深圳市第十四届职工技术创新运动会暨2024年深圳技能大赛—密码技术应用员职业技能竞赛初赛理论知识

一、单选题

1.职业道德的核心原则是（）。……参考答案：B
A、个人发展为首要目标
B、维护社会公平和正义
C、追求个人利益最大化
D、不顾职业伦理，追求个人权力

2.职业道德是指在特定职业领域中所应遵守的道德规范和行为准则，以下（）选项最符合职业道德的定义。……参考答案：B
A、利用职权谋取私利
B、高度责任心和敬业精神
C、不顾职业伦理，追求利益最大化
D、忽视职业道德，只追求个人发展

3.良好的职业道德有利于促进企业的（）。……参考答案：D
A、公信力
B、竞争力
C、生命力
D、以上都是

4.以下不属于良好职业道德所具有的作用是（）。……参考答案：D
A、提高企业信誉度
B、提高企业凝聚力
C、提高企业竞争力
D、提高企业发展力

5.封建社会职业道德的主要特点是（）。……参考答案：B
A、无私奉献
B、等级制度
C、诚实守信
D、尊重他人

6.职业道德的发展可以追溯到（）时期。……参考答案：A
A、原始社会
B、奴隶社会

C、封建社会
D、资本主义社会

7.关于职业道德的作用，以下说法正确的是（）。……参考答案：A
A、在适用范围上具有普遍性
B、只在少数行业起作用
C、会降低企业的竞争力
D、不同职业职业道德普遍不相同

8.社会主义职业道德的核心是（）。……参考答案：B
A、诚实守信
B、服务群众
C、爱岗敬业
D、奉献社会

9.实现爱党爱国的具体做法是（）。……参考答案：B
A、诚实守信
B、时刻维护国家声誉
C、停留在口号即可
D、爱岗敬业

10.关于爱党爱国，正确的理解应该是（）。……参考答案：C
A、只在心中即可，行动中无需做到
B、爱党和爱国会损失个人利益
C、爱党和爱国是每个公民的基本义务
D、个人做到即可，企业则不用

11.遵纪守法，诚实守信是对职业人的（）。……参考答案：C
A、严格要求
B、最高要求
C、基本要求
D、强制要求

12.党的十六大报告指出,认真贯彻公民道德建设实施纲要,弘扬爱国主义精神以为人民服务为核心,以集体主义为原则,以（）为重点。……参考答案：B
A、无私奉献
B、诚实守信
C、爱岗敬业
D、遵纪守法

13.以下（）行为不属于严守秘密的行为。……参考答案：C
A、不随意谈论客户隐私
B、关键技术保密
C、闭门造车，不参与讨论

D、不在机房重地拍照

14.关于坚持原则，严守秘密的做法不正确的是（）。……参考答案：D
A、自觉维护商业秘密，不随意泄露
B、有自己的行为准则，不随波逐流
C、不应金钱和权力而放弃原则
D、为利益而放弃底线

15.关于爱岗敬业，正确的理解应该是（）。……参考答案：D
A、阻碍了人员寻找更好的职业机遇
B、在岗位上一辈子无私奉献
C、不符合现代人力流动的需求
D、干一行，爱一行

16.提升职业责任感是（）职业守则的基本要求。……参考答案：A
A、爱岗敬业
B、团结协作
C、遵纪守法
D、诚实守信

17.以下做法中，符合积极进取，刻苦钻研精神的是（）。……参考答案：A
A、勇于挑战自我和难题
B、按时上下班
C、安于现状
D、畏惧困难

18.下面说法，你认为正确的是（）。……参考答案：C
A、积极进取一定要别人看到才有效果
B、刻苦钻研要求独自解决难题
C、积极进取，刻苦钻研往往会提升个人发展前期
D、刻苦钻研就是闭门造车

19.奉献的属性是（）。……参考答案：A
A、可为性
B、功利性
C、回报性
D、普遍性

20.二进制中的负数的补码的定义是（）。……参考答案：C
A、原码加一
B、反码减一
C、反码加一
D、原码减一

21.以下负责计算机系统中的算术和逻辑运算的部件是（）。……参考答案：D
A、算术逻辑单元（ALU）
B、控制单元（CU）
C、存储器管理单元（MMU）
D、中央处理器(CPU)

22.关于 CPU 中指令执行的描述，以下描述正确的是（）。……参考答案：B
A、指令的执行过程包括取指、译码、调试三个阶段
B、CPU 中的控制单元负责解析和执行指令，协调计算机各个部件的操作。
C、所有指令都需要经过完整的指令周期才能执行完毕。
D、微程序控制的计算机不能执行宏指令。

23.操作系统(OS)的主要功能是（）。……参考答案：B
A、运行游戏
B、管理计算机硬件资源和提供为用户和其他软件提供服务的接口
C、进行文字处理
D、上网

24.编程语言中的变量是用来存储（）。……参考答案：B
A、操作步骤
B、数值和数据
C、用户输入
D、程序代码

25.TCP 和 UDP 在互联网协议栈中属于（）。……参考答案：B
A、应用层
B、传输层
C、会话层
D、链路层

26.在 OSI 的七层模型中，（）负责建立、维护和终止通信会话。……参考答案：C
A、应用层
B、传输层
C、会话层
D、网络层

27.在网络中，交换机工作的协议层是（）。……参考答案：C
A、应用层
B、传输层
C、数据链路层
D、网络层

28.交换机和路由器在计算机网络中扮演的角色是（）。……参考答案：C
A、交换机用于连接不同的网络，路由器用于内部网络通信

B、路由器用于内部网络通信，交换机用于连接不同的网络
C、交换机用于内部网络通信，路由器用于连接不同的网络
D、路由器用于数据包的路由选择，交换机用于数据的转发

29.在模拟电路中，控制电流流动的方向的元件是（）。……参考答案：C
A、电阻器
B、电容器
C、二极管
D、变压器

30.在数字电路中，只有当所有输入都为高电平时，输出才会是高电平的逻辑门是（）。……参考答案：A
A、AND 门
B、OR 门
C、NAND 门
D、NOR 门

31.负数-1 的八位二进制中的补码的表示正确的是（）。……参考答案：D
A、00000001
B、10000000
C、11111110
D、11111111

32.在二进制系统中，数字 1011 对应的十进制数是（）。……参考答案：B
A、10
B、11
C、12
D、13

33.在 Windows 中，用于打开任务管理器的快捷键是（）。……参考答案：A
A、Ctrl + Shift + Esc
B、Ctrl + Alt + Del
C、Alt + F4
D、Windows + R

34.Windows 系统的“安全模式”用于（）。……参考答案：D
A、提高系统安全
B、数据恢复
C、提高运行速度
D、故障排查

35.在 Linux 中，用于改变文件或目录的所有者的命令是（）。……参考答案：C
A、chgrp
B、mv

C、chown
D、chmod

36.在 Linux 中用于压缩文件的命令是（）。……参考答案：B
A、tar
B、gzip
C、unzip
D、touch

37.在 SQL 中，JOIN 操作是用来（）。……参考答案：B
A、连接不同的数据库
B、连接表中的行
C、合并相同的记录
D、创建新的表

38.在关系型数据库中，“ACID”特性中的 D 代表（）。……参考答案：D
A、数据
B、依赖
C、字典
D、持久性

39.下列非关系型数据库适合于处理具有复杂关系的数据的是（）。……参考答案：D
A、键值存储
B、文档存储
C、列存储
D、图形数据库

40.在非关系型数据库中，CAP 定理主要关注（）。……参考答案：A
A、一致性、可用性、分区容错性
B、连接性、可用性、性能
C、安全性、可用性、性能
D、存储、查询、索引

41.在 Microsoft Word 中，用于更改文档的页面方向的选项是（）。……参考答案：B
A、页面布局
B、页面设置
C、页面视图
D、页面边距

42.在 MicrosoftWord 中，“样式”通常用于（）。……参考答案：C
A、插入图片
B、创建目录
C、格式化文本
D、添加脚注

43.在 OA 系统中，通常用于跟踪项目进度的功能是（）。……参考答案：C
A、邮件
B、日历
C、任务管理
D、文件共享

44.电子邮件中，（）是用于确保接收人阅读了邮件。……参考答案：A
A、回执
B、密送
C、抄送
D、优先级

45.攻击方式中（）可以通过数据完整性机制预防。……参考答案：C
A、假冒源地址或用户的地址欺骗攻击
B、数据中途被攻击者窃听获取
C、数据在途中被攻击者篡改或破坏
D、抵赖做过信息的递交行为

46.信息安全的主要目的是为了保证信息的（）。……参考答案：A
A、完整性、机密性、可用性
B、安全性、可用性、机密性
C、完整性、安全性、机密性
D、可用性、传播性、整体性

47.不属于脆弱性范畴的是（）。……参考答案：D
A、操作系统漏洞
B、人员的不良操作习惯
C、应用程序 BUG
D、黑客攻击

48.漏洞扫描扫描出的漏洞往往存在一定的误报，这往往是由漏扫的原理决定的，关于漏扫的原理描述正确的是（）。……参考答案：B
A、通过探测版本信息识别具体版本号，对比该版本存在相关漏洞，这种方法误报率较低
B、通过构造特定的检测数据包，例如 poc&exp，这种方式误报率较低
C、不安全的配置扫描误报率较高，因此不需要进行扫描
D、漏扫设备可以检测的 web 漏洞包括 sql 注入、xss、逻辑漏洞等

49.客户有一台很老而且不经常使用的服务器上存在一个低危的 csrf 漏洞，可以建议客户选择的风险处置方式是（ ）。……参考答案：D
A、风险转嫁
B、风险规避
C、风险降低
D、风险接受

50.风险的特性不包括（）。……参考答案：B
A、不确定性
B、偶然性
C、可识别性
D、可控性

51.某用户新采购入侵防御系统，用于阻止常见的网络袭击，这种风险管理策略类型是（）。……参考答案：C
A、风险接受
B、风险规避
C、风险降低
D、风险转移

52.业务连续性计划可以包括以下（）。……参考答案：C
A、利用备份磁带恢复数据
B、执行 RAID
C、切换到冷站点
D、重启业务操作

53.下列防病毒软件的实施策略在内部公司网络中最有效的是（）。……参考答案：C
A、部署防毒墙
B、开启主机自带的防病毒软件
C、定期更新病毒库
D、配置访问控制策略

54.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（）。……参考答案：B
A、防病毒软件
B、入侵防御系统
C、SSLVPN
D、个人防火墙

55.以下身份验证因素中能和密码一同使用，从而实现多因素身份验证机制的是（）。……参考答案：B
A、用户名
B、个人识别码
C、安全问题
D、指纹扫描

56.下列方法最能够满足双因子认证需求的是（）。……参考答案：D
A、用户名和口令
B、虹膜扫描和指纹扫描
C、磁卡和用户 PIN

D、智能卡和用户 PIN

57.在评估逻辑访问控制时，应该首先做的是（）。……参考答案：A
A、对信息流程的安全风险进行了解
B、把应用在潜在访问路径上的控制项记录下来
C、在访问路径上测试控制来检测是否他们具功能化
D、按照写明的策略和实践评估安全环境

58. 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（）。 ……参考答案：D
A、规定人员的职责
B、为每个员工提供专门的数字证书
C、所有应用均使用 TLS 加密
D、制定明确的访问控制和身份鉴别措施

59.可用于等级测评的测评技术不包含（）。……参考答案：D
A、检查技术
B、识别和分析技术
C、漏洞验证技术
D、协助安全加固技术

60.针对等保测评中高风险项的说法正确的有（）。……参考答案：A
A、凡是存在高风险项，测评结论一律为差；
B、高风险项不能通过补偿措施进行削弱，从而降低风险等级；
C、存在高风险项，测评结论也可以是良；
D、等保测评结论跟高风险项没有直接关系；

61.进行测试之前，（）评估能为审计人员提供系统架构的详细知识。……参考答案：A
A、白盒测试
B、灰盒测试
C、黑盒测试
D、零知识测试

62.为了向使用公司服务的客户提供安全评估信息，（）可以确保最多的客户对评估信息满意。……参考答案：B
A、使用公司内部审计团队根据内部指标进行自我评估
B、使用第三方审计
C、了解系统的内部技术人员进行评估
D、使用内部审计团队根据 COBIT 等通用标准进行自我评估。

63.在信息安全管理体系的实施过程中，管理者的作用对于信息安全管理体系能否成功 实施非常重要，但是以下选项中不属于管理者应有职责的是（）。……参考答案：D
A、制定并颁布信息安全方针，为组织的信息安全管理体系建设指明方向并提供总体纲领，明确总体要求

B、确保组织的信息安全管理体系目标和相应的计划得以制定，目标应明确、 可度量，计划应具体、可实施
C、向组织传达满足信息安全的重要性，传达满足信息安全要求、达成信息安 全目标、符合信息安全方针、履行法律责任和持续改进的重要性
D、建立健全信息安全制度，明确安全风险管理作用，实施信息安全风险评估 过程，确保信息安全风险评估技术选择合理、计算正确

64.小张在学习信息安全管理体系相关知识之后，对于建立信息安全管理体系，自己总结了下面四条要求，其中理解不正确的是（）。……参考答案：A
A、信息安全管理体系的建立应基于最新的信息安全技术，因为这是国家有关信息安全的法律和法规方面的要求，这体现以预防控制为主的思想
B、信息安全管理体系的建立应参照国际国内有关标准实施，因为这些标准是标准化组织在总结研究了很多实际的或潜在的问题后，制定的能共同的和重复使用的规则
C、信息安全管理体系应强调全过程和动态控制的思想，因为安全问题是动态的，系统所处的安全环境也不会一成不变的，不可能建设永远安全的系统
D、信息安全管理体系应体现科学性和全面性的特点，因为要对信息安全管理设计的方方面面实施较为均衡的管理，避免遗漏某些方面而导致组织的整体信息安全水平过低

65.小王的老板告诉他，他将接替公司现任的安全经理。老板向他解释说，尚未实施标准方式的安全措施，因此有些系统具有适当的安全配置，有些则没有。他的老板要了解系统配置错误的风险有多大，以及在这种情况下应该做的内容，以下（）最能描述小王需要为确保操作人员配置的标准化而创建的内容。……参考答案：D
A、双重控制
B、冗余
C、培训
D、基线

66.即使已经被证明有效，因为（）组织还需要定期测试灾难恢复和业务连续性计划。……参考答案：A
A、环境变化可能使得它们随着时间的推移变得无效
B、对测试人员的能力缺乏信心
C、安抚高层领导
D、各种资源可能无法在将来再次测试时使用

67.以下（）最能体现 27002 管理控制措施中预防控制措施的目的。……参考答案：D
A、减少威胁的可能性
B、保护企业的弱点区域
C、减少灾难发生的可能性
D、防御风险的发生并降低其影响

68.以下（）不是可以用来保护系统和应用程序免受攻击的基本预防措施。……参考答案：D
A、维护所有操作系统当前的补丁级别
B、部署入侵检测和预防系统
C、删除不必要的帐户和服务。

D、对所有系统进行取证成像。

69.下列（）是决定数据分级时最重要的标准。……参考答案：A
A、数据泄露可能造成的损害程度
B、数据意外或恶意披露的可能性
C、组织不在其管辖范围内运营的监管要求
D、实施数据控制的成本

70.数据分级分类可按照数据特性进行分类，（）不属于数据特性。……参考答案：C
A、数据价值
B、敏感程度
C、数据量大小
D、影响程度

71.移动状态（动态 In Motion）数据通常（）。……参考答案：C
A、存储在硬盘中
B、存储在寄存器中
C、通过网络传输
D、存储在外部存储设备中

72.静止状态数据通常（）。……参考答案：D
A、使用 RESTful 协议进行传输
B、存储在寄存器中
C、通过网络传输
D、存储在外部存储设备中

73.在信息生命周期的（）阶段，密码学是一种有效的控制手段。……参考答案：D
A、使用
B、归档
C、废弃
D、以上都是

74.在进行应用系统的测试时，应尽可能避免使用包含个人稳私和其它敏感信息的实际生产系统中的数据，如果需要使用时，以下（）不是必须做的。……参考答案：B
A、测试系统应使用不低于生产系统的访问控制措施
B、为测试系统中的数据部署完善的备份与恢复措施
C、在测试完成后立即清除测试系统中的所有敏感数据
D、部署审计措施，记录生产数据的拷贝和使用

75.以下人员中，（）负有决定信息分类级别的责任。……参考答案：B
A、用户
B、数据所有者
C、审计员
D、安全员

76.用于处理数据的信息系统具有（）数据角色。……参考答案：C
A、数据所有者
B、任务所有者
C、数据处理者
D、保管者

77.SM3 算法于（）成为 ISO/IEC 国际标准。……参考答案：D
A、2012 年
B、2016 年
C、2017 年
D、2018 年

78.1949 年，“信息论之父”（）发表的《保密系统的通信理论》学术论文标志着现代密码学的真正开始。……参考答案：D
A、图灵
B、布尔
C、迪菲
D、香农

79.在 SM4 算法中，可以并行处理多组消息分组的工作模式是（）。……参考答案：A
A、ECB
B、CBC
C、OFB
D、CFB

80.ZUC-128 算法是一个面向字的序列密码，密钥长度和初始向量的长度都为（）。……参考答案：B
A、64 比特
B、128 比特
C、256 比特
D、1024 比特

81.SM2 算法与 RSA 算法相比，下列（）不属于 SM2 算法的优势。……参考答案：C
A、安全性高
B、密钥短
C、私钥产生复杂
D、签名速度快

82.SM2 算法于（）转化为国家标准。……参考答案：B
A、2012 年
B、2016 年
C、2017 年
D、2018 年

83.密码杂凑函数可以分为带密钥的杂凑函数和不带密钥的杂凑函数两大类，属于带密钥的杂凑函数的是（）。……参考答案：C
A、MD5
B、MAC
C、HMAC
D、SHA1

84.密码杂凑函数的功能不包括（）。……参考答案：D
A、不能逆向执行
B、提供了消息的完整性
C、单向哈希的结果是报文杂凑值
D、提供了消息的保密性

85.IPSec VPN 的 ISAKMP 分为两个阶段，其中第一阶段主模式实现的功能为（）。……参考答案：A
A、实现通信双方身份的鉴别和密钥交 换，得到工作密钥
B、实现通信双方身份的鉴别和 IPSec SA 的协商
C、实现通信双方 IPSecSA 的协商
D、实现通信双方身份的鉴别、密钥的交换以及 IPSec SA 的协商

86.根据 GM/T0024《SSLVPN 技术规范》，SSLVPN 协议中 IBC 和 IBSDH 的算法为（）。……参考答案：D
A、RSA
B、SM1
C、SM2
D、SM9

87.以下（）格式描述了证书请求语法。……参考答案：D
A、PKCS#7
B、PKCS#8
C、PKCS#9
D、PKCS#10

88.我国 PKI 系统目前采用双证书体系，关于 PKI 双证书说法正确的是（）。参考答案：C
A、签名密钥对和加密密钥对均可进行归档保存
B、签名证书密钥由密钥管理中心 KMC 生成，签名证书由 CA 签发
C、签名密钥对由用户自己生成，加密密钥对由 KMC 生成，签名证书和加密证书由 CA 签发
D、PKI 双证书中签名密钥对和加密密钥对均由用户自己生成后，CA 签发签名证书和加密证书

89.实体鉴别过程中，如果采用时间值或序号，则单向鉴别和相互鉴别和相互鉴别分别需要（）次消息传递。……参考答案：C

A、1 和 3
B、2 和 3
C、1 和 2
D、2 和 2

90.实体鉴别过程中，如果采用使用随机数的“挑战一响应”方法，相互鉴别需要（）次消息传递。……参考答案：D
A、2
B、3
C、4
D、3 或 4

91.著名的 Diffie-Hellman 密钥交换协议是在（）年提出的。……参考答案：A
A、1976
B、1977
C、1978
D、1979

92.SM9 密钥交换协议使通信双方通过对方的标识和自身的私钥经（）信息传递过程，计算获取一个由双方共同决定的共享秘密密钥。……参考答案：D
A、一次
B、二次
C、三次
D、两次或三次

93.以下密钥导出方式不安全的是（）。……参考答案：D
A、利用对称加密技术对密钥进行加密后导出
B、利用非对称加
密技术对密钥进行加密后导出
C、利用门限算法进行拆分后导出
D、将密钥截取为若干段的方式导出

94.以下关于密钥存储描述错误的是（）。……参考答案：B
A、密钥可存储在密码产品中，密码产品中的密钥一般采取分层次的方式，逐层进行保护
B、密钥可存储在密码产品中，对于顶层的密钥加密密钥，需在密码产品中密文存储
C、若密钥数量较大，可将密钥加密后而将密钥存储在通用存储设备或系统（如数据库）中
D、将密钥以密文的形式存储在数据库中，需要利用密码算法对密钥进行必要的保密性和完整性保护

