数据安全100问

编制：合规社

2024年2月18日

前 言

在数字化浪潮席卷全球的今天，数据成为了企业和个人最宝贵的资产之一。随之而来的，是对数据安全的关注也达到了前所未有的高度。《数据安全100问》从基础概念到深入实践，从技术细节到管理策略，涵盖了数据安全领域的重要方面。在这本问答手册中，我们精心设计了100个问题，希望能够引导大家逐步构建起对数据安全的深入理解，并在实际工作中能够有效地识别和防范安全风险。

目录

contents

目录

contents

01 问：什么是数据安全，法律上如何定义？

- 通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

- 数据安全有对立的两方面的含义：一是数据本身的安全，主要是指采用现代密码算法对数据进行主动保护，如数据保密、数据完整性、双向强身份认证等，二是数据防护的安全，主要是采用现代信息存储手段对数据进行主动防护，如通过磁盘阵列、数据备份、异地容灾等手段保证数据的安全，数据安全是一种主动的保护措施，数据本身的安全必须基于可靠的加密算法与安全体系，主要是有对称算法与公开密钥密码体系两种。

发布日期	法律政策/ 标准文件	定义
2021.6.10	《中华人民共和国数据安全法》	通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。
2019.8.30	《信息安全技术 数据安全能力成熟度模型（GB/T 37988-2019）》	通过管理和技术措施，确保数据有效保护和合规使用的状态。
2022.4.15	《信息安全技术 网络数据处理安全要求（GB/T 41479-2022）》	通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

02 问：数据安全有哪些基本特征?

数据安全原则

- **机密性（Confidentiality）**
  - 确保信息仅对授权个人或系统可用或可见。机密性的保护措施旨在防止敏感数据被未授权访问或泄露。
- **完整性（Integrity）**
  - 保证信息和数据在创建、存储、传输和处理过程中的准确性和完整性未被未授权地篡改。完整性措施确保数据在其生命周期内保持真实、未被更改。
- **可用性（Availability）**
  - 确保数据和信息系统在需要时可被授权用户访问和使用。可用性涉及到确保系统、网络和应用程序能够抵御攻击、故障和灾难，保持运行和响应。
- **可审计性（Auditability）**
  - 指数据和操作可以被检查和审计，以验证是否遵循了相应的安全策略和控制措施。通过审计日志和记录，可以追踪数据的访问和处理，便于事后分析和取证。
- **责任性（Accountability）**
  - 确保所有对数据和系统的操作都可以追溯到特定的个体。这通过身份验证、访问控制和审计日志等手段实现，以确保用户对其行为负责。
- **非否认性（Non-repudiation）**
  - 确保数据的发送者和接收者不能否认已发送或接收过数据。这通常通过数字签名和加密技术实现，为电子交易和通信提供法律上的凭据。
- **真实性（Authenticity）**
  - 确保数据、事务和通信的参与者是真实的，未被冒充。这通常通过身份验证机制实现，如使用密码、数字证书和双因素认证等。

03 问：什么是数据全生命周期?

- 数据全生命周期是指数据从创建或收集开始，直至销毁结束的整个过程。

数据采集	数据传输	数据存储	数据处理	数据交换	数据销毁
• 数据采集是指从各种来源获取数据的过程。	• 将数据从一个位置移动到另一个位置的过程。	• 将数据保存在某种形式的存储介质上的过程。	• 组织在内部对数据进行计算、分析、可视化等操作的阶段。	• 组织与组织或个人进行数据交换的阶段。	• 对数据及数据存储媒体通过相应的操作手段，使数据彻底删除且无法通过任何手段恢复的过程。

04 问：什么是数据采集，包含哪些采集方式?

- 数据采集是指从各种来源获取数据的过程，包括直接从用户输入、通过自动化工具收集网络数据、从第三方服务获取等。

数据采集方式

自动化数据采集

- **API收集**：通过应用程序编程接口自动从其他系统或服务获取数据。
- **网络抓取**：使用网络爬虫技术从网页抓取信息。
- **日志文件分析**：自动从系统和应用的日志文件中提取数据。
- **物联网设备**：从连接互联网的设备和传感器自动收集数据。

人工数据采集

- **在线和数字表单**：通过网站和应用程序的表单收集用户手动输入的数据。
- **调查和访谈**：通过问卷、电话或面对面访谈收集信息。
- **移动数据采集**：使用移动设备在现场手动输入或捕捉数据。

第三方和公共数据源

- **社交媒体数据**：从社交媒体平台收集公开分享的数据。
- **公共记录和数据库**：从政府、机构或商业数据库中获取公开可用的数据集。
- **交易数据**：从电子交易记录中提取数据。

高级技术数据采集

- **遥感技术**：利用卫星图像和遥感设备收集地理和环境数据。
- **传感器数据采集**：使用专业传感器收集特定环境或设备的数据。

05 问：什么是数据传输，有哪些传输方式?

- 数据传输是指将数据从一个位置移动到另一个位置的过程，可以是内部系统间的传输，也可以是与外部实体的数据交换。

内部传输

系统间传输
数据在不同的内部系统或平台之间移动，例如，从CRM系统传输到财务系统。

网络内传输
数据在组织内部的网络中传输，比如局域网中的数据共享。

部门间传输
不同部门之间的数据交换，如销售部门与市场部门之间共享客户信息。

外部传输

与合作伙伴的数据交换
与业务合作伙伴共享或接收数据，可能涉及合作项目、共同研究等。

供应商数据传输
将数据发送给供应商或从供应商处接收数据，如订单信息、库存数据等。

客户数据传输
与客户之间的数据交换，包括订单处理、客户支持和服务提供等。

云服务和外部存储
将数据上传到云服务或外部存储解决方案，或从这些服务中检索数据。

06 问：什么是数据出境，主动和被动是指什么？

数据主动出境

- 数据处理者将在境内运营中收集和产生的数据**传输**、**存储**至境外；

数据被动出境

- 数据处理者收集和产生的数据存储在境内，境外的机构、组织或者个人可以查询、调取、下载、导出；

其他情形

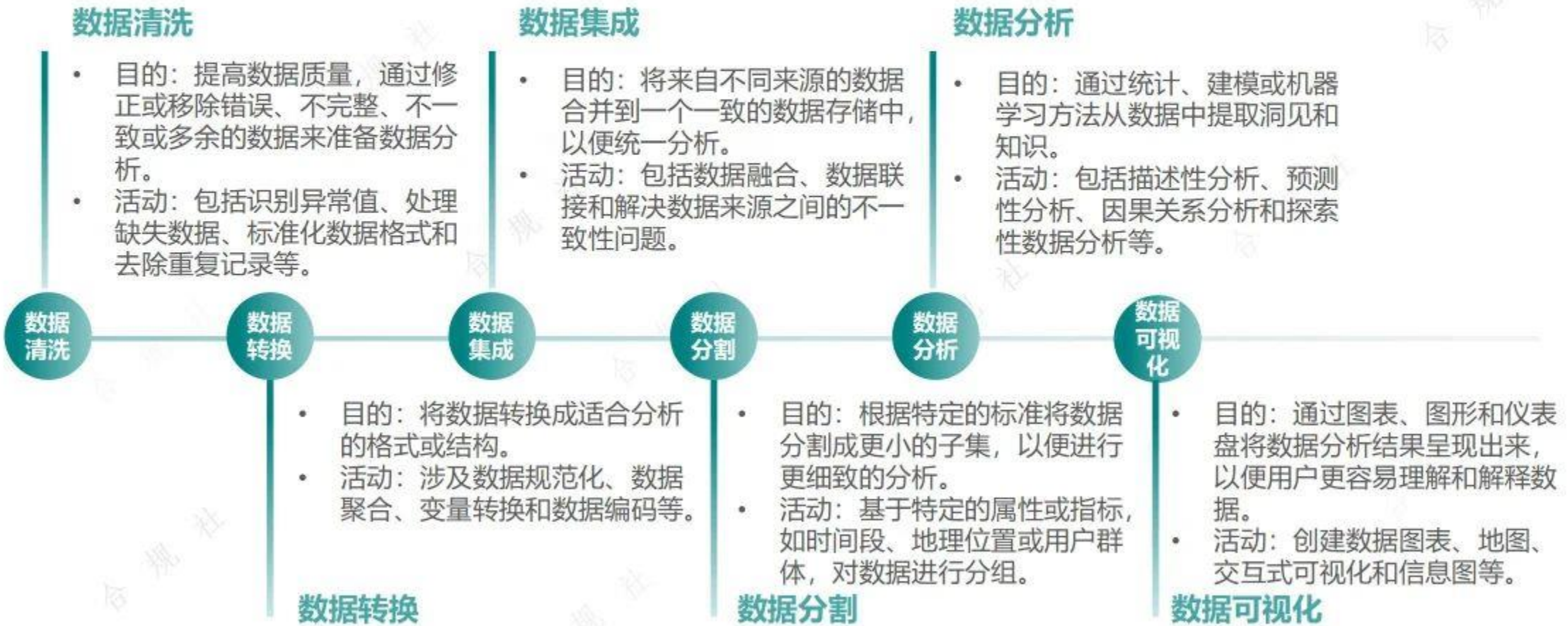
- 国家网信办规定的其他数据出境行为。

07 问：什么是数据存储，一般有哪些存储介质?

- 数据存储是指将数据保存在某种形式的存储介质上的过程，无论是物理的（如硬盘、USB驱动器）还是数字的（如云存储服务）。

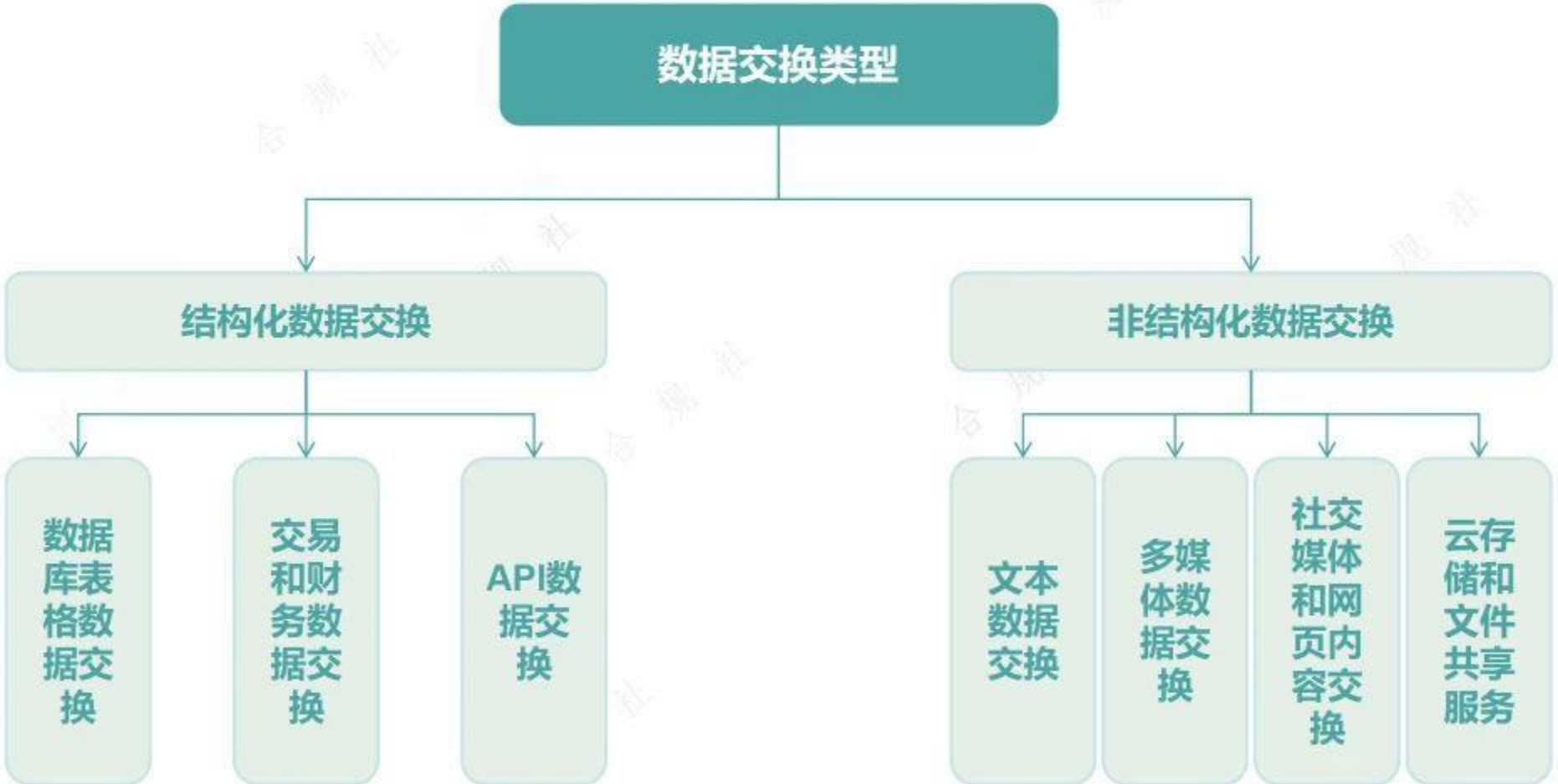
08 问：什么是数据处理，包含哪些关键环节？

- 数据处理是指组织在内部对数据进行计算、分析、可视化等操作的阶段。



09 问：什么是数据交换，有哪些数据交换类型？

- 数据交换是指组织与组织或个人进行数据交换的阶段。



10 问：什么是数据销毁，有哪些数据销毁方式？

- 数据销毁对数据及数据存储媒体通过相应的操作手段，使数据彻底删除且无法通过任何手段恢复的过程。

数据销毁方式	方法
物理销毁	• **粉碎：**使用专业的粉碎机将硬盘驱动器、CD/DVD和其他存储介质物理粉碎成碎片，使其无法再使用。 • **切割：**物理切割或在硬盘等存储介质上钻孔，破坏存储介质，使数据无法读取。 • **燃烧：**在受控环境中燃烧存储介质，完全破坏其物理形态以及其中的数据。 • **退磁：**使用退磁器消除磁性存储介质（如硬盘和磁带）的磁性信号，使数据无法恢复。
逻辑销毁	• **数据擦除：**通过专门的软件工具将存储介质上的所有数据覆写一次或多次，使用无意义的数据替换原有数据，确保原数据无法恢复。 • **加密和销毁密钥：**对数据进行加密处理，并销毁用于加密的密钥。没有密钥，加密数据实际上变得无法解析，相当于被销毁。 • **格式化：**对存储介质进行高级格式化，删除存储上的所有文件系统和数据。需要注意的是，标准格式化可能无法彻底销毁数据，高级或安全格式化选项通常更为彻底。

目录

contents

11 问：数据安全面临的内部威胁主要有哪些？

- 数据安全的内部威胁主要来源于组织内部，包括员工、业务伙伴或任何有系统访问权限的人。这些威胁可能是有意的，也可能是无意的，但都有可能对组织的数据安全造成严重影响。

内部威胁的常见形式

恶意行为

- 故意泄露、窃取或破坏组织的敏感数据和知识产权，可能是出于报复、贪婪或其他个人动机。
- 故意安装恶意软件或其他恶意代码，破坏组织的系统和数据。

疏忽或无意的错误

- 由于疏忽或缺乏安全意识，无意中泄露敏感信息，如通过不安全的网络连接发送敏感数据，或将敏感文件遗留在公共场所。
- 遵循不安全的工作实践，如使用弱密码、共享账户凭证或未锁定在非监管区域留下的设备。

利用内部权限

- 滥用授予的访问权限，访问无正当业务理由查看的敏感信息。
- 未经授权修改、删除或导出敏感数据。

社会工程学

- 内部人员可能成为外部攻击者社会工程学策略（如钓鱼攻击）的目标，无意中协助攻击者获取对组织系统的访问。

退出威胁

- 离职员工在离开组织时可能会带走敏感信息，或在离开前故意对组织的数据和系统造成损害。

12 问：什么是恶意软件，常见类型有哪些?

