国家环境信息与统计能力建设项目

环境信息安全测试与评估技术规定

Environmental Information Security Testing and Evaluation requirement

（征求意见稿）

《环境信息安全测试与评估技术规定》编制组

2010 年 10 月

目录

1 适用范围 3
2 术语和定义 3
3 总则 3
4 安全测评单位 4
5 评估对象 4
6 安全测试与评估的内容 4
7 安全测试与评估的实施 11
附录 A 14
环境信息安全检查表样例 14
附录 B 16
环境信息安全测试用例 16

环境信息安全测试与评估技术规定

1 适用范围

本技术规定规定了环境信息安全进行安全测试与评估的流程和实施要求。

本技术规定适用于国家环境信息与统计能力项目中对于环境信息安全进行安全测试与评估的活动。

2 术语和定义

2.1 可用性 Availability

保证信息和通信服务能够按预期投入使用的特性。

2.2 机密性 Confidentiality

数据所具有的特性，表示数据所达到的未提供或未泄露给未授权的个人、过程或其他实体的程度。

2.3 信息保障 Information Assurance（IA）

保护信息及信息系统的机密性、完整性、可用性、可核查性、真实性、抗抵赖性，通常包括信息系统的保护、检测和恢复能力。

2.4 信息系统 Information System(IS)

用于采集、处理、存储、传输、分发和部署信息的整个基础设施、组织结构、人员和组件的总和。

2.5 信息系统安全 Information System Security (INFOSEC)

使用合理安全措施保护信息系统中的信息在存储、处理或传输等过程中不会被未授权用户访问，并保障授权用户能够正常使用系统。

2.6 完整性 Integrity

保证信息及信息系统不会被有意地或无意地更改或破坏的特性。

2.7 风险 Risk

风险表现为一种可能性，由威胁发生的可能性、威胁所能导致的不利影响以及影响的严重程度共同决定。

2.8 安全域 Security Domain

安全域是一个逻辑范围或区域,在同一范围或区域中的各信息单元具有相同或相近的安全等级或安全防护需求，安全服务的管理员定义和实施统一的安全策略。它是从安全策略的角度划分的区域。

