CIA考试辅导：从控制角度来看信息系统构成内审师资格考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/639/2021_2022_CIA_E8_80_83_E8_AF_95_E8_c53_639052.htm 1、一般控制：管理控制/系统实施控制/运行控制/软件控制/硬件控制/物理访问控制/逻辑访问控制 2、应用控制：输入控制/处理控制/输出控制 3、保障控制：灾难恢复与应急计划/环境控制/设备来源控制 1、信息系统的战略、政策和过程 1.1信息系统的战略性应用目标：战略、政策、过程：通过应用信息系统，达到改进组织的目标、经营和服务或组织与环境的关系，从而帮助组织改善与客户的关系，取得竞争优势。战略性的应用系统渗透于业务层、企业层及行业层面 1.2信息系统的应用推动组织结构变革：自动化/流程合理话/业务流程再造/异化 1.3信息系统应用模式的演变：主机/终端模式客户机/服务器模式浏览器/服务器模式 与信息应用模式相关的问题：降型化/开放系统/遗产系统 1.4信息系统的功能分类： 作业层（事物处理系统TPS）知识层（知识工作系统KWS/办公自动户化系统OAS）管理层（管理信息系统MIS/决策支持DSS）战略层（高级经理支持系统ESS） 1.5信息系统部门的职责 系统开发小组（系统分析员是联络的桥梁、设计、编程、测试）系统运行小组（确保正常运行/帮助平台、咨询） 1.6信息系统安全主管的责任 信息系统高层管理人员的职责：评估风险/控制成本/制定风险控制目标与措施 信息安全主管的职责：制定安全政策/评价安全控制/检测调查不成功的访问企图/监督特权用户的访问 1.7新兴技术人工智能：专家系统（商品赊销的审批、医疗专家系统）/神经网络（超音速飞机的控制系统、电力系统负荷预

测）/模糊逻辑（人像识别系统）/遗传算法（煤气管道控制、机器人控制）/智能代理（互联网搜索引擎、电子邮件过滤器） 1.8第三方服务机构的角色 设备管理机构（按用户要求运行、维护数据处理）计算机租赁公司（只提供设备）服务局（管理运行自己的数据处理设备，用户只需求提供数据，根据服务结果付费）共享服务商（管理运营自己的数据处理设备、使各类组织可以使用他们的系统） 2、硬件、平台、网络与远程通讯 2.1各种计算机媒体：磁带（容量大、价格低顺序存储）、磁带库（容纳多盘磁带、机械臂抓取）、软盘（直接存取、便于携带）、硬盘（直接存取、速度快、容量大）、廉价冗余磁盘阵列/廉价光盘重复排列（重构数据、容错能力强）、CD-ROM（保存数字文件容量大、便宜、不能写入）、光盘库（容纳多个光盘）、一次写多次读光盘（WORM适用不须更新、记录内容） 2.2计算机类型：个人计算机/工作站/网络计算机 2.3各类计算机外部设备：不间断电源/光学字符识别/打印机/扫描仪/绘图仪/条码阅读器 2.4外部接口：串口/并口/USB口 2.5操作系统：分配、调度、监视系统资源，保证雇员只对被授权的数据进行读写访问DOA/UNIX/VMS 2.6监视器：辨别硬件的瓶颈和软件设计问题/调整运行负荷/发现网络反应时间恶化情况 2.7图形化用户接口：用鼠标点击图形来输入命令如WINDOWS 2.8大型计算机的使用：影响大型计算机运行速度的因素有：应用软件的是设计效率/数据库管理软件的效率/数据的结构网络容量及传输速度/系统负荷/存储器容量/安全检查及备份的频率/软件初始化选择的正确性 2.9个人计算机与大型计算机的接口：通过局域网连接、口令登陆 终端仿真的风险：雇员利用微机

