

CISP-DSG 数据安全治理专业人员 考试大 纲与高频试题解析

一、CISP-DSG 认证简介

CISP-DSG (Certified Information Security Professional - Data Security Governance)，中文全称为注册信息安全专业人员-数据安全治理专业人员，是由中国信息安全测评中心联合天融信开发的国家级认证培训，是业界首个针对数据安全治理方向的权威认证。该认证旨在培养具备数据安全治理过程管理、数据安全技术体系设计、数据安全管理体系设计基本知识和能力的专业人才。

证书持有人员主要从事数据安全治理相关工作，具有数据安全治理过程管理、数据安全技术体系设计、数据安全管理体系设计的基本知识和能力。随着《网络安全法》《数据安全法》《个人信息保护法》等法律法规的相继落地，数据安全治理已从企业的可选项变为必答题，CISP-DSG 认证已成为遴选高级人才和业务伙伴的重要评判指标。

1.1 报考条件

- 具备一定数据安全治理基础，或有意向从事数据安全治理的人员
- 无学历与工作经验的报考要求（含相关专业的高校学生可报名）
- 同意并遵守 CISP 职业道德准则
- 必须参加授权培训机构的培训才可考试

1.2 考试形式与评分标准

项目	说明
考试题型	单项选择题（闭卷笔试）
题目数量	100 道
每题分值	1 分
试卷满分	100 分
通过标准	70 分及以上（含 70 分）
考试时长	120 分钟（2 小时）
考试机会	共 3 次（含 2 次补考）
证书有效期	三年

二、知识体系结构

CISP-DSG 知识体系结构共包含四个知识类，每个知识类根据其逻辑划分为多个知识体，每个知识体包含多个知识域，每个知识域由一个或多个知识子域组成。知识体系中每一个知识要点的内容和深度要求分为了解、理解和掌握三类。

知识类	核心内容	课程模块
信息安全知识	信息安全保障、信息安全评估、网络安全监管、信息安全支撑技术	模块 1-4

知识类	核心内容	课程模块
数据安全基础体系	结构化数据应用、非结构化数据应用、大数据应用、数据生命周期	模块 5-8
数据安全技术体系	数据安全风险、结构化数据安全技术、非结构数据安全技术、大数据安全技术、数据安全运维	模块 9-15
数据安全管理体系	数据安全制度、数据安全标准、数据安全策略、数据安全规范、数据安全规划	模块 16-19

三、四大知识类详解

3.1 信息安全知识

作为数据安全的基础支撑，该知识类聚焦信息安全的通用理论与支撑技术，是数据安全治理的基础知识储备。

3.1.1 信息安全保障

- 信息安全保障基础概念：保密性、完整性、可用性（CIA 三要素）
- 安全保障框架模型：IATF 信息保障技术框架、PDR 模型、APPDRR 模型
- 信息系统安全保障评估框架（GB/T 20274）

3.1.2 信息安全评估

- 信息安全评估基础：风险评估的基本概念与方法
- 评估实施流程：资产识别、威胁识别、脆弱性识别、风险分析、风险处置
- 信息系统安全等级保护（等保 2.0）

3.1.3 网络安全监管

- 网络安全法律体系：《网络安全法》《数据安全法》《个人信息保护法》
- 国家网络安全政策与监管体系
- 信息安全道德准则与信息安全标准

3.1.4 信息安全支撑技术

- 密码学基础：对称加密、非对称加密、哈希算法、数字签名
- 身份鉴别机制：基于知识的认证、基于令牌的认证、生物特征认证
- 访问控制模型：DAC、MAC、RBAC、ABAC

3.2 数据安全基础体系

该知识类聚焦数据本身的特性与应用场景，是技术体系与治理体系的共同基础。

3.2.1 结构化数据应用

- 关系型数据库基本概念：表、字段、记录、主键、外键、索引
- 数据库管理系统（DBMS）架构与 SQL 语言
- 数据仓库与 OLAP/OLTP

3.2.2 非结构化数据应用

- 非结构化数据类型：文档、图像、音视频、网页
- 非结构化数据存储与检索技术
- 文档管理系统与内容管理

3.2.3 大数据应用

- 大数据平台架构：Hadoop 生态体系（HDFS、MapReduce、HBase）
- 大数据处理与分析技术：Spark、Flink
- 数据挖掘与机器学习基础

3.2.4 数据安全基础知识

- 数据分类分级：按关系分类（来源、内容、用途）、按特性分级（价值、敏感程度、影响范围）
- 数据生命周期：创建、存储、传输、使用、共享、归档、销毁
- 数据安全基本原则：最小必要原则、目的限制原则、公开透明原则
- 数据安全能力成熟度模型（DSMM/GB/T 37988）：5 个等级（非正式执行、计划跟踪、充分定义、量化控制、持续优化）

3.3 数据安全技术体系

以具体防护手段为核心，聚焦数据全生命周期的技术保障能力。

3.3.1 数据安全治理与保障框架

- 数据安全治理概念：以数据为中心的安全体系
- Gartner 数据安全治理框架
- 数据安全治理与保障框架的核心要素

3.3.2 数据安全治理

- 数据安全组织架构与责任分工
- 数据安全制度体系建设
- 数据安全人员管理与培训

3.3.3 数据安全评估

- 数据安全风险评估方法与流程
- 数据资产识别与数据流分析
- 个人信息保护影响评估（PIA）

3.3.4 数据安全策略要求

- 数据安全策略制定原则
- 数据分类分级安全策略
- 数据全生命周期安全策略

3.3.5 数据安全技术要求

- 数据防泄漏技术（DLP）：终端 DLP、网络 DLP、邮件 DLP、云 DLP
- 数据脱敏技术：静态脱敏、动态脱敏、掩码、泛化、匿名化
- 数据库安全技术：数据库审计、数据库防火墙、加密传输、透明加密

3.3.6 数据安全运营要求

- 数据安全监控与告警
- 数据安全事件响应与应急处置
- 数据安全审计与合规检查

3.3.7 数据安全评测要求

- 数据安全合规评测标准
- 数据安全能力成熟度评估
- 数据安全评测实施流程

3.3.8 数据可用性保障

- 数据备份策略：全量备份、增量备份、差异备份
- 容灾技术：RPO（恢复点目标）与 RTO（恢复时间目标）
- 高可用架构与数据恢复

3.3.9 大数据安全防护技术

- Hadoop 生态安全：Knox 网关、Ranger 访问控制、Kerberos 认证
- 大数据加密技术：列级加密、透明数据加密
- 隐私计算技术：差分隐私、同态加密、联邦学习、安全多方计算

3.4 数据安全管理体系

从制度流程与合规视角出发，构建数据安全管理框架，涵盖制度、标准、策略、规范和规划。

3.4.1 数据安全制度

- 数据安全管理制度体系框架
- 数据安全责任制与追责机制
- 数据安全应急预案与事件管理制度

3.4.2 数据安全标准

- 国家标准：GB/T 35273《个人信息安全规范》、GB/T 37988《数据安全能力成熟度模型》
- 行业标准与团体标准
- 数据安全标准体系建设路径

3.4.3 数据安全策略

- 数据安全总体策略与子策略
- 数据分类分级保护策略
- 数据跨境传输安全策略

3.4.4 数据安全规范

- 数据安全操作规范与流程
- 数据共享与开放安全规范
- 第三方数据处理安全规范

3.4.5 数据安全规划

- 数据安全战略规划与路线图
- 数据安全能力建设规划
- 数据安全治理成熟度提升路径

四大知识类并非独立存在，而是形成基础支撑-技术落地-管理保障的闭环体系：信息安全知识是整体安全的通用基础，数据安全基础体系在此之上聚焦数据特性，为技术体系（具体防护手段）与治理体系（制度流程设计）提供底层支撑。技术体系侧重如何做（如用 DLP 技术防泄露），治理体系侧重谁来做、怎么做规范（如明确数据安全责任人、制定 DLP 部署标准），二者共同保障数据安全目标的实现。

