全国计算机技术与软件专业技术资格（水平）考试

中级 系统集成项目管理工程师 第十七章 信息系统安全管理

试题一 信息系统的安全属性包括( )和不可抵赖性。

A. 保密性、完整性、可用性　　B. 符合性、完整性、可用性

C. 保密性、完整性、可靠性　　D. 保密性、可用性、可维护性

试题二 应用数据完整性机制可以防止( )。

A. 假冒源地址或用户地址的欺骗攻击　　B. 抵赖做过信息的递交行为

C. 数据中途被攻击者窃听获取　　D. 数据在途中被攻击者篡改或破坏

试题三 应用系统运行中涉及的安全和保密层次包括 4 层，这 4 个层次按粒度从粗到细的排列顺序是( )。

A. 数据域安全、功能性安全、资源访问安全、系统级安全　　B. 数据域安全、资源访问安全、功能性安全、系统级安全

C. 系统级安全、资源访问安全、功能性安全、数据域安全　　D. 系统级安全、功能性安全、资源访问安全、数据域安全

试题四 为了确保系统运行的安全，针对用户管理，下列做法不妥当的是( )。

A. 建立用户身份识别与验证机制，防止非法用户进入应用系统

B. 用户权限的分配应遵循“最小特权”原则

C. 用户密码应严格保密，并定时更新

D. 为了防止重要密码丢失，把密码记录在纸质介质上

试题五 某企业应用系统为保证运行安全，只允许操作人员在规定的工作时间段内登录该系统进行业务操作，这种安全策略属于( )层次。

A. 数据域安全　　B. 功能性安全　　C. 资源访问安全　　D. 系统级安全

试题六 基于用户名和口令的用户入网访问控制可分为( )三个步骤。

A. 用户名的识别与验证、用户口令的识别与验证、用户账号的默认限制检查

B. 用户名的识别与验证、用户口令的识别与验证、用户权限的识别与控制

C. 用户身份识别与验证、用户口令的识别与验证、用户权限的识别与控制

D. 用户账号的默认限制检查、用户口令的识别与验证、用户权限的识别与控制

试题七 应用系统运行中涉及的安全和保密层次包括系统级安全、资源访问安全、功能性安全和数据域安全。以下关于这四个层次安全的，错误的是( )。

A. 按粒度从粗到细排序为系统级安全、资源访问安全、功能性安全、数据域安全
B. 系统级安全是应用系统的第一道防线
C. 所有的应用系统都会涉及资源访问安全问题
D. 数据域安全可以细分为记录级数据域安全和字段级数据域安全

试题八 某公司接到通知，上级领导要在下午对该公司机房进行安全检查，为此公司做了如下安排：

①了解检查组人员数量及姓名，为其准备访客证件

②安排专人陪同检查人员对机房安全进行检查

③为了体现检查的公正，下午为领导安排了一个小时的自由查看时间

④根据检查要求，在机房内临时设置一处吸烟区，明确规定检查期间机房内其他区域严禁烟火

上述安排符合《GB/T20269-2006 信息安全技术信息系统安全管理要求》的做法是( )。
A. ③④ B. ②③ C. ①② D. ②④

试题九 信息安全的级别划分有不同的维度，以下级别划分正确的是( )。

A. 系统运行安全和保密有 5 个层次，包括设备级安全、系统级安全、资源访问安全、功能性安全和数据安全
B. 机房分为 4 个级别： A 级、 B 级、 C 级、 D 级
C. 根据系统处理数据划分系统保密等级为绝密、机密和秘密
D. 根据系统处理数据的重要性，系统可靠性分 A 级和 B 级

试题一十 系统运行安全的关键是管理，下列关于日常安全管理的做法，不正确的是( )。
A. 系统开发人员和系统操作人员应职责分离 B. 信息化部门领导安全管理组织，一年进行一次安全检查
C. 用户权限设定应遵循“最小特权”原则 D. 在数据转储、维护时要有专职安全人员进行监督

试题一十一 在某次针对数据库的信息安全风险评估中，发现其中对财务核心数据的逻辑访问密码长期不变。基于以上现象，下列说法正确的是( )。

A. 该数据不会对计算机构成威胁，因此没有脆弱性　　B. 密码和授权长期不变是安全漏洞，属于该数据的脆弱性
C. 密码和授权长期不变是安全漏洞，属于对该数据的威胁　　D. 风险评估针对设施和软件，不针对数据

试题一十二　完整性是信息系统未经授权不能进行改变的特性，它要求保持信息的原样。下列方法中，不能用来保证应用系统完整性的措施是( )。
A. 安全协议　　B. 纠错编码　　C. 数字签名　　D. 信息加密

试题一十三　在信息系统安全技术体系中，环境安全主要指中心机房的安全保护。以下不属于该体系环境安全内容的是( )。
A. 设备防盗器　　B. 接地和防雷击　　C. 机房控制　　D. 防电磁泄漏

试题一十四　物理安全是整个信息系统安全的前提，以下安全防护措施中不属于物理安全范畴的是( )。

A. 安装烟感、温感报警系统，禁止工作人员在主机房内吸烟或者使用火源
B. 要求工作人员在主机房内工作时必须穿着防静电工装和防静电鞋，并定期喷涂防静电剂
C. 为工作人员建立生物特征信息库，并在主机房入口安装指纹识别系统，禁止未经授权人员进入主机房
D. 对因被解雇、退休、辞职活其他原因离开信息系统岗位的人员，收回所有相关证件、徽章、密匙和访问控制标记等

试题一十五　系统运行安全和保护的层次按照粒度从粗到细排序为( ) 。
A. 系统级安全，资源访问安全，数据域安全，功栽性安全　　B. 系统级安全，资源访问安全，功能性安全，数据域安全
C. 资源访问安全，系统级安全，数据域安全，功能性安全　　D. 资源访问安全，系统级安全，功能性安全，数据域安全

试题一十六　以下不属于主动式攻击策略的是( )。
A. 中断　　B. 篡改　　C. 伪造　　D. 窃听

试题一十七　在信息系统安全管理中，业务流控制，路由选择控制和审计跟踪等技术主要用于提高信息系统的( )。
A. 保密性　　B. 可用性　　C. 完整性　　D. 不可抵赖性

试题一十八 根据《信息安全技术信息系统安全通用性技术要求 GB/T27201-2006 》，信息系统安全的技术体系包括( )。

A. 物理安全、运行安全、数据安全　　B. 物理安全、网络安全、运行安全

C. 人类安全、资源安全、过程安全　　D. 方法安全、过程安全、工具安全

试题一十九 按照系统安全等级中的可靠性等级由高到低分别为( )。

A. 绝密、机密、秘密　　B. 军用、商用、民用　　C．A 级、 B 级、 C 级　　D. 使用级、修改级、控制级

试题二十 应用系统运行的安全管理中心，数据域安全是其中非常重要的内容数据域安全包括( )。

A. 行级数据域安全，字段级数据域安全　　B. 系统性数据域安全，功能性数据域安全

C. 数据资源安全，应用性数据安全　　D. 组织级数据域安全，访问性数据域安全

试题二十一 某公司系统安全管理员在建立公司的“安全管理体系”时，根据 GB/T20269-2006 《信息安全技术信息系统安全管理要求》，对当前公司的安全风险进行了分析和评估，他分析了常见病毒对计算机系统、数据文件等的破坏程度及感染特点，制定了相应的防病毒措施。这一做法符合( )的要求。

A. 资产识别和评估　　B. 威胁识别和分析　　C. 脆弱性识别和分析　　D. 等保识别和分析

试题二十二 信息安全策略应该全面地保护信息系统整体的安全，网络安全体系设计是编辑设计工作的重要内容之一，可从物理线路安全、网络安全、系统安全、应用安全等方面来进行安全体系的设计与规划。其中，数据库的容灾属于( )的内容。

A. 物理线路安全与网络安全　　B. 网络安全与系统安全　　C. 物理线路安全与系统安全

D. 系统安全与应用安全

试题二十三 以下不属于物理访问控制要点的是( )。

A. 硬件设施在合理范围内是否能防止强制入侵　　B. 计算机设备的钥匙是否有良好的控制

C. 计算机设备电源供应是否能适当控制在合理的规格范围内　　D. 计算机设备在搬动时是否需要设备授权同行证明

试题二十四 MD5 常用于数据( )保护。

A. 校验　　B. 完整　　C. 机密　　D. 可靠

试题二十五 GB/T14394-93《计算机软件可靠性和可维护性管理》标准提出了软件生存周期各阶段的可靠性和可维护性要求。其中“分析和确定软件可靠性和可维护性目标”是( )的要求。

A. 需求分析阶段　　B. 概要设计阶段　　C. 详细设计阶段　　D. 实现阶段

试题二十六 具有保密资质的公司中一名涉密的负责信息系统安全的安全管理员提出了离职申请，公司采取的以下安全控制措施中，( )可能存在安全隐患.