95.商用密码产品认证型式试验结束后将进入（）阶段。……参考答案：B
A、认证评价与决定
B、初始工厂检查
C、获证后监督
D、认证委托

96.商用密码产品认证证书有效期是（）年。……参考答案：C
A、3
B、4
C、5
D、6

97.依据 GM/T 0034《基于 SM2 密码算法的证书认证系统密码及其相关安全技术规范》，以下关于密钥库的说法不正确的是（ ）。……参考答案：B
A、历史库存放过期或已被注销的密钥对
B、CA 申请的密钥从在用库中取出
C、分为备用库、在用库和历史库
D、密钥库中的密钥数据应加密存放

98.以下关于 RA 的说法不正确的是（）。……参考答案：D
A、受理用户证书申请
B、对用户证书申请进行形式审查
C、证书数据验证
D、进行签发证书

99.根据 GM/T 0104《云服务器密码机技术规范》，云服务器密码机中宿主机的日志不包括（）。……参考答案：C
A、宿主机登录认证、系统配置等管理员操作行为
B、虚拟密码机的创建、启动、关闭、删除、漂移等操作或事件及其结果
C、虚拟密码机管理员操作行为，包括登录认证、系统配置、密钥管理等操作
D、接受云平台管理系统的相应管理命令及操作

100.根据 GM/T0030《服务器密码机技术规范》，服务器密码机必须支持的算法工作模式包括（）。……参考答案：B
A、ECB、OFB
B、ECB、CBC
C、ECB、OFB
D、CBC、CFB

101.根据 GM/T 0029《签名验签服务器技术规范》， 下列说法错误的是（）。……参考答案：C
A、应用实体的证书更新时必须保存原来的证书
B、签名验签服务器应支持备份/恢复功能
C、签名验签服务器可以不支持 CRL 连接配置功能
D、签名验签服务器能够配置时间源服务器，自动同步时间

102.根据 GM/T0060《签名验签服务器检测规范》，签名验签服务器必须支持的算法工作模式不包括（）。……参考答案：C
A、ECB

B、CBC
C、CFB
D、OFB

103.根据 GM/T 0023《IPSec VPN 网关产品规范》，IPSec VPN 网关产品的工作密钥最大更新周期不大于（）。……参考答案：C
A、6h
B、12h
C、24h
D、36h

104.根据 GM/T0025《SSLVPN 网关产品规范》，SSL 网关产品管理员使用错误口令或非法身份登录的次数限制应不超过（）。……参考答案：C
A、3
B、5
C、8
D、10

105.根据 GM/T 0027《智能密码钥匙技术规范》中要求，智能密码钥匙支持的 APDU 命令应符合（）要求。……参考答案：B
A、GM/T 0016
B、GM/T 0017
C、GM/T 0018
D、GM/T 0019

106.根据 GM/T0021《动态口令密码应用技术规范》中要求，种子密钥的长度不少于（）比特。……参考答案：C
A、64
B、96
C、128
D、256

107.基于 SM1/SM4 算法的非接触式 CPU 卡方案中，门禁后台管理系统使用（）生成门禁系统根密钥。……参考答案：C
A、应用系统密码模块
B、密钥管理子系统密码设备
C、门禁读卡器密码模块
D、门禁卡密码模块

108.基于 SM7 的非接触逻辑加密卡门禁系统方案中使用()算法实现密钥分散。……参考答案：
A、SM1
B、SM3
C、SM4

D、SM7

109.通过（）技术保障电子印章的完整性、不可伪造性。……参考答案：C
A、PKI 技术
B、图像处理技术
C、数字签名
D、组件技术

110.电子印章系统中（）具有签署和管理电子印章信息权限。……参考答案：D
A、签章人
B、管理员
C、最终用户
D、制章人

111.使用（）密码技术来保证数据原发行为的不可否认性和数据接收行为的不可否认性。……参考答案：C
A、基于对称密码算法等
B、基于公钥密码算法的加解密机制等
C、基于公钥密码算法的数学签名机制等
D、基于非对称密码的原理等

112.使用密码技术的（）实现机密性。……参考答案：B
A、数字签名功能
B、加解密功能
C、密码协议
D、签名验签

113.密码应用安全评估要求中信息系统密码应用第一到第五级通用要求描述不正确的是（）。……参考答案：D
A、信息系统中使用的密码算法应符合法律、法规的规定和密码相关国家标准、行业标准的有关要求。
B、信息系统中使用的密码技术应遵循密码相关国家标准和行业标准。
C、信息系统中使用的密码产品、密码服务应符合法律法规的相关要求。
D、信息系统中使用的通用硬件产品应符合国家相关部门检测认证

114.密码应用安全评估要求中关于管理制度描述不正确的是（）。……参考答案：A
A、一级系统中应具备密码应用安全管理制度,包括密码人员管理、密钥管理、建设运行、应急处置、密码软硬件及介质管理等制度。
B、二级系统中应对管理人员或操作人员执行的日常管理操作建立操作规程。
C、三级系统中应根据密码应用方案建立相应密钥管理规则。
D、四级系统中应定期对密码应用安全管理制度和操作规程的合理性和适用性进行论证和审定，对存在不足或需要改进之处进行修订。

115.编写密码应用方案时，GB/T 39786 中有（）的指标项,信息系统责任方自行决定是否采用密码技术保护指标涉及的保护对象,若决定不采用密码技术保护指标涉及的保护对象,指标项可为“不适用”。……参考答案：A
A、可
B、宜
C、应
D、一

116.编写密码应用方案时，GB/T39786 中有（）的指标项，信息系统采用替代性风险控制措施满足风险控制需求,指标项可为“不适用”。……参考答案：B
A、可
B、宜
C、应
D、一

117.劳动合同可以约定试用期。试用期最长不得超过（）。……参考答案：B
A、三个月
B、六个月
C、九个月
D、十二个月

118.《中华人民共和国劳动法》制定的目的不包括（）。……参考答案：A
A、保护企业的合法权益
B、调整劳动关系
C、建立和维护适应社会主义市场经济的劳动制度
D、促进经济发展和社会进步

119.《中华人民共和国劳动合同法》自（）起施行。……参考答案：A
A、2013 年 7 月 1 日
B、2013 年 8 月 1 日
C、2013 年 9 月 1 日
D、2013 年 10 月 1 日

120.用人单位自用工之日起超过一个月不满一年未与劳动者订立书面劳动合同的，应当向劳动者支付（）的工资。……参考答案：C
A、除每月工资外，再追加二个月的工资
B、除每月工资外，再追加一个月的工资
C、每月二倍
D、除每月工资外，依照法规向劳动者支付赔偿

121.《中华人民共和国密码法》施行的时间为（）。……参考答案：D
A、2020 年 1 月 1 日
B、2019 年 1 月 1 日
C、2021 年 1 月 1 日

D、2020 年 10 月 1 日

122.商用密码用于保护（）的信息。……参考答案：D
A、属于商业秘密
B、属于商业秘密和工作秘密
C、属于商业秘密和个人秘密
D、不属于国家秘密

123.以下有关《中华人民共和国电子签名法》的说法，正确的是（）。……参考答案：B
A、电子签名人可以依照有关规定转让或转借电子签名制作数据。
B、电子签名人应当妥善保管电子签名制作数据
C、电子签名与手写签名或者盖章不具有同等的法律效力
D、电子签名制作数据用于电子签名时，属于第三方认证机构所有

124.《中华人民共和国电子签名法》于（）年施行，最近的一次修正是在（）年。……参考答案：C
A、2005；2015
B、2015；2019
C、2005；2019
D、2009；2015

125.国家建立和完善（）标准体系。国务院标准化行政主管部门和国务院其他有关部门根据各自的职责，组织制定并适时修订有关网络安全管理以及网络产品、服务和运行安全的国家标准、行业标准。……参考答案：B
A、数据安全
B、网络安全
C、信息安全
D、系统安全

126.我们国家实行下列的（）制度。……参考答案：C
A、网络等级
B、网络保护
C、网络安全等级保护
D、网络安全

127.涉密信息系统不得与国际互联网或者其他公共信息网络连接，必须实行（）。……参考答案：B
A、防火墙隔离
B、物理隔离
C、逻辑隔离
D、外部隔离

128.（）主管全国的保密工作。……参考答案：D
A、国家安全部门

B、公安部门
C、中央保密委员会
D、国家保密行政管理部门

129.国家数据安全工作协调机制统筹协调有关部门制定（）。……参考答案：D
A、机构数据目录
B、关键数据目录
C、要害数据目录
D、重要数据目录

130.我们国家建立数据（）制度。……参考答案：B
A、安全
B、分级分类保护
C、分类分级
D、保护

131.根据《中华人民共和国个人信息保护法》，个人信息处理者因业务等需要，确需向中华人民共和国境外提供个人信息的，应当通过（ ）组织的安全评估。……参考答案：A
A、国家网信部门
B、国家公安部门
C、社区
D、市、县政府

132.根据《中华人民共和国个人信息保护法》，为了保护（），规范个人信息处理活动，促进个人信息合理利用，根据宪法，制定本法。……参考答案：D
A、个人数据安全
B、企业机构信息安全
C、个人信息权益
D、个人信息安全

133.根据《商用密码管理条例》，商用密码可以保护的范畴为（ ）。……参考答案：D
A、绝密级以下（含绝密级）的国家秘密
B、机密级以下（含机密级）的国家秘密
C、密级以下（含秘密级）的国家秘密
D、不属于国家秘密的信息

134.根据《密码法》，关于商用密码的使用，下列说法错误的是（）。……参考答案：B
A、公民可以使用商用密码保护个人信息
B、关键信息基础设施运营者只能使用商用密码保护国家秘密
C、重要数据处理者可以使用商用密码保护重要数据
D、企业可以使用商用密码保护商业秘密

135.根据 GB/T 39786《信息安全技术 信息系统密码应用基本要求》，对于密码应用第三级信息系统所采用的密码产品，以下说法正确的是（ ）。……参考答案：B

A、应达到 GB/T 37092 三级及以上安全级别
B、应达到 GB/T 37092 二级及以上安全级别
C、应达到 GB/T 37092 二级及以下安全级别
D、无需具有商密认证证书

136.根据 GB/T39786《信息安全技术信息系统密码应用基本要求》，对于密码应用第三级信息系统，远程管理设备时，（）采用密码技术保证远程管理通道安全。……参考答案：A
A、应
B、宜
C、可
D、必

137.信息系统密码应用需求调研主要方法为（）。……参考答案：A
A、问卷调查
B、访谈
C、实地考察
D、配置检查

138.信息系统密码应用规划阶段包括（）、密码应用设计分析、安全与合规性分析。……参考答案：D
A、密码应用需求分析
B、信息系统现状分析
C、安全风险分析
D、密码应用管理情况分析

139.信息系统密码应用需求用户调研问卷中通过调研（）， 确定信息系统密码应用安全要求等级。……参考答案：C
A、行业政策文件要求
B、数据安全等级
C、网络安全保护等级
D、风险评估等级

140.信息系统密码应用需求用户调研问卷中识别信息系统的信息资产，是通过调查信息系统处理的信息资产，识别需要保护的（）。……参考答案：A
A、重要信息资源和重要数据
B、业务系统
C、数据库
D、操作系统

141.信息系统密码应用需求调研方案编制和实施方是（）。……参考答案：B
A、信息系统责任单位
B、密码应用服务机构
C、商用密码应用安全性评估机构
D、密码供应商

142.信息系统密码应用需求调研最终目标是（）。……参考答案：D
A、梳理信息系统现状
B、安全风险分析
C、收集承载业务情况
D、分析并明确密码应用需求

143.信息系统现状分析活动输出为（）。……参考答案：A
A、密码应用方案中系统概述章节
B、密码应用方案中密码应用需求分析章节
C、密码应用方案中设计目标及原则章节
D、密码应用方案中密码应用技术方案章节

144.以下不属于信息系统密码应用现状分析的是（）。……参考答案：D
A、识别信息系统总体信息
B、识别信息系统的管理情况
C、识别信息系统的信息资产
D、识别安全风险等级

145.对于新建且无拟定等级的重要信息系统，其密码应用等级至少应遵循 GB/T 39786 第（）级密码应用基本要求。……参考答案：C
A、一
B、二
C、三
D、四

146.测信息系统密码应用等级定级依据标准为（）。……参考答案：B
A、GB/T39786 信息安全技术信息系统密码应用基本要求
B、GB/T22240 信息安全技术网络安全等级保护定级指南
C、GB/T37092 信息安全技术密块安全要求
D、GB/T22239 信息安全技术网络安全等级保护基本要求

147.信息系统密码相关安全风险分析活动输出为（）。……参考答案：B
A、密码应用方案中系统概述章节
B、密码应用方案中密码应用需求分析章节的安全风险分析部分
C、密码应用方案中密码应用需求分析章节
D、密码应用方案中设计目标及原则章节

148.信息系统面临的密码相关安全风险分析参考标准为（）。……参考答案：B
A、GB/T39786 信息安全技术信息系统密码应用基本要求
B、GB/T20984 信息安全技术信息安全风险评估规范
C、GB/T37092 信息安全技术密块安全要求
D、GB/T22239 信息安全技术网络安全等级保护基本要求

149.密码应用基本需求的确定活动输出为（）。……参考答案：C
A、密码应用方案中系统概述章节
B、密码应用方案中密码应用需求分析章节
C、密码应用方案中密码应用需求分析章节的密码应用基本需求部分
D、密码应用方案中密码应用需求分析章节的密码应用特殊需求部分

150.密码应用基本需求的确定依据标准为（）。……参考答案：A
A、GB/T39786 信息安全技术信息系统密码应用基本要求
B、GB/T20984 信息安全技术信息安全风险评估规范
C、GB/T37092 信息安全技术密块安全要求
D、GB/T22239 信息安全技术网络安全等级保护基本要求

151.信息系统所属行业密码应用合规性特殊需求属于 GB/T 39786 中相关要求（）的密码应用要求。……参考答案：D
A、高于
B、等于
C、未包含
D、未包含或高于

152.密码应用特殊需求的确定活动输出为（）。……参考答案：D
A、密码应用方案中系统概述章节
B、密码应用方案中密码应用需求分析章节
C、密码应用方案中密码应用需求分析章节的密码应用基本需求部分
D、密码应用方案中密码应用需求分析章节的密码应用特殊需求部分

153.密码应用等级第二级信息系统采用的密码产品应采用达到 GB/T 37092（）安全要求。……参考答案：B
A、一级
B、一级及以上
C、二级
D、二级及以上

154.密码应用等级第三级信息系统采用的密码产品应采用达到 GB/T37092（）安全要求。……参考答案：D
A、一级
B、一级及以上
C、二级
D、二级及以上

155.信息系统密码应用需求调研报告编制属于（）。……参考答案：D
A、信息系统现状分析
B、安全风险分析
C、密码应用需求确定
D、需求分析文档化

156.信息系统密码应用需求分析文档化的输出物是（）。……参考答案：A
A、密码应用方案中系统概述章节
B、密码应用方案中密码应用需求分析章节
C、密码应用方案中设计目标及原则章节
D、密码应用方案中密码应用技术方案章节

157.（）不属于商用密码产品认证目录中的产品种类。……参考答案：B
A、密码键盘
B、视频监控系统
C、安全门禁系统
D、智能 IC 卡

158.商用密码产品认证目录第一批和第二批共有（）种产品种类。……参考答案：D
A、22
B、24
C、26
D、28

159.商密产品认证证书上（）信息是唯一。……参考答案：A
A、证书编号
B、产品名称
C、委托人名称
D、签发时间

160.三级信息系统要求采用的密码产品应达到 GB/T37092（）安全要求。……参考答案：D
A、三级
B、三级及以上
C、二级
D、二级及以上

161.（）是物理环境需要提供的保障条件。……参考答案：D
A、机房
B、监控
C、门禁
D、以上都是

162.物理和环境的对象不包括（）。……参考答案：C
A、物理访问的身份鉴别
B、电子门禁记录数据
C、机房巡检记录
D、视频监控记录数据

163.跨网络边界的系统之间的交互，如果通信主体不在其责任范围之内，例如，被测系统与外部系统通过前置机建立通信信道，前置机部署在被测系统内不归属于被测系统责任单位，此通信信道（）测评范围。……参考答案：A
A、需要
B、不需要
C、不适用
D、需判定具体情况

164.依据商用密码应用安全性量化评估规则（2023 版），网络与通信安全层面权重为（）。……参考答案：B
A、10
B、20
C、15
D、30

165.设备与计算的方案设计当中还需要考虑（）。……参考答案：D
A、路由器
B、交换机
C、防火墙
D、堡垒机

166.在密码系统应用中，设备与计算的对象是（）。……参考答案：D
A、终端设备
B、移动设备
C、嵌入式设备
D、密码设备

167.依据 GB/T43207-2023《信息安全技术信息系统密码应用设计指南》，（）不属于密码支撑平台设计内容。……参考答案：D
A、密码服务机构的确定、接入方式和服务策略
B、支持的密码体制和密码算法
C、接口和功能遵循的标准
D、租户需保护的数据类型

168.在 GM/T0011《可信计算可信密码支撑平台功能与接口规范》中，可信计算密码支撑平台以（）为可信根。……参考答案：A
A、可信密码模块
B、可信存储
C、可信度量
D、可信报告

169.应用与数据的方案设计需要考虑（）关键指标。……参考答案：A
A、可落地性
B、简单性

C、可审查性
D、可靠性

170.应用与数据的对象梳理应满足（）原则。……参考答案：A
A、全面性
B、简单性
C、易改造性
D、先进性

171.在信息系统密码应用框架中，用户端使用的计算机设备安全，属于()安全。……参考答案：A
A、计算平台
B、应用安全
C、支撑平台
D、管理平台

172.在信息系统密码应用框架中，用户计算机上运行的业务系统客户端安全，属于（）安全。……参考答案：B
A、计算平台
B、应用安全
C、支撑平台
D、管理平台

173.在信息系统密码应用框架中，租户承担着所属业务应用及其相应的（）。……参考答案：B
A、数据管理职责
B、密钥管理职责
C、安全管理职责
D、制度管理职责

174.云上应用系统所处的云平台的安全级别应（）云上应用系统。……参考答案：A
A、高于
B、低于
C、等于
D、以系统重要性决定

175.针对云平台自身密码应用的测评，该部分测评的责任主体为（）。……参考答案：B
A、云平台租户
B、云平台的运营者
C、云平台的使用者
D、云上应用的用户

176.信息系统的密码应用方案按照逻辑上责任主体的不同,分成（）个部分分别设计。……参考答案：B

A、二
B、三
C、四
D、五

177.在项目执行阶段，客户要求增加一项新功能，项目经理首先响应最合适的方法是（）。……参考答案：B
A、立即开始实施新功能
B、评估新功能对范围、进度和成本的影响
C、拒绝客户的要求
D、更新项目计划以包含新功能

178.关于项目范围管理的主要目的，描述最适合的一项是（）。……参考答案：C
A、确保项目按时完成
B、控制项目成本
C、确保项目满足预定的需求和期望
D、确保项目团队成员满意

179.根据 GB/T 43207 《信息安全技术 信息系统密码应用设计指南》，信息系统密码应用的设计应遵循（）。……参考答案：C
A、安全性原则
B、便捷性原则
C、合规性原则
D、创新性原则

180.在制定项目计划时，通常发生在最后的活动是（）。……参考答案：D
A、识别干系人
B、定义项目范围
C、制定项目时间表
D、获得项目批准

181.项目计划最主要的作用是（）。……参考答案：A
A、指导项目执行
B、控制项目成本
C、预测项目风险
D、确保项目质量

182.根据 GB/T 43207《信息安全技术 信息系统密码应用设计指南》,物理和环境安全层面密码应用方案设计时需要考虑（）。……参考答案：B
A、电子门禁记录数据的存储机密性
B、视频监控记录数据的存储完整性
C、审计数据的存储机密性
D、审计数据的存储完整性

183.在项目实施过程中，确保项目按照计划进行的活动是（）。……参考答案：B
A、项目启动
B、项目监控
C、项目收尾
D、项目变更控制

184.在项目实施阶段，项目经理的主要职责是（）。……参考答案：C
A、确保项目范围不变
B、制定项目计划
C、监督和控制项目的执行
D、管理项目风险

185.根据 GB/T 43207《信息安全技术 信息系统密码应用设计指南》，密码支撑平台为承载在计算平台上的各类业务应用提供密码功能服务，不可依据以下需求进行自行设计（）。……参考答案：D
A、业务应用的密码需求
B、性能需求
C、责任主体的规划要求
D、人员名单

186.在项目实施团队中，负责协调团队成员之间的沟通和协作的角色是（）。……参考答案：A
A、项目经理
B、技术负责人
C、财务经理
D、行政助理

187.在项目团队组织管理中，项目经理的首要职责是（）。……参考答案：A
A、确保项目按时完成
B、监督团队成员的个人工作
C、管理项目预算
D、维护团队士气

188.根据 GB/T 39786《信息安全技术 信息系统密码应用基本要求》、GB/T 43207《信息安全技术 信息系统密码应用设计指南》，信息系统用户通过智能密码钥匙,基于挑战响应的方式登录业务系统，属于（）层面设计的内容。……参考答案：B
A、设备和计算安全
B、业务和应用安全
C、网络和通信安全
D、物理和环境安全

189.在项目成本管理中，用于监控项目成本绩效，确定实际成本与计划成本之间的偏差的工具或技术是（）。……参考答案：D
A、成本估算

B、成本预算
C、成本控制
D、成本偏差分析

190.一般情况下，项目成本管理中，制定项目成本估算时，考虑的因素不包括（）。……参考答案：B
A、项目范围
B、团队成员个人喜好
C、项目规模
D、项目风险

191.