四、高频考试试题及解析

以下 100 道试题覆盖 CISP-DSG 考试大纲四大知识类，包括信息安全知识、数据安全基础体系、数据安全技术体系和数据安全管理体系。每道题均标注所属知识域，并附有正确答案与详细解析。

4.1 信息安全知识（第 1-20 题）

第 1 题【信息安全保障】信息安全的核心目标 CIA 三要素不包括以下哪项？

- A. 保密性
- B. 完整性
- C. 可用性
- D. 不可否认性

正确答案：D

解析：CIA 三要素是指保密性（Confidentiality）、完整性（Integrity）和可用性（Availability）。不可否认性（Non-repudiation）是信息安全附加属性，不属于 CIA 三要素。此知识点属于信息安全保障基础知识，是 CISP-DSG 信息安全知识模块的基础内容。

第 2 题【信息安全保障】在信息安全保障框架中，PDR 模型的三个要素是指？

- A. 保护、检测、响应
- B. 策略、检测、恢复
- C. 防护、检测、恢复
- D. 策略、防御、响应

正确答案：A

解析：PDR 模型是信息安全保障的经典模型，由 Protection（保护）、Detection（检测）和 Response（响应）三个要素组成，强调安全是一个动态的、循环的过程。该模型体现了信息安全的动态保障思想。

第 3 题【信息安全支撑技术】以下哪种加密算法属于对称加密算法？

- A. RSA
- B. AES
- C. ECC
- D. DSA

正确答案：B

解析：AES（Advanced Encryption Standard）是典型的对称加密算法，加密和解密使用同一密钥。RSA 和 ECC 是非对称加密算法，DSA 是数字签名算法。对称加密算法具有加解密速度快的优点，适合大量数据的加密。

第 4 题【网络安全监管】《数据安全法》于何时正式施行？

- A. 2021 年 6 月 1 日
- B. 2021 年 9 月 1 日
- C. 2021 年 11 月 1 日
- D. 2022 年 1 月 1 日

正确答案：B

解析：《中华人民共和国数据安全法》于 2021 年 6 月 10 日经第十三届全国人民代表大会常务委员会第二十九次会议通过，并于 2021 年 9 月 1 日起正式施行。该法是数据安全领域的基础性法律，确立了数据分类分级保护制度。

第 5 题【网络安全监管】《个人信息保护法》规定，处理敏感个人信息应取得个人的？

- A. 默示同意
- B. 书面同意
- C. 单独同意
- D. 口头同意

正确答案：C

解析：根据《个人信息保护法》第二十九条规定，处理敏感个人信息应当取得个人的单独同意。法律、行政法规规定处理敏感个人信息应当取得书面同意的，从其规定。单独同意要求对敏感个人信息的处理进行专门告知并获取明确同意，不能与其他同意事项合并。

第 6 题【信息安全支撑技术】以下哪种访问控制模型是基于角色的访问控制？

- A. DAC
- B. MAC
- C. RBAC
- D. ABAC

正确答案：C

解析：RBAC（Role-Based Access Control）是基于角色的访问控制模型，通过将权限分配给角色，再将角色分配给用户来实现访问控制。DAC 是自主访问控制，MAC 是强制访问控制，ABAC 是基于属性的访问控制。RBAC 是当前企业中最常用的访问控制模型。

第 7 题【信息安全评估】信息安全风险评估中，风险由以下哪两种因素共同构成？

- 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

正确答案：C

解析：在信息安全风险评估中，风险由威胁和脆弱性两个因素共同构成。当威胁利用脆弱性时，就会产生安全事件，形成风险。风险评估的核心就是识别资产面临的威胁和存在的脆弱性，分析威胁利用脆弱性导致安全事件的可能性及影响。

第 8 题【信息安全支撑技术】数字签名的主要作用是？

- A. 加密数据
- B. 验证身份和不可否认性
- C. 防止数据泄露
- D. 提高传输速度

正确答案：B

解析：数字签名的主要作用是验证数据来源的身份真实性和提供不可否认性。数字签名利用非对称加密技术，发送方用私钥对数据摘要进行签名，接收方用公钥验证，确保数据未被篡改且确实来自声称的发送方。

第 9 题【网络安全监管】根据《网络安全法》，关键信息基础设施的运营者在境内收集和产生的个人信息和重要数据应当？

- A. 存储在境外
- B. 存储在境内，确需出境的需经安全评估
- C. 由第三方托管
- D. 无特殊要求

正确答案：B

解析：根据《网络安全法》第三十七条规定，关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估。

第 10 题【信息安全保障】IATF 信息保障技术框架强调的核心原则是？

- A. 纵深防御
- B. 最小权限
- C. 安全隔离
- D. 访问控制

正确答案：A

解析：IATF（Information Assurance Technical Framework）信息保障技术框架由美国国家安全局（NSA）制定，其核心原则是纵深防御（Defense in Depth）。该框架通过在人员、操作和技术三个层面部署多层安全防护措施，确保信息系统的安全性。

第 11 题【信息安全支撑技术】以下哪种哈希算法的输出为 128 位？

- A. SHA-256
- B. MD5
- C. SHA-512
- D. SHA-1

正确答案：B

解析：MD5（Message Digest Algorithm 5）的输出为 128 位（16 字节）。SHA-1 输出为 160 位，SHA-256 输出为 256 位，SHA-512 输出为 512 位。MD5 由于存在碰撞风险，目前不推荐用于安全敏感场景，但仍作为基础知识考察。

第 12 题【网络安全监管】我国数据安全领域的基础性法律是？

- A. 《网络安全法》
- B. 《数据安全法》
- C. 《个人信息保护法》
- D. 《密码法》

正确答案：B

解析：《数据安全法》是我国数据安全领域的基础性法律，于 2021 年 9 月 1 日正式施行。该法以准确定义数据、数据处理、数据安全为出发点，提出解决数据全生命周期中的数

据安全问题，确立了数据分类分级保护制度，是 CISP-DSG 网络安全监管知识域的核心法规。

第 13 题【信息安全评估】信息安全风险评估的第一步是？

- A. 威胁识别
- B. 脆弱性识别
- C. 资产识别
- D. 风险计算

正确答案：C

解析：信息安全风险评估的标准流程为：资产识别与分析、威胁识别、脆弱性识别、风险分析、风险处置。资产识别是第一步，需要识别和评估信息资产的价值，因为资产价值是计算风险大小的重要输入。

第 14 题【信息安全支撑技术】以下哪种认证方式属于多因素认证？

- A. 仅使用用户名和密码
- B. 密码+手机验证码
- C. 仅使用指纹
- D. 仅使用动态令牌

正确答案：B

解析：多因素认证（MFA）要求使用两个或以上不同类型的认证因素。认证因素分为三类：知识因素（你知道什么，如密码）、拥有因素（你拥有什么，如手机/令牌）和生物因素（你是什么，如指纹）。密码+手机验证码结合了知识因素和拥有因素，属于多因素认证。

第 15 题【信息安全保障】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

正确答案：A

解析：信息安全管理关注的核心是通过管理体系来防范各类安全威胁。虽然内部威胁同样重要，但信息安全管理的首要关注点是外部恶意攻击对组织信息资产的威胁，需要通过制度、流程和技术手段综合防范。