A. 立即终止其对安全系统的所有访问权限
B. 收回所有相关的证件、徽章、密钥、访问控制标志、提供的专用设备等
C. 离职员工办理完人事交接，继续工作一个月后离岗
D. 和离职人员签订调离后的保密要求及协议

试题二十七 依据 GB/T20271-2006《信息系统安全技术信息系统通用安全技术要求》中的规定，( )不属于信息系统安全技术体系包含的内容。

A. 物理安全　　B. 运行安全　　C. 人员安全　　D. 数据安全

试题二十八 以下关于入侵检测设备的叙述中，( )是不正确的。

A. 不产生网络流量　　B. 使用在尽可能靠近攻击源的地方
C. 使用在尽可能接近受保护资源的地方　　D. 必须跨接在链路上

试题二十九 代理服务器防火墙主要使用代理技术来阻断内部网络和外部网络之间的通信，达到隐蔽内部网络的目的。以下关于代理服务器防火墙的叙述中，( )是不正确的。

A. 仅“可以信赖的”代理服务才允许通过　　B. 由于已经设立代理，因此任何外部服务都可以访问
C. 允许内部主机使用代理服务器访问 Internet　　D. 不允许外部主机连接到内部安全网络

试题三十 不同安全等级的安全管理机构应该建立自己的信息系统安全组织机构管理体系。在该体系中，最低级别的安全管理要求是( )

A. 建立信息安全保密管理部门　　B. 成立安全领导小组　　C. 建立安全职能部门　　D. 配置安全管理人员

试题三十一 下列属于对称密钥加密算法的是( )。

A．RSA 加密体制　　B．DES 加密体制　　C．ECC 加密体制　　D．Elgamal 加密体制

试题三十二 针对应用程序或工其在使用过程中可能出现计算、传输数据的泄密和失窃，通过其他安全工具或策略来消除隐患属于安全保护措施中的( )。
A. 应用安全　　B. 物理安全　　C. 介质安全　　D. 数据安全

试题三十三 某公司财务管理数据只能提供给授权的用户，通过采取安全管理措施来确保信息不能被未授权的个人、实体或过程利用或知悉，以确保数据的( ) 。
A. 保密性　　B. 完整性　　C. 可用性　　D. 稳定性

试题三十四 访问控制是信息安全管理的重要内容之一。以下关于访问控制规则的叙述中，( )是不正确的。

A. 应确保授权用序对信息系统的正常访问
B. 防止对操作系统的未授权访问
C. 防止对外部网络未经授权进行访问；对内部网络的访问则没有限制
D. 防止对应用系统中的信息未经授权进行访问

试题三十五 依据[2007]43 号《信息安全等级保护管理办法》，我国信息系统的妄全保护等级分为( )级。
A. 三　　B. 五　　C. 四　　D. 二

试题三十六 为了保护计算机机房及其设备的安全，( )做法是不合适的。

A. 机房地板的阻值应控制在不易产生静电的范围
B. 机房隔壁为卫生间或水房，一旦有火灾便于取水灭火
C. 机房的供电系统应将计算机系统供电与其他供电分开
D. 机房设备应具有明显的且无法去除的标记，以方便更换和便于追查

试题三十七 为保障数据的存储和传输安全，防止信息泄露，需要对一些重要数据进行加密。对称密码算法( )。所以特别适合对大量的数据进行加密。
A. 比非对称密码算法更安全　　B. 二比非对称密码算法密钥长度更长
C. 比非对称密码算法效率更高　　D. 还能同时用于身份认证

试题三十八 某招标文件要求投标方应具有计算机信息系统集成资质和 IS09000 质量认证证书，投标人在投标文件中提供了母公司的计算机信息系统集成资质证书和 IS09000 质量认证证书，则该投标人提供的投标文件( )。

A. 符合招标要求　　B. 不符合招标要求　　C. 基本符合招标要求　　D. 完全符合招标要求

试题三十九　堡垒主机是一台完全暴露给外网的主机，在维护内网安全方面发挥着非常大的作用。以下关于堡垒主机的叙述中，不正确的是：( )。

A. 堡垒主机具有输入输出审计功能　　B. 需要设置防火墙以保护堡垒主机

C. 堡垒主机能配置网关服务　　D. 堡垒主机一般配置两块网卡

试题四十　计算机网络安全是指利用管理和技术措施，保证在一个网络环境里，信息的( )受到保护。

A. 完整性、可靠性及可用性　　B. 机密性、完整性及可用性　　C. 可用性、完整性及兼容性　　D. 可用性、完整性及冗余性

试题四十一　系统运行的安全检查是安全管理中的一项重要工作，旨在预防事故、发现隐患、指导整改。在进行系统运行安全检查时，不恰当的做法是：( )。

A. 定期对系统进行恶意代码检查，包括病毒、木马、隐蔽通道等

B. 检查应用系统的配置是否合理和适当

C. 检查应用系统的用户权限分配是否遵循易用性原则

D. 检查应用系统的可用性，包括系统的中断时间、正常服务时间、恢复时间等

试题四十二　数字签名技术属于信息系统安全管理中保证信息( )的技术。

A. 保密性　　B. 可用性　　C. 完整性　　D. 可靠性

试题四十三　应用系统运行中涉及的安全和保密层次包括系统级安全、资源访问安全、功能性安全和数据域安全。针对应用系统安全管理，首先要考虑( )。

A. 系统级安全　　B. 资源访问安全　　C. 功能性安全　　D. 数据域安全

试题四十四　关于信息系统岗位人员的安全管理的描述，不正确的是：( )。

A. 对安全管理员、系统管理员、重要业务操作人员等关键岗位进行统一管理

B. 紧急情况下，关键岗位人员可独自处理重要事务或操作

C. 人员离岗后，应立即中止其所有访问权限

D. 业务开发人员和系统维护人员不能兼任安全管理员

试题四十五 应用系统运行中涉及的安全和保密层次包括系统级安全、资源访问安全、数据域安全等。以下描述不正确的是：( )。

A. 按粒度从大到小排序为系统级安全、资源访问安全、数据域安全
B. 系统级安全是应用系统的第一道防线
C. 功能性安全会对程序流程产生影响
D. 数据域安全可以细分为文本级数据域安全和字段级数据域安全

试题四十六 在信息系统安全技术体系中，安全审计属于( )
A. 物理安全 B. 网络安全 C. 数据安全 D. 运行安全

试题四十七 根据《信息安全等级保护管理办法》规定，信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害，则该信息系统的安全保护等级为( )
A. 一级 B. 二级 C. 三级 D. 四级

试题四十八 DDoS 拒绝服务攻击是以通过大量合法的请求占用大量网络资源，造成网络瘫痪。该网络攻击破坏了信息安全的( )属性。
A. 可控性 B. 可用性 C. 完整性 D. 保密性

试题四十九 关于信息系统岗位人员安全管理的描述，不正确的是( )。

A. 业务应用操作人员不能由系统管理员兼任
B. 业务开发人员不能兼任系统管理员
C. 系统管理员可以兼任数据库管理员
D. 关键岗位人员处理重要事务或操作时，应保持二人同时在场

试题五十 关于信息系统岗位人员管理的要求，不正确的是( )。

A. 安全管理员和系统管理员不能由一人兼任
B. 业务开发人员不能兼任安全管理员、系统管理员
C. 系统管理员、数据库管理员、网络管理员不能相互兼任岗位或工作
D. 关键岗位在处理重要事物或操作时，应保证二人同时在场

试题五十一 通过控制网络上的其他计算机，对目标逐级所在网络服务不断进行干扰，改变其正常的作业流程，执行无关程序使系统变瘫痪，这种行为属于( )。

A. 系统漏洞　　B. 网络瘟疫　　C. 拒绝服务攻击　　D. 种植病毒

试题五十二 关于网络安全的描述，不正确的是：( )。

A. 网络安全工具的每一个单独组件只能完成其中部分功能，而不能完成全部功能
B. 信息安全的基本要素有机密性、完整性、可用性
C. 典型的网络攻击步骤为:信息收集、试探寻找突破口、实施攻击、消除记录、保留访问权限
D. 只有得到允许的人才能修改数据，并且能够判别出数据是否已被篡改，描述的是信息安全的可用性

试题五十三 GB/T22080-2016《信息技术 安全技术 信息安全管理体系要求》标准规定的内容包括( )

①信息安全方针与策略、②人力资源安全、③等级保护、④访问控制、⑤业务连续性管理

A．1234　　B．1245　　C．1345　　D．2345

试题五十四 对信息系统岗位人员的安全管理要求不包括( )