192.在项目变更管理中，用于确定变更对项目影响的过程是（）。……参考答案：B
A、变更识别
B、变更评估
C、变更控制
D、变更实施

193.在项目变更管理中，不是变更请求的典型来源不包含（）。……参考答案：A
A、项目经理
B、行业监管方
C、客户
D、利益相关者

194.形式审核中的内容完整性审核对象是（）。……参考答案：C
A、密码建设文本
B、技术方案
C、方案文本
D、密码项目材料

195.在项目质量管控中，用于识别质量问题根本原因的工具和技术是（）。…参考答案：D
A、质量审计
B、检查表
C、帕累托图
D、因果图

196.在项目质量管控中，质量计划的最核心内容是（）。……参考答案：A
A、质量标准
B、质量控制过程
C、质量保证过程
D、质量改进过程

197.形式审核中的内容一致性审核对象是（）。……参考答案：D

A、调研材料
B、密评报告
C、技术方案
D、方案文本

198.在项目风险识别中，（）方法不是用于识别风险。……参考答案：D
A、文档审查
B、历史信息分析
C、 因果图
D、质量审计

199.在项目风险识别中，（）不是定性风险分析的工具。……参考答案：A
A、概率和影响矩阵
B、情景分析
C、SWOT 分析
D、威胁树分析

200.形式审核中的文本规范性审核对象是（）。……参考答案：D
A、调研材料
B、密评报告
C、密码建设文本
D、方案文本

201.风险处置策略中，涉及避免风险的一项是（）。……参考答案：C
A、风险转移
B、风险减轻
C、风险规避
D、 风险接受

202.在信息系统项目风险处置流程中，首先进行的一项活动是（）。……参考答案：A
A、风险识别
B、风险分析
C、风险应对计划制定
D、风险监控

203.应制定实施保障方案，包含以下内容：（）、实施技术保障、项目质量保障、和项目经费保障。……参考答案：D
A、时间计划保障
B、应急处置保障
C、实施质量保障
D、人员组织保障

204.在制定信息系统项目风险应对措施时，下列非必须考虑的因素是（）。…参考答案：C
A、风险的紧迫性

B、 措施的成本效益
C、项目团队成员的个人喜好
D、 组织的风险承受能力

205.在信息系统项目中，对于已经识别的高概率且影响严重的风险，项目经理首先应该考虑的应对措施是（）。……参考答案：C
A、风险规避
B、风险转移
C、风险减轻
D、风险接受

206.本次实施密评活动人员中至少（）名通过密评人员考试的成绩证明扫描件。……参考答案：B
A、1
B、2
C、3
D、4

207.密码应用现状审核不包含（）。……参考答案：B
A、对象审核
B、形式审核
C、实施审核
D、结果判定

208.密码应用现状需审核的对象没有（）。……参考答案：C
A、系统网络拓扑图
B、系统承载业务
C、硬件设备
D、系统信息种类、关键数据类型

209.网络和通信安全层面的保护对象类型主要不包含（）。……参考答案：D
A、客户端与服务端
B、网络
C、服务端与服务端
D、人员

210.针对密码应用需求及控制措施的描述，以下说法不正确的是（）。……参考答案：C
A、合规性自查表应准确描述相关安全控制措施
B、各安全层面的所有保护对象安全控制措施应无遗漏
C、针对不适用的指标，不需要补充安全控制措施
D、密码产品应按安全控制措施合理部署

211.实施保障方案中，实施内容主要不包含（）。……参考答案：C
A、描述实施对象的边界及密码应用的范围、任务要求等

B、包括但不限于采购、软硬件开发或改造、系统集成、综合调试和试运行等
C、包括实施的计划开销和任务成本核算等
D、分析项目实施的重难点问题,提出实施过程中可能存在的风险点及应对措施

212.合规性审查意见不应综合考虑以下（ ）要素。……参考答案：C
A、法律法规
B、行业标准
C、企业文化
D、社会责任

213.信息系统密码应用的访谈调查通常包括以下的（）参与者。……参考答案：C
A、系统管理员和安全专家
B、开发人员和测试人员
C、最终用户和系统管理员
D、高级管理人员和股东

214.在信息系统密码应用的评估中，采用访谈方式进行用户调研时，可以获得以下类型中的（）信息。……参考答案：A
A、用户对密码安全的理解和意识
B、系统的硬件配置
C、加密算法的详细技术细节
D、网络连接速度

215.通过文档审查，可以检查下列选项中里信息系统密码应用中的（）方面。……参考答案：B
A、用户登录次数
B、密码加密算法
C、用户的地理位置
D、硬件配置

216.文档审查在信息系统密码应用安全性测评中的作用是（）。……参考答案：C
A、直接测试系统的漏洞
B、确定系统的性能指标
C、评估密码策略和安全措施的合规性
D、分析网络流量

217.信息系统密码应用测评准备活动的信息收集和分析任务中，以下（）选项不是文档审查的重点。……参考答案：D
A、调查表格填写不正确的
B、调查表格填写不完善的
C、调查表格存在相互矛盾的
D、未填写调查表格的

218.通过实地查看，可以检查信息系统密码应用中的（）方面。……参考答案：D

A、用户密码复杂度
B、系统的加密算法
C、服务器的存储容量
D、安全摄像头的部署情况

219.实地查看在信息系统密码应用安全性测评中的作用是（）。……参考答案：C
A、检查系统硬件配置
B、确定系统的网络速度
C、评估物理安全措施和访问控制
D、分析系统日志

220.信息系统密码应用测评过程中，以下（）选项任务最有可能用到实地查看。……参考答案：A
A、信息收集和分析
B、测评内容确定
C、结果确认和资料归还
D、单元测评

221.通过配置检查，可以检查信息系统密码应用中的（）方面。……参考答案：B
A、用户登录时间
B、操作系统补丁情况
C、用户密码长度
D、网络带宽利用率

222.配置检查在信息系统密码应用安全性测评中的作用是（）。……参考答案：C
A、确定系统的硬件配置
B、评估系统的性能
C、检查系统的软件版本和安全配置
D、分析用户密码复杂性

223.信息系统密码应用测评过程中，以下（）选项任务最有可能用到配置检查。……参考答案：C
A、项目启动
B、测评内容确定
C、现场测评和结果记录
D、单元测评

224.在信息系统密码应用安全性测评中，统计方法主要用于。……参考答案：B
A、分析用户登录时间
B、收集和分析安全事件的数据
C、测试系统的性能
D、检查系统的加密算法

225.系统概述记录对信息系统密码应用安全性测评的重要性体现在（）。……参考答案：B

A、分析用户的密码习惯
B、提供系统的硬件和软件配置信息
C、检查网络流量
D、评估系统的性能指标

226.信息系统网络拓扑图主要用于。……参考答案：B
A、分析用户密码复杂性
B、显示系统中各个组件之间的连接关系
C、记录用户登录时间
D、分析网络流量

227.服务器密码机在安装时，首要考虑的安全要素是（）。……参考答案：A
A、密码机的物理位置
B、密码机的网络连接
C、密码机的电源保障
D、密码机的管理员权限设置

228.在安装服务器密码机时，以下不是必要的措施是（）。……参考答案：B
A、 确保密码机与服务器之间的通信加密
B、将密码机放置在无尘环境中
C、为密码机配置独立的 UPS 电源
D、使用高强度密码并定期更换

229.根据 GM/T 0116《信息系统密码应用测评过程指南》，系统资产调研是在测评活动准备的（ ）阶段。……参考答案：B
A、项目启动
B、信息收集和分析
C、工具和表单准备
D、密评方案编制

230.签名验签服务器在安装时，对于管理员的身份验证，以下最安全的方式是（）。……参考答案：D
A、仅使用用户名和密码
B、使用智能密码钥匙
C、使用智能 IC 卡
D、结合智能密码钥匙、智能 IC 卡与登录口令

231.在签名验签服务器安装过程中，不是必须功能的是（）。……参考答案：B
A、设备自检功能
B、远程无线控制功能
C、安全存储敏感信息的功能
D、在检查不通过时的报警和停止工作的功能

232.

233.服务端（）由外部导入 SSL VPN 网关产品。……参考答案：D
A、主密钥
B、预主密钥
C、签名密钥对
D、加密密钥对

234.服务端（）由 SSLVPN 网关产品自身产生。……参考答案：A
A、签名密钥对
B、加密密钥对
C、签名证书
D、加密证书

235.在密码服务中，（）的方法主要用于验证用户身份。……参考答案：C
A、散列函数
B、加密算法
C、身份验证协议
D、数字签名

236.属于证书认证密钥管理系统的防火墙的主要安全策略是（）。……参考答案：B
A、及时更新病毒库
B、关闭所有系统不需要的端口
C、密码机应是经国家密码管理主管部门审批的产品
D、设置超级管理员,该管理员由本系统初始化时产生,负责系统的策略管理

237.证书认证密钥管理系统的 KM 与 CA 连接，正确的方式是（）。……参考答案：D
A、KM 与 CA 处于同一局域网内，直接连接
B、KM 与 CA 处于同一局域网内，应通过网络密码机与 CA 连接
C、KM 与 CA 不处于同一局域网内，直接连接
D、KM 与 CA 不处于同一局域网内，应通过网络密码机与 CA 连接

238.根据 GM/T 0116《信息系统密码应用测评过程指南》，测评准备活动不包含下列的（）一项。……参考答案：D
A、项目启动
B、被测系统资产信息收集和分析
C、各种与被测系统相关的技术资料调查
D、测评对象确定

239.使用蓝牙接口的蓝牙智能密码钥匙，在 android 手机安装时，需要开通的服务是（）。……参考答案：A
A、定位服务
B、打印服务
C、内容服务
D、手机网络服务

240.使用蓝牙接口的蓝牙智能密码钥匙，在 android 手机安装时，需要开通的权限是（）。……参考答案：B
A、通信录权限
B、位置权限
C、电话权限
D、媒体权限

241.信息系统密码应用调研问卷中不包含（ ）。……参考答案：D
A、被测信息系统基本信息表
B、被测信息系统网络拓扑图和系统概述
C、被测信息系统密码应用情况
D、被测信息系统负责人是否具备密码技术应用员资质

242.在信息系统密码应用调研问卷中，（ ）不在调研范围内。……参考答案：D
A、密码产品
B、物理环境
C、网络设备及安全设备
D、办公设备

243.信息系统密码应用情况应从（）等层面描述密码应用的工作流程。……参考答案：A
A、物理和环境、网络和通信、设备和计算
B、办公和环境、网络和通信、应用和数据
C、办公和环境、设备和计算、应用和数据
D、办公和环境、网络和通信、设备和计算

244.以下选项中，只有（ ）是密码服务的调研对象。……参考答案：A
A、电子政务电子认证服务
B、商用密码应用安全性评估服务
C、数据加密服务
D、统一密码服务管理平台

245.在信息系统密码应用调研问卷中一般不会获取到（ ）信息。……参考答案：A
A、网络通信数据抓包报文
B、密码产品信息
C、密码服务信息
D、被测信息系统安全相关的人员情况

246.在密码应用安全性评估的项目实施会议中，启动会的主要作用是（ ）。……参考答案：A
A、确定评估的范围和目标
B、分配评估任务和资源
C、总结评估过程和结果
D、安排结束会的时间和地点

247.对同一段明文 abc 进行签名，SM2、RSA1024、RSA2048 三种签名算法测试签名时，最适合的测试方法是（）。……参考答案：A
A、等价值划分
B、边界值分析
C、错误推测
D、随机策略

248.以下关于密码系统的加解密功能测试描述，正确描述是（）。……参考答案：B
A、加密后的密文用对应密钥解密，解密出的明文包含原文内容即测试通过
B、加密后的密文用对应密钥解密，解密出的明文与原文完全一致即测试通过
C、加密后的密文用对应密钥解密，解密出的明文与原文部分一致即测试通过
D、加密后的密文用对应密钥解密，解密出的明文与原文不一定完全一致

249.关于安全通信网络中的网络设备，下列说法错误的是（）。……参考答案：A
A、一般来说，业务高峰期主要的网络设备的 CPU、内存的使用率不宜超过 90%
B、应核查网络设备是否从未出现过因设备性能问题导致的宕机情况
C、为了保证主要网络设备具有足够的处理能力，建议定期检查设备的资源占用情况，确保设备的业务处理能力具有冗余空间
D、应根据实际情况和区域安全防护要求，在主要网络设备上进行 VLAN 划分

250.签名验签服务器的性能测试，不正确的做法是（）。……参考答案：C
A、测试应进行多次,结果取平均值。
B、必须测试所支持的所有密码算法及其各种应用模式。
C、测试应进行多轮, 每轮的测试次数可以选定为 100 次。
D、进行并发性能测试时，必须配置连接数

251.签名验签服务器，数字签名的性能单位为（）。……参考答案：A
A、次/秒
B、秒/次
C、兆比特每秒
D、字节每秒

252.在密码应用安全性评估中，（ ）用于明确评估团队和被评估方之间的责任与权利。……参考答案：B
A、现场测评风险揭示书
B、授权书
C、资料交接单
D、评估报告

253.在物理和环境测评过程中，了解到机房部署国密安全门禁系统，并采用智能 IC 卡识别的方式进行物理访问人员的身份鉴别，测评人员使用监控软件（如 Bus Hound）对智能 IC 卡的（）进行抓取和分析（条件允许时），确认调用指令格式和内容符合预期。……参考答案：D

A、USB 请求
B、AT 指令
C、SCSI 指令
D、APDU 指令

254.物理和环境测评单元包括（）、电子门禁记录数据存储完整性和视频监控记录数据存储完整性。……参考答案：A
A、身份鉴别
B、通信数据完整性
C、通信过程中重要数据的机密性
D、网络边界访问控制信息的完整性

255.使用 SSL 测试工具模拟多个客户端，并发与 SSL VPN 网关建立 SSL 会话并断开，可以测试 SSL VPN 网关的（）。……参考答案：C
A、最大用户数
B、最大连接数
C、每秒新建连接数
D、吞吐率

256.进行 SSLVPN 网关客户端-服务端模式密文测试时，可以发送（）报文。……参考答案：A
A、TCP
B、UDP
C、ICMP
D、ARP

257.针对网络和通信中身份鉴别的测评，下面（）选项的描述适用于等保定级的第三级。……参考答案：C
A、可采用密码技术对通信实体进行身份鉴别，保证通信实体身份的真实性
B、宜采用密码技术对通信实体进行身份鉴别，保证通信实体身份的真实性
C、应采用密码技术对通信实体进行身份鉴别，保证通信实体身份的真实性
D、应采用密码技术对通信实体进行双向身份鉴别，保证通信实体身份的真实性

258.对证书认证密钥管理系统进行系统初始化检测，不需要做的操作是（）。……参考答案：D
A、进行密钥管理系统初始化操作
B、产生审计管理员
C、产生超级管理员
D、产生业务管理员

259.对证书认证密钥管理系统进行网络检测，不需要做的操作是（）。……参考答案：C
A、查阅漏洞扫描记录
B、查阅病毒防治日志
C、查阅安全管理策略和制度

D、查看密码机连接方式

260.

261.系统测试报告的阅读对象是（）。……参考答案：B
A、对系统感兴趣的任意人员
B、授权阅读的项目干系人
C、测试主管
D、研发主管

262.系统测试报告在测试过程中起到了多重作用，它总结了测试活动和结果，评估了（）。……参考答案：D
A、测试覆盖的质量
B、测试过程的质量
C、系统研发的质量
D、系统的质量

263.在应用和数据安全的测评过程中，针对身份鉴别测评单元，系统使用 PKI 技术对用户进行身份鉴别，具体来说是系统用户使用智能密码钥匙+数字证书发起登录请求，系统通过签名验签服务器进行响应，采用 SM2、SM3 算法基于()密码算法的数字签名机制实现用户身份鉴别。……参考答案：A
A、公钥
B、对称
C、杂凑
D、HMAC

264.测试用例的设计依据是（）。……参考答案：B
A、项目计划
B、需求说明
C、详细设计
D、测试报告

265.不属于系统测试用例设计要素的选项是（）。……参考答案：D
A、用例标题
B、测试输入
C、预期结果
D、实测结果

266.密码应用安全性评估中，现场测评的核心目的是（ ）。……参考答案：B
A、测试密码算法的强度
B、验证密码系统的合规性、正确性和有用性
C、检查密码设备的物理安全
D、了解密码系统的日常操作流程

267.在密码应用联调测试中，用于验证密码系统数据防篡改能力的测试类型是（）。……参考答案：B
A、数据加密测试
B、数据完整性测试
C、认证和授权测试
D、安全协议测试

268.在密码应用联调测试中，联调测试的主要目标不包含（）。……参考答案：C
A、验证组件之间的通信是否正常
B、发现并解决组件集成时可能出现的问题
C、进行用户培训
D、验证系统的整体性能和稳定性

269.根据 GM/T 0116《信息系统密码应用测评过程指南》，以下关于密评工作中结果确认和资料归还部分描述不正确的是（ ）。……参考答案：C
A、密评人员在现场测评完成后，应首先汇总现场测评的测评记录，对遗漏和需要进一步验证的内容实施补充测评
B、召开测评现场结束会，对测评过程中得到各类测评结果记录进行现场沟通和确认
C、现场测评活动结束后，可以保留现场测评材料至评估报告编写完成
D、归还测评过程中借阅的所有文档资料，将测评现场环境恢复至测评前状态

270.在密码系统测试缺陷报告中，缺陷"关闭状态"的正确描述是（）。……参考答案：A
A、缺陷已被验证通过
B、开发人员已将缺陷解决
C、开发人员不认可的缺陷
D、短期无法解决的缺陷

271.缺陷报告最重要的信息是（）。……参考答案：C
A、缺陷产生原因
B、缺陷解决方案
C、缺陷描述
D、缺陷报告的编写者姓名

272.根据 GM/T 0116《信息系统密码应用测评过程指南》，以下（）选项不属于现场测评活动的输出文档。……参考答案：D
A、更新确认的密评方案
B、各类测评结果记录
C、签署过的测评授权书
D、项目计划书

273.针对密码应用岗位责任制度的访谈，对等保定级为第三级和第四级的系统，测评指标均要求“应建立密码应用岗位责任制度，明确各岗位在安全系统中的职责和权限”，两者的区别在于（）。……参考答案：D

A、根据密码应用的实际情况，设置密钥管理员、密码安全审计员、密码操作员等关键安全岗位
B、对关键岗位建立多人共管机制
C、密钥管理、密码安全审计、密码操作人员职责互相制约互相监督，其中密码安全审计员岗位不可与密钥管理员、密码操作员兼任
D、密钥管理员、密码安全审计员、密码操作员应由本机构的内部员工担任，并应在任前对其进行背景调查

274.针对操作规程的访谈，测评指标为：应定期对密码应用安全管理制度和操作规程的合理性和适用性进行论证和审定，对存在不足或需要改进之处进行修订。该指标适用于（）到第四级。……参考答案：C
A、第一级
B、第二级
C、第三级
D、第四级

275.随机数检测工具主要对信息系统中用于密码运算的随机数或（）的随机性进行检测。……参考答案：B
A、明文数据
B、密文数据
C、密钥
D、密钥密文

276.在 SSL 握手过程中，以下用于协商加密参数和生成预主密钥的是（）。…参考答案：C
A、客户端问候
B、服务器证书
C、客户端密钥交换
D、服务器确认

277.网络架构是业务运行所需的重要部分，以下不属于网络架构中的要求的是（）。……参考答案：D
A、应保证网络设备的业务处理能力满足业务高峰期需要
B、应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址
C、应提供通信线路、关键网络设备和关键计算设备的硬件冗余，保证系统的可用性
D、应采用校验技术或密码技术保证通信过程中数据的完整性