第 16 题【网络安全监管】《个人信息保护法》中，个人信息处理者处理个人信息应当遵循的原则不包括？

- A. 合法正当原则
- B. 公开透明原则
- C. 最小必要原则
- D. 成本效益原则

正确答案：D

解析：根据《个人信息保护法》第五条至第九条，个人信息处理应当遵循合法、正当、必要和诚信原则，公开透明原则，信息质量原则和安全保障原则。成本效益原则不属于个人信息处理的法定原则。

第 17 题【信息安全评估】等保 2.0 将信息系统安全保护等级分为几级？

- A. 3 级
- B. 4 级
- C. 5 级
- D. 6 级

正确答案：C

解析：信息安全等级保护 2.0（等保 2.0）将信息系统安全保护等级分为五级，从第一级（用户自主保护级）到第五级（专控保护级），级别越高，安全保护要求越严格。第三级以上系统需要进行年度测评。

第 18 题【信息安全支撑技术】PKI 体系中，CA 的全称是？

- A. 认证权威
- B. 证书颁发机构
- C. 密钥管理中心
- D. 注册机构

正确答案：B

解析：CA（Certificate Authority）即证书颁发机构，是 PKI（公钥基础设施）体系的核心组件，负责签发和管理数字证书。CA 通过验证证书申请者的身份，将公钥与持有者身份绑定，确保公钥的可信分发。

第 19 题【信息安全保障】PDCA 循环模型中 D 代表什么？

- A. 设计
- B. 部署

- C. 实施
- D. 检测

正确答案：C

解析：PDCA 循环模型由 Plan（计划）、Do（实施）、Check（检查）和 Act（改进）四个阶段组成。PDCA 是信息安全管理体的经典过程模型，通过持续循环实现安全管理水平的不断提升。

第 20 题【网络安全监管】国家建立数据安全什么制度，根据数据在经济社会发展中的重要程度进行分类分级保护？

- A. 数据审查制度
- B. 数据分类分级保护制度
- C. 数据出境审批制度
- D. 数据备案制度

正确答案：B

解析：根据《数据安全法》第二十一条规定，国家建立数据分类分级保护制度，根据数据在经济社会发展中的重要程度，以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益造成的危害程度，对数据实行分类分级保护。

4.2 数据安全基础体系（第 21-45 题）

第 21 题【数据安全基础知识】数据生命周期的正确顺序是？

- A. 创建、存储、传输、使用、共享、归档、销毁
- B. 采集、存储、处理、传输、共享、销毁
- C. 创建、使用、存储、传输、销毁、归档
- D. 采集、传输、处理、存储、销毁

正确答案：A

解析：数据生命周期通常包括七个阶段：创建（采集）、存储、传输、使用、共享、归档和销毁。每个阶段都面临不同的安全风险，需要实施相应的安全控制措施。数据全生命周期安全是 CISP-DSG 数据安全基础知识的核心内容。

第 22 题【数据安全基础知识】数据分类分级的常见分级方法不包括？

- A. 敏感性分级（秘密、机密、绝密）

- B. 司法监管分级（中国、美国、欧盟）
- C. 关键性分级（重要、内部、公开）
- D. 数据格式分级（文本、图像、视频）

正确答案：D

解析：数据分类分级的常见分级方法包括：按敏感性分级（秘密、机密、绝密）、按司法监管分级（不同国家/地区的法律要求）、按关键性分级（重要、内部、公开）。数据格式（文本、图像、视频）属于数据类型的分类，不是分级方法。

第 23 题【数据安全基础知识】根据《数据安全法》，数据分级分为哪三个层级？

- A. 公开数据、内部数据、敏感数据
- B. 一般数据、重要数据、核心数据
- C. 公共数据、企业数据、个人数据
- D. 基础数据、业务数据、战略数据

正确答案：B

解析：根据《数据安全法》及相关标准，数据分为一般数据、重要数据和核心数据三个层级。核心数据是关乎国家安全和公共利益的最高级别数据，重要数据涉及行业稳定和企业核心利益，一般数据为普通业务数据。这一分级体系是数据安全治理的基础。

第 24 题【数据安全基础知识】GB/T 37988《数据安全能力成熟度模型》(DSMM) 将数据安全能力分为几个等级？

- A. 3 个
- B. 4 个
- C. 5 个
- D. 6 个

正确答案：C

解析：GB/T 37988《数据安全能力成熟度模型》(DSMM) 将数据安全能力成熟度分为 5 个等级：等级 1 非正式执行、等级 2 计划跟踪、等级 3 充分定义、等级 4 量化控制、等级 5 持续优化。该模型是 CISP-DSG 数据安全基础知识的重要考察点。

第 25 题【数据安全基础知识】如果一个组织按照 DSMM 模型，具备以下特征：建立可测安全目标、客观地管理执行、建立了量化目标、安全过程可度量，那么它属于哪个等级？

- A. 等级 1，非正式执行
- B. 等级 2，计划跟踪
- C. 等级 3，充分定义

- D. 等级 4，量化控制

正确答案：D

解析：DSMM 等级 4 为量化控制级，其特征是：建立可测量的安全目标，客观地管理执行，建立了量化目标，安全过程可度量。该等级要求组织能够通过量化指标管理和改进数据安全过程，是较高成熟度等级。

第 26 题【数据安全基础知识】以下哪项不属于数据安全基本原则？

- A. 最小必要原则
- B. 目的限制原则
- C. 成本最优原则
- D. 公开透明原则

正确答案：C

解析：数据安全基本原则包括最小必要原则、目的限制原则、公开透明原则、合法正当原则、安全保障原则等。成本最优原则是经济管理领域的概念，不属于数据安全基本原则。

第 27 题【结构化数据应用】以下关于关系型数据库的描述，错误的是？

- A. 数据以表格形式存储
- B. 使用 SQL 语言进行数据操作
- C. 支持 ACID 事务特性
- D. 天然适合存储海量非结构化数据

正确答案：D

解析：关系型数据库以表格形式存储结构化数据，使用 SQL 语言操作，支持 ACID 事务特性。但关系型数据库不适合存储海量非结构化数据（如文档、图像、视频），这类数据通常使用 NoSQL 数据库或分布式文件系统（如 HDFS）来存储。

第 28 题【结构化数据应用】数据库管理工具的主要功能不包括？

- A. 备份数据库
- B. 数据库操作
- C. 附加数据库
- D. 数据建模

正确答案：D

解析：数据库管理工具的主要功能包括数据库备份与恢复、数据库操作（增删改查）、附加和分离数据库等。数据建模属于数据库设计阶段的专用工具功能，不属于数据库管理工具的日常管理功能。

第 29 题【非结构化数据应用】以下哪类数据属于非结构化数据？

- A. 关系型数据库中的表数据
- B. Excel 表格
- C. 视频文件
- D. XML 文件

正确答案：C

解析：非结构化数据是指没有预定义数据模型或不符合预定义数据模型的数据。视频文件属于典型的非结构化数据。关系型数据库表数据是结构化数据，Excel 表格和 XML 文件属于半结构化数据。

第 30 题【大数据应用】Hadoop 生态系统中，用于分布式文件存储的组件是？

- A. MapReduce
- B. HDFS
- C. HBase
- D. Hive

正确答案：B

解析：HDFS（Hadoop Distributed File System）是 Hadoop 生态系统中的分布式文件系统，负责海量数据的存储。MapReduce 是计算框架，HBase 是分布式数据库，Hive 是数据仓库工具。HDFS 是大数据存储的基础组件。