A. 兼职和轮岗　　B. 权限分散并交叉覆盖　　C. 多人共管　　D. 全面控制

试题五十五 关于人员安全管理的描述，不正确的是：( )

A. 组织可以建立安全领导小组，负责本组织机构的信息系统安全工作
B. 关键岗位人员应定期接受安全培训，加强安全意识
C. 对于离岗人员要收回机构提供的设备
D. 关键岗位离岗人员承诺保密要求且进行安全审查后可办理调离手续

试题五十六 依据《信息安全等级保护管理方法》，信息系统破坏后，会对社会秩序和公共利益造成特别严重损害。或者对国家安全造成严重损害，该信息系统安全保护等级为( )

A. 第二级　　B. 第三级　　C. 第四级　　D. 第五级

试题五十七 试题四(19 分)

阅读下列说明，回答问题 1 至问题 3，将解答填入答题纸的对应栏内。

【说明】

A 集团公司信息中心负责集团及子公司的信息系统建设和运行维护管理工作。为了确保系统安全稳定运行，并为各业务部门(系统使用方)提供良好服务，信息中心将系统运行维护工作外包给了 B 公司,B 公司高层非常重视该项目，任命张伟担任目经理。在项目初期，张伟编制了干系人清单，部分内容如下:

一类干系人(主要干系人):A 公司信息中心管理层。

二类干系人(次要干系人):A 公司信具中心技术人员、 B 公司管理层、 B 公司政部门(为项目提供备件、人员培训等支持)。

三类干系人(一船干系人):A 公司业务部门人员、 B 公司项目组成员、其他人员。

为确保项目沟通顺畅，张伟制定了项日沟通计划.部分内容如下:

项目开展三个月后， B 公司管理层收到了 A 公司信息中心管理层的投诉:

一是对项目的进展情况不了解；二是业务部门反馈服务热线总是占线。张伟解释:很难协调双方公司管理层同时到场，月度项目汇报现场会议一直未能召开； A 公司部分 BI 人员不知道有在线知识库，遇到的大小问题都打服务热线造成了占线。

沟通方式	沟通内容	沟通频率	沟通对象
现场会议	项目日常工作进展	每周	A公司信息中心技术人员、B公司项目组成员
现场会议	项目阶段性总结、汇报	每月	A公司信息中心管理层、B公司管理层
电话	日常工作	按需	所有干系人
电子邮件	项目周报	每周	所有干系人
在线知识库	常见问题解决方案	随时	A公司信息中心技术人员、A公司业务部门人员、B公司项目组成员

【问题1】（10分）

结合案例，请指出张伟在项目沟通管理与干系人管理中存在的问题。

【问题2】（6分）

结合案例，请采用权力/利益方格对A公司信息中心管理层、B公司行政部门、A公司业务部门人员，分别采用什么方式来管理，并给出理由。

【问题3】（3分）

请将下面①-③处的答案填写在答题纸的对应栏内。

案例中沟通的方式，会议属于①；电子邮件属于②；在线知识库属于③。

试题一 答案： A **解析：** 本题考查考生对信息系统安全概念的理解，信息系统安全定义为：确保以电磁信号为主要形式的，在信息网络系统进行通信、处理和使用的信息内容，在各个物理位置逻辑区域、存储、和传输介质中，处于动态和静态过程中的保密性、完整性、可用性和不可抵赖性，以及与网络、环境有关的技术安全、结构安全和管理安全的总

和。其中保密性、完整性和可用性是信息系统安全的基本属性。

最初对信息系统的安全优先考虑的是可用性，随后是保密性和完整性，后来又增加了真实性和不可抵赖性，再后来又有人提出可控性、不可否认性等等。安全属性也扩展 到 5 个：保密性、完整性、可用性、. 真实性和不可抵赖性。

要实现具有这么多安全属性、并达到相互之间平衡的信息系统近乎是件不可能的任务，以至于后来的通用评估准则(CC，ISO/IEC15408，GB / T18336)和风险管理准则 (BS7799，ISO/IEC27001)都直接以安全对象所面临的风险为出发点来分别研究信息安全产品和信息系统安全，针对每一风险来采取措施，其终极安全目标是要保护信息资产的安全，保障业务系统的连续运行。

试题二 答案： D **解析：** 现代电子商务是指使用基于因特网的现代信息技术工具和在线支付方式进行商务活动。电子商务安全要求包括 4 个方面：

(1) 数据传输的安全性。对数据传输的安全性要求在网络传送的数据不被第三方窃取。

(2) 数据的完整性。对数据的完整性要求是指数据在传输过程中不被篡改。

(3) 身份验证。确认双方的账户信息是否真实有效。

(3) 交易的不可抵赖性。保证交易发生纠纷时有所对证。

试题三 答案： C **解析：** 本题考查系统安全问题。

《系统集成项目管理工程师教程》的“17.5.2 应用系统运行中的安全管理”节中系统运行安全与保密的层次构成中指出：应用系统运行中涉及的安全和保密层次，按照粒度从粗到细的排序是系统级安全、资源访问安全、功能性安全和数据域安全。

试题四 答案： D **解析：** 本题考查用户管理制度。

《系统集成项目管理工程师教程》的“17.5.2 应用系统运行中的安全管理”节中指出：系统运行的安全管理中关于用户管理制度的内容包括建立用户身份识别与验证机制， 防止非法用户进入应用系统；对用户及其权限的设定进行严格管理，用户权限的分配遵循“最小特权”原则；用户密码应严格保密，并及时更新；重要用户密码应密封交安全管理员保管，人员调离时应及时修改相关密码和口令。

试题五 答案： D **解析：** 应用系统运行中涉及的安全和保密层次包括系统级安全、资源访向安全、功能性安全和数据安全。这 4 个层次的安全，按照粒度从粗到细的排序是系统级安全、资源访问安全、功能性安全、数据域安全。程序资源访问控制安全的粒度大小界

于系统级安全和功能性安全两者之间，是最常见的应用系统安全问题，几乎所有的应用系统都会涉及这个安全问题。

(1)系统级安全

企业应用越来越复杂，因此制定得力的系统级安全策略才是从根本上解决问题的基础。通过对现行安全技术的分析，制定系统级安全策略，策略包括敏感系统的隔离、访问 IP 地址段的限制、登录时间段的限制、会话时间的限制、连接数的限制、特定时间段内登录次数的限制以及远程访问控制等，系统级安全是应用系统的第一级防护大门。 (2)资源访问安全

对程序资源的访问进行安全控制，在客户端上，为用户提供和其权限相关的用户界面，仅出现和其权限相符的菜单和操作按钮；在服务端则对 URL 程序资源和业务服务类方法的调用进行访问控制。

(3)功能性安全

功能性安全会对程序流程产生影响，如用户在操作业务记录时，是否需要审核，上传附件不能超过指定大小等。这些安全限制已经不是入口级的限制，而是程序流程内的限制，在一定程度上影响程序流程的运行。

(3)数据域安全

数据域安全包括两个层次，其一是行级数据域安全，即用户可以访问哪些业务记录，一般以用户所在单位为条件进行过滤；其二是字段级数据域安全，即用户可以访问业务记录的哪些字段。不同的应用系统数据域安全的需求存在很大的差别，业务相关性比较高。

根据上述定义，只允许操作人员在规定的工作时间段内登录该系统进行业务操作，属于“系统级安全”层次。

试题六 答案： A **解析：** 访问控制是网络安全防范和保护的主要策略，它的主要任务是保证网络资源不被非法使用和访问。它是保证网络安全最重要的核心策略之一。访问控制涉及的技术也比较广，包括入网访问控制、网络权限控制、目录级控制以及属性控制等多种手段。

入网访问控制为网络访问提供了第一层访问控制。它控制哪些用户能够登录到服务器并获取网络资源，控制准许用户入网的间和准许他们在哪台工作站入网。用户的入网访问控制可分为三个步骤：用户名的识别与验证、用户口令的识别与验证、用户账号的默认限制检查。三道关卡中只要任何一关未过，该用户便不能进入该网络。对网络用户的用户名和口令进待验证是防止非法访问的第一道防线。为保证口令的安全性，用户口令不能显示在显示屏上，口令长度应不少于 6 个字符，口令字符最好是数字、字母和其他字符的混合，用户口令必须经过加密。用户还可采用一次性用户口令，也可用便携式验证器(如智能卡)来

验证用户的身份。网络管理员可以控制和限制普通用户的账号使用、访问网络的时间和方式。用户账号应只有系统管理员才能建立。
因此，基于用户名和口令的用户入网访问控制可分为用户名的识别与验证、用户口令的识别与验证、用户账号的默认限制检查等三个步骤。

