息系统安全审计的定义

信息系统安全审计就是对被审计单位的信息系统安全控制体系进行全面审查与评价，确认其是否健全有效，确保信息系统安全运行。

2）信息系统安全审计的目标

信息系统安全审计的目标一般包括：确认被审计单位的各项信息系统安全控制措施是否健全；确认信息系统的安全控制措施是否有效执行；确认被审计单位的信息系统安全策略与程序是否能最大限度地降低信息系统工程安全风险。

3）信息系统安全审计的内容

应从整体业务风险的角度，建立、实施、运行、监视、评审、保持和改进其信息安全管理体系。审计信息安全管理体系，就是要评估其建立、实施、运行、监视、评审、保持和改进信息安全管理体系的全过程，可重点关注以下七个重要审计事项。

（1）信息安全管理体系建设。

信息安全管理系统包括制度体系、组织体系、资产体系。

① 制度体系。安全制度体系包括组织信息安全方针和各层级信息安全实施方案。审计人员应审查被审单位信息安全方针的文件，是否由管理层批准；是否印发给内外部员工；是否明确了信息安全管理工作的总体目标、范围和原则。审阅信息安全实施方案时，应关注实施方案是否以文档形式记录在案；是否具有定期评审的记录，记录的日期间隔与评审周期是否一致；是否记录了相关人员的评审意见。抽查安全管理员对信息安全实施方案的认知程度。

（2）组织体系。安全组织体系是组织建立的信息安全管理机构和岗位。审计人员应查阅被审计单位成立信息安全工作领导小组的文件，是否正式印发；是否由管理层委派负责

人；是否明确其职责。查阅被审计单位信息安全组织体系，应关注是否明确信息安全管理组织的职责；是否明确单位内各部门的职责和分工；各个岗位的职责范围是否清晰、明确；是否包括机房管理员、系统管理员、数据库管理员、网络管理员、安全管理员等重要岗位人员；是否明确应配备专职的安全管理员；是否明确对某些关键事务的管理人员应配备两人或两人以上共同管理；是否明确各个岗位人员应具有的技能要求。审计人员应查阅被审计单位信息安全领导小组和信息安全管理各部门工作记录，关注是否具有日常管理工作执行情况的工作记录；是否切实开展了职责范围内的工作。审计人员应查阅被审计单位内外部员工的信息安全职责和要求，关注被审计单位是否制定了相关文件，规范那些不直接从事信息安全管理工作的内部员工和外包人员的岗位信息安全职责。抽查某内部员工或外包人员对其岗位信息安全职责的认知程度。

③ 资产体系。资产管理体系是不断更新的完整的信息资产清单。审计人员应查阅被审计单位信息资产管理文件，是否明确了信息资产管理的责任部门、责任人；文件内容是否覆盖信息资产使用、传输、存储、维护等方面；是否明确了信息分类标识的原则和方法。审计人员还应查阅被审计单位信息资产清单，是否依据资产的重要程度对资产进行分类和标识管理；不同类别的资产是否采取不同的管理措施。审计人员应查看信息安全资产管理体系是否覆盖资产责任部门、责任人、所处位置和重要程度等方面。

(2) 评估信息安全保护等级。

制定风险评估计划和方案，定期对信息资产进行风险评估，确定其安全保护等级。信息资产发生变化，应及时进行再评估。风险评估和安全等级保护定级结果应记录在案，并按要求向有关部门报备。

审计人员应查阅被审计单位信息安全风险评估方案，是否以文档形式记录在案；是否具有定期评审的记录；记录的日期间隔与评审周期是否一致；是否记录了相关人员的评审意见；是否按照评估方案制定了评估计划。查阅被审计单位信息安全风险评估报告，是否按照评估计划定期进行评估；评估过程中是否确定了信息安全的保护等级；保护等级是否经过定期评审；是否在信息资产发生变化的情况下进行过再评估。查阅重要信息系统等级保护定级报告，是否编制了等级保护定级报告；是否向所在地公安机关和上级主管部门进行备案；有主管部门的，是否经主管部门审核批准。查阅有关文件，确认被审计单位是否建立了信息资产安全等级保护测评机制。

(3) 实施信息安全管理。

针对不同安全等级的信息资产，设定相应具体的控制目标和控制活动，经管理层批准后实施。各级各类信息资产的控制目标和控制活动应记录在案，定期评审，保持更新，并形成文件化的操作规程供员工使用。还应定期实施信息安全等级保护测评。

审计人员应查阅不同安全等级的具体控制目标和控制活动，是否以文档形式记录在案；是否经过了相应管理层的批准；是否具有定期评审的记录；记录的日期间隔与评审周期是否一致；是否记录了相关人员的评审意见。查阅控制活动的实施记录，是否严格按照操作规程实施。查阅信息安全等级保护测评报告，是否定期进行安全等级测评；测评周期是否符合等级保护办法规定。

(4) 人员安全教育培训和管理。

人是信息安全管理体系的核心要素，人员的安全意识将决定组织信息安全管理的成败。

在信息安全教育、人员安全管理和信息安全培训三方面，提高人员的安全意识。

① 制定信息安全教育计划。审计人员应访谈安全管理员、系统管理员、网络管理员和数据库管理员，关注其对工作相关的信息安全基础知识、安全责任和惩戒措施等的理解程度。查阅信息安全教育及技能培训和考核管理文档，是否明确培训周期、培训方式、培训内容和考核方式等相关内容；是否具有不同岗位的培训计划；培训内容是否包含信息安全基础知识、岗位操作规程等。

② 制定人员安全管理政策，在人员录用、人员使用、人员考核和人员离岗四个环节，确保组织聘用的人员安全。人员录用环节，人力资源部门应制定明确的岗位（特别是信息安全岗位）的职责和技能要求，严格规范人员录用过程，对被录用人的身份、背景、专业资格和资质等进行不同程度的审查，与被录用人签订岗位安全协议和保密协议，使其了解所在岗位的信息安全职责，对于关键或敏感岗位的招聘，应尽量在内部人员中选拔；人员使用环节，对于接触被审计单位商业秘密或国家秘密的人员，应进行恰当的警示教育。人员授权使用信息系统或权限变更时，应履行审批手续。建立定期轮岗制度和强制休假制度。建立合理的薪酬体系，确保人员稳定。对于违反信息安全规章制度的人员，应给予必要的处理；在人员考核环节，应定期对各岗位（特别是信息安全管理岗位和关键或敏感岗位）人员的信息安全技能进行考核，并记录在案；在人员离岗环节，对于离岗或岗位变动人员，应敦促其交还原工作岗位的钥匙、工作证件、门禁卡，归还计算机等软硬件设备和其他信息资产，注销其在信息系统中的权限。关键或敏感岗位的人员离岗前，应承诺其调离后的保密义务。

③ 信息安全培训。应定期评估录用人员（特别是信息安全管理人员、信息技术人员、关键或敏感岗位人员）的技能，确保其能够满足岗位信息安全职责的需要，并根据评估结果，制定和不断更新对录用人员的信息安全培训计划。

（5）测评信息安全工作的有效性。

信息系统建设完成后，运营、使用单位或者其主管部门应当定期对信息系统安全等级状况开展等级测评；也应当定期对信息系统安全状况、安全保护制度及措施的落实情况进行自查。

（6）有效弥补信息安全缺陷。

经测评或者自查，信息系统安全状况未达到安全保护等级要求的，运营、使用单位应当制定整改方案，实施整改；还应查阅整改方案和整改报告，关注是否根据自查和测评发现的问题制定了相应的整改方案，整改方案是否有效实施。

（7）确保由外部第三方执行的活动受到足够的控制。

信息安全不仅适用于组织内部的信息系统，同样也适用于由外包商或代表本单位的第三方操作的信息系统。因此，应当制定适当的政策和程序，严格执行和监控，保证那些被外部第三方访问、处理、管理或与外部进行通信的信息和设备的安全。在与外部第三方签订的涉及访问、处理或管理被审计单位的信息或系统的合同中，或在信息系统中增加产品或服务的采购合同中，应涵盖所有的安全要求。在允许客户访问被审计单位的信息系统之前，必须确保所有安全方面的需求都被充分地考虑。