第 31 题【大数据应用】在 Hadoop 生态中，用于提供细粒度数据访问控制的开源组件是？

- A. Knox
- B. Ranger
- C. Falcon
- D. Flume

正确答案：B

解析：Apache Ranger 是 Hadoop 生态中提供细粒度数据访问控制的组件，支持对 HDFS、Hive、HBase 等组件的统一权限管理，可实现基于角色的访问控制和审计日志。Knox 是网关组件，Falcon 是数据治理组件，Flume 是日志采集组件。

第 32 题【数据安全基础知识】我国数据分类中，重要数据是指？

- A. 涉及个人隐私的数据
- B. 危害国家安全、公共利益的数据
- C. 企业内部业务数据
- D. 公开发布的数据

正确答案：B

解析：根据相关法规和标准，重要数据是指一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能危害国家安全、公共利益、生命财产安全、国家关键基础设施、扰乱市场秩序的数据。重要数据的保护要求高于一般数据。

第 33 题【数据安全基础知识】数据安全治理中，谁应承担数据安全的最终责任？

- A. IT 部门
- B. 安全部门
- C. 组织高级管理层
- D. 数据使用者

正确答案：C

解析：在数据安全治理中，组织的高级管理层（如董事会、CEO）应承担数据安全的最终责任。高级管理层负责制定数据安全战略、分配资源、建立问责机制。IT 部门和安全部门负责具体执行，数据使用者需遵守安全规范。

第 34 题【数据安全基础知识】数据分类分级的常见分类方法不包括？

- A. 监管合规分类
- B. 业务功能分类
- C. 数据大小分类
- D. 基于项目分类

正确答案：C

解析：常见的数据分类方法包括按监管合规分类、按业务功能分类、按功能单元分类和基于项目分类。数据大小不是数据分类的标准依据，数据分类应基于数据的内容、来源、用途和敏感程度等维度。

第 35 题【数据安全基础知识】数据安全风险评估应以什么为中心？

- A. 业务流程
- B. 人员管理
- C. 技术工具

- D. 合规要求

正确答案：A

解析：数据安全风险评估应以业务流程为中心。数据安全风险与业务流程紧密相关，通过分析数据在业务流程中的流转路径、处理方式和使用场景，才能准确识别数据安全风险并制定有效的防护措施。

第 36 题【结构化数据应用】SQL 注入攻击主要危害数据库的哪个安全属性？

- A. 保密性
- B. 完整性
- C. 可用性
- D. 以上都是

正确答案：D

解析：SQL 注入攻击可以危害数据库的多个安全属性：通过注入读取未授权数据危害保密性，通过注入修改或删除数据危害完整性，通过注入删除表或消耗资源危害可用性。因此 SQL 注入是数据库安全的重要威胁。

第 37 题【非结构化数据应用】以下哪种技术常用于非结构化数据的检索？

- A. SQL 查询
- B. 全文检索
- C. 表关联
- D. 索引扫描

正确答案：B

解析：非结构化数据（如文档、网页）通常使用全文检索技术进行检索，如 Elasticsearch、Lucene 等搜索引擎。SQL 查询和表关联适用于结构化数据，全文检索通过分词、倒排索引等技术实现非结构化数据的高效检索。

第 38 题【大数据应用】以下哪个不属于大数据的典型特征？

- A. 数据体量大
- B. 处理速度快
- C. 数据类型单一
- D. 价值密度低

正确答案：C

解析: 大数据的典型特征通常概括为 4V: Volume (数据体量大)、Velocity (处理速度快)、Variety (数据类型多样)、Value (价值密度低)。数据类型多样而非单一, 包括结构化、半结构化和非结构化数据。

第 39 题【数据安全基础知识】个人信息中, 能够单独识别自然人身份的信息属于?

- A. 间接个人信息
- B. 直接个人信息
- C. 敏感个人信息
- D. 匿名化信息

正确答案: B

解析: 个人信息分为直接个人信息和间接个人信息。直接个人信息是指能够单独识别自然人身份的信息 (如身份证号、手机号), 间接个人信息是指不能单独识别但与其他信息结合后可以识别自然人身份的信息。

第 40 题【数据安全基础知识】以下哪种信息属于敏感个人信息?

- A. 姓名
- B. 生物识别信息
- C. 通信记录
- D. 位置信息

正确答案: B

解析: 根据《个人信息保护法》第二十八条规定, 敏感个人信息包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息, 以及不满十四周岁未成年人的个人信息。生物识别信息 (如指纹、人脸) 属于敏感个人信息。

第 41 题【数据安全基础知识】数据安全治理中数据分类分级的挑战不包括?

- A. 缺乏对数据保护重要性的认知
- B. 缺乏数据分类分级技术与方法
- C. 缺乏数据安全治理制度和流程
- D. 缺乏足够的存储空间

正确答案: D

解析: 数据分类分级面临的主要挑战包括: 缺乏对数据保护重要性的认知、缺乏数据分类分级技术与方法、缺乏数据安全治理制度和流程。存储空间不足是技术运维问题, 不是数据分类分级的核心挑战。

第 42 题【数据安全基础知识】数据安全风险评估的第一步是？

- A. 数据资产识别与分析
- B. 数据应用场景识别
- C. 数据威胁识别
- D. 数据脆弱性识别

正确答案：A

解析：数据安全风险评估的标准流程为：数据资产识别与分析、数据应用场景识别、数据威胁识别、数据脆弱性识别、风险分析和风险处置。数据资产识别是第一步，需要全面梳理数据资产的分布、分类和价值。

第 43 题【大数据应用】在自然语言处理中，词法分析过程中，词的构成不包括？

- A. 动宾
- B. 动补
- C. 偏正
- D. 主动

正确答案：D

解析：自然语言处理中，汉语词法分析涉及的词的构成关系包括偏正结构、动宾结构、动补结构、并列结构等。主动不属于词法分析中的词构成关系类型，主动/被动是语态概念。

第 44 题【数据安全基础知识】Gartner 用以下哪个比喻来形容数据安全治理（DSG）在数据安全领域中的重要地位？

- A. 风暴之眼
- B. 安全基石
- C. 数据灯塔
- D. 安全盾牌

正确答案：A

解析：国际知名咨询机构 Gartner 用风暴之眼来比喻数据安全治理（DSG）在数据安全领域中的重要地位及作用，形象地说明了数据安全治理处于数据安全的核心位置，是数据安全工作的关键切入点。

第 45 题【数据安全基础知识】以下关于数据脱敏的说法，正确的是？

- A. 数据脱敏会完全破坏数据的可用性
- B. 数据脱敏后的数据无法用于任何业务

- C. 数据脱敏通过替换、掩码等方式保护敏感数据，同时保留业务可用性
- D. 数据脱敏等同于数据加密

正确答案：C

解析：数据脱敏通过对敏感数据进行替换、掩码、删除等处理，使处理后的数据无法直接识别原始信息，同时保留数据的业务可用性。数据脱敏与数据加密不同：脱敏通常不可逆，适用于测试和分析场景；加密可逆，适用于存储和传输场景。

4.3 数据安全技术体系（第 46-80 题）

第 46 题【数据防泄漏技术】DLP（数据防泄漏）技术按部署位置分类，不包括以下哪种？

- A. 终端 DLP
- B. 网络 DLP
- C. 云 DLP
- D. 物理 DLP

正确答案：D

解析：DLP 技术按部署位置分为终端 DLP（部署在工作站/终端）、网络 DLP（部署在网络出口）、邮件 DLP（监控邮件通道）和云 DLP（保护云端数据）。物理 DLP 不是标准分类，DLP 主要关注电子数据防泄漏。