278.在测评网络和通信安全层面时，如果通信过程采用 SSL 协议提供保护，现场抓包，通常查看握手协议的（ ）消息，来获取密码套件属性值，进而判定具体使用的密码算法。……参考答案：B
A、Client Hello
B、Server Hello
C、Server Hello Done
D、Server Key Exchange

279.某应用系统采用统一身份认证进行单点登录时，统一身份认证基于静态口令和手机验证码组合的方式进行身份鉴别，则在应用和数据安全层面“身份鉴别”指标进行测评时，最合适的判定结果为（ ）。……参考答案：C
A、符合
B、部分符合
C、不符合
D、不适用

280.某信息系统的网络和通信安全层面测评对象包括 IPSec VPN 通信信道和 SSL VPN 通信信道。经测评后发现，针对“通信数据保密性”测评单元，IPSec VPN 通信信道符合要求，SSL VPN 通信信道部分符合要求。那么该信息系统在网络和通信安全层面“通信数据保密性”测评单元的最终判定结果为（ ）。……参考答案：B
A、符合
B、部分符合
C、不符合
D、不适用

281.试运行团队组建成员，承担密码设备的服务配置、网络是否正常的角色是以下哪一个。……参考答案：B
A、项目承建单位
B、运维人员
C、试运行工作人员
D、系统管理员

282.试运行团队组建成员，承担系统使用的界面友好性、时间响应效果、功能是否完整的角色是以下的（）。……参考答案：C
A、项目承建单位
B、运维人员
C、试运行工作人员
D、系统管理员

283.试运行结束阶段，输出产出物一般是以下哪一个。……参考答案：B
A、需求说明书
B、试运行报告
C、实施方案
D、合同或协议

284.以下工作成果，哪个属于试运行实施阶段的产物。……参考答案：B
A、需求说明书
B、用户体验测试
C、试运行报告
D、变更说明书

285.根据项目的特点和风险评估结果，建立关键的（），这些指标应能够反映项目运行的安全状态，如系统稳定性、资源利用率、异常事件数量等。……参考答案：B
A、功能指标
B、安全监控指标
C、性能指标
D、密码服务指标

286.项目试运行阶段的安全状态监控管理至关重要，在项目试运行之前，应制定详细的（）。……参考答案：A
A、安全监控计划
B、需求说明书
C、试运行报告
D、变更说明书

287.在一个密码应用类项目，试运行阶段用户提出电子回执数量太多采用手动电子盖章操作比较繁琐，提出变更为服务端自动盖章的密码应用，团队成员经过初步分析判断此变更技术上可以实现，但可能会有新的风险隐患，请问接下来如何操作。……参考答案：B
A、直接更新风险登记册，评估影响
B、与团队分析变更对项目的影响
C、同意变更功能，提升客户满意度，并验证可行性
D、提交变更请求，进行综合分析

288.在密码系统试运行期间，成立一个由项目关键干系人组成的（），负责审批变更请求，确保所有变更都得到适当的管理和批准。……参考答案：B
A、项目团队
B、变更控制委员会
C、实施团队
D、售后服务团队

289.在密码系统试运行过程中，出现异常情况时，最应该优先处理的措施是()。……参考答案：B
A、调整系统配置
B、停止试运行并通知相关部门
C、寻找技术解决方案
D、继续试运行并加强监控

290.试运行过程中，密码系统出现问题时，应急响应过程应重点关注的内容是（）。……参考答案：C
A、人员操作情况
B、设备运行情况
C、系统的稳定性
D、项目进度

291.在密码系统试运行阶段，密码系统试运行报告的主要目的是（）。……参考答案：C

A、撰写用户操作手册
B、测试系统稳定性和数据安全
C、总结系统性能和稳定性以及改进意见
D、确保系统安全

292.在密码系统试运行阶段，下列应包含在密码系统试运行报告中的内容是（）。……参考答案：B
A、操作手册
B、系统问题和改进建议
C、功能和性能测试文档
D、概要设计文档

293.在密码系统的试运行报告中，对数据环境的要求是（）。……参考答案：D
A、数据存储技术
B、数据处理流程描述
C、数据访问权限设定
D、以上都是

294.在试运行阶段，试运行环境中对系统的稳定性影响最大的因素是（）。…参考答案：C
A、网络延迟时间
B、数据存储过程
C、系统资源占用
D、软件兼容性

295.密码系统试运行报告中，记录的每个问题均应具备唯一标识，其作用是（）。……参考答案：C
A、描述问题
B、辅助技术分析
C、追踪问题
D、评估问题严重性

296.在问题记录中，提供截图或日志文件的主要目的是（）。……参考答案：B
A、美化报告文档
B、辅助技术分析问题
C、增加报告详细性
D、指定问题的责任人

297.密码应用在实施阶段，风险评估的目的是（）。……参考答案：D
A、根据系统建设目标和安全需求,对系统的安全功能进行验收测试;评价安全措施能否抵御安全威胁
B、根据系统建设目标和安全需求,对系统的安全功能进行评价，其安全措施能否抵御安全威胁
C、根据系统安全需求和运行环境对系统开发、实施过程进行风险识别,并对设计方案中所提供的安全功能符合性进行判断。

D、根据系统安全需求和运行环境对系统开发、实施过程进行风险识别,并对系统建成后的安全功能进行验证

298.关于密码应用在交付实施过程的风险评估要点，描述错误的是（）。……参考答案：A
A、根据系统建设目标和安全需求，详细分析资产面临的威胁和脆弱性
B、根据系统建设目标和安全需求，对系统的安全功能进行验收测试;评价安全措施能否抵御安全威胁
C、评估是否建立了与整体安全策略一致的组织管理制度
D、对系统实现的风险控制效果与预期设计的符合性进行判断

299.试运行阶段，密码系统试运行报告的总结部分最应该强调的内容是（）。……参考答案：B
A、相关密码产品的优点和市场价值
B、系统在试运行期间的表现及改进空间
C、软件环境的安装部署情况
D、密码保障系统的硬件配置

300.在密码系统试运行报告中，为了提高系统服务水平，建议的措施是（）。……参考答案：D
A、提高数据处理能力
B、升级产品版本或优化性能
C、对关键功能进行全面测试以确保稳定性和可用性
D、以上都是

301.GB/T 43207《信息安全技术 信息系统密码应用设计指南》中提到的密码应用设计过程包括（）阶段。……参考答案：A
A、密码应用需求分析
B、设计方案制定
C、方案实施
D、测试与评估

302.根据 GB/T43207《信息安全技术信息系统密码应用设计指南》，信息系统密码应用的设计应遵循（）。……参考答案：C
A、安全性原则
B、便捷性原则
C、合规性原则
D、创新性原则

303.密码资产软件管理制度中给出了软件资产的示例，以下不属于软件资产的是（　）。……参考答案：D
A、操作系统
B、应用软件
C、数据库
D、工作人员

304.根据 GB/T 39786《信息安全技术 信息系统密码应用基本要求》、GB/T 43207《信息安全技术 信息系统密码应用设计指南》，运维管理员通过智能密码钥匙登录密码产品，属于（）层面的设计内容。……参考答案：A
A、设备和计算安全
B、业务和应用安全
C、网络和通信安全
D、物理和环境安全

305.网络和通信安全密码应用方案设计时，以下描述错误的是（）。……参考答案：B
A、网络和通信安全保护的对象是信息系统与外界交互的通信信道
B、对需要密码保护的重要通信信道进行密码应用设计
C、设计需要考虑选择的密码技术和标准、采用的密码设备、密码设备的部署位置和方式、密码设备的使用和管理等内容
D、需要接入认证的设备，根据具体情况选择使用的密码技术，确定在设备端和认证端部署的密码设备和部署位置，给出密码设备的使用和管理内容

306.密码硬件资源应有统一标识进行区分与管理，标识不应包含（　　）。……参考答案：D
A、设备的型号
B、配置信息
C、位置信息
D、工作安排

307.根据 GB/T 43207《信息安全技术 信息系统密码应用设计指南》，基于经认证合格的密码产品进行密码支撑平台设计时，需要明确（）。……参考答案：D
A、部署的位置和方式
B、接入计算平台的方式
C、密钥管理方式
D、以上都是

308.基于经认证合格的密码产品进行密码支撑平台设计时，设计的内容不包含（）。……参考答案：D
A、密码服务机构的确定、接入方式和服务策略
B、支持的密码体制和密码算法
C、提供的密码功能及接口
D、密码设备选型

309.最不符合介质管理的有（　　）。……参考答案：B
A、建立针对移动存储介质的安全管理制度
B、将密码介质内容删除后可以回收用于其他系统
C、应建立对存储介质申请、使用、更换、维修及报废的管理制度
D、对可重复利用的介质应执行写操作以覆盖旧内容并确保不可恢复

310.根据 GB/T 43207《信息安全技术 信息系统密码应用设计指南》,业务应用的密码应用方案设计时，下列关于密钥管理策略设计的描述错误的是（）。……参考答案：B
A、明确各类型密钥存储的位置和方式，如密钥在符合 GB/T 37092 的密码产品中存储，或者在对密钥进行机密性和完整性保护后，存储在通用设备或系统中
B、密钥不以明文方式存储在密码产品外部并采取严格的安全防护措施，防止密钥被非授权的访问
C、明确各类型密钥的使用要求并按要求使用密钥，包括使用条件、时间和用途等
D、每个密钥一般只有单一的用途

311.根据 GB/T39786《信息安全技术信息系统密码应用基本要求》、GB/T43207《信息安全技术信息系统密码应用设计指南》，信息系统用户通过智能密码钥匙,基于挑战响应的方式登录业务系统，属于（）层面设计的内容。……参考答案：B
A、设备和计算安全
B、业务和应用安全
C、网络和通信安全
D、物理和环境安全

312.信息系统网络拓扑图的制作对于评估系统的安全性的贡献在于（）。……参考答案：B
A、分析用户密码复杂性
B、显示系统中各个组件之间的连接方式
C、记录用户的登录历史
D、评估系统的性能指标

313.在密码应用方案设计时，（）应用等级的信息系统，在可能涉及法律责任认定的应用中,宜采用密码技术提供数据原发证据和数据接收证据,实现数据原发行为的不可否认性和数据接收行为的不可否认性。……参考答案：C
A、第一级
B、第二级
C、第三级
D、第四级

314.以下关于对称加密的说法，不正确的是（）。 ……参考答案：A
A、算法是一组规则，规定如何进行加密和解密。因此对称式加密本身是安全的
B、采用单钥密码系统的加密方法，同一个密钥可以同时用作信息的加密和解密
C、算法是一组规则，规定如何进行加密和解密。因此对称式加密本身是不安全的
D、常用的对称加密有：DES,3DES,AES,RC4,RC5,IDEA 算法等

315.密码资产变更管理规范规定了变更流程，包括（　　）、评审、批准和实施环节。……参考答案：A
A、变更申请
B、开始
C、结束
D、启动

316.以下哪项不是内容完整性需要核对的内容。……参考答案：D
A、背景
B、技术方案
C、安全管理
D、调研材料

317.应用方案内容完整性审核对象是（）。……参考答案：A
A、方案文本
B、密评报告
C、技术方案
D、文本

318.密码资产研发过程管理不包括（　）。……参考答案：D
A、对整个过程有明确的阶段划分和过程管理
B、具备变更管理规范并对变更进行管控
C、应建立技术文档管理规范并对技术性文档进行保存
D、运行记录并存档管理

319.审核内容一致性时，需要针对审核对象审核（）条内容。……参考答案：B
A、5
B、6
C、7
D、8

320.应用方案内容一致性审核对象是（）。……参考答案：D
A、调研材料
B、密评报告
C、技术方案
D、方案文本

321.配置检查通常涉及检查以下（）选项内容。……参考答案：C
A、网络流量分析
B、密码加密算法
C、操作系统和应用程序的安全配置
D、用户登录记录

322.审核文本规范性时，需要针对审核对象审核几（）条内容。……参考答案：A
A、3
B、4
C、5
D、6

323.应用方案文本规范性审核对象是（）。……参考答案：C
A、调研材料

B、密评报告
C、方案文本
D、设计方案

324.密码资产使用过程中，（　　）不应作为日志记录。……参考答案：D
A、用户活动
B、意外和安全事件
C、系统管理员的活动
D、设备性能

325.参照信息系统密码应用方案编制指引时，需要针对安全管理方案审核几条内容。……参考答案：A
A、4
B、5
C、6
D、7

326.应制定实施保障方案，包含以下内容：人员组织保障、实施技术保障、项目质量保障、和（）。……参考答案：A
A、项目经费保障
B、应急处置保障
C、实施质量保障
D、时间计划保障

327.实地查看通常包括以下（）选项活动。……参考答案：B
A、对系统进行渗透测试
B、检查服务器的温度和湿度
C、评估用户密码的强度
D、分析网络流量

328.密码应用方案在密码技术应用、（）和安全管理方面均按照相关要求设计。……参考答案：A
A、密钥管理
B、密码使用
C、人员管理
D、密码设计

329.目前选择（）版本的商用密码应用安全性评估报告是当前适用的版本。…参考答案：C
A、2021 版
B、2022 版
C、2023 版
D、2024 版

330.文档审查通常涉及审查以下（）类型的文档。……参考答案：A

A、用户手册和系统日志
B、财务报表和营销计划
C、服务器配置文件和网络拓扑图
D、员工培训资料和人力资源政策

331.根据信息安全的要求，明确系统信息种类，并识别业务、管理、用户等关键数据类型及安全属性的主要目的是（）。……参考答案：C
A、提升系统信息处理的效率
B、改善系统信息的分类管理
C、加强系统信息的安全性
D、促进系统信息的共享与传播

332. 以下关于非对称加密的说法，不正确的是（）。……参考答案：A
A、常用的非对称加密有：ASE,RSA,DH,DSA,ECC 等
B、非对称加密算法需要两个密钥：公开密钥（publickey）和私有密钥（privatekey）
C、常用的非对称加密有：RSA,DH,DSA,ECC 等
D、如果公开密钥对数据进行加密，只有对应的私有密钥才能解密；如果用私有密钥对数据进行加密，那么只有用对应的公开密钥才能解密。

333.关键岗位人员离岗离职后，应及时(　　)其计算机涉密信息系统访问授权。……参考答案：C
A、保留
B、延长
C、取消
D、缩小

334.以下（）不属于密码应用保护对象的评估内容。……参考答案：D
A、密码策略的合理性
B、密码算法的强度
C、密码管理机制的有效性
D、用户界面的友好性

335.物理与环境安全层面的保护对象设计的机房应包含（）。……参考答案：C
A、管辖范围之内的机房
B、管辖范围之外的机房
C、管辖范围之内和管辖范围之外的机房均包含
D、与被测信息系统相关人员进行沟通和确认

336.《网络安全法》规定，网络运营者应当按照网络安全等级保护制度的要求，履行网络安全保护义务，对（　）采取加密措施。……参考答案：C
A、所有数据
B、一般数据
C、重要数据
D、网络日志

337.以下（）不属于密码策略制定时需要考虑的因素。……参考答案：C
A、系统的安全需求
B、业务的风险承受能力
C、用户的操作习惯
D、密码的更新频率

338.以下（）不属于密码应用需求分析的主要内容。……参考答案：A
A、评估密码应用的性能需求
B、确定密码保护的对象和范围
C、评估密码应用的安全威胁和风险
D、制定密码策略和控制措施

339.对于获得国家密码主管部门批准的密码产品，用户在使用该密码产品时应按照(　　)进行使用。……参考答案：A
A、用户手册
B、二次开发
C、裁剪功能
D、工作需求

340.在保障信息安全中，以下（）实施保障措施是关于密码实施的关键环节。……参考答案：C
A、定期更换硬件设备
B、加强员工的信息安全意识培训
C、确保密码策略的有效实施和定期更新
D、随意分享工作密码以方便同事间协作

341.对于密码管理，以下（）实施保障措施不是有效的密码管理实践。……参考答案：C
A、定期对口令进行审计
B、限制用户尝试登录的次数
C、允许用户将自己的口令告诉他人
D、采用多因素认证机制

342.密钥管理制度规定了对密钥的全生命周期管理，密钥生命周期不包括：密钥的生成、(　　)。……参考答案：D
A、密钥分发
B、密钥存储
C、密钥导入和导出
D、密钥使用

343.进行合规性审查时，以下（）不是审查的基本步骤。……参考答案：B
A、收集相关法律法规和标准资料
B、分析密码设备和密码管理的安全性
C、评估密码策略和密码应用的合规性

D、撰写审查报告和审查意见

344.进行合规性审查时，以下（）不是审查的主要内容。……参考答案：C
A、审查密码策略是否符合国家法律法规和标准
B、审查密码设备是否符合国家认证和检测要求
C、审查密码应用是否符合业务需求和安全性要求
D、审查密码管理是否符合组织内部规定和操作流程

345.密钥备份恢复操作是确保密钥备份和恢复操作安全、可靠和合规的重要组成部分，以下（）选项特性最不适合（　　）。……参考答案：C
A、完整性
B、准确性
C、容错性
D、保密性

346.在撰写合规性审查意见时，（）是评估合规性的最核心要素。……参考答案：B
A、企业内部规定
B、法规要求
C、行业最佳实践
D、竞争对手的实践

347.在撰写合规性审查意见时，以下（）不是审查的目的。……参考答案：C
A、评估合规风险
B、提出改进建议
C、评价绩效
D、确认合规性

348.密码系统安全管理的主要目的是(　　)。……参考答案：C
A、提高系统性能
B、方便用户操作
C、确保信息安全
D、降低维护成本

349.在制定实施保障措施时，（）是评估风险的最常用方法。……参考答案：A
A、风险评估矩阵
B、风险评估问卷
C、风险评估软件
D、直觉判断

350.在实施保障措施/方案的过程中，（）是最有效的方法来确保员工的参与和意识。……参考答案：B
A、定期举行会议
B、提供培训和教育
C、制定惩罚措施

D、依靠员工的自我驱动力

351.下列做法不能有效提高密码系统的安全性是(　　)。……参考答案：C
A、使用强密码策略
B、定期更换密码
C、在公共场合公开密码
D、使用多因素认证

352.在使用替代性风险控制措施而不采用密码技术时，应当（）。……参考答案：D
A、忽略风险评估和论证
B、做出相应的说明
C、仅在密码应用方案设计时进行风险评估
D、同时进行风险评估和论证

353.在设计密码应用方案时，为确保关键数据保护的真实性、机密性、完整性、不可否认性，最核心的因素是（）。……参考答案：B
A、密钥管理策略
B、加密算法选择
C、认证机制的强度
D、安全审计的频率

354.根据《信息系统密码应用测评要求》，应对管理人员或操作人员的（　　）建立操作规程。……参考答案：B
A、行为
B、日常管理操作
C、升级操作
D、更新操作

355.以下（）不属于设备与计算安全层面密码应用的保护对象。……参考答案：B
A、通用服务器
B、防火墙
C、密码产品
D、堡垒机

356.以下（）是网络和通信安全层面主要保护的对象。……参考答案：D
A、受保护的网络区域
B、网络访问的权限
C、受保护的系统
D、跨网络访问的通信信道

357.下列不属于安全管理中心的要求的是（）。……参考答案：D
A、应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计

B、应通过审计管理员对审计记录应进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等
C、应对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律法规要求
D、应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等

358.根据《信息系统密码应用基本要求》，应采用密码技术保证重要数据在存储过程中的（　　）,包括但不限于鉴别数据、重要业务数据和重要用户信息等（第三级到第四级）。……参考答案：C
A、完整性
B、安全性
C、机密性
D、真实性

359.根据《信息系统密码应用基本要求》，应使用密码技术的完整性功能来保证电子门禁系统进出记录的（　　）（第三级到第四级）。……参考答案：A
A、完整性
B、安全性
C、机密性
D、真实性

360.根据《信息系统密码应用基本要求》，应使用密码技术对登录的用户进行身份标识和鉴别，以保证应用系统用户身份的（　　）（第三级到第四级）。……参考答案：D
A、正确性
B、可用性
C、安全性
D、真实性

361.根据 GM/T 0116《信息系统密码应用测评过程指南》，在测评准备活动阶段，除收集调查表格外，以下（）资料是测评方不必要收集的。……参考答案：C
A、被测信息系统总体描述文件、被测信息系统密码应用总体描述文件
B、网络安全等级保护定级报告、安全需求分析报告
C、相关密码产品的购买合同及金额、相关密码产品的操作指南
D、安全总体方案、安全详细涉及方案