4. 信息系统安全审计程序

信息系统安全审计程序通常包括：

（1）询问被审计单位制定信息系统安全策略所依据的标准。

(2) 获取被审计单位制定的各项信息系统安全控制措施。

(3) 复核安全访问规则,确认是否符合企业运营目标,并合理划分职责。

(4) 与安全管理人员、网管人员、数据库管理员、应用系统开发经理进行面谈,了解其工作职责及相应的安全管理过程。

(5) 审查安全策略、标准、规程和指南的使用,并确认有关文档是否已发给相关员工。

(6) 审查安全管理人员、网管人员、数据库管理员、应用系统开发经理是否有足够的经验和专业知识。

(7) 检查被审计单位的实体安全控制、软件安全控制、数据安全控制、系统入侵防范控制、通信网络安全控制和病毒防范控制等安全控制措施,确认其是否健全。

(8) 实地观察被审计单位的实体安全环境,确认其是否符合有关标准。

(9) 实地观察计算机房中水及烟雾探测器的装置,检查其电力供应是否充足,观察这些装置的位置是否有明显的标识。

(10) 查看灭火器的位置是否适当,是否显而易见,最近是否进行过检验。

(11) 审查计算机房防火墙、地板和天花板的耐火能力。

(12) 检查备份电力系统的配置和使用。

(13) 观察电线是否配置在防火板槽里。

(14) 查看监视器和警报系统。

(15) 检查不间断电源的配置情况及测试报告。

(16) 观察机房的进出控制,查看出入登记日志。

(17) 取得一份应急计划,判断是否有信息处理设备保持安全的规定措施,询问负责信息系统的员工对这份计划是否熟悉。

(18) 观察软件访问及操作运行情况。

(19) 检查软件备份及保管情况。

(20) 采集操作系统、数据库管理系统、应用系统和网络设备等的日志进行分析,确认各项安全控制措施是否有效执行。

(21) 检查用户的数据存取权限表及数据读、写、修改和删除等存取控制表,确认是否合理授权。

(22) 询问被审计单位对重要数据是否加密。

(23) 检查备份数据的登记记录,确认所有数据备份是否都清晰登记,并妥善保管。

(24) 试图访问没有访问权限的数据和交易,访问应不会成功,并且会记录在安全报告中,查看非法访问记录与报告。

(25) 审查网络连接图,查看各计算机、终端设备及网络交换机和调制解调器等辅助系统间的通信传输连接点,盘点其数量以确保网络架构图的正确性。

(26) 取得终端设备的存储位置清单,据此盘点终端设备的库存数,确认记录的正确性和终端设备在网络上确实存在。

(27) 查阅访问权限文件样本,判断是否规定适当的权限,权限的取得要求是否合理。

(28) 取得打印的计算规则报表并抽查该报表,判断实际发生的访问是否与核准访问的文件相一致。

(29) 取得终端设备识别卡及钥匙,并谋划越过权限访问计算机数据,了解安全管理员

是否追查越权的非法访问行为。

(30) 建立一个不符合要求的密码,如太短、数字或字符使用不当等,对密码格式要求进行测试。

(31) 抽查密码变更记录,判断用户是否在规定的时间内变更其密码。

(32) 尝试登录终端设备,并故意输入数次错误密码,判断错误密码输入数次后,该登录账号是否被锁定。审查安全管理员是否在验证或核实相关人员身份后才进行解锁。

(33) 登录终端设备并输入密码,观察密码是否屏蔽明文显示。

(34) 检查系统是否安装实施防火墙,评估网络架构和防火墙的配置是否正确设计。

(35) 审查所使用的加密机制和网络安全认证机制。

(36) 模仿入侵访问报告系统,检查系统入侵防范控制是否有效。

(37) 检查入侵访问报告,查看对入侵访问的追踪和审查记录。

(38) 检查是否安装防病毒软件,查看计算机病毒检测和清除的记录。

(39) 抽查安全控制措施进行测试,如果检查出严重的控制弱点,应扩大测试的范围,加大测试力度。

在信息系统安全审计过程中,审计人员在对单项控制的强弱进行测试时,要考虑其对资产保护和信息保护的有效性及信息系统总体安全的影响,不断对信息系统安全性做出全局性的判断。

5.1.5 信息系统业务连续性审计

1. 业务连续与灾难恢复

信息系统的灾难恢复和业务持续计划是企业中总的业务持续计划和灾难恢复计划的重要组成部分。信息系统几乎支持企业所有的业务过程,需要建立恢复设施,保证灾难发生时,信息系统仍然能够正常运行。

1) 灾难与业务中断

灾难可能是由自然灾害引起的,如地震、洪水、龙卷风、雷暴和火灾等,这些灾害可能对信息处理场所与设施造成严重危害;当不能正常提供预期的服务时,就会引起业务中断与损害,如供电、通信、燃气、空调、运输等;人为的破坏也会引起灾难,如恐怖袭击、黑客网络攻击、计算机病毒等。从企业内部系统故障、用户的操作错误到火灾、地震等,都可能造成系统业务中断。

如果没有灾难恢复与业务持续计划,上述风险将给企业造成致命的打击。必须采取必要的程序,使系统服务恢复到正常的运行状态。灾难恢复涉及硬件、软件和数据,为有效地恢复业务,需要对相关的风险进行评估,确定其对业务的影响程度,然后以此为基础,建立灾难恢复与业务持续计划,当灾难发生时,能够快速而有效地响应使系统恢复正常运行。其意义在于:

(1) 当灾难发生时,最大限度地保护企业数据的实时性、完整性和一致性,降低数据的损失,快速恢复操作系统、应用和数据。

(2) 提供各种数据恢复策略选择,尽量减小数据损失和恢复时间。

(3) 保证在发生各种不可预料的故障、破坏性事故或灾难情况时,能够持续服务,确保业务系统的不间断运行,降低损失。

2）灾难恢复与业务持续计划

灾难恢复(Disaster Recovery，也称灾备)，指自然或人为灾害后，重新启用信息系统的数据、硬件及软件设备，恢复正常商业运作的过程。

灾难恢复计划(Disaster Recovery Planning，DRP)是通过有序的计划，帮助企业控制灾难恢复活动，使系统从灾难中恢复过来。灾难恢复计划是业务连续计划的一部分，核心是对企业的灾难性风险做出评估、防范，特别是对关键性业务数据、流程予以及时记录、备份、保护。

业务持续计划(BCP)是为避免关键业务功能中断，减少业务风险而建立的一个控制过程，包括对支持组织关键功能的人力、物力需求和关键功能所需的最小级别服务水平的连续性保证。BCP 关注的是组织日常风险管理程序所不能完全消除的剩余风险，BCP 的目标就是要把组织的剩余风险和因意外事件产生的风险降到组织可接受的程度。

3）业务持续计划生命周期

业务持续计划按其生命周期可分为以下几个阶段：业务影响分析，运行分类和重要性分析，制定业务持续计划和灾难恢复计划，培训与意识教育程序，测试与实施计划，监测。

(1) 业务影响分析(Business Impact Analysis，BIA)。业务影响分析确定影响组织业务连续运行的事件，揭示了每种风险可能对业务造成的损失，评估其对组织的影响。在业务影响分析过程中应该注意考虑以下几方面。

① 关键业务流程。评估每个流程，确定其重要性；流程的中断会引起组织无法接受的收入减少、成本增加；流程中的业务处理所采用的技术和方法，必须满足法律、法规的要求；流程是否是关键流程，还取决于运行时间和运行模式。

② 与关键业务流程相关的关键信息资源。信息资源出现故障并不一定引起灾难，除非它与特定的关键业务流程相关。例如，某个信息资源的失效将影响组织产生利润的业务流程，那么这个资源就是重要资源。

③ 关键恢复时间周期。中断的业务在一定的时间周期内必须恢复，否则将引起组织的重大损失。恢复的时间长短取决于被中断业务的性质，需要考虑恢复成本和停机成本，恢复时间与成本如图 5-2 所示，应当综合考虑停机成本与恢复成本，使总成本最小化。停机成本随着时间的推迟而增加，恢复成本随着时间的推迟而减少，总成本曲线成 U 型，U 型曲线上可以找到成本最低点。