谋取私利/备份不充分/拷贝供个人使用/保存登录序列的文献/任何能访问PC机的人员都可以访问主机。 2.10计算机网络的分类：广域网（覆盖广、速度慢）/局域网（范围小、速度快）/城域网（城市内部高速网） 广域网：专用网络/虚拟专用网/公用交换网络/增值网 局域网：总线网/星型网/环型网或者分为：基于服务器的网络/对等网 2.11网络连接设备：网卡/调制解调器/中绩器/集线器/网桥/网关/路由器 2.12因特网：资源无限，缺点：难以定位最好的资源功能：网络浏览器WEB/电子邮件EMAIL/远程登录TELNET/专题论坛USENET/电子公告牌BBS/其他 2.13数据传输模式：异步传输（利用额外的启动位与停止位同步数据传输/慢，有间隔）/同步传输（同步时钟同步数据传输，快、可连续传输） 各种基础通信网络：公用电话交换网（拨号上网）/DDN数字数据网络/桢中继（降局域网和其他局域网连接，使不很敏感的数据传递）/综合服务数字网ISDN/非对称数字环线ADSL 3、数据处理 3.1个人计算机软件：字处理软件/电子表格/图象处理软件/财务管理/管理软件/光学字符识别软件 3.2程序执行方式：直接执行：语言程序（编译）目标代码（连接）可执行代码（执行）程序运行 解释执行：语言程序（由解释程序转换二进制玛）程序运行 3.3语言类型：机器语言/汇编语言/过程化语言/非过程化语言 3.4文件类型：直接存取文件/顺序文件/索引文件主文件与事务文件/平面文件 3.5数据处理方式：批处理/在线处理或分集中处理/分散处理/分布处理 3.6常用计算机审计技术：测试数据（检查信息系统是否正常）/平行模拟（模拟系统与真实系统比较结果）/继承集成测试（虚构测试数据与真实数据一起处理，缺点：测试数据可能进入委托人的真实数据环境

）/嵌入审计模块（连续监督）/其他技术（电脑化帐务处理系统自动平帐） 3.7关系型数据库的操作：选择（条件选择出记录子集）/连接（按某个共同数据元素结合多个关系型数据库）/映射（将数据库中的部分字段构成新的子表）/修改（锁定/死锁） 3.8数据定义语言：描述数据库内容与结构的语言（建立数据库表结构） 数据操纵语言：修改、操作、插入、查询 数据字典：对数据结构的定义 3.9分布式数据库在各接点的分布方法：快照/复制/分割 数据组织与查询：结构化查询语言（不会对数据库产生风险）/管理查询设施（用于趋势图、制作图表）P304管理查询设施，把“ 数据有效性检查 ”去掉，无法检查数据有效性/；逻辑视图/数据挖掘（分析，发现隐藏在数据后的规律） 3.10电子资金转帐系统（EFT） 风险：未经许可的进入和操作/对交易的重复处理/缺乏备份和恢复能力/未经授权的访问和交易活动风险最大 优势：交易处理成本比手工低/改善与贸易伙伴的业务关系/减少数据错误/提高工作效率 实施第一步：画出未实现组织目标所开展的经营活动的流程图 目标：改善业务关系，提高竞争力 EDI的风险：数据网整形和随意存取数据是EDI的固有风险/数据交换过程中的遗漏、错序或重复、向交易伙伴传输交易信息有时不成功。 EDI的风险防范：应用数据签名技术/给EDI文件顺序编号/通过对方的反馈来确认 4、系统开发获得和维护 4.1系统开发生命周期法（系统、规范、严密）/（快速）原型法（不断修改直至满意，缺点，不系统，不正规） 4.2系统开发的主要活动：系统分析系统设计系统编程测试转换系统维护 系统分析：要解决问题的分析/用户分析和系统可行性分析/系统分析员是信息系统和其他业务部门联系桥梁能力计划《

