第3章

信息系统一般控制及审计

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控制技术的应用，通过案例介绍信息系统审计人员如何对一般控制的检查，能采用合适的方法、合理的技术手段针对被审计组织信息系统的基础设施、访问方法、网络服务、数据保护以及灾难恢复等方面的控制进行检查，以达到从事信息系统审计的主要目的。

3.1 信息系统一般控制概述

信息系统内部控制是一个单位在信息系统环境下，为了保证业务活动的有效进行，保护资产的安全与完整，防止、发现、纠正错误与舞弊，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。它是规范秩序、防范风险、遏制腐败、合理确保信息系统功效的有效途径，从而更好地确保组织目标的实现。凡是与信息系统的建立、运行维护、管理和业务处理有关的部门、人员和活动，都属于信息系统内部控制的对象。信息系统内部控制分为一般控制和应用控制。

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、保护计算机应用程序、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一个重要因素，它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，将会严重地削弱相关的具体应用控制的可靠性。由此，对一般控制的评价通常在应用控制评价之前进行。对一般控制的测评内容包括单位整体范围安全计划和管理、访问控制、应用软件开发和变更控制、系统软件控制、职能分离控制、服务持续性控制。

信息系统应用控制是用于对具体应用系统的控制，一个应用系统一般由多个相关计算机程序组成，有些应用系统可能是复杂的综合系统，牵涉到多个计算机程序和组织单元，与此相应，应用控制包括包含在计算机编码中的日常控制及与用户活动相关的政策和流程。对信息系统应用控制的测评内容包括各项业务的授权控制、完整性控制、准确性控制。

良好的一般控制是应用控制的基础，可以为应用控制的有效性提供有力的保障，某些应用控制的有效性取决于计算机整体环境控制的有效性。当计算机整体环境控制薄弱时，应用控制就无法真正提供合理保障。如果一般控制审计结果很差，应用控制审计就没有进行的必要。

3.2　管理控制及其审计

3.2.1　管理控制的基本内容

信息安全管理是指导组织的安全实践活动，它从管理、技术、人员、过程的角度来定义、建立、实施信息安全管理体系，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，通过在安全方针策略、组织安全、资产分类与控制、人员安全、物理与环境安全、通信与运营安全、访问控制、系统开发与维护、业务持续性管理、符合法律法规要求等领域内建立管理控制措施，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控制的主要目标是实现职责分离和人员的管理。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，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，所以在信息系统环境中，职责分离原则在业务处理层次被削弱，因此信息系统需要从组织结构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。信息系统中的职责分离主要包括系统的开发职务和操作职务，系统的输入职务和审核职务以及系统操作职务和文档管理职务之间的职责分离。信息技术部门应只负责信息系统的开发和维护工作，而日常的业务操作只能由相关业务部门的工作人员来进行，企业内部的日常业务操作不能由信息技术部门的人员来完成，信息技术人员未经批准也不能接触备份的数据，不能进行数据库备份和恢复的工作；信息系统的数据录入人员和复核记账人员不能互相兼任；业务操作人员不能接触除操作手册以外的系统技术文档，也不能管理系统产生的重要业务档案。

信息系统组织管理控制的另一个重点是人员管理的控制，信息系统的运行与人密切相关，一个有效和可靠的系统，人在系统开发、运行和维护中起到至关重要的作用，同时在计算机舞弊和犯罪事件中，人也扮演主要角色，信息系统人员管理的控制对象是人员及其工作的整个过程，包括人员的招聘、工作的分配、培训、离岗和离职等。