试题七 答案： D **解析：** 本题考查的是信息系统安全管理基础知识。出自《系统集成项目管理工程师教程(第 2 版)》第 17 章 信息系统安全管理，全书第 537 页。

系统运行安全与保密的层次构成

应用系统运行中涉及的安全和保密层次包括系统级安全、资源访问安全、功能性安全和数据域安全。这 4 个层次的安全，按粒度从粗到细的排序是：系统级安全、资源访问安全、功能性安全、数据域安全。程序资源访问控制安全的粒度大小界于系统级安全和功能性安全两者之间，是最常见的应用系统安全问题，‘几乎所有的应用系统都会涉及这个安全问题。

(1)系统级安全。

企业应用系统越来越复杂，因此制定得力的系统级安全策略才是从根本上解决问题的基础。应通过对现行系统安全技术的分析，制定系统级安全策略，策略包括敏感系统的隔离、访问 ip 地址段的限制、登录时间段的限制、会话时间的限制、连接数的限制、特定时间段内登录次数的限制以及远程访问控制等，系统级安全是应用系统的第一道防护大门。

(2)资源访问安全。

对程序资源的访问进行安全控制，在客户端上，为用户提供和其权限相关的用户界面，仅出现和其权限相符的菜单和操作按钮：在服务端则对 URL 程序资源和业务服务类方法的调用进行访问控制。

(3)功能性安全。

功能性安全会对程序流程产生影响，如用户在操作业务记录时，是否需要审核，上传附件不能超过指定大小等。这些安全限制已经不是入口级的限制，而是程序流程内的限制，在一定程度上影响程序流程的运行。

(4)数据域安全。

数据域安全包括两个层次，其一是行级数据域安全，即用户可以访问哪些业务记录，一般以用户所在单位为条件进行过滤；其二是字段级数据域安全，即用户可以访问业务记录的哪些字段。不同的应用系统数据域安全的需求存在很大的差别，业务相关性比较高。对于行级的数据域安全，大致可以分为以下几种情况：

①应用组织机构模型允许用户访问其所在单位及下级管辖单位的数据。

②通过数据域配置表配置用户有权访问同级单位及其他行政分支下的单位的数据。

③按用户进行数据安全控制，只允许用户访问自己录入或参与协办的业务数据。

④除进行按单位过滤之外，比较数据行安全级别和用户级别，只有用户的级别大于等于行级安全级别，才能访问到该行数据。

试题八 答案： C **解析：** 在《信息安全技术信息系统安全管理要求 GB/T20269—2006》物理安全管理中给出了技术控制方法：

(1)检测监视系统

应建立门禁控制手段，任何进出机房的人员应经过门禁设施的监控和记录，应有防止绕过门禁设施的手段(可见“③为了体现检查的公正，下午为领导安排了一个小时的自由查看时间是错误的)；门禁系统的电子记录应妥善保存以备查；进入机房的人员应佩戴相应证件(可见“①了解检查组人员数量及姓名，为其准备访客证件”是正确的)；未经批准，禁止任何物理访问；未经批准，禁止任何人移动计算机相关设备或带离机房。

机房所在地应有专设警卫，通道和入口处应设置视频监控点。 24 小时值班监视；所有来访人员的登记记录、门禁系统的电子记录以及监视录像记录应妥善保存以备查；禁止携带移

动电话、电子记事本等具有移动互联功能的个人物品进入机房。

(2)人员进出机房和操作权限范围控制

应明确机房安全管理的责任人，机房出入应有指定人员负责，未经允许的人员不准进入机房；获准进入机房的来访人员，其活动范围应受限制，并有接待人员陪同(可见“②安排专人陪同检查人员对机房安全进行检查”是正确的)；机房钥匙由专人管理，未经批准，不准任何人私自复制机房钥匙或服务器开机钥匙；没有指定管理人员的明确准许，任何记录介质、文件材料及各种被保护品均不准带出机房，与工作无关的物品均不准带入机房；机房内严禁吸烟及带入火种和水源(可见“④根据检查要求，在机房内临 时设置一处吸烟区，明确规定检查期间机房内其他区域严禁烟火”是错误的)。

应要求所有来访人员经过正式批准，登记记录应妥善保存以备查；获准进入机房的人员，一般应禁止携带个人计算机等电子设备进入机房，其活动范围和操作行为应受到限制，并有机房接待人员负责和陪同。

试题九 答案： C **解析：** 根据《电子信息系统机房设计规范》(GB50174—2008)可知，电子信息系统机房分为三级，由高到低分别为A级、 B级和C级。

根据《系统集成项目管理工程师教程》(全国计算机专业技术资格考试办公室组编)第17.5.2小节的相关内容可知，应用系统中涉及的安全保密层次包括系统级安全、资源访问安全、功能性安全和数据域安全。安全等级可分为保密等级和可靠性等级两种，系统的保密等级与可靠性等级可以不同。保密等级应按有关规定划为绝密、机密和秘密。 可靠性等级可分为三级，对可靠性要求最高的是A级，系统运行所要求的最低限度可靠性为C级，介于中间的为B级。

综上可知，保密等级应按有关规定划为绝密、机密和秘密。

试题一十 答案： B **解析：** 根据《系统集成项目管理工程师教程》(全国计算机专业技术资格考试办公室组编)第17.5.2小节的内容可知，在系统运行的安全管理组织中，安全组织由单位主要领导人领导，不能隶属于计算机运行或应用部门。在系统运行操作规程中，对系统开发人员和系统操作人员要进行职责分离。在用户管理制度中，对用户及其权限的设定应进行严格管理，用户权限的分配必须遵循“最小特权”原则。在系统运行维护制度中，对系统进行维护时，应采取数据保护措施。如数据转储、涂抹、卸下磁盘磁带，维护时安全人员必须在场等。

信息化部门领导安全管理组织的做法不符合上述系统运行安全管理制度。

试题一十一 答案： B **解析：** 威胁、脆弱性、影响之间存在着一定的对应关系，威胁可看成从系统外部对系统产生的作用，而导致系统功能及目标受阻的所有现象。而脆弱性则可以看成是系统内部的薄弱点。脆弱性是客观存在的，脆弱性本身没有实际的伤害，但威胁可以利用脆弱性发挥作用。假设威胁不存在，系统本身的脆弱性仍然带来一定的风险。系统本身脆弱性导致的损失，与威胁不一定相关。

密码和授权长期不变是系统内部客观存在的薄弱点，因此属于脆弱性。

试题一十二 答案： D **解析：** 根据《系统集成项目管理工程师教程》中“17.2.2 信息系统安全属性”一节的所述内容，完整性是信息未经授权不能进行改变的特性。即应用系统的信息在存储或传输过程中保持不被偶然或者蓄意地删除、修改、伪造、乱序、重放和插入等破坏和丢失的特性。完整性是一种面向信息的安全性，它要求保持信息的原样，即信息的正确生成及正确存储和传输。

完整性与保密性不同，保密性要求信息不被泄露给未授权的人，而完整性则要求信息不致受到各种原因的破坏。

保障应用系统完整性的主要方法包括：协议、纠错编码、密码教育和方法、数字签名、公证。

由此可知，安全协议、纠错编码、数字签名均属于保证应用系统完整性的措施，而“信息加密”是保障应用系统保密性的常用技术。

试题一十三 答案： A **解析：** 根据《系统集成项目管理工程师教程》中“17.2.3 信息系统安全管理体系”一节的所述内容，在 GB/T20271—2006 《信息安全技术信息系统通用安全技术要求》中将信息系统安全技术体系具体描述如下。

(1)物理安全。

①环境安全。

主要指中心机房的安全保护，包括：

机房场地选择。

机房内部安全防护。

机房防火。

机房供、配电。

机房空调、降温。

机房防水与防潮。

机房防静电。

机房接地与防雷击。

机房电磁防护。

②设备安全。

设备的防盗和防毁。

设备的安全可用。

根据以上内容可知，接地和防雷击、机房控制、防电磁泄漏均属于环境安全内容。设备防盗器属于设备安全的内容，而不属于环境安全内容。

试题一十四 答案： D **解析：** 根据《系统集成项目管理工程师教程》中“17.3 物理安全管理”一节的所述内容，物理安全管理包括安全区域的管理、设备设施的安全管理、对环境威胁的防范以及电磁辐射的管理等。

安装烟感、温感报警系统，禁止工作人员在主机房内吸烟或者使用火源和要求工作人员在主机房内工作时必须穿着防静电工装和防静电鞋，并定期喷涂防静电剂是计算机机房防火、防静电方面的安全防护措施，属于计算机机房与设施安全管理范畴；为工作人员建立生物特征信息库，并在主机房入口安装指纹识别系统，禁止未经授权人员进入主机房是建立一种门禁控制机制，属于物理安全管理的技术控制手段。因此上述三项均属于物理安全范畴。