第 47 题【数据库安全技术】数据库审计的核心目的是？

- A. 提高数据库性能
- B. 记录和分析数据库操作行为，发现违规访问
- C. 加密数据库中的数据
- D. 备份数据库

正确答案：B

解析：数据库审计的核心目的是记录和分析对数据库的所有访问和操作行为，通过对 SQL 语句的解析和审计，发现违规访问、异常操作和潜在的数据泄露行为，为事后追溯和合规检查提供证据。

第 48 题【数据防泄漏技术】对客户手机号采用部分掩码显示（如 138****5678）的技术属于？

- A. 数据加密
- B. 数据脱敏
- C. 数据备份

- D. 访问控制

正确答案：B

解析：对手机号进行部分掩码显示是数据脱敏技术的一种应用。数据脱敏通过对敏感数据进行替换、掩码、删除等处理，使处理后的数据无法直接识别原始信息，同时保留数据的业务可用性，适用于客服、数据分析等需要展示数据但不能泄露隐私的场景。

第 49 题【数据可用性保障】备份的指标 RTO 是指？

- A. 恢复点目标，指有效备份点到灾难之间的时间间隔
- B. 灾难发生后从系统宕机到业务恢复运营的时间段
- C. 数据备份的频率
- D. 备份文件的保留期限

正确答案：B

解析：RTO (Recovery Time Objective, 恢复时间目标)是指灾难发生后，从 IT 系统宕机导致业务停顿之刻开始，到业务恢复运营之时的时间段。RPO (Recovery Point Objective, 恢复点目标)是指灾难发生时，有效备份点到灾难之间的时间间隔。RTO 关注恢复速度，RPO 关注数据丢失量。

第 50 题【数据可用性保障】某云平台采用可用性区+跨区域复制策略，RPO=0、RTO<15min，该策略主要应对的风险是？

- A. 逻辑错误
- B. 单点故障
- C. 大规模自然灾害
- D. 内部人员恶意删除

正确答案：C

解析：RPO=0 意味着零数据丢失，RTO<15min 意味着快速恢复。跨区域复制策略将数据复制到不同地理区域，主要应对大规模自然灾害导致整个区域不可用的风险。可用性区应对单点故障，但无法应对区域级灾难。

第 51 题【数据库安全技术】数据库防火墙的主要功能是？

- A. 拦截异常 SQL 查询操作
- B. 加密数据库中的数据
- C. 备份和恢复数据库
- D. 管理数据库用户权限

正确答案：A

解析：数据库防火墙部署在数据库前端，通过解析和分析 SQL 语句，实时拦截异常查询、SQL 注入攻击、批量数据导出等危险操作。它与数据库审计的区别在于：审计是事后记录分析，防火墙是事前拦截防护。

第 52 题【数据防泄漏技术】静态脱敏与动态脱敏的主要区别是？

- A. 静态脱敏用于生产环境，动态脱敏用于测试环境
- B. 静态脱敏生成脱敏后的数据副本，动态脱敏在数据访问时实时脱敏
- C. 静态脱敏不可逆，动态脱敏可逆
- D. 静态脱敏安全性低，动态脱敏安全性高

正确答案：B

解析：静态脱敏是在数据使用前生成脱敏后的数据副本，适用于测试环境数据准备。动态脱敏是在用户访问数据时实时进行脱敏处理，不改变原始数据，适用于生产环境中不同角色看到不同脱敏程度的数据。两者各有适用场景。

第 53 题【大数据安全防护技术】在 Hadoop 生态中，Knox 网关的主要安全功能是？

- A. 细粒度访问控制
- B. 统一认证和网关代理
- C. 数据加密
- D. 审计日志

正确答案：B

解析：Apache Knox 是 Hadoop 生态中的统一网关组件，提供统一的认证、授权和代理服务。它作为 Hadoop 集群的统一入口，对外提供 REST API，隐藏内部集群拓扑。细粒度访问控制由 Ranger 负责，Knox 侧重于边界安全和统一认证。

第 54 题【大数据安全防护技术】以下哪种技术属于隐私计算技术？

- A. 数据脱敏
- B. 差分隐私
- C. 数据备份
- D. 访问控制

正确答案：B

解析：隐私计算技术包括差分隐私、同态加密、安全多方计算（MPC）、联邦学习等。差分隐私通过在查询结果中添加噪声来保护个体隐私，同时保留数据的统计特征。数据脱敏和访问控制是传统数据安全技术，不属于隐私计算范畴。

第 55 题【数据安全治理与保障框架】数据安全治理的核心思想是？

- A. 以技术为中心
- B. 以数据为中心
- C. 以网络为中心
- D. 以人员为中心

正确答案：B

解析：数据安全治理的核心思想是以数据为中心，区别于传统以网络边界为中心的安全防护模式。数据安全治理关注数据全生命周期的安全，从数据分类分级入手，建立覆盖管理、技术和运营的体系化安全保障框架。

第 56 题【数据安全评估】个人信息保护影响评估（PIA）的法律依据是？

- A. 《网络安全法》
- B. 《数据安全法》
- C. 《个人信息保护法》
- D. 《密码法》

正确答案：C

解析：个人信息保护影响评估（PIA）的法律依据是《个人信息保护法》第五十五条和第五十六条。该法规定，在处理敏感个人信息、向境外提供个人信息等特定情形下，个人信息处理者应当事前进行个人信息保护影响评估。

第 57 题【数据安全技术要求】在数据脱敏的可逆性要求中，若需支持业务回滚，应优先选择？

- A. 掩码
- B. 哈希加盐
- C. 格式保持加密
- D. 截断

正确答案：C

解析：当脱敏需要支持业务回滚时，应选择可逆的脱敏方法。格式保持加密（FPE）在保持数据格式不变的同时进行加密，可以通过解密恢复原始数据，适合需要回滚的场景。掩码、哈希加盐和截断通常不可逆。

第 58 题【数据安全运营要求】数据安全事件响应的四个阶段不包括？

- A. 准备阶段
- B. 检测阶段
- C. 分析阶段
- D. 恢复阶段

正确答案：C

解析：数据安全事件响应通常分为四个阶段：准备阶段（建立应急响应能力）、检测阶段（发现和确认安全事件）、遏制/根除/恢复阶段（处置事件并恢复业务）和总结阶段（事后分析和改进）。分析阶段不是一个独立的阶段，而是贯穿在检测和处置过程中。

第 59 题【数据可用性保障】数据备份策略中，增量备份的特点是？

- A. 每次备份所有数据
- B. 只备份自上次全量备份以来变化的数据
- C. 只备份自上次任意备份以来变化的数据
- D. 实时备份所有变化

正确答案：C

解析：增量备份只备份自上次任意类型备份（包括全量备份和增量备份）以来发生变化的数据。其优点是备份速度快、存储空间小，缺点是恢复时需要全量备份和所有增量备份，恢复时间较长。全量备份备份所有数据，差异备份备份自上次全量备份以来的变化。

第 60 题【数据库安全技术】数据库透明加密（TDE）的特点是？

- A. 需要修改应用程序代码
- B. 对应用程序透明，无需修改代码
- C. 只能加密特定字段
- D. 加密后无法进行查询

正确答案：B

解析：数据库透明加密（Transparent Data Encryption, TDE）在数据库引擎层对数据文件进行加密，对应用程序完全透明，无需修改应用代码。TDE 通常加密数据文件和日志文件，在读取时自动解密，写入时自动加密，提供静态数据保护。

