**信息安全管理体系培训**

**习**

**题**

**汇**

**编**

**目 录**

**练习题一单项选择题 ………………………………………….1**

**练习题二多项选择题 …………………………………………19**

**练习题三判断题 …………………………………………….27**

**练习题四案例分析题.......................................................29**

**ISMS 测验一 ...............................................................35**

**ISMS 测验二 ...............................................................49**

**ISMS测验三 ...............................................................52**

**练习题一参考答案 ......................................................60**

**练习题二参考答案 ......................................................61**

**练习题三参考答案 ......................................................61**

**练习题四参考答案 ......................................................62**

**ISMS测验一参考答案 .................................................63**

**ISMS测验二参考答案 .................................................64**

**ISMS测验三参考答案 .................................................64**

**练习题一单项选择题**

**从下面各题选项中选出一个最恰当的答案，并将相应字母填在下表相应位置中。**

1、ISMS文件的多少和详细程度取于D

(A)组织的规模和活动的类型 (B)过程及其相互作用的复杂程度

(C)人员的能力 (D) A+B+C

2、对于所釘拟定的纠正和预防措施，在实施前应通过（ B ）过程进行评审。

(A)薄弱环节识别 （B)风险分析

(C)管理方案 （D） A+C (E) A+B

3、组织机构在建立和评审ISMS时，应考虑（E ）

(A)风险评估的结果 （B）管理方案

(C)法律、法规和其它要求 （D） A+B (E) A+C

4、ISMS管理评审的输出应包括(C )

(A)可能影响ISMS的任何变更

(B)以往风险评估没有充分强调的脆弱点或威胁

C)风险评估和风险处理计划的更新

(D)改进的建议

5、在信息安全管理中进行（B ），可以有效解决人员安全意识薄弱问题。

(A)内容监控 (B)安全教育和培训

(C)责任追查和惩处 (D)访问控制

6、经过风险处理后遗留的风险是( D )

（A）重大风险 (B)有条件的接受风险

（C）不可接受的风险 （D）残余风险

7、( A )是指系统、服务或网络的一种可识别的状态的发生，它可能是对信息安全策略的违反或防护措施的失效，或是和安全关联的一个先前未知的状态。

（A)信息安全事态 （B)信息安全事件

（C)信息安全事故 （D)信息安全故障

8、系统备份与普通数据备份的不同在于，它不仅备份系统屮的数据，还备份系统中安装的应用程序、数据库系统、用户设置、系统参数等信息，以便迅速（ D）。

（A）恢复全部程序 （B)恢复网络设置

（C）恢复所有数据 (D)恢复整个系统

9、不属于计算机病毒防治的策略的是（ D ）

（A）确认您手头常备一张真正“干净”的引导盘

（B）及时、可靠升级反病毒产品

（C）新购置的计算机软件也要进行病毒检测

（D）整理磁盘

10、抵御电子邮箱入侵措施中，不正确的是( D)

（A）不用生日做密码 （B）不要使用少于5位的密码

（C）不要使用纯数字 （D）自己做服务器

11、不属于常见的危险密码是（D）

（A）跟用户名相同的密码 （B）使用生日作为密码

（C）只有4位数的密码 （D）10位的综合型密码

12、在每天下午5点使计算机结束时断开终端的连接属于（ A）

（A）外部终端的物理安全 （B）通信线的物理安全

（C）窃听数据 （D）网络地址欺骗

13、不属于WEB服务器的安全措施的是 （ D）

(A)保证注册帐户的时效性 (B)删除死帐户

(C )强制用户使用不易被破解的密码 (D)所有用户使用一次性密码

14、1999年，我国发布的第一个信息安全等级保护的国家标准GB 17859-1999，提出将信息系统的安全等级划分为（ D）个等级，并提出每个级别的安全功能要求。

（A) 7 (B) 8 (C) 6 (D) 5

15、文件初审是评价受审方ISMS文件的描述与审核准则的（D ）

（A)充分性和适宜性 （B)有效性和符合性

（C)适宜性、充分性和有效性 （D)以上都不对

16、在认证审核时，一阶段帝核是（C）

(A)是了解受审方ISMS是否正常运行的过程 (B)是必须进行的

(C)不是必须的过程 (D)以上都不准确

17、末次会议包括（D）

（A）请受审核方确认不符合报告、并签字 （B）向审核方递交审核报告

（C）双方就审核发现的不同意见进行讨论 （D）以上都不准确

18、审核组长在末次会议上宣布的审核结论是依据（E）得出的。

( A)审核目的 ( B)不符合项的严重程度

(C)所有的审核发现 (D) A+B (E) A+B+C

19、将收集到的审核证据对照（ C）进行评价的结果是审核发现。

(A)GB/T 22080标准 （B）法律、法规要求

(C)审核准则 （D)信息安全管理体系文件

20、审核准则有关的并且能够证实的记录、事实陈述或其他信息称为（B）

（A）信息安全信息 （B)审核证据

（C）检验记录 （D)信息源

21、现场审核吋间应该包括（B）

(A)文件评审时间 （B)首、末次会议的时间

(C)编写审核报告的时间 （D)午餐时间

22、在第三方认证审核时，（C）不是审核员的职责。

(A)实施审核 （B)确定不合格项

(C)对发现的不合格项采取纠正措施

(D)验证受审核方所采取纠正措施的有效性

23、审核的工作文件包括（ D）。

(A)检杳表 （B)审核抽样计划

(C)信息记录表格 （D) a+b+c

24、在市核中发现了正在使用的某个文件，这是（B）。

(A)审核准则 （B)审核发现

(C)审核证据 （D)車核结论

25、下列说法不正确的是（C）。

（A）审核组可以由一名或多名审核员组成

（B）至少配备一名经认可具有专业能力的成员

（C）实习审核员可在技术专家指导下承担审核任务

（D）审核组长通常由高级审核员担任

26、现场审核的结束是指（A）。

(A)末次会议结束 （B)对不符合项纠正措施进行验证后

(C)发了经批准的审核报告时 （D)监督审核结束

27、信息安全管理体系中提到的“资产责任人”是指：（ C）

(A)对资产拥有财产权的人。 （B)使用资产的人。

(C)有权限变更资产安全属性的人。（D)资产所在部门负责人。

28、组织应给予信息以适当级别的保护，是指：（B）

(A)应实施尽可能先进的保护措施以确保其保密性。

(B)应按信息对于组织业务的关键性给予充分和必要的保护。

(C)应确保信息对于组织内的所有员工可用。

(D)以上都对。

29、认证审核时，审核组应：（A）

(A)在审核前将审核计划提交受审核方确认。

(B)在审核结朿时将帘核计划提交受屯核方确认。

(C)随着审核的进展与受审核方共同确认审核计划。

(D)将审核计划提交审核委托方批准即可。

30、考虑设备安全是为了：（D ）

(A)防止设备丢失、损坏带来的财产损失。

(B)有序保障设备维修时的备件供应。

(C)及时对设备进行升级和更新换代。

(D)控制资产的丢失、损坏、失窃、危及资产安全以及组织活动中断的风险。

31、信息处理设施的变更管理不包括：（D)

(A)信息处理设施用途的变更。

(B)信息处理设施故障部件的更换。

(C)信息处理设施软件的升级。

(D)以上都不对。

32、定期备份和测试信息是指：（ C）

(A)每次备份完成吋对备份结果进行检査，以确保备份效采。

(B)对系统测试记录进行定期备份。

(C)定期备份，定期对备份数据的完整性和可用性进行测试。

(D)定期检查备份存储介质的容量。

1. 一个组织或安全域内所有信息处理设施」；；已设精确时钟源同步是为了：（B

(A)便于针对使用信息处理设施的人员计算工时

(B)便于探测未经授权的信息处理活动的发生

(C)确保信息处理的及时性得到控制

(D)人员异地工作时统一作息时间。

34、第三方认证审核时，对于审核提出的不符合项，审核组应：（B )

(A)与受审核方共同评审不符合项以确认不符合的条款。

(B)与受审核方共同评审不符合项以确认不符合事实的准确性。

(C)与受审核方共同评审不符合以确认不符合的性质。

(D)以上都对。

35、为防止对网络服务的未授权访问，组织应：（ A)

(A)制定安全策略，确保用户应仅能访问已获专门授权使用的服务。

(B)禁止内部人员访问互联网。

(C)禁止外部人员访问组织局域网。

(D)以上都对。

36、组织应进行安全需求分析，规定对安全控制的要求，由( D)