系统需求分析规格书》 系统设计：逻辑设计/物理设计《系统设计规格书》 系统编程：将设计规格书转化成计算机软件代码的过程《软件程序代码》 在软件需求与设计阶段审计师关注点：需求阶段安全需求是否完备，能否保证信息系统机密、完整、可用，是否有足够的审计踪迹/审计设计阶段检查安全需求是否有足够的控制已集成到系统定义和测试计划中，连续性在线审计功能是否集成到系统中/在系统设计阶段的基线上是否建立变动控制/检查相关文档是否齐全 测试：模块测试/系统测试/验收测试 转换：平行转换/直接转换/试点转换/分阶段的转换策略 4.3内部审计师对信息系统开发的参与 参与方式：连续参与开发/在系统开发结束时参与/在系统实施后参与 连续参与的好处：最大限度地降低系统重新设计的成本 4.4系统维护与变动的控制： 程序变动控制：经管理层批准/经全面测试并保存文档/必须留下何人、何时、何事的线索 修改软件的风险：使用未经审查、测试的修改软件，使被处理信息的可靠性减弱 4.5最终用户开发的风险 系统分析功能被忽略/难集成/系统内产生专用信息系统/缺乏标准和文档，使用和维护都依赖开发者/缺乏监督，失去数据一致性 4.6降低最终用户开发的风险：成立信息中心/集中系统开发专家对用户进行培训/提个开发工具与指导，协助建立质量标准/信息中心直接参与系统分析与设计/对终端用户开发的审计（确定终端用户开发的程序对应用程序进行风险排序对控制情况进行文件处理与测试） 4.7软件许可问题： 使用盗版软件的危害（违法/易感染病毒）/防止使用非法软件的方法（建立制度/版权法教育/定期鉴别/专人保管安装盘）/非法软件的发现（比较采购记录与可执行文件/比较序列号） 5、信息系统安全 5.1

常见攻击手段：黑客/阻塞/窃听/重演/诈骗/中断/病毒 5.2不同层次的信息系统安全控制：一般控制/应用控制 一般控制：管理控制：制定政策与程序/职责分离系统实施控制：开发实施过程中建立控制点编制文档/运行控制：数据存储、运行规范化要求，例如在对不需要的文件要在授权条件下及时删除，管理系统操作、性能监测、系统备份、审计日志__软件控制：未经许可不得修改、在独立的计算机上测试所有的要进入生产环境的软件硬件控制：保证正常运行：回拨检测、奇偶校验访问控制（重点）：标识/口令/授权/访问日志/自动注销登录/回拨/对工具软件的限制 5.3访问控制的类型：标识（唯一确定用户身份）/口令（弱控制）/授权（建立访问控制表预防未经授权访问修改敏感信息）/访问日志（检测性控制措施）/回拨（保护信息按指定路径传送）/自动注销登录（防止通过无人照管的终端来访问主机敏感信息）/对工具软件的限制 5.4加密和解密算法和密钥加密密钥和解密密钥公钥和私钥数字证书数字签名认证中心 5.5电子邮件的安全控制：禁止用EMAIL发送高度敏感或机密信息/加密/限使用数量/工作终端的商用电子邮件保存备查/归档和分级管理。 5.6防火墙：数据包过滤型/应用网关开型 5.7应用软件控制：：输入控制（输入授权、数据转换、编辑检验）处理控制（运行总数、计算机匹配、并发控制）、输出控制输出控制（平衡总数、复核日志、审核报告、审核制度文件） 5.8计算机的物理安全：保证传输线路的安全以防止非法访问网络/尽量不要暴露数据中心的位置以防止恐怖分子袭击/不间断电源可以在停电时维持电脑系统的运行/防火防潮/生物统计访问系统 5.9应急计划：故障弱化保护/灾难恢复计划第一步风险分析，其次才

识策略、文档、计划执行测试等/灾难恢复计划的一个重要组成部分是备份和重新启动程序/当组织的结构和运营发生改变时，灾难恢复计划必须随之改变以保证恢复计划的及时有效。