- 恶意软件，是设计用来损害、干扰、窃取或以其他方式对计算机系统、网络或设备造成不良影响的任何软件。它可以以多种形式出现，每种类型都有其特定的行为、传播方式和破坏手段。

13 问：什么是社会工程学攻击，有哪些常见攻击手段?

定义

- 社会工程攻击，是一种利用"社会工程学" 来实施的网络攻击行为。在计算机科学中，社会工程学指的是通过与他人的合法地交流，来使其心理受到影响，做出某些动作或者是透露一些机密信息的方式。这通常被认为是一种欺诈他人以收集信息、行骗和入侵计算机系统的行为。

社会工程学攻击的常见手段

网络钓鱼	捕鲸攻击	诱饵
转移盗窃	商业电子邮件妥协	短信钓鱼
交易交换	编造借口	蜜罐陷阱
尾随/搭便车	诱骗电话	冒充

14 问：网络钓鱼攻击常用哪些手段?

欺骗性电子邮件

- 攻击者发送伪造的电子邮件，看起来好像来自合法的公司（如银行、社交媒体平台或公司内部IT部门），要求用户更新账户信息、验证身份或更改密码，常常附带一个指向恶意网站的链接。

欺骗性链接

- 邮件中的链接可能看起来指向合法网站，但实际上会重定向到攻击者控制的恶意网站。有时，链接使用短网址服务进行掩饰，使得目标难以看出实际目的地。

恶意附件

- 钓鱼邮件可能包含恶意附件，如文档、PDF或可执行文件，一旦打开，就可能安装恶意软件（如勒索软件、间谍软件）到用户的设备上。

社交媒体钓鱼

- 攻击者在社交媒体平台上创建假账户，或者劫持真实账户，然后向受害者发送包含恶意链接或请求的私信。

冒充品牌和组织

- 攻击者常常通过仿冒知名品牌或机构的方式来增加钓鱼邮件的可信度，使用官方的徽标、设计和语言风格，使邮件看上去更加正式和真实。

威胁性语言

- 钓鱼邮件通常使用紧迫的语言来创造一种紧迫感，如声称账户即将被冻结或存在未授权活动，促使用户立即行动，而不是仔细审视邮件的真实性。

域名欺骗

- 攻击者使用与真实网站非常相似的域名，诱骗用户访问并输入敏感信息。这些网站在视觉上可能与真实网站难以区分。

短信诈骗

- 通过短信发送钓鱼信息，利用紧急或诱人的语言诱导用户点击链接或提供个人信息。
- 6. 语音诈骗（Vishing）

15 问：什么是勒索软件，有哪些防御措施？

定义

- 勒索软件是一种恶意软件，它通过加密受害者的文件或锁定用户访问其设备，然后要求支付赎金以恢复对文件或设备的访问。勒索软件攻击直接威胁到数据安全，因为它阻止用户访问自己的数据，并且即使支付了赎金，也没有保证数据会被成功解密或恢复。

感染 ⇨ 加密 ⇨ 赎金要求 ⇨ 解密承诺

勒索软件对数据安全的影响

- **数据不可用性**：加密的文件无法访问，影响业务运营和个人工作。
- **数据丢失风险**：即使支付了赎金，也没有保证能够完全恢复数据。
- **财务损失**：支付赎金代表直接的财务损失，而且可能鼓励攻击者继续进行勒索活动。
- **信誉损害**：遭受勒索软件攻击的组织可能面临信誉损害和客户信任的丧失。

勒索软件防御措施

- **备份数据**：定期备份重要数据，并确保备份在与主系统隔离的安全位置。
- **更新和打补丁**：保持操作系统和软件的更新，及时修补已知的安全漏洞。
- **使用安全软件**：安装并更新防病毒软件和防勒索软件工具。
- **限制权限**：应用最小权限原则，限制对重要文件和系统的访问。

16 问：什么是DDoS攻击，有哪些防御措施？

定义

- DDoS是Distributed Denial of Service的缩写，翻译成中文就是“分布式拒绝服务”。DDoS攻击将处于不同位置的多个计算机联合起来作为攻击平台，对一个和多个目标发动DDoS攻击，从而成倍提高攻击威力。由于攻击的发出点分布在不同地方，因此称这类攻击为分布式拒绝服务攻击。

防御DDoS攻击的措施

带宽扩展

增加带宽可以在一定程度上吸收或分散DDoS流量，虽然这不能完全阻止攻击，但能提高抵御小规模攻击的能力。

边缘安全措施

在网络边缘部署防火墙、入侵检测系统和入侵防御系统等设备，配置适当的规则来识别和过滤异常流量。

内容分发网络

利用CDN可以分散流量，提高网站的负载能力和可用性，同时减轻针对单一服务器的攻击压力。

流量清洗服务

流量清洗服务能够识别并过滤掉恶意流量，只允许清洁流量通过。这些服务通常由第三方专业提供商提供。

网络架构优化

设计具有冗余和分布性的网络架构，避免单点故障，确保关键资源和服务的可用性即使在受到攻击时也不会完全中断。

应用层保护

对于针对特定应用的DDoS攻击，在应用层实施额外的保护措施，如Web应用防火墙和速率限制。

17 问：什么是零日攻击，有哪些防御措施?

定义

- 零日攻击是指利用软件、硬件或固件中未知漏洞进行的攻击。这种漏洞被称为“零日”，因为在开发者和公众知晓之前就已经被攻击者发现并利用，即开发者有“零天”时间来修补这个漏洞。零日攻击对数据安全构成严重威胁，攻击者可以利用这个漏洞来获取未经授权的访问权限、窃取敏感数据、植入恶意软件或对目标系统造成其他形式的破坏。

零日攻击的防御措施

防御措施	具体
及时更新和打补丁	虽然零日漏洞本质上在被发现之前难以防御，但定期更新软件和系统可以最小化其他已知漏洞的风险。
使用入侵防御系统和入侵防护系统	这些系统可以帮助检测和阻止异常行为，可能有效阻止某些基于零日漏洞的攻击。
沙箱技术	使用沙箱技术执行可疑代码或文件，可以在一个隔离的环境中检测恶意行为，而不影响主系统。
最小权限原则	限制用户和应用程序的权限可以减少零日攻击的潜在影响。

18 问：什么是SQL注入攻击，有哪些防御措施？

定义

- SQL注入攻击是一种常见的网络安全威胁，攻击者通过在Web应用程序的输入字段中注入恶意的SQL代码，试图执行非法的SQL语句，以此来操纵后端数据库。这种攻击可以用来绕过应用程序的安全措施，获取、修改、删除或添加存储在数据库中的数据，对数据安全构成严重威胁。

防御SQL注入攻击的措施

输入验证	• 对所有用户输入进行严格的验证，确保输入内容符合预期格式，拒绝任何可疑	**使用参数化查询**	• 参数化查询通过预先定义SQL结构并分离数据输入，有效防止了SQL注入，因为它阻止了恶意输入被解释为代码的一部分。
漏洞扫描	• 系统管理员应定期使用SQL漏洞扫描工具检测系统漏洞，以及时发现并防范SQL注入攻击。	**最小权限原则**	• 确保数据库连接使用的账户仅具有执行当前任务所需的最小权限，以减少潜在的损害。
错误处理	• 避免在错误消息中泄露有关数据库结构的信息，这些信息可能被攻击者利用。	**分级管理**	• 通过分级管理用户并限制权限，普通用户仅有必要权限，而完整的数据库操作权限仅授予系统管理员。

19 问：什么是跨站脚本攻击，有哪些防御措施？

- 跨站脚本攻击（Cross-Site Scripting，XSS）攻击通过在Web应用中注入恶意脚本，使之在用户浏览器中执行，从而窃取敏感信息或操纵用户交互，主要由于应用对用户输入的处理不当。XSS攻击主要威胁数据安全，因为可以用来窃取用户信息、会话令牌或其他敏感数据，甚至可以操纵受害者对网站的交互。

防御跨站脚本攻击的措施

输出编码

- 在将用户输入的数据呈现给浏览器时，对HTML、JavaScript等进行适当编码，以防止恶意脚本的执行。

使用HTTP头

- 使用如Content Security Policy（CSP）之类的HTTP响应头，可以限制浏览器中可以执行的脚本类型，从而防止XSS攻击。

框架和库

- 使用现代Web开发框架和库，它们通常提供自动的XSS防护措施。

使用脚本过滤器

- 使用脚本过滤器，如Google的Closure Library和jQuery库等，能够对来自用户的数据进行过滤和检查。

20 问：什么是高级长期威胁，有哪些防御措施？

- 高级长期威胁（Advanced Persistent Threat，APT），又称先进持续性威胁，是指隐匿而持久的电脑入侵过程，通常由某些人员精心策划，针对特定的目标。其通常是出于商业或政治动机，针对特定组织或国家，并要求在长时间内保持高隐蔽性。高级长期威胁包含三个要素：高级、长期、威胁。高级强调的是使用复杂精密的恶意软件及技术以利用系统中的漏洞。长期暗指某个外部力量会持续监控特定目标，并从其获取数据。威胁则指人为参与策划的攻击。

高级长期威胁的防御措施：

1

威胁情报共享

- 加入威胁情报共享平台，了解最新的威胁趋势和攻击手段，及时更新防御策略。

2

多层防御策略

- 实施多层防御机制（防火墙、入侵检测系统、入侵防御系统、沙箱等）以在不同层次上阻挡攻击。

3

细粒度访问控制和权限管理

- 采用最小权限原则，严格控制对敏感数据和关键资源的访问。

4

网络分割和数据隔离

- 将关键资产隔离在安全的网络区域中，以减少横向移动的风险。

21 问：什么是跨站请求伪造，有哪些防御措施？

- 跨站请求伪造（Cross-site request forgery，通常缩写为 CSRF 或者 XSRF），用了网站对用户浏览器的信任。攻击者通过诱导用户（通常是通过点击链接、加载图片或访问控制了的网站）发送一个未经授权的请求到另一个网站，在用户不知情的情况下，在该网站上执行操作，如更改密码、转账、改变电子邮件设置等。

防御CSRF攻击的措施

- **使用Anti-CSRF令牌：**

通过为每个会话生成独特的Anti-CSRF令牌并要求提交的请求必须包含此令牌，可以阻止攻击者的伪造请求。

- **检查Referer头：**

服务器可以验证请求是不是来自于一个合法的源，但这种方法不是完全可靠，因为Referer头可以被禁用或伪造。

- **使用自定义请求头：**

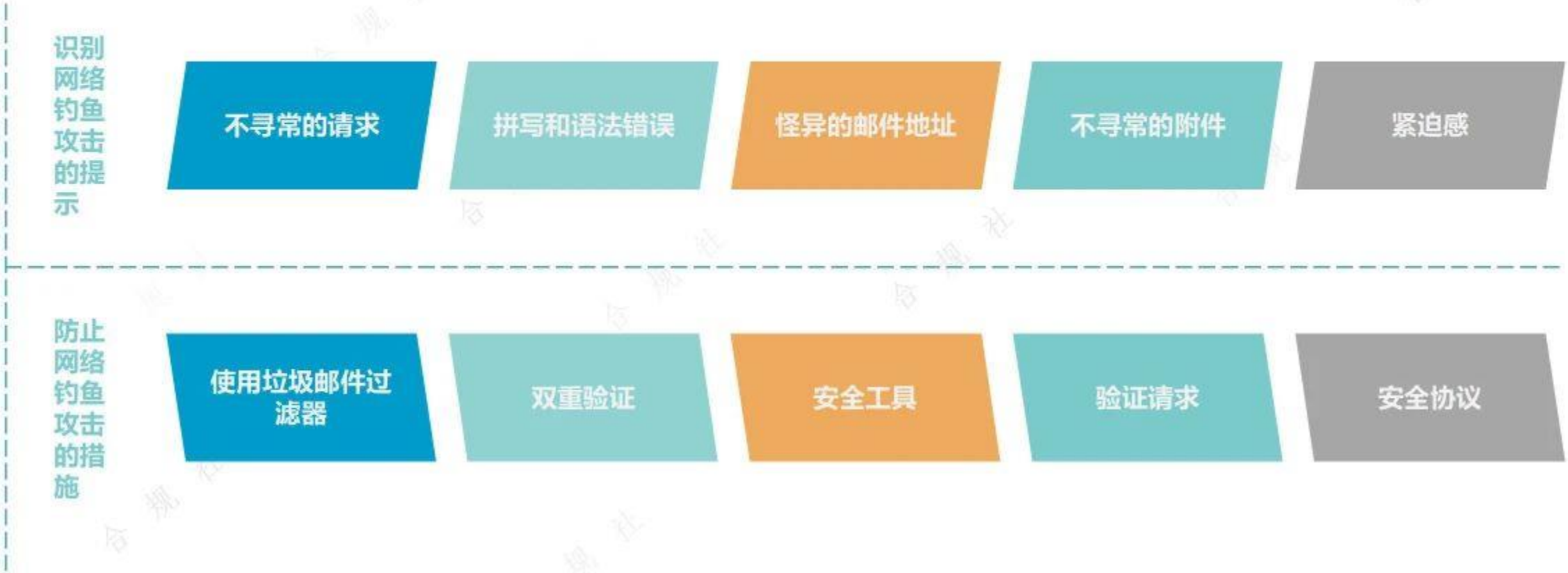
由于跨站请求通常无法设置自定义请求头，因此检查这些头部的存在可以帮助识别和阻止CSRF攻击。