根据《系统集成项目管理工程师教程》中“17.4 人员安全管理”一节所述内容，对人员离岗的管理，可以根据离岗人员的关键程度，采取下列控制措施。

(1)基本要求：立即中止被解雇的、退休的、辞职的或其他原因离开的人员的所有访问权限：收回所有相关证件、徽章、密钥和访问控制标记等：收回机构提供的设备等。

(2)调离后的保密要求：在上述基础上，管理层和信息系统关键岗位人员调离岗位，必须经单位人事部门严格办理调离手续，承诺其调离后的保密要求。

(3)离岗的审计要求：在上述基础上，设计组织机构管理层和信息系统关键岗位的人员调离单位，必须进行离岗安全审查，在规定的脱密期限后，方可调离。

(3)关键部位人员的离岗要求：在上述基础上，关键部位的信息系统安全管理人员离岗，应按照机要人员管理办法办理。

根据以上分析可知，对因被解雇、退休、辞职活其他原因离开信息系统岗位的人员，收回所有相关证件、徽章、密匙和访问控制标记等属于人员安全管理范畴，而不属于物理安全范畴。

试题一十五 答案： B **解析：** 根据《系统集成项目管理工程师教程》书中“17.5.2 应用系统运行中的安全管理”一节的所述内容，应用系统运行中涉及的安全和保密层次包括系统级安全、资源访问安全、功能性安全和数据域安全。这 4 个层次的安全，按粒度从粗到

细的排序是系统级安全、资源访问安全、功能性安全、数据域安全。程序资源访问控制安全的粒度大小介于系统级安全和功能性安全两者之间，是最常见的应用系统安全问题，几乎所有的应用系统都会涉及这个安全问题。

试题一十六 答案： D **解析：** 计算机网络上的通信面临以下 4 种威胁：

(1)截获。从网络上窃听他人的通信内容。

(2)中断。有意中断他人在网络上的通信。

(3)篡改。故意篡改网络上传送的报文。

(3)伪造。伪造信息在网络上传送。

所谓主动攻击是指更改信息和拒绝用户使用资源的攻击，攻击者对某个连接中通过的 PDU 进行各种处理。

所谓被动攻击是指截获信息的攻击，攻击者只是观察和分析某一个协议数据单元 PDU 而不干扰信息流。

因此，截获属于被动攻击；而中断、篡改、伪造属于主动攻击。

试题一十七 答案： B **解析：** 根据《系统集成项目管理工程师教程》中“17.2.2 信息系统安全属性”一节关于“可用性”的所述内容，

可用性是应用系统信息可被授权实体访问并按需求使用的特性。即信息服务在需要时，允许授权用户或实体使用的特性，或者是网络部分曼损或需要降级使用时，仍能为授权用户提供有效服务的特性。可用性是应用系统面向用户的安全性能。应用系统最基本的功能是向用户提供服务，而用户的需求是随机的、多方面的、有时还有时间要求。可用性一般用系统正常使用时间和整个工作时间之比来度量。

可用性还应该满足以下要求：身份识别与确认、访问控制(对用户的权限进行控制，只能访问相应权限的资源，防止或限制经隐蔽通道的非法访问。包括自主访问控制和强制访问控制)、业务流控制(利用均分负荷方法，防止业务流量过度集中而引起网络阻塞)、路由选择控制(选择那些稳定可靠的子网、中继线或链路等)、审计跟踪(把应用系统中发生的所有安全事件情况存储在安全审计跟踪之中，以便分析原因，分清责任，及时采取相应的措施。审计跟踪的信息主要包括事件类型、被管信息等级、事件时间、事件信息、事件回答以及事件统计等方面的信息)。

试题一十八 答案： A **解析：** 根据《系统集成项目管理工程师教程》中“17.2.3 信息系统安全管理体系”一节的所述内容，在 GB/T20271-2006 《信息安全技术信息系统通用安全

技术要求》中将信息系统安全技术体系具体描述如下。

(1)物理安全。

①环境安全。

主要指中心机房的安全保护，包括：

•机房场地选择。

•机房内部安全防护。

•机房防火。

•机房供、配电。

•机房空调、降温。

•机房防水与防潮。

•机房防静电。

•机房接地与防雷击。

•机房电磁防护。

②设备安全。

•设备的防盗和防毁。

•设备的安全可用。

③记录介质安全。

运行安全。

①风险分析。

②信息系统安全性检测分析。

③信息系统安全监控。

④安全审计。

⑤信息系统边界安全防护。

⑥备份与故障恢复。

⑦恶意代码防护。

⑧信息系统的应急处理。

⑨可信计算和可信连接技术。

数据安全。

①身份鉴别。

②用户标识与鉴别。

③用于主体绑定。

•隐秘。

•设备标识和鉴别。

④抗抵赖。

•抗原发抵赖。

•抗接收抵赖。

⑤自主访问控制。

•访问控制策略。

•访问控制功能。

•访问控制范围。

•访问控制粒度。

⑥标记。

•主体标记。

•客体标记。

•标记的输出。

•标记的输入。

⑦强制访问控制。

•访问控制策略。

•访问控制功能。

•访问控制范围。

•访问控制粒度。

•访问控制环境。

⑧数据完整性保护。

•存储数据的完整性。

•传输数据的完整性。

•处理数据的完整性。

⑨用户数据保密性保护。

•存储数据保密性保护。

•传输数据保密性保护。

•客体安全重用。

⑩数据流控制。

可信路径。

密码支持。

试题一十九 答案： C **解析：** 根据《系统集成项目管理工程师教程》中“17.5.2 应用系统运行中的安全管理”一节的所述内容，系统安全等级管理是根据应用系统所处理数据的秘密性和重要性确定安全等级，并据此采用有关规范和制定相应管理制度。安全等级可分

为保密等级和可靠性等级两种，系统的保密等级与可靠性等级可以不同。保密等级应按有关规定划为绝密、机密和秘密。可靠性等级可分为三级，对可靠性要求最高的为A级，系统运行所要求的最低限度可靠性为C级，介于中间的为B级。安全等级管理就是根据信息的保密性及可靠性要求采取相应的控制措施，以保证应用系统及数据在既定的约束条件下合理合法的使用。

试题二十 答案： A **解析：** 此题考察的是信息安全知识

数据域安全包括两个层次，其一是行级数据域安全,即用户可以访问哪些业务记录，一般以用户所在单位为条件进行过滤；其二是字段级数据域安全,即用户可以访问业务记录的哪些字段。

试题二十一 答案： B **解析：** 按照GB/T20269-2006《信息安全技术信息系统安全管理要求》，风险分析和评估包括：

•资产识别和分析

对资产识别和分析，不同安全等级应有选择地满足以下要求的一项：

①信息系统的资产统计和分类：确定信息系统的资产范围，进行统计和编制资产清单，并进行资产分类和重要性标识。

②信息系统的体系特征描述：在①的基础上，根据对信息系统的硬件、软件、系统接口、数据和信息、人员等方面的分析和识别，对信息系统的体系特征进行描述，至少应阐明信息系统的使命、边界、功能，以及系统和数据的关键性、敏感性等内容。

•威胁识别和分析

对威胁识别和分析，不同安全等级应有选择地满足以下要求的一项：

①威胁的基本分析：应根据以往发生的安全事件、外部提供的资料和积累的经验等，对威胁进行粗略的分析。

②威胁列表：在①的基础上，结合业务应用、系统结构特点以及访问流程等因素，建立并维护威胁列表；由于不同业务系统面临的威胁是不同的，应针对每个或者每类资产有一个威胁列表。

③威胁的详细分析：在②的基础上，考虑威胁源在保密性、完整性或可用性等方面造成损害，对威胁的可能性和影响等属性进行分析，从而得到威胁的等级；威胁等级也可通过综合威胁GB/T20269—200611的可能性和强度的评价获得。

④使用检测工具捕捉攻击：在③的基础上，对关键区域或部位进行威胁分析和评估，在业务应用许可并得到批准的条件下，可使用检测工具在特定时间捕捉攻击信息进行威胁分析。

•脆弱性识别和分析

对脆弱性识别和分析，不同安全等级应有选择地满足以下要求的一项：

①脆弱性工具扫描：应通过扫描器等工具来获得对系统脆弱性的认识，包括对网络设备、主机设备、安全设备的脆弱性扫描，并编制脆弱性列表，作为系统加固、改进和安全项目建设的依据；可以针对资产组合、资产分类编制脆弱性列表和脆弱性检查表。