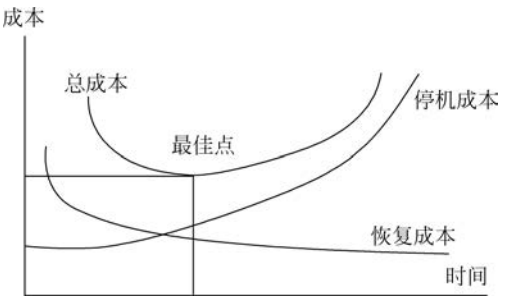

图 5-2　恢复时间与成本

(2) 重要性分类。制定业务持续计划的重要依据就是对应用的重要性进行分类，分类的尺度与系统的风险大小有关，系统的风险级别取决于重要业务发生中断的可能性，以及关

键恢复时间周期对业务运行的影响。一个典型的风险排序系统应当包含如表 5-2 所示的分类标准。

表 5-2 风险排序系统包含的重要性分类标准

重要性分类	描 述
关键的(Critical)	因灾难停机后,除非使用同样能力的系统进行替代,否则这些功能不再起作用。关键应用只能是计算机系统控制的全自动方式。不能使用人工方式替代,组织对系统中断的忍耐力非常有限,所以停机的成本很高,必须对系统立即恢复(通常是几小时到 1 天)
重要的(Vital)	因灾难停机后,这些功能可以由人工方式完成,但只能维护一段时间,与关键的系统相比,此级别的系统可以对系统中断有更强的忍耐力,所以可以降低中断成本,在一定时间范围内恢复系统(通常是 1～5 天)
敏感的(Sensitive)	因灾难停机后,这些功能可以由人工方式完成,可以允许有一个较长时间的恢复期(一周以上),因此恢复成本较低。虽然可以人工完成,但流程较困难,需要增加额外的员工
不敏感的(Nonsensitive)	因灾难停机后,对业务流程没有什么影响,恢复期可以延长到更长时间,对组织来说,基本没有什么恢复成本

(3) 恢复操作。灾难恢复系统的操作方式分为全自动恢复和人工恢复。

① 全自动恢复。通过一些高可靠性软件的控制,在灾害发生时使生产系统的应用切换到灾难备份系统,并把生产系统的数据切换到灾难恢复站点,在生产系统修复后,把在灾难恢复站点运行的应用返回给生产系统,很好地保证了重要业务应用的连续性。这种方法的优点是:切换速度快,大大地减少了系统管理员在灾难发生后的工作量。缺点是:成本高;一些次要因素,如服务器死机、通信联络中断等,也随时有可能引发主生产系统切换到灾难恢复站点的操作。

② 人工恢复。利用人工方式在灾难恢复站点把应用加载到服务器上,同时以人工方式将存储在备份介质上的生产系统备份数据输入恢复站点。这种方法的优点是:操作人根据实际情况做出判断并采取相应行动;系统恢复的安全性好,不会出现自动恢复系统中因为服务器或网卡损坏而发生误切换的情况;人工恢复的成本较低。缺点是:对操作人员的技能水平与反应能力有较高要求;操作人员工作量加大;会产生较长时间的业务应用中断。

(4) 恢复策略。应当采取合理的、具有可接受的恢复成本的策略,恢复关键信息系统,即恢复成本不应大于停机成本。支持关键业务的应用系统恢复策略,对于那些使组织遭受较大损失的中断,特别是影响主要物理设施的灾难,要建立异地备份方案。

① 热站(hot site)。热站提供从机房环境、网络、主机、操作系统、数据库、通信等各方面的全部配置,灾难发生后,一般几个小时就可以使业务系统恢复运行。热站提供的硬件设施与系统软件必须与原有系统一致,启用时,只需操作人员到位并安装应用程序、数据与文件即可运行。热站主要是为组织提供一个在有限时间内的应急手段,并不适合长期使用,应当看作灾难或中断发生后,为保证重要业务连续运行所采取的一种临时性的方法,使用时间不要超过几周。在使用热站的同时,要做好下一步的计划,尽快恢复主系统的运行。主系统恢复后,服务商将把组织的恢复策略从热站转移到温站或冷站中,以空出热站供其他申请者使用。

② 温站(Warm Site)。温站只配备了部分设备,通常没有主机,只提供网络连接和一些外部设备(如存储设备、UPS 设备等)。使用温站是基于这样一个前提,计算机很容易获得,并可以快速安装使用,平时不提供计算机是为了节约成本,降低温站的费用。安装计算机或其他缺少的设备可能要花几天时间,但一旦所需组件安装完毕,温站可以在几小时内提供服务。

③ 冷站(Cold Site)。冷站只提供支持信息处理设施运行的基本环境(如电线、空调、场地等)。灾难发生时,所有设备都必须运送到站点上,要从基础设施开始安装,因此故障恢复时间可能会很长。

④ 冗余信息处理设施。冗余信息处理设施是企业自己配备的、专用的恢复站点,用来对关键应用系统进行备份与恢复。建立冗余的信息处理设施有一个前提:两套系统的软件、硬件之间必须具有兼容性和可用性。采用这种备份方式,要注意以下问题:选择的恢复站点不能像主站点那样面临同样的自然灾难;应当在双方之间建立一个软件、硬件的协调策略,备份系统应当与主系统有充分的兼容性作为备份的基础;备份与恢复过程中需要用到的资源要有保证;即使是冗余信息处理设施与主机系统属于同一个所有者,处在同样的管理之下,也要对其备份与恢复操作进行经常性的测试。

⑤ 移动站点(Mobile Site)。移动站点是一种特别设计的拖车式计算设备,它可以快速地转移到业务部门或者恢复站点。移动站点是一个已做好充分准备的信息处理设施,可以提供满足特定条件的恢复服务。

⑥ 组织之间签订互惠协议(Reciprocal Agreement with Other Organization)。组织之间签订互惠协议是指具有相同设备与应用系统的两个组织或多个组织之间互相为对方建立备份的方法。通过签订协议,承诺当任何一方发生应用中断时,另一方必须为其提供计算机供对方作为备份系统使用。

(5) 制订灾难恢复与业务持续计划。业务持续计划和灾难恢复计划应当涉及业务流程中断后所有的相关问题,应当简洁并正式成文,便于理解,并在异地备份场所存放一份计划的副本。当灾难发生时,明确恢复工作中的任务与职责。

灾难恢复计划的负责人组建团队实施灾难恢复策略,确定与各个团队相关的关键决策者、信息部门和终端用户的相关职责。建议通过团队类型和恢复工作相关关系矩阵图,明确相关团队的责任。团队的成员都应该得到培训,并时刻准备在突发事件发生时启动灾难恢复计划。

业务持续计划的最终目标是保护业务的持续运行。业务持续计划不仅要考虑信息系统的服务需要,还要考虑整个组织的业务需要。业务持续计划主要组成部分有:业务持续计划关键决策人员、对所需软硬件系统的备份、组织、职责分配、通信网络和保险。

(6) 业务持续计划(BCP)的测试。

业务持续计划的测试应当完成下列任务:验证 BCP 的完全性或准确性;评价 BCP 测试中个人的绩效;评价对非 BCP 团队成员的其他员工的教育与培训;评价 BCP 团队与外部供应商之间的协调性;通过实施预定的程序来测试备份站点的能力与容量;评估重要记录的检索能力;评价要转移到恢复站点的设备的状态、数量及供应情况;评价与维护业务实体有关的运行活动和信息系统处理活动的绩效。

实施 BCP 测试。在 BCP 测试实施前,为正式测试做一系列必要的准备工作,这些恢复

准备工作应当在灾难发生前就做好安排，一旦灾难发生，就可以快速启动 BCP，缩短恢复时间；在真正 BCP 测试阶段，通过实际的运行活动来测试 BCP 的特定目标，评估人员审核相关人员的操作活动，测试的目的就是衡量组织是否可以对可能出现的紧急情况进行有效响应。在测试后续阶段，对 BCP 计划进行正式的总体评价，并提出进一步完善的建议。

建立测试文档。在测试的每个阶段，应当对观察到的现象、出现的问题和提出的解决方案建立详细的文件，每个团队都应当把日常工作中的重要步骤与信息记录在日志文件中，这些文件应当成为重要的历史信息，以对将来的灾难恢复工作提供参考指南，同时这些文件也可成为分析 BCP 优劣的重要依据。