(A)组织需建立新的信息系统时；

(B)组织的原有信息系统扩容或升级时；

(C)组织向顾客交付软件系统时；

(D)A+B

37、确定资产的可用性要求须依据：（A ）

(A)授权实体的需求。 (B)信息系统的实际性能水平。

(C)组织可支付的经济成本。 (D)最高管理者的决定。

38、残余风险是：（ C）

(A)低于可接受风险水平的风险。 (B)高于可接受风险水平的风险。

(C)经过风险处置后剩余的风险。 (D)未经处置的风险。

39、国家对于经背性互联网信息服务实施：（B）

(A)备案制度。 (B)许可制度。

(C)行政监管制度。 (D)备案与行政监管相结合的管理制度。

40、网络路由控制应遵从：（C）

(A)端到端连接最短路径策略；

(B)信息系统应用的最佳效率策略；

(C)确保计算机连接和信息留不违反业务应用的访问控制策略；

(D)A+B+C0

41、认证审核初审时，可以不进行第一阶段现场审核的条件之一是：（ B）

(A)审核组考虑时间效率可用一个阶段审核完成所有的审核准则要求。

(B)审核组长己充分了解受审核方的信息安全管理过程。

(C)受审核方认为一个阶段的审核能完成全部的审核要求。

(D)不允许第一阶段不进行现场审核的情况。

42、对于第三方服务提供方，以下描述正确的是：（ B）

(A)为了监视和评审第三方提供的服务，第三方人员提供服务时应有人员全程陪同。

(B)应定期度量和评价第三方遵从商定的安全策略和服务水平的程度。

(C)第三方服务提供方应有符合ITIL的流程。

(D)第三方服务的变更须向组织呈报以备案。

43、为了确保布缆安全，以下正确的做法是：（ D）

(A)使用同一电缆管道铺设电源电缆和通信电缆。

(B)网络电缆采用明线架设，以便于探查故障和维修。

(C)配线盘应尽量放置在公共可访问区域，以便于应急管理。

(D)使用配线标记和设备标记，编制配线列表。

44、针对获证组织扩大范围的审核，以下说法正确的是：（AC）

(A)可以和监督审核•起进行。 (B)是监督审核的形式之一。

(C)一种特殊审核。 (D)以上都对。

45、对于针对信息系统的软件包，以下说法正确的是：（B ）

(A)组织应具有有能力的人员，以便随吋对软件包进行适出性修改。

(B)应尽量劝阻对软件包实施变更，以规避变更的风险。

(C)软件包不必作为配置项进行管理。

(D)软件包的安装必须由其开发商实施安装。

46、以下不属于信息安全事态或事件的是：（ D）

(A)服务、设备或设施的丢失 (B)系统故障或超负载

(C)物理安全要求的违规 (D)安全策略变更的临时通知

47、以下可认定为审核范围变更的事项是：（ D）

(A)受审核组织增加一个制造场所。 (B)受审核组织职能单元和人员规模增加。

(C)受审核组织业务过程增加。 (D) 以上全部。

48、在认证审核时，审核组在现场有权限自行决定变更的事项包括：（C）

(A)帘核准则 (B)审核人日数

(C)审核路线 (D)应受审核的业务过程

49、审核员的检查表应：（B ）

(A)事先提交受审核方评审确认。

(B)基于审核准则事先编制。

(C)针对不同的受审核组织应统一格式和内容。

(D)由审核组长负责编制审核组使用的检查表。

50、以下属于信息安全管理体系审核发现的是(C )

(A)审核员看到的物理入口控制方式

（B）审核员看到的信息系统资源阈值

(C)审核员看到的移动介质的使用与安全策略的符合性

(D)审核员看到的项目质量保证活动与CMMI规程的符合性

51、审核组中的技术专家是：（ A）

(A)为审核组提供文化、法律、技术等方面知识咨询的人员。

(B)特別负责对受审核方的专业技术过程进行审核的人员。

(C)审核期间为受审核方提供技术咨询的人员。

（D）从专业的角度对审核员的审核进行观察评价的人员。

52、审核人日数的计算方式是审核天数乘以：（C ）

(A)审核组中审核员+实习审核员+技术专家+观察员的总人数

(B)审核组中审核员+实习审核员的总人数

(C)审核组中审核员的总人数

(D)审核组屮审核员+实审核员+技术专家的总人数

53、信息安全管理体系初次认证审核时，第一阶段审核应：(D )

(A)对受审核方信息安企管理体系的策划进行审核和评价，对应GB/T22080-2008的 4.2.1条要求。

(B)对受审核方信息安全管理体系的内部审核及管理评审的有效性进行审核和评价。

(C)对受审核方信息安全管理体系文件的符合性、适宜性和有效性进行审核和评价。

(D)对受审核方信息安全管理体系文件进行审核和符合性评价。

54、按照“PDCA”思路进行审核，是指：( A)

(A)按照受审核区域的信息安全管理活动的"PDCA"过程进行审核。

(B)按照认证机构的“PDCA”流程进行审核。

(C)按照认可规范中规定的“PDCA”流程进行审核。

(D)以上都对。

55、关于审核结论，以下说法正确的是：（ D）

(A)审核组综合了所有审核证据进行合理推断的结果。

(B)审核组综合了所有审核证据与受审核方充分协商的结果。

(C)审核组权衡了不符合的审核发现的数量及严重程度后得出的结果。

(D)审核组考虑了审核目的和所有审核发现后得出的审核结果。

56、第三方认证审核时确定审核范围的程序是：( B)

(A)组织提出、与审核组协商、认证机构确认、认证合同规定

(B)组织申请、认证机构评审、认证合同规定、审核组确认

(C)组织提出、与咨询机构协商、认证机构确认

(D)认证机构提出、与组织协商、审核组确认、认证合同规定

57、审核报告是：（ C）

(A)受审核方的资产。 (B)审核委托方和受审核方的共同资产。

(C)审核委托方的资产。 (D)审核组和审核委托方的资产。

58、认证审核前，审核组长须与受审核方确认审核的可行性，特别应考虑：（ A）

(A)核实组织申请认证范围内需接受审核的组织结构、场所分布等基本信息。

(B)注总审核的程序性安排事先应对受审核组织保密。

(C)注意审核拟访问的文件、记录、场所等事先应对受审核组织保密。

(D)要求受审核组织做好准备向审核组开放所有信息的访问权。

59、信息安全管理体系认证审核时，为了获取审核证据，应考虑的信息源为：（D )

(A)受审核方的办公自动化系统管理与维护相关的过程和活动。

(B)受审核方场所内已确定为涉及国家秘密的相关过程和活动。

(C)受审核方的核心财务系统的管理与维护相关的过程和活动。

(D)受审核方中请认证范\_内的业务过程和活动。

60、认证审核时，审核组拟抽査的样本应：（B）

(A)山受审核方熟悉的人员事先选取，做好准备。

(B)由审核组明确总体并在受控状态下独立抽样。

(C)由审核组和受审核方人员协商抽样。

(D)由受审核方安排的向导实施抽样。

61、认证审核期间，当审核证据表明审核目的不能实现时，审核组应（D ）

(A)—起讨论，决定后续措施。 (B)审核组长权衡，决定后续措施。

(C)由受审核方决定后续措施。 (D)报告审核委托方并说明理由，确定后续措施。

62、认证审核时，对于审核组提出的不符合审核准则的审核发现，以下说法正确的是（B）

(A)受审核方负责采取纠正措施，纠正措施的实施是审核活动的一部分。

(B)审核组须验证纠正措施的有效性，纠正措施的实施不是审核活动的一部分。

(C)审核组须就不符合项的原因分析提出建议，确定纠正措施是否正确。

(D)采取纠正措施是受审核方的职责，审核组什么都不做。

63、信息安全管理体系认证过程包含了：（D）

(A)现场审核首次会议开始到末次会议结束的所有活动。

(B)从审核准备到审核报告提交期间的所有活动。

(C)一次初审以及至少2次监督审核的所有活动。

(D)从受理认证到证书到期期间所有的审核以及认证服务和管理活动。

64、第三方认证时的监督审核不一定是对整个体系的审核，以下说法正确的是：（D）

(A)组织获得认证范围内的职能区域可以抽查，但标准条款不可以抽查。

(B)组织获得认证范围内的业务过程可以抽沓，但职能区域不可以抽杳。

(C)组织获得认证范围内的业务过程和职能区域都不可以抽查，仅标准条款可以抽杳。

(D)标准条款可以抽查，但针对内审和管理评审以及持续改进方面的审核不可缺少。

65、设立信息安全管理体系认证机构，须得到以下哪个机构的批准，方可在中国境内从事认证活动：( B )

(A)中国合格评定国家认可委员会

(B)屮国国家认证认可监督管理委员会

(C)中国认证认可协会

(D)工商注册管理部门

66、国家信息安全等级保护采取（A）

（A）自主定级、自主保护的原则。

（B）国家保密部门定级、自主保护的原则。

（C）公安部门定级、自主保护的原则。

（D）国家保密部门定级、公安部门监督保护的原则。

67、信息安全管埋体系是指：（C）

(A)信息系统设施 (B)防火墙

(C)组织建立信息安全方针和目标并实现这些目标的体系

(D)网络维护人员的工作的集合

68、信息安全管理体系可以:（D）

(A)帮助组织实现信息安全目标 （B)提供持续改进的框架

(C)向组织和顾客提供信任 （D) a+b+c

69、系统的识别和管理组织所应用的过程，特别是这些过程之间的相互作用，称为：（D)

