1.　以下对信息安全描述不正确的是

A.信息安全的基本要素包括保密性、完整性和可用性

B.信息安全就是保障企业信息系统能够连续、可靠、正常地运行，使安全事件对业务造成的影响减到最小，确保组织业务运行的连续性

C.信息安全就是不出安全事故　/事件

D.信息安全不仅仅只考虑防止信息泄密就可以了

【答案】　C

2.　以下对信息安全管理的描述错误的是

A.保密性、完整性、可用性

B.抗抵赖性、可追溯性

C.真实性私密性可靠性

D.增值性

【答案】　D

3.　以下对信息安全管理的描述错误的是

A.信息安全管理的核心就是风险管理

B.人们常说，三分技术，七分管理，可见管理对信息安全的重要性

C.安全技术是信息安全的构筑材料，安全管理是真正的粘合剂和催化剂

D.信息安全管理工作的重点是信息系统，而不是人

【答案】　D

4.　企业按照ＩＳＯ２７００１标准建立信息安全管理体系的过程中，对关键成功因素的描述不正确的是

A.　不需要全体员工的参入，只要ＩＴ部门的人员参入即可

B.　来自高级管理层的明确的支持和承诺

C.对企业员工提供必要的安全意识和技能的培训和教育

D.　所有管理者、 员工及其他伙伴方理解企业信息安全策略、　指南和标准，并遵照执行

【答案】　A

5.　信息安全管理体系（　ISMS）是一个怎样的体系，以下描述不正确的是

A. ISMS是一个遵循　PDCA模式的动态发展的体系

B.　ISMS是一个文件化、系统化的体系

C.ISMS 采取的各项风险控制措施应该根据风险评估等途径得出的需求而定

D.　ISMS 应该是一步到位的，应该解决所有的信息安全问题

【答案】　D

6.　PDCA特征的描述不正确的是

A.　顺序进行，周而复始，发现问题，分析问题，然后是解决问题

B.　大环套小环，安全目标的达成都是分解成多个小目标，一层层地解决问题

C.阶梯式上升，每次循环都要进行总结，巩固成绩，改进不足

D.　信息安全风险管理的思路不符合　PDCA的问题解决思路

【答案】　D

7.　以下哪个不是信息安全项目的需求来源

A.　国家和地方政府法律法规与合同的要求

B.　风险评估的结果

C.组织原则目标和业务需要

D. 企业领导的个人意志

【答案】　D

8.　ISO27001 认证项目一般有哪几个阶段？

A. 管理评估，技术评估，操作流程评估

B.　确定范围和安全方针，　风险评估，风险控制（文件编写），体系运行，认证

C.产品方案需求分析，解决方案提供，实施解决方案

D. 基础培训，　RA 培训，文件编写培训，内部审核培训

【答案】　B

9.　构成风险的关键因素有哪些？

A. 人，财，物

B.　技术，管理和操作

C.资产，威胁和弱点

D. 资产，可能性和严重性

【答案】　C

10.　以下哪些不是应该识别的信息资产？

A.　网络设备

B.客户资料

C. 办公桌椅

D. 系统管理员

【答案】　C

11.　以下哪些是可能存在的威胁因素？　　B

A.　设备老化故障

B.病毒和蠕虫

C. 系统设计缺陷

D. 保安工作不得力

【答案】　B

12.　以下哪些不是可能存在的弱点问题？

A.　保安工作不得力

B.应用系统存在　Bug

C. 内部人员故意泄密

D. 物理隔离不足

【答案】　C

13.　风险评估的过程中，首先要识别信息资产，资产识别时，以下哪个不是需要遵循的原则？

A.　只识别与业务及信息系统有关的信息资产，分类识别

B.所有公司资产都要识别

C. 可以从业务流程出发，识别各个环节和阶段所需要以及所产出的关键资产

D. 资产识别务必明确责任人、保管者和用户

【答案】　B

14.　风险分析的目的是？

A.　在实施保护所需的成本与风险可能造成的影响之间进行技术平衡；

B.在实施保护所需的成本与风险可能造成的影响之间进行运作平衡；

C. 在实施保护所需的成本与风险可能造成的影响之间进行经济平衡；

D. 在实施保护所需的成本与风险可能造成的影响之间进行法律平衡；

【答案】　C

15.　对于信息安全风险的描述不正确的是？

A. 企业信息安全风险管理就是要做到零风险

B.　在信息安全领域，风险（　Risk）就是指信息资产遭受损坏并给企业带来负面影响及其潜在可能性

C.风险管理（ Risk Management ）就是以可接受的代价，识别控制减少或消除可能影响信息系统的安全风险的过程。

D. 风险评估（Risk Assessment）就是对信息和信息处理设施面临的威胁、受到的影响、存在的弱点以及威胁发生的可能性的评估。

【答案】　A

16.　有关定性风险评估和定量风险评估的区别，以下描述不正确的是

A. 定性风险评估比较主观，而定量风险评估更客观

B.　定性风险评估容易实施，定量风险评估往往数据准确性很难保证

C.定性风险评估更成熟，定量风险评估还停留在理论阶段

D. 定性风险评估和定量风险评估没有本质区别，可以通用

【答案】　D

17.　降低企业所面临的信息安全风险，可能的处理手段不包括哪些

A. 通过良好的系统设计、及时更新系统补丁，降低或减少信息系统自身的缺陷

B.　通过数据备份、双机热备等冗余手段来提升信息系统的可靠性；

C.建立必要的安全制度和部署必要的技术手段，防范黑客和恶意软件的攻击

D. 通过业务外包的方式，转嫁所有的安全风险

【答案】　D

18.　风险评估的基本过程是怎样的？

A. 识别并评估重要的信息资产，识别各种可能的威胁和严重的弱点，最终确定风险

B.　通过以往发生的信息安全事件，找到风险所在

C.风险评估就是对照安全检查单，查看相关的管理和技术措施是否到位

D. 风险评估并没有规律可循，完全取决于评估者的经验所在

【答案】　A

19.　企业从获得良好的信息安全管控水平的角度出发，以下哪些行为是适当的

A. 只关注外来的威胁，忽视企业内部人员的问题

B.　相信来自陌生人的邮件，好奇打开邮件附件

C.开着电脑离开，就像离开家却忘记关灯那样

D. 及时更新系统和安装系统和应用的补丁

【答案】　D

20.　以下对 ISO27001 标准的描述不正确的是

A. 企业通过 ISO27001 认证则必须符合 ISO27001 信息安全管理体系规范

的所有要求

B.　ISO27001标准与信息系统等级保护等国家标准相冲突

C.ISO27001是源自于英国的国家标准　　BS7799

D.　ISO27001 是当前国际上最被认可的信息安全管理标准

【答案】　B

21.　对安全策略的描述不正确的是

A.　信息安全策略（或者方针）是由组织的最高管理者正式制订和发布的描述企业信息安全目标和方向，用于指导信息安全管理体系的建立和实施过程

B.　策略应有一个属主，负责按复查程序维护和复查该策略

C.安全策略的内容包括管理层对信息安全目标和原则的声明和承诺；

D.　安全策略一旦建立和发布，则不可变更；

【答案】　D

22.　以下对企业信息安全活动的组织描述不正确的是

A.　企业应该在组织内建立发起和控制信息安全实施的管理框架。

B.　企业应该维护被外部合作伙伴或者客户访问和使用的企业信息处理设施和信息资产的安全。

C.在没有采取必要控制措施，包括签署相关协议之前，不应该授权给外部伙伴访问。应该让外部伙伴意识到其责任和必须遵守的规定。

D.　企业在开展业务活动的过程中，　应该完全相信员工，　不应该对内部员工采取安全管控措施

【答案】　D

23.　企业信息资产的管理和控制的描述不正确的是

A.　企业应该建立和维护一个完整的信息资产清单，并明确信息资产的管控责任；

B.　企业应该根据信息资产的重要性和安全级别的不同要求，采取对应的管控措施；

C.企业的信息资产不应该分类分级，所有的信息系统要统一对待

D.　企业可以根据业务运作流程和信息系统拓扑结构来识别所有的信息资产

【答案】　C

24.　有关人员安全的描述不正确的是

A.　人员的安全管理是企业信息安全管理活动中最难的环节

B.　重要或敏感岗位的人员入职之前，需要做好人员的背景检查

C.企业人员预算受限的情况下，　职责分离难以实施，　企业对此无能为力，也无需做任何工作

D.　人员离职之后，必须清除离职员工所有的逻辑访问帐号

【答案】　C

25.　以下有关通信与日常操作描述不正确的是

A.　信息系统的变更应该是受控的

B.　企业在岗位设计和人员工作分配时应该遵循职责分离的原则

C移动介质使用是一个管理难题，应该采取有效措施，防止信息泄漏

D.　内部安全审计无需遵循独立性、客观性的原则

【答案】　D

26. 以下有关访问控制的描述不正确的是

A. 口令是最常见的验证身份的措施，也是重要的信息资产，应妥善保护和管理

B. 系统管理员在给用户分配访问权限时，应该遵循“最小特权原则”，即分配给员工的访问权限只需满足其工作需要的权限，工作之外的权限一律不能分配

C.单点登录系统（一次登录/验证，即可访问多个系统）最大的优势是提升了便利性，但是又面临着“把所有鸡蛋放在一个篮子”的风险；

D. 双因子认证（又称强认证）就是一个系统需要两道密码才能进入；

【答案】 D

27. 有关信息系统的设计、开发、实施、运行和维护过程中的安全问题，以下描述错误的是

A. 信息系统的开发设计，应该越早考虑系统的安全需求越好

B. 信息系统的设计、开发、实施、运行和维护过程中的安全问题，不仅仅要考虑提供一个安全的开发环境，同时还要考虑开发出安全的系统

C.信息系统在加密技术的应用方面，其关键是选择密码算法，而不是密钥的管理

D. 运营系统上的敏感、真实数据直接用作测试数据将带来很大的安全风险

【答案】 C

28. 有关信息安全事件的描述不正确的是

A. 信息安全事件的处理应该分类、分级

B. 信息安全事件的数量可以反映企业的信息安全管控水平

C.某个时期内企业的信息安全事件的数量为零，这意味着企业面临的信息安全风险很小

D. 信息安全事件处理流程中的一个重要环节是对事件发生的根源的追溯，以吸取教训、总结经验，防止类似事情再次发生

【答案】 C

29. 以下有关信息安全方面的业务连续性管理的描述，不正确的是

A. 信息安全方面的业务连续性管理就是要保障企业关键业务在遭受重大灾难/破坏时，能够及时恢复，保障企业业务持续运营

B. 企业在业务连续性建设项目一个重要任务就是识别企业关键的、核心业务

C.业务连续性计划文档要随着业务的外部环境的变化，及时修订连续性计划文档

D. 信息安全方面的业务连续性管理只与 IT 部门相关，与其他业务部门人员无须参入

【答案】 D

30. 企业信息安全事件的恢复过程中，以下哪个是最关键的？

A. 数据

B. 应用系统

C.通信链路

D. 硬件/软件

【答案】 A

31. 企业 ISMS(信息安全管理体系)建设的原则不包括以下哪个

A. 管理层足够重视

B. 需要全员参与

C.不必遵循过程的方法

D. 需要持续改进

【答案】 C

32. PDCA特征的描述不正确的是

A. 顺序进行，周而复始，发现问题，分析问题，然后是解决问题

B. 大环套小环，安全目标的达成都是分解成多个小目标，一层层地解决问题

C.阶梯式上升，每次循环都要进行总结，巩固成绩，改进不足

D. 信息安全风险管理的思路不符合 PDCA的问题解决思路

【答案】 D

33. 对于在 ISMS 内审中所发现的问题，在审核之后应该实施必要的改进措施并进行跟踪和评价，以下描述不正确的是？

A. 改进措施包括纠正和预防措施

B. 改进措施可由受审单位提出并实施

C.不可以对体系文件进行更新或修改

D. 对改进措施的评价应该包括措施的有效性的分析

【答案】 C

34. ISMS的审核的层次不包括以下哪个？

A. 符合性审核

B. 有效性审核

C.正确性审核

D. 文件审核

【答案】 C

35. 以下哪个不可以作为 ISMS管理评审的输入

A. ISMS审计和评审的结果

B. 来自利益伙伴的反馈

C. 某个信息安全项目的技术方案

D. 预防和纠正措施的状态

【答案】 C

36. 有关认证和认可的描述，以下不正确的是

A. 认证就是第三方依据程序对产品、过程、服务符合规定要求给予书面保证（合格证书）

B. 根据对象的不同，认证通常分为产品认证和体系认证

C.认可是由某权威机构依据程序对某团体或个人具有从事特定任务的能力给予的正式承认

D. 企业通过 ISO27001 认证则说明企业符合 ISO27001 和 ISO27002 标准的要求

【答案】 D

37. 信息的存在及传播方式

A. 存在于计算机、磁带、纸张等介质中

B. 记忆在人的大脑里

C..　　通过网络打印机复印机等方式进行传播

D.　通过投影仪显示

【答案】　D

38.　下面哪个组合不是是信息资产

A.　硬件、软件、文档资料

B.　　关键人员

C..　　组织提供的信息服务

D.　桌子、椅子

【答案】　D

39.　实施 ISMS 内审时，确定　ISMS 的控制目标、控制措施、过程和程序应该要符合相关要求，以下哪个不是？

A.　约定的标准及相关法律的要求

B.已识别的安全需求

C. 控制措施有效实施和维护

D. ISO13335 风险评估方法

【答案】　D

40.　以下对审核发现描述正确的是

A.　用作依据的一组方针、程序或要求

B.与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

C. 将收集到的审核证据依照审核准则进行评价的结果，　　可以是合格 / 符合项，也可以是不合格 / 不符合项

D. 对审核对象的物理位置、组织结构、活动和过程以及时限的描述

【答案】　C

41.　ISMS 审核常用的审核方法不包括？

A.　纠正预防

B.文件审核

C. 现场审核

D. 渗透测试

【答案】　A

42.　ISMS 的内部审核员（非审核组长）的责任不包括？

A.　熟悉必要的文件和程序；

B.根据要求编制检查列表；

C. 配合支持审核组长的工作，有效完成审核任务；

D. 负责实施整改内审中发现的问题；