分析测试结果。通过基于实际观察的、量化的评价来判断 BCP 计划是否成功，是否达到预定的目标。

维护测试计划。定期对业务性连续性计划和策略进行审核与更新，持续跟进需求变化。

(7) 异地备份。

异地存储是为了保证组织的重要盈利活动不在灾难事件中被中断，采用存储介质将重要的程序及数据存储在异地，以备恢复系统使用。

数据备份有多种方式：完全备份、增量备份、差分备份等，组织可以根据实际情况，灵活使用，采用多种方式结合的备份策略。完全备份是将系统中所有的数据信息全部备份；增量备份是只备份上次备份后系统中变化过的数据信息。差分备份是只备份上次完全备份以后变化过的数据信息。

由于数据备份的方式不同，恢复数据时需要的备份介质数量也不一样：如果使用完全备份方式，只需上次的完全备份数据就可以恢复所有数据；如果使用完全备份＋增量备份方式，则需要上次的完全备份数据＋上次完全备份后的所有增量备份数据才能恢复所有数据；如果使用完全备份＋差分备份方式，只需上次完全备份＋最近的差分备份数据就可以恢复所有数据。

2. 灾难恢复与业务持续计划的审计

1) 业务持续计划的审计任务

在灾难恢复与业务持续计划审计时，信息系统审计人员的主要任务是理解与评价组织的业务持续策略及其与组织业务目标的符合性；参考相应的标准和法律法规，评估业务持续计划的充分性和时效性；审核业务持续计划测试结果，验证计划的有效性；审核异地备份设施和环境，评估异地备份站点的适当性；审核应急措施、员工培训、测试结果，评估紧急情况下的有效反应能力；审核业务持续计划的维护措施有效性。

2) 业务持续计划的审计步骤

信息系统审计人员验证业务持续计划的基本要素，应该审核业务持续计划的测试结果，并检查是否把相关纠正措施纳入整个计划中。信息系统审计师应该评估测试结果的完备性与准确性。判断测试结果是否被组织中的相关管理人员复核，是否达到了预期的目标，是否发现了问题的趋势及提出了可能的解决方案。

信息系统审计师应当对异地存储设施进行评价，以检查重要的介质和文档是否存在，并保持与原始介质的同步。应该评估异地存储场所的安全性，检查是否对其建立了适当的物理和环境访问的控制措施，以保证只有授权人员访问存储设施。

信息系统审计师应该访问业务连续性计划的重要参与人员，了解他们的职责，并且检查详细描述其职责的最新文件。

审计师应当检查与业务持续计划有关的厂商所签订的合同，以及厂商的相关记录及信用情况，厂商的承诺都应当有正式的书面记录并进行验证。

信息系统审计师还应当审核灾难恢复计划中的保险事务，判断保险费用的合理性。并检查组织在存储介质的损失、业务中断、设备更换和业务连续性等方面的保险项目的充分性。

5.2　一般控制审计程序

一般控制主要包括基础设施控制、系统访问控制、网络架构控制、数据及数据库安全控制、灾难恢复与业务持续性控制等。对一般控制进行审计，需要对上述控制分别进行审计。

5.2.1　基础设施控制审计

(1) 物理环境的检查。审计人员可以从以下四个方面检查机房设施：机房的防水、防火系统是否满足消防要求；机房设备是否有浪涌(超出正常工作电压的瞬间过电压)和备份电力设备；机房的温度、湿度是否合规；机房建设是否考虑灾难恢复。

(2) 逻辑环境的检查。主要检查信息系统对防杀病毒的措施；信息系统对外界的网络攻击屏障。

(3) 硬件基础设施的检查。主要检查硬件的配置对业务的支持程度和硬件的采购是否合规。

(4) 软件设施的检查。主要检查软件采购的效益性和合规性；软件的配置是否符合系统的总体规划；软件的维护和变更情况。

5.2.2　系统访问控制审计

(1) 逻辑访问控制审计。逻辑访问控制是主要的控制措施，审计人员应分析、评价逻辑访问控制在实施组织信息安全目标过程中的有效性，并对信息系统处理设施的技术、管理、安全环境进行了解。具体应做到以下几点。

① 验证逻辑访问路径。审计人员应验证所有可能的访问路径已被正确识别，并采取了有效的控制措施。

② 检查逻辑访问控制软件。在信息系统所有架构层面上都应实施有效的访问控制措施。

③ 检查身份识别与验证。检查账号、口令。

④ 检查逻辑访问授权。检查系统是否能识别并区别出不同类型的用户，且按级别进行了正确的授权。

⑤ 检查远程访问控制。对远程访问和移动设备的管理进行检查。

(2) 利用审计日志检测系统访问。

(3) 物理访问控制审计。到现场实地察看对敏感区域、敏感文件的物理访问控制,以确保只有经授权的人才能访问,如门锁、日志、监控、警报等。

5.2.3 系统网络架构控制审计

(1) 局域网风险与控制审计。对局域网进行全面了解的基础上,检查局域网软件与访问控制管理。

(2) 客户机/服务器架构安全审计。检查访问节点及其相互间的关系,确保任何路径都不存在暴露风险,同时检查客户机/服务器架构控制措施的有效性。

(3) 互联网安全控制审计。了解风险及安全因素,检查是否采取了必要的安全控制措施。

(4) 网络安全技术应用的审计。包括网络防火墙、入侵检测系统、加密技术与网络安全协议、虚拟私有网络、防病毒技术等。

(5) 网络基础架构审计。主要包括:

① 审核网络拓扑图,确定网络结构及设施。

② 审核对局域网的控制,保证体系结构的设计和选择遵循了适当的标准,以及获取和运行成本不超过其效益,包括:物理控制审核、环境控制审核、逻辑控制审核。

③ 远程访问审核。重点对来自非信任网络环境的授权用户进行的远程访问的安全控制措施进行审核,并检查所有远程访问进入点,测试拨号访问控制。

④ 网络穿透测试。

⑤ 网络变更控制审核。

5.2.4 数据安全控制审计

(1) 审核信息系统在数据处理、传输过程中的数据加密、数字签名、数字信封、数字证书认证等安全策略控制是否完整有效,评价系统数据的机密性、完整性和可靠性。

(2) 审核数据库的存取管理、安全管理和数据库加密技术,评价数据库的安全性。

(3) 审核数据库用户的角色、权限管理、身份验证和访问控制等安全控制,评价数据库的安全性。

(4) 审核数据库的备份和恢复策略,检查备份数据存放、安全、维护管理,确保数据库的可用性。

5.2.5 灾难恢复与业务持续性审计

企业必须有完善的信息系统的灾难恢复和业务持续计划来保证发生灾难时,信息系统仍然能够正常运行。具体应该做到以下几点。

(1) 评价被审计单位的业务持续性策略及其与业务目标的符合性、充分性和有效性。

(2) 审核信息系统和终端用户以前所做测试的结果,验证业务持续计划的有效性。

(3) 审核异地应急措施及其内容、安全和环境控制,评估异地存储站点的适当性。

(4) 审核应急措施、员工培训、测试结果,评估信息系统和终端用户在紧急情况下的有效反应能力。

(5) 审核被审计单位对业务持续计划的维护措施。

5.3　一般控制审计案例——社保信息系统审计

5.3.1　案例摘要

在社保信息系统审计项目中，审计人员从一般控制到应用控制进行了全面审计，本案例涉及的一般控制审计事项名称及所属审计事项类别如表 5-3 所示。

表 5-3　审计事项列表

审计事项类别	审计事项子类	审计事项名称	审计事项编码
一般控制审计（GC）	总体 IT 控制环境审计	IT 规划及组织结构审计	GC-1
		IT 管理政策审计	GC-3
	基础设施控制审计	机房物理环境控制审计	GC-4
	信息系统生命周期控制审计	系统开发和变更控制审计	GC-7
	信息安全控制审计	逻辑访问控制审计	GC-10
		网络安全控制审计	GC-11
		操作系统和数据库系统安全控制审计	GC-12
	信息系统运营维护控制审计	系统操作管理控制审计	GC-15
		系统变更管理控制审计	GC-16
		系统灾难恢复控制审计	GC-17

5.3.2　审计技术方法

（1）问卷调查法。审计人员设计调查问卷，从组织管理情况、数据资源管理、系统环境安全管理、系统运行管理等几个方面进行审计调查，通过分析问卷反馈信息，总体把握信息系统一般控制和应用控制的基本情况。