362.根据 GM/T0116《信息系统密码应用测评过程指南》，当发现调查表格中系统资产不完善时，以下做法不正确的是（）。……参考答案：A
A、密评人员不需要与填表人进行沟通和确认，待正式进场实施后再重新调研、核实
B、密评人员及时与填表人进行沟通和确认
C、必要时，测评方应安排现场调查
D、与被测信息系统相关人员进行沟通和确认

363.根据《信息安全技术 证书认证系统密码及其相关安全技术规范》，为防止非授权人员操作密钥管理系统，在每一个操作终端上应设有操作员身份鉴别系统，对系统的部分重要操作要对有关操作员进行身份鉴别和权限控制，（　　）可以记录在工作日志中系统不做鉴别。……参考答案：D
A、密码应用操作
B、升级操作
C、备份操作
D、非重要操作

364. 以下关于 IDEA 的说法，不正确的是（）。……参考答案：A
A、分组长度为 128 位的分组密码算法
B、分组长度为 64 位的分组密码算法
C、密钥长度为 128 位
D、抗强力攻击能力比 DES 强

365.以下哪项不属于信息系统密码应用情况记录内容（）。……参考答案：D
A、物理和环境安全
B、网络和通信安全
C、应用和数据安全
D、管理制度

366.根据 GMT 0030-2014 《服务器密码机技术规范》，为了确认密码设备是否正常，需要对密码设备进行自检，下列选项中不属于设备自检功能的是（　　）。……参考答案：C
A、密码算法正确性检查
B、随机数发生器检查
C、存储密钥和数据的机密性检查
D、关键部件的正确性检测

367.在密码服务中，哪种统计方法用于分析密码泄露的风险（）。……参考答案：A
A、频率分析
B、相关性分析
C、回归分析
D、生存分析

368.在密码服务中，下列的（）方法主要用于验证用户身份。……参考答案：C
A、散列函数
B、加密算法
C、身份验证协议
D、数字签名

369.为了确认密码软件系统是否可以通过运行在 Windows 主机上的国密浏览器使用 TLCP 协议访问，可以通过 Wireshark 或 tcpdump 抓取数据报文进行分析，以下描述错误的是（）。……参考答案：C

A、可以在安装密码软件系统的服务器上使用 tcpdump 工具抓取数据报文并保存到文件中，然后下载抓包文件并通过 Wireshark 打开进行分析
B、可以在运行国密浏览器的 Windows 系统上使用 Wireshark 直接抓取报文进行分析
C、使用 Wireshark 工具对抓取的报文进行分析时，可以在 Client Key Exchange 数据报文中获取通信双方所协商的密码套件
D、使用 Wireshark 工具对抓取的报文进行分析时，如果找不到与客户端匹配的密码套件，服务端将回应 handshake failure 报警消息

370.根据 GM/T 0116《信息系统密码应用测评过程指南》，以下关于调查表格记录和统计结果的说法，不正确的是（
）。……参考答案：B
A、测评方将被测信息系统基本情况调查表格提交给被测单位，协助并督促被测信息系统相关人员准确填写调查表格
B、测评方只回收填写完的调查表格，不需要对调查表格记录的内容进行分析
C、测评方需要对调查表格内的记录内容进行分析，并确保调查信息的正确性
D、测评方除对调查表格记录进行统计外，还需要统计各种与被测信息系统相关的技术资料

371.根据 GM/T 0116《信息系统密码应用测评过程指南》，测评方对调查表格记录和统计结果汇总的目的表述错误的是（ ）。……参考答案：C
A、了解被测信息系统的构成和密码应用情况
B、为编写密评方案和开展现场测评工作奠定基础
C、只是形式化工作流程
D、测评方可以使用调查表格、查阅被测信息系统资料等方式，对被测信息系统情况进行记录和统计

372.根据 GMT 0030-2014 《服务器密码机技术规范》，对管理工具的描述不正确的是（）。……参考答案：D
A、管理工具必须安装在服务器密码机之外的管理终端上
B、管理工具必须安装在服务器密码机上
C、服务器密码机不可以通过外部管理中心管理
D、服务器密码机可以接受其他管理系统的管理

373.需要重点说明被测信息系统承载的（）。……参考答案：A
A、密码应用需求
B、岗位设计
C、资金需求
D、口令复杂度设计

374.（）不在信息系统密码应用调研问卷范围内。……参考答案：D
A、密码服务
B、被测信息系统网络拓扑图和系统概述
C、被测信息系统密码应用情况
D、被测信息系统负责人是否具备密码技术应用员资质

375.文档审查方式适用于评估信息系统密码应用中的（）方面。……参考答案：C
A、硬件性能
B、软件版本更新
C、密码策略和访问控制
D、网络带宽利用率

376.在系统资产中，不需要调研（）。……参考答案：D
A、密码产品
B、物理环境
C、网络设备及安全设备
D、办公设备

377.物理安防设施中需要调研的对象包括（）。……参考答案：B
A、报警系统
B、电子门禁系统
C、门窗防撬装置
D、围墙和栅栏

378.密码软件系统进行集群部署时，(　　)开源服务程序可以用于设置虚拟 IP，对上层应用提供统一的 IP 地址。……参考答案：C
A、nginx
B、lvs
C、keepalived
D、HAproxy

379.从物理和环境、设备和计算、（　　）、应用和数据等不同层面描述信息系统密码应用的工作流程。……参考答案：C
A、网络设备及安全设备
B、密码产品
C、网络和通信
D、密码服务

380.信息系统密码应用情况可以主要围绕所使用的（）展开介绍。……参考答案：A
A、密码产品
B、网络设备及安全设备
C、数据库服务器
D、关键数据

381.关于服务器密码机密码设备日志管理的要求，下列说法不正确的是（）。……参考答案：B
A、日志管理应包含记录、查看、导出等功能。
B、日志内容应包含管理操作行为、用户访问行为、异常事件等。
C、管理员操作行为包含包括登录认证、系统配置、密钥管理等操作。
D、如与设备管理中心连接，则应对相应操作进行记录。

382.电子认证服务属于（）。……参考答案：C
A、密码产品
B、密码设备
C、密码服务
D、密码系统

383.密码服务的调研对象包括（）。……参考答案：A
A、电子政务电子认证服务
B、统一身份验证平台
C、数据加密服务
D、商用密码应用安全性评估服务

384.对影响信息系统密码应用的关键要素进行分析，确定密码应用安全状态监控的对象，不包含下列（）。……参考答案：C
A、信息系统内所使用的密码产品
B、密码服务中使用的第三方组件
C、信息系统密码应用中使用的硬件设备
D、信息系统密码应用中使用的第三方组件

385.在被测信息系统基本信息表中需要调研的信息包含（ ）。……参考答案：B
A、网络和通信安全密码应用情况
B、网络安全等级保护定级和备案情况
C、被测信息系统安全相关的人员情况
D、关键数据

386.在信息系统密码应用调研问卷中可以获取（）信息。……参考答案：D
A、被测信息系统机房门禁记录
B、被测信息系统网络与通信安全中的网络通信数据抓包报文
C、设备和计算安全中设备身份鉴别实现代码片段
D、应用和数据安全中涉及的关键数据类型

387.针对管理制度发布流程的访谈，采用访谈和文档审查方式，核查密码应用安全管理制度是否有发布流程，是否为发布的正式版，是否有（），是否有发布执行记录。……参考答案：B
A、审查记录
B、版本标识
C、注释
D、关键字标记

388.针对密码应用岗位责任制度的访谈，针对等保定级为第三级的系统，应建立密码应用岗位责任制度，明确各岗位在安全系统中的职责和权限，根据密码应用的实际情况，设置（）、密码安全审计员、密码操作员等关键安全岗位。……参考答案：A
A、密钥管理员

B、系统管理员
C、机房管理员
D、密钥记录员

389.在密码应用安全性评估的项目实施会议中，结束会通常在（ ）进行。……参考答案：C
A、评估工作开始前
B、评估过程中任意时间
C、所有评估工作完成后
D、评估报告发布后

390.在密码应用安全性评估的项目实施会议中，启动会的主要作用是（）。…参考答案：A
A、确定评估的范围和目标
B、分配评估任务和资源
C、总结评估过程和结果
D、安排结束会的时间和地点

391.密码系统运维过程中，技术人员填写的应急处置操作记录中的事件标识的作用
(　　)。……参考答案：B
A、记录事件日期
B、追踪和引用事件
C、显示事件的严重性
D、评估事件影响

392.在密码应用安全性评估过程中，（)主要用于确保被评估方对评估过程中可能存在的风险有充分了解。……参考答案：B
A、评估报告
B、现场测评风险揭示书
C、授权书
D、资料交接单

393.在密码应用安全性评估中，（）用于明确评估团队和被评估方之间的责任与权利。……参考答案：B
A、现场测评风险揭示书
B、授权书
C、资料交接单
D、评估报告

394.安装密码系统管理工具时应遵循什么原则，以确保只有授权人员进行管理操作
(　　)。……参考答案：B
A、最低成本原则
B、最小权限原则
C、最高权限原则
D、最佳性能原则

395.在系统管理工具中，（）类型的工具用于自动化部署和配置系统。……参考答案：A
A、脚本编写工具
B、远程桌面工具
C、网络管理工具
D、故障排除工具

396.在纵向加密认证网关通信信道的场景下，针对网络和通信安全的“通信过程中重要数据的机密性”测评单元，通过查看纵向加密认证网关策略配置，可知通信双方采用加密策略实现通信数据机密性保护，通过查看纵向加密认证网关密码检测报告，通信数据保护采用（）算法，通过对通信过程中的数据包分析，可知通信机密性保护措施有效。……参考答案：A
A、SSF09
B、AES
C、SM1
D、SM3

397.在网络和通信安全的测评过程中，针对身份鉴别测评单元，可能涉及到的测评对象不包括（）。……参考答案：B
A、两个机房之间的通信信道
B、电子政务电子认证服务
C、客户端浏览器与业务应用系统服务端之间的通信信道
D、安全浏览器与被测系统安全认证网关之间的通信信道

398.在网络和通信安全的测评过程中，针对身份鉴别测评单元，可能需要测评的密码产品不包括（）。……参考答案：D
A、IPSec VPN 产品/安全网关
B、SSL VPN 产品/安全网关
C、智能密码钥匙
D、CA 签名算法

399.在 SSL/TLS 通信信道的场景下，针对网络和通信安全的“通信过程中重要数据的机密性”测评单元，测评人员通过对 SSL 协议握手阶段的 ServerHello 消息数据包分析，可知通信双方协定采用 SM4 算法实现通信数据机密性保护，ServerHello 消息数据包中的密码套件为 ECC_SM4_CBC_SM3，套件标识为（）。……参考答案：C
A、0xc030
B、0x1301
C、0xe013
D、0x009d

400.以下（）选项不是密码管理工具的日常运维管理的内容。……参考答案：D
A、定期审计与监控密码库的安全性
B、对用户操作日志进行定期审查
C、定期备份密码库并测试恢复流程
D、安全管理员更新密码管理工具的软件版本和安全补丁

401.在设备和计算安全的测评过程中，针对身份鉴别测评单元，测评人员采用密码协议分析类工具，捕获并分析用户登录各类设备时的通信数据包，分析用户身份鉴别机制是否符合预期；采用密码算法实现（）检测类工具对签名值进行校验，分析基于数字签名技术的身份鉴别机制采用的密码算法是否合规。……参考答案：A
A、正确性
B、挑战-响应值
C、口令
D、随机验证码

402. 以下关于 HASH 散列函数的说法，不正确的是（）。……参考答案：A
A、Hash 函数: h=H(x), 要求可作用于有限尺寸数据且均产生定长输出
B、一种直接产生认证码的方法
C、Hash 函数值可以看成大文件的‘数字指纹’
D、著名的 Hash 函数有 MD2、MD5、SHA 和基于分组密码的构造的等

403.在应用和数据安全的测评过程中，针对身份鉴别测评单元，测评人员发现系统用户使用动态令牌发起登录请求，系统通过动态令牌认证系统进行响应，采用 SM3 算法基于动态口令技术实现用户身份鉴别。其中种子密钥长度不少于（）比特，用于动态口令生成。……参考答案：D
A、1024
B、512
C、256
D、128

404.在应用和数据安全的测评过程中，针对“访问控制信息完整性”的测评单元，测评人员发现系统使用传统密码产品对访问控制信息进行完整性保护，其中用于完整性保护的技术包括（）、签名验签技术。……参考答案：A
A、消息鉴别码技术
B、生物识别技术
C、数字水印技术
D、人工智能技术

405.针对设备和计算安全中身份鉴别的测评，下面（）选项描述适用于等保定级的第三级。……参考答案：C
A、可采用密码技术对登录设备的用户进行身份鉴别，保证用户身份的真实性
B、宜采用密码技术对登录设备的用户进行身份鉴别，保证用户身份的真实性
C、应采用密码技术对登录设备的用户进行身份鉴别，保证用户身份的真实性
D、应采用密码技术对通信实体进行双向身份鉴别，保证通信实体身份的真实性

406.在密码应用安全性评估的现场测评中，（ ）不是必须考虑的因素。……参考答案：C
A、密码管理政策和程序的执行情况
B、密码设备的安全配置
C、密码算法的国际标准
D、 密码系统与其他系统的集成情况

407.密码应用安全性评估中，现场测评的核心目的是（）。……参考答案：B
A、测试密码算法的强度
B、验证密码系统的合规性、正确性和有效性
C、检查密码设备的物理安全
D、了解密码系统的日常操作流程

408.在密码应用安全性评估的结果确认环节，必需的操作项是（ ）。……参考答案：B
A、与被评估方进行口头沟通
B、编写详细的结果确认报告
C、仅依赖评估工具的输出结果
D、 无需任何操作，自动确认结果

409.在密码应用安全性评估过程中，结果确认的主要目的是（）。……参考答案：A
A、验证评估结果的准确性
B、确定评估是否满足所有要求
C、评估密码系统的性能
D、确保所有资料已归还

410.在 GM/T 0116《信息系统密码应用测评过程指南》中，关于现场测评活动的输出文档，描述正确的是（ ）。……参考答案：C
A、输出文档应仅包含技术细节
B、输出文档应简洁明了，不包含任何建议
C、输出文档应详细记录测评过程中发现的所有问题
D、输出文档无需包含对测评结果的解释

411.根据 GM/T0116《信息系统密码应用测评过程指南》，以下（）选项是属于现场测评活动的输出文档。……参考答案：D
A、测评报告
B、测评总结
C、测评工具使用手册
D、测评结果记录

412.在随机数检测中，以下哪个指标用于衡量随机数序列的统计特性是否符合预期（）。……参考答案：D
A、熵
B、频率
C、周期性
D、均匀性

413.IPSec 协议检测工具通常用于以下哪个阶段的安全评估（）。……参考答案：C
A、安全规划
B、安全设计
C、安全实施

D、安全监控

414.在 SSL 握手过程中，以下选项用于协商加密参数和生成预主密钥的是（）。……
参考答案：C
A、客户端问候
B、服务器证书
C、客户端密钥交换
D、服务器确认

415.以下哪个工具不是用于端口扫描的（）。……参考答案：C
A、 Nmap
B、Nessus
C、Wireshark
D、Zmap

416.端口扫描工具可以帮助测评人员分析和判断被测信息系统中 VPN、服务器密码机等设备的（）。……参考答案：B
A、网络拓扑结构
B、开放的端口和服务
C、用户行为分析
D、网络带宽使用情况

417.在测评时发现某信息系统数据库中某数据杂凑长度为 256 比特，则其使用的算法可能为（ ）。……参考答案：B
A、SHA-512
B、SM3
C、MD5
D、SHA-384

418.在测评实施过程中，发现用户虽然使用 HMAC-SM3 对口令数据进行完整性保护，且采用认证合格的智能密码钥匙生成 MAC，但只截取使用 MAC 值的前 8 个比特，那么对应用和数据安全层面的“重要数据存储完整性保护”指标判定时，以下 DAK 判定最为合理的是（）。……参考答案：A
A、√ √ √
B、√ √ ×
C、√ × ×
D、× √ √

419.某应用系统面向业务用户提供 WEB 端和 APP 端 2 种访问方式，在 WEB 端，用户浏览器与应用系统服务端采用国密 SSL 协议（由国密浏览器实现）保障通信数据机密性，APP 客户端与应用系统服务端之间采用 HTTP 协议传输，经核查发现应用系统用户鉴别数据均以明文方式传输，经整体测评后，鉴别数据在应用和数据安全层面“重要数据传输机密性”指标的测评结果最可能为（ ）。……参考答案：C
A、符合

B、部分符合
C、不符合
D、无法判断

420.某网上银行系统在应用和数据安全层面“不可否认性”指标测评时，对象包括用户关键交易操作、与外部系统的关键交易操作。经核查发现，关键交易操作不可否认性实现均采用数字签名技术，且密码产品、密码服务符合 GM/T0115 通用测评要求，部分网银用户仍使用 RSA1024 数字证书，则本单元的测评结果最合适的是（）。……参考答案：B
A、符合
B、部分符合
C、不符合
D、无法判断

421.某信息系统涉及 2 个物理机房。根据密码应用方案和现场测评结果，其中物理机房 A 的物理和环境安全层面“身份鉴别”项测评结果为不适用，物理机房 B 为部分符合。则该系统物理和环境安全层面“身份鉴别”测评单元，最终判定结果为（ ）。……参考答案：B
A、符合
B、部分符合
C、不符合
D、不适用

422.某信息系统所在机房部署了电子门禁系统进行物理访问身份鉴别，经核查发现，电子门禁系统基于指纹对人员进行身份鉴别，则物理和环境安全层面“身份鉴别”测评单元如何判定，风险等级如何变化（）。……参考答案：B
A、符合
B、风险等级降低
C、风险等级不变
D、不适用

423.对于符合 GM/T 0051 的对称密钥产品，在进行司法密钥恢复时，应由注册过的两名（ ）与密钥管理中心具备相应权限的操作人员共同操作。……参考答案：D
A、系统管理员、安全管理员
B、系统审计员、安全管理员
C、司法恢复专职人员、安全管理员
D、系统管理员、系统审计员

424.对于符合 GM/T0034 的 CA 系统，在 CA 中应设置的角色包括：超级管理员和（）。……参考答案：D
A、用户
B、维护员
C、操作员
D、业务管理员

425.机房管理人员对密码资产的管理方式，描述有误的是（ ）。……参考答案：D

A、设备管理软件
B、电子表格记录
C、手写登记
D、以上均不对

426.密码硬件资源应有统一标识进行区分与管理，标识应不包含（）。……参考答案：D
A、设备的型号
B、配置信息
C、位置信息
D、配置效率

427.针对存储介质管理制度、安全策略和生命周期管理，其中不包括（　　）。……参考答案：C
A、申请
B、使用
C、采购
D、报废

428.以下最不符合介质管理的有（）。……参考答案：B
A、建立针对移动存储介质的安全管理制度
B、将密码介质内容删除后可以回收用于其他系统
C、应建立对存储介质申请、使用、更换、维修及报废的管理制度
D、对可重复利用的介质应执行写操作以覆盖旧内容并确保不可恢复

429.在设备和计算安全的测评过程中，针对远程管理通道的测评单元，测评人员通过分析流量数据包，发现系统采用 HTTPS 协议远程管理堡垒机和密码产品，发现 Server Hello 消息数据包中的密码套件为（），套件标识为 0xc030。……参考答案：A
A、TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
B、TLS_AES_128_GCM_SHA256
C、TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
D、TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

430. 以下关于椭圆曲线密码的说法，不正确的是（）。……参考答案：A
A、比 RSA 算法钥慢得多
B、利用椭圆曲线上离散对数代替有限域上离散对数，可以构作公钥位数较小的 ELGamal 类公钥密码
C、基于有限域上椭圆曲线的离散对数计算的困难性
D、较 RSA 更高的安全强度

431.在应用和数据安全的测评过程中，针对身份鉴别测评单元，如果系统用户采用动态令牌发起登录请求，系统通过动态令牌认证系统进行响应，采用 SM3 算法基于动态口令技术实现用户身份鉴别。其中种子密钥长度不少于（）比特，用于动态口令生成。…参考答案：D
A、1024
B、512

C、256
D、128

432.在应用和数据安全的测评过程中，针对“访问控制信息完整性”的测评单元，测评人员发现系统使用传统密码产品对访问控制信息进行完整性保护，其中用于完整性保护的技术包括（）、消息鉴别码技术。……参考答案：A
A、签名验签技术
B、生物识别技术
C、数字水印技术
D、人工智能技术