【答案】　D

43.　审核在实施审核时，所使用的检查表不包括的内容有？

A.　审核依据

B.审核证据记录

C. 审核发现

D. 数据收集方法和工具

【答案】　C

44.　ISMS 审核时，首次会议的目的不包括以下哪个？

A.　明确审核目的、审核准则和审核范围

B.明确审核员的分工

C. 明确接受审核方责任，为配合审核提供必要资源和授权

D. 明确审核进度和审核方法，且在整个审核过程中不可调整

【答案】 D

45. ISMS审核时，对审核发现中，以下哪个是属于严重不符合项？

A. 关键的控制程序没有得到贯彻，缺乏标准规定的要求可构成严重不符合项

B.风险评估方法没有按照 ISO27005（信息安全风险管理）标准进行

C. 孤立的偶发性的且对信息安全管理体系无直接影响的问题；

D. 审核员识别的可能改进项

【答案】 D

46. 以下关于 ISMS内部审核报告的描述不正确的是？

A. 内审报告是作为内审小组提交给管理者代表或最高管理者的工作成果

B.内审报告中必须包含对不符合性项的改进建议

C. 内审报告在提交给管理者代表或者最高管理者之前应该受审方管理者沟通协商，核实报告内容。

D. 内审报告中必须包括对纠正预防措施实施情况的跟踪

【答案】 D

47. 信息系统审核员应该预期谁来授权对生产数据和生产系统的访问？

A.流程所有者

B.系统管理员

C.安全管理员

D.数据所有者

【答案】 D

48. 当保护组织的信息系统时，在网络防火墙被破坏以后，通常的下一道防线是下列哪一项？

A. 个人防火墙

B.防病毒软件

C.入侵检测系统

D.虚拟局域网设置

【答案】 C

49. 负责授权访问业务系统的职责应该属于：

A.数据拥有者

B.安全管理员

C. IT 安全经理

D.请求者的直接上司

【答案】 A

50. 在提供给一个外部代理商访问信息处理设施前，一个组织应该怎么做？

A.外部代理商的处理应该接受一个来自独立代理进行的 IS 审计。

B.外部代理商的员工必须接受该组织的安全程序的培训。

C. 来自外部代理商的任何访问必须限制在停火区（ DMZ）

D.该组织应该进行风险评估，并制定和实施适当的控制。

【答案】　　D

51.　处理报废电脑的流程时，以下哪一个选项对于安全专业人员来说是最重要考虑的内容？

A.在扇区这个级别上，硬盘已经被多次重复写入，但是在离开组织前没有进行重新格式化。

B.硬盘上所有的文件和文件夹都分别删除了，并在离开组织进行重新格式化。

C. 在离开组织前，通过在硬盘特定位置上洞穿盘片，进行打洞，使得硬盘变得不可读取。

D.由内部的安全人员将硬盘送到附近的金属回收公司，对硬盘进行登记并粉碎。

【答案】　　B

52.　一个组织已经创建了一个策略来定义用户禁止访问的网站类型。哪个是最有效的技术来达成这个策略？

A.A.状态检测防火墙

B.B.网页内容过滤

C..网页缓存服务器

D.D.代理服务器

【答案】　B

53.　当组织将客户信用审查系统外包给第三方服务提供商时，下列哪一项是信息安全专业人士最重要的考虑因素？该提供商：

A.满足并超过行业安全标准

B.同意可以接受外部安全审查

C.其服务和经验有很好的市场声誉

D.符合组织的安全策略

【答案】　D

54.　一个组织将制定一项策略以定义了禁止用户访问的　　WEB 站点类型。为强制执行这一策略，最有效的技术是什么？

A.状态检测防火墙

B.WE 内容过滤器

C.WEB 缓存服务器

D.应该代理服务器

【答案】　B

55.　在制定一个正式的企业安全计划时，最关键的成功因素将是？

A.成立一个审查委员会

B.建立一个安全部门

C.向执行层发起人提供有效支持

D.选择一个安全流程的所有者

【答案】　C

56.　对业务应用系统授权访问的责任属于：

A.数据所有者

B.安全管理员

C.IT 安全经理

D.申请人的直线主管

【答案】 A

57. 下列哪一项是首席安全官的正常职责？

A.定期审查和评价安全策略

B.执行用户应用系统和软件测试与评价

C.授予或废除用户对 IT 资源的访问权限

D.批准对数据和应用系统的访问权限

【答案】 B

58. 向外部机构提供其信息处理设施的物理访问权限前，组织应当做什么？

A.该外部机构的过程应当可以被独立机构进行 IT 审计

B.该组织应执行一个风险评估，设计并实施适当的控制

C.该外部机构的任何访问应被限制在 DMZ 区之内

D.应当给该外部机构的员工培训其安全程序

【答案】 B

59. 某组织的信息系统策略规定， 终端用户的 ID 在该用户终止后 90 天内失效。组织的信息安全内审核员应：

A.报告该控制是有效的， 因为用户 ID 失效是符合信息系统策略规定的时间段的

B.核实用户的访问权限是基于用所必需原则的

C.建议改变这个信息系统策略，以保证用户 ID 的失效与用户终止一致

D.建议终止用户的活动日志能被定期审查

【答案】 C

60. 减少与钓鱼相关的风险的最有效控制是：

A.系统的集中监控

B.钓鱼的信号包括在防病毒软件中

C.在内部网络上发布反钓鱼策略

D.对所有用户进行安全培训

【答案】 D

61. 在人力资源审计期间， 安全管理体系内审员被告知在 IT 部门和人力资源部门中有一个关于期望的 IT 服务水平的口头协议。 安全管理体系内审员首先应该做什么？

A.为两部门起草一份服务水平协议

B.向高级管理层报告存在未被书面签订的协议

C.向两部门确认协议的内容

D.推迟审计直到协议成为书面文档

【答案】 C

62. 下面哪一个是定义深度防御安全原则的例子？

A.使用由两个不同提供商提供的防火墙检查进入网络的流量

B.在主机上使用防火墙和逻辑访问控制来控制进入网络的流量

C.在数据中心建设中不使用明显标志

D.使用两个防火墙检查不同类型进入网络的流量

【答案】 A

63. 下面哪一种是最安全和最经济的方法，对于在一个小规模到一个中等规模的组织中通过互联网连接私有网络？

A.　虚拟专用网

B.专线

C. 租用线路

D. 综合服务数字网　.

【答案】　A

64.　通过社会工程的方法进行非授权访问的风险可以通过以下方法避免：

A.　安全意识程序

B.非对称加密

C. 入侵侦测系统

D. 非军事区

【答案】　A

65.　在安全人员的帮助下，对数据提供访问权的责任在于：

A.　数据所有者　.

B.程序员

C. 系统分析师　.

D. 库管员

【答案】　A

66.　信息安全策略　,声称 "密码的显示必须以掩码的形式　　"的目的是防范下面哪种攻击风险？

A.　尾随

B.垃圾搜索

C. 肩窥

D. 冒充

【答案】　C

67.　管理体系审计员进行通信访问控制审查，首先应该关注：

A.　维护使用各种系统资源的访问日志

B.在用户访问系统资源之前的授权和认证

C. 通过加密或其他方式对存储在服务器上数据的充分保护

D. 确定是否可以利用终端系统资源的责任制和能力　　.

【答案】　D

68.　下列哪一种防病毒软件的实施策略在内部公司网络中是最有效的：

A.　服务器防毒软件

B.病毒墙

C. 工作站防病毒软件

D. 病毒库及时更新

【答案】　D

69.　测试程序变更管理流程时，安全管理体系内审员使用的最有效的方法是：

A.由系统生成的信息跟踪到变更管理文档

B.检查变更管理文档中涉及的证据的精确性和正确性

C. 由变更管理文档跟踪到生成审计轨迹的系统

D. 检查变更管理文档中涉及的证据的完整性

【答案】　A

70. 内部审计部门 ,从组织结构上向财务总监而不是审计委员会报告 ,最有可能：

A.导致对其审计独立性的质疑

B.报告较多业务细节和相关发现

C. 加强了审计建议的执行

D. 在建议中采取更对有效行动

【答案】 A

71. 下面哪一种情况可以使信息系统安全官员实现有效进行安全控制的目的 ？

A.完整性控制的需求是基于风险分析的结果

B.控制已经过了测试

C. 安全控制规范是基于风险分析的结果

D. 控制是在可重复的基础上被测试的

【答案】 D

72. 下列哪一种情况会损害计算机安全策略的有效性？

A.发布安全策略时

B.重新检查安全策略时

C. 测试安全策略时

D. 可以预测到违反安全策略的强制性措施时

【答案】 D

73. 组织的安全策略可以是广义的，也可以是狭义的，下面哪一条是属于广义的安全策略？

A.应急计划

B.远程办法

C. 计算机安全程序

D. 电子邮件个人隐私

【答案】 C

74. 基本的计算机安全需求不包括下列哪一条：

A.安全策略和标识

B.绝对的保证和持续的保护

C. 身份鉴别和落实责任

D. 合理的保证和连续的保护

【答案】 B

75. 软件的盗版是一个严重的问题。在下面哪一种说法中反盗版的策略和实际行为是矛盾的？

A.员工的教育和培训

B.远距离工作（ Telecommuting）与禁止员工携带工作软件回家

C. 自动日志和审计软件

D. 策略的发布与策略的强制执行

【答案】 B

76. 组织内数据安全官的最为重要的职责是：

A.推荐并监督数据安全策略

B.在组织内推广安全意识

C. 制定 IT 安全策略下的安全程序 /流程

D. 管理物理和逻辑访问控制
【答案】 A
77. 下面哪一种方式，能够最有效的约束雇员只能履行其分内的工作？
A.应用级访问控制
B.数据加密
C. 卸掉雇员电脑上的软盘和光盘驱动器
D. 使用网络监控设备
【答案】 A
78. 内部审计师发现不是所有雇员都了解企业的信息安全策略。内部审计师应当得出以下哪项结论：
A.这种缺乏了解会导致不经意地泄露敏感信息
B.信息安全不是对所有职能都是关键的
C. IS审计应当为那些雇员提供培训
D. 该审计发现应当促使管理层对员工进行继续教育
【答案】 A
79. 设计信息安全策略时，最重要的一点是所有的信息安全策略应该 :
A. 非现场存储
B.b) 由 IS经理签署
C. 发布并传播给用户
D. 经常更新
【答案】 C
80. 负责制定、执行和维护内部安全控制制度的责任在于 :
A. IS 审计员．
B.管理层．
C.外部审计师 ．
D.程序开发人员 ．
【答案】 B
81. 组织与供应商协商服务水平协议，下面哪一个最先发生？
A.制定可行性研究 ．
B.检查是否符合公司策略 ．
C.草拟服务水平协议 ．
D.草拟服务水平要求
【答案】 B
82. 以下哪一个是数据保护的最重要的目标？
A.确定需要访问信息的人员
B.确保信息的完整性
C.拒绝或授权对系统的访问
D.监控逻辑访问
【答案】 A
83. 在逻辑访问控制中如果用户账户被共享，这种局面可能造成的最大风险是：
A.非授权用户可以使用 ID 擅自进入 ．
B.用户访问管理费时 ．
C.很容易猜测密码 ．

D.无法确定用户责任
【答案】 D
84. 作为信息安全治理的成果 ,战略方针提供了 :
A.企业所需的安全要求
B.遵从最佳实务的安全基准
C. 日常化制度化的解决方案
D. 风险暴露的理解
【答案】 A
85. 企业由于人力资源短缺, IT 支持一直以来由一位最终用户兼职，最恰当的补偿性控制是：
A.限制物理访问计算设备
B.检查事务和应用日志
C. 雇用新 IT 员工之前进行背景调查
D. 在双休日锁定用户会话
【答案】 B
86. 关于安全策略的说法，不正确的是
A.得到安全经理的审核批准后发布
B. 应采取适当的方式让有关人员获得并理解最新版本的策略文档
C.控制安全策略的发布范围，注意保密
D.系统变更后和定期的策略文件评审和改进
【答案】 A
87. 哪一项不是管理层承诺完成的？
A.确定组织的总体安全目标
B. 购买性能良好的信息安全产品
C.推动安全意识教育
D. 评审安全策略的有效性
【答案】 B
88. 安全策略体系文件应当包括的内容不包括
A.信息安全的定义、总体目标、范围及对组织的重要性
B.对安全管理职责的定义和划分
C. 口令、加密的使用是阻止性的技术控制措施；
D. 违反安全策略的后果
【答案】 C
89. 对信息安全的理解，正确的是
A.信息资产的保密性、完整性和可用性不受损害的能力，是通过信息安全保障措施实现的
B. 通过信息安全保障措施，确保信息不被丢失
C. 通过信息安全保证措施，确保固定资产及相关财务信息的完整性
D. 通过技术保障措施，确保信息系统及财务数据的完整性、机密性及可用性
【答案】 A
90. 以下哪项是组织中为了完成信息安全目标，针对信息系统，遵循安全策略，按照规定的程序，运用恰当的方法，而进行的规划、组织、指导、协调和控制等活动？

A.反应业务目标的信息安全方针、目标以及活动；
B.来自所有级别管理者的可视化的支持与承诺；
C.提供适当的意识、教育与培训
D.以上所有
【答案】 D
91. 信息安全管理体系要求的核心内容是？
A.风险评估
B.关键路径法
C.PDCA循环
D.PERT
【答案】 C
92. 有效减少偶然或故意的未授权访问、误用和滥用的有效方法是如下哪项？
A.访问控制
B.职责分离
C.加密
D.认证
【答案】 B
93. 下面哪一项组成了 CIA 三元组？
A.保密性，完整性，保障
B.保密性，完整性，可用性
C.保密性，综合性，保障
D.保密性，综合性，可用性
【答案】 B
94. 在信息安全策略体系中，下面哪一项属于计算机或信息安全的强制性规则？
A.标准（ Standard）
B.安全策略（ Security policy ）
C.方针（ Guideline ）
D.流程（ Procedure）
【答案】 A
95. 在许多组织机构中，产生总体安全性问题的主要原因是：
A.缺少安全性管理
B.缺少故障管理
C.缺少风险分析
D.缺少技术控制机制
【答案】 A
96. 下面哪一项最好地描述了风险分析的目的？
A.识别用于保护资产的责任义务和规章制度
B.识别资产以及保护资产所使用的技术控制措施
C.识别资产、脆弱性并计算潜在的风险
D.识别同责任义务有直接关系的威胁
【答案】 C
97. 以下哪一项对安全风险的描述是准确的？