（2）业务流程图法。审计人员详细了解社保业务办理流程和系统数据流程，绘制相应的业务流程图与数据流程图，便于熟悉信息系统构架和各业务表之间的关联关系。

（3）人员访谈法。审计人员针对信息系统的各控制点，对相关部门人员进行访谈，了解信息系统的使用情况，从不同的层面发现存在的信息系统问题。

（4）现场观察法。审计人员对被审计单位的机房等地进行现场观察和实地了解，掌握被审计单位计算机机房的建设和管理情况，发现被审计单位在机房管理方面存在的不足；审计人员现场观察业务人员实际办理社保业务时，使用系统进行操作的情况，从而直观了解系统功能是否满足业务需求，发现系统存在的问题。

（5）资料查阅法。审计人员通过查阅被审计单位信息化建设相关的文档资料，详细了解了被审计单位的信息化规划和建设情况；通过查阅社保系统的软件开发文档和使用手册等资料，了解该信息系统的业务需求、主要功能和业务流程等。

（6）工具检测法。审计人员利用软硬件工具对被审计单位的主要服务器和主机等设备进行扫描检测，收集并分析技术数据，发现其操作系统和数据库系统存在的安全隐患。

（7）测试用例法。审计人员通过编写相应的用户测试用例，对系统访问控制及信息系统的输入、处理、输出控制进行实质性测试，检查系统安全可靠程度及信息系统功能对用户

需求的满足程度，测试信息系统处理数据的正确性和真实性。

（8）程序代码检查法。审计人员获取系统核心业务程序代码，结合相关政策进行检查，发现系统数据处理逻辑方面存在的问题。

（9）平行模拟法。审计人员对信息系统的后台数据，编写 SQL 语句，模拟系统的业务处理逻辑进行分析处理，将计算的结果与实际结果比照，提取疑点，进行延伸，发现系统处理逻辑方面的问题及利用系统进行违法违规业务操作的问题。

（10）综合测试法。审计人员在被审计单位的测试系统中建立一个虚拟实体，由系统处理该虚拟实体的测试数据，将处理结果同预期结果进行比较，确定该系统的处理控制是否恰当、可靠。

5.3.3 审计发现和建议

1. 审计发现

审计发现社保信息系统的一般控制总体情况较好，机房设施配置基本齐备，性能良好，系统总体运营情况良好，功能基本满足业务需求，但还存在以下问题。

（1）组织管理存在风险。每个子系统均由同一人负责数据库维护和应用系统的开发、测试、运行维护等工作，岗位职责不分离，关键性业务缺乏后备人员，这种管理模式有潜在风险。

（2）系统安全存在漏洞。机房物理环境不符合规范要求，网络系统缺少入侵检测、漏洞扫描、业务审计等网络安全措施，信息安全存在隐患。主服务器等设备的操作系统和数据库系统存在漏洞。

（3）无灾难恢复计划与方案，没有进行灾难恢复测试。

（4）系统开发和变更缺乏过程控制；部分系统变更无测试，系统变更后文档资料没有及时更新。

2. 审计建议

针对以上问题，审计组提出了纠正和改进建议。

（1）建议该单位加强职责分离控制，加强培训，对关键技术岗位配备后备人员。

（2）建议该单位尽快更换老化和超负荷运载设备、规范机房环境控制，加强网络安全措施，排除安全隐患。

（3）建议该单位建立完善而可行的灾难恢复方案，并定期进行恢复测试，记录并分析测试结果。

（4）建议该单位加强系统开发变更过程控制，补齐系统开发及变更资料；加强系统变更测试，及时更新系统变更后文档资料。

5.3.4 被审计单位信息系统一般控制情况

在一般控制方面，主要建立和完善了组织管理、机房物理环境、网络安全、服务器及数据库、软件开发变更等方面的制度控制及管理机制。社保信息系统一般控制情况如图 5-3 所示。

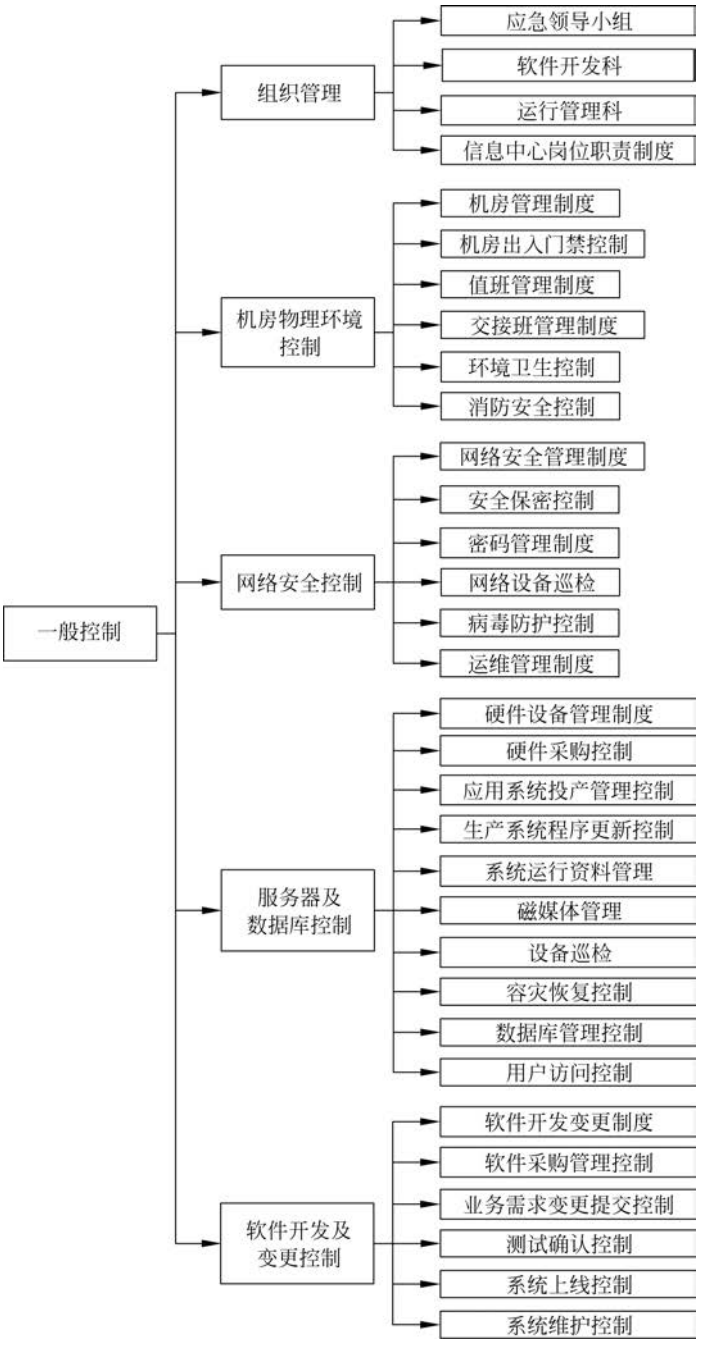

图 5-3　被审计单位社保信息系统一般控制

5.3.5　一般控制审计重点内容及审计事项

1. IT 规划及组织结构审计

1）具体审计目标

检查被审计单位 IT 规划情况和 IT 组织结构情况，有无符合其业务需求和信息需求的

长远发展规划和执行计划，组织流程和组织架构是否满足控制要求，岗位分工和职责划分是否合理合规。

2）审计测试过程

（1）要求被审计单位提供信息系统规划文档、IT 组织结构图、重要岗位的职能和业务流程等资料。

（2）对信息中心发放“组织管理控制调查表”（表 5-4）和“数据资源管理的控制调查表”（表 5-5），并对被审计单位填写的内容逐一核对、落实。

表 5-4 组织管理控制调查表

序号	控制措施调查问题	是	否	不适用	备注
1	是否成立了专门的组织机构对信息系统进行管理	√			信息中心
2	是否对未来几年信息化建设有统一的规划	√			
3	是否成立网络安全领导小组，对计算机信息系统网络安全和信息使用工作进行统一领导	√			
4	是否制定了职责分离的规章制度	√			
5	业务人员的工作职责明确清晰	√			
6	信息技术部门只负责信息系统的开发和维护工作，日常的业务操作只能由相关业务部门的工作人员来进行	√			
7	是否有规范的数据备份和恢复程序步骤	√			
8	系统的输入人员与复核人员不能相互兼任	√			
9	业务操作人员不能保管除操作手册以外的系统技术文档	√			
10	业务操作人员不能管理系统产生的重要的业务档案	√			
11	聘用人员与工作岗位是否相符	√			
12	对因工作需要接触秘密数据的工作人员签订保密协议书	√			
13	对关键性业务配备了后备人员		√		
14	定期对工作人员的工作进行考核	√			
15	定期对信息系统人员进行培训	√			
16	关键技术有多人掌握		√		
17	人员离岗后，信息系统中的账号和口令及时删除	√			
18	人员离岗后，及时归还所有的报告、文档和书籍	√			