- **利用SameSite Cookie属性：**

设置Cookies的SameSite属性可以限制Cookies随跨站请求发送，从而帮助防止CSRF攻击。

22 问：如何识别和防止网络钓鱼攻击？

- 在数据安全领域，网络钓鱼是一种常见的攻击方式，攻击者通过假冒可信的电子通信（如电子邮件、短信、即时消息等）来诱骗受害者透露敏感信息（如用户名、密码、信用卡信息等）。识别和防止网络钓鱼攻击是保护个人和组织数据安全的重要方面。

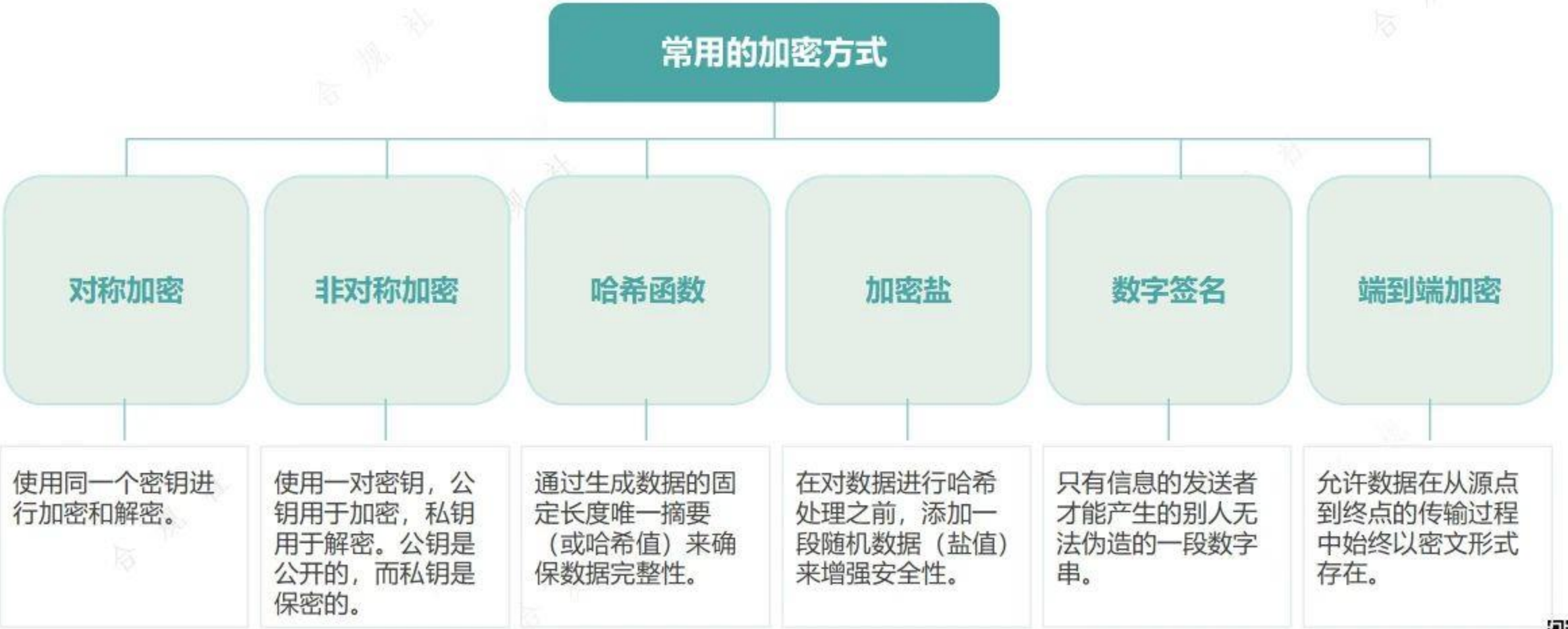


23 问：什么是端口扫描，有哪些类型？

- 端口扫描是一种网络活动，用于探测服务器、网络设备或个人计算机上开放的端口及其服务。通过扫描端口，可以发现网络中的设备、运行的服务以及这些服务的状态（如开放、关闭或过滤）。端口扫描通常用于网络安全评估和管理，帮助网络管理员发现潜在的安全漏洞和不必要的开放服务，从而加强数据安全。然而，它也可能被恶意攻击者用来识别攻击目标和制定攻击策略。

24 问：什么是加密，它如何保护数据？

- 加密是一种安全技术，用于将可读的数据（明文）转化为不可读的形式（密文），以保护数据的机密性。加密使用密钥来进行转换和还原，只有拥有正确密钥的人才能解密密文并恢复原始的明文数据。



25 问：什么是防火墙，它如何保护数据？

- 防火墙是一种网络安全系统，它监控和控制进出某一网络的网络流量。防火墙可以是硬件设备，也可以是软件程序，或者两者的结合。它的基本功能是根据一系列预定的安全规则来允许或阻止数据包的传输，以保护网络不受未经授权的访问和各种网络威胁，如病毒、蠕虫、木马等恶意软件的侵害。从数据安全的角度来看，防火墙是一种关键的防御措施，用于保护存储和传输中的数据不受未授权访问和网络攻击的影响。

访问控制	防止入侵	数据过滤	监控和记录	隔离和分段
防火墙能够限制和控制对网络和网络资源的访问，确保只有经过授权的用户和服务可以访问敏感或关键的数据。这种访问控制可以基于IP地址、端口号或应用程序类型等来实施。	通过监控进出网络的数据流量，防火墙可以检测并阻止潜在的入侵尝试，如端口扫描或未授权的访问尝试，从而保护存储在网络内部的数据不被恶意访问。	防火墙可以检查通过网络传输的数据包，并根据预定义的安全策略对数据进行过滤。这包括阻止恶意软件、病毒和其他恶意代码的传播，防止它们侵入网络并损害或窃取数据。	防火墙可以记录网络活动，提供有关数据流向、访问尝试和潜在安全威胁的详细日志信息。这些日志对于检测异常行为、审计和遵守数据保护法规非常重要。	在更复杂的网络环境中，防火墙可以用来创建网络分段，将敏感数据区域隔离开来，从而在不同的网络区域之间提供额外的保护层。这有助于限制在一部分网络中发生的安全事件对整个网络的影响。

26 问：什么是VPN，它如何提供安全连接?

- VPN，Virtual Private Network，虚拟专用网，也称虚拟私有网络，是一种网络技术，用于在公共网络上创建安全的、加密的连接，使远程用户和分支机构能够通过互联网安全地访问企业内部网络或其他网络资源。

VPN安全机理

加密：VPN的核心功能之一是对数据进行加密，确保数据在传输过程中的安全性和私密性。即使数据在传输过程中被拦截，没有密钥的第三方也无法解读数据内容。

隧道协议：VPN使用所谓的隧道协议来封装和传输数据。这些协议（如PPTP、L2TP、OpenVPN、IPSec等）创建了一个“隧道”，通过公共网络安全地传输加密数据。这种隧道技术防止数据泄露，并保护数据免受外部干扰和监听。

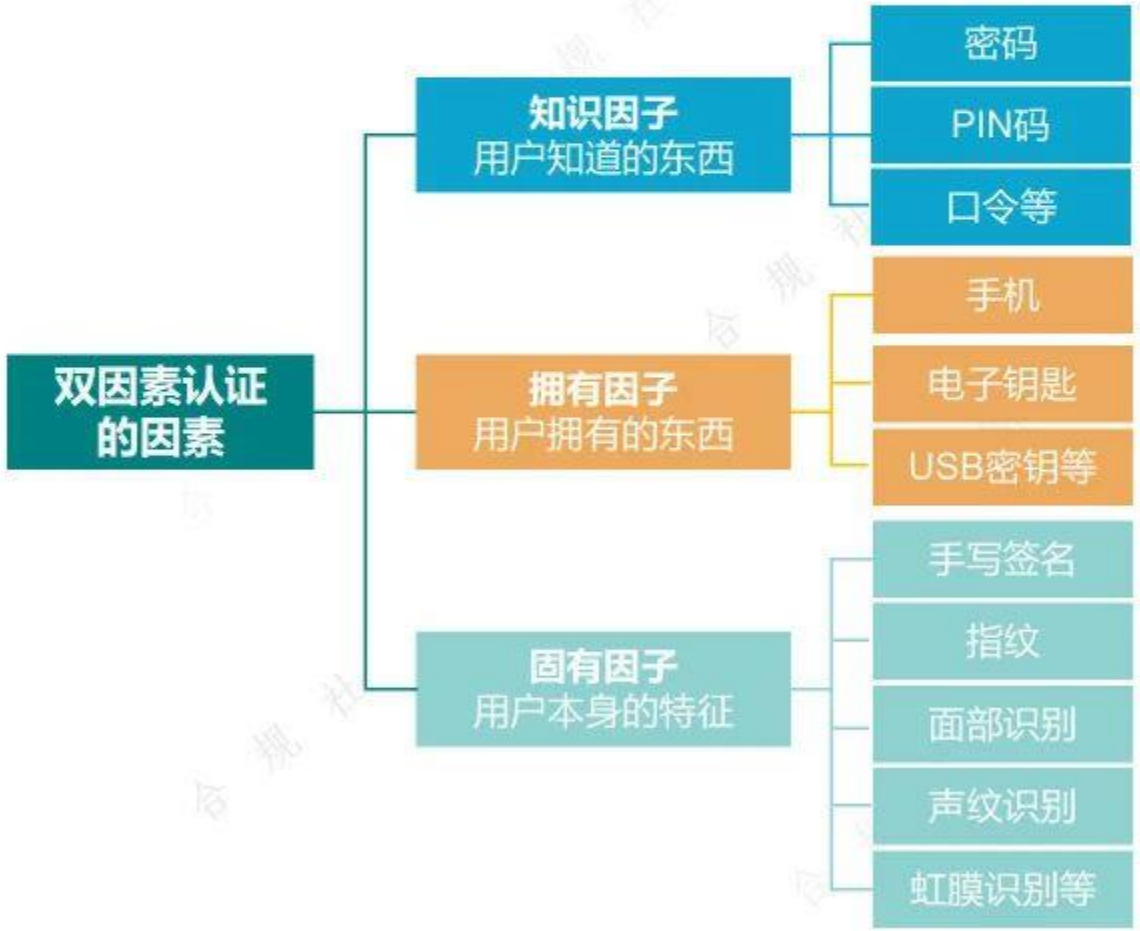
身份验证：VPN在建立连接前要求用户进行身份验证，可以是用户名和密码、数字证书或双因素认证等形式。这确保了只有授权用户才能访问VPN和通过VPN访问的网络资源。

数据完整性：VPN技术通常包括数据完整性检查，确保在传输过程中数据未被篡改。这通过各种校验和散列算法来实现，如果数据在传输过程中被修改，系统将能够检测到并采取措施。

IP隐藏和伪装：VPN还可以隐藏用户的实际IP地址，并为其提供一个临时的IP地址，通常是VPN服务器的地址。这增加了匿名性，使用户的网络活动和地理位置更难被追踪。

27 问：什么是双因素认证，它为何重要？

- 双因素认证（英语：Two-factor authentication，缩写为2FA），又译为双重验证、双重认证、二元认证，又称两步骤验证（2-Step Verification，又译两步验证），是一种认证方法。双因素认证要求用户提供两种不同形式的身份验证来证明自己的身份，这比单一的密码验证提供了更高的安全级别。