433.测试服务器密码机 GM/T 0018 签名验签接口前，必须先生成（）。……参考答案：C
A、密钥加密密钥
B、会话密钥
C、签名密钥对
D、加密密钥对

434.测试服务器密码机 GM/T0018 密码运算接口前，必须先调用（）接口。…参考答案：A
A、打开设备和会话
B、关闭设备和会话
C、获取设备信息
D、获取随机数

435.如果被测信息系统重要资产采取多平台部署或部署在不同的机房内，则信息系统机房调查应包括（ ）。……参考答案：A
A、所有被测信息系统涉及的机房
B、仅部署密码设备的机房或平台
C、只包含被测信息系统重要资产的机房
D、主机房和备份机房

436.根据 GM/T0116《信息系统密码应用测评过程指南》，在密码应用安全性评估活动中，系统资产调研是在（）阶段。……参考答案：A
A、测评活动准备
B、方案编制活动
C、现场测评活动
D、分析与报告编制活动

437.信息系统信息种类的审核定义需基于（）明确。……参考答案：D
A、不同的的用户类别
B、应用系统完备的业务流程
C、信息系统单位的安全管理制度
D、识别业务、管理、用户等关键数据类型及安全属性

438.密码应用现状中针对网络拓扑，最核心审核要点为（）。……参考答案：B

A、体现完整网络设备
B、系统网络边界划分清晰
C、业务场景清晰
D、逻辑架构得体

439.根据《密码法》，密码工作坚持（　），遵循统一领导、分级负责，创新发展、服务大局，依法管理、保障安全的原则。……参考答案：A
A、总体国家安全观
B、整体国家安全观
C、综合国家安全观
D、安全发展观

440.根据《密码法》和《网络安全法》，某黑客为炫耀技术能力，非法侵入他人的密码保障系统并受到治安管理处罚，则公安机关能够对其进行的行政处罚包括（ ）。……参考答案：D
A、使其终身不得从事网络运营关键岗位
B、使其二十年内不得从事网络运营关键岗位
C、使其十年内不得从事网络运营关键岗位
D、使其五年内不得从事网络运营关键岗位

441.关于密码系统测试报告总结中软件的兼容性说明，描述错误的是（）。…参考答案：D
A、软件与不同硬件设备的兼容性
B、软件与其他软件共存的能力
C、软件能否正确处理不同来源的数据
D、软件的吞吐量

442.密码系统测试报告总结中对软件质量进行总体评价，通常不需要包含（）。……参考答案：C
A、软件的功能性
B、软件的可靠性
C、软件的缺陷详情
D、软件的兼容性

443.根据 GM/T 0116《信息系统密码应用测评过程指南》，测评准备活动不包含下列哪一项（ ）。……参考答案：C
A、项目启动
B、软硬件重要性及部署情况调查
C、测评对象确定
D、系统资产调查与记录全面

444.根据 GM/T0116《信息系统密码应用测评过程指南》，以下选项（）不是在调查表格中收集的内容。……参考答案：B
A、业务流程
B、密码管理策略

C、项目概述
D、行业特征

445.密钥备份机制是确保密钥安全的重要组成部分之一，它包括一系列策略和技术，其中最不符合项（　）。……参考答案：A
A、安全扫描
B、定期备份策略
C、完整性验证
D、加密备份数据

446.密钥备份恢复操作是确保密钥备份和恢复操作安全、可靠和合规的重要组成部分，以下选项中特性最不适合的是（）。……参考答案：C
A、完整性
B、准确性
C、容错性
D、保密性

447.对于符合 GM/T 0051 的对称密钥产品，在进行司法密钥恢复时，应由注册过的（　）与密钥管理中心具备相应权限的操作人员共同操作。……参考答案：C
A、系统管理员
B、系统审计员
C、司法恢复专职人员
D、安全管理员

448.对于符合 GM/T0034 的 CA 系统，在 CA 中应设置的角色包括：审计管理员和（）。……参考答案：D
A、用户
B、维护员
C、操作员
D、审计员

449.当密码系统出现故障时，应由(　)负责故障排查和恢复。……参考答案：B
A、密码审计员
B、密码操作员
C、系统管理员
D、安全管理员

450.在密码系统岗位责任制度中，（）主要负责密码策略的制定和审查。……参考答案：A
A、密码管理员
B、密码操作员
C、密码审计员
D、密码策略制定员

451.在对应用和数据安全中的“重要数据存储完整性”指标测评时，采用以下（ ）密码技术无法被判定为符合。……参考答案：A
A、采用 SM3 算法计算杂凑值
B、使用 SM4-CBC 模式生成消息鉴别码，其中初始向量为全 0,消息长度为约定好的固定长度
C、使用 SM3 和 SM2 算法计算签名值
D、采用 SM3-HMAC 算法计算消息鉴别码

452.对数字证书分析，一般要分析（）内容。……参考答案：D
A、查看数字证书密钥用法
B、查看数字证书密钥用法、验证数字证书链
C、验证数字证书数字签名、验证数字证书链
D、查看数字证书密钥用法、验证数字证书数字签名、验证数字证书链

453.某 OA 办公系统面向办公人员提供在线办公、公文意见签批等服务，管理员登录后台进行系统管理操作。经现场测评，办公人员身份鉴别判定为“不符合”，管理员身份鉴别判定为“符合 ”，则针对应用和数据安全层面的“身份鉴别”测评单元，最终判定结果为（ ）。……参考答案：B
A、符合
B、部分符合
C、不符合
D、不适用

454.某信息系统管理员在互联网通过合规的 SSLVPN 接入系统内网，管理员使用合规的智能密码钥匙登录 SSLVPN，并正确启用国密算法，数字证书由合规的 CA 机构颁发，则网络和通信安全层面的“身份鉴别”指标应判定为（）。……参考答案：D
A、符合
B、部分符合
C、不符合
D、无法判断

455.某机关办公 OA 信息系统面向机关内所有办公人员提供服务，信息系统系统通过管理员进行运行维护。经测评，如果办公人员身份鉴别判定为不符合，管理员身份鉴别判定为符合，针对应用和数据层面的“身份鉴别”测评单元，最终判定结果为（ ）。……参考答案：B
A、符合
B、部分符合
C、不符合
D、不适用

456.根据《信息安全技术 电子文件密码应用指南》，应用系统建立用户权限表时，限定用户的最小权限集，需要保证任何用户不能同时拥有（ ）的权限。……参考答案：D
A、系统管理员和存储管理员
B、系统管理员和操作员
C、保密管理员和加密管理员

D、系统管理员和审计管理员

457.根据《随机性检测规范》，需要检测待检序列中给定长度的子序列之间的线性独立性时，使用（　）检测。……参考答案：C
A、线性复杂度检测方法
B、累加和检测方法
C、矩阵秩检测方法
D、离散傅立叶检测方法

458.根据《信息安全技术证书认证系统密码及其相关安全技术规范》，证书认证系统应采用（），并建设双中心(证书认证中心和密钥管理中心)。……参考答案：A
A、双证书机制
B、证书机制
C、数字签名证书机制
D、数据加密证书机制

459.在 linux 服务器上安装密码系统管理工具前，需要确认端口 9000 是否被占用，以下哪个选项不能确认 9000 端口是否被占用（　）。……参考答案：A
A、netstat -tn|grep 9000
B、netstat -tunlp|grep 9000
C、ss -tulpn | grep 9000
D、lsof -i:9000

460.密码系统管理工具安装包 scm_client.tar.gz 上传到 linux 服务器后，以下解压命令正确的是（）。……参考答案：B
A、tar –zcvf ./scm_client.tar.gz
B、tar –zxvf ./scm_client.tar.gz
C、tar –zcf ./scm_client.tar.gz
D、tar –cf ./scm_client.tar.gz

461.对于一个信息系统，使用了签名验签服务器和安全接入网关，现需要对接入的多个用户进行授权访问签名验签服务器，管理员可登录安全接入网关通过将多个用户加入同一个（　）来授权多个用户均可以访问签名验签服务器。……参考答案：D
A、群
B、IP
C、资源
D、用户组

462.对于 VPN 产品，运维人员可通过登录管理页面，设置（），对流向本机的数据包执行过虑。……参考答案：B
A、转发过滤规则
B、入包过滤规则
C、出包过滤规则
D、DNAT

463.使用 Wireshark 抓取密码系统 API 接口通信报文时，过滤 http 的 get 请求报文，以下过滤规则正确的是（）。……参考答案：B
A、http.method=="GET"
B、http.request.method=="GET"
C、http.method=="POST"
D、http and method=="GET"

464.使用 xshell 登录部署密码软件系统的服务器，需要服务端开放以下()端口。……参考答案：B
A、20
B、22
C、23
D、25

465.关于服务器密码机密码设备日志管理的要求，下列说法不正确的是（　　）。……参考答案：B
A、日志管理应包含记录、查看、导出等功能。
B、日志内容应包含管理操作行为、用户访问行为、异常事件等。
C、管理员操作行为包含包括登录认证、系统配置、密钥管理等操作。
D、如与设备管理中心连接，则应对相应操作进行记录

466.关于信息系统安全运维管理中，日志管理的目的不包含（）。……参考答案：B
A、发现攻击线索
B、责任追究
C、恢复数据
D、司法证据

467.审计人员应当以风险导向为基础开展 IT 审计，（　　）应当贯穿于 IT 审计的全过程。……参考答案：B
A、审计日志
B、风险评估
C、审计工具
D、风险处置

468.信息安全技术中，密码系统作为网络安全管理支撑系统之一，其系统日志由（）管理。……参考答案：C
A、系统管理员
B、安全管理员
C、审计管理员
D、网络管理员

469.密码应用安全状态监控对象列表，需要考虑的因素，描述不正确的是（　　）。……参考答案：D

A、分析监控的必要性
B、分析监控的可行性
C、分析监控的开销和成本
D、分析监控的有效性

470.密码应用安全状态监控中，通过对（）进行分析，及时发现密码应用安全事件或安全变更需求，并对其影响程度和范围进行分析，分析这些变化对安全的影响，并评估是否有必要作出响应。……参考答案：B
A、密码应用安全状态监控对象列表
B、密码应用安全状态信息
C、密码应用安全状态分析报告
D、密码应用安全状态自查报告

471.应急处置操作记录中，影响范围的记录主要描述（　　）。……参考答案：B
A、事件的严重性
B、受影响的系统、数据和用户
C、事件的经济损失
D、事件的解决方案

472.应急处置操作记录的“故障原因”一栏中，应包含（）。……参考答案：C
A、解决方案
B、故障现象描述
C、故障产生的原因分析
D、故障影响范围

473.为了确保密码系统管理工具的安装过程符合组织的安全要求，需要（　　）。……参考答案：C
A、忽略安全策略
B、仅依赖自动化工具的默认设置
C、审核安全策略
D、避免记录操作步骤

474.安装密码系统管理工具之后，进行安全测试的目的是（）。……参考答案：A
A、确保没有引入新的安全漏洞
B、评估工具的用户界面
C、测试网络速度
D、增强用户满意度

475.密码系统管理工具在配置时，技术人员设置了定期变更密码的配置，要目的是（　　）。……参考答案：C
A、防止密码疲劳
B、提升用户体验
C、增强安全性
D、降低成本

476.密码系统管理工具在配置时，技术人员配置了多因素认证（MFA），目的是提高（）的安全性。……参考答案：B
A、密码生成环节
B、身份鉴别过程
C、日志审计环节
D、业务培训环节

477.关于密码系统管理工具的日常运维工作，以下（）做法是推荐的最佳实践。……参考答案：C
A、允许密码系统管理工具自动执行更新
B、为了提高效率，应取消操作日志的记录功能，以减少处理时间
C、定期为管理工具的用户账号和权限进行审计，以确保符合最小权限原则
D、在生产环境中进行重要的系统配置变更

478.以下选项（）不是密码管理工具的日常运维管理的内容。……参考答案：D
A、定期审计与监控密码库的安全性
B、对用户操作日志进行定期审查
C、定期备份密码库并测试恢复流程
D、安全管理员更新密码管理工具的软件版本和安全补丁

479.密码系统管理人员应当(　　)处理废弃或过期的密码。……参考答案：B
A、存档备份
B、立即删除
C、加密存储
D、转移给新用户

480.密码系统管理人员在（）情况下应该立即上报密码安全问题。……参考答案：C
A、发现系统性能下降
B、用户反映密码重置问题
C、怀疑密码泄露或被非法访问
D、系统升级完成

481.东进技术服务器密码机管理工具可执行的初始化操作不包括以下哪个选项（　　）。……参考答案：C
A、原始初始化
B、恢复初始化
C、设备初始化
D、出厂初始化

482.东进技术服务器密码机管理工具的设备自检功能不包括以下哪个选项（　　）。……参考答案：B
A、物理噪声源检测
B、关键参数机密性检测

C、密钥库完整性检测
D、SM1/SM2/SM3/SM4 算法检测

483.对于符合 GM/T 0034 的 CA 系统，审计员进行系统安全审计是，需检查 CA 的操作系统、数据库系统日志、防火墙日志、(　　)等的日志。……参考答案：A
A、CA 系统
B、KM
C、KMP
D、KMC

484.密码系统日志应进行保护，日志信息免受破坏和（　　）访问。……参考答案：B
A、授权的
B、未授权的
C、限制
D、远程

485.以下哪个属于密码安全事件处理规划和准备阶段的工作（　　）。……参考答案：C
A、通过人工或自动方式,发现并报告信息安全事态的发生或信息
安全脆弱性的存在
B、收集有关信息安全事态或脆弱性的信息
C、设计和开发信息安全事态、事件和脆弱性管理的意识教育和培训课程
D、进行法律取证分析

486.以下哪个属于密码安全事件处理发现和报告阶段的工作（　　）。……参考答案：A
A、从内部和外部数据源收集态势感知信息,包括本地系统和网络的
流量和活动日志、可能影响事件活动的当前政治、社会或经济活动的新闻报道、事件趋势的外部报道、新的攻击向量、现有攻击指标以及新的缓解对策和技术
B、测试信息安全事件管理计划及其过程和规程
C、建立、实施和运行技术上、组织上和操作上的机制,来支持信息安全事件管理计划和 IRT 的工作。开发和部署必要的信息系统来支持 IRT,包括信息安全数据库。这些机制和系统旨在防止信息安全事件发生或降低信息安全事件发生的可能性
D、按照指南对信息安全事态以及在被归为信息安全事件后的
后续行动进行完整的文档化

487.网络安全事件分为（　　）个级别。……参考答案：B
A、3 个
B、4 个
C、5 个
D、6 个

488.如果事件影响为受到破坏后,对社会秩序、经济建设和公共利益造成危害,或对相关公民、法人和其他组织的合法权益造成严重或特别严重损害,但不危害国家安全，属于哪个级别的影响（）。……参考答案：B
A、特别重要

B、重要
C、一般
D、较小

489.以下哪种属于恶意程序事件（　　）。……参考答案：D
A、漏洞利用事件
B、DNS 污染事件
C、数据篡改事件
D、计算机病毒事件

490.密钥泄露属于哪种网络安全事件分类（　　）。……参考答案：B
A、网络攻击事件
B、数据安全事件
C、信息内容安全事件
D、设备设施故障事件

491.密码安全事件的成因分析不包括（　　）。……参考答案：D
A、了解事件破坏方法、破坏类型、破坏者或恶意程序的标识和特征；对异常文件进行备份；
B、明确破坏所跨越网络路径，涉及网络区域（外网、内网、子网、骨干网）
C、破坏者取得何种权限（破坏是否已取得超级用户特权）
D、不对存的证据进行合理的汇总和归纳

492.密码安全事件事态详情包括事态发生的时间和日期、（　　）、事件被报告的日期和时间。……参考答案：C
A、事态终止的时间和日期
B、识别的任何脆弱
C、事态被发现的时间和日期
D、报告人的联系方式

493.以下（　　）不是密码安全事件上报的要求。……参考答案：D
A、及时性
B、保密性
C、合规性
D、先进性

494.发生密码安全相关的事件时，应按照规定的程序向信息系统主管部门和（）进行报告。……参考答案：B
A、公安部门
B、密码管理部门
C、检察机关
D、民政部门

495.以下（）不是密码场景应急预案的内容。……参考答案：D
A、应急响应小组

B、应急响应流程
C、应急响应保障
D、密码应用方案

496.密码场景应急预案是指针对（）或紧急情况所制定的应对计划。……参考答案：C
A、密码产品认证
B、密码产品检测
C、密码安全事件
D、密钥管理

497.当召集应急团队时，下列（　　）是必要的。……参考答案：B
A、仅召集网络管理员。
B、分配任务和责任给团队成员。
C、只通知管理层，不必召集其他团队成员。
D、不需要召集团队，单独处理异常情况

498.在应急处理流程中，下列（）属于正确做法。……参考答案：B
A、立即采取措施进行修复。
B、确认异常事件的性质和范围。
C、不必分析可能的影响和风险。
D、忽略异常事件，等待自行解决。

499.密码应急处置报告的目的是（　　）。……参考答案：C
A、详细描述事件调查过程
B、记录沟通与通知过程
C、提出防范措施和改进建议
D、概述事件的影响和风险

500.在应急处置报告中，下列（）属于报告基本信息的内容。……参考答案：C
A、事件调查与分析
B、影响分析
C、报告标题和编制日期
D、防范措施

二、多选题

1.道德的基本特征包括以下哪些方面。……参考答案：AC
A、客观性
B、主观性
C、普遍性
D、相对性

2.在职业道德的培养中，起着关键作用的因素是（）。……参考答案：BC
A、政府法律法规的约束
B、个人价值观的塑造

C、职业道德教育课程的学习
D、行业的自我监管机制

3.职业道德在不同历史时期的主要表现有（）。……参考答案：ABCD
A、原始社会：无私为人，团结互助
B、奴隶社会：忠诚至上，敬畏权威
C、封建社会：仁爱待人，忠诚敬业
D、资本主义社会：契约精神，公平竞争

4.职业道德的遵守主要依靠（）。……参考答案：ABD
A、自我控制，自我约束
B、社会的舆论和普遍认知
C、前辈的言传身教
D、自身职业道德修养

5.关于立场坚定的说法，正确的是（）。……参考答案：AD
A、保持本色不随波逐流
B、根据环境的变换时常改变底线
C、立场坚定就是墨守成规
D、保持做人原则的不变也是立场坚定的一种表现

6.实现企业诚实守信的做法有（）。……参考答案：AB
A、履行合约内容
B、不偷工减料
C、提高员工福利
D、参与社会服务工作

7.坚持原则的做法中属于正确的原则有（）。……参考答案：BCD
A、利己主义
B、不损人利己
C、廉洁公正
D、遵纪守法

8.关于爱国敬业的理解正确的是（）。……参考答案：CD
A、热爱有钱的岗位
B、不应该转行
C、强化岗位责任
D、梳理职业理想

9.职业人员在日常工作应保持（）的职业守则。……参考答案：ABC
A、积极进取
B、刻苦钻研
C、甘于奉献
D、追名逐利

10.以下（）做法符合团结协作的要求。……参考答案：BCD
A、埋头苦干
B、积极分享
C、合理分工
D、按劳分配

11.以下属于计算机的基本组成部分的部件是（）。……参考答案：BD
A、CPU 散热器
B、图形处理单元（GPU）
C、操作系统
D、硬盘驱动器

12.操作系统(OS)负责管理计算机的基本资源，包括（）。……参考答案：ABCD
A、CPU 时间
B、内存空间
C、文件系统
D、电源

13.属于传输层的协议是（）。……参考答案：AB
A、TCP
B、UDP
C、IP
D、HTTP

14.以下关于交换机的描述中，正确的是（）。……参考答案：AB
A、交换机可以学习 MAC 地址并据此转发帧
B、交换机可以减少网络中的广播流量
C、交换机只能在相同类型的网络间进行通信
D、交换机能够对数据包进行分段和重组

15.在电子电路设计中，用来提高电路的功率效率的方法包括（）。……参考答案：CD
A、增加供电电压
B、增加负载电阻
C、使用高效率的电源转换器
D、优化电路布局以减少能量损耗