A.安全风险是指一种特定脆弱性利用一种或一组威胁造成组织的资产损失或损害的可能性。

B.安全风险是指一种特定的威胁利用一种或一组脆弱性造成组织的资产损失事实。

C.安全风险是指一种特定的威胁利用一种或一组脆弱性造成组织的资产损失或损害的可能性

D.安全风险是指资产的脆弱性被威胁利用的情形。

【答案】 C

98. 以下哪些不属于脆弱性范畴？

A.黑客攻击

B.操作系统漏洞

C.应用程序 BUG

D.人员的不良操作习惯

【答案】 A

99. 依据信息系统安全保障模型，以下那个不是安全保证对象

A.机密性

B.管理

C过程

D.人员

【答案】 A

100. 以下哪一项是已经被确认了的具有一定合理性的风险？

A.总风险

B.最小化风险

C.可接受风险

D.残余风险

【答案】 C

101. 以下哪一种人给公司带来最大的安全风险？

A.临时工

B.咨询人员

C以前员工

D.当前员工

【答案】 D

102. 一组将输入转化为输出的相互关联或相互作用的什么叫做过程？

A.数据

B.信息流

C.活动

D.模块

【答案】 C

103. 系统地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，称为什么？

A.戴明循环

B.过程方法

C.管理体系

D. 服务管理

【答案】　B

104.　拒绝式服务攻击会影响信息系统的哪个特性？

A.完整性

B.可用性

C.机密性

D.可控性

【答案】　B

105.　在信息系统安全中，风险由以下哪两种因素共同构成的？

A.攻击和脆弱性

B.威胁和攻击

C.威胁和脆弱性

D.威胁和破坏

【答案】　C

106.　在信息系统安全中，暴露由以下哪两种因素共同构成的？

A.攻击和脆弱性

B.威胁和攻击

C.威胁和脆弱性

D.威胁和破坏

【答案】　A

107.　信息安全管理最关注的是？

A.外部恶意攻击

B.病毒对 PC的影响

C.内部恶意攻击

D. 病毒对网络的影响

【答案】　C

108.　从风险管理的角度，以下哪种方法不可取？

A.接受风险

B.分散风险

C.转移风险

D.拖延风险

【答案】　D

109.　ISMS 文档体系中第一层文件是？

A.信息安全方针政策

B.信息安全工作程序

C.信息安全作业指导书

D.信息安全工作记录

【答案】　A

110.　以下哪种风险被定义为合理的风险？

A.最小的风险

B.可接收风险

C.残余风险

D.总风险

【答案】　B

111.　从目前的情况看，对所有的计算机系统来说，以下哪种威胁是最

为严重的，可能造成巨大的损害？

A.没有充分训练或粗心的用户

B.第三方

C.黑客

D.心怀不满的雇员

【答案】　D

112.　如果将风险管理分为风险评估和风险减缓，那么以下哪个不属于风险减缓的内容？

A.计算风险

B.选择合适的安全措施

C.实现安全措施

D.接受残余风险

【答案】　A

113.　通常最好由谁来确定系统和数据的敏感性级别？

A.审计师

B.终端用户

C.拥有者

D.系统分析员

【答案】　C

114.　风险分析的目的是？

A.在实施保护所需的成本与风险可能造成的影响之间进行技术平衡；

B.在实施保护所需的成本与风险可能造成的影响之间进行运作平衡；

C.在实施保护所需的成本与风险可能造成的影响之间进行经济平衡；

D.在实施保护所需的成本与风险可能造成的影响之间进行法律平衡；

【答案】　C

115.　以下哪个不属于信息安全的三要素之一？

A.　机密性

B.　完整性

C.抗抵赖性

D.可用性

【答案】　C

116.　ISMS 指的是什么？

A.信息安全管理

B.信息系统管理体系

C.信息系统管理安全

D.信息安全管理体系

【答案】　D

117.　在确定威胁的可能性时，可以不考虑以下哪个？

A.　威胁源

B.潜在弱点

C现有控制措施

D.攻击所产生的负面影响

【答案】　D

118.　在风险分析中，以下哪种说法是正确的？

A.定量影响分析的主要优点是它对风险进行排序并对那些需要立即改善的环节进行标识。

B. 定性影响分析可以很容易地对控制进行成本收益分析。

C.定量影响分析不能用在对控制进行的成本收益分析中。

D. 定量影响分析的主要优点是它对影响大小给出了一个度量

【答案】 D

119. 通常情况下，怎样计算风险？

A.将威胁可能性等级乘以威胁影响就得出了风险。

B. 将威胁可能性等级加上威胁影响就得出了风险。

C.用威胁影响除以威胁的发生概率就得出了风险。

D. 用威胁概率作为指数对威胁影响进行乘方运算就得出了风险。

【答案】 A

120. 资产清单可包括？

A.服务及无形资产

B.信息资产

C.人员

D.以上所有

【答案】 D

121. 评估 IT 风险被很好的达到，可以通过：

A.评估 IT 资产和 IT 项目总共的威胁

B.用公司的以前的真的损失经验来决定现在的弱点和威胁

C.审查可比较的组织出版的损失数据

D.一句审计拔高审查 IT 控制弱点

【答案】 A

122. 在部署风险管理程序的时候，哪项应该最先考虑到：

A.组织威胁，弱点和风险概括的理解

B. 揭露风险的理解和妥协的潜在后果

C. 基于潜在结果的风险管理优先级的决心

D. 风险缓解战略足够在一个可以接受的水平上保持风险的结果

【答案】 A

123. 为了解决操作人员执行日常备份的失误，管理层要求系统管理员签字日常备份，这是一个风险 ,, 例子：

A.防止

B.转移

C. 缓解

D.接受

【答案】 C

124. 以下哪项不属于 PDCA循环的特点？

A.按顺序进行， 它靠组织的力量来推动， 像车轮一样向前进， 周而复始，不断循环

B.组织中的每个部分，甚至个人，均可以 PDCA循环，大环套小环，一层一层地解决问题

C.每通过一次 PDCA 循环，都要进行总结，提出新目标，再进行第二次 PDCA 循环

D.D. 组织中的每个部分， 不包括个人， 均可以 PDCA循环，大环套小环，一层一层地解决问题

【答案】 D

125. 戴明循环执行顺序，下面哪项正确？

A.. PLAN-ACT-DO-CHECK

B. CHECK-PLAN-ACT-DO

C. PLAN-DO-CHECK-ACT

D. ACT-PLAN-CHECK-DO

【答案】 C

126. 建立 ISMS 的第一步是？

A.风险评估

B.设计 ISMS文档

C. 明确 ISMS 范围

D. 确定 ISMS 策略

【答案】 C

127. 建立 ISMS 的步骤正确的是？

A.明确 ISMS 范围 -确定 ISMS策略 -定义风险评估方法 -进行风险评估 -设计和选择风险处置方法 -设计 ISMS文件 -进行管理者承诺（审批）

B.定义风险评估方法 -进行风险评估 -设计和选择风险处置方法 -设计 ISMS文件 -进行管理者承诺（审批） -确定 ISMS策略

C.确定 ISMS 策略 -明确 ISMS 范围 -定义风险评估方法 -进行风险评估 -设计和选择风险处置方法 -设计 ISMS文件 -进行管理者承诺（审批）

D.明确 ISMS范围 -定义风险评估方法 -进行风险评估 -设计和选择风险处置方法 -确定 ISMS策略 -设计 ISMS 文件 -进行管理者承诺（审批）

【答案】 A

128. 除以下哪项可作为 ISMS 审核（包括内审和外审）的依据，文件审核、现场审核的依据？

A.机房登记记录

B.信息安全管理体系

C.权限申请记录

D.离职人员的口述

【答案】 D

129. 以下哪项是 ISMS文件的作用？

A. 是指导组织有关信息安全工作方面的内部 “ 法规 ”--使工作有章可循。

B.是控制措施（ controls）的重要部分

C.提供客观证据 --为满足相关方要求，以及持续改进提供依据

D.以上所有

【答案】 D

130. 以下哪项不是记录控制的要求？

A.清晰、易于识别和检索

B.记录的标识、贮存、保护、检索、保存期限和处置所需的控制措施应形成文件并实施

C. 建立并保持，以提供证据

D.记录应尽可能的达到最详细

【答案】　D

131.　下面哪项是信息安全管理体系中　　CHECK（检查）中的工作内容？

A.按照计划的时间间隔进行风险评估的评审

B.实施所选择的控制措施

C.采取合适的纠正和预防措施。从其它组织和组织自身的安全经验中吸取教训

D.确保改进达到了预期目标

【答案】　A

132.　指导和规范信息安全管理的所有活动的文件叫做？

A.过程

B.安全目标

C.安全策略

D.安全范围

【答案】　C

133.　信息安全管理措施不包括：

A. 安全策略

B.物理和环境安全

C.访问控制

D.安全范围

【答案】　D

134.　下面安全策略的特性中，不包括哪一项？

A. 指导性

B.静态性

C.可审核性

D.非技术性

【答案】　B

135.　信息安全活动应由来自组织不同部门并具备相关角色和工作职责的代表进行，下面哪项包括非典型的安全协调应包括的人员？

A.管理人员、用户、应用设计人员

B.系统运维人员、内部审计人员、安全专员

C.内部审计人员、安全专员、领域专家

D.应用设计人员、内部审计人员、离职人员

【答案】　D

136.　下面那一项不是风险评估的目的？

A.分析组织的安全需求

B.制订安全策略和实施安防措施的依据

C.组织实现信息安全的必要的、重要的步骤

D.完全消除组织的风险

【答案】　D

137.　下面那个不是信息安全风险的要素？

A.资产及其价值

B.数据安全

C.威胁

D.控制措施

【答案】　B

138.　信息安全风险管理的对象不包括如下哪项

A.信息自身

B.信息载体

C.信息网络

D.信息环境

【答案】　C

139.　信息安全风险管理的最终责任人是？

A.决策层

B.管理层

C.执行层

D.支持层

【答案】　A

140.　信息安全风险评估对象确立的主要依据是什么

A.系统设备的类型

B.系统的业务目标和特性

C.系统的技术架构

D.系统的网络环境

【答案】　B

141.　下面哪一项不是风险评估的过程？

A.风险因素识别

B.风险程度分析

C.风险控制选择

D.风险等级评价

【答案】　C

142.　风险控制是依据风险评估的结果，选择和实施合适的安全措施。下面哪个不是风险控制的方式？

A.规避风险

B.转移风险

C.接受风险

D.降低风险

【答案】　C

143.　降低风险的控制措施有很多，下面哪一个不属于降低风险的措施？

A.在网络上部署防火墙

B.对网络上传输的数据进行加密

C.制定机房安全管理制度

D.购买物理场所的财产保险

【答案】　D

144.　信息安全审核是指通过审查、测试、评审等手段，检验风险评估和风险控制的结果是否满足信息系统的安全要求，这个工作一般由谁完成？

A.机构内部人员

B.外部专业机构

C.独立第三方机构

D.以上皆可

【答案】　D

145.　如何对信息安全风险评估的过程进行质量监控和管理？

A.对风险评估发现的漏洞进行确认

B.针对风险评估的过程文档和结果报告进行监控和审查

C.对风险评估的信息系统进行安全调查

D.对风险控制测措施有有效性进行测试

【答案】　B

146.　信息系统的价值确定需要与哪个部门进行有效沟通确定？

A.系统维护部门

B.系统开发部门

C.财务部门

D.业务部门

【答案】　D

147.　下面哪一个不是系统规划阶段风险管理的工作内容

A.明确安全总体方针

B.明确系统安全架构

C.风险评价准则达成一致

D.安全需求分析

【答案】　B

148.　下面哪一个不是系统设计阶段风险管理的工作内容

A.安全技术选择

B.软件设计风险控制

C.安全产品选择

D.安全需求分析

【答案】　D

149.　下面哪一个不是系统实施阶段风险管理的工作内容

A.安全测试

B.检查与配置

C.配置变更

D.人员培训

【答案】　C

150.　下面哪一个不是系统运行维护阶段风险管理的工作内容

A.安全运行和管理

B.安全测试

C.变更管理

D.风险再次评估

【答案】　B

151.　下面哪一个不是系统废弃阶段风险管理的工作内容

A.安全测试

B.对废弃对象的风险评估

C.防止敏感信息泄漏

D.人员培训

【答案】 A

152. 系统上线前应当对系统安全配置进行检查，不包括下列哪种安全检查

A.主机操作系统安全配置检查

B.网络设备安全配置检查

C.系统软件安全漏洞检查

D.数据库安全配置检查

【答案】 C

153. 风险评估实施过程中资产识别的依据是什么

A.依据资产分类分级的标准

B.依据资产调查的结果

C.依据人员访谈的结果

D.依据技术人员提供的资产清单

【答案】 A

154. 风险评估实施过程中资产识别的范围主要包括什么类别

A.网络硬件资产

B.数据资产

C.软件资产

D.以上都包括

【答案】 D

155. 风险评估实施过程中脆弱性识别主要包括什么方面

A.软件开发漏洞

B.网站应用漏洞

C.主机系统漏洞

D.技术漏洞与管理漏洞

【答案】 D

156. 下面哪一个不是脆弱性识别的手段

A.人员访谈

B.技术工具检测

C.信息资产核查

D.安全专家人工分析

【答案】 C

157. 信息资产面临的主要威胁来源主要包括

A.自然灾害

B.系统故障

C.内部人员操作失误

D.以上都包括

【答案】 D

158. 下面关于定性风险评估方法的说法正确的是

A.通过将资产价值和风险等量化为财务价值和方式来进行计算的一种方法

B.采用文字形式或叙述性的数值范围来描述潜在后果的大小程度及这些后果发生的可能性

C.在后果和可能性分析中采用数值，并采用从各种各样的来源中得到的

数据

D.定性风险分析提供了较好的成本效益分析

【答案】 B

159. 下面关于定性风险评估方法的说法不正确的是

A.易于操作，可以对风险进行排序并能够对那些需要立即改善的环节进行标识

B.主观性强，分析结果的质量取决于风险评估小组成员的经验和素质

C."耗时短、成本低、可控性高
"

D.能够提供量化的数据支持，易被管理层所理解和接受

【答案】 D

160. 下面关于定量风险评估方法的说法正确的是

A.易于操作，可以对风险进行排序并能够对那些需要立即改善的环节进行标识

B.能够通过成本效益分析控制成本

C."耗时短、成本低、可控性高
"

D.主观性强，分析结果的质量取决于风险评估小组成员的经验和素质

【答案】 B

161. 年度损失值（ ALE）的计算方法是什么

A.ALE=ARO*AV

B.ALE=AV*SLE

C."ALE=ARO*SLE
"

D.ALE=AV*EF

【答案】 C

162. 矩阵分析法通常是哪种风险评估采用的方法

A.定性风险评估

B.定量分析评估

C.安全漏洞评估

D.安全管理评估

【答案】 A

163. 风险评估和管理工具通常是指什么工具

A.漏洞扫描工具

B.入侵检测系统

C.安全审计工具

D.安全评估流程管理工具

【答案】 D

164. 安全管理评估工具通常不包括

A.调查问卷

B.检查列表

C.访谈提纲

D.漏洞扫描

【答案】 D

165.　安全技术评估工具通常不包括

A.漏洞扫描工具

B.入侵检测系统

C.调查问卷

D.渗透测试工具

【答案】　C

166.　对于信息安全管理，风险评估的方法比起基线的方法，主要的优势在于它确保

A.信息资产被过度保护

B.不考虑资产的价值，基本水平的保护都会被实施

C.对信息资产实施适当水平的保护

D.对所有信息资产保护都投入相同的资源

【答案】　C

167.　区别脆弱性评估和渗透测试是脆弱性评估

A.检查基础设施并探测脆弱性，然而穿透性测试目的在于通过脆弱性检测其可能带来的损失

B.和渗透测试为不同的名称但是同一活动

C.是通过自动化工具执行，而渗透测试是一种完全的手动过程

D.是通过商业工具执行，而渗透测试是执行公共进程

【答案】　A

168.　合适的信息资产存放的安全措施维护是谁的责任

A.安全管理员

B.系统管理员

C.数据和系统所有者

D.系统运行组

【答案】　C

169.　要很好的评估信息安全风险，可以通过：

A.评估 IT 资产和 IT 项目的威胁

B.用公司的以前的真的损失经验来决定现在的弱点和威胁

C.审查可比较的组织公开的损失统计

D.审查在审计报告中的可识别的　　IT 控制缺陷

【答案】　A

170.　下列哪项是用于降低风险的机制

A.安全和控制实践

B.财产和责任保险

C.审计与认证

D.合同和服务水平协议

【答案】　A

171.　回顾组织的风险评估流程时应首先

A.鉴别对于信息资产威胁的合理性

B.分析技术和组织弱点

C.鉴别并对信息资产进行分级

D.对潜在的安全漏洞效果进行评价

【答案】　C

172.　在实施风险分析期间，识别出威胁和潜在影响后应该

A.识别和评定管理层使用的风险评估方法

B.识别信息资产和基本系统

C.揭示对管理的威胁和影响

D.识别和评价现有控制

【答案】　D

173.　在制定控制前，管理层首先应该保证控制

A.满足控制一个风险问题的要求

B.不减少生产力

C.基于成本效益的分析

D.检测行或改正性的

【答案】　A

174.　在未受保护的通信线路上传输数据和使用弱口令是一种？

A.弱点

B.威胁

C.可能性

D.影响

【答案】　A

175.　数据保护最重要的目标是以下项目中的哪一个

A.识别需要获得相关信息的用户

B.确保信息的完整性

C.对信息系统的访问进行拒绝或授权

D.监控逻辑访问

【答案】　B

176.　对一项应用的控制进行了检查　　,将会评估

A.该应用在满足业务流程上的效率

B.任何被发现风险影响

C.业务流程服务的应用

D.应用程序的优化

【答案】　B

177.　在评估逻辑访问控制时，应该首先做什么

A.把应用在潜在访问路径上的控制项记录下来

B.在访问路径上测试控制来检测是否他们具功能化

C.按照写明的策略和实践评估安全环境

D.对信息流程的安全风险进行了解

【答案】　D

178.　在评估信息系统的管理风险。首先要查看

A.控制措施已经适当

B.控制的有效性适当

C.监测资产有关风险的机制

D.影响资产的漏洞和威胁

【答案】　D

179.　在开发一个风险管理程序时，什么是首先完成的活动

A.威胁评估

B.数据分类

C.资产清单

D.关键程度分析

【答案】 C

180. 在检查 IT 安全风险管理程序，安全风险的测量应该

A.列举所有的网络风险

B.对应 IT 战略计划持续跟踪

C.考虑整个 IT 环境

D.识别对 (信息系统)的弱点的容忍度的结果

【答案】 C

181. 在实施风险管理程序的时候，下列哪一项应该被最先考虑到：

A.组织的威胁，弱点和风险概貌的理解

B.揭露风险的理解和妥协的潜在后果

C.基于潜在结果的风险管理优先级的决心

D.风险缓解战略足够使风险的结果保持在一个可以接受的水平上

【答案】 A

182. 授权访问信息资产的责任人应该是

A.资产保管员

B.安全管理员

C.资产所有人

D.安全主管

【答案】 C

183. 渗透测试作为网络安全评估的一部分

A.提供保证所有弱点都被发现

B.在不需要警告所有组织的管理层的情况下执行

C.找到存在的能够获得未授权访问的漏洞

D.在网络边界上执行不会破坏信息资产

【答案】 C

184. 一个组织的网络设备的资产价值为 100000 元，一场意外火灾使其损坏了价值的 25%,按照经验统计，这种火灾一般每 5 年发生一次，年预期损失 ALE为