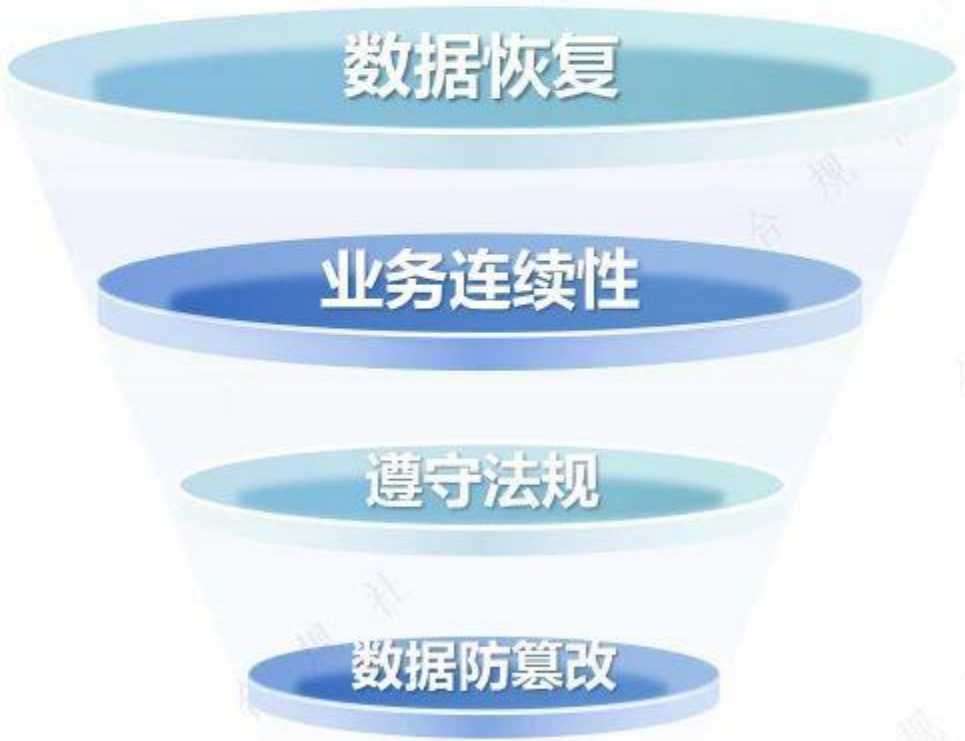
双因素认证的重要性

- **增强安全性：**通过结合两种不同类型的认证，双因素认证为账户提供了额外的保护层，使未经授权的访问变得更加困难。
- **减少数据泄露风险：**即使密码被猜到、泄露或通过网络钓鱼手段获得，双因素认证也可以阻止未授权的访问者进入账户。
- **符合合规要求：**许多行业标准和政府法规，都要求使用双因素认证来增加数据保护。
- **提高用户信心：**为客户提供双因素认证选项可以增加他们对系统安全性的信心，尤其是在处理敏感的财务或个人数据时。

28 问：数据备份为什么重要，应如何执行？

- 数据备份是指将数据的副本存储在主数据源之外的过程，这是确保数据安全性和可恢复性的关键措施，对于防止数据丢失和灾难恢复至关重要，应定期执行，并存储在安全的位置。

数据备份的重要性



如何执行数据备份

确定备份内容	首先确定哪些数据是关键的，需要备份。
选择备份方式	有多种备份方式，包括全备份、增量备份和差异备份。
选择备份介质和位置	数据可以备份到多种介质上，包括硬盘、光盘或云存储。备份数据应该存储在物理位置与原始数据不同的地方。
实施定期备份	根据数据的重要性和变化频率，制定定期备份的计划。
测试和验证备份	定期测试备份文件的完整性和可恢复性是非常重要的
保持备份安全	备份数据需要像处理原始数据一样进行保护，包括加密存储和传输过程中的备份数据

29 问：什么是数据脱敏，有哪些常用的数据脱敏技术方法?

- 数据脱敏是一种数据保护技术，旨在通过修改敏感数据的原始数据，以防止敏感信息的泄露，同时保持数据的实用性。这一过程涉及将敏感数据替换、屏蔽或混淆，以便在不暴露原始数据的情况下，使数据仍可用于测试、分析、培训或其他非生产目的。

数据脱敏技术方法

泛化： 泛化是通过减少数据的精确度来保护敏感信息，例如，将出生日期泛化为出生年份，或将具体地址泛化为城市或州。这种方法降低了数据的精确度，从而保护了个人隐私，同时仍保留了数据的一些实用性。

抑制： 抑制是指移除或隐藏数据集中的全部或部分敏感信息。例如，可以完全删除某些记录或某些字段，如社会保障号码或电话号码，以防止敏感信息泄露。

扰乱： 扰乱是通过对数据进行小幅度修改来实现脱敏，这种修改足以保护数据的隐私，但不会显著影响数据的整体分布或统计特性。例如，可以对数值数据添加随机噪声。

有损： 有损脱敏通过改变数据的原始值来保护隐私，与扰乱类似，但可能会更显著地改变数据。这可能通过各种算法实现，包括添加噪声、数据混淆或数据置换等。

30 问：如何保护无线网络安全?

- 保护无线网络安全是维护数据安全和隐私的重要组成部分，尤其是在日益增长的无线设备连接需求和网络攻击的背景下。保护无线网络安全对于防止未授权访问和保护网络上传输的数据至关重要。

保护无线网络的关键措施

01.更改默认的网络名称和密码

- 避免使用默认名称，因为默认名称可能会暴露路由器的型号和制造商，为攻击者提供线索。

02. 启用强加密

- 在无线网络设置中选择使用高级别的加密标准来保护网络传输的数据，防止未经授权的用户截取。

03. 启用网络防火墙

- 在计算机和移动设备上安装和更新防火墙和安全软件是保护无线网络的关键步骤。

04. 禁用WPS功能（Wi-Fi Protected Setup）

- Wi-Fi Protected Setup功能可能存在安全漏洞，使攻击者能够更轻松地破解您的无线网络密码。

05. 使用MAC地址过滤

- MAC地址过滤可以增加一层安全性，通过只允许已知设备的MAC地址连接到网络来限制访问。

06. 关闭网络广播

- 禁用SSID广播可以隐藏你的网络，使其不会在周围设备的可用网络列表中显示，从而减少未经授权的连接尝试。

07. 定期更新路由器固件

- 定期检查并安装路由器制造商提供的固件更新。更新固件可以修复已知的安全漏洞、增加新功能、提升性能以及改善稳定性。

08. 设置访客网络

- 如果需要为访客提供Wi-Fi接入，应设置一个单独的访客网络。这可以防止访客访问你的主网络及其中的敏感资源。

09. 限制无线信号范围

- 如果可能，调整无线路由器的信号强度，以限制其覆盖范围，只覆盖需要使用Wi-Fi的区域。

10.使用虚拟专用网络（VPN）

- 对于需要访问敏感信息的用户，使用虚拟私人网络可以提供一个加密的通道，保护数据在无线网络中的传输。

31 问：如何保护远程工作安全？

远程工作安全保护

更新路由器和Wi-Fi

- 更改默认设置并为您的宽带路由器和Wi-Fi 网络使用复杂密码。

定期更新软件

- 软件更新为新发现的安全威胁和漏洞提供关键补丁和安全修复。

删除不必要的服务和软件

- 不必要的软件会降低设备性能、扩大网络和设备遭受攻击的范围。

更改默认配置

- 需要更改这些默认配置，设定独特的、复杂的密码和自定义的设置，以此增强安全性，减少被黑客攻击的机会。

更改默认登录密码和用户名

- 在设备初次设置后立即更改这些默认的登录密码和用户名，使用难以猜测的密码和用户名来代替。

32 问：如何保护移动设备的安全？

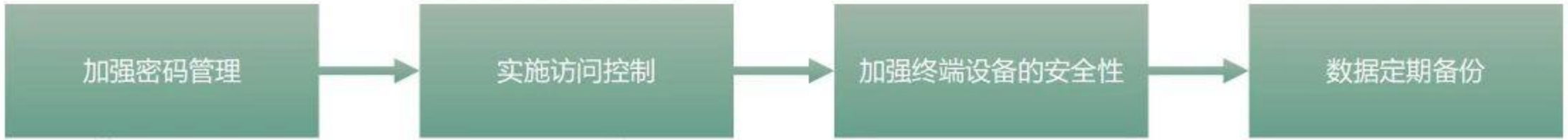
- 移动设备通常存储大量个人和敏感信息，它们面临着丢失、盗窃、恶意软件、数据泄露和未经授权的访问等风险。同时，移动设备的连通性和便携性使得它们更容易遭受网络攻击。需要采取适当的安全措施来保护移动设备和其中的数据安全。

1. **设备访问控制**
   - 采用生物识别和强密码组合，保护设备免遭未授权访问。
2. **应用程序管理**
   - 仅从官方应用商店下载应用，避免安装未经验证的第三方应用。
3. **设备更新和补丁管理**
   - 自动设置设备更新，以确保操作系统和应用程序及时接收安全补丁。
4. **防盗和远程擦除**
   - 启用设备追踪和远程擦除功能，以防设备丢失或被盗时保护数据。
5. **小心应用权限**
   - 仔细检查并管理应用请求的权限，避免授予不必要的访问权。

33 问：什么是终端安全，为什么它如此重要?

- 终端安全是指保护连接到企业网络的所有设备免受各种形式的网络威胁和攻击的策略和技术。终端安全的目标是确保这些设备及其上存储和传输的数据在面对恶意软件、黑客攻击、数据泄露等安全威胁时能够得到有效的保护。

终端安全管理措施



34 问：什么是应用程序安全，为什么应用程序安全很重要?

- 终端安全是指保护连接到企业网络的所有设备免受各种形式的网络威胁和攻击的策略和技术。终端安全的目标是确保这些设备及其上存储和传输的数据在面对恶意软件、黑客攻击、数据泄露等安全威胁时能够得到有效的保护。

云应用程序安全、Web 应用程序安全和移动应用程序安全

云应用程序安全

- **关注点：**云应用程序安全关注的是在云环境中托管的应用程序的安全性。这包括云基础设施的安全性、云服务配置、数据安全、身份和访问管理、以及与云服务供应商的合规性和安全协议。
- **挑战：**主要挑战包括多租户环境下的数据隔离、云资源的配置错误、访问控制和身份管理、以及对云服务供应商安全实践的依赖。

Web应用程序安全

- **关注点：**Web 应用程序安全专注于通过浏览器访问的应用程序的安全性。这包括保护应用程序免受SQL注入、跨站脚本（XSS）、跨站请求伪造（CSRF）等常见的Web攻击手段。
- **挑战：**主要挑战包括保护Web应用程序免受各种Web攻击、管理公开的Web界面和API的安全性、以及保护用户数据和会话信息。

移动应用程序安全

- **关注点：**移动应用程序安全关注的是在移动设备上运行的应用程序的安全性。这包括保护应用程序免受恶意软件攻击、确保数据在传输和存储时的加密、处理设备的多样性和操作系统的更新问题、以及管理应用权限。
- **挑战：**主要挑战包括设备的安全性、数据在不安全网络上的传输、敏感数据在本地存储的安全性、以及第三方库和API的安全问题。

35 问：如何结合漏洞识别和防御策略来保护数据安全？

持续的漏洞识别和评估

定期进行漏洞扫描和渗透测试，以识别新出现的安全漏洞和潜在的攻击路径。

敏捷的安全响应计划

详细的安全事件响应计划，确保在发现漏洞或攻击时能够迅速有效地应对。

安全配置和加固

对系统和应用进行安全配置和加固，以减少可被利用的攻击面。

风险基础的优先级排序

根据漏洞对数据安全的潜在风险进行评估，优先处理那些影响最严重、最有可能被利用的漏洞。

补丁管理和更新

及时应用安全补丁和更新，修复已知漏洞，防止被攻击者利用。

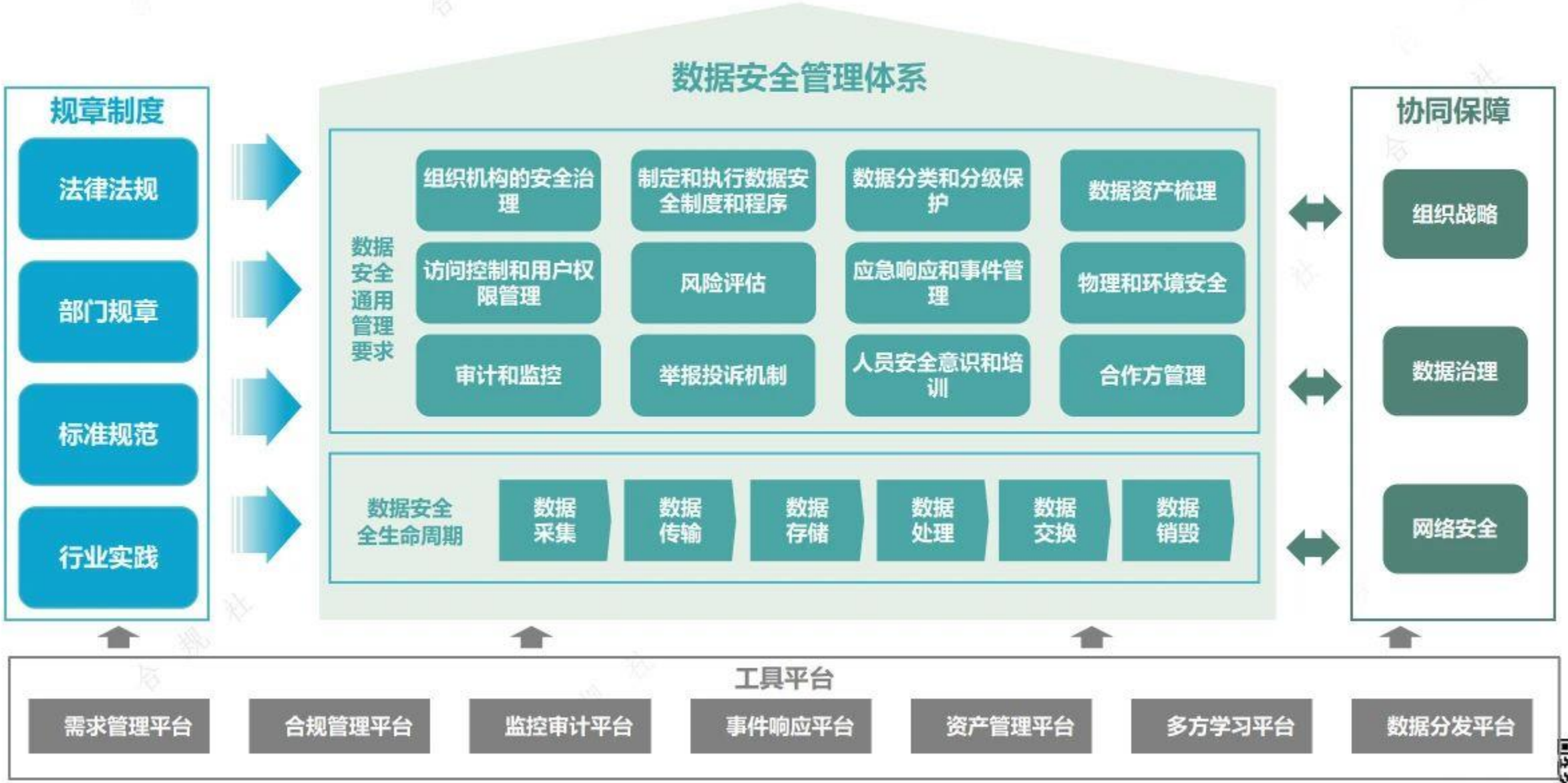
多层防御策略

施多层防御机制（如防火墙、入侵检测系统、Web应用防火墙等），以防御不同类型的攻击，包括DDoS攻击、零日攻击等。

目录

contents

36 问：数据安全治理框架的关键组成部分有哪些？



37 问：数据安全的通用性管理要求包含哪些?