2.9 威胁 Threat

来自于信息系统外部的，能够通过未授权访问、毁坏、揭露、数据修改和/或拒绝服务对系统造成潜在危害的任何环境或事件。

2.10 脆弱性 Vulnerability

存在于信息系统、系统安全程序、管理控制、物理设计、内部控制或实现中的，可能被攻击者利用来获得未授权的信息或破坏关键处理的弱点。

3 总则

环境信息系统的安全测试与评估是在开展环境保护工作中对环境信息系统的安全策略、内控制度、风险管理、系统安全、客户保护等方面进行的安全测试和管控能力的考察与评价。

各有关单位应根据环境信息系统发展和管理的需要，至少每2年对环境信息系统进行一次全面的安全评估，其中等级保护三级的信息系统每年进行一次。

可以由第三方社会专业化机构对环境信息系统进行安全评估，也可以由系统内独立于环境信息系统业务运营和管理部门的评估部门对环境信息系统进行安全评估。

应建立环境信息系统安全评估的规章制度体系和工作规程，保证环境信息系统安全评估能够及时、客观地得以实施。

4 安全测评单位

承担环保机构环境信息系统安全评估工作的测评单位，可以是第三方社会专业化机构，也可以是环保系统内具备相应条件的相对独立部门。

第三方社会专业化机构从事环境信息系统安全评估，应具备国家认可的信息安全测评资质。

环保机构应与聘用的环境信息系统安全测评单位签订书面服务协议，协议中必须含有明确的保密条款和保密责任。

环保机构选择系统内作为测评单位时，应由环境信息系统管理部门与评估部门签订评估责任确定书。

安全测评单位应根据评估协议的规定，认真履行评估职责，真实评估被测评单位环境信息系统安全状况。

5 评估对象

环境信息安全测试与评估的对象为环境信息系统内的各类软硬件资产、应用系统、数据资源及相关组织人员与管理情况。

6 安全测试与评估的内容

6.1 评估流程

环境信息安全测试与评估流程主要包括系统识别、物理安全评估、现场技术实施评估、现场管理评估、工具测试、系统整改与安全评估结论等，信息安全评估流程如图1所示。

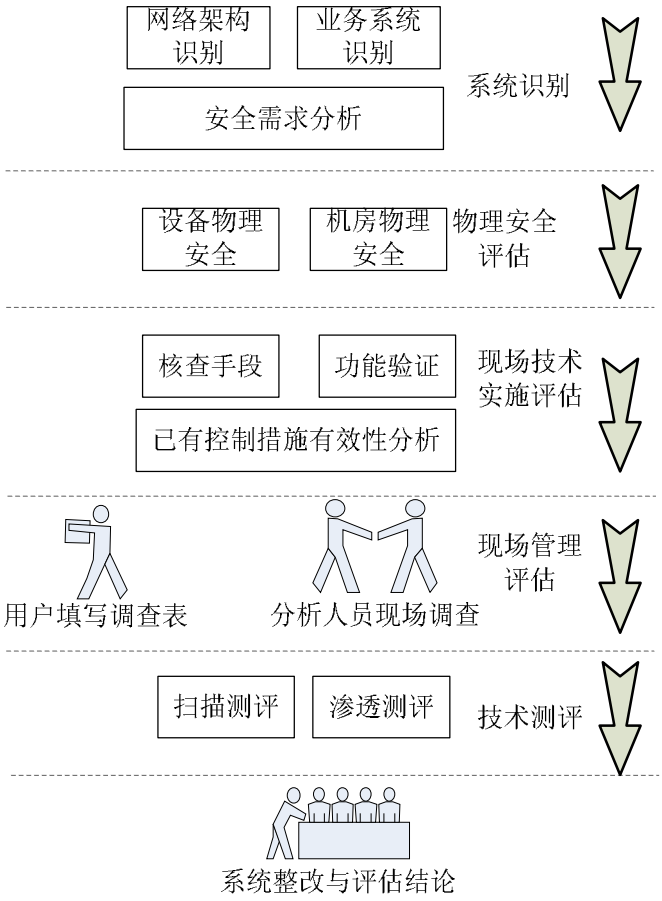

图1 信息安全评估流程

1) 系统识别

系统识别包括网络架构识别、业务系统识别、安全需求分析等三个部分。系统识别阶段分析安全需求、确定安全评估范围。

2) 物理安全评估

对设备物理安全及系统部署情况进行安全评估。

3) 现场技术实施评估

技术实施要求与信息系统提供的安全机制有关，主要通过在信息系统中部署软硬件并正确的配置其安全功能来实现，现场技术实施评估是指对系统实施过程中的策略配置、业务安全措施进行核查，核查安全技术实施是否达到技术方案要求，是否满足《环境信息系统安全技术规范》。

4) 现场管理评估

管理安全要求与信息系统中各种角色参与的活动有关，主要通过控制各种角色的活动，从政策、制度、规范、流程以及记录等方面做出规定来实现。现场管理评估是指从人员、环境、管理等方面对安全的落实情况进行评估，核查是否达到管理方案要求。

5) 技术测试

采用安全扫描软件对安全漏洞进行远程的检测和评估。采用攻击软件对系统、网络进行渗透攻击，从而对系统的安全性进行全面评估。

6) 安全评估结论

针对评估中的不足提出系统整改方案并予以实施，给出最终的安全评估报告。

6.2 现场技术实施评估

6.2.1 物理安全评估

应按照GB 50174－1993 电子计算机机房设计规范、GB/T 2887-2000 电子计算机场地通用规范等描述的相关要求以及环境信息系统安全技术规范，对设备物理安全及系统部署情况进行安全评估。评估内容包括：

1) 是否确保机房的机柜、交换机以及安全设备不存在不同安全域的交叉混用现象，物理结构划分应有利于分域管理；
2) 是否实现办公区和业务区逻辑隔离。

6.2.2 网络安全

6.2.2.1 结构安全

评估内容包括：

1) 是否保证关键网络设备的业务处理能力满足基本业务需要；
2) 是否保证接入网络和核心网络的带宽满足基本业务需要；
3) 是否保证各级环保部门能够利用网络基础设施，实施环境信息工程；
4) 是否实现部门、单位间网络逻辑隔离，降低内部攻击风险；
5) 是否绘制与当前运行情况相符的网络拓扑结构图。