A.5000 元

B.10000 元

C.25000 元

D.15000 元

【答案】 A

185. 一个个人经济上存在问题的公司职员有权独立访问高敏感度的信息，他可能窃取这些信息卖给公司的竞争对手，如何控制这个风险

A.开除这名职员

B.限制这名职员访问敏感信息

C.删除敏感信息

D.将此职员送公安部门

【答案】 B

186. 以下哪一种人最有可能给公司带来最大的安全风险？

A.临时工

B.当前员工

C以前员工

D.咨询人员

【答案】 B

187. 当以下哪一类人员维护应用系统软件的时候，会造成对“职责分离”原则的违背？

A.数据维护管理员

B.系统故障处理员

C.系统维护管理员

D.系统程序员

【答案】 D

188. 下列角色谁应该承担决定信息系统资源所需的保护级别的主要责任？

A.信息系统安全专家

B.业务主管

C.安全主管

D.系统审查员

【答案】 B

189. 职责分离的主要目的是？

A.防止一个人从头到尾整个控制某一交易或者活动

B.不同部门的雇员不可以在一起工作

C.对于所有的资源都必须有保护措施

D.对于所有的设备都必须有操作控制措施

【答案】 A

190. 以下哪种做法是正确的“职责分离”做法？

A.程序员不允许访问产品数据文件

B.程序员可以使用系统控制台

C.控制台操作员可以操作磁带和硬盘

D.磁带操作员可以使用系统控制台

【答案】 A

191. 以下哪个是数据库管理员（ DBA）可以行使的职责？

A.计算机的操作

B.应用程序开发

C.系统容量规划

D.应用程序维护

【答案】 C

192. 信息安全管理体系策略文件中第一层文件是？

A.信息安全工作程序

B.信息安全方针政策

C.信息安全作业指导书

D.信息安全工作记录

【答案】 B

193. 对安全策略的描述不正确的是？

A.信息安全策略应得到组织的最高管理者批准。

B.策略应有一个所有者，负责按复查程序维护和复查该策略。

C.安全策略应包括管理层对信息安全管理工作的承诺。

D.安全策略一旦建立和发布，则不可变更。

【答案】 D

194. 有关人员安全管理的描述不正确的是？

A.人员的安全管理是企业信息安全管理活动中最难的环节。

B.重要或敏感岗位的人员入职之前，需要做好人员的背景检查。

C.如职责分离难以实施，企业对此无能为力，也无需做任何工作。

D.人员离职之后，必须清除离职员工所有的逻辑访问帐号。

【答案】 C

195. 关于信息安全策略文件以下说法不正确的是哪个？

A.信息安全策略文件应由管理者批准、发布。

B.信息安全策略文件并传达给所有员工和外部相关方。

C.信息安全策略文件必须打印成纸质文件进行分发。

D.信息安全策略文件应说明管理承诺，并提出组织的管理信息安全的方法。

【答案】 C

196. 关于信息安全策略文件的评审以下说法不正确的是哪个？

A.信息安全策略应由专人负责制定、评审。

B.信息安全策略评审每年应进行两次，上半年、下半年各进行一次。

C.在信息安全策略文件的评审过程中应考虑组织业务的重大变化。

D.在信息安全策略文件的评审过程中应考虑相关法律法规及技术环境的重大变化。

【答案】 B

197. 高层管理者对信息安全管理的承诺以下说法不正确的是？

A.制定、评审、批准信息安全方针。

B.为信息安全提供明确的方向和支持。

C.为信息安全提供所需的资源。

D.对各项信息安全工作进行执行、监督与检查。

【答案】 D

198. 信息安全管理组织说法以下说法不正确的是？

A.信息安全管理组织人员应来自不同的部门。

B.信息安全管理组织的所有人员应该为专职人员。

C.信息安全管理组织应考虑聘请外部专家。

D.信息安全管理组织应建立沟通、协调机制。

【答案】 B

199. 在制定组织间的保密协议，以下哪一个不是需要考虑的内容？

A.需要保护的信息。

B.协议期望持续时间。

C.合同双方的人员数量要求。

D.违反协议后采取的措施。

【答案】 C

200. 在信息安全管理日常工作中，需要与哪些机构保持联系？

A.政府部门

B.监管部门

C.外部专家

D.以上都是

【答案】 D

201. 当涉及到信息算计系统犯罪取证时，应与哪个部门取得联系？

A.监管机构

B.重要客户

C.供应商

D.政府部门

【答案】 D

202. 信息安全管理工作小组可就哪些问题向外部安全专家或特定外部组织寻求信息安全方面的建议？

A.相关安全信息的最佳实践和最新状态知识。

B.尽早接受到关于攻击和脆弱点的警告、建议和补丁

C. 分享和交换关于新的技术、产品、威胁或脆弱点信息

D. 以上都是

【答案】 D

203. 当客户需要访问组织信息资产时，下面正确的做法是？

A.应向其传达信息安全要求及应注意的信息安全问题。

B.尽量配合客户访问信息资产。

C.不允许客户访问组织信息资产。

D.不加干涉，由客户自己访问信息资产。

【答案】 A

204. 对于外部组织访问企业信息资产的过程中相关说法不正确的是？

A.为了信息资产更加安全，禁止外部组织人员访问信息资产。

B.应确保相关信息处理设施和信息资产得到可靠的安全保护。

C.访问前应得到信息资产所有者或管理者的批准。

D.应告知其所应当遵守的信息安全要求。

【答案】 A

205. 外部组织使用组织敏感信息资产时，以下正确的做法是？

A.确保使用者得到正确的信息资产。

B.与信息资产使用者签署保密协议。

C.告知信息资产使用的时间限制。

D.告知信息资产的重要性。

【答案】 B

206. 在进行人员的职责定义时，在信息安全方面应考虑什么因素？

A.人员的背景、资质的可靠性

B.人员需要履行的信息安全职责

C.人员的工作能力

D.人员沟通、协调能力

【答案】 B

207. 下列岗位哪个在招聘前最需要进行背景调查？

A.采购人员

B.销售人员

C.财务总监

D.行政人员

【答案】 C

208. 在招聘过程中，如果在岗位人员的背景调查中出现问题时，以下做法正确的是？

A.继续执行招聘流程。

B.停止招聘流程，取消应聘人员资格。

C.与应聘人员沟通出现的问题。

D.再进行一次背景调查。

【答案】 B

209. 人员入职过程中，以下做法不正确的是？

A.入职中签署劳动合同及保密协议。

B.分配工作需要的最低权限。

C.允许访问企业所有的信息资产。

D.进行安全意思培训。

【答案】 C

210. 单位中下面几种人员中哪种安全风险最大？

A.临时员工

B.外部咨询人员

C.现在对公司不满的员工

D.离职的员工

【答案】 C

211. 对磁介质的最有效好销毁方法是？

A.格式化

B.物理破坏

C.消磁

D.删除

【答案】 B

212. TCP/IP协议的 4 层概念模型是？

A.应用层、传输层、网络层和网络接口层

B.应用层、传输层、网络层和物理层

C. 应用层、数据链路层、网络层和网络接口层

D.会话层、数据链路层、网络层和网络接口层

【答案】 A

213. 多层的楼房中，最适合做数据中心的位置是：

A.一楼

B.地下室

C.顶楼

D.除以上外的任何楼层

【答案】 D

214. 计算机安全事故发生时，下列哪些人不被通知或者最后才被通知：

A.系统管理员

B.律师

C.恢复协调员

D.硬件和软件厂商

【答案】 B

215. 下面哪种方法可以替代电子银行中的个人标识号 （PINs）的作用？

A.虹膜检测技术

B.语音标识技术

C.笔迹标识技术

D.指纹标识技术

【答案】 A

216. “如果一条链路发生故障，那么只有和该链路相连的终端才会受到影响”，这一说法是适合于以下哪一种拓扑结构的网络的？

A.星型

B.树型

C.环型

D.复合型

【答案】 A

217. 为了有效的完成工作，信息系统安全部门员工最需要以下哪一项技能？

A.人际关系技能

B.项目管理技能

C.技术技能

D.沟通技能

【答案】 D

218. 目前，我国信息安全管理格局是一个多方“齐抓共管”的体制，多头管理现状决定法出多门，《计算机信息系统国际联网保密管理规定》是由下列哪个部门所制定的规章制度？

A.公安部

B.国家保密局

C.信息产业部

D.国家密码管理委员会办公室

【答案】 B

219. "在选择外部供货生产商时，评价标准按照重要性的排列顺序是：

1. 供货商与信息系统部门的接近程度
2. 供货商雇员的态度
3. 供货商的信誉、专业知识、技术
4. 供货商的财政状况和管理情况

"

A.4，3，1，2

B.3，4，2，1

C.3，2，4，1

D.1，2，3，4

【答案】 B

220. 下列哪一项能够提高网络的可用性？

A.数据冗余

B.链路冗余

C.软件冗余

D.电源冗余

【答案】 B

221. 系统管理员属于？

A.决策层

B.管理层

C.执行层

D.既可以划为管理层，又可以划为执行层

【答案】 C

222. 为了保护企业的知识产权和其它资产，当终止与员工的聘用关系时下面哪一项是最好的方法？

A.进行离职谈话，让员工签署保密协议，禁止员工账号，更改密码

B.进行离职谈话，禁止员工账号，更改密码

C.让员工签署跨边界协议

D.列出员工在解聘前需要注意的所有责任

【答案】 A

223. 信息安全管理最关注的是？

A.外部恶意攻击

B.病毒对 PC的影响

C.内部恶意攻击

D.病毒对网络的影响

【答案】 C

224. 以下哪个选项不是信息中心（ IC）工作职能的一部分？

A.准备最终用户的预算

B.选择 PC的硬件和软件

C.保持所有 PC的硬件和软件的清单

D.提供被认可的硬件和软件的技术支持

【答案】 A

225. 以下哪些不是设备资产：

A.机房设施

B.周边设施

C.管理终端

D.操作系统

【答案】 D

226. 以下哪些不是网络类资产：

A.网络设备

B.基础服务平台

C.网络安全设备

D.主干线路

【答案】 B

227. 以下哪些不是介质类资产：

A.纸质文档

B.存储介质

C.软件介质

D.凭证

【答案】 A

228. 以下哪些不是无形资产

A.客户关系

B.电子数据

C.商业信誉

D.企业品牌

【答案】 B

229. 以下哪些是信息资产无需明确的

A.所有者

B.管理者

C.厂商

D.使用者

【答案】 C

230. 信息资产敏感性指的是：

A.机密性

B.完整性

C.可用性

D.安全性

【答案】 A

231. 以下哪些不属于敏感性标识

A.不干贴方式

B.印章方式

C.电子标签

D.个人签名

【答案】 D

232. 设施、网络、平台、介质、应用类信息资产的保密期限为

A.3 年

B.长期

C.4 月

D.短期

【答案】 B

233. 当曾经用于存放机密资料的 PC在公开市场出售时

A.对磁盘进行消磁

B. 对 磁盘低级格式化

C.删除数据

D.对磁盘重整

【答案】 A

234. 防止擅自使用资料档案的最有效的预防方法是 :

A.自动化的档案访问入口

B.磁带库管理

C.使用访问控制软件

D. 锁定资料馆

【答案】

235. 维持对于信息资产的适当的安全措施的责任在于

A.安全管理员

B.系统管理员

C.数据和系统的所有者

D.系统作业人员

【答案】 A

236. 给计算机系统的资产分配的记号被称为什么

A.安全属性

B.安全特征

C.安全标记

D.安全级别

【答案】 C

237. 所有进入物理安全区域的人员都需经过

A.考核

B.授权

C.批准

D.认可

【答案】 B

238. 下面哪种方法在数据中心灭火最有效并且是环保的？

A.哈龙气体

B.湿管

C.干管

D.二氧化碳气

【答案】 A

239. 在数据中心使用稳压电源，以保证 ：

A. 硬件免受电源浪涌

B. 主电源被破坏后的完整性维护

C.主电源失效后可以立即使用

D.针对长期电力波动的硬件包含

【答案】 A

240. 干管灭火器系统使用

A. 水，但是只有在发现火警以后水才进入管道

B. 水，但是水管中有特殊的防水剂

C. CO_2代替水

D. 哈龙代替水

【答案】 A

241. 下面哪一种物理访问控制能够对非授权访问提供最高级别的安全？

A.bolting 门锁

B.Cipher 密码锁

C.电子门锁

D.指纹扫描器

【答案】 D

242. 来自终端的电磁泄露风险，因为它们 ：

A.导致噪音污染

B. 破坏处理程序

C. 产生危险水平的电流

D. 可以被捕获并还原

【答案】 D

243. 射频识别 (RFID)标签容易受到以下哪种风险 ？

A. 进程劫持

B.窃听

C. 恶意代码

D. Phishing

【答案】 B

244. 有什么方法可以测试办公部门的无线安全？

A. War dialing战争语言

B. 社会工程学

C. 战争驾驶

D. 密码破解

【答案】 D

245. 以下哪一个是对于参观者访问数据中心的最有效的控制？

A.陪同参观者

B.参观者佩戴证件

C.参观者签字

D.参观者由工作人员抽样检查

【答案】 A

246. 信息安全政策声明： ”每个人必须在进入每一个控制门时，都必须读取自己的证件” ,防范的是哪一种攻击方式 ？

A.尾随 Piggybacking

B.肩窥 Shoulder surfing

C.Dumpster diving

D.冒充 Impersonation

【答案】 A

247. 以下哪一种环境控制适用于保护短期内电力环境不稳定条件下的计算机设备？

A.电路调整器 Power line conditioners

B.电流浪涌防护装置 A surge protective device

C.替代电源

D.不间断供电

【答案】 B

248. 以下哪些模型可以用来保护分级信息的机密性？

A.Biba 模型和 Bell－Lapadula 模型

B.Bell－Lapadula 模型和信息流模型

C.Bell－Lapadula 模型和 Clark－Wilson 模型

D.Clark－Wilson 模型和信息流模型

【答案】 B

名称	属性	类型	应用	读写
BLP	机密性	多极	政府、军队	上读 下写
信息流模型	机密性			
Chinese Wall	机密性	多边	金融	
Biba	完整性	多极		下读 上写
Clark-wilson	完整性	多极	商业	
BMA	机密性完整性	多边	医疗	