②脆弱性分析和渗透测试：在①的基础上，脆弱性的人工分析至少应进行网络设备、安全设备以及主机系统配置检查、用户管理检查、系统日志和审计检查等；使用渗透测试应根据需要分别从组织机构的网络内部和网络外部选择不同的接入点进行；应了解测试可能带来的后果，并做好充分准备；针对不同的资产和资产组合，综合应用人工评估、工具扫描、渗透性测试等方法对系统的脆弱性进行分析和评估；对不同的方法和工具所得出的评估结果，应进行综合分析，从而得到脆弱性的等级。

③制度化脆弱性评估：在②的基础上，坚持制度化脆弱性评估，应明确规定进行脆弱性评估的时间和系统范围、人员和责任、评估结果的分析和报告程序，以及报告中包括新发现的漏洞、已修补的漏洞、漏洞趋势分析等。

试题二十二 答案： D **解析：** 数据库容灾，即在异地部署一个一模一样的数据库，一个数据库所处的地理位置发生自燃灾害了导致当前数据库发生灾难，另一个数据库会立马顶替工作。

试题二十三 答案： A **解析：** 入侵是指在非授权的情况下，试图存取信息、处理信息或破坏系统以使系统不可靠、不可用的故意行为，不属于物理控制的范围。其他三项都属于外在物理方面的访问控制。

试题二十四 答案： B **解析：** 保密性应用系统的信息不被泄露给非授权的用户、实体或过程，或供其利用的特性。应用系统常用的保密技术如下：最小授权原则、防暴露、信息加密、物理保密。

完整性是信息未经授权不能进行改变的特性。即应用系统的信息在存储或传输过程中保持不被偶然或蓄意地删除、修改、伪造、乱序、重放和插入等破坏和丢失的特性。保障应用系统的完整性的主要方法如下：安全协议、纠错编码、密钥校验、数字签名、 公证。

MD5 技术是在数据或文件上生成一个唯一的 md5 码，数据接收者利用一些工具对数据进行校验，确保数据的完整性。

试题二十五 答案： A **解析：** 在概念活动中的可靠性和可维护性管理要求：进行软件可行性分析，制定初步软件开发计划，提出软件可靠性和可维护性分解目标、要求及经费。

在需求活动中的可靠性和可维护性管理要求：分析和确定软件可靠性和可维护性的具体设计目标，确保与研制任务书或合同中相应要求的可追踪性，制定实施计划，制定各实施阶段的基本准则，确定各实施阶段的验证方法。

在设计活动中的可靠性和可维护性管理要求：进行软件可靠性和可维护性分析和设计，编写相应的设计说明，明确对编码、测试阶段的具体要求，组织设计评审，并验证可靠性和可维护性目标的实施和与需求活动中所提相应要求的可追踪性。

在实现活动中的可靠性和可维护性管理要求：按照规定的规则，在软件编码过程中依据需求和设计活动中相应的规定实现可靠性和可维护性要求，进行单元测试，做好后续测试工作的准备，评价或审查代码以验证相应要求的实现。

在测试活动中的可靠性和可维护性管理要求：在单元和集成测试阶段，验证相应可靠性和可维护性要求的实现，进行重用软件的可靠性和可维护性管理。在软件配置项测试和系统集成测试阶段，建立适当的软件可靠性测试环境，组织分析测试和测量的数据，验证软件可靠性和可维护性的实现，进行风险分析，决定交付时机。

在安装和验收活动中的可靠性和可维护性管理要求：采取联合评审、审核、软件合格性测试和系统合格性测试等手段对可靠性和可维护性进行最终验证和评定。

试题二十六 答案： C **解析：** 计算机安全管理中包括人员安全管理，人员安全管理又包括离岗人员安全管理。对人员离岗的管理，可以根据离岗人员的关键程度，采取下列控制措施。

(1）基本要求：立即中止被解雇的、退休的、辞职的或其他原因离开的人员的所有访问权限：收回所有相关证件、徽章、密钥和访问控制标记等，收回机构提供的设备等。

(2）调离后的保密要求：在上述基础上，管理层和信息系统关键岗位人员调离岗位，必须经单位人事部门严格办理调离手续，承诺其调离后的保密要求。

(3）离岗的审计要求：在上述基础上，设计组织机构管理层和信息系统关键岗位的人员调离单位，必须进行离岗安全审查，在规定的脱密期限后，方可调离。

(3）关键部位人员离岗要求：在上述基础上，关键部位的信息系统安全管理人员离岗，应按照机要人员管理办法办理。

试题二十七 答案： C **解析：** 依据 GBAT20271-2006 《信息系统安全技术信息系统通用安全技术要求》中的规定，信息系统安全技术体系包含物理安全、运行安全和数据安全。物理安全也称实体安全，是指包括支持信息系统运行的所有计算机、网络的物理设备、设

施和记录介质在内的所有硬件及其环境的安全。它是对计算机、网络设备、设施、环境、人员等采取适当措施来保证信息系统安全、可靠、不间断运行，并确保其在对信息进行采集、加工、存储、传输等处理过程中，不致因设备、介质和环境条件等受到人为和自然因素的危害，而使信息丢失、泄露或破坏。物理安全是一个信息系统安全运行的物理基础。运行安全，是指在物理安全得到保障的前提下，为确保信息系统安全运行而采取的各种检测、监控、审计、分析、容错备份及故障恢复等技术和措施。这些技术和措施以软、硬件机制、装置或设备的形式，确保信息系统不因人为的攻击、破坏或自然的原因而无法正常运行。

在系统运行安全得到保障的前提下，对在信息系统中存储、传输和处理的数据信息进行有效的保护，使其不因人为的或自然的原因被泄露、篡改和破坏，是数据安全的总体要求。虽然物理安全和运行安全对系统的整体安全有着十分重要的作用，然而，数据安全仍然无可争辩地是信息系统安全保护最主要的内容和最终的目标。实际上，物理安全和运行安全也是对数据安全的支持和保障，而数据安全所采用的技术和措施，对运行安全也会有一定作用，因为作为系统运行主体的软件，本身就是由程序和数据组成的。

试题二十八 答案： D **解析：** 入侵检测设备是对外部入侵进行侦测的设备，一般搭载有入侵检测系统(intrusiondetectionsystem,简称“IDS”)， IDS 是一种对网络传输进行即时监视，在发现可疑传输时发出警报或者采取主动反应措施的网络安全设备。它与其他网络安全设备的不同之处便在于， IDS 是一种积极主动的安全防护技术。

对各种事件进行分析，从中发现违反安全策略的行为是入侵检测系统的核心功能。从技术上，入侵检测分为两类：一种基于标志(signature-based),另一种基于异常情况 (anomaly-based)。

对于基于标志的检测技术来说，首先要定义违背安全策略的事件的特征，如网络数据包的某些头信息。检测主要判别这类特征是否在所收集到的数据中出现，此方法非常类似杀毒软件。而基于异常的检测技术则是先定义一组系统“正常”情况的数值，如 CPU 利用率、内存利用率、文件校验和等(这类数据可以人为定义，也可以通过观察系统、并用统计的办法得出)，然后将系统运行时的数值与所定义的“正常”情况比较，得出是否有被攻击的迹象。这种检测方式的核心在于如何定义所谓的“正常”情况。

两种检测技术的方法，所得出的结论有非常大的差异。基于标志的检测技术的核心是维护一个知识库。对于已知的攻击，它可以详细、准确的报告出攻击类型，但是对未知攻击却效果有限，而且知识库必须不断更新。基于异常的检测技术则无法准确判别出攻击的手法，但它可以(至少在理论上可以)判别更广范，甚至未发觉的攻击。

不同于防火墙， IDS 入侵检测系统是一个监听设备，没有跨接在任何链路上，无须网络流

量流经它便可以工作。因此，对 IDS 的部署，唯一的要求是： IDS 应当挂接在所有所关注流量都必须流经的链路上。在这里，“所关注流量”指的是来自高危网络区域的访问流量和需要进行统计、监视的网络报文。在如今的网络拓扑中，已经很难找到以前的 HUB 式的共享介质冲突域的网络，绝大部分的网络区域都已经全面升级到交换式的网络结构。因此， IDS 在交换式网络中的位置一般选择在：(1)尽可能靠近攻击源：(2) 尽可能靠近受保护资源。这些位置通常是：服务器区域的交换机上、 Internet 接入路由器之后的第一台交换机上。