组织机构的安全治理	制定和执行数据安全制度和程序	数据分类和分级保护	数据资产梳理
• 建立专门的数据安全管理部门或指定安全负责人，负责制定和执行数据安全政策。 • 确保所有员工都了解其在数据安全中的角色和责任。	• 制定全面的数据安全制度，涵盖数据的收集、处理、存储、传输、共享和销毁等所有方面。 • 设定明确的操作程序，确保数据处理活动符合组织的安全政策和法律法规要求。	• 根据数据的敏感性和重要性对数据进行分类和分级。 • 对不同级别的数据实施相应级别的保护措施，确保敏感和重要数据得到更高级别的保护。	• 对组织内部所有数据资产进行系统性的识别、分类、评估和管理。 • 识别数据处理中涉及的数据，包括个人信息、重要数据和其他数据，形成数据保护目录，并及时更新。

访问控制和用户权限管理	风险评估	应急响应和事件管理	物理和环境安全
• 实施基于角色的访问控制，确保员工仅能访问其工作所需的数据。 • 定期审查和调整用户访问权限，特别是在员工职位变动或离职时。	• 组织应实施持续的风险评估流程，以识别、评估和优先处理数据处理活动中的潜在风险。	• 制定数据泄露和安全事件的应急响应计划。 • 在发生数据安全事件时，能够迅速采取行动，减轻损失并进行事后分析和整改。	• 保护数据处理和存储设施的物理安全，防止未经授权的访问和环境威胁（如火灾、水灾）。

审计和监控	举报投诉机制	人员安全意识和培训	合作方管理
• 实施数据处理活动的审计和监控措施，记录关键操作和事件。 • 定期审查审计日志，及时发现和应对数据安全事件。	• 为员工和相关方提供明确、易于访问的举报渠道，以报告数据处理中的安全问题、违规行为或其他相关担忧。	• 定期对员工进行数据安全意识和技能培训，提高他们对潜在数据安全威胁的认识。 • 确保员工了解如何安全地处理数据，以及在发现数据安全事件时的应对措施。	• 对与组织共享、处理或存储数据的外部合作伙伴、供应商或服务提供商制定及实施一系列安全控制和管理措施

38 问：企业数据安全组织架构及角色职能如何定义？

- 数据安全官负责整个组织的数据安全战略、政策和程序。数据安全官是连接高层管理与数据安全团队之间的桥梁，确保数据安全战略与业务目标一致。

架构	角色职能
数据安全决策	审议数据安全总体方针政策
	审批数据安全管理制度
	审批数据安全防护制度
	决策数据安全保障体系的技术执行
	处置数据安全突发事件预防及应对
数据安全管理	起草及修订数据安全管理制度等
	起草及规划数据安全规划、预算等内容
	起草数据安全风险报告
	监管落实数据安全控制执行的进度工作
	组织数据安全相关意识及能力培训
数据安全执行	参与及评议数据安全管理制度等
	落实数据安全控制策略执行工作
	落实数据安全意识及能力工作
	提出数据安全需求和报告数据安全事态工作
数据安全参与	参与数据安全控制策略执行工作
	参与数据安全技防能力建设工作
	上报数据安全风险工作
数据安全监督	督查落实数据安全管理制度等执行情况
	督查落实数据安全技防措施等执行情况
	督查落实数据安全意识及能力执行情况

39 问：数据安全责任人有哪些主要职责，需要具备怎样的履职能力？

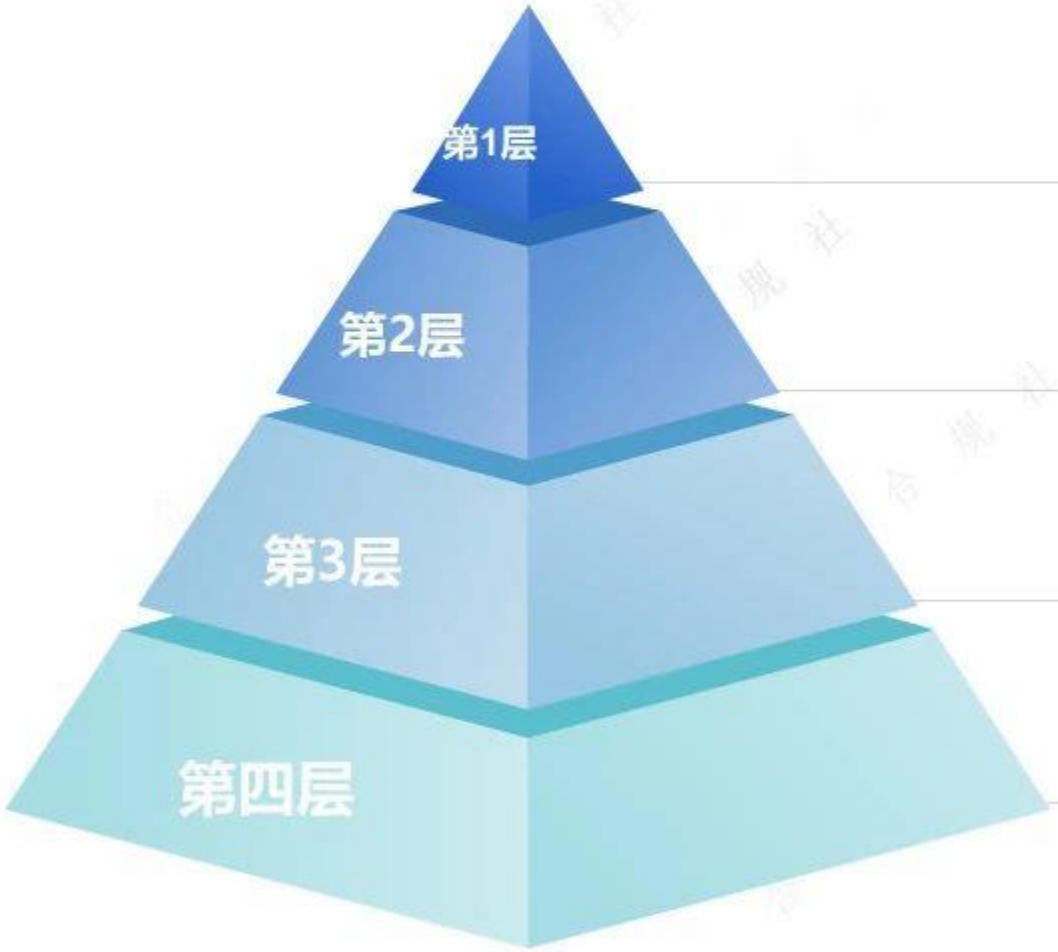
主要职责

- 组织确定数据保护目录，制定数据安全保护计划并督促落实
- 组织开展数据安全影响分析和风险评估，督促整改安全隐患
- 依法向有关部门报告数据安全保护和事件处置情况
- 组织受理和处置数据安全投诉、举报

素质（能力）	内容
技术专长	• **信息安全知识：**深入了解信息安全的原则、框架、标准和最佳实践。 • **技术领域专长：**熟悉网络安全、应用程序安全、终端安全、数据保护、加密技术等领域。 • **风险管理：**能够识别、评估和管理与信息安全相关的风险。
管理与领导	• **战略规划：**能够制定和实施长期和短期的信息安全战略，确保与组织的总体目标一致。 • **团队领导：**具备建立、领导和激励跨职能团队的能力。 • **项目管理：**能够有效地管理信息安全项目，确保按时按质完成。
商业和法律	• **业务理解：**对组织的业务模式、流程和关键驱动因素有深入的理解。 • **法律和合规：**熟悉与数据保护和信息安全相关的法律、法规和合规性要求。 • **财务管理：**理解信息安全投资的经济学，能够进行成本效益分析和预算管理。
沟通与影响力	• **沟通技能：**能够清晰地与不同层级的利益相关者沟通，包括技术团队、业务领导和外部合作伙伴。 • **影响力和说服力：**能够影响和说服组织内外的利益相关者，以支持安全计划和倡议。 • **危机管理：**在发生安全事件时，能够有效地沟通和管理危机情况。
学习和适应	• **持续学习：**信息安全领域不断变化，数据安全官需要持续学习最新的技术、威胁和防御措。 • **适应性：**能够适应快速变化的环境和不断变化的安全威胁景观。

40 问：什么是数据安全四级管理文档体系？

- 数据安全四级管理体系通常指的是将数据安全管理职责和措施分为不同的级别，以建立一套完整的文档体系。这种分级体系可以帮助组织确保从高层策略到具体操作都有明确的指导和记录。虽然具体的分级可能因组织而异，但通常包含以下四个层级：



政策层

包括数据安全政策和总体指导原则。这些文档定义了组织对数据安全的总体承诺，目标和方向，以及管理层的责任。

程序层

包括具体的数据安全程序和计划。这些文档详细说明了实现安全政策的步骤，包括风险评估、数据分类、数据处理和响应措施。

指导层

包含操作指导和标准操作程序。在这一层，会详细描述员工在日常工作中应遵循的具体数据安全实践和流程。

记录层

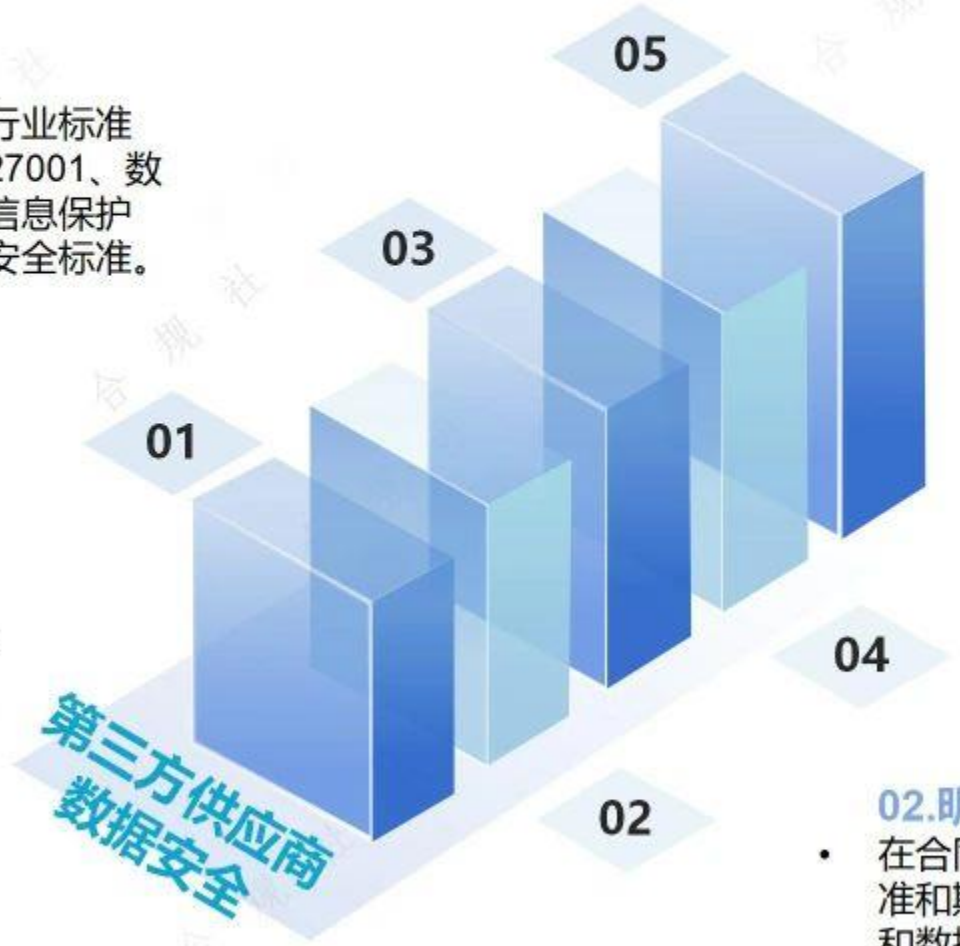
包括各种记录和表格，如安全事件报告、访问控制记录、审核报告和改进记录等。这一层的文档用于记录执行安全措施的结果和任何必要的后续行动。

41 问：如何评估和管理第三方供应商以保障数据安全？

- 第三方供应商可能成为数据泄露和安全漏洞的潜在来源。若供应商的数据保护措施不足或安全政策不严格，可能会导致数据被误用、泄露或未经授权的访问，进而对组织的声誉、客户信任以及合规状态造成严重影响。因此，确保第三方供应商的数据安全至关重要，以下是一些关键的措施来应对这些风险：

03.要求合规性证明：

- 在要求供应商提供遵守行业标准和法规的证明，如ISO 27001、数据安全管理认证、个人信息保护认证或其他相关的数据安全标准。



05.实施访问控制和最小权限原则：

- 确保第三方供应商只能访问执行其服务所必需的数据，并实行最小权限原则。

04.定期审计和监控：

- 与供应商约定定期的安全审计，评估其遵守合同中安全要求的程度。监控供应商的安全性能，确保持续符合约定的安全标准。

01.评估供应商的安全措施：

- 在选择供应商之前，进行安全评估，了解第三方的数据保护政策、安全控制措施和合规性记录。考虑使用第三方安全评估机构来进行更深入的审查。

02.明确合同条款和数据安全要求：

- 在合同中明确规定数据安全的责任、标准和期望，包括对数据加密、访问控制和数据处理的具体要求。确保合同中包含有关数据泄露通知和应对措施的条款。

更多精彩内容点击→

42 问：数据安全审计是什么，它包括哪些关键步骤？

定义

- 数据安全审计是一个系统的过程，用于评估和验证组织中数据管理实践的有效性，确保数据保护措施符合既定的安全政策、标准和法律法规要求。数据安全审计的目的是识别数据处理和存储中的潜在漏洞和不足，确保数据的保密性、完整性和可用性得到保护，同时提高组织对数据安全的整体态度和实践。

数据安全审计的关键步骤

43 问：有哪些国推的数据安全认证?