3.2.2　管理控制审计

在信息安全实践中，对信息安全管理框架进行审计与评价是一项基本的工作。具体包括：

1. 审计书面策略、流程与标准

信息系统审计师应该先检查这些策略及程序，以决定公司是否建立了正确的安全方针，是否为安全的计算机处理环境建立明确的责任归属和操作程序。

2. 审计逻辑访问安全策略

此策略应当为逻辑访问建立“知所必需”的原则，并合理评估在访问过程中暴露的风险。

3. 审计安全意识的培训

提倡及宣传安全意识是一种预防性的控制方法。通过这种方法，使员工意识到他们维护良好物理和逻辑安全的责任。这也可以被视为一种检测性控制，因为它鼓励员工举报违反安全规定的行为。安全培训要从新员工的入职教育开始，并通过公司的刊物、公告、安全人员的检查及部门会议中强调等一系列活动来进行经常性的安全宣传。应当由安全管理员直接负责安全意识教育的管理及执行，信息系统审计师应抽查公司员工以评估员工的计算机安全意识状况。

4. 审查数据所有权、数据所有人和数据使用者

数据的所有权指在信息资源适当分类的基础上，对保护信息资源机密性、完整性、准确性方面的责任分配。建立数据的所有权的关键点是针对特定员工赋予保管计算机资源的相应责任，并确保这种责任的可追查性。信息系统审计师应检查组织中是否建立了数据所有权关系，并根据所有权向员工落实了具体责任。信息系统审计师在审核数据所有权关系时，应当抽样检查员工的工作描述，以确认其工作职责与所有权关系相一致，同时也应该判断对信息资产的分类是否适当。数据所有人通常是那些对利用信息运营和控制业务活动负有责任的管理人员，他们的安全责任包括对系统访问进行授权；确保人员职责发生变动时，访问规则要及时更新；定期检查访问规则及被保护的计算机数据。数据使用者指最终用户，包括内部和外部用户或用户组。数据使用者要访问计算机数据，必须事先获得数据所有者批准，并由安全管理员监控和管理其使用。用户必须遵守组织制订的安全政策与程序，并对其工作区域中的非授权人员的物理与逻辑访问保持警觉。

5. 审查数据保管员

数据保管员是负责保存并看管计算机数据的人员。一些信息部门人员，如系统分析员和计算机操作人员也有此职责。

6. 审查安全管理员

安全管理员负责为信息系统程序、数据和设备提供充分的物理与逻辑安全。通常组织制定的信息安全策略要对安全管理员工作提供基本的指南。

7. 审查书面授权

数据访问必须先经书面核准与授权。信息系统审计师应该抽样检查这些授权情况，判断授权等级是否充分和合理，是否只有数据所有人才能核准数据访问权限。

8. 审查离职员工的访问控制

一般来说，员工离职的情况主要有请辞、聘用合同期满和非自愿离职 3 种。对于非自愿

离职的员工，组织应当在解除其职务前，及时收回或严格限制其对组织信息资源的访问权，使其不能继续访问组织的机密信息，或使其不能破坏组织有价值的信息资产。如果对于这类员工还需要保留一部分访问权，必须得到相关管理层批准，并对其进行严格的监督。对其他两种离职的员工，由管理层批准是否保留他们的访问权，这取决于每一种人所处的特定的环境、员工所访问的 IT 资产的敏感程度以及组织的信息安全政策、标准和程序的要求。

9. 审查访问标准

信息系统审计师应该审核访问标准，确保其符合组织职责划分的原则，避免错误和舞弊现象的发生，降低非授权访问的风险。安全标准一般包括账号与密码标准、特定机器使用规则、特定应用系统访问规则等。

3.2.3　管理控制测试

控制测试是审计工作中的重要步骤，从系统审计角度来说，测试分为符合性测试和实质性测试，对信息系统一般控制的测试，是检查相关控制的存在性和有效性，属于符合性测试。信息系统审计应当针对一般控制的具体区域，参照风险控制的模型，根据控制矩阵进行控制测试，测试一般可采用检查控制文档、问卷调查、会谈、观察等手段进行，并完成控制测试矩阵，表 3.1 为一个简单的管理控制测试矩阵。