6.2.2.2 访问控制

评估内容包括：

1) 是否在网络边界部署访问控制设备，启用访问控制功能；
2) 是否根据访问控制列表对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包出入；
3) 是否通过访问控制列表对系统资源实现允许或拒绝用户访问，控制粒度至少为用户组。

6.2.2.3 网络设备防护

评估内容包括：

1) 是否对登录网络设备的用户进行身份鉴别；
2) 是否具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施；
3) 是否在对网络设备进行远程管理时，采取了必要措施防止鉴别信息在网络传输过程中被窃听。

6.2.2.4 传输安全

是否确保环境信息数据在环保网络传输中的机密性、完整性。通过在VPN前的网络边界处进行抓包分析，核查移动办公用户、直属机构、各地环境信息中心在访问敏感区的业务时是否进行传输加密保护。

6.2.2.5 安全审计

是否提供基本的网络审计功能，支持基于主机的审计、基于用户的审计等。

6.2.3 主机安全

6.2.3.1 操作系统安全

评估内容包括：

1) 是否使用正版操作系统，应用最新的操作系统补丁；
2) 是否关闭多余端口。

6.2.3.2 身份鉴别

是否对登录用户进行身份标识和鉴别。

6.2.3.3 访问控制

评估内容包括：

1） 是否启用访问控制功能，依据安全策略控制用户对资源的访问；

2） 是否限制默认帐户的访问权限、重命名系统默认帐户、修改这些帐户的默认口令；

3） 是否及时删除多余的、过期的帐户，避免共享帐户的存在。

6.2.3.4 入侵防范

操作系统是否遵循最小安装的原则，仅安装需要的组件和应用程序，并保持系统补丁及时得到更新。

6.2.3.5 恶意代码防范

是否安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库。

6.2.4 应用安全

6.2.4.1 身份鉴别

评估内容包括：

1） 是否提供专用的登录控制模块对登录用户进行身份标识和鉴别；

2） 是否提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；

3） 是否启用身份鉴别和登录失败处理功能，并根据安全策略配置相关参数。

6.2.4.2 访问控制

评估内容包括：

1） 是否提供访问控制功能控制用户组/用户对系统功能和用户数据的访问；

2） 是否由授权主体配置访问控制策略，并严格限制默认用户的访问权限。

6.2.4.3 通信完整性

是否采用约定通信会话方式的方法保证通信过程中数据的完整性。

6.2.4.4 软件容错

是否提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的数据格式或长度符合系统设定要求。

6.2.5 数据安全及备份恢复

6.2.5.1 数据完整性

是否能够检测到**重要**用户数据在传输过程中完整性受到破坏。

6.2.5.2 备份和恢复

评估内容包括：

1） 是否能够对重要信息进行备份和恢复；

2） 环境信息网络核心业务区是否有双链路备份。

6.2.6 业务安全评估

6.2.6.1 办公安全评估

评估内容包括：

1) 系统中所有页面是否提供权限检查，保证非法用户无法绕过认证系统进入应用系统；

2) 用户退出应用系统时是否能够及时清除用户登录会话信息；

3) 对用户权限的改变是否能够在系统中及时得到体现；

4) 是否保证用户权限的改变可以及时体现，未授权用户无法使用未授权的菜单；

5) 关键业务是否检测数字证书，符合等级保护要求；

6) 系统部署是否符合分等级按区域部署要求。

6.2.6.2 公共服务可信核查

评估内容包括：

1) 系统部署是否符合分等级按区域部署要求；

2) 对用户权限的改变是否能够在系统中及时得到体现；

3) 是否保证信息发布的真实性；

4) 是否提供有网页防窜改措施。

6.3 现场管理实施评估

6.3.1 安全管理制度

6.3.1.1 管理制度

是否建立日常管理活动中常用的安全管理制度。

6.3.1.2 制定和发布

评估内容包括：

1) 是否指定或授权专门的人员负责安全管理制度的制订；

2) 是否将安全管理制度以某种方式发布到相关人员手中。

6.3.2 安全管理机构

6.3.2.1 岗位设置

是否设立系统管理员、网络管理员、安全管理员等岗位，并定义各个工作岗位的职责。

6.3.2.2 人员配备

是否配备系统管理员、网络管理员、安全管理员等。

6.3.2.3 授权和审批

是否根据各个部门和岗位的职责，明确授权审批部门及批准人，对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批。