- **2019年3月15日**
- 国家市场监管总局 中央网信办《关于开展App安全认证工作的公告》

移动互联网应用程序（App）安全认证

- **2022年6月5日**
- 国家市场监管总局 中央网信办关于开展数据安全管理认证工作的公告

数据安全管理认证

- **2022年11月18日**
- 国家市场监管总局 中央网信办《关于实施个人信息保护认证的公告》

个人信息保护认证

44 问：数据安全管理认证包括哪些步骤？

认证委托

- 认证机构应当明确认证委托资料要求，包括但不限于认证委托人基本材料、认证委托书、相关证明文档等。
- 认证委托人应当按认证机构要求提交认证委托资料，认证机构在对认证委托资料审查后及时反馈是否受理。
- 认证机构应当根据认证委托资料确定认证方案，包括数据类型和数量、涉及的数据处理活动范围、技术验证机构信息等，并通知认证委托人。

技术验证

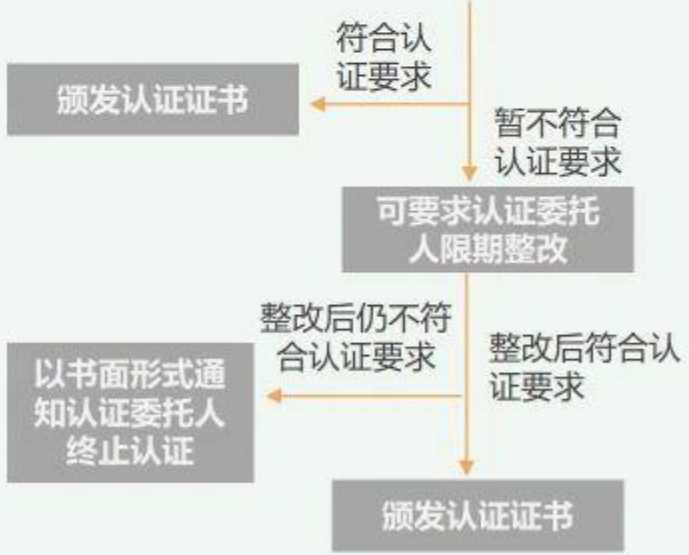
- 技术验证机构应当按照认证方案实施技术验证，并向认证机构和认证委托人出具技术验证报告。

现场审核

- 认证机构实施现场审核，并向认证委托人出具现场审核报告

认证结果评价和批准

- ✓ 认证委托资料
- ✓ 技术验证报告
- ✓ 现场审核报告
- ✓ 其他相关资料



获证后监督

- **监督的频次：**
  认证机构应当在认证有效期内，对获得认证的网络运营者进行持续监督并合理确定监督频次。
- **监督的内容：**
  认证机构应当采取适当的方式实施获证后监督，确保获得认证的网络运营者持续符合认证要求。
- **获证后监督结果评价：**
  认证机构对获证后监督结论和其他相关资料信息进行综合评价，评价通过的，可继续保持认证证书；不通过的，认证机构应当根据相应情形作出暂停直至撤销认证证书的处理。

认证时限

- 认证机构应当对认证各环节的时限作出明确规定，并确保相关工作按时限要求完成。
- 认证委托人应当对认证活动予以积极配合。

45 问：个人信息保护认证的法律依据有哪些?

文件名称	法律效力位阶	制定机关	施行日期	相关规定/意义
《中华人民共和国认证认可条例》	行政法规	国务院	2020年11月29日	第十六条　国家根据经济和社会发展的需要，推行产品、服务、管理体系**认证**。 第六十二条　国家网信部门统筹协调有关部门依据本法推进下列个人信息保护工作： （四）推进个人信息保护社会化服务体系建设，支持有关机构开展个人信息保护评估、**认证**服务；
《中华人民共和国个人信息保护法》	法律	全国人民代表大会常务委员会	2021年11月1日	第三十八条　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，应当具备下列条件之一： （二）按照国家网信部门的规定经专业机构进行个人信息保护**认证**；
《网络安全标准实践指南—个人信息跨境处理活动安全认证规范（V2.0-202212）》	标准技术文件	全国信息安全标准化技术委员会秘书处	2022年12月	为认证机构对个人信息处理者的个人信息跨境处理活动开展**认证**提供依据。
《个人信息保护认证实施规则》	规范性文件	国家市场监督管理总局、国家互联网信息办公室	2022年11月18日	从事个人信息保护认证工作的认证机构应当经批准后开展有关认证活动，并按照《个人信息保护认证实施规则》实施**认证**。

46 问：《数据安全法》规定了哪些违法后果？

情节	处罚（企业/责任人）	加重处罚（企业/责任人）	其他
一般违法	5-50万/1-10万	50-200万/5-20万	◘ 企业作为责任主体违法的，直接负责的主管人员和其他责任人也会被处罚。 ◘ 并根据情况责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照。
违反国家核心数据管理制度，危害国家主权、安全和发展利益	200-1000万		
向境外提供重要数据的	10-100万/1-10万	100-1000万/10-100万	
拒不配合数据调取	5-50万/1-10万		
未经主管机关批准向外国司法或者执法机构提供数据	10-100万/1-10万	100-500万/5-50万	

47 问：《个人信息保护法》规定了哪些违法后果？

停业整顿、吊销业务许可（营业执照）、市场禁入

责令暂停或终止提供服务

三类处罚措施，最高处罚五千万或5%营业额

- 处理个人信息未履行个人信息保护义务的，由履行个人信息保护职责的部门**责令改正，给予警告，没收违法所得**，对违法处理个人信息的应用程序，**责令暂停或者终止提供服务**；拒不改正的，并处**一百万元以下罚款**；对直接负责的**主管人员和其他直接责任人员处一万元以上十万元以下罚款。**
- 处理个人信息未履行个人信息保护义务情节严重的，由省级以上履行个人信息保护职责的部门责令改正，没收违法所得，**并处五千万元以下或者上一年度营业额百分之五以下罚款**，并可以责令暂停相关业务或者停业整顿、通报有关主管部门**吊销相关业务许可或者吊销营业执照**；对直接负责的主管人员和其他直接责任人员处**十万元以上一百万元以下罚款**，并可以决定**禁止其在一定期限内担任**相关企业的董事、监事、高级管理人员和个人信息保护负责人。

48 问：什么是关键信息基础设施?

- 关键信息基础设施：公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等。

公共通信和信息服务	能源	交通	水利
金融	公共服务	电子政务	国防科技工业

其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等。

49 问：关键信息基础设施运营者有哪些特定义务？

01 **安全保护措施三同步：**安全保护措施应当与关键信息基础设施同步规划、同步建设、同步使用

02 **设置专门安全管理机构职责：**对安全管理机构负责人和关键岗位人员进行安全背景审查；保障专门安全管理机构的运营经费、配备相应人员。

03 **网络安全检测与风险评估：**自行或者委托网络安全服务机构对关键信息基础设施每年至少进行一次网络安全检测和风险评估

04 **安全事件报告：**重大网络安全事件或者发现重大网络安全威胁，向保护工作部门、公安机关报告；特别重大网络安全事件或威胁，向国家网信部门报告、国务院公安部门报告。

05 **采购网络产品和服务时的义务：**采购网络产品或服务可能影响国家安全的，应当按照国家网络安全规定通过安全审查；与网络产品和服务提供商签订安全保密协议。

06 **境内存储与出境时的安全评估义务：**在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。

50 问：关键信息基础设施安全保护应包括哪些内容？

- 关键信息基础设施安全保护包括分析识别、安全防护、检测评估、监测预警、主动防御、事件处置六个方面。

分析识别	安全防护	检测评估	监测预警	主动防御	事件处置
围绕关键信息基础设施承载的关键业务，开展业务依赖性识别、关键资产识别、风险识别等活动。本活动是开展安全防护、检测评估、监测预警、主动防御、事件处置等活动的基础。	根据已识别的关键业务、资产、安全风险，在安全管理制度、安全管理机构、安全管理人员、安全通信网络、安全计算环境、安全建设管理、安全运维管理等方面实施安全管理和技术保护措施，确保关键信息基础设施的运行安全。	为检验安全防护措施的有效性，发现网络安全风险隐患，应建立相应的检测评估制度，确定检测评估的流程及内容等，开展安全检测与风险隐患评估，分析潜在安全风险可能引发的安全事件。	建立并实施网络安全监测预警和信息通报制度，针对发生的网络安全事件或发现的网络安全威胁，提前或及时发出安全警示。建立威胁情报和信息共享机制，落实相关措施，提高主动发现攻击能力。	以应对攻击行为的监测发现为基础，主动采取收敛暴露面、捕获、溯源、干扰和阻断等措施，开展攻防演习和威胁情报工作，提升对网络威胁与攻击行为的识别、分析和主动防御能力。	运营者对网络安全事件进行报告和处置，并采取适当的应对措施，恢复由于网络安全事件而受损的功能或服务。

参考：《信息安全技术 关键信息基础设施安全保护要求（GB/T 39204-2022）》

51 问：关键信息基础设施在数据安全方面有哪些防护要求？

序号	数据安全防护要求
1	应建立数据安全管理责任和评价考核制度，编制数据安全保护计划，实施数据安全技术防护，开展数据安全风险评估，制定数据安全事件应急预案，及时处置安全事件，组织数据安全教育、培训。
2	应建立基于数据分类分级的数据安全保护策略，明确重要数据和个人信息保护的相应措施。
3	将在我国境内运营中收集和产生的个人信息和重要数据存储在境内。因业务需要，确需向境外提供数据的，应当按照国家相关规定和标准进行安全评估。法律、行政法规另有规定的，依照其规定。
4	应严格控制重要数据的使用、加工、传输、提供和公开等关键环节，并采取加密、脱敏、去标识化等技术手段保护敏感数据安全。
5	应建立业务连续性管理及容灾备份机制，重要系统和数据库实现异地备份。
6	数据可用性要求高的，应采取数据库异地实时备份措施。业务连续性要求高的，应采取系统异地实时备份措施，确保关键信息基础设施一旦被破坏，可及时进行恢复和补救。
7	应在关键信息基础设施退役废弃时，按照数据安全保护策略对存储的数据进行处理。
8	应建立数据处理活动全流程的安全能力，并符合相关国家标准关于数据安全保护的要求。

参考：《信息安全技术 关键信息基础设施安全保护要求（GB/T 39204-2022）》

目录

contents

52 问：什么是数据分类分级?

- 数据分类分级是一种数据管理策略，通过对数据进行系统的评估和分类，将数据划分为不同的类别和级别，以便更有效、更安全地管理和使用数据。这一过程涉及到对数据的价值、敏感性和重要性进行识别和评估，然后根据这些特征将数据分配到适当的分类中。每个分类都对应一套特定的管理措施、安全要求和访问控制策略。

国家建立数据分类分级保护制

《中华人民共和国数据安全法》第二十一条：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。国家数据安全工作协调机制统筹协调有关部门制定重要数据目录，加强对重要数据的保护。

关系国家安全、国民经济命脉、重要民生、重大公共利益等数据属于国家核心数据，实行更加严格的管理制度。

各地区、各部门应当按照数据分类分级保护制度，确定本地区、本部门以及相关行业、领域的重要数据具体目录，对列入目录的数据进行重点保护。

53 问：实施数据分类分级保护制度的原因?

01

国家监管角度： 落实管理《网络安全法》、《数据安全法》、《个人信息保护法》等法规管理重要数据和其他受监管数据的必要措施。

02

合规义务角度： 目前数据分类分级制度已成为企业基本的法定义务，既面临个人信息、重要数据等合规义务，也必须遵守其所在行业、领域的特殊类型数据的合规义务。

03

资源优化配置： 不同类型和级别的数据需要不同程度的安全措施，数据分类分级有助于组织合理分配安全资源，确保高风险数据得到足够的保护，同时避免对低风险数据过度投入资源。

04

法律后果角度： 按照相关法律法规，未履行数据分类分级义务的企业可能受到信用惩戒、公开曝光、没收违法所得、罚款、暂停营业、停业整顿、关闭网站、吊销业务许可证或者吊销营业执照等行政处罚等。

54 问：数据分类分级应遵循哪些基本原则？

01

科学实用原则

数据分类应从便于数据管理和使用的角度，科学选择常见、稳定的属性或特征作为数据分类的依据，并结合实际需要对数据进行细化分类。

02

边界清晰原则

数据分级的主要目的是为了数据安全，各个数据级别应做到边界清晰，对不同级别的数据采取相应的保护措施。

03

就高从严原则

采用就高不就低的原则确定数据分级，当多个因素可能影响数据分级时，按照可能造成的最高影响对象和影响程度确定数据级别。

04

点面结合原则

数据分级既要考虑单项数据分级，也要充分考虑多个领域、群体或区域的数据汇聚融合后对数据重要性、安全风险等的影响，通过定量与定性相结合的方式综合确定数据级别。

05

动态更新原则

根据数据的业务属性、重要性和可能造成的危害程度的变化，对数据分类分级、重要数据目录等进行定期审核更新。

55 问：数据分类的一般流程是怎样的?

- 数据分类一般流程包括几个关键步骤，旨在确保数据被适当地识别、分类并根据其敏感性和重要性应用合适的保护措施。

数据分类流程的主要步骤：

01	• 确定数据处理者业务涉及的行业领域，如，工业、电信、金融、能源、交通运输、自然能源、卫生健康、教育等。
02	• 按照业务所属行业领域的数据分类规则，对该业务运营过程中收集和产生的数据进行分类。
03	• 识别是否存在法律法规或主管监管部门有专门管理要求的数据类别（如个人信息），对个人信息、敏感个人信息进行区分标识。
04	• 如果存在行业领域数据分类规则未覆盖的数据类型，可以从组织经营角度结合自身数据管理和使用需要对数据进行分类。

56 问：如何理解数据分级框架?