(A)管理的系统方法 （B)信息安全管理体系方法

(C)过程方法 （D)以事实为基础的决策方法

70、下列措施中，哪些是风险管理的内容：（D）

(A)识别风险 （B)风险优先级评价

(C)风险化解 （D)以上都是

71、与审核准则有关的并且能够证实的记录、事实陈述或其它信息称为：（A）

(A)审核证据 （B)安全信息

(C)记录 （D) a+b+c

72、选择的控制目标和控制措施、以及选择的原因应记录在下列那个文件中：（C）

(A)安全方针 （B)风险评估报告

(C)适用性声明 （D)风险处置计划

73、风险处置计划应该包含：(D

(A)管理措施 （B)资源需求

(B)职责分配 （D) a+b+c

74、实施第三方信息安全管理体系审核，主要是为了：(D)

(A)发现尽可能多的不符合项

(B)检测信息安全产品质量的符合性

(C)建立互利的供方关系

(D)证实组织的信息安全管理体系符合已确定的审核准则的程度要求

75、文件在信息安全管理体系中是一个必须的耍素，文件有助于：(CD)

(A)审核员进行文件审查 （B)评价体系的有效性

(C)确保可追溯性 （D) b+c

76、ISO/IEC 27001 是(AD)

(A)以信息安全为主题的管理标准 （B)与信息安全相关的技术性标准

(C)编制业务连续性计划的指南 （D)以上都不是

77、网页防篡改技术的0的是保护网页发布信息的：（B)

A)保密性 （B)完整性

C)可用性 (D)以上全部

78、标准GB/T22080中"物理安全周边”指的是：（D ）

(A)组织的建筑物边界 （B)计算机机房出入口

(C)组织的前台接待处 （D)含有信息和信息处理设施的区域周边

79、标准GB/T22080中所措资产的价值取决于：（B）

A)资产的价格 （B)资产对于业务的敏感程度

C)资产的折损率 （D)以上全部

80、对一段时间内发生的信息安全事件类型、频次、处理成本的统计分析（A ）

A)属于事件管理 （B)属于问题管理

C)属于变更管理 （D)属于配置管理

81、在组织的整体业务连续性管理过程中应考虑( A).

(A)信息安全的需求 （B)问题管理的需求

(C)变更管理的需求 （D)配置管理的需求

82、下面哪一种安全技术是鉴别用户身份的最好方法：（B )

A)智能卡 （B)生物测量技术

(C)挑战-响应令牌 （D)用户身份识别码和口令

83、最佳的提供本地服务器上的处理工资数据的访问控制是：（C）

(A)记录每次访问的信息

(B)对敏感的交易事务使用单独的密码/口令

(C)使用软件来约束授权用户的访问

(D)限制只有营业时间内才允许系统访问

84、当计划对组织的远程办公系统进行加密吋，应该首先冋答下面哪一个问题?(D)

（A）什么样的数据属于机密信息

（B）员工需要访问什么样的系统和数据

（C）需要什么样类型的访问

（D）系统和数据具有什么样的敏感程度

85、下面哪一种属于网络上的被动攻击（CD）

(A)消息总改 （B)伪装

（C）拒绝服务 （D)流量分析

86、虚拟专用网（VPN)提供以下哪一种功能？（B）

（A）对网络嗅探器隐藏信息 （B）强制实施安全策略

（C）检测到网络错误和用户对网络资源的滥用 （D）制定访问规则

87、在本地服务器上不启动动态主机配置协议（DHCP)，可以：（A）

(A)降低未授权访问网络资源的风险 (B)不适用于小型网络

(C)能自动分配IP地址 (D)增加无线加密协议（WEP)相关的风险

**练习题二多项选择题**

**从下面各题选项中选出两个或两个以上最恰当的答案，并将答案填在下表相应位置中。**

1、在信息安全事件管理中，（AC）是所有员工应该完成的活动。

(A)报告安全方面的漏洞或弱点 （B)对漏洞进行修补

(C)发现并报告安全事件 （D)发现立即处理安全事件

2、信息系统安全保护法律规范的基本原则是（ACD

(A)谁主管谁负责的原则 （B)全面管理的原则

(C)预防为主的原则 （D)风险管理的原则

3、以下说法正确的是（AC ）

(A)信息网络的物理安全要从环境安全和设备安全两个角度来考虑。

(B)计算机场地可以选择在化工厂生产车间附近。

(C)计算机场地在正常情况下温度保持在18～28摄氏度。

(D)机房供电线路和动力、照明用电可以用同一线路。

4、标准GB/T22080中“支持性设施”指的是：(ABCD )

（A）UPS电源 （B)电力设施 （C)空调系统 （D)消防设施

5、信息安全的符合性检查包括：（ ABC）

（A）法律法规符合性 （B)技术标准符合性

(C)安全策略符合性 （D)内部审核活动

6、基于风险的考虑，组织应予以管理的第三方服务的变更包括（ACD

(A)服务级别的变更 (B)第三方后台服务流程的变更

(C)服务定义的变更 (D)服务提供人员的变更

7、( ABCD )是建立有效的计算机病毒防御体系所需要的技术措施。

(A)防火墙 （B)补丁管理系统 (C)网络入侵检测 （D)杀毒软件 （E)漏洞扫描

8、审核范围的确定应考虑：（ BCD）。

(A)组织的管理权限 (B)组织的活动领域

(C)组织的现场区域 (D)覆盖的时期

9、审核原则是审核员从事审核活动应遵循的基本要求，以下什么是审核员应遵循的原则(ABCD）

（A）道德行为 （B)保守机密 （C）公正表达 （D)职业素如 (E)独立性

10、根据国家发布的<认证及认证培训咨询人员管埋办法>规定,以下哪些人员不得在一个认证机构从事认证活动（ ABCD）。

(A)已经在另外一个认证机构从事认证活动的人员

(B)国家公务员

(C)从事认证咨询活动的人员

(D)已经与认证咨询机构签订合同的认证咨询人员

11、信息安全管理体系认证审核的范围即（CD）。

（A）组织的全部经营管理范围。

（B）组织的全部信息安全管理范围。

（C）组织根据其业务、组织、位置、资产和技术等方面的特性确定信息安企管理体系范围。

（D）组织承诺按照GB/T 22080标准要求建立、实施和保持信息安全管理体系的范围。

12、为防止业务中断，保护关键业务过程免受信息系统失误或灾难的影响，应（ ABD）。

（A）定义恢复的优先顺序；

（B）定义恢复时间指标；

（C）按事件管理流程进行处置；

（D）针对业务中断进行风险评估。

13、信息安全管理体系认证是：（ ABC）。

（A）与信息安全管理体系有关的规定要求得到满足的证实活动。

（B）对信息系统是否满足有关的规定要求的评价。

（C）信息安全管理体系认证是合格评定活动的一种。

（D）是信息安全风险管理的实施活动。

14、以下符合“责任分割”原则的做法是：（ BCD）。

（A）不同职级人员工作区域隔离。

（B）保持安全审核人员的独立性。

（C）授权者、操作者和监视者三者责任分离。

（D）事件报告人员与事件处理人员职责分离。

15、访问信息系统的用户注册的管理是：（AB）。

（A）对用户访问信息系统和服务的授权的管理。

（B）对用户予以注册时须同时考虑与访问控制策略的一致性。

(C)当I（D)资源充裕时可允许用户使用多个I（D)

(D)用户在组织内变换丁.作岗位吋不必重新评审其所用I（D)的访问权。

16、对于用户访问信息系统使用的口令，以下说法正确的是：（CD）。

（A）口令必须定期更换。

（B）同一工作组的成员可以共享口令。

（C）如果使用生物识别技术，可替代口令。

（D）如果使用智能卡鉴别技术，可替代U令。

17、可以通过使用适宜的加密技术实现的安全目标包括：（ABCD）。

（A）信息的保密性 （B）信息的完整性

（C）信息的真实性 （D）信息的抗抵赖性

18、信息安全管理体系审核的抽样过程是:( ACD)。

（A）调查性质的抽样。 （B）验收性质的抽样。

（C）通过对样本的评价来推断总体。 （D）有弃真的风险和取伪的风险。

19、关于商用密码技术和产品，以下说法正确的是：（BCD）。

（A）任何组织不得随意进口密码产品，但可以出口商用密码产品。

（B）商用密码技术属于国家秘密。

（C）商用密码是对不涉及国家秘密的内容进行加密保护的产品。

（D）商用密码产品的用户不得转让其使用的商用密码产品。

20、可被视为可靠的电子签名须同时符合以下条件：（ABCD）。

（A）电子签名制作数据用于电子签名时，属于电子签名人专有。

（B）签署时电子签名制作数据仅由电子签名人控制。

（C）签署后对电子签名的任何改动能够被发现。

（D）签署后对数据电文内容和形式的任何改的那个能够被发现。

21、降低风险的处置措施可以是（AB）

（A）降低某项威胁发生的可能性 （B）降低某项威胁导致的后果严重程度

（C）杜绝某项威胁的发生的可能性 （D）杜绝威胁导致的后果

22、以下说法正确的是：（ABD）

（A）应考虑组织架构与业务目标的变化对风险评估结果进行再评审。

（B）应考虑以往未充分识别的威胁对风险评估结果进行再评审。

（C）制造部增加的生产场所对信息安全风险无影响。

（D）安全计划应适时更新。

23、信息系统审计需考虑：（AB）

（A）信息系统审计的控制措施 （B）信息系统审计工具的保护

（C）技术符含性核查 （D）知识产权

24、从安全的角度来看，能提前做好安全防范准备的组织，对安全事件的处理不恰当的是( ABD )