6.3.3 人员安全管理

6.3.3.1 人员录用

评估内容包括：

1) 是否指定或授权专门的部门或人员负责人员录用；

2) 是否对被录用人的身份和专业资格等进行审查，并确保其具有基本的专业技术水平和安全管理知识。

6.3.3.2 人员离岗

评估内容包括：

1) 是否立即终止由于各种原因离岗员工的所有访问权限；

2) 是否取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备。

6.3.3.3 安全意识教育和培训

评估内容包括：

1) 是否对各类人员进行安全意识教育和岗位技能培训；

2) 是否告知人员相关的安全责任和惩戒措施。

6.3.3.4 外部人员访问管理

是否确保在外部人员访问受控区域前得到授权或审批。

6.3.4 系统运维管理

6.3.4.1 环境管理

评估内容包括：

1) 是否指定专门的部门或人员定期对机房供配电、空调、温湿度控制等设施进行维护管理；

2) 是否对机房的出入、服务器的开机或关机等工作进行管理；

3) 是否建立机房安全管理制度，对有关机房物理访问，物品带进、带出机房和机房环境安全等方面的管理作出规定。

6.3.4.2 资产管理

是否编制与信息系统相关的资产清单，包括资产责任部门、重要程度和所处位置等内容。

6.3.4.3 介质管理

评估内容包括：

1) 是否确保介质存放在安全的环境中，对各类介质进行控制和保护；

2) 是否对介质归档和查询等过程进行记录，并根据存档介质的目录清单定期盘点。

6.3.4.4 设备管理

评估内容包括：

1) 是否对信息系统相关的各种设备、线路等指定专门的部门或人员定期进行维护管理；

2) 是否建立基于申报、审批和专人负责的设备安全管理制度，对信息系统的各种软硬件设备的选型、采购、发放和领用等过程进行规范化管理。

6.3.4.5 网络安全管理

评估内容包括：

1) 是否指定人员对网络进行管理，负责运行日志、网络监控记录的日常维护和报警信息分析和处理工作；

2) 是否定期进行网络系统漏洞扫描，对发现的网络系统安全漏洞进行及时的修补。

6.3.4.6 系统安全管理

评估内容包括：

1) 是否根据业务需求和系统安全分析确定系统的访问控制策略；

2) 是否定期进行漏洞扫描，对发现的系统安全漏洞进行及时的修补；

3) 是否安装系统的最新补丁程序，并在安装系统补丁前对现有的重要文件进行备份。

6.3.4.7 恶意代码防范管理

是否提高所有人员的防病毒意识，告知及时升级防病毒软件，在读取移动存储设备上的数据以及网络上接收文件或邮件之前，先进行病毒检查，对外来计算机或存储设备接入网络系统之前也应进行病毒检查。

6.3.4.8 安全事件处置

评估内容包括：

1) 是否及时报告所发现的安全弱点和可疑事件，但任何情况下用户均不应尝试验证弱点；

2) 是否制定安全事件报告和处置管理制度，规定安全事件的现场处理、事件报告和后期恢复的管理职责。

6.4 技术测试

使用测试工具对环境信息系统进行安全扫描和渗透测试。

6.4.1 检测范围

测试范围应包括环境信息应用平台的安全防护设备和应用服务器，涉及的区域如下：

1) 安全管理区；

2) 敏感数据处理区；

3) 公开数据处理区；

4) 安全服务区；

5) 办公区

6.4.2 检测方法

6.4.2.1 安全扫描

通过收集系统的信息来自动检测远程或者本地主机安全性脆弱点。通过使用安全扫描，可以了解被检测端的大量信息，例如，开放端口、提供的服务、操作系统版本、软件版本等。通过这些信息，可以了解到远程主机所存在的安全问题，从而能够及时修补系统存在的安全隐患。