试题二十九 答案： B **解析：** 代理服务型防火墙是防火墙的一种，代表某个专用网络同互联网进行通讯的防火墙。当你将浏览器配置成使用代理功能时，防火墙就将你的浏览器的请求转给互联网：当互联网返回响应时，代理服务器再把它转给你的浏览器。代理服务器也用于页面的缓存，代理服务器在从互联网上下载特定页面前先从缓存器取出这些页面。内部网络与外部网络之间不存在直接连接，主要在应用层实现。当代理服务器收到一个客户的连接请求时，先核实该请求，然后将处理后的请求转发给真实服务器，在接受真实服务器应答并做进一步处理后，再将回复交给发出请求的客户。代理服务器在外部网络和内部网络之间，发挥了中间转接的作用。所以，代理服务器有时也称作应用层网关。
代理服务器可对网络上任一层的数据包进行检查并经过身份认证，让符合安全规则的包通过，并丢弃其余的包。它允许通过的数据包由网关复制并传递，防止在受信任服务器和客户机与不受信任的主机间直接建立联系。
代理服务器型防火墙，则是利用代理服务器主机将外部网络和内部网络分开。从内部发出的数据包经过这样的防火墙处理后，就像是源于防火墙外部的网卡一样，从而可以达到隐藏内部网络结构的作用。内部网络的主机，无需设置防火墙为网关，只需直接将需要服务的 IP 地址指向代理服务器主机，就可以获取 Internet 资源。
使用代理服务器型防火墙的好处是。它可以提供用户级的身份认证、日志记录和账号管理，彻底分隔外部与内部网络。但是，所有内部网络的主机均需通过代理服务器主机才能获得 Internet 上的资源，因此会造成使用上的不便，而且代理服务器很有可能会成为系统的“瓶颈”。

试题三十 答案： D **解析：** 在组织机构中需建立安全管理机构，不同安全等级的安全管理机构可按下列顺序逐步建立自己的信息系统安全组织机构管理体系。
①配备安全管理人员：管理层中应有一人分管信息系统安全工作，并为信息系统的安全管理配备专职或兼职的安全管理人员。
②建立安全职能部门：在①的基础上，应建立管理信息系统安全工作的职能部门，或者明

确指定一个职能部门监管信息安全工作，作为该部门的关键职责之一。
③成立安全领导小组：在②的基础上，应在管理层成立信息系统安全管理委员会或信息系统安全领导小组，对覆盖全国或跨地区的组织机构，应在总部和下级单位建立各级信息系统安全领导小组，在基层至少要有一位专职的安全管理人员负责信息系统安全工作。
④主要负责人出任领导：在③的基础上，应由组织机构的主要负责人出任信息系统安全领导小组负责人。
⑤建立信息安全保密管理部门：在④的基础上，应建立信息系统安全保密监督管理的职能部门，或对原有保密部门明确信息安全保密管理责任，加强对信息系统安全管理重要过程和管理人员的保密监督管理。

试题三十一 答案： B **解析：** 加密算法有两种类型。加密和解密函数都使用同一个密钥，则这个算法是“对称的”。
常见的对称密钥算法有： DES 、 TripleDES 、 RC2 、 RC4 、 RC5 和 Blowfish 等。
使用两个不同但是相关的密钥来执行加密和解密。用于加密的密钥称为“公钥”， 用于解密的密钥称为“私钥”。这种算法称为“非对称密钥算法”。
常见的非对称密钥算法有： RSA(基于大数分解)、 Elgamal 、背包算法、 Rabin, D-H 、ECC (椭圆曲线加密算法)。

试题三十二 答案： A **解析：** 应用安全，就是针对应用程序或工具在使用过程中可能出现计算、传输数据的泄露和失窃，通过其他安全工具或策略来消除隐患。
物理安全是指为了保证计算机系统安全、可靠地运行，确保系统在对信息进行采集、传输、存储、处理、显示、分发和利用的过程中不会受到人为或自然因素的危害而使信息丢失、泄漏和破坏，对计算机系统设备、通信与网络设备、存储媒体设备和人员所采取的安全技术措施。实体安全包括环境安全，设备安全和媒体安全三个方面。
环境安全包括受灾防护、区域防护；设备安全包括设备防盗、设备防毁、防止电磁信息泄露、防止线路截获、抗电磁干扰、电源保护等；媒体安全是媒体数据和媒体本身。

试题三十三 答案： A **解析：** 保密性是应用系统的信息不被泄露给非授权的用户、实体或过程，或供其利用的特性。即防止信息泄漏给非授权个人或实体，信息只为授权用户使用的特性。

试题三十四 答案： C **解析：** 访问控制包括对用户的权限进行控制，只能访问相应权限的资源，防止或限制经隐蔽通道的非法访问。包括自主访问控制和强制访问控制。既包括对外部网络的访问控制，也包括对内部网络的访问控制。

试题三十五 答案： B **解析：** 依据《信息安全等级保护管理办法》第七条，信息系统的安全保护等级分为五级。
5 个等级：用户自主保护级、系统审计保护级、安全标记保护级、结构化保护级、访问验证保护级。

试题三十六 答案： B **解析：** 机房应进行静电防护处理，地面铺设防静电地板。供电系统应将计算机系统供电和其他供电分开。标记应明确。机房隔壁不应为卫生间或水房。

试题三十七 答案： C **解析：** 对称加密算法的特点是算法公开、计算量小、加密速度快、加密效率高。对称加密算法的优点在于加解密的高速度和使用长密钥时的难破解性。

试题三十八 答案： B **解析：** 母公司的资质不能代替子公司的资质，因此投标文件不符合招标要求。

试题三十九 答案： B **解析：** 本题考察堡垒主机的知识。堡垒主机既然是一台完全暴露给外网的主机，那肯定是不需要防火墙来保护了的。它没有任何防火墙或者包过虑路由器设备保护。

试题四十 答案： B **解析：** 本题考察计算机网络安全知识。网络安全主要用于保证网络的可用性，以及网络中所传输的信息的完整性和机密性。

试题四十一 答案： C **解析：** 本题考察计算机安全知识。系统运行安全检查与记录不包括检查应用系统的用户权限分配是否遵循易用性原则。

试题四十二 答案： C **解析：** P4
完整性(Integrity),是指“保护资产的正确和完整的特性”。简单地说，就是确保接收到

的数据就是发送的数据。数据不应该被改变，这需要某种方法去进行验证。确保数据完整性的技术包括： CA 认证；数字签名；防火墙系统；传输安全(通信安全)；入侵检测系统。

试题四十三 答案： A 解析： P537

应用系统运行中涉及的安全和保密层次包括系统级安全、资源访问安全、功能性安全和数据域安全 4 个层次，系统级安全是应用系统的第一道防护大门。

试题四十四 答案： B 解析： P534

本题考查的是岗位安全考核与培训基础知识。出自《系统集成项目管理工程师教程(第 2 版)》第 18 章 信息系统安全管理，全书第 534 页。

多人共管要求：在上述基础上，关键岗位人员处理重要事务或操作时，应保持二人同时在场，关键事务应多人共管。

试题四十五 答案： D 解析： P537

本题考查的是信息系统安全管理基础知识。出自《系统集成项目管理工程师教程(第 2 版)》第 17 章 信息系统安全管理，全书第 537 页。

系统运行安全与保密的层次构成

应用系统运行中涉及的安全和保密层次包括系统级安全、资源访问安全、功能性安全和数据域安全。这 4 个层次的安全，按粒度从粗到细的排序是：系统级安全、资源访问安全、功能性安全、数据域安全。程序资源访问控制安全的粒度大小界于系统级安全和功能性安全两者之间，是最常见的应用系统安全问题，‘几乎所有的应用系统都会涉及这个安全问题。

(l)系统级安全。

企业应用系统越来越复杂，因此制定得力的系统级安全策略才是从根本上解决问题的基础。应通过对现行系统安全技术的分析，制定系统级安全策略，策略包括敏感系统的隔离、访问 m 地址段的限制、登录时间段的限制、会话时间的限制、连接数的限制、特定时间段内登录次数的限制以及远程访问控制等，系统级安全是应用系统的第一道防护大门。

(2)资源访问安全。

对程序资源的访问进行安全控制，在客户端上，为用户提供和其权限相关的用户界面，仅出现和其权限相符的菜单和操作按钮：在服务端则对 URL 程序资源和业务服务类方法的调用进行访问控制。

(3)功能性安全。

功能性安全会对程序流程产生影响，如用户在操作业务记录时，是否需要审核，上传附件不能超过指定大小等。这些安全限制已经不是入口级的限制，而是程序流程内的限制，在一定程度上影响程序流程的运行。

(3)数据域安全。

数据域安全包括两个层次，其一是行级数据域安全，即用户可以访问哪些业务记录，一般以用户所在单位为条件进行过滤；其二是字段级数据域安全，即用户可以访问业务记录的哪些字段。不同的应用系统数据域安全的需求存在很大的差别，业务相关性比较高。对于行级的数据域安全，大致可以分为以下几种情况：