（A）较高的成本，较小的事件，较慢的恢复

（B）中等成本，中等的事件，屮等速度的恢复

（C）较低的成本，较小的事件，较快的恢复

（D）较高的成本，较大的事件，较快的恢复

25、使用电子通信设施进行信息交换的规程和控制宜考虑（ABCD)

（A）电子通信设施可接受使用的策略或指南

（B）检测和防止可能通过使用电子通信传输的恶意代码的规程

（C）维护数据的授权接受者的正式记录

（D）密码技术的使用

1. 应用结束时终止活动的会话，除非采—种合造的锁定机制保证其安全，符合信息安全的（ ABCD）措施

（A）使用网络服务的策略 （B)清空桌雨和屏幕策略

（C）无人值守的用P设备 （D)使用密码的控制策略

27、在网络访问控制中，对外部连接的用户鉴别时，宜考虑：( ABD )

（A）回拨规程

（B）硬件令牌或询问

（C）使用回拨调制解调器控制措施，可以使用呼叫转发的网络服务

（D）基于密码技术的方法

28、关于口令管理系统，描述正确的有：( ABC)

（A）口令是确认用户具有访问计算机服务的授权的主要手段之一

（B）维护用户以前使用的口令的记录，并防止重复使用

（C）分开存储口令文件和应用系统数据

（D）不允许用户变更自己的口令

29、开发和支持过程中的安全，包括：( ABCD )

（A）变更控制规程 （B)操作系统变更后应用的技术评审

（C）对程序源代码的访问控制 （D)软件包变更的限制

30、对技术符合性进行核查，若使用渗透测试或脆弱性评估时：（ABC ）

(A)测试宜预先计划，并形成文件 （B)需要专业技术专家执行

（C）计划可重复执行 （D)可以代替风险评估

31、在业务连续性管理过程中的关键要素包括：（ BD）

（A）确保人员的安全、信息处理设施和组织财产得到保护

（B）定期测试和更新已有的计划和过程

（C）调整或增加访问控制措施

（D）识别关键业务过程中涉及的所有资产

32、对程序源代码访问控制的目的包括：（ ABCD）

（A）避免无意识的变更 （B)以减少潜在的计算机程序的破坏

（C）以防引入非授权功能 （D)维护所有软件更新的版本控制

33、应用系统的设计与实施宜确保导致完整性损坏的处理故障的风险减至最小，要考虑的特定范围包括：（ABCD）

（A）确认系统生成的输入数据

（B）使用添加、修改和删除功能，以实现数据变更

（C）使用适当的规程恢复故障，以确保数据的正确处理

（D）防范利用缓冲区超出/益处进行的攻击

34、与信息处理或通信系统的问题有关的用户或系统程序所报告的故障进行处置，处置规则包括：（ABC）

（A）评审纠正措施，以及所采取措施给予了充分的授权

（B）评审故障日志，以确保故障已得到令人满意的解决

（C）如果具有出错记录的系统功能，宜确保该功能处于开启状态

（D）评审纠正措施，以确保没有损害控制措施

**练习题四案例分析题**

**请对以下场景进行分析，写出不符合标准条款的编号及内容，并写出不符合事实。**

1、审査某知名网站的总部时，审核员来到公司陈列室发现任何客户可以随意进入，并且该陈列室中有5 台演示用的台式电脑可以连接外网和内网，现场有参观人员正在上网查询该公司网站的资料。

A11.4.6

1. 市核员在审核公司设备和网络操作机房时发现，作为公司资料和数据的中心，中心有程序文件（GX28) 规定必须对进出机房人员进行控制，除授权工作人员可凭磁卡进出外，其余人员进出均须办理准入和登记手续。现场发现未经授权的人员张XX进出机器和网络操作机房，却没有任何登记记录，工作人员解释说是供应商正在调试网络设备。

A9.1.2

1. 审核员扫描XX公司的网络，发现在用软件只有很少的计算机打了补丁程序，并且运行的操作系统上的多数软件是网络下载，多数是免费版本，现场管理人员认为下载的软件都是从知名网站上下载的,不会有问题。

4.2.1D3

1. xx银行在2008年一季度发生了10起开通网上转帐客户的资金损失事故，最后银行承认密码系统设计太简单，并赔偿客户损失。但在2008年4~5月又发生7起类似事故,系统管理说：“我们目前也没有办法， 只能赔款了”。

A13.2.2

1. 审核员在现场审核吋发现公司存有一份软件淸单，当询问淸单上所列的软件足否都是通过正规途径购买的软件，管理员回答有的是到正规商店，有的是通过网络购买的。

A10.2.1

1. 审核员来到某软件开发公司进行审核时，来到计算机机房时发现，公司的服务器、数据库均在内，中心内部设置有前、后两个门，前门有门禁系统，只有授权人员凭门卡能进入，而后门则锁住了，当询问谁有钥匙，机房主管回答：前门口保安有。当来到前门门岗时，发现钥匙挂在保安办公室的钥匙箱内，而该钥匙箱没有锁，保安主管说：有需要的时候任何人可以打开取钥匙且不用办理登记手续。

A9.1.2

7、审核员在公司的资产登记表中发现，公司于年初将一批2003年购置的电脑特价处理给员工，这些电脑原用于核心业务系统。当询问系统管理员是否在出售前进行了格式化处理，该系统管理员说：“由于当时新进了许多新的电脑设备，需要安装调试，没空处理老的电脑，再说这些都是卖给自己员工的，他们本身就接触到这些信息。”

A9.2.6

1. 审核员发现某软件开发公司在暑假期间聘请了三位大学生来做软件测试，但在人事部门未找到相关的保密协议，也未见有关要求的培训记录，人事经理解释说:“他们在测试期间没有接触到软件的核心机密信息，所以不需要签保密协议，也不需要进行ISMS的培训。“

A8.2.2

9、审核员在审核过程中发现，公司的系统用户账户中有多个账号的用户名的主人是一些己经离开公司的人员，且此类账户拥有较高级别的访问权限，系统管理员介绍说：“由于公司耍求所有的员工必须按耍求登录自己的账户，这样对一些分公司来出差的人员很不方便，因此用这些老账户让他们使用，便于他们登录使用公司的网络资源，反正都是公司的员工，不会出问题的。”

A8.3.3

1. 审查技术部门在完成软件开发源代码任务并递交客户后，按公司要求应定时销毁在具体开发人员PC 机内的该项目源代码，以防止源代码的泄露，但是该部门却提供不出该源代码被销毁的证据。

4.3.3

1. 在某软件开发企业，质景保证部负责对软件开发成果物进行测试，该部门测试人员使用名为“Bugfree”的系统记录测试发现的问题,然后由开发人员针对测试人员提出的问题,确定软件修改方案，修改后重新提交测试，通过后由测试人员给出“最终测试通过”的结论。软件开发人员的修改方案以及修改后重新测试的信息也分别在该"Bugfree”系统中予以记录。审核员请开发人员演示上述过程时发现，开发人员也可以登录测试问题记录的页面，且能够修改测试记录信息。当审核员问为什么会这样，该开发人员回答说，有时候开发人员与测试人员就软件问题的判定有争议，因此允许开发人员修改测试问题记录，否则会影响开发 人员的绩效考核。

A11.6.1

1. 审核员在某公司审核时，按计划到公司的计算机机房现场查看。审核员看到系统管理员王某正忙着安装、调试邮件服务器。丨T部主任解释说，公司在现写字楼的租赁已到期，已决定迁至另一街区的某写字楼。王某因下班路上路过新地址，于是在前一天下班时就将邮件服务器拆除，顺便带到新写字楼，并将电源接通。但今天发现，公司各业务部门搬家的时间表不一致，有几个业务部门仍在现写字楼办公，但因邮件服务器已搬走，无法与境外客户联络，对此这几个部门今天有不少抱怨。为弥补这一情况,系统管理员只好又将邮件服务器拆除装回原机房。

A10.1.2

1. 某公司主营业务为工业设备代理销售。审核员在审核销售部时发现，公司的全部销售业务以及与顾客的关系管理数据的维护均依赖网络及信息系统完成，当问及这些系统的维护和管理时，公司管理者代表解释说，公司维护IT系统的工作全由沈某一人担任，称沈某人非常正直可靠，所有的IT系统维护和监控项目均由其1人完成，从未出过信息安全事故。审核员请来沈某询问，沈某确认其工作职责包括对各业务线小组人员的权限设置、系统运行监视、系统维护和升级、以及系统安全策略符合性审核等所有的内容。

A10.1.3

1. 某公司是定向为顾客开发软件的企业。审核组在公司平台业务开发部审核时，抽查到公司正在为顾客开发的“数据管理平台”项目，该项目的系统设计文件由公司高级系统架构师完成，平台开发部主任说：这份系统设计文件因涉及到顾客"数据管理平台”的结构设计，非常敏感，公司要求开发人员只可读、不可修改，且不可以在公司其他部门传阅。开发人员向审核员演示其对该设计文件的访问权限为只读、可打印， 但审核员在平台业务部工作区未看到有打印机。开发人员解释说，平台业务开发部和处于该楼层的其他几个部门共用一台网络打印机，并带审核员去查看。审核员发现，为了方便各部门使用，这台打印机放置在该楼层的“公共休息区”内。