6.4.2.2 渗透测试

渗透测试是对安全扫描结果的进一步验证。渗透测试被设计用于描述安全机制的有效性和对攻击者的控制能力。这些测试都是从一个攻击者的角度出发对目标的安全性进行考察。

6.4.3 扫描测试

6.4.3.1 扫描测试点

应该包括内网检测点和外网检测点在内的多个扫描测试点。

6.4.3.2 扫描对象

扫描对象包括：

1) 边界防护设备
   a) 路由器、交换机、VPN
   b) 防火墙
   c) 互联网上装有 VPN 客户端的移动安全接入终端
2) 重要服务器
   a) 安全管理区服务器
   b) 敏感数据处理区服务器
   c) 公开数据处理区服务器
   d) 安全服务区服务器
   e) 用户终端

6.4.3.3 扫描工具

应同时使用主机漏洞扫描工具和网络漏洞扫描工具：

1) 主机漏洞扫描工具：通过在主机本地的代理程序对系统配置、注册表、系统日志、文件系统或数据库活动进行监视扫描，搜集它们的信息，然后与系统的漏洞库进行比较，如果满足匹配条件，则认为安全漏洞存在；
2) 网络漏洞扫描工具：通过远程检测目标主机 TCP/IP 不同端口的服务，记录目标给予的应答，来搜集目标主机上的各种信息，然后与系统的漏洞库进行匹配，如果满足匹配条件，则认为安全漏洞存在；或者通过模拟黑客的攻击手法对目标主机进行攻击，如果模拟攻击成功，则认为安全漏洞存在。

6.4.4 渗透测试

渗透测试建立在扫描测试的基础上，针对开放的服务及发现的漏洞，利用一些工具对目标实施攻击，看是否能够提升攻击者的权限或能否对目标机的正常运行产生影响。渗透测试点与测试范围与扫描测试相同。渗透测试可能会对系统造成损害，实际测试时应慎重，尤其对正式运行的系统要适度进行。

6.5 系统整改

系统评估后应给出评估结论。并对于评估过程中出现的问题进行逐一整改，整改结果要经过评估人员的复查。

7 安全测试与评估的实施

7.1 评估的主要环节和程序

7.1.1 常规自我测评

7.1.1.1 准备阶段

1）根据信息安全工作状况和安全工作计划，确定委托测评单位进行测评工作。

2）测评单位对信息系统进行必要的技术调查，获取相关技术资料和网络应用、运行管理的资料。

3）测评单位组织测试评估小组并制订具有针对性的信息安全测试分析方案，参考附录B：环境信息安全测试用例进行测试用例的编写。

4）审批信息安全测试分析方案。

5）双方确认具体工作日程与相关配合条件。

6）测评单位根据“信息安全测试分析方案”模拟调试相关工具。

7.1.1.2 实施阶段

1）测评单位进入测试现场，并与环保机构共同确认：

- 环境信息系统的网络拓扑图；
- 环境信息系统的网络物理布置图；
- 本次测评的逻辑和物理测试点；
- 本次测评的测试项和查验项。

2）远程测试。

3）内网测试。

4）攻击性实验。

5）其他测试。

6）汇总测试记录和测试数据。

7.1.1.3 测评结果处理阶段

1）整理分析测试记录和测试数据。

2）归并查验结果。

3）形成测评报告和工作总结报告。

4）提交环保机构本次测评结论及整改建议。

7.1.2 重点检查测评

7.1.2.1 准备阶段

准备阶段即是在常规自我测评的基础上计划重点测评任务。在此阶段，委托测评机构与检查方（相关环境信息系统管理机关）及被检查环境系统就检查任务进行充分沟通，并经由检查方获得相关领导对安全测评工作的批准，制定出切实可行的安全测评计划。