16.以下二进制数值大于十进制中的数值 5 是（）。……参考答案：BCD
A、101
B、1001
C、110
D、1011

17.Windows 操作系统中，用于优化系统性能的措施包括（）。……参考答案：ABC

A、定期运行病毒扫描
B、安装最新的系统更新
C、清理临时文件
D、增加更多 RAM

18.Linux 系统的广泛应用主要是因为以下特性（）。……参考答案：ABCD
A、安全性
B、稳定性
C、免费和开源
D、高自定义性

19.在关系型数据库中，常见的完整性约束有（）。……参考答案：ABCD
A、PRIMARY KEY
B、FOREIGN KEY
C、CHECK
D、UNIQUE

20.非关系型数据库的特点包括（）。……参考答案：ACD
A、高可扩展性
B、严格的 ACID 属性
C、灵活的数据模型
D、简单的横向扩展

21.在文字处理软件中，可以插入到文档中的元素有（）。……参考答案：ABCD
A、图片
B、表格
C、脚注
D、超链接

22.电子邮件中的哪些功能对提高工作效率特别有帮助（）。……参考答案：ABCD
A、自动回复
B、邮件过滤器
C、邮件归档
D、邮件标签

23.保证网络安全的要素包括（）。……参考答案：ABC
A、信息的保密性
B、发送信息的不可否认性
C、数据的完整性
D、数据存储的唯一性

24.属于脆弱性识别手段的有（）。……参考答案：ABCD
A、漏洞扫描
B、基线核查

C、弱口令检测
D、渗透测试

25.风险评估服务带给客户的服务价值有（）。……参考答案：ABCD
A、资产全面梳理
B、潜伏威胁检查
C、了解安全防护现状
D、辅助管理层科学决策

26.有关人员安全的描述不正确的是（）。……参考答案：ACD
A、人员的安全管理是企业信息安全管理活动中最简单的环节
B、人员离职之后，必须清除离职员工所有的逻辑访问帐号
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、由于公司急需用人，重要或敏感岗位的人员未经审查即允许其入职

27.企业从获得良好的信息安全管控水平的角度出发，以下行为不适当是（）。……参考答案：ACD
A、只关注外来的威胁,忽视企业内部人员的问题
B、及时更新系统和安装系统和应用的补丁
C、开着电脑离开工位
D、相信来自陌生人的邮件，好奇打开邮件附件

28.鉴别的基本途径有 3 种：所知、所有和个人特征，其中基于所知的是（）。……参考答案：ACD
A、口令
B、令牌
C、知识
D、密码

29.以下访问控制策略中，不需要安全标签的是（）。……参考答案：ACD
A、基于角色的策略
B、强制访问控制策略
C、基于标识的策略
D、用户指向的策略

30.在通信传输控制点中，要求应采用密码技术保证通信过程中的数据保密性，以下保密措施正确的是（）。……参考答案：ABC
A、采用加密软件对链路中的数据进行加密
B、通过 HTTPS 协议对整个链路的传输做加密
C、通过 SSH 协议进行加密
D、通过 FTP 对链路中数据传输做加密

31.（）是安全审计流程的步骤。……参考答案：ACD

A、记录结果
B、召集管理评审
C、让正确的业务部门领导参与
D、确定范围

32.关于信息安全管理体系（Information Security Management Systems,ISMS）,下面描述不正确的是（）。……参考答案：C
A、是一个组织整体管理体系的组成部分
B、是有范围和边界的
C、是风险评估的手段
D、其基本过程应遵循 PDCA 循环

33.变更控制流程包含（）步骤。……参考答案：ABCD
A、请求执行变更、变更的批准
B、变更的记录
C、测试和提交
D、变更的实施

34.以下安全控制措施中，属于预防性的有（）。……参考答案：AD
A、网络防火墙
B、RAID3
C、银行账单监督复审
D、分配计算机用户标识

35.以下可能用来确定数据敏感性的因素有（）。……参考答案：ABCD
A、数据价值
B、如果数据泄密，可能造成的损害程度
C、如果篡改或破坏数据，可能造成的损害程度
D、数据保护的法律、法规或合同约束

36.（）不能描述加密技术在静止数据保护中的应用。……参考答案：ABD
A、虚拟专用网
B、消磁
C、全盘加密
D、RAID 0

37.为解决数据残留问题，要慎重制定用于确保正确地移除(Remove)隐私数据的工作程序。一般来说，可采用如下（）方法来完全消除(Eliminate)数据残留。……参考答案：ABCD
A、覆写技术
B、消磁技术
C、强密钥加密技术
D、物理销毁

38.数据所有者通常可以由（）担任。……参考答案：BCD

A、IT 工程师
B、CEO
C、部门经理
D、高级管理层成员

39.目前尚未找到有效量子攻击方法的公钥密码体制有（）。……参考答案：ABCD
A、基于格的密码
B、基于多变量的密码
C、基于编码的密码
D、基于杂凑函数的密码

40.下列关于 SM4 的密钥扩展算法叙述正确的是（）。……参考答案：ABC
A、采用 32 轮非线性迭代结构
B、每次迭代生成 32 比特轮密钥
C、采用与加密算法相同的 S 盒
D、采用与加密算法相同的线性变换

41.公钥密码体制的算法包括（）。……参考答案：ABCD
A、基于大整数因子分解困难的 RSA 密码算法
B、基于有限域上的离散对数问题的密码算法
C、基于椭圆曲线上的离散对数问题的密码算法
D、后量子密码算法

42.密码杂凑函数有多种构造方式，采用 M-D 结构的算法为（）。……参考答案：ABD
A、MD5
B、SHA-1
C、SHA-3
D、SM3

43.根据 GM/T 0022《IPSec VPN 技术规范》，AH 协议可提供（）安全功能。……参考答案：BCD
A、数据保密性
B、数据完整性校验
C、数据源身份鉴别
D、抗重放攻击

44.PKI 的组成部分一般包括（）。……参考答案：ABCD
A、签发证书的证书机构 CA
B、登记证书的注册机构 RA
C、证书库
D、密钥管理系统 KM

45.GB/T 15843《信息技术安全技术实体鉴别》中给出了以下几种鉴别机制（）。……参考答案：ABCD

A、采用对称加密算法的机制
B、采用数字签名技术的机制
C、采用密码校验函数的机制
D、使用零知识技术的机制

46.SM9 密钥交换协议的辅助函数包括（）。……参考答案：ABD
A、密钥派生函数
B、杂凑函数
C、分组密码算法
D、随机数发生器

47.密钥生成时，一般会伴随（）密钥控制信息。……参考答案：ABCD
A、密钥拥有者
B、密钥用途
C、密钥索引号
D、生命周期起止时间

48.以下（）密码产品适用于 GM/T0028《密码模块安全技术要求》。……参考答案：AD
A、服务器密码机
B、安全芯片
C、CA/KM 系统
D、智能密码钥匙

49.在 GM/T 0034《基于 SM2 密码算法的证书认证系统密码及其相关安全技术规范》中，证书状态查询有几种提供服务的方式（）……参考答案：BD
A、官网查询
B、OCSP 查询
C、EMAIL 查询
D、CRL 查询

50.根据 GM/T 0104《云服务器密码机技术规范》，云服务器密码机宿主机的初始化应包括（）。……参考答案：ABC
A、宿主机密钥的生成（恢复）与安装
B、生成管理员
C、对密钥进行安全存储与备份
D、系统配置和密钥管理

三、判断题

1. 道德是人们在社会生活中遵守的行为准则和价值观。 ……参考答案：（√）

2. 职业道德的社会功用包括维护公共利益和增强社会信任度。……参考答案：（√）

3.职业道德是在封建社会形成的。……参考答案：（×）

4.职业道德的展现形式具有多样性。……参考答案：（√）

5.爱党爱国，立场坚定只是个人的要去，企业不需要践行。……参考答案：（×）

6.只要做到遵纪守法，诚实守信就不需要遵循其他的道德标准了。……参考答案：（×）

7.坚持原则一定会损害自身的利益。……参考答案：（×）

8.忠于职守要求我们要经常加班。……参考答案：（×）

9.积极进取是一种心态，不需要付出行动。……参考答案：（×）

10.团结协作一定会造成利益冲突。……参考答案：（×）

11.所有的数据在传输到 CPU 之前都必须经过存储器管理单元（MMU）。…参考答案：（×）

12.IPv6 地址的长度为 32 位，与 IPv4 地址长度相同。……参考答案：（×）

13.UDP 协议提供无连接的服务。……参考答案：（√）

14.在局域网中，交换机可以减少广播风暴的影响。……参考答案：（√）

15.在电子电路中，电容器主要用于存储电能。……参考答案：（√）

16.二进制数系统中，十进制数字“5”被表示为“1010”。……参考答案：（×）

17.在 Windows 中，可以通过“任务视图”创建和管理虚拟桌面。……参考答案：（√）

18.Linux 系统不支持多用户并发使用。……参考答案：（×）

19.在 SQL 中，ORDER BY 子句用于对结果进行分组。……参考答案：（×）

20.非关系型数据库通常不适用于复杂的查询操作。……参考答案：（×）

21.通过“页眉和页脚”功能，可以在文档的每一页顶部和底部添加相同的文本或图形。……参考答案：（√）

22.OA 系统中的任务管理器可以用来分配和监控员工的工作任务。…参考答案：（√）

23.数据保密性是指保护网络中各系统之间交换的数据， 防止因数据被截获而造成泄密。……参考答案：（×）

24.起不到应有作用的安全保护措施不属于脆弱性。……参考答案：（×）

25.风险闭环的责任人是风险上报人。……参考答案：（×）

26.信息安全应急响应计划总则包括编制目的、编制依据、工作原则。……参考答案：（√）

27.应用级访问控制策略能够最有效的约束雇员只能履行其分内的工作。……参考答案：（√）

28.令牌属于鉴别的基本途径中的基于所知。……参考答案：（×）

29.访问控制表与访问能力表相比，访问控制表更适用于集中式系统。…参考答案：（√）

30.根据等级保护相关管理文件，网络安全等级保护等级分为 5 个级别。……参考答案：（√）

31.渗透测试中必须要查看软件源代码，因此测试中发现的漏洞更多。…参考答案：（×）

32.信息安全管理体系 (ISMS)是一系列策略、流程和系统的集合，用于管理 ISO/IEC27001 中概述的信息资产风险。……参考答案：（√）

33.变更管理是一个业务流程，旨在规范业务活动（如项目）的变化，组织的信息安全人员只需要参与变更管理流程，不负责变更管理。……参考答案：（√）

34.岗位轮换就是指随着时间的推移，公司内部有不止一名员工执行同一个岗位的任务。这可使公司有超过一名员工能理解某个特定职位的职责和相关任务，能在人员离职或不在岗时提供后备人员。岗位轮换同样可帮助识别欺诈行为，也因此被视为一种检测型控制。……参考答案：（√）

35.数据泄露意味着数据的完整性已受到损害。……参考答案：（×）

36.处理状态数据(Data In Use)是驻留在主存储设备中的数据。这些主存储设备包括易失性内存（如 RAM）、存储缓存或 CPU 寄存器等。……参考答案：（√）

37.信息生命周期所有阶段都需要使用密码系统进行有效控制。……参考答案：（√）

38.数据所有者负责决定所拥有数据的分级，并在业务运营需求出现变化时调整数据分级方案。……参考答案：（√）

39.多表代换密码可以抵抗频率分析攻击。……参考答案：（√）

40.基于 ZUC 的两种算法包括机密性算法 128-EEA3 和完整性算法 128-EIA3。……参考答案：（√）

41.SM9 密码算法的应用与管理需要数字证书。……参考答案：（×）

42.SM3 算法和 SHA-256 算法的杂凑值长度相等。……参考答案：（√）

43.在 GM/T 0022《IPSec VPN 技术规范》中，AH 协议可单独用于封装 IP 数据报文，不需要和 ESP 协议嵌套使用。……参考答案：（×）

44.在 PKI 系统中，由 RA 机构绑定用户的身份信息和公钥。……参考答案：（×）

45.相互鉴别是指两个通信实体运用该机制彼此进行鉴别。……参考答案：（√）

46.SM2 密钥交换协议为 MQV 的一个变种，同样具有鉴别通信双方身份真实性的功能。……参考答案：（√）

47.密钥在其生命周期结束时，应当进行销毁。但是出于解密历史数据和验证历史签名的需要，有些不在生命周期内的密钥可能需要持续保存，故加密密钥对的私钥和签名密钥对的私钥应进行归档。……参考答案：（×）

48.安全二级在安全一级的基础上增加了拆卸证据、基于角色的鉴别等功能要求。……参考答案：（√）

49.依据 GM/T 0014《数字证书认证系统密码协议规范》，OCSP 是一种用于查询数字证书状态的协议，使得应用程序可获得所需要检验证书的状态。……参考答案：（√）

50.根据 GM/T 0030《服务器密码机技术规范》，服务器密码机的应用编程接口必须遵循 GM/T 0018。……参考答案：（√）

51.根据 GM/T 0029《签名验签服务器技术规范》，签名验签服务器的管理员身份鉴别应通过智能密码钥匙、智能 IC 卡与口令相结合的方式。……参考答案：（√）

52.根据 GM/T 0023《IPSec VPN 网关产品规范》，IPSec VPN 网关产品应具有随机数生成功能，其随机数应由多路硬件噪声源产生。。……参考答案：（√）

53.根据 GM/T 0027《智能密码钥匙技术规范》中要求，智能密码钥匙必须支持 SM1 算法。……参考答案：（×）

54.门禁卡发卡和密码模块发行时，密钥注入过程中不得泄露明文密钥的任何组成部分。……参考答案：（√）

55.签章人数字证书在有效期内被吊销后，则其签章时间均无效。……参考答案：（×）

56.应用系统的用户身份鉴别必须采用基于公钥密码算法的数字签名机制等密码技术实现真实性。……参考答案：（×）

57.密码应用安全评估要求，当密码应用安全时间发生时，应立即启动应急处置措施，事后，应及时向应急主管部门报告。……参考答案：（×）

58.计算密码平台应用方案中，应包含物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全等方面。……参考答案：（×）

59.劳动合同的期限只存在有固定期限和无固定期限两种。……参考答案：（×）

60.劳务派遣单位应当依照公司法的有关规定设立，注册资本不得少于五十万元。……参考答案：（√）

61.任何组织或者个人不得利用密码从事危害国家安全、社会公共利益、他人合法权益等违法犯罪活动。……参考答案：（√）

62.电子签名人，是指持有电子签名制作数据并以本人身份或者以其所代表的人的名义实施电子签名的人。……参考答案：（√）

63.国家网信部门负责统筹协调网络安全工作和相关监督管理工作。国务院电信主管部门、公安部门和其他有关机关依照本法和有关法律、行政法规的规定，在各自职责范围内负责网络安全保护和监督管理工作。……参考答案：（√）

64.涉密人员禁止向境外期刊等新闻出版机构投寄稿件。……参考答案：（×）

65.任何组织、个人可以随意收集数据。……参考答案：（×）

66.根据《中华人民共和国个人信息保护法》，经个人同意后，个人信息处理者即可对个人信息进行收集、存储、使用。……参考答案：（×）

67.根据《商用密码管理条例》，商用密码服务使用网络关键设备和网络安全专用产品的，应当经商用密码认证机构对该商用密码服务认证合格。……参考答案：（√）

68.GB/T 39786 中第三级要求规定，在设备计算层面，“宜”采用合规密码技术实现身份鉴别。……参考答案：（×）

69.在密码应用需求调研过程中，需要确保数据的准确性和完整性，但无需对调研数据做保密要求。……参考答案：（×）

70.信息系统密码应用需求调研问卷设计只针对已完成建设的改建系统。……参考答案：（×）

71.信息系统密码应用的密码应用需求调研属于信息系统密码应用建设阶段。……参考答案：（×）

72.信息系统现状分析活动是分析信息系统现状，明确需要保护的信息资源和所涉及的范围，形成信息系统综合描述。……参考答案：（√）

73.等保定级为第三级的网络与信息系统可遵循 GB/T 39786 第二级密码应用基本要求。……参考答案：（×）

74.信息系统密码相关安全风险分析目标是根据信息系统现状，分析信息系统中存在的密码相关安全风险。……参考答案：（√）

75.GB/T 39786《信息安全技术信息系统密码应用基本要求》从管理制度、人员管理、建设运行和应急处置四个方面提出管理基本需求。……参考答案：（√）

76.信息系统密码应用特殊需求包括所属行业及关键信息基础设施的合规性特殊需求和重要信息资产保护特殊需求。……参考答案：（√）

77.信息系统中使用的密码产品、密码服务可根据项目实际情况选择符合法律法规的相关要求。……参考答案：（×）

78.信息系统密码应用需求分析文档化活动目的是总结密码应用基本需求和密码应用特殊需求，形成密码应用需求分析。……参考答案：（√）

79.商密产品认证证书目录是保密的，无法通过互联网查询确认。……参考答案：（×）

80.安全芯片、密码系统类不依据密码模块标准进行检测和认证。……参考答案：（√）

81.物理和环境的方案设计是业务系统部署的机房。……参考答案：（√）

82.网络与通信对象指的是信息系统与外界交互的通道。……参考答案：（√）

83.设备与计算的方案设计中不需要考虑堡垒机。……参考答案：（×）

84.支撑平台的自身安全性,包括密钥安全、访问安全、管理安全和租户间的隔离安全等。……参考答案：（√）

85.应用与数据的改造对象只要包含客户端即可。……参考答案：（×）

86.用户属于应用和数据安全层面身份鉴别的测评对象。……参考答案：（√）

87.在信息系统密码应用框架中，租户是业务应用的所有者和用户的管理者。……参考答案：（√）

88.在信息系统密码应用框架中，三种责任主体需分别对应不同的现实主体。……参考答案：（×）

89.项目范围说明书是项目范围管理的主要输出之一。……参考答案：（√）

90.在项目计划管理中，项目经理需要确保所有团队成员都理解和遵循项目计划。……参考答案：（√）

91.在项目实施阶段，项目经理应该避免对项目计划进行任何更改。……参考答案：（×）

92.项目实施团队中，所有团队成员都应该参与项目决策过程。……参考答案：（√）

93.在项目成本管理中，成本控制的主要目标是确保项目成本不超过预算。……参考答案：（√）

94.在项目变更管理中，变更请求一旦被批准，就可以立即实施，无需进一步分析。……参考答案：（×）

95.在项目质量管控中，质量改进过程应该在项目开始时启动，并在整个项目期间持续进行。……参考答案：（√）

96.在项目风险识别中，风险识别是一个一次性的活动，不需要重复进行。……参考答案：（×）

97.在项目风险识别中，所有的风险都是可以被量化的。……参考答案：（×）

98.风险监控是在整个项目生命周期中持续进行的活动。……参考答案：（√）

99.风险应对计划只需要在项目开始前制定一次，之后无需更新。……参考答案：（×）

100.风险应对措施应该只针对那些已经被识别并记录在风险登记册中的风险。……参考答案：（×）

101.在信息系统项目中，风险应对措施的有效性可以在项目结束后通过回顾和总结经验来评估。……参考答案：（√）

102.密码产品的物理安全是安装的基本要求之一。应确保密码设备放置在安全可靠的环境中，防止未经授权的访问和物理破坏。此外，应定期检查物理环境的安全性，如机房的出入管理、监控系统等。……参考答案：（√）

103.密码产品安装应采取严格的密钥管理措施，确保密钥的完整性和机密性。应使用安全的密钥存储和传输方式，并定期更换密钥。同时，应定期审查密钥管理过程，以确保其始终符合相关标准和最佳使用需求。……参考答案：（√）

104.密码产品的正常运行需要在一个低电磁干扰的环境中进行。因此，应远离大型电动机、高压电线等。……参考答案：（√）

105.密码产品可以采取电磁屏蔽措施，如使用金属外壳，以减少电磁干扰对密码产品的影响。……参考答案：（√）

106.密码产品安装软件环境要求一般不需要管理员权限。……参考答案：（×）

107.密码产品安装软件环境要求不包含硬件要求。……参考答案：（×）

108.为确保密码产品的安全性和稳定性，须根据网络和系统的安全需求和密码应用的实际情况，采用物理隔离或逻辑隔离两种方式，进行严格网络隔离。……参考答案：（√）

109.为了防止外部攻击和未经授权的访问，应配置适当的防火墙规则：限制对密码产品的网络访问，只允许必要的网络流量通过。同时，对密码产品进行安全加固，关闭不必要的端口和服务，以减少潜在的攻击面。……参考答案：（√）

110.密码设备的初始化，除必须由厂商进行的操作外，系统配置、密钥的生成和管理、管理员的产生等均应由用户方设备管理人员完成。……参考答案：（√）

111.密码设备必须配置密码主管角色。……参考答案：（√）

112.服务器密码机在安装完成后，不需要进行任何形式的安全测试即可投入使用。……参考答案：（×）

113.服务器密码机的安装必须由经过专业培训的人员进行，以确保正确安装和配置。……参考答案：（√）

114.签名验签服务器在初始化时，应由设备供应商完成系统配置和密钥的生成。……参考答案：（×）

115.签名验签服务器的物理安全防护不重要，因为主要的安全措施应在网络层面实施。……参考答案：（×）

116.服务端签名密钥对由 SSL VPN 网关产品自身产生。……参考答案：（√）

117.服务端加密密钥对由 SSL VPN 网关产品自身产生。……参考答案：（×）

118.证书认证密钥管理系统的 KM 与 CA 必须处于同一局域网内。……参考答案：(×)