①应用组织机构模型允许用户访问其所在单位及下级管辖单位的数据。

②通过数据域配置表配置用户有权访问同级单位及其他行政分支下的单位的数据。

③按用户进行数据安全控制，只允许用户访问自己录入或参与协办的业务数据。

④除进行按单位过滤之外，比较数据行安全级别和用户级别，只有用户的级别大于等于行级安全级别，才能访问到该行数据。

试题四十六 答案： D **解析：** P572

本题考查的是网络安全基础知识。出自《系统集成项目管理工程师教程(第 2 版)》第 3 章信息系统集成专业技术知识，全书第 159 页。

网络安全工具包括安全操作系统、应用系统、防火墙、网络监控、扫描器、防毒软件、安全审计系统。

技术安全体系描述具体包括：物理安全、运行安全和数据安全，其中运行安全包括： 1. 风险分析； 2. 安全性监测分析； 3. 信息系统安全监控； 4. 安全审计； 5. 防护； 6. 备份与恢复。

试题四十七 答案： C **解析：** P525

本题考查的是信息安全等级保护基础知识。出自《系统集成项目管理工程师教程(第 2 版)》第 17 章 信息系统安全管理，全书第 541 页。

第三级，信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。

试题四十八 答案： B **解析：** 参考教程 P158，信息安全的基本要素，

机密性：确保信息不暴露给未授权的实体或进程；

完整性：只有得到允许的人才能修改数据，并且能够判别出数据是否已被篡改

可用性：得到授权的实体在需要时可访问数据，即攻击者不能占用所有的资源二阻碍授权者的工作。

分布式拒绝服务(DDoS:DistributedDenialofService)攻击指借助于客户/服务器技术，将多个计算机联合起来作为攻击平台，对一个或多个目标发动 DDoS 攻击，从而成倍地提高拒绝服务攻击的威力。

拒绝服务攻击，针对的目标正是“可用性”。该攻击方式利用目标系统网络服务功能缺陷或者直接消耗其系统资源，使得该目标系统无法提供正常的服务。

试题四十九 答案： C **解析：** 参考教程 P535，岗位安全考核与培训；关键岗位“权限分散、不得交叉覆盖”的原则，系统管理员、数据库管理员、网络管理员不能相互兼任岗位或工作。

试题五十 答案： A **解析：** 参考第二版教材 P534 岗位安全考核与培训

对信息系统岗位人员的管理，应根据其关键程度建立相应的管理要求。

(1)对安全管理员、系统管理员、数据库管理员、网络管理员、重要业务开发人员、系统维护人员和重要业务应用操作人员等信息系统关键岗位人员进行统一管理:允许一人多岗，但业务应用操作人员不能由其他关键岗位人员兼任:关键岗位人员应定期接受安全培训，加强安全意识和风险防范意识。

(2)兼职和轮岗要求:业务开发人员和系统维护人员不能兼任或担负安全管理员、系统管理员、数据库管理员、网络管理员和重要业务应用操作人员等岗位或工作:必要时关键岗位人员应采取定期轮岗制度。

(3)权限分散要求:在上述基础上，应坚持关键岗位“权限分散、不得交叉覆盖”的原则，系统管理员、数据库管理员、网络管理员不能相互兼任岗位或工作。

(3)多人共管要求:在上述基础上，关键岗位人员处理重要事务或操作时，应保持二人同时在场，关键事务应多人共管。

(5)全面控制要求:在上述基础上，应采取对内部人员全面控制的安全保证措施，对所有岗位工作人员实施全面安全管理。

试题五十一 答案： C **解析：** 本题考查网络安全，参考集成第二版教程 P158 。除了对数据的攻击外，还有一种叫“拒绝服务”攻击，即通过控制网络上的其他机露，对目标主机所在网络服务不断进行干扰，改变其正常的作业流程，执行无关程序使系统响应减慢甚

至瘫痪，影响正常用户的使用，甚至使合法用户被排斥而不能进入计算机网络系统或不能得到相应的服务。

试题五十二 答案： D **解析：** P158，完整性：只有得到允许的人才能修改数据，并且能能够判别出数据是否已被篡改。可用性：得到授权的实体在需要时可访问数据，即攻击者不能占用所有的资源而

阻碍授权者的工作。

试题五十三 答案： B **解析：** P

在 ISO/IEC 27000 系列标准中,它将信息安全管理的内容主要概括为如下 14 个方面：信息安全方针与策略；组织信息安全；人力资源安全；资产安全；访问控制；密码；物理和环境安全；运行安全；通信安全；信息系统的获取、开发和保持；供应商关系；信息安全事件管理；业务持续性管理；符合性；

试题五十四 答案： B **解析：** P534

权限分散要求：应坚持关键岗位“权限分散、不得交叉覆盖”的原则，系统管理员、数据库管理员、网络管理员不能相互兼任岗位或工作。

试题五十五 答案： D **解析：** P534

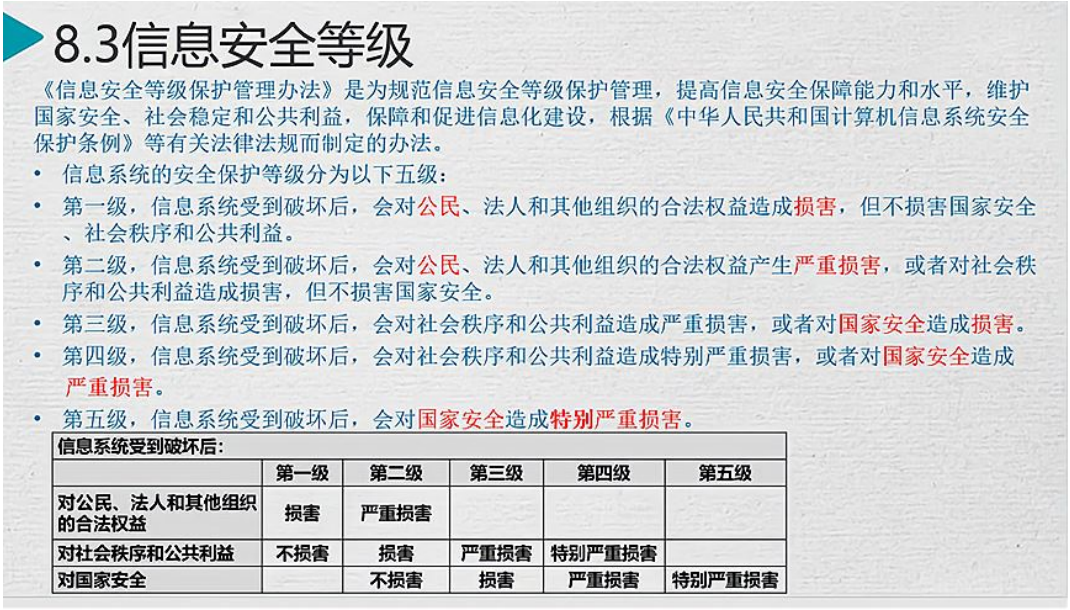
对人员离岗的管理，可以根据离岗人员的关键程度，采取下列控制措施。

(1）基本要求：立即中止被解雇的、退休的、辞职的或其他原因离开的人员的所有访问权限；收回所有相关证件、徽章、密钥和访问控制标记等；收回机构提供的设备等。

(2）调离后的保密要求：在上述基础上，管理层和信息系统关键岗位人员调离岗位，必须经单位人事部门严格办理调离手续，承诺其调离后的保密要求。

(3）离岗的审计要求：在上述基础上，涉及组织机构管理层和信息系统关键岗位的人员调离单位，必须进行离岗安全审查，在规定的脱密期限后，方可调离。

试题五十六 答案： C **解析：** P541



试题五十七 答案： 解析： 【问题 1 】（10 分）

1 、沟通管理计划编制得不完善。

2 、沟通管理计划不能只由张伟一人制定。

3 、沟通管理计划没有经过评审，没有告知所有干系人。

4 、管理沟通做得不好，没有按沟通计划执行沟通工作。

5 、控制沟通做得不好，对存在的沟通问题没有及时发现和解决 6 、没有制定干系人管理计划

7 、干系人的分类存在问题，不应该将 A 公司业务部分人员分为一般干系人 8 、管理干系人存在问题，没有与之及时沟通，导致出现投诉。

（每条 2 分，最多 10 分）

【问题 2 】（6 分）

A 公司管理层：重点管理，及时报告。因为 A 公司管理层权利高，利益高。（2 分）

B 公司行政部门：令其满意，因为 B 公司行政部门权力高，利益低。（2 分）

A 公司业务部门人员：随时告知，因为 A 公司业务部门人员权力低，利益高。（2 分）

【问题 3 】（3 分）

① 交互式沟通(1 分)

② 推式沟通(1 分)

③ 拉式沟通(1 分)