第 61 题【数据防泄漏技术】DLP 系统通过以下哪种方式识别敏感数据？

- A. 仅通过文件名识别
- B. 通过内容识别技术，如关键词、正则表达式、数据指纹等
- C. 仅通过文件大小识别

- D. 仅通过文件类型识别

正确答案：B

解析：DLP 系统通过内容识别技术来识别敏感数据，常用方法包括：关键词匹配、正则表达式匹配（如身份证号、银行卡号模式）、数据指纹（对已知敏感数据生成指纹用于比对）、精确数据匹配（EDM）和文档分类等。仅靠文件名、大小或类型无法准确识别敏感数据。

第 62 题【大数据安全防护技术】Kerberos 认证协议使用的票据类型包括？

- A. 请求票据和服务票据
- B. 票据授予票据（TGT）和服务票据（ST）
- C. 认证票据和授权票据
- D. 临时票据和永久票据

正确答案：B

解析：Kerberos 认证协议使用两种票据：TGT（Ticket Granting Ticket，票据授予票据）由 AS（认证服务器）颁发，用于向 TGS 请求服务票据；ST（Service Ticket，服务票据）由 TGS（票据授予服务器）颁发，用于访问具体服务。Kerberos 是 Hadoop 生态常用的认证机制。

第 63 题【数据安全策略要求】数据分类分级安全策略要求对不同级别的数据实施？

- A. 相同的安全控制措施
- B. 不同的安全控制措施
- C. 仅对高级别数据实施控制
- D. 不需要实施控制

正确答案：B

解析：数据分类分级安全策略的核心是针对不同级别的数据实施不同强度的安全控制措施。高级别数据（如核心数据、重要数据）需要更严格的加密、访问控制和审计措施，低级别数据可以采用相对宽松的控制措施，实现安全与效率的平衡。

第 64 题【数据安全评估】数据安全风险评估中，采用 FAIR 模型量化风险时，损失事件频率需输入的参数不包括？

- A. 威胁事件频率
- B. 脆弱性
- C. 资产价值
- D. 控制有效性

正确答案：C

解析：FAIR（Factor Analysis of Information Risk）模型中，损失事件频率（LEF）由威胁事件频率（TEF）和脆弱性（Vuln）决定，控制有效性影响脆弱性。资产价值是计算损失幅度（LM）的输入参数，不属于损失事件频率的输入。

第 65 题【数据安全技术要求】数据脱敏技术中，将身份证号 44010619900101XXXX 处理为 440106XXXX 的方法属于？

- A. 掩码处理
- B. 泛化处理
- C. 匿名化处理
- D. 去标识化处理

正确答案：A

解析：掩码处理是将敏感数据的部分字符用特殊字符（如*或X）替换的脱敏方法。将身份证号的部分位数用X替换属于掩码处理。泛化处理是将具体值替换为更宽泛的类别（如将年龄替换为年龄段），匿名化和去标识化是更广泛的概念。

第 66 题【数据安全运营要求】数据安全审计的核心目的是？

- A. 提高系统性能
- B. 记录和追溯数据访问行为，确保合规性
- C. 加密敏感数据
- D. 防止网络攻击

正确答案：B

解析：数据安全审计的核心目的是全面记录和追溯数据的访问、修改、传输等操作行为，为合规检查、事后追溯和风险分析提供证据支持。通过审计日志可以发现异常访问模式、违规操作和潜在的数据泄露行为。

第 67 题【数据安全评测要求】数据安全能力成熟度评估的依据标准是？

- A. GB/T 22239（等保 2.0）
- B. GB/T 37988（DSMM）
- C. GB/T 35273（个人信息安全规范）
- D. ISO 27001

正确答案：B

解析：数据安全能力成熟度评估的依据标准是 GB/T 37988《数据安全能力成熟度模型》（DSMM）。该标准定义了数据安全能力的 5 个成熟度等级和评估方法。等保 2.0（GB/T 22239）是信息系统安全等级保护标准，与 DSMM 关注维度不同。

第 68 题【大数据安全防护技术】以下关于同态加密的说法，正确的是？

- A. CKKS 方案支持精确整数运算
- B. BGV 方案支持浮点数近似运算
- C. Paillier 支持无限次乘法同态
- D. BFV 方案属于 Leveled FHE

正确答案：D

解析：BFV（Brakerski-Fan-Vercauteren）方案属于 Leveled FHE（层级全同态加密），支持有限深度的同态运算。CKKS 支持浮点数近似运算而非精确整数运算，BGV 支持整数运算而非浮点数，Paillier 仅支持加法同态和有限次标量乘法，不支持无限次乘法同态。

第 69 题【数据可用性保障】异地备份中心的核心目的是？

- A. 与生产中心不在同一城市
- B. 与生产中心距离 100 公里以上
- C. 与生产中心距离 200 公里以上
- D. 减少与生产中心面临相同区域性风险的机率

正确答案：D

解析：异地备份中心的核心目的是减少与生产中心面临相同区域性风险的概率。建立异地备份中心不仅仅是距离要求，更重要的是确保备份中心与生产中心不会同时受到同一区域性灾害（如地震、洪水）的影响。

第 70 题【数据库安全技术】数据库管理员对部分数据表实施去除规范化操作来提高数据库性能，这样做将增加下列哪项风险？

- A. 访问的不一致
- B. 数据泄露
- C. SQL 注入
- D. 权限提升

正确答案：A

解析：去除规范化（Denormalization）通过冗余存储数据来提高查询性能，但会导致同一数据在多处存储，增加了数据不一致的风险。当一处数据更新时，其他冗余副本可能未同步更新，导致访问到不一致的数据。

第 71 题【数据防泄漏技术】以下哪种场景最适合使用动态脱敏？

- A. 为测试环境准备数据
- B. 为开发团队提供脱敏数据副本
- C. 生产环境中不同角色访问同一数据时看到不同脱敏程度
- D. 数据归档

正确答案：C

解析：动态脱敏适合在生产环境中，当不同角色的用户访问同一数据时，根据角色权限实时展示不同脱敏程度的数据。静态脱敏适合为测试和开发环境准备脱敏数据副本。动态脱敏不改变原始数据，仅在展示时进行脱敏处理。

第 72 题【数据安全治理与保障框架】数据安全治理与信息安全管理的主要区别是？

- A. 数据安全治理只关注技术，信息安全管理只关注管理
- B. 数据安全治理以数据为中心，信息安全管理以系统/网络为中心
- C. 数据安全治理是信息安全管理的一部分
- D. 两者没有区别

正确答案：B

解析：数据安全治理以数据为中心，关注数据全生命周期的安全，从数据分类分级入手建立防护体系。信息安全管理以系统和网络为中心，关注信息系统的安全保障。数据安全治理不是信息安全管理的一部分，而是独立的、以数据为核心的安全体系。

第 73 题【数据安全策略要求】针对个人信息数据制定的防护策略应包含？

- A. 最小权限+加密传输
- B. 最大权限+明文传输
- C. 最小权限+明文存储
- D. 无需特殊策略

正确答案：A

解析：针对个人信息数据应制定最小权限+加密传输的防护策略。最小权限原则确保只有必要的人员才能访问个人信息，加密传输确保数据在传输过程中不被窃取。此外还应包括数据脱敏、访问审计等措施，形成多层次的防护体系。