249. BLP 模型基于两种规则来保障数据的机秘度与敏感度，它们是什么？

A.下读，主体不可读安全级别高于它的数据；上写，主体不可写安全级别低于它的数据

B.上读，主体不可读安全级别高于它的数据；下写，主体不可写安全级别低于它的数据

C.上读，主体不可读安全级别低于它的数据；下写，主体不可写安全级别高于它的数据

D.下读，主体不可读安全级别低于它的数据；上写，主体不可写安全级别高于它的数据

【答案】 B

250. BIBA 模型基于两种规则来保障数据的完整性的保密性，分别是：

A.上读，主体不可读安全级别高于它的数据；下写，主体不可写安全级别低于它的数据

B.下读，主体不可读安全级别高于它的数据；上写，主体不可写安全级别低于它的数据

C.上读，主体不可读安全级别低于它的数据；下写，主体不可写安全级别高于它的数据

D.下读，主体不可读安全级别低于它的数据；上写，主体不可写安全级别高于它的数据

【答案】 D

251. 以下哪组全部是完整性模型？

A.BLP模型和 BIBA模型

B.BIBA模型和 Clark－Wilson 模型

C.Chinese wall模型和 BIBA 模型

D.Clark－Wilson 模型和 Chinese wall 模型

【答案】 B 多边： Chinese Wall\BMA ；完整性： Biba, Clark-Wilson

252. 以下哪个模型主要用于医疗资料的保护？

A.Chinese wall 模型

B.BIBA 模型

C.Clark－ Wilson 模型

D.BMA 模型

【答案】 D

253. 以下哪个模型主要用于金融机构信息系统的保护？

A.Chinese wall 模型

B.BIBA 模型

C.Clark－ Wilson 模型

D.BMA 模型

【答案】 A

254. 以下哪组全部都是多边安全模型？

A.BLP 模型和 BIBA 模型

B.BIBA 模型和 Clark－Wilson 模型

C.Chinese wall 模型和 BMA 模型

D.Clark－ Wilson 模型和 Chinese wall 模型

【答案】 C

255. 以下哪种访问控制策略需要安全标签？

A.基于角色的策略

B.基于标识的策略

C.用户指向的策略

D.强制访问控制策略

【答案】 D

256. 应急响应哪一个阶段用来降低事件再次发生的风险

A.遏制

B.根除

C.跟踪

D.恢复

【答案】 C

257. 信息安全应急响应计划总则中，不包括以下哪个

A.编制目的

B.编制依据

C.工作原则

D.角色职责

【答案】 D

258. 以下哪项描述是错误的

A.应急响应计划与应急响应这两个方面是相互补充与促进的关系

B.应急响应计划为信息安全事件发生后的应急响应提供了指导策略和规程

C.应急响应可能发现事前应急响应计划的不足

D.应急响应必须完全依照应急响应计划执行

【答案】 D

259. 应急响应计划应该多久测试一次？

A.10 年

B.当基础环境或设施发生变化时

C.2 年

D.当组织内业务发生重大的变更时

【答案】 D

260. 建立应急响应计划时候第一步应该做什么？

A.建立备份解决方案

B.实施业务影响分析

C.建立业务恢复计划

D.确定应急人员名单

【答案】 B

261. 建立应急响应计划最重要的是

A.业务影响分析

B.测试及演练

C.各部门的参与

D.管理层的支持

【答案】 D

262. 以下谁具有批准应急响应计划的权利

A.应急委员会

B.各部门

C.管理层

D.外部专家

【答案】 C

263. 哪一项不是业务影响分析（ BIA）的工作内容

A.确定应急响应的恢复目标

B.确定公司的关键系统和业务

C.确定业务面临风险时的潜在损失和影响

D.确定支持公司运行的关键系统

【答案】 C

264. 制定应急响应策略主要需要考虑

A.系统恢复能力等级划分

B.系统恢复资源的要求

C.费用考虑

D.人员考虑

【答案】 D

265. 应急响应领导小组主要职责包括：

A.对应急响应工作的承诺和支持, 包括发布正式文件、 提供必要资源 （人财物）等；

B.审核并批准应急响应计划；

C.负责组织的外部协作工作

D.组织应急响应计划演练

【答案】 D

266. 应急响应领导小组组长应由以下哪个选项担任？

A.最高管理层

B.信息技术部门领导

C.业务部门领导

D.外部专家
【答案】　A
267.　应急响应流程一般顺序是
A.信息安全事件通告、信息安全事件评估、应急启动、应急处置和后期处置
B.信息安全事件评估、信息安全事件通告、应急启动、应急处置和后期处置
C.应急启动、应急处置、信息安全事件评估、信息安全事件通告、后期处置
D.信息安全事件评估、应急启动、信息安全事件通告、应急处置和后期处置
【答案】　A
268.　组织内应急通知应主要采用以下哪种方式
A.电话
B.电子邮件
C.人员
D.公司 OA
【答案】　A
269.　如果可能最应该得到第一个应急事件通知的小组是
A.应急响应领导小组
B.应急响应日常运行小组
C.应急响应技术保障小组
D.应急响应实施小组
【答案】　B
270.　恢复阶段的行动一般包括
A.建立临时业务处理能力
B.修复原系统损害
C.在原系统或新设施中恢复运行业务能力
D.避免造成更大损失
【答案】　D
271.　在正常情况下，应急响应计划培训应该至少多久一次
A.1 年
B.2 年
C.半年
D.5 年
【答案】　A
272.　在正常情况下，应急计划应该至少多久进行一次针对正确性和完整性的检查
A.1 年
B.2 年
C.半年
D.5 年
【答案】　A
273.　应急响应计划文档不应该

A.分发给公司所有人员

B.分发给参与应急响应工作的所有人员

C.具有多份拷贝在不同的地点保存

D.由专人负责保存与分发

【答案】 A

274. 业务影响分析的主要目的是：

A.在灾难之后提供一个恢复行动的计划

B.识别能够影响组织运营持续性的事件

C.公布组织对物理和逻辑安全的义务

D.提供一个有效灾难恢复计划的框架

【答案】 B

275. 评估应急响应计划时，下列哪一项应当最被关注：

A.灾难等级基于受损功能的范围，而不是持续时间

B.低级别灾难和软件事件之间的区别不清晰

C.总体应急响应计划被文档化，但详细恢复步骤没有规定

D.事件通告的职责没有被识别

【答案】 D

276. 事件响应六个阶段定义了安全事件处理的流程，这个流程的顺序是

A.准备－遏制－确认－根除－恢复－跟踪

B.准备－确认－遏制－恢复－根除－跟踪

C.准备－确认－遏制－根除－恢复－跟踪

D.准备－遏制－根除－确认－恢复－跟踪

【答案】 B

277. 发现一台被病毒感染的终端后，首先应：

A.拔掉网线

B.判断病毒的性质、采用的端口

C.在网上搜寻病毒解决方法

D.呼叫公司技术人员

【答案】 A

278. 我国信息安全事件分级分为以下哪些级别

A.特别重大事件 -重大事件 -较大事件 -一般事件

B.特别重大事件 -重大事件 -严重事件 -较大事件 -一般事件

C.特别严重事件 -严重事件 -重大事件 -较大事件 -一般事件

D.特别严重事件 -严重事件 -较大事件 -一般事件

【答案】 A

279. 我国信息安全事件分级不考虑下列哪一个要素？

A.信息系统的重要程度

B.系统损失

C.社会影响

D.业务损失

【答案】 D

280. 校园网内由于病毒攻击、 非法入侵等原因， 200 台以内的用户主机不能正常工作，属于以下哪种级别事件

A.特别重大事件

B.重大事件

C.较大事件

D.一般事件

【答案】 D

281. 由于病毒攻击、 非法入侵等原因， 校园网部分楼宇出现网络瘫痪，或者 FTP及部分网站服务器不能响应用户请求，属于以下哪种级别事件

A.特别重大事件

B.重大事件

C.较大事件

D.一般事件

【答案】 C

282. 由于病毒攻击、非法入侵等原因，校园网部分园区瘫痪，或者邮件、计费服务器不能正常工作，属于以下哪种级别事件

A.特别重大事件

B.重大事件

C.较大事件

D.一般事件

【答案】 B

283. 由于病毒攻击、非法入侵等原因，校园网整体瘫痪，或者校园网络中心全部 DNS、主 WEB服务器不能正常工作；由于病毒攻击、非法入侵、人为破坏或不可抗力等原因，造成校园网出口中断，属于以下哪种级别事件

A.特别重大事件

B.重大事件

C.较大事件

D.一般事件

【答案】 A

284. 由于独立的信息系统增加，一个国有房产公司要求在发生重大故障后，必须保证能够继续提供 IT 服务。需要实施哪个流程才能提供这种保证性？

A.可用性管理

B. IT 服务连续性管理

C.服务级别管理

D.服务管理

【答案】 B

285. 在一家企业的业务持续性计划中，什么情况被宣布为一个危机没有被定义。这一点关系到的主要风险是：

A.对这种情况的评估可能会延迟

B.灾难恢复计划的执行可能会被影响

C.团队通知可能不会发生

D.对潜在危机的识别可能会无效

【答案】 B

286. 在信息处理设施（ IPF）的硬件更换之后，业务连续性流程经理首

先应该实施下列哪项活动？

A.验证与热门站点的兼容性

B.检查实施报告

C.进行灾难恢复计划的演练

D.更新信息资产清单

【答案】 D

287. 组织的灾难恢复计划应该 :

A.减少恢复时间，降低恢复费用

B.增加恢复时间，提高恢复费用

C.减少恢复的持续时间，提高恢复费用

D.对恢复时间和费用都不影响

【答案】 A

288. 一个组织具有的大量分支机构且分布地理区域较广。以确保各方面的灾难恢复计划的评估，具有成本效益的方式，应建议使用：

A.数据恢复测试

B.充分的业务测试

C.前后测试

D.预案测试

【答案】 D

289. 较低的恢复时间目标（恢复时间目标）的会有如下结果：

A.更高的容灾

B.成本较高

C.更长的中断时间

D.更多许可的数据丢失

【答案】 B

290. 组织实施了灾难恢复计划。下列哪些步骤应下一步执行？

A.取得高级管理人员认可

B.确定的业务需求

C.进行纸面测试

D.进行系统还原测试

【答案】 C

291. 灾难性恢复计划 (DRP) 基于：

A.技术方面的业务连续性计划

B.操作部分的业务连续性计划

C.功能方面的业务连续性计划

D.总体协调的业务连续性计划

【答案】 A

292. 下面哪一项是恢复非关键系统的最合理方案 ？

A.温站

B.移动站

C.热站

D.冷站

【答案】 D

293. 下列哪一项是一个适当的测试方法适用于业务连续性计划 (BCP)?

A.试运行

B.纸面测试

C.单元

D.系统

【答案】　B

294.　在一个中断和灾难事件中，以下哪一项提供了持续运营的技术手段？

A.负载平衡

B.硬件冗余

C.分布式备份

D.高可用性处理

【答案】　B

295.　在一份业务持续计划，下列发现中哪一项是最重要的？

A.不可用的交互　PBX 系统

B.骨干网备份的缺失

C.用户　PC机缺乏备份机制

D.门禁系统的失效

【答案】　B

296.　在一份热站、温站或冷站协议中，协议条款应包含以下哪一项需考虑的事项

A.具体的保证设施

B.订户的总数

C.同时允许使用设施的订户数量

D.涉及的其他用户

【答案】　C

297.　企业的业务持续性计划中应该以记录以下内容的预定规则为基础

A.损耗的持续时间

B.损耗的类型

C.损耗的可能性

D.损耗的原因

【答案】　A

298.　当更新一个正在运行的在线订购系统时，更新都记录在一个交易磁带和交易日志副本。在一天业务结束后，订单文件备份在磁带上。在备份过程中，驱动器故障和订单文件丢失。以下哪项对于恢复文件是必须的？

A.前一天的备份文件和当前的交易磁带

B.前一天的交易文件和当前的交易磁带

C.当前的交易磁带和当前的交易日志副本

D.当前的交易日志副本和前一天的交易交易文件

【答案】　A

299.　业务影响分析的主要目的是：

A.在灾难之后提供一个恢复行动的计划

B.识别能够影响组织运营持续性的事件

C.公布组织对物理和逻辑安全的义务

D.提供一个有效灾难恢复计划的框架
【答案】　B

300.　当建立一个业务持续性计划时，使用下面哪一个工具用来理解组织业务流程？

A.业务持续性自我评估

B.资源的恢复分析

C.风险评估和业务影响评估

D.差异分析
【答案】　C

301.　下列哪一项最好地支持了　24/7 可用性？

A.日常备份

B.离线存储

C.镜像

D.定期测试
【答案】　C

302.　评估 BCP时，下列哪一项应当最被关注：

A.灾难等级基于受损功能的范围，而不是持续时间

B.低级别灾难和软件事件之间的区别不清晰

C.总体 BCP被文档化，但详细恢复步骤没有规定

D.宣布灾难的职责没有被识别
【答案】　D

303.　在一个业务继续计划的模拟演练中，发现报警系统严重受到设施破坏。下列选项中，哪个是可以提供的最佳建议：

A.培训救护组如何使用报警系统

B.报警系统为备份提供恢复

C.建立冗余的报警系统

D.把报警系统存放地窖里
【答案】　C

304.　评估业务连续计划效果最好的方法是：

A.使用适当的标准进行规划和比较

B.之前的测试结果

C.紧急预案和员工培训

D.环境控制和存储站点
【答案】　B

305.　以下哪种为丢弃废旧磁带前的最佳处理方式？

A.复写磁带

B.初始化磁带卷标

C.对磁带进行消磁

D.删除磁带
【答案】　C

306.　组织中对于每个独立流程都有对应的业务连续性计划，但缺乏全面的业务连续性计划，应采取下面哪一项行动？

A.建议建立全面的业务连续性计划

B.确认所有的业务连续性计划是否相容

C.接受已有业务连续性计划

D.建议建立单独的业务连续性计划

【答案】 B

307. 组织已经完成了年度风险评估，关于业务持续计划组织应执行下面哪项工作？

A.回顾并评价业务持续计划是否恰当

B.对业务持续计划进行完整的演练

C.对职员进行商业持续计划的培训

D.将商业持续计划通报关键联络人

【答案】 A

308. 组织回顾信息系统灾难恢复计划时应：

A.每半年演练一次

B.周期性回顾并更新

C经首席执行官 (CEO)认可

D.与组织的所有部门负责人沟通

【答案】 B

309. 相对于不存在灾难恢复计划，和当前灾难恢复计划的成本对比，最接近的是：

A.增加

B.减少

C.保持不变

D.不可预知

【答案】 A

310. 根据组织业务连续性计划（ BCP）的复杂程度，可以建立多个计划来满足业务连续和和灾难恢复的各方面。在这种情况下，有必要：

A.每个计划和其它计划保持协调一致

B.所有的计划要整合到一个计划中

C.每个计划和其他计划相互依赖

D.指定所有计划实施的顺序

【答案】 A

311. 使用热站作为备份的优点是：

A.热站的费用低

B.热站能够延长使用时间

C.热站在短时间内可运作

D.热站不需要和主站点兼容的设备和系统软件

【答案】 C

312. 在完成了业务影响分析（ BIA）后，下一步的业务持续性计划应该是什么

A.测试和维护业务持续性计划

B.制定一个针对性计划

C.制定恢复策略

D.实施业务持续性计划

【答案】 C

313. 一个备份站点包括电线、空调和地板，但不包括计算机和通讯设

备，那么它属于

A.冷站

B.温站

C.直线站点

D.镜像站点

【答案】 A

314. 以下关于备份站点的说法哪项是正确的

A.应与原业务系统具有同样的物理访问控制措施

B.应容易被找到以便于在灾难发生时以备紧急情况的需要

C.应部署在离原业务系统所在地较近的地方

D.不需要具有和原业务系统相同的环境监控等级

【答案】 A

315. 在对业务持续性计划进行验证时，以下哪项最为重要

A.数据备份准时执行

B.备份站点已签订合约，并且在需要时可以使用

C.人员安全计划部署适当

D.保险

【答案】 C

316. 组织在制定灾难恢复计划时，应该最先针对以下哪点制定

A.所有信息系统流程

B.所有应用系统流程

C.信息系统经理指派的路程

D.业务经理定义的流程优先级

【答案】 D

317. 拥有电子资金转帐销售点设备的大型连锁商场，有中央通信处理器连接银行网络， 对于通信处理机， 下面哪一项是最好的灾难恢复计划。

A.每日备份离线存储

B.选择在线备份程序

C.安装双通讯设备

D.在另外的网络节点选择备份程序

【答案】 D

318. 在进行业务连续性检测时，下列哪一个是被认为最重要的审查？

A.热站的建立和有效是必要

B.业务连续性手册是有效的和最新的

C.保险责任范围是适当的并且保费有效

D.及时进行介质备份和异地存储

【答案】 D

319. 在准备灾难恢复计划时下列哪项应该首先实施？

A.做出恢复策略

B.执行业务影响分析

C.明确软件系统、硬件和网络组件结构

D.委任具有明确的雇员、角色和层级的恢复团队

【答案】 B

320. 由于 IT 的发展， 灾难恢复计划在大型组织中的应用也发生了变化。

如果新计划没有被测试下面哪项是最主要的风险

A.灾难性的断电

B.资源的高消耗

C."恢复的总成本不能被最小化

"