1）测评机构应根据本地实际和工作需要，制定重点测评任务计划书。

2）测评机构应向被检查方通报技术安全重点测评工作。

3）测评机构根据技术安全重点测评任务计划书的有关内容，制定安全核查初访计划，并向相关环境信息系统管理机关发出接受委托和进行安全核查准备的回函，必要时派员赴项目所在地实施初访计划，即与环境信息系统管理机关共同到被检查方考察安全核查前的准备情况，对不符合核查条件的地方提出指导性意见，进一步落实核查计划，并收集必要的文档资料。

7.1.2.2 现场核查阶段

在此阶段，各方组织召开首次会，介绍核查目的、范围、依据和方法，然后开始进行现场观察询问、列表调查和网络测试工作。调查测试完毕经核查组内部统一意见后，向受核查方通报检查情况并召开末次会，宣布核查初步结果。

1）核查组应首先与委托方工作计划。

2）召开首次会，会上由检查组介绍检查目的、意义、内容、方式、要求和工作日程，介绍测评方；其次由核查组长介绍测评方背景、测评方业务特点、环保机关信息系统的安全策略以及测评方的工作方法、核查方式及受核查方的配合条件；由被检查方提出有关疑问并对核查中需要配合的条件要求予以承诺。

3）检查组可分两个小组进行安全核查，一组对被检查方有关部门和人员进行现场观察询问及列表调查；另一组进行网络安全测试。

4）整理调查结果和测试数据，得到初步结果后召开内部交流会，根据两组的结果，确定不符合项目，开列不合格报告单。讨论对被测系统安全性的总体看法，对新发现的问题，拟订补充调查测试任务，同时总结本次检查的经验教训。

6）召开末次会，介绍检查经过，宣布不合格项和不合格程度，提出初步整改要求，通告初步核查结果。

7.1.2.3 后期阶段

1）进行补充调查和测试。

2）综合分析调查结果和测试结果，产生安全检查报告。

3）安全检查程序执行完毕后，应有关情况上报上级环保机关。

7.2 安全评估活动的管理

环保机构应当按照有关规定对完成测试的环境信息系统进行上线前的安全评估。

针对各级环境信息系统，有下列情形之一的，应立即组织安全评估：

1） 由于安全漏洞导致系统被攻击瘫痪，修复运行的；

2） 环境信息系统进行重大更新或升级后，出现系统意外停机12小时以上的；

3） 环境信息系统关键设备与设施更换后，出现重大事故修复后仍不能保持连续不间断运行的；

4） 基于环境信息系统安全管理需要立即评估的。

环境信息系统安全评估工作，确需由多个测评单位共同承担或实施时，环保机构应确定一个主要的测评单位协调总体评估工作，负责总体评估报告的编制。

环保机构将环境信息系统系统委托给不同的测评单位进行安全评估，应当明确每个测评单位安全评估的范围，并保证全面覆盖了应评估的事项，没有遗漏。

环境保护部信息中心根据监管工作的需要，可派员参加环保机构环境信息系统安全评估工作，但不作为正式评估人员，不提供评估意见。

测评单位应本着客观、公正、真实和自主的原则，开展评估活动，并严格保守在评估过程中获悉的商业机密。

未经主管部门批准，环境信息系统安全评估报告不得作为广告宣传资料使用，也不得提供给除主管部门以外的第三方机构。

对于评估报告中所反映出的问题，环保机构应采取有效的措施加以纠正。

附录 A

（资料性附录）

环境信息安全检查表样例

以下所列是环境信息安全技术检查可能涉及的部分事项举例。本清单供参考，不能涵盖所有安全检查内容。

检查对象基本信息	系统名称			
	运行单位			
	负责人			
评估方式	□访谈　□管理核查　□技术检测		**评估时间**	
初步结论				
评估人员	甲方：_____（签字）		乙方：_____（签字）	