A7.1.3

15、某公司为国家相关部门指定的敏感票据印刷企业。审核员在现场巡查时发现，公司制版车间的一张办公桌上散放着工作号为111字9、10、11号的三份《票据生产通知单》，通知单中分别详细列出了三种票据的制版工艺要求。审核员问道这是谁的办公桌时，车间主任回答说，这是制版工艺师的办公桌，他今天请假了，没来上班。审核员观察到，制版车间与其他车间共处一个较大的生产厂房内，在上班时间各车间是互通的。

A11.3.3

**ISMS测验一**

**一、单项选择题(从下面各题选项中选出一个最怡当的答案，并将相应字母填在下表相应位置中。每 题1分，共30分。)**

1、信息安全管理体系中提到的"资产责任人"是指：（C )

（A）对资产拥有财产权的人。

（B）使用资产的人。

（C）有权限变更资产安全属性的人。

（D）资产所在部门负责人。

2、组织应给予信息以适当级别的保护，是指：（B )

（A )应实施尽可能先进的保护措施以确保其保密性。

（B )应按信息对于组织业务的关键性给予充分和必要的保护。

（C )应确保信息对于组织内的所有员工可用。

（D)以上都对。

3、考虑设备安全是为了：（D )

（A）防止设备丟失、损坏带来的财产损失。

（B）有序保障设雛修时的备件供应。

（C )及时对设备进研级和更新换代。

（D)控制资产的丟失、损坏、失窃、危及资产安全以及组织活动中断的风险。

4、信息处理设施的变更管理不包括：(D )

（A）信息处理设施用途的变更。

（B）信息处理设施故障部件的更换。

（C）信息处理臟软件的升级。

（D）以上都不对。

5、定期备份和测试信息是指：（C )

（A )每次备份完成时对备份结果进行检査，以确保备份效果。

（B )对系统测试记录进行定期备份。

（C )定期备份，定期对备份麵的完整性和可用性进行测试。

（D)定期检査备份存储介质的容量。

6、一个组织或安全域内所有信息处理设施与已设精确时钟源同步是为了：（ B）

（A）便于针对使用信息处理设施的人员计算工时

（B )便于探测未经授权的信息处理活动的发生

（C )确保信息处理的及时性得到控制

（D）人员异地工作时统一作息时间。

7、为防止对网络服务的未授权访问，组织应(A )

（A）制定安全策略，确保用户应仅能访问已获专门授权使用的服务。

（B）禁止内部人员访问互联网。

（C）禁止外部人员访问组织局域网。

（D）以上都对。

8、组织应进行安全需求分析,规定对安全控制的要求，当：( D)

（A）组织需建立新的信息系统时； （B）组织的原有信息系统扩容或升级时；

（C）组织向顾客交付软件系统时； （D）A+B

9、确定资产的可用性要求须依据：( A)

（A）授权实体的需求。 （B）信息系统的实际性能水平。

（C）组织可支付的经济成本。 （D）最高管理者的决定。

10、残余风险是：( C)

（A）低于可接受风险水平的风险。 （B）高于可接受风险水平的风险。

（C）经过风险处置后剩余的风险。 （D）未经处置的风险。

11、对计算机病毒和危害社会公共安全的有害数据的防治研究工作由：(B）

（A）工业和信息化部归口難。 （B）公安部归口管理。

（C）国家互联网信息办公室归口管理。 （D）信息安全产品研制企业自行管理。

12、网络路由控制应遵从：（C )

（A）端到端连接最短路径策略； （B）信息系统应用的最佳效率策略；

（C）确保计算机连接和信息流不违反业务应用的访问控制策略, （D）A+B+C

13、对于第三方服务提供方，以下描述正确的是：(B )

（A）为了监视和评审第三方提供的服务，第三方人员提供服务时应有人员全程陪同

（B）应定期度量和评价第三方遵从商定的安全策略和服务水平的程度。

（C）第三方服务提供方应有符合ITIL的流程。

（D）第三方服务的变更须向组织呈报以备案。

14、为了确保布缆安全，以下正确的做法是：(D )

（A）使用同一电缆管道铺设电源电缆和通信电缆。

（B）网络电缆采用明线架设，以便于探査故障和维修。

（C）配线盘应尽量放置在公共可访问区域，以便于应急管理。

（D）使用配线标记和设备标记，编制配线列表。

15、对于针对信息系统的软件包，以下说法正确的是：（ B）

（A）组织应具有有能力的人员，以便随时对软件包进行适用性修改。

（B）应尽量劝阻对软件包实施变更，以规避变更的风险。

（C）软件包不必作为配置项进行管理。

（D）软件包的安装必须由其开发商实施安装。

16、以下不属于信息安全事态或事件的是：（ D）

（A）服务、设备或设施的丟失 （B）系统故障或超负载

（C）物理安全要求的违规 （D）安全策略变更的临时通知

17、设立信息安全管理体系认证机构，须得到以下哪个机构的批准，方可在中国境内从事认证活动 (A )

（A）中国合格评定国家认可委员会 （B）中国国家认证认可监督管理委员会

（C）中国认证认可协会 （D）工商注册管理部门

18、国家信息安全等级保护采取。( A)

（A）自主定级、自主保护的原则。

（B）国家保密部门定级、自主保护的原则。

（C）公安部门定级、自主保护的原则。

（D）国家保密部门定级、公安部门监督保护的原则。

19、信息安全管理中，关于脆弱性,以下说法正确的是:( B)

（A）组织使用的开源软件不须考虑其技术脆弱性。

（B）软件开发人员为方便维护留的后门是脆弱性的一种。

（C）识别资产脆弱性时应考虑资产的固有特性，不包括当前安全控制措施。

（D）使信息系统与网络物理隔离可社绝其脆弱性被威胁利用的机会。

20、信息安全管理中，对于安全违规人员的正式纪律处理过程中必不可少的活动是（C ）

（A）警告与罚款。 （B）就违规的详情向所有人员通报。

（C）评估违规对业务造成的影响。 （D）责成违规人员修复造成的损害。

21、信息安全管理中，关于撤销访问权，不包括以下哪种情况：(D )

（A）员工离职时。 （B）组织内项目人员调换到不同的项目组时。

（C）顾客或第三方人员结束访问时。（D）以上都不对。

22、依据GB/T22080,信息系统在开发时应考虑信息安全要求，这包括：( C)

（A）管理人员应提醒使用者在使用应用系统时注意确认输入输出\_。

（B）质量人员介入验证输入输出数据。

（C）应用系统在设计时考虑对输入数据、内部处理和输出数据进行确认的措施。

（D）在用户须知中增加“提醒”或"警告"内容。

23、监视和评审ISMS,应考虑：（ C)

（A）统计和评估已造成不良后果的安全违规和事件，不包括未造成不良后果的事件。

（B）针对网络安全事件，不包括管理性安全措施执行情况。

（C）迅速识别试图的和得逞的安全违规事件,包括技术符合性事件和管理性安全措施执行情况。

（D）针对管理性安全措施执行情况，不包括技术符合性事件。

1. 依据GB/T22080 ,业务连续性管理活动不包括：( D )

（A）针对业务中断进行风险评估。 （B）定义恢复的优先顺序。

（C）定义恢复时间指标。 （D）按事件管理流程进行处置。

1. 以下不属于"责任分割"原则范畴的做法是：（A）

（A）不同职级人员工作区域隔离。

（B）保持安全审核人员的独立性。

（C）授权者、操作者和监视者三者责任分离。

（D）事件报告人员与事件处理人员职责分离。

26、访问信息系统的用户注册的管理不正确的做法是：（C)

（A）对用户访问信息系统和服务的授权的管理。

（B）对用户予以注册时须同时考虑与访问控制策略的一致性。

（C）当ID资源充裕时可允许用户使用多个ID.