D.用户和恢复团队在实施计划时可能面临服务器问题

【答案】 A

321. 下面各种方法，哪个是制定灾难恢复策略必须最先评估的

A.所有的威胁可以被完全移除

B.一个可以实现的成本效益，内置的复原

C.恢复时间可以优化

D.恢复成本可以最小化

【答案】 B

322. 作为业务继续计划流程中的一部分，在业务影响分析中下面哪个选项应该最先确认？

A.组织的风险，像单点失败或设备风险

B.重要业务流程的威胁

C.根据恢复优先级设定的重要业务流程

D.重建业务的所需的资源

【答案】 C

323. 在设计业务连续性计划时，企业影响分析可以用来识别关键业务流程和相应的支持程序，它主要会影响到下面哪一项内容的制定？

A.维护业务连续性计划的职责

B.选择站点恢复供应商的条件

C.恢复策略

D.关键人员的职责

【答案】 C

324. 如果恢复时间目标增加，则

A.灾难容忍度增加

B.恢复成本增加

C.不能使用冷备援计算机中心

D.数据备份频率增加

【答案】 A

325. 在计算可接受的关键业务流程恢复时间时

A.只需考虑停机时间的成本

B.需要分析恢复操作的成本

C.停机时间成本和恢复操作成本都需要考虑

D.可以忽略间接的停机成本

【答案】 C

326. 当发生灾难时，以下哪一项能保证业务交易的有效性

A.从当前区域外的地方持续每小时 1 次地传送交易磁带

B.从当前区域外的地方持续每天 1 次地传送交易磁带

C.抓取交易以整合存储设备

D.从当前区域外的地方实时传送交易磁带
【答案】　D
327.　当审核一个组织的业务连续性计划时，某　　IS 审计师观察到这个被审计组织的数据和软件文件被周期性的进行了备份。有效性计划哪一个特性在这里被证明？
A.防止
B.减轻
C.恢复
D.响应
【答案】　B
328.　在业务持续性计划中，下面哪一项具有最高的优先级？
A.恢复关键流程
B.恢复敏感流程
C.恢复站点
D.将运行过程重新部署到一个替代的站点
【答案】　A
329.　在什么情况下，热站会作为一个恢复策略被执行？
A.低灾难容忍度
B.高恢复点目标（　RPO）
C.高恢复时间目标（　RTO）
D.高灾难容忍度
【答案】　A
330.　以下哪种情形下最适合使用数据镜像来作为恢复策略？
A.高的灾难容忍度
B.高的恢复时间目标　(RTO)
C.低的恢复点目标　(RPO)
D.高的恢复点目标　(RPO)
【答案】　C
331.　以下哪一项是两家公司为灾难恢复签订互惠协议而面临的最大风险？
A.各自的发展将导致　(互相间)软硬件不兼容。
B.当需要时资源未必可用。
C.恢复计划无法演练。
D.各家公司的安全基础架构可能不同。
【答案】　A
332.　如果数据中心发生灾难，下列那一项完整恢复一个关键数据库的策略是最适合的　？
A.每日备份到磁带并存储到异地
B.实时复制到异地
C.硬盘镜像到本地服务器
D.实时数据备份到本地网格存储
【答案】　B
333.　在评估一个高可用性网络的恢复能力时，下列情况风险最高：
A.设备在地理位置上分散

B.网络服务器位于同一地点

C.热站就绪可以被激活

D.网络执行了不同行程

【答案】 B

334. 在一个分布式环境中，以下哪一项能够最大程度减轻服务器故障的影响？

A.冗余路径

B.(服务器)集群

C.拨号备份链路

D.备份电源

【答案】 B

335. 以下关于风险评估的描述不正确的是？

A.作为风险评估的要素之一，威胁发生的可能需要被评估

B.作为风险评估的要素之一，威胁发生后产生的影响需要被评估

C.风险评估是风险管理的第一步

D.风险评估是风险管理的最终结果

【答案】 D

336. 以下关于安全控制措施的选择，哪一个选项是错误的 ？

A.维护成本需要被考虑在总体控制成本之内

B.最好的控制措施应被不计成本的实施

C.应考虑控制措施的成本效益

D.在计算整体控制成本的时候，应考虑多方面的因素

【答案】 B

337. 在进行风险分析的时候，发现预测可能造成的风险的经济损失时有一定困难。为了评估潜在的损失，应该：

A.计算相关信息资产的摊销费用

B.计算投资的回报

C.应用定性的方法进行评估

D.花费必要的时间去评估具体的损失的金额

【答案】 C

338. 以下哪个选项是缺乏适当的安全控制的表现

A.威胁

B.脆弱性

C.资产

D.影响

【答案】 B

339. 以下关于标准的描述，那一项是正确的？

A.标准是高级管理层对支持信息安全的声明

B.标准是建立有效安全策略的第一要素

C.标准用来描述组织内安全策略如何实施的

D.标准是高级管理层建立信息系统安全的指示

【答案】 C

340. 关于标准、指南、程序的描述，哪一项是最准确的？

A.标准是建议性的策略，指南是强制执行的策略

B.程序为符合强制性指南的一般性建议

C.程序是为符合强制性指南的一般性建议

D.程序是为符合强制性标准的的说明

【答案】 D

341. 如果出现 IT 人员和最终用户职责分工的问题，下面哪个选项是合适的补偿性控制？

A.限制物理访问计算机设备

B.检查应用及事务处理日志

C.在聘请 IT 人员之前进行背景检查

D.在不活动的特定时间后，锁定用户会话

【答案】 B

342. 以下信息安全原则，哪一项是错误的？

A.实施最小授权原则

B.假设外部系统是不安全的

C.消除所有级别的信息安全风险

D.最小化可信任的系统组件

【答案】 C

343. 下列生物识别设备，哪一项的交差错判率（ CER）最高？

A.虹膜识别设备

B.手掌识别设备

C.声音识别设备

D.指纹识别设备

【答案】 C

344. 为什么实现单点登录的批处理文件及脚本文件需要被保护存储？

A.因为最小授权原则

B.因为它们不可以被操作员访问到

C.因为它们可能包含用户身份信息

D.因为知所必须原则

【答案】 C

345. 下列哪个选项是描述 *- 完整性公理的？

A.Biba 模型中不能向上写

B.Biba 模型中不能向下读

C.BLP模型中不能向下写

D.BLP模型中不能向上读

【答案】 A

346. 实施信息系统访问控制首先需要进行如下哪一项工作？

A.信息系统资产分类

B.信息系统资产标识

C.创建访问控制列表

D.梳理信息系统相关信息资产

【答案】 D

347. 某个机构的网络遭受多次入侵攻击，下面那一种技术可以提前检测到这种行为？

A.杀毒软件

B.包过滤路由器

C.蜜罐

D.服务器加固

【答案】 C

348. 以下哪一个选项是从软件自身功能出发，进行威胁分析

A.攻击面分析

B.威胁建模

C.架构设计

D.详细设计

【答案】 A

349. 在软件开发的需求定义阶段，在软件测试方面，以下哪一个选项被制定？

A.覆盖关键应用的测试数据

B.详细的安全测试计划

C.质量保证测试标准

D.用户验收测试标准

【答案】 D

350. 下面哪个功能属于操作系统中的安全功能

A.控制用户的作业排序和运行

B.对计算机用户访问系统和资源情况进行记录

C.保护系统程序和作业，禁止不合要求的对程序和数据的访问

D.实现主机和外设的并行处理以及异常情况的处理

【答案】 C

351. DDoS 攻击的主要目换是 ：

A.破坏完整性和机密性

B.破坏可用性

C.破坏机密性和可用性

D.破坏机密性

【答案】 B

352. 下列哪个为我国计算机安全测评机构

A.CNITSEC

B.TCSEC

C.FC

D.CC

【答案】 A

353. Windows 组策略适用于

A.S

B.D

C.O

D.S、D、OU

【答案】 D

354. 下列哪一个是国家推荐标准

A.GB/T 18020-1999

B.SJ/T 30003-93

C.ISO/IEC15408

D. GA 243-2000

【答案】 A

355. 黑客造成的主要危害是

A. 破坏系统、窃取信息及伪造信息

B. 攻击系统、获取信息及假冒信息

C. 进入系统、损毁信息及谣传信息

D. 进入系统，获取信息及伪造信息

【答案】 A

356. 下面哪一个不是对点击劫持的描述

A.是一种恶意攻击技术，用于跟踪网络用户并获取私密信息

B.通过让用户来点击看似正常的网页来远程控制其电脑

C.可以用嵌入代码或文本的形式出现，在用户毫不知情的情况下完成攻击

D.可以对方网络瘫痪

【答案】 D

357. 下面哪一层可以实现编码，加密

A.传输层

B.会话层

C.网络层

D.物理层

【答案】 B

358. 下面哪一个描术错误的

A.ＴＣＰ是面向连接可靠的传输控制协议

B.UDP 是无连接用户数据报协议

C.UDP 相比 TCP的优点是速度快

D.TCP/IP协议本身具有安全特性

【答案】 D

359. 特洛伊木马攻击的危胁类型属于

A.授权侵犯威胁

B.植入威胁

C.渗入威胁

D.破坏威胁

【答案】 B

360. 如果双方使用的密钥不同，从其中的一个密钥很难推出另外一个密钥，这样的系统称为

A.常规加密系统

B.单密钥加密系统

C.公钥加密系统

D.对称加密系统

【答案】 C

361. 在数据链路层中 MAC 子层主要实现的功能是

A.介质访问控制

B.物理地址识别

C.通信协议产生

D.数据编码

【答案】 A

362. 路由器工作在 OSI的哪一层

A.传输层

B.数据链路层

C.网络层

D.应用层

【答案】 C

363. 以下哪个命令可以查看端口对应的 PID

A.netstat -ano

B.ipconfig /all

C.tracert

D.netsh

【答案】 A

364. 用于跟踪路由的命令是

A.nestat

B.regedit

C.systeminfo

D.tracert

【答案】 D

365. CA 的核心职责是

A.签发和管理证书

B.审核用户真实信息

C.发布黑名单

D.建立实体链路安全

【答案】 A

366. 以下只用于密钥交换的算法是

A.RSA

B.ECC

C.DH

D.RC4

【答案】 C

367. 以下哪一个是 ITU 的数字证书标准

A.SSL

B.SHTTP

C.x.509

D.SOCKS

【答案】 A

368. 在 TCP中的六个控制位哪一个是用来请求同步的

A.SYN

B.ACK

C.FIN

D.RST

【答案】 A

369. 在 TCP中的六个控制位哪一个是用来请求结束会话的

A.SYN

B.ACK

C.FIN

D.RST

【答案】 C

370. 如果只能使用口令远程认证，以下哪种方案安全性最好？

A.高质量静态口令，散列保护传输

B.高质量静态口令，固定密钥加密保护传输

C.动态随机口令，明文传输

D.高质量静态口令，增加随机值，明文传输

【答案】 C

371. SSO（单点登录）有若干实现方法，以下哪种方案不能实现 SSO?

A.Kerberos 协议

B.自动化登录脚本

C.自动化验证代理

D.SSL VPN网关

【答案】

372. RADIUS是 AAA 协议，涉及三个主要角色：用户 PC，RADIUS客户机，RADIUS服务器，以下说法不正确的是？

A.用户 PC通过 PPP协议连入 RADIUS客户机

B.RADIUS客户机和 RADIUS服务器之间是加密信道

C.RADIUS客户机执行对用户 PC进行认证、授权和记账

D.用户 PC和 RADIUS客户机之间是加密信道

【答案】

373. 一家小型公司需要在两地 Ethernet 之间进行安全通信，以下哪种方案最好？

A.两地边界部署隧道模式的 IPSec VPN网关

B.购买电信光纤电路

C.两地部署基于 SSL协议的 VPN 网关

D.两地边界部署基于 PPTP协议的 VPN 服务器

【答案】

374. 电子银行普遍使用了网银盾进行认证，下面说法正确的是？

A.网银盾不能丢失，因为证书丢了身份会被冒充

B.网银盾不能丢失，因为私钥丢了身份会被冒充

C.数字证书不需要保密，只要证书有备份，网银盾丢了无所谓

D.以上说法都正确

【答案】

375. 一名安全顾问在分析 DLP（数字防泄漏系统）产品的加密技术前，在密码学认识上以下哪条是错误的？

A.当前流行公钥密码技术， DLP应选择公钥算法

B.对称密码技术加密效率高，但密钥管理非常重要，需要特别关注。

C.对称密码技术的密钥和算法模式安全性很关键，需要特别关注

D.如果 DLP 中能把公钥技术和对称密码技术完美结合起来，那最好了。
【答案】

376. 计算机安全有许多最佳设计原则，以下哪个是错误的描述？

A.访问控制应采用默认拒绝的原则

B.安全机制应满足尽量简单的经济性原则

C.安全不应依赖于设计上保密的开放性原则

D.计算机安全应满足以人为本的服务性原则

【答案】

377. 密码学产品涉及密钥管理，这非常重要，以下哪一个不是密钥管理的正确理念？

A.密钥越随机越好，密钥最好存放在只读设备上

B.密钥交换应该采用安全协议自动完成，避免人为干预

C.不要长期使用一个密钥，密钥应有主密钥、子密钥的层次

D.密钥需要保密，不能有 2 个以上的备份，增加泄露风险

【答案】

378. 一个网站允许用户上传文件，但是必须拦截含有恶意代码的文件，同时能提醒用户上载失败，以下哪种方案可行？

A.在网站安装主机版防病毒软件

B.在内网安装网络版防病毒软件

C.在内网部署防病毒网关

D.在内网段部署 IPS

【答案】

379. 网络安全协议普遍使用公钥密码技术和对称密码技术，这么设计的一般原理是以下哪一条？

A.公钥和对称密码的结合，一方面利用公钥便于密钥分配、保护数据完整性的优点，另一方面利用对称密钥加密强、速度快的优点

B.公钥密码技术能实现数字签名，安全协议都需要用到数字签名

C.对称密码技术不能保护信息完整性，必须加入公钥密码技术才能弥补这个缺陷

D.公钥密码技术加密效果不好，必须加入对称密码技术才能弥补这个缺陷

【答案】

380. 3G 智能手机通过 WAP（无线应用协议）网关上网， WAP 使用什么协议保证安全性？

A.TLS

B.WTLS

C.IPSec

D.WEP

【答案】

381. 数字签名总是和散列函数联合使用，以下哪一条是最正确的描述？

A.直接对原始消息签名，速度太慢，利用散列函数能将原始消息转换成唯一的摘要，使数字签名一次完成

B.数字签名应保护整个原始消息，散列函数能将原始消息转换成唯一的

摘要，两者结合使用保护了消息的完整性和真实性

C.没有散列函数，数字签名无法完成

D.没有数字签名，散列函数毫无意义

【答案】

382. 公钥算法无论基于哪种数学难题，他们都有哪一个共同的特点？

A.原始消息都被解析为二进制整数输入算法

B.原始消息都被解析为二进制位串输入算法

C.原始消息都被解析为结构化数据输入算法

D.原始消息都被解析为非结构化数据输入算法

【答案】

383. 软件系统加固的重要工作之一是及时更新以弥补漏洞，以下哪个不是加固更新包？

A.热修补（ Hotfix ）

B.服务包（ Service pack）

C.固件（ Firmware ）包

D.补丁（ Patch）

【答案】

384. 一组安全顾问团队给一个公司的做全面安全渗透测试，以下不正确的说法是？

A.渗透测试应获得公司书面批准，可以采用白盒或黑盒测试方法，白盒测试能发现更多的漏洞，黑盒测试更贴合实际。

B.渗透测试应获得公司书面批准，公司里越少人知道越好，可以充分发挥渗漏威力。

C.渗透测试需要获得公司免责申明，因此安全顾问可以私下保留发现的漏洞供未来使用。

D.渗透测试虽然获得了公司免责申明，但安全顾问不可以私下保留发现的漏洞，除非获得公司使用授权。

【答案】

385. BS7799 这个标准是由下面哪个机构研发出来的？

A.美国标准协会

B.英国标准协会

C.中国标准协会

D.国际标准协会

【答案】 B

386. 以下哪个标准是 ISO 27001 的前身标准？

A.BS5750

B. BS7750

C.BS7799

D.BS15000

【答案】 C

387. 以下标准内容为“ 信息安全管理体系要求 ”的是哪个？

A.ISO 27000

B.ISO 27001

C.ISO 27002

D.ISO 27003
【答案】 B
388. 信息安全属性不包括以下哪个？
A.保密性
B.完整性
C.可用性
D.增值性
【答案】 D
389. 以下对信息安全描述不正确的是
A.信息安全的基本要素包括保密性、完整性和可用性
B.信息安全就是保障企业信息系统能够连续、可靠、正常地运行
C.信息安全就是不出安全事故 /事件
D.信息安全风险是科技风险的一部分
【答案】 C
390. 以下对信息安全管理的描述错误的是
A.信息安全管理的核心就是风险管理
B.人们常说，三分技术，七分管理，可见管理对信息安全的重要性
C.安全技术是信息安全的构筑材料，安全管理是真正的粘合剂和催化剂
D.信息安全管理工作的重点是信息系统，而不是人
【答案】 D
391. 以下不是信息资产是哪一项？
A.服务器
B.机房空调
C.鼠标垫
D.U 盘
【答案】 C
392. 企业按照 ISO 27001 标准建立信息安全管理体系的过程中， 对关键成功因素的描述不正确的是
A.不需要全体员工的参入，只要 IT 部门的人员参入即可
B.来自高级管理层的明确的支持和承诺
C.对企业员工提供必要的安全意识和技能的培训和教育
D.所有管理者、员工能够理解企业信息安全策略、指南和标准，并遵照执行
【答案】 A
393. 信息安全管理手段不包括以下哪一项
A.技术
B.流程
C.人员
D.市场
【答案】 B
394. 信息安全管理体系（ ISMS）是一个怎样的体系，以下描述不正确的是
A.ISMS 是一个遵循 PDCA模式的动态发展的体系
B.ISMS是一个文件化、系统化的体系