第 74 题【数据安全评估】数据安全风险评估中，资产价值的评估维度不包括？

- A. 数据对业务的支撑程度
- B. 数据泄露后的经济损失
- C. 数据的存储介质类型
- D. 数据涉及的个人信息数量

正确答案：C

解析：数据资产价值评估维度包括：数据对业务的支撑程度（业务价值）、数据泄露后的经济损失（经济影响）、数据涉及的个人信息数量和敏感程度（合规影响）。数据的存储介质类型是技术属性，不直接反映数据资产的安全价值。

第 75 题【大数据安全防护技术】差分隐私技术中，若查询函数全局敏感度为 Δ ，隐私预算为 ϵ ，则拉普拉斯机制所需噪声尺度参数为？

- A. ϵ/Δ
- B. Δ/ϵ
- C. $\epsilon*\Delta$
- D. $\sqrt{\epsilon*\Delta}$

正确答案：B

解析：在差分隐私的拉普拉斯机制中，噪声尺度参数 $b = \Delta/\epsilon$ ，其中 Δ 是查询函数的全局敏感度， ϵ 是隐私预算。隐私预算 ϵ 越小，隐私保护越强，但添加的噪声越大，数据可用性越低。

第 76 题【数据安全技术要求】采用 AES-GCM 模式对数据加密时，若初始化向量（IV）重复，直接导致的安全问题是？

- A. 密钥泄露
- B. 明文可被重放
- C. 完整性校验失效并可被重放
- D. 加密速度变慢

正确答案：C

解析：AES-GCM 是一种认证加密模式，同时提供机密性和完整性保护。如果 IV 重复使用，攻击者可以通过异或操作推导明文关系，导致完整性校验失效并可能被重放攻击。因此 GCM 模式严格要求 IV 不可重复使用。

第 77 题【数据安全运营要求】数据安全事件的严重等级划分依据不包括？

- A. 影响范围

- B. 经济损失
- C. 社会影响
- D. 响应时间

正确答案：D

解析：数据安全事件严重等级通常根据影响范围（受影响的数据量和用户数）、经济损失（直接和间接损失）、社会影响（对公共利益和社会秩序的影响）来划分。响应时间是事件处置的时效要求，不是事件等级的划分依据。

第 78 题【数据安全评测要求】数据安全合规评测的依据不包括？

- A. 法律法规
- B. 行业标准
- C. 企业内部制度
- D. 市场竞争策略

正确答案：D

解析：数据安全合规评测的依据包括：法律法规（如《数据安全法》《个人信息保护法》）、行业标准（如 GB/T 35273）、企业内部制度（如数据安全管理制度）。市场竞争策略属于商业决策，不属于合规评测的依据。

第 79 题【数据库安全技术】数据库审计日志管理功能不包括？

- A. 防止审计员误删审计记录，审计日志必须先转储后删除
- B. 对转储的审计记录提供完整性和机密性保护
- C. 对数据库中的数据进行加密管理
- D. 只允许审计员查阅和转出审计记录

正确答案：C

解析：数据库审计日志管理功能包括：防止审计员误删审计记录（日志先转储后删除）、对转储记录提供完整性和机密性保护、限制审计记录的查阅和转出权限。对数据库中的数据进行加密管理属于数据库加密功能，不属于审计日志管理功能。

第 80 题【大数据安全防护技术】在 SparkSQL 中，开启列级加密后，执行下列哪类操作会导致明文泄露？

- A. `select aes_decrypt(col) from t`
- B. `select col from t where id=1`
- C. `cache table t`
- D. `explain select col from t`

正确答案：C

解析：在 SparkSQL 中开启列级加密后，使用 cache table 操作会将解密后的明文数据缓存到内存中，可能导致明文泄露。select aes_decrypt(col)是显式解密操作，select col 返回密文，explain 只显示执行计划不涉及数据访问。缓存操作需要特别注意明文泄露风险。

4.4 数据安全管理体系（第 81-100 题）

第 81 题【数据安全制度】数据安全管理制度体系的核心是？

- A. 技术工具
- B. 责任制
- C. 审计报告
- D. 培训计划

正确答案：B

解析：数据安全管理制度体系的核心是责任制，明确各级人员的数据安全职责，建立从决策层到执行层的责任链条。制度体系还应包括数据分类分级管理制度、数据全生命周期管理制度、数据安全事件响应制度等。

第 82 题【数据安全标准】GB/T 35273《信息安全技术 个人信息安全规范》属于哪类标准？

- A. 强制性国家标准
- B. 推荐性国家标准
- C. 行业标准
- D. 团体标准

正确答案：B

解析：GB/T 35273 是推荐性国家标准（GB/T 中的 T 代表推荐）。该标准规定了个人信息处理活动中个人信息安全的原则、要求和方法，虽为推荐性标准，但在实际数据安全治理实践中被广泛参照和采用。

第 83 题【数据安全策略】数据跨境传输安全策略要求，重要数据出境时运营者应当报经谁批准？

- A. 行业主管部门
- B. 国家数据安全工作协调机制
- C. 省级数据安全监管部门
- D. 公安机关网络安全部门

正确答案：B

解析：根据《数据安全法》第三十一条规定，重要数据出境时，运营者应当按照规定报国家数据安全工作协调机制批准。关键信息基础设施运营者和处理重要数据的处理者出境数据，需通过国家网信部门的安全评估。

第 84 题【数据安全规范】以下哪种场景不属于个人信息最小必要原则的应用？

- A. 购物 APP 仅收集姓名、手机号、收货地址完成下单
- B. 健康类 APP 要求用户提供婚姻状况信息
- C. 银行 APP 仅获取位置信息用于附近网点查询
- D. 教育类 APP 收集学生姓名、课程成绩用于教学管理

正确答案：B

解析：最小必要原则要求收集的个人信息类型应与处理目的直接相关，且不超过实现处理目的的最小范围。健康类 APP 要求用户提供婚姻状况信息与健康管理无直接关联，违反了最小必要原则。其他选项收集的信息均与其业务目的直接相关。

第 85 题【数据安全规划】数据安全治理成熟度提升路径通常遵循的顺序是？

- A. 评估现状-制定规划-实施建设-持续改进
- B. 制定规划-评估现状-实施建设-持续改进
- C. 实施建设-评估现状-制定规划-持续改进
- D. 持续改进-评估现状-制定规划-实施建设

正确答案：A

解析：数据安全治理成熟度提升的标准路径是：首先评估现状（了解当前数据安全能力成熟度等级），然后制定规划（明确目标和路线图），接着实施建设（落实安全控制措施），最后持续改进（通过 PDCA 循环不断优化）。

第 86 题【数据安全制度】数据安全责任矩阵中 R 代表？

- A. 责任人
- B. 审批人
- C. 咨询人
- D. 知情人

正确答案：A

解析：数据安全责任矩阵通常采用 RACI 模型：R（Responsible）责任人负责执行任务，A（Accountable）审批人对结果负责，C（Consulted）咨询人提供专业意见，I（Informed）知情人需被告知结果。

第 87 题【数据安全标准】数据安全能力成熟度模型（DSMM）中，等级 3 充分定义级的特征是？

- A. 安全过程不可定义，依赖个人能力
- B. 定义了安全过程并能够跟踪执行
- C. 安全过程被充分定义、文档化并标准化执行
- D. 安全过程可量化测量和优化

正确答案：C

解析：DSMM 等级 3 充分定义级的特征是：数据安全过程被充分定义、文档化并标准化执行，组织层面建立了标准化的数据安全流程和规范。等级 1 是非正式执行，等级 2 是计划跟踪，等级 4 是量化控制，等级 5 是持续优化。