（D）用户在组织内变换工作岗位时须重新评审其所用ID的访问权。

27、对于用户访问信息系统使用的口令，以下说法正确的是：（C ）

（A）口令必酿期更换。 （B）同一工作组的成员可以共享口令。

（C）如果使用生物识别技术，可替代口令。 （D）以上全部。

28、关于保密性，以下说法正确的是：（A ）

（A）规定被授权的个人和实体，同时规定访问时间和访问范围以及访问类型。

（B）职级越高可访问信息范围越大。

（C）默认情况下IT系统维护人员可以任何类型访问所有信息。

（D）顾客对信息的访问权按顾客需求而定。

29、关于商用密码技术和产品,以下说法不正确的是：( A）

（A）任何组织不得随意进口密码产品，但可以出口商用密码产品。

（B）商用密码技术属于国家秘密。

（C）商用密码是对不涉及国家秘密的内容进行加密保护的产品。

（D）商用密码产品的用户不得转让其使用的商用密码产品。

30、数据信息资源的访问控制指：（B ）

（A）允许访问者访问即访问者可获取、拷贝或其他访问者需要的操作。

（B）允许访问者访问即访问者按访问权规定的的方式访问数据信息资源。

（C）编制一份授权实体清单并保持不变。

（D）如果访问时间足够短则不须提请批准。

31、信息安全管理中的应急预案应指：(D )

（A）如何获取备份数据的计划。

（B）描述应急响应方法与措施的计划。

（C）规定如何获取灾后恢复所需资源以及技术措施的计划。

（D） 以上全部。

32、信息安全管理中的灾难恢复计划应描述的内容包括：（C）

（A）灾难后信息系统恢复过程所需要的数据和资源。

（B）灾难后信息系统恢复过程所需要的任务和行动计划。

（C）A+B

（D）一份描述原信息系统配置清单的文件。

33、依据GB/T 22080,风险评估过程包含：( A)

（A）风险分析和风险评价的活动。

（B）风险管理和风险处置的活动。

（C）风险识别与风险分析的活动。

（D）风险处置和估计参与风险的活动。

34、信息安全管理中，以下哪一种描述能说明“完整性"：( B)

（A）资产与原配置相比不发生缺失的情况。

（B）资产不发生任何非授权的变更。

（C）软件或信息资产内容构成与原件相比不发生缺失的情况。

（D）设备系统的部件和配件不发生缺失的情况。

35、信息安全灾备管理中，”恢复点目标”指：（ C)

（A）灾难发生后，信息系统或业务功能从停顿到必须恢复的时间。

（B）灾难发生后，信息系统或业务功能项恢复的范围。

（C）灾难发生后，系统和必须恢复到的时间点要求。

（D）灾难发生后，关键数据能被复原的范围。

36、信息安全灾备管理中，"灾难备份"指：（D )

（A）备份数据发生了灾难性破坏。

（B）为灾难恢复而对数据、数据处理系统、网络系统进行备份的过程。

（C）为灾难恢复而对基础设施、专业技术支持能力和运行管理能力进行备份的过程.

（D）B+C

37、信息安全管理中，"最小特定权限”指：（B )

（A）访问控制权限列表中权限最低者。

（B）执行授权活动所必需的权限。

（C）对新入职者规定的最低授权。

（D）执行授权活动至少应被授予的权限。

38、信息安全管理中,”远程访问”指：（ D)

（A）访问者的物理位置与被访问客体不在一个城市。

（B）访问者的物理位置与被访问客体的距离大于30米。

（C）访问者的物理位置与被访问客体的距离大于15米。

（D）访问者从并不永久连接到所访问网络的终端访问资源。

39、信息技术中，"端口"即：（D )

（A）设备配线的物理接口。 （B）逻辑信道端点，如80端口。

（C）计算机的USB接口。 （D）A+B

40、以下可接受的正确做法是：（D )

（A）使用网盘存储涉及国家秘密的信息。

（B）IT系统维护人员使用自用的计算机对涉密计算机系统进行测试。

（C）将涉密移动硬盘的信息简单刪除后作为普通存储装置使用。

（D）被确定涉及国家秘密的计算机系统即切断其可与互联网的连接。

41、关于认证人员执业要求以下说法正确的是：（B)

（A）注册审核员只能在一个认证机构和一个咨询机构执业。

（B）注册审核员和认证决定人员只能在一个认证机构执业。

（C）注册审核员只能在一个认证机构执业，非注册的认证决定人员不受此限制。

（D）在咨询机构任专职咨询师的人员，只能在认证机构任兼职认证决定人员。

1. 依据GB/T22080 ,以下不是"适用性声明〃文件必须包含的内容是：(A )

（A）实施信息安全控制措施的角色、职责和权限。

（B）组织选择的控制目标和控制措施，以及选择的理由。

（C）当前实施的控制目标和控制措施。

（D）对附录A中可控制目标和控制措施的刪减，以及删减的合理性说明。

43、确定组织的信息安全管理体系范围应依据：( D)

（A）组织整体业务活动的性质。

（B）组织计算机信息系统以及其他技术的特性。

（C）组织的资产所处的位置和物理环境。

（D）以上全部。

1. 组织选择信息安全风险评估方法，应考虑：( A)

（A）适合于组织的ISMS、已识别的安全要求和法律法规要求。

（B）只有采用准确性高的概率模型才能得出可信的结果。

（C）必须采用易学易用的定性评估方法才能提高效率。

（D）必须采用国家标准规定的相加法或相乘法。

45、信息安全管理中，识别资产时须考虑：( C)

（A）优先识别计算机信息系统相关的资产。 （B）依据财务资产台账。

（C）ISMS范围内对组织业务有价值的资产。 （D）不包括制造设备。

46、关于IT系统审计，以下说法正确的是：（B ）

（A） IT系统审计是发现系统脆弱性的有效手段，不可删减。

（B）组织经评估认为IT系统审计的风险不可接受时，可以删减。

（C）组织认为IT系统审计成本太高时，可以删减。

（D）组织自己不具备实施IT系统审计的能力时，可以删减。

47、依据GB/T 22080 ,组织监视外包软件开发应考虑：( C)

（A）监督外包方及时交付软件的能力。 （B）监督外包方的开发成果物质量。

（C）确保外包方的开发满足组织安全需求。（D）验证外包方的开发过程符合CMMI要求。

48、信息安全管理中，"防止滥用信息处理设施"是为了防止：(D )

（A）工作场所出现“公私不分"的情况 （B）组织信息保密性受损。

（C）组织资产可用性受损。 （D）B+C。

49、GB/T 22080标准中所指"组织与外部方交换信息和软件的协议"必须包含的内容是：(A )

（A）相关各方的信息安全责任和义务。 （B）相关各方的商务利益。

（C）相关各方的技术支持责任。 （D）质量保证条款。

1. 依据GB/T 22080 ,为防止信息未授权的泄露或不当使用，介质处置时的信息处理规程须规定:（D）

（A）向介质写入信息时如何确保符合安全要求。

（B）介质在改变用途前如何妥善处理信息确保符合安全要求。

（C）介质在弃置前如何妥善处理信息确保符合安全要求。

（D）A+B+C

51、监视、调整资源的使用并预测未来容量需求，这是为了保证：（A）

（A）资产的可用性满足业务要求。 （B）资产的完整性符合安全策略。

（C）资产的配置具有可追溯性。 （D）降低成本。

52、是否或如何为办公室增加物理安全防护设计取决于：( D)

（A）该办公室业务活动涉及资产的关键性程度。

（B）该办公室资产被非授权访问或信息泄露的可能性。

（C）安全防护方案的技术难度和成本。

（D）A+B

53、以下属于信息安全事件的情况是：( D)

（A）通信线路出现未知的干扰噪声。

（B）邮件通信被捆绑垃圾邮件。

（C）监视系统侦测到未遂的尝试破解密码行为。

（D）B+C。

54、某软件企业自行开发了用于管理其软件产品的配置管理工具，以下说法错误的是：（C）

（A）该企业用于向顾客交付的软件产品的测试数据应认真加以选择、保护和控制。

（B）该企业的配置管理工具的测试数据应认真加以选择、保护和控制。

（C）该企业配置管理工具不是向顾客交付的成果，因此其测试数据不是需要保护的对象。

（D）该企业配置管理库中的配置项应识别为信息安全相关资产。

55、依据GB/T 22080 ,信息的标记应表明：（ B）

（A）相关供应商信息、日期、资产序列号。

（B）其敏感性和关键性的类别和等级。

（C）所属部门和批准人。

（D）信息的性质，如软件、文档。

56、依据GB/T 22080 ,组织与员工的保密性协议的内容应：(C )

（A）规定的保密责任永久有效。 （B）内容不可变更。

（C）反映组织信息保护需要的保密性或不泄露协议要求。 （D）A+C

57、为了防止对应用系统中信息的未授权访问，正确的做法是：（D）

（A）定期变更用户名和登录口令。（B）按照访问控制策略限制用户访问应用系统功能。-

（C）隔离敏感系统。 （D）B+C

1. 为了实现在网络上自动标识设备，以下做法错误的是（A）

（A）启用动DHCP动态分配IP地址功能。

（B）为网络设备分配固定IP地址。

（C）将每一台计算机MAC与一个IP地址绑定。

（D）采取有效措施禁止修改MAC。

59、信息安全灾备管理中，关于灾难恢复能力，以下说法正确的是：(A

(A )恢复能力等级越高，恢复时间目标越短，恢复点目标越近。

(B )恢复能力等级越高，恢复时间目标越长，恢复点目标越长。

(C )恢复能力等级越高,恢复时间目标越短，恢复点目标越长。

(D )恢复能力等级越高，恢复时间目标越短，恢复点目标越长。

1. 依据GB/T22080,以下属于设备安全中的"支持性设施"的是：（D）

(A)电磁屏蔽系统、照明设施。 (B )环境监控系统、安全防范系统。

(C )不间断电源、消防设施、空气调节装置。 (D)以上全部。

**ISMS测验二**

**一、简述题（每题5分，共10分）**

1、审核员在某公司审核时，发现该公司从保安公司聘用的保安的门卡可通行公司所有的门禁。公司主管信息安全的负责人解释说,因保安负责公司的物理区域安全，他们夜里以及节假日要值班和巡査所有区域，所以只能给保安全权限门卡。审核员对此解释表示认同。如果你是审核员，你将如何做？