表 3.1　管理控制测试矩阵

序号	控制措施	控制目标		备注
		职责分离	人员管理控制	
1	是否制定了职责分离的规章制度	√	√	
2	业务人员的工作职责明确清晰	√	√	
3	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	√		
4	信息技术人员未经批准不能接触备份的数据，不能在无监督的情况下进行数据备份和恢复的工作	√		
5	系统的输入人员与复核人员不能相互兼任	√		
6	操作人员不能保管除操作手册以外的系统技术文档	√		
7	业务操作人员不能管理系统产生的重要的业务档案	√		
8	聘用人员与工作岗位是否相符		√	
9	对接触秘密数据的工作人员签订保密协议书		√	
10	对关键性业务配备了后备人员		√	
11	定期对工作人员的工作进行考核		√	
12	定期对信息系统人员进行培训		√	
13	关键技术由多人掌握		√	
14	人员离岗后，信息系统中的账号和口令及时删除		√	
15	人员离岗后，及时归还所有的报告、文档和书籍		√	

3.3 系统基础设施控制及其审计

系统基础设施是指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系统基础设施，设计必要的控制措施，以保障信息系统安全、可靠地运行。系统基础设施控制重点是信息系统环境以及信息系统软硬件的采购、配置、运行与管理。

3.3.1 信息系统环境控制

1. 环境风险

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；环境风险还可能来自电力故障、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、电压不稳以及电磁干扰等 4 种情况。

对于信息系统内部控制人员来说，检查环境风险应当着重考虑以下问题：

- 计算机设备电源供应是否能适当控制在设备制造商要求的规格范围内？
- 计算机设备的空调、湿度、通风控制系统是否能维持适当温度和湿度，以符合制造商要求？
- 计算机设备是否提供静电保护（如防静电地毯、抗静电喷雾器）？
- 计算机设备是否能防尘、防烟及其他特殊物品如食品？
- 是否明文规定禁止在计算机设备旁就餐、喝饮料及吸烟？
- 是否对备份磁盘及磁带提供保护措施，使其免受极端温度的损害、磁场的影响、水的侵害？

2. 对环境风险的控制

为了有效控制信息处理设施的环境风险，对于信息处理设施的物理位置需要进行认真的考虑，如为了避免水淹的威胁，计算机机房不可设置在地下室。如果在多层建筑物中，研究表明 3～6 层楼是最佳的计算机机房位置，可降低水灾、烟雾及火灾的危险。当需要放置计算机设施时，对相邻组织的活动要特别注意，比如应当避免把计算机设施放置在化学工厂、机场附近（可能释放有害气体），以免面临环境风险。

针对上述环境风险，通常采用的控制设施和控制技术包括以下内容。

1）安装与使用报警控制面板

根据国家有关法律、法规的要求，信息系统物理环境必须设置报警控制面板，面板安装要与建筑物中的防盗系统或安全系统相分离，但要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，要遵守制造商的温度要求，另外要使用单独的电源或专用电源对其供电，以保障在特殊情况下能正常运行。

2）水灾探测器

水灾探测器被利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。水灾探测器必须设置在高架地板下与排水孔附近。当警报启动时，声响必须足以让安全及控制人员听到。如果水灾探测器放置在衣帽架地板下，必须作记号以便识别及维护。收到报警信息后，必须有专人负责调查其原因并采取适当行动。

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、地板以及天花板必须为防火材料，必须具备阻隔火灾、避免其扩散的功能。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，在信息处理设施中常用办公设施（如垃圾桶、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以及手提式灭火器，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唯一选择，一般被选用的惰性气体有卤代烷（Halon）和七氟丙烷（FM-200）两种，近年来由于前者对大气臭氧层破坏严重而逐渐被禁止使用。

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，比如可以通过浪涌保护器加以保护；持续几秒到30分钟的电力中断可以采取不间断电源（UPS）加以保护；持续几个小时到几天的电力中断可以采用后备发电机供电，发电机可能是移动式或固定式，可以采用多种燃料方式，如柴油、汽油动力发电机。

电源线通常暴露在许多环境的危害下，如水、火、闪电、意外挖断等。为了降低这些事件造成的电力中断的危险，应当具有来自不同电网的备份电力系统。这样，当一套电力系统中断时，不影响到正常的电力供应。