评估内容	**评估结果**			**说明**
	访谈	**管理核查**	**技术检测**	
1.　物理安全				
办公楼入口(比如设备入口、维护入口、紧急出口)是否采用了某种访问控制机制?				
机房是否拥有独立于办公楼或计算机室访问控制系统之外的控制机制?				
是否随时对机房实施准入控制?(如果不是，什么时候未控制?)				
在火灾、重大断电事故和其它紧急事件和灾难情况下，相关紧急事件处理人员进入机房需要实施哪些步骤?				
如果采用了自动系统，该系统是否记录雇员进出时间、确认进入人员身份以及其它授权机制(徽标、卡片等)?				
机房闭路电视和警报系统传输信号是否传送到特定位置，这里能够采取及时的回应和其它行动?				
紧急情况下如何对机房实施控制?				
是否实施了任何物理访问控制系统以限制对机房的访问?				
机房入口是否使用密码锁实施控制?(如果是,安装前是否更该了厂家默认设置)				
机房组合锁定密码多长时间更该一次?(至少每 90 天更换一次。)				
机房的房门是否锁定以防止未经授权的人员进入?				
为了实现系统维修与维护,是否利用了某种密钥/锁系统以保护这种访问?				
机房内是否通过徽标识别人员?				
是否要求来访者在进入机房之前填写来访日志?来访者是否有陪同?				
对操作手册、系统规范文档、用户文档和系统软件的访问权限是否实施了限制?				
是否仅由事先通过安全检查的人员对计算机系统实施清洁、维护和维修?				
是否仅由事先通过安全检查的可靠人员清理计算机机房?				
2.　网络安全				
网络中是否存在单点隐患				
网络采取路由模式是否满足要求				
网络中是否采用了安全隔离措施				
对网络的访问权限是否利用了严格控制的口令措施?				
是否有负载均衡设备				
是否考虑采用加密登录的方式				
是否集中采集网络设备的日志				
是否对日志进行审计				
是否采用了网络管理软件或工具				
是否对配置文件的传输和保存进行安全控制				

网络是否具有流量管理软件				
是否使用防火墙进行访问管理控制				
3. 系统安全				
系统上是否只安装了 Windows 一种操作系统？				
是否用 NTFS 文件系统，而不是 FAT 文件系统，对所有驱动器进行格式化？				
是否除非人工清除日志，否则不允许安全日志对以前的安全事件进行改写？				
是否允许使用空口令？				
是否启用了审计子系统？				
当系统处于无人看管的情况时，是否通过有口令保护的屏幕保护程序将系统锁定？				
系统管理工具是否已配置妥当？ 是否对用户使用系统管理工具的行为进行限制？				
系统中的用户和组是否拥有了适当（最低限度）的权限？				
对于运行第三方服务的帐户，是否对其权力进行了适当的调整，只包括了使第三方服务发挥作用所必须的权力？				
是否只有拥有特殊权限的用户才能关闭、重新引导、重新启动系统（本地或远程）？				
是否设置了唯一的用户引导或系统固件口令，并对系统进行了适当的配置，只有输入口令才能将系统引导到单用户状态？				
是否对关键系统进行了物理保护,使得攻击者无法替换 BIOS、给 BIOS 电池放电或移走磁盘驱动器？				
是否将所有可移动的介质保存在安全的地点？（系统管理员和用户应该知道，文件系统安全机制并不能保护软盘和备份介质上的数据）				
4. 应用安全				
用户权限是否被严格划分？				
存储过程能否修改系统表？				
是否启用了登陆日至功能？				
是否存在空口令用户？				
是否存在用户名和口令一致的帐户？				
日常维护是否使用数据库管理员或系统管理员？				
是否定期检查数据库中的用户、权限和口令？				
对密码的复杂程度有无限制？				
是否有数据库性能监控程序？				
在补丁更新前是否进行测试？				
5. 数据备份与恢复				
是否对备份操作小组的成员进行仔细遴选？他们所拥有的权限是否是进行日常工作所必须的？				
备份操作员是否有一个不同于普通用户帐户的特殊帐户，用来进行备份工作？				
是否对备份操作员帐户的活动情况进行记录和监视？				
是否经常更改备份操作员帐户口令和帐号本身？				
是否至少每星期备份信息一次（或者根据书面计算机安全策略每星期备份一次以上）？				
谁负责执行计算机系统备份?（请写出备份人员的角色）				
谁执行重要信息备份操作?				
是否已经制定了机房紧急意外事件计划？				
计算机资源人员是否每年对所有紧急响应措施实施一次审阅？				
涉及所有人员和资源的紧急计划“测试或模拟”是否每年进行？				
多长时间对灾难恢复计划的有效性实施一次测试？				
是否制定了管理人员/所有人联系清单,以便在任何紧急事件情况下立即通知他们？				
是否所有重要业务文件均以原件、硬拷贝或备份形式保存？				
这些备份文件是否保存在安全的地方？				