第 88 题【数据安全策略】数据安全总体策略应包含的核心要素不包括？

- A. 数据安全目标
- B. 数据安全组织架构
- C. 数据分类分级原则
- D. 具体技术产品型号

正确答案：D

解析：数据安全总体策略应包含数据安全目标、数据安全组织架构与责任、数据分类分级原则、数据安全控制要求等核心要素。具体技术产品型号属于实施层面的技术选型，不属于总体策略层面应规定的内容。

第 89 题【数据安全规范】第三方数据处理安全规范要求，委托第三方处理数据时应当？

- A. 直接将数据交给第三方无需约束
- B. 签订数据处理协议，明确安全责任和义务
- C. 仅口头约定数据处理要求
- D. 由第三方自行决定安全措施

正确答案：B

解析：根据《个人信息保护法》等法规要求，委托第三方处理数据时，应当与受托方签订数据处理协议，明确双方的数据安全责任和义务，包括数据处理目的、方式、安全措施、数据删除要求等。协议是约束第三方数据处理行为的重要法律保障。

第 90 题【数据安全规划】数据安全战略规划应与什么对齐？

- A. 仅与 IT 战略对齐
- B. 仅与安全战略对齐
- C. 与组织整体业务战略对齐
- D. 与行业趋势对齐

正确答案：C

解析：数据安全战略规划应与组织整体业务战略对齐。数据安全不是孤立的 IT 或安全问题，而是服务于业务发展的保障措施。只有与业务战略对齐，才能确保数据安全投入与业务需求匹配，实现安全与业务的协同发展。

第 91 题【数据安全制度】数据安全事件报告的时限要求通常是发现后？

- A. 24 小时内
- B. 48 小时内
- C. 72 小时内
- D. 7 个工作日内

正确答案：A

解析：根据相关法规要求，发生数据安全事件时，数据处理者应当立即采取处置措施，并在发现后 24 小时内向有关主管部门报告。事件报告应包括事件类型、影响范围、处置措施等内容。及时报告是数据安全事件管理的重要法定义务。

第 92 题【数据安全标准】以下哪个标准不是数据安全领域的国家标准？

- A. GB/T 35273《个人信息安全规范》
- B. GB/T 37988《数据安全能力成熟度模型》
- C. GB/T 22239《网络安全等级保护基本要求》
- D. GB/T 19001《质量管理体系》

正确答案：D

解析：GB/T 19001 是质量管理体系标准，不属于数据安全领域。GB/T 35273 是个人信息安全规范，GB/T 37988 是数据安全能力成熟度模型，GB/T 22239 是网络安全等级保护基本要求，这三者都与数据安全直接相关。

第 93 题【数据安全策略】数据全生命周期安全策略中，数据销毁环节应采取的措施不包括？

- A. 选择合适的销毁方式（物理销毁/逻辑销毁）
- B. 记录销毁过程
- C. 销毁后进行数据恢复测试确认

- D. 将数据备份后永久保留在云端

正确答案：D

解析：数据销毁环节应选择合适的销毁方式（物理或逻辑销毁）、记录销毁过程以备审计、必要时进行销毁后验证确保数据不可恢复。将数据备份后永久保留在云端违背了数据销毁的目的，数据销毁意味着数据应被彻底删除且不可恢复。

第 94 题【数据安全规范】数据共享与开放安全规范要求，在数据共享前应进行？

- A. 直接共享无需评估
- B. 数据安全风险评估和脱敏处理
- C. 仅通知数据所有者
- D. 仅加密后共享

正确答案：B

解析：数据共享与开放前应进行数据安全风险评估，识别共享数据中的敏感信息，并根据评估结果进行相应的脱敏或匿名化处理。同时需要签订数据共享协议，明确双方安全责任，确保数据在共享过程中的安全。

第 95 题【数据安全规划】数据安全能力建设规划中，应优先建设的内容是？

- A. 最先进的安全技术产品
- B. 数据分类分级体系和数据资产盘点
- C. 大规模安全团队
- D. 完善的办公环境

正确答案：B

解析：数据安全能力建设应优先进行数据分类分级体系和数据资产盘点。数据分类分级是数据安全治理的基础，只有清晰了解数据的分布、分类和级别，才能有针对性地部署安全控制措施。盲目采购技术产品或扩充团队而不了解数据现状是低效的。

第 96 题【数据安全制度】数据安全培训的内容不包括？

- A. 法律法规要求
- B. 技术防护措施
- C. 应急响应流程
- D. 产品营销策略

正确答案：D

解析：数据安全培训内容应包括法律法规要求（如《数据安全法》《个人信息保护法》）、技术防护措施（如加密、脱敏、访问控制）、应急响应流程、数据安全管理制度和操作规范等。产品营销策略属于业务培训范畴，不属于数据安全培训内容。

第 97 题【数据安全标准】数据安全管理体系的文档化要求中，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

正确答案：A

解析：数据安全管理体系文档通常分为四层：第一层是方针政策（顶层策略文件），第二层是工作程序（管理流程和制度），第三层是作业指导书（具体操作规范），第四层是工作记录（执行证据）。第一层文件是整个体系的纲领性文件。

第 98 题【数据安全策略】建立数据安全管理体系的第一步是？

- A. 风险评估
- B. 设计体系文档
- C. 明确数据安全管理体系范围
- D. 确定安全策略

正确答案：C

解析：建立数据安全管理体系的第一步是明确体系范围，确定哪些业务、系统、数据和人员纳入管理体系覆盖范围。在明确范围后，才能进行风险评估、设计文档和制定策略。范围定义决定了后续工作的边界和资源配置。

第 99 题【数据安全规范】根据《个人信息保护法》，个人在个人信息处理中拥有的权利不包括？

- A. 知情同意权
- B. 删除权
- C. 不予提供权
- D. 永久控制权

正确答案：D

解析：根据《个人信息保护法》，个人享有知情权和决定权、查阅复制权、更正补充权、删除权、请求解释权等。个人有权拒绝处理者处理其个人信息（不予提供权）。但永久控制权不是法定权利，个人信息处理者在合法合规前提下可以处理个人信息。

第 100 题【数据安全规划】CISP-DSG 认证证书的有效期和维持费用是？

- A. 5 年，每年 500 元
- B. 3 年，每年 500 元共 1500 元
- C. 终身有效，无需维持
- D. 1 年，每年 2000 元

正确答案：B

解析：CISP-DSG 证书有效期为三年。到期后，学员可向授权维持机构提交维持申请表，并缴纳维持费用每年 500 元，三年共 1500 元。持证人员需要在有效期内持续从事数据安全相关工作，并完成必要的继续教育。

参考来源

- [1] 中国信息安全测评中心. 注册数据安全治理专业人员(CISP-DSG)白皮书. 2019.
- [2] 天融信. CISP-DSG(数据安全治理)课程大纲. topsec.com.cn.
- [3] 《中华人民共和国数据安全法》. 2021 年 9 月 1 日施行.
- [4] 《中华人民共和国个人信息保护法》. 2021 年 11 月 1 日施行.
- [5] 《中华人民共和国网络安全法》. 2017 年 6 月 1 日施行.
- [6] GB/T 37988-2019《数据安全能力成熟度模型》.
- [7] GB/T 35273-2020《信息安全技术 个人信息安全规范》.
- [8] 安恒信息. 注册数据安全治理专业人员 CISP-DSG 认证培训. dbappsecurity.com.cn.
- [9] 中培伟业. CISP-DSG 认证考试内容与难度分析. zpedu.com. 2025.
- [10] 谷安天下. CISP-DSG 数据安全治理培训资料. 2025.