表 5-5 数据资源管理的控制调查表

序号	控制措施调查问题	是	否	不适用	备注
1	定期备份重要的数据	√			实物
2	在对数据资源进行重要的处理之前，对数据进行备份	√			计算机使用管理规定
3	备份的数据异地存放	√			实物
4	备份的数据由非技术人员的专人保管		√		
5	信息技术人员未经批准不能接触备份数据			√	

续表

序号	控制措施调查问题	是	否	不适用	备注
6	数据库备份和恢复工作需要在有监督的情况下进行	√			计算机使用管理规定
7	系统的维护工作需要在有监督的情况下进行	√			计算机使用管理规定
8	由专人负责重要数据的备份和恢复工作	√			计算机使用管理规定
9	备份数据的存放和领用要有相应的记录	√			
10	需要授权才能领取备份的数据	√			专人负责
11	对备份或恢复工作日志进行了记录		√		
12	明文规定了数据备份和恢复工作的规范步骤		√		
13	备份数据的恢复工作需要得到批准	√			专人负责
14	对系统的操作人员实施密码控制，防止无关人员使用系统	√			计算机使用管理规定
15	业务报告或报表要经过批准才能产生	√			系统内已设定权限
16	对系统的操作人员实施权限控制，保证不同权限的人员只能操作权限规定的功能或只能访问权限规定的数据	√			系统实际应用
17	对操作人员的管理建立日志，记录有关操作人员的增加、删除及对操作人员的口令或权限的更改的详细情况		√		
18	对操作人员的工作建立审计日志，记录进入系统工作的人员、时间、调用的功能模块、访问的数据、所做的操作等情况		√		
19	操作人员未经批准不能擅自复制数据	√			计算机使用管理规定
20	对高度敏感的数据以加密的方式存储和传输			√	
21	存放数据的房间能够防潮、恒温、防毒和防止强磁场干扰	√			
22	定期检查并记录存放数据的介质是否存在故障		√		

3）审计发现问题和思考

（1）岗位职责分离方面存在漏洞。审计发现该单位没有按照职责分工为系统设置相应的管理岗位，每个子系统均由一人既负责数据库维护，又负责软件系统的开发、测试、运行维护等工作，存在舞弊行为的潜在风险。

（2）关键性业务缺乏后备人员。某些关键技术仅依赖一到两个核心人员，人员离、缺岗将影响业务正常进行。

2. IT 管理政策审计

1）具体审计目标

检查被审计单位 IT 管理政策情况，是否制定了完善可行的 IT 管理政策，政策执行是

否顺利。

2）审计测试过程

（1）要求被审计单位提供机房管理制度、人员管理制度等IT相关管理政策。查阅被审计单位提供的“机房管理制度”“人员管理制度”“软硬件管理制度”“网络安全制度”“保密制度”等，检查其管理政策是否完善合理、有效可行。

（2）走访信息中心和业务部门的部分员工，询问他们对于上述政策制度的了解程度，现场观察员工的操作是否符合管理制度。

3）审计发现问题和建议

在IT管理政策方面控制较为严格，各项管理政策比较完善合理，员工执行情况良好。

3. 机房物理环境控制审计

1）具体审计目标

检查被审计单位基础设置控制情况，重点审查其机房物理环境的安全控制措施是否健全，能否保证信息系统的软硬件和数据资源受到妥善保护，能否保证信息系统能够持续正常地运行。

2）审计测试过程

（1）发放“机房物理环境控制调查表”（表5-6），并对其填写的内容逐一核实。

表5-6 机房物理环境控制调查表

序号	控制措施调查问题	是	否	不适用	备注
1	计算机房或数据存放中心应远离加油站、储气站、蓄水池	√			实际情况
2	机房安装温、湿度环境传感器		√		
3	计算机房制定了防止火灾、水灾、防尘和防潮的规章制度	√			机房管理规定
4	计算机房或数据存放的房间配备了干粉灭火器	√			气体
5	计算机房或数据存放的房间设置了火灾警探测器和水灾探测器	√			实物
6	计算机房或数据存放的房间设置了火灾警报和水灾警报	√			
7	定期对计算机房空气进行净化处理		√		
8	计算机房具有防潮和恒温设备	√			实物
9	计算机房配置了备用电源或独立的备份供电	√			实物
10	计算机房配置了电源稳压装置	√			实物
11	计算机设备的电源与空调、照明和其他动力用电的电源相互独立	√			实物
12	制定了人员出入机房的制度	√			机房管理规定与登记表
13	机房和数据存放地设置了门禁系统和门卫	√			
14	人员出入机房和数据存放地时使用门禁卡并进行登记	√			

续表

序号	控制措施调查问题	是	否	不适用	备注
15	安装了闭路电视或成像系统等监视装置	√			
16	安装了自动报警系统		√		
17	重要的设备使用了电磁屏蔽，防止重要数据通过电磁辐射泄漏	√			
18	重要数据的备份由专人负责存放	√			

（2）审计人员亲临现场对机房进行实地观察，以确认各项机房物理环境控制的有效性。

（3）对机房管理人员访谈，详细调查了解部分机房设备不能满足系统运行需要的实际情况并分析原因。

3）审计发现问题和建议

（1）机房内未安装温、湿度环境传感器；空调设备老化，功率较低，不能满足机房温、湿度控制需要；机房监控未安装自动报警系统。

（2）专用配电柜较小，已不能满足配电需要，部分电源空气开关安装在配电柜外；机房门禁未采用 UPS 供电；UPS 单机运行，负载已达 76%；UPS 电池组满载供电延时时间仅为半小时。

（3）没有办公楼综合布线图、测试报告；存在线槽外走线且强、弱电未完全分开现象。

4. 系统开发和变更控制审计

1）具体审计目标

检查被审计单位在系统开发过程中，对系统分析、系统设计和系统实施过程所进行的控制措施情况，能否保证信息系统的质量及安全可靠性；确定系统开发的各个阶段是否都经过严格审核与批准；确认系统文档是否准确完整；确认系统实施之前是否经过全面测试，而不存在重大错误和舞弊。

2）审计测试过程

（1）与管理人员、业务人员、软件开发人员座谈进行询问，了解系统开发和变更的流程、授权控制情况和质量控制情况。

（2）要求被审计单位提供可行性研究报告、项目开发计划、软件需求规格说明书、数据需求规格说明书或数据表 E-R 模型图、概要设计说明书或程序设计说明书、详细设计说明书或模块设计说明书、测试计划、测试分析报告、开发进度月报、项目开发总结报告、维护修改日志或软件开发变更说明、操作手册或用户使用手册等。被审计单位仅提供了可行性研究报告、项目开发计划、软件需求规格说明书、数据需求规格说明书、概要设计说明书、详细设计说明书、开发进度月报、项目开发总结报告、操作手册。审计人员审阅所提交的系统文档。

3）审计发现问题和建议

开发文档不齐全、不系统，缺少数据流图、数据库 E-R 模型图、系统测试计划、测试分析报告、系统开发变更的说明文档。

5. 逻辑访问控制审计

1）审计具体目标

检查被审计单位在逻辑访问控制方面的措施是否完善可行，能否有效地保证系统软件

和数据的安全。

2）审计测试过程

（1）检查系统管理人员的权限是否清晰，不同人员访问和修改不同的数据；当人员离职、终止工作或调离工作岗位时，其账户密码是否及时废除；使用系统的人员口令是否合乎规范，是否定期更换。