附录 B

（资料性附录）

环境信息安全测试用例

系统测评用例

测试级别：系统测评

测试对象：xxx_Windows2000 操作系统

测试类：安全审计

测试项：

测试内容：

被测操作系统应对重要操作，如用户登录开启安全审计，以记录用户对系统资源的使用，系统应根据安全审计范围对日志文件大小、覆盖策略、存放位置等做必要配置。

测试方法：

查看Windows操作系统审计事件是否开启，日志审计范围、文件存放位置等。

- 开始|程序|管理工具|本地安全设置|安全设置|本地策略|审核策略
- 开始|程序|管理工具|计算机管理|系统工具|事件查看器|应用日志，右键选择“属性”，日志大小、改写方式。

测试记录：

操作系统是否开启审计？□

审核策略更改：　成功 □　失败 □　　审核登陆事件：　成功 □　失败 □

审核对象访问：　成功 □　失败 □　　审核过程追踪：　成功 □　失败 □

审核目录服务访问：成功 □　失败 □　　审核特权使用：　成功 □　失败 □

审核系统事件：　成功 □　失败 □　　审核账户登陆事件：成功 □　失败 □

审核账户管理：　成功 □　失败 □

是否对备份和还原权限的使用进行审计？□

打印机审计：

目录、文件审计：

系统日志存储位置：默认 □　其他 _____

最大日志文件大小：默认512K □ 其他 _____

日至覆写规则：默认覆盖7天 □　其他 _____

安全日志存储位置：默认 □　其他 _____

最大日志文件大小：默认512K □ 其他 _____

日至覆写规则：默认覆盖7天 □　其他 _____

应用日志存储位置：默认 □　其他 _____

最大日志文件大小：默认512K □ 其他 _____

日至覆写规则：默认覆盖7天 □　其他 _____

如果无法纪录安全审计则立即关闭系统（本地安全策略--安全选项）？ □

是否根据需要配置性能日志和警报？□

备注：

签名：　　测试日期：

设备测评用例

测试对象	XXX防火墙			
测试类别	安全性测试			
测试项目	访问控制			
测试要求	1. 待测目标的安全功能应根据如下项目对客体实施未鉴别的端到端策略： a) 源地址 b) 目的地址 c) 传输层协议 d) 请求的服务（如，源端口号，目的端口号） 2. 待测目标的安全功能应实施如下附加规则，以确定是否允许受控主体和受控客体之间的某一操作： a) 待测目标应当拒绝下述几种从外部非保护网络上未鉴别主机发出的访问或服务请求 ● 其源地址为内部保护网络上的主机地址 ● 其原地址为内部广播网络上的主机地址 ● 其源地址为内部保留网络上的主机地址 ● 其源地址为内部环路网络上的主机地址 b) 待测目标应当拒绝下述几种自外部网络发出的访问或服务请求： ● 其源地址为内部保护网络上的主机地址 ● 其原地址为内部广播网络上的主机地址 ● 其源地址为内部保留网络上的主机地址 ● 其源地址为内部环路网络上的主机地址			
测试方法及内容	1. 根据上述标准要求1中的各种安全属性来配置防火墙的未鉴别的访问控制策略，在防火墙的各网段中执行相应的主体与客体间的未鉴别访问，验证防火墙能否依据相应属性来实施安全策略； 2. 测试防火墙能否拒绝来自外网上主机发出的源地址为内部保护、广播、保留和环路地址的访问数据包。			
测试结果				
测试结论	□符合 □ 基本符合 □不符合			
备 注				
测试人员				
测试期限	开始日期		完成日期	