C.ISMS 采取的各项风险控制措施应该根据风险评估等途径得出的需求而定

D.ISMS应该是一步到位的，应该解决所有的信息安全问题

【答案】 D

395. 构成风险的关键因素有哪些？

A.人，财，物

B.技术，管理和操作

C.资产，威胁和弱点

D.资产，可能性和严重性

【答案】 C

396. 对于信息安全风险的描述不正确的是

A.企业信息安全风险管理就是要做到零风险

B.在信息安全领域，风险就是指信息资产遭受损坏并给企业带来负面影响及其潜在可能性

C.风险管理就是以可接受的代价，识别、控制、减少或消除可能影响信息系统的安全风险的过程。

D.风险评估就是对信息和信息处理设施面临的威胁、受到的影响、存在的弱点以及威胁发生的可能性的评估。

【答案】 A

397. 降低企业所面临的信息安全风险的手段，以下说法不正确的是？

A.通过良好的系统设计、及时更新系统补丁，降低或减少信息系统自身的缺陷

B.通过数据备份、双机热备等冗余手段来提升信息系统的可靠性；

C.建立必要的安全制度和部署必要的技术手段，防范黑客和恶意软件的攻击

D.通过业务外包的方式，转嫁所有的安全风险责任

【答案】 D

398. 风险评估的基本过程是怎样的？

A.识别并评估重要的信息资产，识别各种可能的威胁和严重的弱点，最终确定风险

B.通过以往发生的信息安全事件，找到风险所在

C.风险评估就是对照安全检查单，查看相关的管理和技术措施是否到位

D.风险评估并没有规律可循，完全取决于评估者的经验所在

【答案】 A

399. 以下对企业信息安全活动的组织描述不正确的是

A.企业应该在组织内建立发起和控制信息安全实施的管理框架。

B.企业应该维护被外部合作伙伴或者客户访问和使用的企业信息处理设施和信息资产的安全。

C.在没有采取必要控制措施，包括签署相关协议之前，不应该授权给外部伙伴访问。应该让外部伙伴意识到其责任和必须遵守的规定。

D.企业在开展业务活动的过程中，应该完全相信员工，不应该对内部员工采取安全管控措施

【答案】 D

400. 企业信息资产的管理和控制的描述不正确的是

A.企业应该建立和维护一个完整的信息资产清单，并明确信息资产的管控责任；

B.企业应该根据信息资产的重要性和安全级别的不同要求，采取对应的管控措施；

C.企业的信息资产不应该分类分级，所有的信息系统要统一对待

D.企业可以根据业务运作流程和信息系统拓扑结构来识别所有的信息资产

【答案】 C

401. 企业 ISMS(信息安全管理体系)建设的原则不包括以下哪个

A.管理层足够重视

B.需要全员参与

C.不必遵循过程的方法

D.需要持续改进

【答案】 C

402. PDCA特征的描述不正确的是

A.顺序进行，周而复始，发现问题，分析问题，然后是解决问题

B.大环套小环，安全目标的达成都是分解成多个小目标，一层层地解决问题

C.阶梯式上升，每次循环都要进行总结，巩固成绩，改进不足

D.信息安全风险管理的思路不符合 PDCA的问题解决思路

【答案】 D

403. 以下有关通信与日常操作描述不正确的是？

A.信息系统的变更应该是受控的

B.企业在岗位设计和人员工作分配时应该遵循职责分离的原则

C.移动介质使用是一个管理难题，应该采取有效措施，防止信息泄漏

D.所有日常操作按照最佳实践来进行操作，无需形成操作手册。

【答案】 C

404. 有关信息安全事件的描述不正确的是？

A.信息安全事件的处理应该分类、分级

B.信息安全事件的数量可以反映企业的信息安全管控水平

C.对于一些信息安全隐患，如果还没造成损失，就没必要进行报告。

D.信息安全事件处理流程中的一个重要环节是对事件发生的根源的追溯，以吸取教训、总结经验，防止类似事情再次发生

【答案】 C

405. 以下哪项不属于信息安全管理的工作内容

A.信息安全培训

B.信息安全考核

C.信息安全规划

D.安全漏洞扫描

【答案】 D

406. 以下哪项不是信息安全的主要目标

A.确保业务连续性

B.保护信息免受各种威胁的损害

C.防止黑客窃取员工个人信息

D.投资回报和商业机遇最大化
【答案】　C
407.　信息安全需求获取的主要手段
A.信息安全风险评估
B.领导的指示
C.信息安全技术
D.信息安全产品
【答案】　A
408.　下面哪项不是实施信息安全管理的关键成功因素
A.理解组织文化
B.得到高层承诺
C.部署安全产品
D.纳入奖惩机制
【答案】　C
409.　下面哪一个不是高层安全方针所关注的
A.识别关键业务目标
B.定义安全组织职责
C.定义安全目标
D.定义防火墙边界防护策略
【答案】　D
410.　谁对组织的信息安全负最终责任？
A.安全经理
B.高管层
C.IT经理
D.业务经理
【答案】　B
411.　ISO27004 是指以下哪个标准
A.《信息安全管理体系要求》
B.《信息安全管理实用规则》
C.《信息安全管理度量》
D.《ISMS 实施指南》
【答案】　C
412.　下面哪一项不是　ISMS Plan阶段的工作？
A.定义 ISMS方针
B.实施信息安全风险评估
C.实施信息安全培训
D.定义 ISMS范围
【答案】　C
413.　下面哪一项不是　ISMS Check阶段的工作？
A.安全事件响应
B.安全内部审核
C.管理评审
D.更新安全计划
【答案】　A

414. 定义 ISMS 范围时，下列哪项不是考虑的重点

A.组织现有的部门

B.信息资产的数量与分布

C.信息技术的应用区域

D.IT 人员数量

【答案】 D

415. 当选择的控制措施成本高于风险带来的损失时，应考虑

A.降低风险

B.转移风险

C.避免风险

D.接受风险

【答案】 D

416. 关于控制措施选择描述不正确的是

A.总成本中应考虑控制措施维护成本

B.只要控制措施有效，不管成本都应该首先选择

C.首先要考虑控制措施的成本效益

D.应该考虑控制措施实施的成熟度

【答案】 B

417. 信息资产分级的最关键要素是

A.价值

B.时间

C.安全性

D.所有者

【答案】 A

418. 管理评审的最主要目的是

A.确认信息安全工作是否得到执行

B.检查信息安全管理体系的有效性

C.找到信息安全的漏洞

D.考核信息安全部门的工作是否满足要求

【答案】 B

419. 内部审核的最主要目的是

A.检查信息安全控制措施的执行情况

B.检查系统安全漏洞

C.检查信息安全管理体系的有效性

D.检查人员安全意识

【答案】 A

420. 在某个公司中 ,以下哪个角色最适合评估信息安全的有效性 ?

A.公司的专家

B.业务经理

C.IT 审计员

D.信息安全经理

【答案】 C

421. 安全评估人员正为某个医疗机构的生产和测试环境进行评估。在访谈中，注意到生产数据被用于测试环境测试，这种情况下存在哪种最

有可能的潜在风险？

A.测试环境可能没有充足的控制确保数据的精确性

B.测试环境可能由于使用生产数据而产生不精确的结果

C.测试环境的硬件可能与生产环境的不同

D.测试环境可能没有充分的访问控制以确保数据机密性

【答案】 D

422. 在软件程序测试的哪个阶段一个组织应该进行体系结构设计测试 ?

A.可接受性测试

B.系统测试

C.集成测试

D.单元测试

【答案】 C

423. 什么类型的软件应用测试被用于测试的最后阶段，并且通常包含不属于开发团队之内的用户成员 ?

A.Alpha 测试

B.白盒测试

C.回归测试

D.Beta 测试

【答案】 D

424. 在系统实施后评审过程中，应该执行下面哪个活动？

A.用户验收测试

B.投资收益分析

C.激活审计模块

D.更新未来企业架构

【答案】 B

425. 某公司的在实施一个 DRP项目 ,项目按照计划完成后。聘请了专家团队进行评审，评审过程中发现了几个方而的问题 ,以下哪个代表最大的风险

A.没有执行 DRP测试

B.灾难恢复策略没有使用热站进行恢复

C.进行了 BIA，但其结果没有被使用

D.灾难恢复经理近期离开了公司

【答案】 C

426. 在设计某公司技术性的恢复策略时 ,以下哪个方面是安全人员最为关注的 ？

A.目标恢复时间 RTO

B.业务影响分析

C.从严重灾难中恢复的能力

D.目标恢复点 RPO

【答案】 B

427. 时间的流逝对服务中断损失成本和中断恢复成本会有什么影响？

A.两个成本增加

B.中断的损失成本增加，中断恢复的成本随时问的流逝而减少

C.两个成本都随时间的流逝而减少

D.没有影响
【答案】 B
428. 恢复策略的选择最可能取决于
A.基础设施和系统的恢复成本
B.恢复站点的可用性
C.关键性业务流程
D.事件响应流程
【答案】 C
429. 某公司在测试灾难恢复计划时是发现恢复业务运营所必要的关键数据没有被保留 ,可能由于什么没有明确导致的 ?
A.服务中断的时间间隔
B.目标恢复时间 (RTO)
C.服务交付目标
D.目标恢复点 (RPO)
【答案】 D
430. 下面哪个是管理业务连续性计划中最重要的方面 ?
A.备份站点安全以及距离主站点的距离。
B.定期测试恢复计划
C.完全测试过的备份硬件在备份站点可有
D.多个网络服务的网络连接是可用
【答案】 B
431. 一个组织的灾难恢复 (DR, disaster recovery) 策略的变更时将公司的关键任务应用的恢复点目标 (RPO)被缩短了，下述哪个是该变更的最显著风险？
A.现有的 DR 计划没有更新以符合新的 RPO
B.DR小组没有基于新的 RPO进行培训
C.备份没有以足够的频率进行以实现新的 RPO
D.该计划没有基于新的 RPO进行测试
【答案】 C
432. 在加固数据库时 ,以下哪个是数据库加固最需要考虑的？
A.修改默认配置
B.规范数据库所有的表空间
C.存储数据被加密
D.修改数据库服务的服务端口
【答案】 A
433. 数据库管理员执行以下那个动作可能会产生风险 ?
A.根据变更流程执行数据库变更
B.安装操作系统的补丁和更新
C.排列表空间并考虑表合并的限制
D.执行备份和恢复流程
【答案】 B
434. 一个公司解雇了一个数据库管理员 ,并且解雇时立刻取消了数据库管理员对公司所有系统的访问权 ,但是数据管理员威胁说数据库在两个月内将被删除，除非公司付他一大笔钱。数据管理员最有可能采用下面哪

种手段删除数据库？

A.放置病毒

B.蠕虫感染

C.DoS攻击

D.逻辑炸弹攻击

【答案】 D

435. 20 世纪 70－90 年代，信息安全所面临的威胁主要是非法访问、恶意代码和脆弱口令等，请问这是信息安全发展的什么阶段？

A.通信安全。

B.计算机安全。

C.信息系统安全。

D.信息安全保障。

【答案】 B

436. 以下哪项不属于造成信息安全问题的自然环境因素？

A.纵火。

B.地震。

C.极端天气。

D.洪水。

【答案】 A

437. 以下哪项不属于信息系统安全保障模型包含的方面？

A.保障要素。

B.生命周期。

C.安全特征。

D.通信安全。

【答案】 D

438. 以下哪项是正确的信息安全保障发展历史顺序？

A.通信安全→计算机安全→信息系统安全→信息安全保障→网络空间安全/ 信息安全保障

B.通信安全→信息安全保障→计算机安全→信息系统安全→网络空间安全/ 信息安全保障

C.计算机安全→通信安全→信息系统安全→信息安全保障→网络空间安全/ 信息安全保障

D.通信安全→信息系统安全→计算机安全→信息安全保障→网络空间安全/ 信息安全保障

【答案】 A

439. 对于信息安全策略的描述错误的是？

A.信息安全策略是以风险管理为基础，需要做到面面俱到，杜绝风险的存在。

B.信息安全策略是在有限资源的前提下选择最优的风险管理对策。

C.防范不足会造成直接的损失；防范过多又会造成间接的损失。

D.信息安全保障需要从经济、技术、管理的可行性和有效性上做出权衡和取舍。

【答案】 A

440. 安全模型是用于精确和形式地描述信息系统的安全特征，解释系

统安全相关行为。关于它的作用描述不正确的是？

A.准确的描述安全的重要方面与系统行为的关系。

B.开发出一套安全性评估准则，和关键的描述变量。

C.提高对成功实现关键安全需求的理解层次。

D.强调了风险评估的重要性。

【答案】 D

441. 信息保障技术框架（ IATF）是美国国家安全局（ NSA）制定的，为保护美国政府和工业界的信息与信息技术设施提供技术指南，关于 IATF 的说法错误的是？

A.IATF的代表理论为“ 深度防御 ” 。

B.IATF强调人、 技术、 操作这三个核心要素， 从多种不同的角度对信息系统进行防护。

C.IATF关注本地计算环境、 区域边界、 网络和基础设施三个信息安全保障领域。

D.IATF 论述了系统工程、系统采购、风险管理、认证和鉴定以及生命周期支持等过程。

【答案】 C

442. P2DR 模型强调了落实反应和系统安全的动态性，其中的“ 检测 ”使用的主要方法是？

A.检测。

B.报警。

C.记录。

D.实时监控。

【答案】 C

443. P2DR 模型通过传统的静态安全技术和方法提高网络的防护能力，这些技术包括？

A.实时监控技术。

B.访问控制技术。

C.信息加密技术。

D.身份认证技术。

【答案】 A

444. P2DR 模型中的“ 反应 ”是在检测到安全漏洞和安全事件时，通过及时的响应措施将网络系统的安全性调整到风险最低的状态，这些措施包括？

A.关闭服务。

B.向上级汇报。

C.跟踪。

D.消除影响。

【答案】 B

445. 下面哪一个机构不属于美国信息安全保障管理部门？

A.国土安全部。

B.国防部。

C.国家基础设施顾问委员会。

D.国家标准技术研究所。

【答案】　C

446.　第一个建立电子政务标准的国家是？

A.英国。

B.美国。

C.德国。

D.俄罗斯。

【答案】　C

447.　2008 年 1 月 8 日，布什以第　54 号国家安全总统令和第　　23 号国土安全总统令的形式签署的文件是？

A.国家网络安全战略。

B.国家网络安全综合计划。

C.信息基础设施保护计划。

D.强化信息系统安全国家计划。

【答案】　B

448.　我国的信息安全保障基本原则是？

A.正确处理安全与发展的关系，以安全保发展，在发展中求安全。

B.立足国情，以我为主，坚持管理与技术并重。

C.强化未来安全环境，增强研究、开发和教育以及投资先进的技术来构建将来的环境。

D.明确国家、企业、个人的责任和义务，充分发挥各方面的积极性，共同构筑国家信息安全保障体系。

【答案】　C

449.　我国的信息安全测评主要对象不包括？

A.信息产品安全测评。

B.信息安全人员资质测评。

C.服务商资质测评。

D.信息保障安全测评。

【答案】　D

450.　以下哪一个不是网络隐藏技术？

A.端口复用

B."无端口技术

"