（2）检查系统操作日志，从而发现逻辑访问控制方面的违规行为。

3）审计发现问题和建议

（1）操作人员对系统的操作没有日志记录。

（2）未修改 Oracle 数据库账号默认密码，非授权人员可利用账号默认密码进入数据库操控数据。

（3）数据库管理员及软件开发人员混合使用账号操作 Oracle 生产数据库，未按岗位职责设置账号。

6. 网络安全控制审计

1）审计具体目标

检查被审计单位的网络安全控制措施是否健全有效，确定能否保证信息资产的安全。

2）审计测试过程

（1）对网络运行专管员进行访谈，了解网络系统运转情况的日常监督情况、网络设备实施、配置情况等。

（2）获取该单位“生产中心拓扑图”，通过对拓扑图分析，检查网络拓扑结构是否满足业务需求和工作流程的需要；审阅办公楼综合布线测试报告和综合布线验收意见；取得 VLAN 划分列表，对照该单位各部门的分布，分析 VLAN 划分的合理性、有效性；现场观察是否配备了网络防火墙、入侵检测、安全审计、漏洞扫描、网络管理等。

（3）设计“网络安全审计部分测试用例”（表 5-7）对防火墙情况进行实质性测试。

表 5-7 网络安全审计部分测试用例

类别	子类	要求内容	检测方法		是否合格
			检测操作步骤	判定条件	
防火墙	日志配置	配置防火墙规则，记录防火墙拒绝和丢弃报文的日志	查看是否配置了对防火墙拒绝和丢弃报文的日志记录	应已开启	否
防火墙	日志配置	配置记录防火墙管理员操作日志，如管理员登录，修改管理员组操作、账号解锁等信息。配置防火墙将相关的操作日志送往操作日志审计系统或者其他相关的安全管控系统	（1）查看是否配置记录防火墙管理员操作日志。 （2）查看是否配置将相关的操作日志送往操作日志审计系统或者其他相关的安全管控系统	（1）应已开启防火墙管理员操作日志记录功能，如管理员登录，修改管理员组操作、账号解锁等信息。 （2）如有操作日志审计系统或者其他相关的安全管控系统，应配置发送相关的操作日志	否

续表

类别	子类	要求内容	检测方法		是否合格
			检测操作步骤	判定条件	
防火墙	告警配置	配置告警功能，报告对防火墙本身的攻击或者防火墙的系统内部错误	查看是否配置告警功能，报告对防火墙本身的攻击或者防火墙的系统内部错误	应已开启	是
防火墙	告警配置	配置告警功能，报告网络流量中对 TCP/IP 网络层异常报文攻击的相关告警	查看设备是否启用报告网络流量中对 TCP/IP 网络层异常报文攻击的相关告警检测	应已开启	是
防火墙	安全策略配置	防火墙在配置访问规则列表时，最后一条必须是拒绝一切策略	查看设备策略列表，检查最后一条是否为拒绝一切策略	在策略列表最后一项应为拒绝一切策略	是
防火墙	安全策略配置	配置 NAT 地址转换，对互联网隐藏内网主机的实际地址	从外网使用 NAT 地址访问内网主机	在外网使用 NAT 地址能正常访问提供服务的内网主机	是
防火墙	攻击防护配置	配置访问控制规则，拒绝对防火墙保护的系统中常见漏洞所对应端口或者服务的访问	检查设备策略设置，检查是否有对常见漏洞端口进行访问控制	常见漏洞端口应在策略设置上设置禁止访问	是
防火墙	其他	对防火墙的管理地址做源地址限制	检查设备管理地址设置	应已设置	是

3）审计发现问题和建议

没有建立全面、有效的信息系统安全防范体系，安全方案中无防火墙设置方式及控制策略，防火墙无操作日志，网络系统缺少入侵检测、漏洞扫描、业务审计等网络安全措施。

7. 操作系统和数据库系统安全控制审计

1）审计具体目标

检查被审计单位重要主机和服务器的操作系统和数据库系统安全控制措施，能够有效保证操作系统和数据库系统不受软硬件失灵、软件差错、人为故障和病毒侵蚀等因素干扰，是否有重大漏洞，是否能保证数据安全。

2）审计测试过程

（1）针对操作系统和数据库系统安全控制点，审计人员设计了“主机及操作系统安全审计测试用例”（表 5-8）和“Oracle 数据库测试用例”（略），进行实质性测试，评估操作系统和数据库系统安全控制情况。

（2）审计人员利用 X-SCAN 等工具软件对该单位 10 台主服务器等关键设备的端口、文件系统等进行了安全性扫描，依据 ISACA“信息资产保护”中关于逻辑访问风险与控制的有关规定，对扫描检测数据进行综合性分析。

表 5-8 主机及操作系统安全审计测试用例

子类	要求内容	检测方法		是否合格
		检测操作步骤	判定条件	
账号	按照用户分配账号。根据系统的要求，设定不同的账户和账户组、管理员用户、数据库用户、审计用户、来宾用户等	进入“控制面板”→“管理工具”→“计算机管理”，在“系统工具”→“本地用户和组”查看根据系统的要求，设定不同的账户和账户组、管理员用户、数据库用户、审计用户、来宾用户	结合要求和实际业务情况判断符合要求，根据系统的要求，设定不同的账户和账户组、管理员用户、数据库用户、审计用户、来宾用户	是
口令	最短密码长度为 6 个字符，启用本机组策略中密码必须符合复杂性要求的策略。即密码至少包含以下四种类别的字符中的三种： • 英语大写字母 A，B，C，…，Z • 英语小写字母 a，b，c，…，z • 西方阿拉伯数字 0，1，2，…，9 • 非字母数字字符，如标点符号，@，#，$，%，&，* 等	进入“控制面板”→“管理工具”→“本地安全策略”，在“账户策略”→“密码策略”查看是否“密码必须符合复杂性要求”，选择“已启动”	“密码必须符合复杂性要求”选择“已启动”	是
口令	对于采用静态口令认证技术的设备，账户口令的生存期不长于 90 天	进入“控制面板”→“管理工具”→“本地安全策略”，在“账户策略”→“密码策略”查看是否“密码最长存留期”设置为“90 天”	“密码最长存留期”设置为“90 天”	是
口令	对于采用静态口令认证技术的设备，应配置当用户连续认证失败次数超过 6 次（不含 6 次），锁定该用户使用的账号	进入“控制面板”→“管理工具”→“本地安全策略”，在“账户策略”→“账户锁定策略”查看是否“账户锁定阈值”设置为小于或等于 6 次	“账户锁定阈值”设置为小于或等于 6 次	是
授权	在本地安全设置中从远端系统强制关机只指派给 Administrators 组	进入“控制面板”→“管理工具”→“本地安全策略”，在“本地策略”→“用户权利指派”查看是否“从远端系统强制关机”设置为“只指派给 Administrators 组”	“从远端系统强制关机”设置为“只指派给 Administrtors 组”	是
授权	在本地安全设置中关闭系统仅指派给 Administrators 组	进入“控制面板”→“管理工具”→“本地安全策略”，在“本地策略”→“用户权利指派”查看“关闭系统”设置为“只指派给 Administrators 组”	“关闭系统”设置为“只指派给 Administrators 组”	是

续表

子类	要求内容	检测方法		是否合格
		检测操作步骤	判定条件	
授权	在本地安全设置中配置指定授权用户允许本地登录此计算机	进入“控制面板”→“管理工具”→“本地安全策略”，在“本地策略”→“用户权利指派”查看是否“从本地登录此计算机”设置为“指定授权用户”	“从本地登录此计算机”设置为“指定授权用户”	是
授权	在组策略中只允许授权账号从网络访问(包括网络共享等，但不包括终端服务)此计算机	进入“控制面板”→“管理工具”→“本地安全策略”，在“本地策略”→“用户权利指派”查看是否“从网络访问此计算机”设置为“指定授权用户”	“从网络访问此计算机”设置为“指定授权用户”	是
日志配置操作	设备应配置日志功能，对用户登录进行记录，记录内容包括用户登录使用的账号，登录是否成功，登录时间，以及远程登录时用户使用的 IP 地址	进入“开始”→“运行”→“控制面板”→“管理工具”→“本地安全策略”→“审核策略”审核登录事件，双击，查看是否设置为成功和失败都审核	审核登录事件，设置为成功和失败都审核	是
设备其他配置操作	安装防病毒软件，并及时更新	进入“控制面板”→“添加或删除程序”检查是否安装防病毒软件。打开防病毒软件控制面板，查看病毒库更新日期	已安装防病毒软件，病毒库更新时间不早于 1 个月，各系统病毒库升级时间要求参见各系统相关规定	是
设备其他配置操作	列出所需要服务的列表(包括所需的系统服务)，不在此列表的服务需关闭	进入“控制面板”→“管理工具”→“计算机管理”，进入“服务和应用程序”查看所有服务，不在此列表的服务是否已关闭	系统管理员应出具系统所必要的服务列表。 查看所有服务，不在此列表的服务需关闭	是