在计算机机房发生火灾或要求紧急疏散时，必须能立即切断计算机及周边设备的电力。应当具备两个紧急断电装置设施，一个在计算机机房内，一个靠近计算机机房，但设置在机房外面。它们必须清楚地标示并且容易使用，但是必须对其进行保护，以防止不恰当的使用或意外的启动。

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），所以必须公开声明禁止，例如入口处贴上警示标语。

紧急疏散计划必须在强调人员的安全的同时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。

3.3.2 信息系统硬件控制与审计

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采购、运行、维护、监控和能力管理等方面。

1. 硬件基础设施采购控制

选择计算机硬件和软件环境，经常需要向软硬件供应商发布一个规格，并制定评估供应商建议的准则。这类规格以招标书（ITT）或者请求建议书（RFP）的形式送达供应商。该规格必须尽可能全面地说明所需设备的用途、任务和要求，并包括对设备所处环境的描述，具体应包括组织的描述、信息系统处理需求、硬件需求、系统软件应用、支持需求、适应性需求、转换需求和约束条件等。

从供应商处采购（获取）软硬件时，应充分考虑各种因素进行评标，可作为参考的有其他用户的推荐书、竞争性出价、根据需求分析投标书、供应商的财务状况、供应商维护和支持（包括培训）的能力、交付日程、软硬件升级能力、性能等。

在硬件采购中通常考虑的技术指标包括运转时间、响应时间、吞吐量、负载、兼容性、容量以及利用率等。

信息系统审计在考虑硬件获取时，要确定该获取过程是否开始于业务需求，其硬件需求是否在规格中体现，确定是否考虑了多个供应商，并根据上述准则对其进行了比较。

2. 硬件基础设施维护与监控

信息系统硬件基础设施必须进行日常清洁和保养以保证其正常运行。维护需求随系统复杂性和运行负载的不同而不同（如处理需求、终端访问以及应用的数量等）。但无论如何，维护计划应最大限度地满足供应商要求的规格。硬件维护程序就是将硬件维护的执行过程形成文件。

在对该维护过程进行审计时，IS 审计师应该确定已形成正式的维护计划并得到管理层的批准，并检查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，或即将到来的硬件变动，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，可考虑的参数和报告有：

1）硬件错误报告

标识出CPU、输入输出、电源和存储故障。IS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。过多的宕机时间意味着不充分的硬件设施、过度的操作系统维护、缺乏预防性维护、不充分的环境设施（如电源和空调）或不充分的操作员培训。

3）利用率报告

这些是系统自动形成的文件，记录了机器和外设的使用情况。软件监视器用于捕获处理器、通道和二级存储介质（如磁盘驱动器）的有效利用状况。一般来说，大型机的平均利用率应在85%～95%之间，偶尔可达到100%或低于70%。IS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%，IS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，和/或调研是否能通过杜绝不必要的处理或将非关键的处理挪至较为空闲的时间（如夜间）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. 硬件基础设施能力管理

能力管理是对计算机资源的计划和监控，其目标是根据总体业务的增长或减少动态地增减资源，以确保可用资源的有效利用。能力计划应由用户和IS管理部门共同参与完成，并至少每年进行审查和修改。

能力计划应包括被以往经验所证实的预测，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。

审计应当清楚上述需求的数量和分布具有固有的灵活性，某一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获知控制的有效性。

审查硬件获取计划可以判断该计划是否定期地与管理层的硬件计划进行比较，了解信息系统环境设施是否足以适应当前安装的硬件，审核硬件获取计划是否和IS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、安装要求以及交货时间等说明的准确性。

通过检查微机（或PC）获取标准可以了解IS管理层是否已经发布了关于微机获取及使用的书面的政策性陈述，而且这些政策已经传达给了用户；检查微机获取标准是否设计了程序和表格以实现获取的批准流程，检查获取微机的请求经过了成本-效益分析，并且检查所有微机均由采购部门集中采购以获得批量折扣或其他优惠。