1. 请阐述对GB/T 22080中A.13.2.2的审核思路。

**二、案例分析题（每题6分，共30分）**

**请对以下场景进行分析，写出不符合标准条款的编号及内容，并写出不符合事实。**

1. 在某软件开发企业,质量保证部负责对软件开发成果物进行测试,该部门测试人员使用名为"Bugfree“ 的系统记录测试发现的问题，然后由开发人员针对测试人员提出的问题，确定软件修改方案，修改后重新提交测试,通过后由测试人员给出"最终测试通过"的结论。软件开发人员的修改方案以及修改后重新测试的信息也分别在该"Bugfree"系统中予以记录。审核员请开发人员演示上述过程时发现, 幵发人员也可以登录测试问题记录的页面，且能够修改测试记录信息。当审核员问为什么会这样，该开发人员回答说，有时候开发人员与测试人员就软件问题的判定有争议，因此允许开发人员修改测试问题记录，否则会影响开发人员的绩效考核。

A12.4.2

1. 审核员在某公司审核时，按计划到公司的计算机机房现场査看。审核员看到系统管理员王某正忙着安装、调试邮件服务器。IT部主任解释说,公司在现写字楼的租赁已到期，已决定迁至另一街区的某写字楼。王某因下班路上路过新地址，于是在前一天下班时就将邮件服务器拆除，顺便带到新写字楼， 并将电源接通。但今天发现，公司各业务部门搬家的时间表不一致，有几个业务部门仍在现写字楼办公，但因邮件服务器已搬走，无法与境外客户联络，对此这几个部门今天有不少抱怨。为弥补这一情况，系统管理员只好又将邮件服务器拆除装回原机房。

A10.1.2

1. 某公司主营业务为工业设备代理销售。审核员在审核销售部时发现，公司的全部销售业务以及与顾客的关系管理数据的维护均依赖网络及信息系统完成，当问及这些系统的维护和管理时，公司管理者代表解释说，公司维护IT系统的工作全由沈某一人担任，称沈某人非常正直可靠，所有的IT系统维护和监控项目均由其1人完成，从未出过信息安全事故。审核员请来沈某询问，沈某确认其工作职责包括对各业务线小组人员的权限设置、系统运行监视、系飯隹护和升级、以及系统安全策略符合性审核等所有的内容。

A10.1.3

1. 某公司是定向为顾客开发软件的企业。审核组在公司平台业务开发部审核时，抽査到公司正在为顾客开发的"数据管理平台"项目，该项目的系统设计文件由公司高级系统架构师完成，平台开发部主任说：这份系统设计文件因涉及到顾客”数据管理平台“的结沟设计，非常敏感，公司要求开发人员只可读、不可修改，且不可以在公司其他部门传阅。开发人员向审核员演示其对该设计文件的访问权限为只读、可打印，审核员问该开发人员究竟是否被允许打印这份文件，该开发人员表示公司确实没有明确指示他是否可以打印，并补充说："如果您需要，我可以打印给您看，不过请不要带走。

A8.2.2 7.1.3

1. 某公司为国家相关部门指定的敏感票据印刷企业。审核员在现场巡査时发现，公司制版车间的一张办 公桌上散放着工作号为111字9、10、11号的三份《票据生产通知单》，通知单中分别详细列出了三种票据的制版工艺要求。审核员问道这是谁的办公桌时，车间主任回答说，这是制版工艺师的办公桌，他今天请假了，没来上班。

A11.3.3

**ISMS测验三**

**一、单项选择题(从下面各题选项中选出一个最怡当的答案，并将相应字母填在下表相应位置中。每 题1分，共30分。）**

1、认证审核时，审核组应：( A)

（A）在审核前将审核计划提交受审核方确认。

（B）在审核结束时将审核计划提交受审核方确认。

（C）随着审核的进展与受审核方共同确认审核计划。

（D）将审核计划提交审核委托方批准即可。

2、第三方认证审核时，对于审核提出的不符合项，审核组应：( B)

（A）与受审核方共同评审不符合项以确认不符合的条款。

（B）与受审核方共同评审不符合项以确认不符合事实的准确性。

（C）与受审核方共同评审不符合以确认不符合的性质。

（D）以上都对。

3、认证审核初审时，可以不进行第一阶段现场审核的条件之一是：( B)

（A）审核组考虑时间效率可用一个阶段审核完成所有的审核准则要求。

（B）审核组长已充分了解受审核方的管理过程。

（C）受审核方认为一个阶段的审核能完成全部的审核要求。

（D）不允许第一阶段不逬行现场审核的情况。

4、针对获证组织扩大范围的审核，以下说法正确的是：（ A）

（A）一种特殊审核,可以和监督审核一起进行。 （B）是监督审核的形式之一。

（C）审核时抽样的样本范围和监督审核相同。 （D）以上都对。

5、以下可认定为审核范围变更的事项是:( D)

（A）受审核组织增加一个制造场所。（B）受审核组织职能单元和人员规模增加。

（C）受审核组织业务过程增加。 （D）以上全部。

6、在认证审核时,审核组在现场有权限自行决定变更的事项包括：(C )

（A）审核准则。 （B）审核人曰数。

（C）审核路线。 （D）应受审核的业务过程。

7、审核员的检査表应：（B )

（A）事先提交受审核方评审确认。

（B）基于审核准则事先编制。

（C）针对不同的受审核组织应统一格式和内容

（D）由审核组长负责编制审核组使用的检査表。

8、以下属于管理体系审核发现的是：（ C）

（A）审核员看到的物理入口控制方式。

（B）审核员看到的信息系统资源阈值。

（C）审核员看到的移动介质的使用与规定要求的符合性。

（D）审核员看到的项目质量保证活动与CMMI规程的符合性。

9、审核组中的技术专家是：(A )

（A）为审核组提供文化、法律、技术等方面知识咨询的人员。

（B）特别负责对受审核方的专业技术过程进行审核的人员。

（C）审核期间为受审核方提供技术咨询的人员。

（D）从专业的角度对审核员的审核进行观察评价的人员。

10、审核人曰数的计算方式是审核天数乘以：（C)

（A）审核组中审核员+实习审核员+技术专家+观察员的总人数。

（B）审核组中审核员+实习审核员的总人数。

（C）审核组中审核员的总人数。

（D）审核组中审核员+实习审核员+技术专家的总人数。

11、管理体系初次认证审核时，第一阶段审核应：( D )

（A）对受审核方管理体系的策划进行审核和评价，对应标准策划部分条款的要求。

（B）对受审核方管理体系的内部审核及管理评审的有效性进行审核和评价。

（C）对受审核方管理体系文件的符合性、适宜性和有效注进行审核和评价。

（D）对受审核方管理体系文件进行审核和符合性评价。

12、按照”PDCA“思路进行审核，是指：（A )

（A）按照受审核区域活动的"PDCA"过程进行审核。

（B）按照认证机构的"PDCA"流程进行审核。

（C）按照认可规范中规定的"PDCA"流程进行审核。

（D）以上都对。

13、关于审核结论，以下说法正确的是：（D）

（A）审核组综合了所有审核证据进行合理推断的结果。

（B）审核组综合了所有审核证据与受审核方充分协商的结果。

（C）审核组权衡了不符合的审核发现的数量及严重程度后得出的结果。

（D）审核组考虑了审核目的和所有审核发现后得出的审核结果。

14、第三方认证审核时确定审核范围的程序是：(B )

（A）组织提出、与审核组协商、认证机构确认、认证合同规定。

（B）组织申请、认证机构评审、认证合同规定、审核组确认。

（C）组织提出、与咨询机构协商、认证机构确认。

（D）认证机构提出、与组织协商、审核组确认、认证合同规定。

15、审核报告是：（ C)

（A）受审核方的资产。 （B）审核委托方和受审核方的共同资产。

（C）审核委托方的资产。 （D）审核组和审核委托方的资产。

1. 认证审核前,审核祖长须与受审核方确认审核的可行性，特别应考虑：(A)

（A）核实组织申请认证范围内需接受审核的组织结构、场所分布等基本信息。

（B）注意审核的程序性安排事先应对受审核组织保密。

（C）注意审核拟访问的文件、记录、场所等事先应对受审核组织保密。

（D）要求受审核组织做好准备向审核组开放所有信息的访问权。

17、管理体系认证审核时,为了获取审核证据，应考虑的信息源为：（C）

（A）受审核方的业务信息系统相关的活动和数据。

（B）受审核方场所中已确定为管理体系范围内的相关过程和活动。

（C）受审核方申请认证范围内的业务过程和活动。

（D）以上全部。

18、认证审核时，审核拟抽査的样本应：(B)

（A）由受审核方熟悉的人员事先选取，做好准备。

（B）由审核组明确总体并在受控状态下独立抽样。

（C）由审核组和受审核方人员协商抽样。

（D）由受审核方安排的向导实施抽样。

19、认证审核期间，当审核证据表明审核目的不能实现时，审核组应：(D )