3) 审计发现问题和建议

(1) 对该单位 10 台主服务器进行隐患扫描，发现操作系统和数据库系统漏洞 18 个、警告 64 个、提示 442 个。操作系统和数据库系统的补丁没有及时打上，不必要的端口地址没有封死，易被人利用对系统实施攻击。

(2) 未修改 Oracle 数据库账号的默认密码，非授权人员可利用上述账号进入数据库操控数据；没有开启数据库审计功能，无法记录和跟踪对数据库的操作。

8. 系统变更控制审计

1) 审计具体目标

检查系统变更控制机制，是否存在未经授权擅自变更系统的问题。

2）审计测试过程

（1）审查系统变更流程，是否存在未经授权擅自变更系统的风险。

（2）抽查系统变更申请单，查看主管部门的授权签名，检查是否存在未经授权而变更系统的情况。

（3）检查系统变更测试文档，确认系统变更是否经过严格的测试；检查文档资料，确认系统变更后相关的文档资料是否及时更新。

3）审计发现问题和建议

系统变更流程相对较为严密，审批和验收手续完善，但系统变更测试不严格，部分系统变更无测试，系统变更后文档资料未及时更新。建议加强系统变更测试，系统变更后文档资料及时更新。

9. 系统灾难恢复控制审计

1）审计具体目标

检查被审计单位是否有完整的灾难恢复计划和方案，审核灾难恢复的流程和步骤，能够保证在信息系统受到灾难性毁损后，迅速恢复系统，并使损失降至最低。

2）审计测试过程

（1）发放调查问卷“数据资源管理的控制调查表”（表 5-9），并对被审计单位填写的内容逐一核对、落实。

表 5-9 数据资源管理的控制调查表

序号	控制措施调查问题	是	否	不适用	备注
1	定期备份重要的数据	√			实物
2	在对数据资源进行重要的处理之前，对数据进行备份	√			计算机使用管理规定（暂行无文号）
3	备份的数据异地存放	√			实物
4	备份的数据由非技术人员的专人保管		√		
5	信息技术人员未经批准不能接触备份数据			√	
6	数据库备份和恢复工作需要在有监督的情况下进行	√			计算机使用管理规定（暂行无文号）
7	系统的维护工作需要在有监督的情况下进行	√			计算机使用管理规定（暂行无文号）
8	由专人负责重要数据的备份和恢复工作	√			计算机使用管理规定（暂行无文号）
9	备份数据的存放和领用要有相应的记录		√		
10	需要授权才能领取备份的数据	√			专人负责
11	对备份或恢复工作日志进行了记录		√		
12	明文规定了数据备份和恢复工作的规范步骤		√		
13	备份数据的恢复工作需要得到批准	√			专人负责

续表

序号	控制措施调查问题	是	否	不适用	备注
14	对系统的操作人员实施密码控制，防止无关人员使用系统	√			计算机使用管理规定（暂行无文号）
15	业务报告或报表要经过批准才能产生	√			系统内已设定权限
16	对系统的操作人员实施权限控制，保证不同权限的人员只能操作权限规定的功能或只能访问权限规定的数据	√			系统实际应用
17	对操作人员的管理建立日志，记录有关操作人员的增加、删除及对操作人员的口令或权限的更改的详细情况			√	
18	对操作人员的工作建立审计日志，记录进入系统工作的人员、时间、调用的功能模块、访问的数据、所做的操作等情况	√			系统有记录
19	操作人员未经批准不能擅自复制数据	√			计算机使用管理规定（暂行无文号）
20	对高度敏感的数据以加密的方式存储和传输			√	
21	存放数据的房间能够防潮、恒温、防毒和防止强磁场干扰		√		
22	定期检查并记录存放数据的介质是否存在故障		√		

（2）审阅灾难恢复计划和操作手册，确认其是否为最新的计划和操作手册，检查所制定的灾难恢复计划是否为处理受灾的现实解决方案。

（3）查看备份现场，评估现场的安排是否恰当；检查异地备份情况。

（4）对有关人员进行访谈，检查灾难恢复小组成员是否为在职人员，分担的职责是否恰当；询问灾难恢复人员是否熟悉灾难恢复流程和步骤。

（5）检查关键数据文件是否依据灾难恢复计划进行备份；检查灾难恢复计划的测试文档，确认是否经过灾难恢复测试，测试结果是否达到预期目标。

3）审计发现问题和建议

（1）审计发现没有制定灾难恢复计划规范的测试流程和计划。

（2）没有实施灾难恢复测试的情况说明和分析，没有发生故障后应急预案和处理流程，无法确定 BCP 的有效性。

小　　结

（1）信息系统内部控制是一个单位在信息系统环境下，为了保证业务活动有效进行，保护资产的安全与完整，防止、发现、纠正错误与舞弊，合理确保信息系统提供信息的真实、合

法、完整，而制定和实施的一系列政策与程序措施。

（2）信息系统内部控制审计是对信息系统各项内部控制措施的健全性和有效性进行审查和评价。只有健全有效的内部控制，才能确保信息系统安全、可靠和有效运行。

（3）信息系统内部控制分为一般控制和应用控制。

（4）信息系统一般控制是指对整个计算机信息系统及环境要素实施的，对系统所有的应用或功能模块具有普遍影响的控制措施。

（5）信息系统安全审计就是对被审计单位的信息系统安全控制体系进行全面审查与评价，确认其是否健全有效，确保信息系统安全运行。

（6）业务持续计划（BCP）是组织为避免关键业务功能中断，减少业务风险而建立的一个控制过程。

复习思考题

一、单选题

1. 下面哪位对有效的业务连续和灾难恢复控制负有根本责任？（　　）

A. 股东　　B. 安全管理员　　C. 网络管理员　　D. 执行官

2. 授权最主要的特性是（　　）。

A. 按照最小权利的原则授予资源访问的权限

B. 用户提供用户名和口令

C. 授予用户的用户名和口令

D. 证明用户被授权

3. 拒绝服务攻击损害了下列哪种信息安全的特征？（　　）

A. 完整性　　B. 可用性　　C. 机密性　　D. 可靠性

4. 采取热站异地处理设备的特点是（　　）。

A. 高的实施和维护成本　　B. 减少恢复时间

C. 减少灾难准备成本　　D. A 和 B

5. 某企业欲处置若干曾用于保存机密数据的计算机，该企业应首先（　　）。

A. 将硬盘消磁　　B. 低级格式化硬盘

C. 删除硬盘所有数据　　D. 对硬盘进行碎片处理

6. 下面哪种控制最有效地保护软件和敏感数据的访问？（　　）

A. 安全政策

B. 物理控制对服务器房间的访问

C. 对整个系统和数据冗余的容忍度

D. 对操作系统、应用数据的逻辑访问控制

7. 对于所有的计算机系统来说，存在的最大威胁是（　　）。

A. 没有经过培训和粗心大意的人　　B. 供应商和承包商

C. 黑客或解密高手　　D. 员工

8. 下面哪条措施不能防止数据泄露？（　　）

A. 数据冗余　　B. 数据加密　　C. 访问控制　　D. 密码系统

二、填空题

1. 信息系统的内部控制分为_____和_____。

2. _____控制重点是信息系统环境及信息系统软硬件的采购、配置、运行与管理。

3. 信息系统访问控制可以分为_____和_____。

4. 信息系统访问控制应当建立在“知所必需”的基础上，按照_____和_____来分配系统访问权限，只对必须使用资源的人进行必要的授权。

5. _____是指遵循不相容职责相分离的原则，实现合理的组织分工。

6. _____是指自然或人为灾害后，重新启用信息系统的数据、硬件及软件设备，恢复正常商业运作的过程。

三、简答题

1. 信息系统一般控制包括哪些内容？

2. 信息系统面临的威胁有哪些？

3. 信息系统安全审计的定义是什么？

4. 一般控制审计程序包括哪些内容？

5. 什么是业务持续计划？什么是灾难恢复计划？