- 根据数据在经济社会发展中的重要程度，以及一旦遭到泄露、篡改、破坏或者非法获取、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，将数据从高到低分为核心、重要、一般三个级别。

数据分级	定义	示例	保护措施
核心数据	一旦被泄露、篡改、破坏或者非法获取、非法利用、非法共享，可能直接危害政治安全、国家安全重点领域、国民经济命脉、重要民生、重大公共利益。	国家安全数据、关键基础设施的控制系统数据、重要的政府决策数据等。	对于核心数据，需要实施最高级别的安全保护措施，包括但不限于高度加密、严格的物理和网络访问控制、持续的安全监控和评估等。
重要数据	一旦被泄露、篡改、破坏或者非法获取、非法利用、非法共享，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全。	企业的商业秘密、个人的敏感个人信息（如健康记录）、重要的财务数据等。	重要数据需要较高级别的保护，包括访问控制、数据加密、数据备份和灾难恢复计划等。
一般数据	据一旦被泄露、篡改、破坏或者非法获取、非法利用、非法共享，仅影响小范围的组织或公民个体合法权益。	公开的政府信息、企业的一般业务数据、个人的非敏感信息等。	一般数据的保护措施相对宽松，主要确保数据的可用性和完整性，如基本的访问控制和常规的数据备份等。

57 问：数据分级的一般流程是怎样的？

58 问：数据分级的确定参考规则？

影响程度

影响对象	影响程度		
	特别严重危害	严重危害	一般危害
国家安全	核心数据	核心数据	重要数据
经济运行	核心数据	重要数据	重要数据
社会稳定	核心数据	重要数据	一般数据
公共利益	核心数据	重要数据	一般数据
组织权益、个人权益	一般数据	一般数据	一般数据

影响对象

59 问：个人金融信息通常如何分类分级？

- 中国人民银行于2020年2月13日发布并实施的金融行业标准《个人金融信息保护技术规范》，针对自然人的个人金融信息类别标准，即根据信息遭到未经授权的查看或未经授权的变更后所产生的影响和危害，将个人金融信息按敏感程度从高到低划分为三个类别。

类别	说明	举例
C3	C3 类别信息主要为用户鉴别信息。该类信息一旦遭到未经授权的查看或未经授权的变更，会对个人金融信息主体的信息安全与财产安全造成严重危害。	•银行卡磁道数据（或芯片等效信息）、卡片验证码（CVN 和 CVN2）、卡片有效期、银行卡密码、网络支付交易密码； •账户（包括但不限于支付账号、证券账户、保险账户）登录密码、交易密码、查询密码； •用于用户鉴别的个人生物识别信息。
C2	C2 类别信息主要为可识别特定个人金融信息主体身份与金融状况的个人金融信息，以及用于金融产品与服务的关键信息。该类信息一旦遭到未经授权的查看或未经授权的变更，会对个人金融信息主体的信息安全与财产安全造成一定危害。	•支付账号及其等效信息，如支付账号、证件类识别标识与证件信息（身份证、护照等）、手机号码。 •账户（包括但不限于支付账号、证券账户、保险账户）登录的用户名。 •用户鉴别辅助信息，如动态口令、短信验证码、密码提示问题答案、动态声纹密码；若用户鉴别辅助信息与账号结合使用可直接完成用户鉴别，则属于 C3 类别信息。 •直接反映个人金融信息主体金融状况的信息，如个人财产信息（包括网络支付账号余额）、借贷信息。 •用于金融产品与服务的关键信息，如交易信息（如交易指令、交易流水、证券委托、保险理赔）等。 •用于履行了解你的客户（KYC）要求，以及按行业主管部门存证、保全等需要，在提供产品和服务过程中收集的个人金融信息主体照片、音视频等影像信息。 •其他能够识别出特定主体的信息，如家庭地址等。
C1	C1 类别信息主要为机构内部的信息资产，主要指供金融业机构内部使用的个人金融信息。该类信息一旦遭到未经授权的查看或未经授权的变更，可能会对个人金融信息主体的信息安全与财产安全造成一定影响	•账户开立时间、开户机构； •基于账户信息产生的支付标记信息； •C2 和 C3 类别信息中未包含的其他个人金融信息。

级别	数据特征
5级	• 重要数据，通常主要用于金融业大型或特大型机构、金融交易过程中重要核心节点类机构的关键业务使用，一般针对特定人员公开，且仅为必须知悉的对象访问或使用。 • 数据安全性遭到破坏后，对国家安全造成影响，或对公众权益造成严重影响。
4级	• 数据通常主要用于金融业大型或特大型机构、金融交易过程中重要核心节点类机构的重要业务使用，一般针对特定人员公开，且仅为必须知悉的对象访问或使用。 • 个人金融信息中的 C3 类信息。 • 数据安全性遭到破坏后，对公众权益造成一般影响，或对个人隐私或企业合法权益造成严重影响，但不影响国家安全。
3级	• 数据用于金融业机构关键或重要业务使用，一般针对特定人员公开，且仅为必须知悉的对象访问或使用。 • 个人金融信息中的 C2 类信息。 • 数据的安全性遭到破坏后，对公众权益造成轻微影响，或对个人隐私或企业合法权益造成一般影响，但不影响国家安全。
2级	• 数据用于金融业机构一般业务使用，一般针对受限对象公开，通常为内部管理且不宜广泛公开的数据。 • 个人金融信息中的 C1 类信息。 • 数据的安全性遭到破坏后，对个人隐私或企业合法权益造成轻微影响，但不影响国家安全、公众权益。
1级	• 数据一般可被公开或可被公众获知、使用。 • 个人金融信息主体主动公开的信息。 • 数据的安全性遭到破坏后，可能对个人隐私或企业合法权益不造成影响，或仅造成微弱影响但不影响国家安全、公众权益。

60 问：个人健康医疗数据通常如何分类分级？

- 2021年7月1日 实施的国标《信息安全技术 健康医疗数据安全指南（ GB/T 39725—2020）》将健康医疗数分为个人属性数据、健康状况数据、医疗应用数据、医疗支付数据、卫生资源数据以及公共卫生数据等类别，根据数据重要程度和风险级别以及对个人健康医疗数据主体可能造成的损害以及影响的级别将数据划分为以下5级。

数据类别	范围
个人属性数据	1)人口统计信息，包括姓名、出生日期、性别、民族、国籍、职业、住址、工作单位、家庭成员信息、联系人信息、收入、婚姻状态等； 2)个人身份信息，包括姓名、身份证、工作证、居住证、社保卡、可识别个人的影像图像、健康卡号、住院号、各类检查检验相关单号； 3)个人通讯信息，包括个人电话号码、邮箱、账号及关联信息等； 4)个人生物识别信息，包括基因、指纹、声纹、掌纹、耳廓、虹膜、面部特征等； 5)个人健康监测传感设备ID等
健康状况数据	主诉、现病史、既往病史、体格检查（体征）、家族史、症状、检验检查数据、遗传咨询数据、可穿戴设备采集的健康相关数据、生活方式、基因测序、转录产物测序、蛋白质分析测定、代谢小分子检测、人体微生物检测等
医疗应用数据	门（急）诊病历、住院医嘱、检查检验报告、用药信息、病程记录、手术记录、麻醉记录、输血记录、护理记录、入院记录、出院小结、转诊（院）记录、知情告知信息等
医疗支付数据	1)医疗交易信息，包括医保支付信息、交易金额、交易记录等； 2)保险信息，包括保险状态、保险金额等
卫生资源数据	医院基本数据、医院运营数据等
公共卫生数据	环境卫生数据、传染病疫情数据、疾病监测数据、疾病预防数据、出生死亡数据等

等级	使用范围	举例
第1级	可完全公开使用。	医院名称、地址、电话等，可直接在互联网面向公众公开。
第2级	可在较大范围内供访问使用。	不能识别个人身份的数据，各科室医生经过申请审批可用于研究分析。
第3级	可在中等范围内供访问使用。	经过部分去标识化处理，但仍可能重标识的数据，仅限于获得授权项目组范围内使用。
第4级	在较小范围内供访问使用。	可以直接标识个人身份的数据，仅限于参与诊疗活动的医护人员访问使用。
第5级	仅在极小范围内且在严格限制条件下供访问使用。	特殊病种（如艾滋病、性病）的详细资料，仅限于主治医护人员访问且需要进行严格管控。

61 问：数据识别流程包括哪些关键步骤？

- 进行数据资产的盘点、整理和分类，以创建一份详尽的数据资产目录。

- 识别数据资产中的重要数据和核心数据。

- 对判定为重要数据、核心数据的数据对象，增加重要数据、核心数据标识。

梳理 → 判断 → 识别 → 审核 → 标识 → 形成目录

- 确定资产清单中不同类型数据的价值和敏感性，以及数据受损可能对国家安全和公共利益带来的后果。

- 对识别出的重要数据和核心数据进行审核

- 填表描述经审核确定的重要数据和核心数据，以目录形式形成重要数据和核心数据最终识别结果，并定期更新。

62 问：重要数据的识别因素包含哪些?

- 参考2022年5月全国信息安全标准化技术委员会发布了《信息安全技术 重要数据识别规则（征求意见稿）》，重要数据识别识别因素包含19项。

重要数据

01 直接影响国家主权、政权安全、政治制度、意识形态安全，如用以实施社会动员的数据等属于重要数据；

02 直接影响领土安全和国家统一，或反映国家自然资源基础情况，如未公开的领陆、领水、领空数据等；

03 可被其他国家或组织利用发起对我国的军事打击，或反映我国战略储备、应急动员、作战等能力，如满足一定精度指标的地理信息或战略物资产能、储备量信息等；

04 直接影响市场秩序或国家经济命脉安全，如支撑关键基础设施所在行业、领域核心业务运行或重要经济领域生产的数据等；

05 反映我国语言文字、历史、风俗习惯、民族价值观念等特质，如历史文化遗产信息等；

06 反映重点目标、重要场所物理安全保护情况或未公开地理目标的位置，可被恐怖分子、犯罪分子利用实施破坏，如重点安保单位、重要生产企业、国家重要资产的施工图、内部结构、安防等信息，以及未公开的专用公路、机场信息等；

07 关系国家科技实力、影响国际竞争力，或关系出口管制物项，如反映国家科技创新重大成果，或描述我国禁止出口限制出口物项的设计原理、工艺流程、制作方法等的信息以及源代码、集成电路布图、技术方案、重要参数、实验数据、检测报告等；

08 反映关键信息基础设施总体运行、发展和安全保护情况，可被利用实施对关键信息基础设施的网络攻击，如反映关键信息基础设施系统配置信息、核心软硬件设计信息、系统拓扑、应急预案、测评、监测、审计等情况的数据；

09 可被利用实施对关键设备、系统组件供应链的破坏，以发起高级持续性威胁等网络攻击，如政府或军工单位客户清单、未公开的产品和服务采购情况、未公开的重大漏洞等；

10 反映自然环境、生产生活环境基础情况，或可被利用造成环境安全事件，如未公开的土壤数据、气象观测数据、环保监测数据等；

11 反映水资源、能源资源、土地资源、矿产资源等资源储备和开发、供给情况，如未公开的水文观测结果、未公开的耕地面积或质量变化情况等

12 关系海外能源资源安全、海上战略通道安全、海外公民和法人安全，或可被利用实施对我国参与国际经贸、文化交流活动的破坏或对我国实施歧视性禁止、限制或其他类似措施，如国际贸易中特殊物项生产交易及特殊装备配备、使用情况等；

13 关系我国在太空、深海、极地等战略新疆域的现实或潜在利益，如未公开的科学考察、开发利用数据和影响人员安全进出的数据等属于重要数据；

14 反映生物技术研究、开发和应用情况，反映族群特征、遗传信息，关系重大突发传染病、动植物疫情，关系生物实验室安全，或可能被利用制造生物武器、实施生物恐怖袭击，关系外来物种入侵和生物多样性，如重要生物资源数据、微生物耐药基础研究数据等属于重要数据；

15 未公开的政务数据、情报数据和执法司法数据，如未公开的统计数据等属于重要数据；

16 反映全局性或重点领域经济运行、金融活动状况，关系产业竞争力，可造成公共安全事故或影响公民生命安全，可引发群体性活动或影响群体情感与认知，如未公开的统计数据、重点企业 商业秘密，以及危化品制作工艺、危化品储备地点等属于重要数据；

17 反映国家或地区群体健康生理状况，关系疾病传播与防治，关系食品药品安全，如健康医疗资源数据、批量人口的诊疗与健康管理数据、疾控防疫数据、健康救援保障数据、特定药品实验 数据、食品安全溯源标识信息等属于重要数据；

18 其他可能影响国家政治、国土、军事、经济、文化、社会、科技、网络、生态、资源、核、海外利益、太空、极地、深海、生物等安全的数据。

63 问：什么是重要数据，工业、汽车、教育领域的重要数据如何识别？

- 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、公共利益或者个人、组织合法权益的数据。

工业领域重要数据识别规则

（一）工业数据处理者收集和产生的达到一定数量或影响一定范围的个人信息，包括：
1.100 万人以上的个人信息；
2.10万人以上具有一定特征群体的个人信息，例如，军人、公务员等群体的个人信息。
（二）工业和信息化主管部门确定的其他一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能严重影响国家安全、社会稳定、工业经济运行、工业生产安全，或引发的事件影响范围涉及多个行业、区域或者行业内多个企业或影响持续时间长，对行业发展、技术进步和产业生态等造成严重影响的工业数据。

汽车领域重要数据识别规则

（一）军事管理区、国防科工单位以及县级以上党政机关等重要敏感区域的地理信息、人员流量、车辆流量等数据；
（二）车辆流量、物流等反映经济运行情况的数据；
（三）汽车充电网的运行数据；
（四）包含人脸信息、车牌信息等的车外视频、图像数据；
（五）涉及个人信息主体超过10万人的个人信息；
（六）国家网信部门和国务院发展改革、工业和信息化、公安、交通运输等有关部门确定的其他可能危害国家安全、公共利益或者个人、组织合法权益的数据。