（A）—起讨论,决定后续措施。

（B）审核组长权衡，决定后续措施。

（C）由受审核方决定后续措施。

（D）报告审核委托方并说明理由，确定后续措施。

1. 认证审核时，对于审核组提出的不符合审核准则的审核发现，以下说法正确的是( B）

（A）受审核方负责采取纠正措施，纠正措施的实施是审核活动的一部分。

（B）审核组须验证纠正措施的有效性，纠正措施的实施不是审核活动的一部分。

（C）审核组须就不符合项的原因分析提出建议，确定纠正措施是否正确。

（D）采取纠正措施是受审核方的职责，审核组什么都不做。

21、管理体系认证过程包含了：（ D）

（A）现场审核首次会议开始到末次会议结束的所有活动。

（B）从审核准备到审核报告提交期间的所有活动。

（C）一次初审以及至少2次监督审核的所有活动。

（D）从受理认证到证书到期期间所有的审核以及认证服务和管理活动。

22、第三方认证时的监督审核不一定是对整个体系的审核，以下说法正确的是：（D）

（A）组织获得认证范围内的职能区域可以抽査，但标准条款不可以抽査。

（B）组织获得认证范围内的业务过程可以抽査，但职能区域不可以抽査。

（C）组织获得认证范围内的业务过程和职能区域都不可以抽査，仅标准条款可以抽査,

（D）标准条款可以抽査，但针对内审和管理评审以及持续改进方面的审核不可缺少。

23、关于审核组的现场审核,以下说法错误的是:A

（A）审核组在审核期间现场可根据受审核方实际情况及时变更审核范围。

（B）审核组在审核期间现场可调整审核路线和审核资源分配。

（C）审核组遇到重大风险应报告委托方以决定后续措施。

（D）审核组遇到重大风险应报告受审核方以决定后续措施。

24、以下说法正确的是：（A）

（A）审核组的每一次审核，均应向委托所是交审核报告。

（B）认证审核的一阶段审核,可视情况决定是否需要提交审核报告。

（C）监督审核不要求提交审核报告。

（D）特殊审核可视情况决定是否需要提交审核报告。

25、关于管理体系"审核"，以下说法正确的是：（C）

（A）审核是基于文审的方法。

（B）审核是验收性的抽样方法。

（C）审核须采用基于证据的方法。

（D）审核抽样取决于审核的总人日数。

26、关于"审核发现"，以下说法正确的是：（B）

（A）审核发现即审核员观察到的事实。

（B）审核发现可以表明正面的或负面的结果。

（C）审核发现即审核组提出的不符合项报告。

（D）审核发现即审核结论意见。

27、关于"纠正措施"，以下说法正确的是:（C）

（A）针对不符合的原因分析必须采用"因果分析法'

（B）审核组对于不符合项原因分析的准确性影响纠正措施的有效性。

（C）受审核方对于不符合项原因分析的准确性是影响纠正措施有效性的因素之一。

（D）以上都对。

1. 管理体系认证审核的范围即：（ C）

（A）组织的全部经营管理范围。

（B）组织的全部信息系统机房所在的范围。

（C）组织承诺建立、实施和保持管理体系相关的组织' 位置、过程和活动以及时期的范围。

（D）组织机构中所有业务职能涉及的活动范围。

29、管理体系认证是：（A ）。

（A）与管理体系有关的规定要求得到满足的证实活动。

（B）对信息系统是否满足有关的规定要求的评价。

（C）管理体系认证不是合格评定活动。

（D）是信息系统风险管理的实施活动。

30、管理体系审核的抽样过程是：（ D）。

(A )由受审核方负责策划系统性的抽样方案。

(B )验收性质的抽样，决定是否可以认证通过。

(C )通过对总体的评价来推断样本信息。

(D )调査性质的抽样，有弃真的风险和取伪的风险。

**练习题一 单项选择题 参考答案**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **题号** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** |
| **答案** | A | B | C | D | B | D | A | D | A | D | D |
| **题号** | **12** | **13** | **14** | **15** | **16** | **17** | **18** | **19** | **20** | **21** | **22** |
| **答案** | A | A | D | A | B | D | E | C | B | B | C |
| **题号** | **23** | **24** | **25** | **26** | **27** | **28** | **29** | **30** | **31** | **32** | **33** |
| **答案** | D | A | C | A | C | B | A | D | D | C | B |
| **题号** | **34** | **35** | **36** | **37** | **38** | **39** | **40** | **41** | **42** | **43** | **44** |
| **答案** | D | A | D | A | C | BD | C | B | B | D | AC |
| **题号** | **45** | **46** | **47** | **48** | **49** | **50** | **51** | **52** | **53** | **54** | **55** |
| **答案** | B | D | D | C | B | C | A | C | D | A | D |
| **题号** | **56** | **57** | **58** | **59** | **60** | **61** | **62** | **63** | **64** | **65** | **66** |
| **答案** | B | C | A | D | B | D | B | D | D | B | A |
| **题号** | **67** | **68** | **69** | **70** | **71** | **72** | **73** | **74** | **75** | **76** | **77** |
| **答案** | C | D | C | D | A | C | D | D | CD | AD | B |
| **题号** | **78** | **79** | **80** | **81** | **82** | **83** | **84** | **85** | **86** | **87** | **88** |
| **答案** | D | B | A | A | B | C | D | CD | B | A | / |

**练习题二 多项选择题 参考答案**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **题号** | **1** | **2** | **3** | **4** | **5** | **6** | **7** |
| **答案** | AC | ACD | AC | ABCD | ABC | ACD | ABCD |
| **题号** | **8** | **9** | **10** | **11** | **12** | **13** | **14** |
| **答案** | BCD | ABCD | ABCD | CD | ABD | ABC | BCD |
| **题号** | **15** | **16** | **17** | **18** | **19** | **20** | **21** |
| **答案** | AB | CD | ABCD | ACD | BCD | ABCD | AB |
| **题号** | **22** | **23** | **24** | **25** | **26** | **27** | **28** |
| **答案** | ABD | AB | ABD | ABCD | ABCD | ABD | ABC |
| **题号** | **29** | **30** | **31** | **32** | **33** | **34** | **35** |
| **答案** | ABCD | ABC | BD | ABCD | ABCD | ABC | / |

**练习题三 判断题**

**参考答案**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **题号** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** |
| **答案** | T | T | T | F | F | F | T | F | F | T |
| **题号** | **11** | **12** | **13** | **14** | **15** | **16** | **17** | **18** | **19** | **20** |
| **答案** | T | T | F | F | T | F | F | F | T | F |
| **题号** | **21** | **22** | **23** | **24** | **25** | **26** | **27** | **28** | **29** | **30** |
| **答案** | T | T | T | F | T | F | T | T | T | F |

**练习题四 案例分析题**

**参考答案**

1. **不符合条款：A11.4.6**
2. **不符合条款：A9.1.2**
3. **不符合条款：4.2.1d)3**
4. **不符合条款：A13.2.2**
5. **不符合条款：A10.2.1**
6. **不符合条款：A9.1.2**
7. **不符合条款：A9.2.6**
8. **不符合条款：A8.2.2**
9. **不符合条款：A8.3.3**
10. **不符合条款：4.3.3**
11. **不符合条款：A11.6.1**
12. **不符合条款：A10.1.2**
13. **不符合条款：A10.1.3**
14. **不符合条款：A7.1.3**
15. **不符合条款：A11.3.3**

**ISMS测验一 参考答案**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **题号** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** |
| **答案** | C | B | D | D | C | B | A | D | A | C |
| **题号** | **11** | **12** | **13** | **14** | **15** | **16** | **17** | **18** | **19** | **20** |
| **答案** | B | C | B | D | B | D | A | A | B | C |
| **题号** | **21** | **22** | **23** | **24** | **25** | **26** | **27** | **28** | **29** | **30** |
| **答案** | D | C | C | D | A | C | C | A | A | B |
| **题号** | **31** | **32** | **33** | **34** | **35** | **36** | **37** | **38** | **39** | **40** |
| **答案** | D | C | A | B | C | D | B | D | D | D |
| **题号** | **41** | **42** | **43** | **44** | **45** | **46** | **47** | **48** | **49** | **50** |
| **答案** | B | A | D | A | C | B | C | D | A | D |
| **题号** | **51** | **52** | **53** | **54** | **55** | **56** | **57** | **58** | **59** | **60** |
| **答案** | A | D | D | C | B | C | D | A | A | D |

**ISMS测验二 参考答案**

1. **简述题（每题5分，共10分）**

**二、案例分析题（每题6分，共30分)**

**不符合条款：A12.4.2**

**不符合条款：A10.1.2**

**不符合条款：A10.1.3**

**不符合条款：A8.2.2 7.1.3**

**不符合条款：A11.3.3**

**ISMS测验三 参考答案**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **题号** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| **答案** | A | B | B | A | D | C | B | C | A | C |
| **题号** | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| **答案** | D | A | D | B | C | A | C | B | D | B |
| **题号** | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 |
| **答案** | D | D | A | A | C | B | C | C | A | D |