C.反弹端口技术

D.DLL注入

【答案】　D

451.　监视恶意代码主体程序是否正常的技术是？

A.进程守护

B.备份文件

C.超级权限

D.HOOK技术

【答案】　A

452.　以下哪一个不是安全审计的作用？

A.记录系统被访问的过程及系统保护机制的运行状态。

B.发现试图绕过保护机制的行为。

C.及时发现并阻止用户身份的变化

D.报告并阻碍绕过保护机制的行为并记录相关进程，为灾难恢复提供信息。

【答案】 C

453. 以下哪一个不是安全审计需要具备的功能？

A.记录关键事件

B.提供可集中处理审计日志的数据形式

C.实时安全报警

D.审计日志访问控制

【答案】 D

454. 以下哪一个是在所有的 WINDOWS2000和 WINDOWS系统中都存在的日志是？

A.目录服务日志

B.文件复制日志

C.应用服务日志

D.DNS服务日志

【答案】 C

455. 恶意代码的第一个雏形是？

A.磁芯大战

B.爬行者

C.清除者

D.BRAIN

【答案】 A

456. 以下哪一个是包过滤防火墙的优点？

A.可以与认证、授权等安全手段方便的集成。

B.与应用层无关，无须改动任何客户机和主机的应用程序，易于安装和使用。

C.提供透明的加密机制

D.可以给单个用户授权

【答案】 C

457. 以下哪一个不是 VLAN的划分方式

A.根据 TCP端口来划分

B.根据 MAC 地址来划分

C.根据 IP 组播划分

D."根据网络层划分

"

【答案】 A

458. 以下哪一个不是 OSI安全体系结构中的安全机制

A.数字签名

B.路由控制

C.数据交换

D.抗抵赖

【答案】 D

459. 程序设计和编码的问题引入的风险为：

A."网络钓鱼
"

B."缓冲区溢出
"

C."SYN 攻击
"

D.暴力破解
【答案】 B

460. CC中的评估保证级 4 级（EAL3）对应 TCSEC和 ITSEC的哪个级别？

A."对应 TCSEC B1级，对应 ITSEC E4级
"

B."对应 TCSEC C2级，对应 ITSEC E4级
"

C."对应 TCSEC B1级，对应 ITSEC E3级
"

D." 对应 TCSEC C2级，对应 ITSEC E2级
"

【答案】 D

461. ISO/IEC27002 由以下哪一个标准演变而来？

A.BS7799-1

B.BS7799-2

C.ISO/IEC 17799

D.ISO/IEC13335

【答案】 C

462. 以下哪一个不是风险控制的主要方式

A.规避方式

B.转移方式

C.降低方式

D.隔离方式

【答案】 D

463. 《关于信息安全等级保护的实施意见》中信息和信息系统安全保护等级的第三级的定义是

A.自主保护级

B.指导保护级

C.强制保护级

D.监督保护级

【答案】 D

464. 灾难恢复 SHARE78的第三层是指

A.卡车运送

B.电子链接

C.活动状态的备份中心

D.0 数据丢失

【答案】 B

465. 以下关于在 UNIX 系统里启动与关闭服务的说法不正确的是？

A.在 UNIX 系统中，服务可以通过 inetd 进程来启动

B.通过在 /etc/inetd.conf 文件中注释关闭正在运行的服务

C.通过改变脚本名称的方式禁用脚本启动的服务

D.在 UNIX 系统中，服务可以通过启动脚本来启动

【答案】 B

466. 以下关于 UNIX 引导过程描述正确的是？

A."1. 开始引导装入程序 (boot loader)

2. 开始其他系统“自发的”进程

3.内核初始化并运行内核程序

4. 运行系统起始脚本

"

B."1. 开始引导装入程序 (boot loader)

2. 内核初始化并运行内核程序

3. 开始其他系统“自发的”进程

4. 运行系统起始脚本

"

C."1. 开始引导装入程序 (boot loader)

2. 内核初始化并运行内核程序

3. 运行系统起始脚本

4. 开始其他系统“自发的”进程 "

D."1. 内核初始化并运行内核程序

2. 开始引导装入程序 (boot loader)

3. 开始其他系统“自发的”进程

4. 运行系统起始脚本 "

【答案】 B

467. 以下哪个进程不属于 NFS服务器端的进程？

A.statd

B.mountd

C.nfsd

D.Automounter

【答案】 A

468. Linux 文件系统采用的是树型结构， 在根目录下默认存在 var 目录，它的的功用是？

A.公用的临时文件存储点

B.系统提供这个目录是让用户临时挂载其他的文件系统

C.某些大文件的溢出区

D.最庞大的目录，要用到的应用程序和文件几乎都在这个目录

【答案】 C

469. 在 Linux 操作系统中， 为了授权用户具有管理员的某些个性需求的权限所采取的措施是什么？

A.告诉其他用户 root 密码

B.将普通用户加入到管理员组

C.使用 visudo 命令授权用户的个性需求

D.创建单独的虚拟账户

【答案】 C

470. 在对 Linux 系统中 dir 目录及其子目录进行权限权限统一调整时所使用的命令是什么？

A.rm -fr -755 /dir

B.ls -755 /dir

C.chmod 755 /dir/*

D.chmod -R 755 /dir

【答案】 D

471. 默认情况下 Linux 主机在机房托管期间被恶意用户进行了 SSH远程的暴力破解，此时安全工程师需要拒绝其访问的源地址，应该使用那种方式查询其访问的记录？

A.cat /var/log/secure

B.who

C.whoami

D.cat /etc/security/access.log

【答案】 A

472. Linux 系统一般使用 GRUB作为启动的 MBR 程序， GRUB如何配置才能放置用户加入单用户模式重置 root 密码？

A.删除敏感的配置文件

B.注释 grub.conf 文件中的启动项

C.在对应的启动 title 上配置进入单用户的密码

D.将 GRUB程序使用非对称秘钥加密

【答案】 C

473. 以下发现属于 Linux 系统严重威胁的是什么？

A.发现不明的 SUID可执行文件

B.发现应用的配置文件被管理员变更

C.发现有恶意程序在实时的攻击系统

D.发现防护程序收集了很多黑客攻击的源地址

【答案】 A

474. 以下哪项行为可能使用嗅探泄露系统的管理员密码？

A.使用 root 用户访问 FTP程序

B.使用 root 用户连接 SSH服务

C.使用 root 进行 SCP文件传输

D.在本地使用 root 用户登录

【答案】 A

475. 以下不属于 Linux 安全加固的内容是什么？

A.配置 iptables

B.配置 Tcpwapper

C.启用 Selinux

D.修改 root 的 UID

【答案】 D

476. 以下描述中不属于 SSH用途的为？

A.用于远程的安全管理，使用 SSH 客户端连接远程 SSH服务器，建立安全的 Shell 交互环境

B.用于本地到远程隧道的建立，进而提供安全通道，保证某些业务安全传输

C.进行对本地数据使用 SSH 的秘钥进行加密报错，以提高其业务的可靠性

D.SCP远程安全数据复制借助 SSH协议进行传输， SSH提供其安全隧道保障

【答案】 C

477. 对于 Linux 的安全加固项说法错误的是哪项？

A.使用 uname -a 确认其内核是否有漏洞

B.检查系统是否有重复的 UID 用户

C.查看 login.defs 文件对于密码的限制

D.查看 hosts 文件确保 Tcpwapper 生效

【答案】 D

478. 对于 Linux 审计说法错误的是？

A.Linux 系统支持细粒度的审计操作

B.Linux 系统可以使用自带的软件发送审计日志到 SOC平台

C.Linux 系统一般使用 auditd 进程产生日志文件

D.Linux 在 secure 日志中登陆成功日志和审计日志是一个文件

【答案】 D

479. 对于 Linux 操作系统中 shadow 文件说法不正确的是？

A.shadow 文件可以指定用户的目录

B.shadow 文件中定义了密码的使用期限

C.读取 shadow 文件能够发现秘钥的加密方法

D.shadow 文件对于任何人是不可以读取的

【答案】 A

480. 以下关于软件安全测试说法正确的是？

A.软件安全测试就是黑盒测试。

B.Fuzz测试是经常采用的安全测试方法之一。

C.软件安全测试关注的是软件的功能。

D.软件安全测试可以发现软件中产生的所有安全问题。

【答案】 B

481. 作为信息安全管理人员，你认为变更管理过程最重要的是？

A.变更过程要留痕

B.变更申请与上线提出要经过审批

C.变更过程要坚持环境分离和人员分离原则

D.变更要与容灾预案同步

【答案】 B

482. 如果恶意开发人员想在代码中隐藏逻辑炸弹，什么预防方式最有效？

A.源代码周期性安全扫描

B.源代码人工审计

C.渗透测试

D.对系统的运行情况进行不间断监测记录

【答案】 B

483. 测试人员与开发人员交互测试发现的过程中，开发人员最关注的什么？

A.bug 的数量

B.bug 的严重程度

C.bug 的复现过程

D.bug 修复的可行性

【答案】 C

484. 安全开发制度中， QA 最关注的的制度是

A.系统后评价规定

B.可行性分析与需求分析规定

C.安全开发流程的定义、交付物和交付物衡量标准

D.需求变更规定

【答案】 C

485. 项目经理欲提高信息系统安全性，他首先要做的工作是

A.考虑安全开发需要什么样的资源与预算

B.考虑安全开发在开发生命周期各阶段应开展哪些工作

C.对开发团队进行信息安全培训

D.购买一定的安全工具，如代码扫描工具等

【答案】 B

486. 输入参数过滤可以预防以下哪些攻击

A.SQL注入、跨站脚本、缓冲区溢出

B.SQL注入、跨站脚本、 DNS 毒药

C.SQL注入、跨站请求伪造、网络窃听

D.跨站请求伪造、跨站脚本、 DNS毒药

【答案】 A

487. 以下哪项机制与数据处理完整性相关

A.数据库事务完整性机制

B.数据库自动备份复制机制

C.双机并行处理，并相互验证

D.加密算法

【答案】 D

488. 面向对象的开发方法中，以下哪些机制对安全有帮助

A.封装

B.多态

C.继承

D.重载

【答案】 A

489. 对系统安全需求进行评审，以下那类人不适合参与

A.系统分析员

B.业务代表

C.安全专家

D.合规代表

【答案】 A

490. 以下哪项活动对安全编码没有帮助

A.代码审计

B.安全编码规范

C.编码培训

D.代码版本管理

【答案】 D

491. 开发人员认为系统架构设计不合理，需要讨论调整后，再次进入编码阶段。开发团队可能采取的开发方法为

A.瀑布模型

B.净室模型

C.XP模型

D.迭代模型

【答案】 A

492. 为了预防逻辑炸弹，项目经理采取的最有效的措施应该是

A.对每日提交的新代码进行人工审计

B.代码安全扫描

C.安全意识教育

D.安全编码培训教育

【答案】 A

493. 对缓冲区溢出攻击预防没有帮助的做法包括

A.输入参数过滤，安全编译选项

B.操作系统安全机制、禁止使用禁用 API

C.安全编码教育

D.渗透测试

【答案】 D

494. 从业务角度出发，最大的风险可能发生在那个阶段

A.立项可行性分析阶段

B.系统需求分析阶段

C.架构设计和编码阶段

D.投产上线阶段

【答案】 A

495. 那种测试结果对开发人员的影响最大

A.单元测试和集成测试

B.系统测试

C.验收测试

D.渗透测试

【答案】 C

496. 下面对自由访问控制（ DAC）描述正确的是

A.比较强制访问控制而言不太灵活

B.基于安全标签

C.关注信息流

D.在商业环境中广泛使用

【答案】 D

497. 下列哪项是系统问责时不需要的？

A.认证

B.鉴定

C.授权

D.审计

【答案】 C

498. 下列哪项是多级安全策略的必要组成部分？

A.主体、客体的敏感标签和自主访问控制。

B.客体敏感标签和强制访问控制。

C.主体的安全凭证、客体的安全标签和强制访问控制。

D.主体、客体的敏感标签和对其“系统高安全模式”的评价

【答案】 C

499. 有关 Kerberos 说法下列哪项是正确的？

A.它利用公钥加密技术。

B.它依靠对称密码技术。

C.它是第二方的认证系统。

D.票据授予之后将加密数据，但以明文方式交换密码

【答案】 B

500. 下列哪项不是 Kerberos 密钥分发服务（ KDS）的一部分？

A.Kerberos 票证授予服务器（ TGS）。

B.Kerberos 身份验证服务器（ KAS）。

C.存放用户名和密码的数据库。

D.Kerberos 票证吊销服务器（ TRS）。

【答案】 D

501. 下列哪项是系统问责所需要的？

A.授权。

B.多人共用同一帐号。

C.审计机制。

D.系统设计的形式化验证

【答案】 C

502. 下列关于 Kerberos 的描述，哪一项是正确的？

A.埃及神话中的有三个头的狗。

B.安全模型。

C.远程身份验证拨入用户服务器。

D.一个值得信赖的第三方认证协议。

【答案】 D

503. Kerberos 依赖什么加密方式？

A. El Gamal 密码加密

B.秘密密钥加密。

C.Blowfish 加密。

D.公钥加密。

【答案】 B

504. 及时审查系统访问审计记录是以下哪种基本安全功能？

A.威慑。

B.规避。

C.预防。

D.检测。

【答案】　D

505.　个人问责不包括下列哪一项？

A.访问规则。

B.策略与程序。

C.审计跟踪。

D.唯一身份标识符。

【答案】　B

506.　下列哪一项体现了适当的职责分离？

A.磁带操作员被允许使用系统控制台。

B.操作员是不允许修改系统时间。

C.允许程序员使用系统控制台。

D.控制台操作员被允许装载磁带和磁盘。

【答案】　B

507.　实施逻辑访问安全时，以下哪项不是逻辑访问？

A.用户 ID。

B.访问配置文件。

C.员工胸牌。

D.密码。

【答案】　C

508.　银行柜员的访问控制策略实施以下的哪一种？

A.基于角色的策略。

B.基于身份的策略。

C.基于用户的策略。

D.基于规则政策。

【答案】　A

509.　以下哪一种身份验证机制为移动用户带来验证问题？

A.可重复使用的密码机制

B.一次性口令机制。

C.挑战响应机制。

D.基于 IP 地址的机制

【答案】　D

510.　组织允许外部通过互联网访问组织的局域网之前，首先要考虑实施以下哪项措施？

A.保护调制解调器池。

B.考虑适当的身份验证方式。

C.为用户提供账户使用信息。

D.实施工作站锁定机制。

【答案】　B

511.　防范密码嗅探攻击计算机系统的控制措施包括下列哪一项？

A.静态和重复使用的密码。

B.加密和重复使用的密码。

C.一次性密码和加密。

D.静态和一次性密码。

【答案】　C

512.　Kerberos 可以防止以下哪种攻击？

A.隧道攻击。

B.重放攻击。

C.破坏性攻击。

D.处理攻击。

【答案】　B

513.　在自主访问环境中，以下哪个实体可以将信息访问权授予给其他人？

A.经理

B.集团负责人

C.安全经理

D.数据所有者

【答案】　D

514.　单点登录系统主要的关切是什么？

A.密码一旦泄露，最大程度的非授权访问将可能发生。

B.将增加用户的访问权限。

C.用户的密码太难记。

D.安全管理员的工作量会增加。

【答案】　A

515.　不受限制的访问生产系统程序的权限将授予以下哪些人？

A.审计师

B.不可授予任何人

C.系统的属主。

D.只有维护程序员

【答案】　B