审查硬件的能力管理程序和性能评估程序可以确定它们是否能保证对硬件和系统软件

的性能和能力进行连续的审查；判断 IS 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。

信息系统审计师还需要审查变更管理控制以确定有关信息系统变更的相关控制的存在与有效性。检查 IS 管理层是否已经设计并强制实施变更日程表；审核在硬件变更实施前。IS 部门内使用的操作员文档已经进行了适当的修订，判断变更计划是否对正常的 IS 处理产生影响，并检查所有硬件变更情况是否已经通知系统程序员、应用程序员和 IS 职员，以确保对变更和测试进行适当的调整。

3.3.3 系统软件控制

计算机系统具有层次型的体系结构，其最底层是计算机硬件和固件，硬件与固件的上一层是操作系统，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的管理者和控制者。

对于一个完整的信息系统而言，系统软件还包括数据库管理系统、通信软件、数据管理软件、作业调度软件、程序库管理系统、磁带/磁盘管理系统和系统工具软件。这些系统软件为业务系统的正确运行提供系统级的保障，当然也是信息系统控制与审计需要关注的关键区域。

1. 系统软件的获取与实施

技术的快速发展使得系统软件的功能也在不断提升，它们可以改进业务流程，并以更有效的方式为业务和客户提供扩充的应用服务。管理层应保证组织内使用的系统软件具有最新的版本，以保证组织的竞争能力。非最新版本的系统软件可能逐渐过时并不再被供应商所支持；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。系统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，所以从控制与审计角度对系统软件的获取也要有相应的控制手段。

然而由于系统软件自身的特点及其与硬件的附着性，一般情况下，信息系统硬件的采购、实施与系统软件通常是同时进行的，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。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。

- 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。

系统软件的实施需要制定组织内使用的标准配置，包括功能特征、配置选项和控制方

法。从信息系统审计角度，需要对系统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。

2. 系统软件的变更控制

系统软件的实施涉及大量的变更，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到系统软件的变更过程中，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对生产系统的影响已经得到适当的评估，在系统软件安装失败时这一评估尤为重要，保证有适当的备份/恢复程序使得一旦发生安装失败，能使其影响最小化。例如，当安装一个安全补丁时，有一个配置管理系统来保留安装前操作系统版本和状态。

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。

在将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。

3. 系统软件的版权与许可

软件版权保护是被大多数国家立法予以保障的，但计算机数据文件的易传播性和互联网的发展，使盗版软件的使用日益猖獗。对于应用信息系统进行日常业务处理的组织来说，盗版软件也是损害组织利益，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，而且大量盗版软件也使组织面临诉讼风险。当前，信息系统越来越多的关键业务应用运行在分布式处理环境和客户机/服务器平台上，这大大增加了侵犯软件版权的可能性。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，保证组织为其信息系统部门建立了标准的计算机桌面环境和软件许可策略，通常的做法有：

- 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。
- 审查所有标准的、已用的和许可的应用及系统软件列表。将该列表和网络内各种服务器中所安装的软件相比较。对于特定 PC 中所安装的软件，也应建立并检查随机抽样的或全包含的软件列表。
- 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。
- 要求所有的 PC 均是无盘工作站，并只通过安全局域网来访问应用程序。
- 在局域网中安装计量软件，并要求所有的 PC 通过该计量软件来访问应用程序。
- 定期扫描 PC，确保 PC 中没有安装非授权的软件备份。

防止在同一网络中的多台 PC 上非法复制软件的另一个有用的控制是和软件供应商签署站点许可协议，站点许可协议基于访问网络的用户数目，而不是针对特定的用户或机器。

在考虑成本效益的情况下，为了限制许可成本，企业还可以选择并发许可协议。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。