119.证书认证密钥管理系统的防火墙安全策略可以设置为路由模式。…参考答案：（√）

120.智能密码钥匙在设备发行时，必须对设备认证密钥进行修改。……参考答案：(√)

121.智能密码钥匙在设备发行时，必须设置设备标签。……参考答案：（×）

122.密码系统功能测试的基本方法是构造一些输入内容，检查输出是否为预期结果相同。……参考答案：（√）

123.测试密码系统的加解密功能时，加密密钥与解密密钥一定是相同的。……参考答案：（×）

124.签名验签服务器，进行 SM3 算法运算性能测试，选择数据报文长度为 32 字节，是合适的。……参考答案：（√）

125.签名验签服务器，进行并发性能测试时，配置并发连接数为 10 次，是合适的。……参考答案：（×）

126.测试服务器密码机 GM/T 0018 接口签名验签接口前，必须先生成密钥加密密钥。……参考答案：（×）

127.测试服务器密码机 GM/T 0018 对称加密接口前，必须先生成会话密钥。……参考答案：（√）

128.进行SSL VPN网关客户端-服务端模式密文测试时，可以发送TCP报文。……参考答案：（√）

129.进行SSL VPN网关客户端-服务端模式密文测试时，可以发送UDP报文。……参考答案：（×）

130.证书认证密钥管理系统在对场地检测时，测试机房屏蔽的做法是，在机房中查看手机是否有信号。……参考答案：（×）

131.证书认证密钥管理系统，对备份与恢复的测试点有两个，一是备份后，可以使用该备份正确恢复系统；二是备份与恢复，按策略正确进行。……参考答案：（×）

132.系统测试报告需系统测试通过后才能输出。……参考答案：（×）

133.编写系统测试报告目的是总结测试阶段的测试以及分析测试结果，描述系统是否符合需求。……参考答案：（√）

134.系统测试用例的重要级别分高、中、低三类，冒烟测试可从优先级较高的用例中挑选执行，保障核心/重要功能正常。……参考答案：（√）

135.每次测试执行都需要执行所有的测试用例。……参考答案：（×）

136.应用联调测试主要包括系统的功能性、安全性和用户界面设计。……参考答案：（×）

137.在密码应用联调测试中，测试的范围通常包括对外部接口的测试。…参考答案：（√）

138.缺陷报告的核心要素包括:缺陷编号、缺陷状态、缺陷标题、重现步骤、严重程度、优先级、缺陷类型、测试环境。……参考答案：（√）

139.缺陷报告的主要目的是确认测试缺陷已经得到了解决。……参考答案：（×）

140.密码系统测试报告总结中需要明确指出软件是否满足发布或接受标准。……参考答案：（√）

141.密码系统测试报告总结中关于风险，需要给出具体的解决方案。……参考答案：（×）

142.试运行期间需要构建团队管理，对操作人员进行有效地组织和安排。……参考答案：（√）

143.试运行团队管理只需要试运行工作人员反馈系统运行效果并上报即可，不需要其他工作内容参与。……参考答案：（×）

144.试运行结束后，收集了一些问题记录，因为系统已经在运行了，不需要调整和优化。……参考答案：（×）

145.通过有效的安全状态监控管理，可以确保项目在试运行阶段的安全性和稳定性，降低风险并提升项目的成功率。……参考答案：（√）

146.确保项目试运行的安全状态监控管理符合相关的合规性和法律要求。这包括遵守行业标准、遵循法律法规、满足合同要求等。……参考答案：（√）

147.密码应用类项目试运行阶段，针对用户提出的问题进行记录，为快速响应用户提出的变更需求，无需变更控制委员会同意，直接执行变更即可。……参考答案：（×）

148.密码类项目在试运行期间，变更请求需要以书面形式提出，并正式记录在变更日志中。……参考答案：（√）

149.密码系统试运行过程中，若出现数据泄露事件，应立即通知相关人员并启动应急预案。……参考答案：（√）

150.密码系统试运行过程中，加强系统监控，及时发现异常情况是必要的。……参考答案：（√）

151.密码系统试运行报告的结论部分只需概括性地描述试运行结果，无需提出改进措施和建议。……参考答案：（×）

152.在试运行阶段中，通常会对系统的网络环境进行详细描述，包括网络延迟、带宽、数据安全性等方面。……参考答案：（√）

153.试运行报告中的软件环境要求通常会涉及操作系统兼容性、数据库系统兼容性等方面。……参考答案：（√）

154.问题发生时间的准确记录对原因分析和解决问题不太重要。……参考答案：（×）

155.密码应用在实施阶段，风险评估主要对系统的开发与技术/产品获取、系统交付实施两个过程进行评估。……参考答案：（√）

156.密码应用在实施阶段，风险评估的目的是根据系统安全需求和运行环境对系统开发,实施过程进行风险识别,并对设计方案中所提供的安全功能符合性进行判断。……参考答案：（×）

157.系统试运行报告的总结章节应对试运行期间出现的问题、性能评估、用户反馈和建议进行全面总结，并提出未来改进方向。……参考答案：（√）

158.在系统试运行报告的总结中，重点关注问题的处理情况，可以不提及用户反馈和建议。……参考答案：（×）

159.GB/T 39786 中有“应”、“宜”的指标项而实际信息系统中不存在对应对象，指标项可为“不适用”。……参考答案：（√）

160.密码应用方案设计过程中，对于适用的项，逐条对照 GB/T 39786 对应等级下的各项密码应用技术要求，对方案的安全控制措施进行分析与自评，若指标涉及的所有保护对象的相应安全控制措施有效,则该指标的自评结果为通过。……参考答案:（×）

161.物理和环境安全保护的对象是物理访问的身份鉴别、电子门禁记录数据和视频监控记录数据。……参考答案：（√）

162.网络和通信安全保护的对象是信息系统与外界交互的通信信道。…参考答案：（√）

163.密码支撑服务必须采用经认证合格的密码支撑服务产品（如密码服务平台等）。……参考答案：（×）

164.基于经认证合格的密码产品进行设计密码支撑设计时，需要考虑提供的密码支撑方式（如租密码机方式、租密码服务器方式和租密码服务方式）。……参考答案：（√）

165.业务应用保护的对象是信息系统中的所有应用及其重要数据。……参考答案：（√）

166.在进行业务应用的密码应用方案设计时，使用签名功能的，需指明签名算法和签名机制（如签名内容、签名主体和签名位置等）。……参考答案：（√）

167.在进行密码应用方案设计时，业务应用现状的描述需包括业务应用的基本情况、承载的业务情况及系统软硬件构成。……参考答案：（×）

168.安全管理方案包括管理制度、人员管理、建设运行和应急处置。……参考答案：（√）

169.审核实施时，针对审核对象，对照附录 A 逐条审核。……参考答案：（√）

170.内容完整性审核实施需要针对技术方案的1-6项进行审核。……参考答案：(×)

171.审核内容一致性时，需要针对密码应用部署网络拓扑图、密码应用安全需求、安全控制措施是否具有一致性。……参考答案：（√）

172.审核内容一致性时，密码应用技术框架、密码应用三个安全层面设计具有一致性。……参考答案：（×）

173.文本规范性是指方案文字表述规范、专业术语准确，无影响阅读和理解的掉、错字，排版错误等问题。……参考答案：（√）

174.在文本规范性方面应涉及的密码技术专业术语使用需准确。……参考答案：（√）

175.信息系统密码应用方案编制时，关于系统概述部分，不应该明确给出当前系统等保定级情况。……参考答案：（×）

176.应制定实施保障方案，包含以下内容：人员组织保障、实施技术保障、项目质量保障、项目经费保障。……参考答案：（√）

177.编写方案密评报告时，若所有指标的安全控制措施评估结果均为通过，且初步量化评估分数能够达到阈值要求，则方案评估结论为通过；否则为不通过。…参考答案：（√）

178.在方案密评报告中应该体现出正确的系统网络拓扑图，并给出相应文字说明。包括网络体系架
构、网络区域划分、系统软硬件构成。……参考答案：（√）

179.密码应用现状应明确描述系统信息种类，并识别业务、管理、用户等关键数据类型及安全属性等。……参考答案：（√）

180.为了确保跨网络访问的通信信道明确标识，各类跨网通道的用户与数据逻辑关系必须明确。……参考答案：（√）

181.物理和环境安全层面的保护对象类型应包含电子门禁系统、 视频监控系统、环控系统以及消防系统。……参考答案：（×）

182.在云平台的密码应用设计中，密码管理平台可不作为应用和数据安全层面的保护对象。……参考答案：（×）

183.合规性自查表不适用项论证说明应充分、合理，且给出替代性风险控制措施。……参考答案：（√）

184.安全控制措施应满足密码应用需求，并具有合理性、可行性，不可存在高风险项。……参考答案：（√）

185.实施保障应包括项目实施过程中的组织保障、人员保障、经费保障、质量保障和监督检查等。……参考答案：（√）

186.实施保障方案应具备措施完备、有效，具备保障方案落地的流程和关键要素。……参考答案：（√）

187.合规性审查主要是为了确保业务/行为不违反任何法律法规，因此只需在出现问题时进行一次性审查即可。……参考答案：（×）

188.在撰写合规性审查意见时，除要关注自身的业务行为是否符合法律法规要求，还需考虑行业标准或道德规范。……参考答案：（√）

189.相较于等保 1.0，等保 2.0 的主要变化包括测评机构能力要求变化、定级对象变化、安全要求变化、控制措施分类结构变化。……参考答案：（×）

190.在等级保护 2.0，等保二级属于监督保护级。……参考答案：（×）

191.访谈方式在信息系统密码应用安全性测评中主要用于评估系统的硬件配置和网络连接稳定性。……参考答案：（×）

192.访谈方式在信息系统密码应用安全性测评中的优势之一是可以深入了解用户对密码策略和系统安全性的看法，收集用户的反馈和建议。……参考答案：（√）

193.文档审查方式在信息系统密码应用安全性测评中通常用于评估系统的物理安全措施和网络拓扑结构。……参考答案：（×）

194.文档审查方式在信息系统密码应用安全性测评中的优势之一是可以评估密码策略、安全配置文件和系统日志，以发现潜在的安全问题。……参考答案：（√）

195.实地查看方式在信息系统密码应用安全性测评中主要用于评估密码复杂性和用户登录频率。……参考答案：（×）

196.实地查看方式在信息系统密码应用安全性测评中的优势是可以直接评估物理安全措施和环境安全性，例如检查服务器机房的门禁措施和安全摄像头的部署情况。……参考答案：（√）

197.配置检查方式在信息系统密码应用安全性测评中是用来评估系统硬件配置和网络连接稳定性的。……参考答案：（×）

198.配置检查方式在信息系统密码应用安全性测评中的优势是可以直接评估操作系统和应用程序的安全配置，发现可能存在的配置漏洞。……参考答案：（√）

199.根据 GM/T 0116《信息系统密码应用测评过程指南》，在进行信息收集和分析任务中，对系统资产进行统计时，应确保资产调查信息的正确性和完整性。……参考答案：（√）

200.根据 GM/T 0116《信息系统密码应用测评过程指南》，测评方对填写完成的调查表格的进行分析时，可以采信自查结果、上次网络安全保护等级测评报告或商用密码应用安全性评估报告中的可信结果。……参考答案：（√）

201.在信息系统中，密码应用情况记录的主要目的是用于提高用户的工作效率。……参考答案：（×）

202.管理制度属于信息系统密码应用情况记录内容。……参考答案：（×）

203.在测评开始前，采用密码服务记录和统计方法的目的是检测信息系统中使用的密码技术是否遵循密码相关国家标准和行业标准。……参考答案：（×）

204.在密码服务中，验证用户身份可以用身份验证协议实现。……参考答案：（√）

205.根据 GM/T 0116《信息系统密码应用测评过程指南》，在测评准备活动阶段，需要对被测信息系统的核心资产进行确定。……参考答案：（×）

206.测评方之前对被测系统进行过商用密评应用安全性评估，熟悉被测信息系统情况，且存在以往的调查资料，因此，不需要重新进行被测信息系统资产等进行调研。……参考答案：（×）

207.被测信息系统网络拓扑图及描述主要介绍信息系统边界。……参考答案：（×）

208.被测信息系统承载的业务情况中需要重点说明业务的密码应用需求。……参考答案：（√）

209.在调研被测系统资产时，无需要调研被测信息系统安全相关的人员情况。……参考答案：（×）

210.从物理和环境、应用和数据不同层面描述信息系统密码应用的工作流程。……参考答案：（×）

211.在信息系统密码应用情况调研中需要考虑设备和计算安全层面的密码应用工作流程。……参考答案：（√）

212.被测信息系统使用的密码服务只能为电子政务电子认证服务。……参考答案：（×）

213.被测信息系统使用的密码服务应经商用密码认证机构认证合格和取得国家密码管理部门同意使用的证明文件。……参考答案：（×）

214.在信息系统密码应用调研问卷中，需要调研被测系统前次测评情况。……参考答案：（√）

215.在信息系统密码应用调研问卷中可以获取被测信息系统系统资产相关情况。……参考答案：（√）

216.在密码应用安全性评估的项目实施会议中，启动会和结束会是两个独立的环节，它们之间不需要有任何联系。……参考答案：（×）

217.在密码应用安全性评估的结束会中，通常会对评估过程中发现的问题和改进建议进行详细的讨论和确认。……参考答案：（√）

218.密码应用安全性评估的现场测评风险揭示书是一份单向文件，仅由评估团队提供给被评估方，无需被评估方的确认或反馈。……参考答案：（×）

219.在密码应用安全性评估中，授权书一旦签署，其有效期即与评估项目的整个周期相同，无需进行更新或续签。……参考答案：（×）

220.在物理和环境测评过程中，查看安全门禁系统数据库存储的日志记录，得到如下一条记录：B4BAD0B6BA19F13EAB2DCE29C5260C198469D6D74795F481583744F1719C899C，并通过查看相关代码判断系统采用 HMAC-SM3 算法来保证门禁记录数据的存储完整性，测评人员判断其 HMAC 值长度符合预期。……参考答案：（√）

221.在物理和环境测评过程中，经查看，测评人员发现电子门禁系统调用外置密码产品：一台签名验签服务器，并发现采用 HMAC-SM3 算法实现门禁记录数据的完整性保护，其中签名验签服务器具有商用密码产品认证证书，且密码模块安全等级为一级，测评人员判断符合预期。……参考答案：（×）

222.针对网络和通信安全的“重要数据传输机密性”测评单元，对于等保定级为第三级的系统，可采用密码技术保证通信过程中数据的完整性。……参考答案：（×）

223.针对网络和通信安全的“通信数据完整性”测评单元，针对 IPSec VPN 网关，测评人员进行如下测评操作：核查 IPSec VPN 网关的网络连接地址、报文封装方式、密码算法等安全策略配置，分析通信数据完整性和机密性保护采用的密码算法、密码技术是否符合预期；在 IPSec VPN 网关外网口或外侧出口路由器或防火墙上，通过镜像端口接入专用测试终端（如便携式电脑），在终端上利用密码协议分析类工具，捕获并分析 IPSec VPN 网关通信数据包，分析通信数据是否加密和完整性保护，分析密码算法、密码协议的合规性和正确性，请问如上操作是否正确。……参考答案：（√）

224.在设备和计算安全的测评过程中，针对身份鉴别测评单元，当系统使用堡垒机用于对设备进行集中管理时，堡垒机不必测评。……参考答案：（×）

225.在设备和计算安全的测评过程中，针对身份鉴别测评单元，测评对象不含密码服务，例如电子政务电子认证服务。……参考答案：（×）

226.在应用和数据安全的测评过程中，针对“重要数据传输完整性”的测评单元，对应的测评指标包括：针对等保定级的第二级，必须采用密码技术保证信息系统应用的重要数据在传输过程中的完整性。……参考答案：（×）

227.在应用和数据安全的测评过程中，针对身份鉴别测评单元，测评人员发现系统的身份鉴别基于协同签名技术，其中涉及到的用户签名密钥对，属于非对称密钥对，私钥分量分别存储在客户终端密码模块和协同签名服务器中。……参考答案：（√）

228.密码应用安全性评估的现场测评只需要关注密码系统的技术层面，无需考虑人员和管理层面的因素。……参考答案：（×）

229.对于已经取得相应证书的密码产品，在进行现场测评时不对其本身进行重复测评，主要进行符合性核验和配置检查。……参考答案：（√）

230.结果确认和资料归还是密码应用安全性评估过程中的两个重要环节，它们需要相互协调，以确保评估的完整性和保密性。……参考答案：（√）

231.根据密码应用安全性评估的标准流程，评估结束后，所有相关资料应立即归还给被评估方，无需等待结果确认。……参考答案：（×）

232.根据 GM/T 0116《信息系统密码应用测评过程指南》，现场测评活动的输出文档内容应包括工作计划和内容安排、双方人员的协调、被测单位应提供的配合与支持、工具测试的记录及测评结果、测评活动中发现的问题。……参考答案：（√）

233.现场测评活动的输出文档应仅由项目组长编写。……参考答案：（×）

234.针对密码应用岗位责任制度的访谈，针对等保定级为第三级的系统，密钥管理、密码安全审计、密码操作人员职责互相制约互相监督，其中密码安全审计员岗位可与密钥管理员、密码操作员兼任。……参考答案：（×）

235.针对操作规程的修正，测评指标为：应对管理人员或操作人员执行的日常管理操作建立操作规程，该指标适用于第一级到第四级。……参考答案：（×）

236.在随机数检测中，熵值越接近 1，说明生成的随机数质量越好。……参考答案：（√）

237.随机性检测工具主要依据 GM/T0005-2021《随机性检测规范》，对信息系统中用于密码运算的随机数进行检测，判断其是否合规。……参考答案：（√）

238.主动式扫描实现对 SSLVPN 的主动式扫描，可以通过主动式扫描探测发现 SSLVPN 服务器支持的所有密码算法。……参考答案：（×）

239.被动式扫描实现对 SSLVPN 和 IPSecVPN 的被动嗅探分析，解析出当前协议所使用的密码套件。……参考答案：（×）

240.协议分析工具主要用于对常见通信协议进行抓包、解析分析，支持对常见的网络传输协议、串口通信协议、蓝牙协议、移动通信协议（3G、4G）、无线局域网协议等进行协议抓包解析。……参考答案：（√）

241.逆向分析工具是指在没有源代码的情况下，通过分析应用程序可执行文件二进制代码，探究 应用程序内部组成结构及工作原理的工具。……参考答案：（√）

242.访谈管理员得知采用国密 VPN 进行通信,在客户端 PC 抓包分析握手过程并查看 VPN 客户端日志，基于 ECC_SM4_SM3 密码套件进行通信。请判断是否满足需求。……参考答案：（√）

243.某信息系统使用 HMAC-SM3 算法对设备和计算安全层面日志记录进行完整性保护。使用 SM4 算法对 HMAC-SM3 密钥进行加密存储，SM4 密钥存储在配置文件中；对 HMAC-SM3 密钥进行杂凑运算，并存储杂凑值，其值为 0xD033E22AE348AEB5660FC2140AEC35850C4DA997。请判断是否满足需求。……参考答案：（×）

244.某应用系统基于服务器密码机索引号为 42 的密钥实现重要数据的存储保密性和完整性，同时密钥通过服务器密码机加密后本地存储。请判断是否正确。…参考答案：（×）

245.被测业务应用在身份鉴别、重要数据传输机密性、重要数据传输完整性方面均未采用密码技术，整体测评时，依据 GM/T 0115《信息系统密码应用测评要求》，可能通过网络和通信安全层面的通信过程中“重要数据的机密性及通信数据完整性”对应用和数据安全层面进行弥补。……参考答案：（√）

246.经测评发现，某信息系统中所有设备不涉及重要信息资源安全标记，测评人员则对设备和计算安全层面的重要信息资源安全标记完整性测评单元判定结果为不符合。……参考答案：（×）

247.某信息系统管理员在互联网通过合规的 SSL VPN 接入系统内网后登录堡垒机对通用服务器进行远程管理，SSL VPN 建立合规的 GMSSL 通道并正确启用国密算法，则设备和计算安全层面“远程管理通道安全”测评单元可判定为“符合”。……参考答案：（×）

248.使用密码系统的人员管理一定包括管理制度发布流程。……参考答案：（√）

249.密码系统的关键岗位人员应签署保密协议。……参考答案：（√）

250.运维人员可直接增加或搬离密码硬件。……参考答案：（×）