4. 操作系统软件控制参数

许多系统软件产品，尤其是操作系统提供参数和选项，用于系统剪裁和特征激活。

参数的重要性在于它决定了系统的设置与行为特征，从而可以使一个标准的系统软件适合各种不同的环境。参数选择应适应组织的工作负载和控制环境结构，判断一个系统软件的控制运行状况的最有效的手段是检查其软件控制特征和/或参数。对操作系统的不适当的实施和参数设置会导致隐藏的错误和数据毁坏，以及非授权的访问和不准确的日志等。

操作系统利用特殊的硬件或软件设置保护自身避免遭受破坏和修改，保护系统关键进程的安全，保证系统软件的完整性，操作系统完整性依赖于管理层对授权技术的使用，管理层应防止非授权用户获取执行特权指令的能力并进而控制整个系统。在评估操作系统完整性时，应检查系统控制选项及保存在系统目录中的参数。例如 Windows 操作系统的注册表、组策略等组件，可以针对不同控制需求进行参数设置(见图 3.1)。

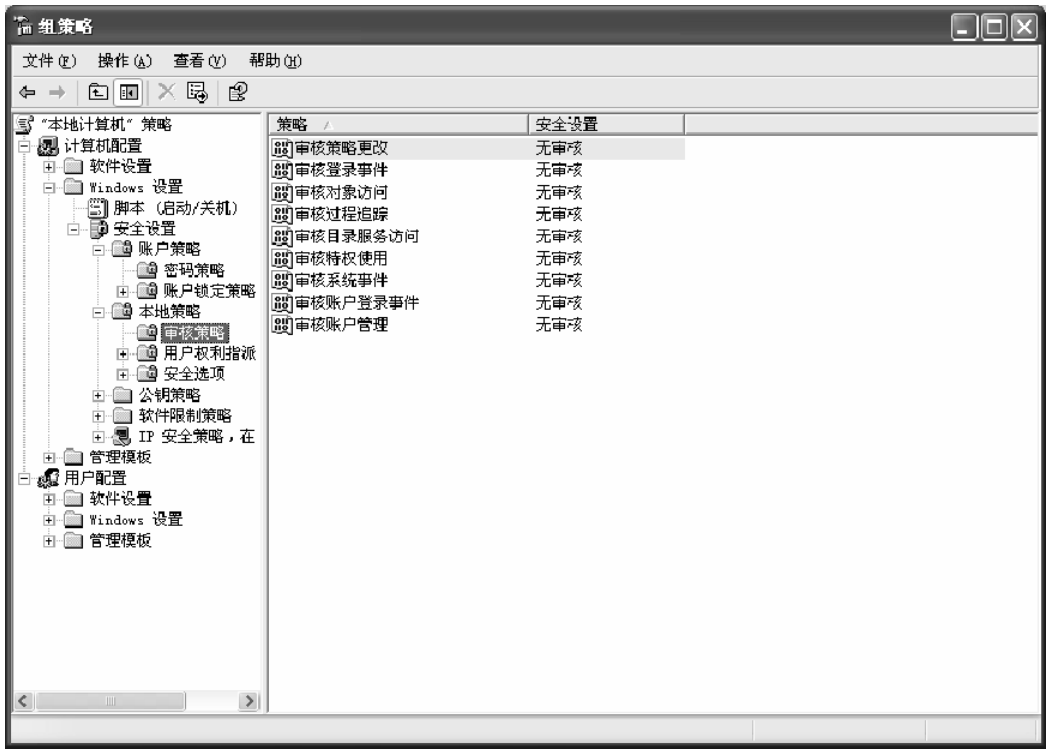

图 3.1 Windows 系统组策略控制设置

系统软件一般提供日志文件，记录计算机处理过程并用于分析系统的行为，通常需要关注的活动日志项目有：

- 生产处理所用数据文件的版本。
- 对敏感数据的程序访问。
- 调度并运行的程序。
- 操作系统的操作。以保证系统不因对系统参数和库程序的不适当变更而危及系统的完整性。
- 数据库。评价数据库结构的有效性及数据库安全，验证 DBA 文档，确定组织的标准是否得到遵循。