教育领域重要数据识别规则

（一）覆盖全国范围的教育机构数据；
（二）1000 万人及以上个人信息或 100 万人及以上敏感个人信息；
（三）全国性的业务数据；
（四）在生成国家秘密的过程中所使用分析的原始非秘密数据；
（五） 经评估的其他数据。

目录

contents

64 问：什么是数据安全风险评估，风险评估的主要内容有哪些？

- 数据安全风险评估是对数据和数据处理活动安全进行信息调研、风险识别、风险分析和风险评价的整个过程。

数据安全风险评估主要内容

信息调研

- 对可能影响数据安全风险的要素的情况调研，包括数据处理者、业务和信息系统、数据资产、数据处理活动、数据安全防护措施。掌握数据处理者、业务和信息系统基本情况，梳理涉及的数据资产和数据处理活动，了解采取的数据安全防护措施情况，掌握被评估对象或同行业相关数据安全事件历史发生情况。

风险识别

- 基于信息调研情况，从数据安全管理、数据处理活动安全、数据安全技术、个人信息保护等方面进行数据安全风险识别，识别评估对象现有安全措施完备性并对其有效性进行验证，识别可能存在的风险源。

风险分析与评价

- 通过分析风险类型、风险危害程度和可能性，评价风险等级。

65 问：有哪些典型的数据安全风险？

序号	风险类别	描述
1	数据泄露风险	由于数据窃取、爬取、脱库、撞库等安全威胁，或者缺乏有效的安全措施、人员操作失误或有意盗取等，导致数据泄露、恶意窃取、未授权访问等影响数据保密性的风险。
2	数据篡改风险	由于数据注入、中间人攻击等安全威胁，或者缺乏有效的安全措施、人员有意或无意操作等，导致数据被未授权篡改等影响数据完整性的风险。
3	数据破坏风险	由于拒绝服务攻击、自然灾害、嵌入恶意代码、数据污染、设备故障等安全威胁，或者缺乏有效的安全措施、人员有意或无意操作等，导致数据被破坏、毁损、数据质量下降等影响数据可用性的风险。
4	数据丢失风险	由于数据过载、软硬件故障、备份失效、链路过载等问题，或者缺乏有效的安全措施、人员有意或无意操作等，导致数据丢失、难以恢复等安全风险。
5	数据滥用风险	由于缺乏授权访问控制、权限管控等有效的安全管控措施、人员有意或无意操作等，导致数据被未授权或超出授权范围使用、加工的风险。
6	数据伪造风险	由于数据源欺骗、深度伪造等安全威胁，或者缺乏有效的安全措施、人员有意或无意操作等，导致数据或数据源被伪造、数据主体被仿冒等安全风险。
7	违法违规获取数据	违反法律、行政法规等有关规定，非法或违规获取、收集数据的风险。
8	违法违规出售数据	违反法律、行政法规等有关规定，非法或违规向他人出售、交易数据的风险。
9	违法违规保存数据	违反法律、行政法规等有关规定，非法或违规留存数据的风险，如逾期留存、违规境外存储等。
10	违法违规利用数据	违反法律、行政法规等有关规定，非法或违规使用、加工、委托处理数据的风险。
11	违法违规提供数据	违反法律、行政法规等有关规定，非法或违规向他人提供、共享、交换、转移数据的风险。
12	违法违规公开数据	违反法律、行政法规等有关规定，非法或违规公开数据的风险。

序号	风险类别	描述
13	违法违规购买数据	违反法律、行政法规等有关规定，非法或违规购买、收受数据的风险。
14	违法违规出境数据	违反法律、行政法规等有关规定，非法或违规向境外提供数据的风险。
15	超范围处理数据	数据处理活动违反必要性原则，超范围或过度收集使用个人信息或重要数据的风险。
16	数据处理缺乏正当性	违反正当性原则，数据处理活动缺乏明确、合理的处理目的。
17	未有效保障个人信息主体权利	由于未采取有效的个人信息保护措施、人员操作或外部威胁等，导致未能有效保障个人信息主体的知情权、决定权、限制或者拒绝个人信息处理等个人信息主体合法权利。
18	App 违法违规收集使用个人信息	App 违反个人信息监管政策或标准规范，存在违法违规收集使用个人信息行为的风险。
19	数据处理缺乏公平公正	由于缺乏安全管控措施、人员有意或无意操作等，导致数据处理违反公平公正、诚实守信原则，侵犯其他组织或个人合法权益的风险。
20	数据处理抵赖风险	由于外部攻击威胁、缺乏有效安全管控措施、人员有意或无意操作等，导致处理者或第三方否认数据处理行为或绕过数据安全措施等风险。
21	数据不可控风险	由于第三方数据安全能力不足、缺乏有效的第三方管控措施、合同协议缺失、外包人员操作等，导致委托处理或合作的第三方违反法律法规或合同协议约定处理数据，造成第三方超范围处理数据、逾期留存数据、违规再转移等数据不可控风险。
22	数据推断风险	由于未考虑数据之间的关联关系，导致从公开数据可推断出核心数据、重要数据、未公开的个人数据等，包括但不限于面向人工智能模型的推理攻击、面向基础设施的跨域推断攻击等
23	其他风险	其他可能影响国家安全、公共利益或组织、个人合法权益的数据安全风险。

参考：《信息安全技术 数据安全风险评估方法（征求意见稿）》

66 问：数据安全风险评估的内容框架包含哪些？

数据安全管理

- 制度流程
- 组织机构
- 分类分级
- 人员管理
- 合作外包管理
- 安全威胁和应急管理
- 开发运维
- 云数据安全

数据处理活动安全

- 数据收集
- 数据存储
- 数据传输
- 数据使用和加工
- 数据提供
- 数据公开
- 数据删除

个人信息保护

- 基本原则
- 告知同意
- 保护义务
- 主体权利
- 投诉举报
- 个人信息处理
- 敏感个人信息保护
- 大型网络平台

数据安全技术

- 网络安全防护
- 身份鉴别与访问控制
- 监测预警
- 数据脱敏
- 数据防泄漏
- 接口安全
- 备份恢复
- 安全审计

信息调研

- 数据处理者基本情况
- 业务和信息系统
- 数据资产情况
- 数据处理活动情况
- 安全防护措施

67 问：数据安全风险评估的一般实施流程？

阶段	具体工作	主要产出物
评估准备	1.确定评估目标 2.确定评估范围 3.组建评估团队 4.开展前期准备 5.制定评估方案	《调研表》 《评估方案》
信息调研	1.数据处理者调研 2.业务和信息系统调研 3.数据资产调研 4.数据处理活动调研 5.安全措施调研	《处理者基本情况》《数据处理活动清单》 《业务清单》《数据流图》 《信息系统清单》《安全措施情况》
风险识别	1.数据安全管理 2.数据处理活动 3.数据安全技术 4.个人信息处理	《文档查阅记录文档》《安全检查记录文档》 《人员访谈记录文档》《技术检测报告》
综合分析	1.梳理问题清单 2.风险分析与评价 3.提出整改建议	《数据安全问题清单》 《数据安全风险》 《整改建议》
评估总结	1.风险评估报告 2.安全风险处置	《风险评估报告》

来源：数据安全风险评估方法（征求意见稿）

68 问：数据安全风险评估的可采取哪些评估方式?

- **人员访谈：**对相关人员进行访谈，核查制度规章、防护措施、安全责任落实情况。

- **问卷调查：**通过设计的问题来了解组织内部员工或相关方对数据安全政策、程序和实践的理解和遵守情况。

- **文档查验：**查验安全管理制度、风险评估报告、等保测评报告等有关材料及制度落实情况的证 明材料。

- **安全核查：**核查网络环境、数据库和大数据平台等相关系统和设备安全策略、配置、防护措施 情况。

- **技术测试：**应用技术工具、渗透测试等手段查看数据资产情况、检测防护措施有效性。

- **威胁建模：**通过威胁建模，识别可能影响组织数据安全的潜在威胁，包括外部攻击者、内部恶意行为和意外泄露等。

69 问：哪些情形易触发数据安全风险评估?

新系统或应用的部署

在新IT系统、软件或应用投入使用前，评估它们是否符合组织的数据安全标准。

01

重大变更或更新

对现有系统、应用或数据处理流程进行重大修改或更新时进行评估。

02

合规性要求

为满足数据安全法律规定或行业主管部门要求，进行数据安全评估。

03

安全事件后

在数据泄露、安全漏洞被发现或其他安全事件后，评估数据安全风险和影响。

04

定期审计

根据组织的政策和程序，定期进行评估以识别和缓解潜在的安全风险。

05

业务扩展或变化

当组织的业务模型、流程或数据处理活动发生重大变化时。

06

第三方服务或供应商变更

在引入新的第三方服务提供商或对现有供应商的服务进行重大更改时。

07

技术环境变化

如云服务迁移、系统升级或新技术的采用等情况下。

08

70 问：金融业机构在哪些情形下需要进行数据安全评估?

- 《金融数据安全 数据安全评估规范》规定金融数据安全评估指金融业机构对其数据处理活动定期或按需开展的风险评估活动，用于评价金融业机构自身和数据处理活动第三方合作机构的数据安全保护能力，为金融业机构建立数据安全保护体系、明确数据安全保护策略和加强第三方合作机构数据安全管理提供参考性资料。金融数据安全评估工作的触发条件至少包括以下情形：

01 对3级及以上数据进行加工前，应进行数据安全评估。

02 使用外部的软件开发包、组件、源码等开展开发测试工作前，应进行数据安全评估。

03 将数据委托给第三方机构进行处理前，应对被委托方的数据安全防护能力进行数据安全评估。

04 与外部机构进行数据共享，应定期对数据接收方的数据安全保护能力进行数据安全评估。

05 在金融产品或服务上线发布前，数据安全管理委员会应组织开展数据安全评估，避免不当的数据采集、使用、共享等行为。

06 若有第三方机构参与到金融业机构数据全生命周期过程，应根据其数据安全保护能力进行数据安全评估。

07 在金融业机构业务功能发生重大变化时，应及时进行数据安全评估。

08 在国家及行业主管部门的相关要求发生变化时，或在业务模式、信息系统、运行环境发生重大变更时，或发生重大数据安全事件时，应进行数据安全评估。

09 每年至少应开展1次全面的数据安全检查评估，评估方式至少包括自评估、外部第三方机构评估等。

71 问：数据安全评估有哪些参与方？

- 数据安全评估通常涉及多个参与方，他们从不同的角度贡献于评估的全面性和有效性。主要参与方包括：信息安全团队、IT部门、法律和合规团队、业务部门代表、数据所有者和数据管理者、高级管理层等。以金融行业为例，《金融数据安全数据安全评估规范》规定了三类评估参与方：

评估参与方	*主要职责*	*部门*
数据安全评估的牵头部门	• 金融数据安全评估的牵头部门，作为评估工作的主要参与方，负责牵头开展评估工作，协调各方资源，保证评估工作的开展，并对评估结果的质量负责。**牵头部门或人员应具有独立性**，不受到被评估方的影响，**通常由机构的数据安全管理有关责任部门担任。**	数据安全管理部门
评估工作过程涉及的内部部门	• 根据金融数据安全评估的范围和内容，识别并确认本次评估工作过程涉及的本机构内部各部门，如业务部门、法务部门、合规部门、技术部门等内部组织，作为本次评估工作的其他参与方。**负责配合开展各部分评估工作**，并负责各有关外部合作方的协调和管理工作，确保评估工作的顺利开展，并对发现的问题进行确认和整改。	参与部门 业务部门 法务部门 合规部门 技术部门 其他部门
独立评审组	• 立独立评审组，**负责对评估过程与结果做真实性与合规性的评审，并确保评审过程的独立性。**评审组直接向本机构本次金融数据安全评估工作最高负责人或本机构数据安全管理委员会领导小组负责。	数据安全评估工作最高负责人/数据安全管理委员会领导小组 独立评审组

72 问：什么是个人信息保护影响评估，如何执行？

- “个人信息保护影响评估”也称“个人信息安全影响评估”，是针对个人信息处理活动，检验其合法合规程度，判断其对个人合法权益造成损害的各种风险，以及评估用于保护个人的各项措施有效性的过程。个人信息保护影响评估是一种风险管理工具，它可以帮助个人信息处理者识别和分析其处理活动可能带来的法律、技术、组织等方面的风险，并采取相应的措施来降低或消除这些风险，从而提高个人信息处理的安全性和合规性。

第一阶段
评估准备阶段

评估必要性分析

- 合规差距评估
- 尽责性风险评估

评估准备工作

- 组织评估团队
- 制定评估计划
- 确定评估对象和范围
- 制定相关方咨询计划

第二阶段
评估实施阶段

- 数据映射分析
- 风险源识别
- 个人权益影响分析
- 安全风险综合分析

第三阶段
报告形成阶段

- 评估报告
- 风险处置和持续改进
- 制定报告发布策略

73 问：开展个人信息保护影响评估有哪些价值?

01 识别风险：在开展个人信息处理前，组织可通过影响评估，识别可能导致个人信息主体权益遭受损害的风险，并据此采用适当的个人信息安全控制措施。

02 控制风险：对于正在开展的个人信息处理，组织可通过影响评估，综合考虑内外部因素的变化情形，持续修正已采取的个人信息安全控制措施，确保对个人合法权益不利影响的风险处于总体可控的状态。

03 有效证明：个人信息安全影响评估及其形成的记录文档，可帮助组织在政府、相关机构或商业伙伴的调查、执法、合规性审计等中，证明其遵守了个人信息保护与数据安全等方面的法律、法规和标准的要求。

04 合规抗辩：在发生个人信息安全事件时，个人信息安全影响评估及其形成的记录文档，可用于证明组织已经主动评估风险并采取一定的安全保护措施，有助于减轻、甚至免除组织相关责任和名誉损失。

05 提升风险意识：组织可通过个人信息安全影响评估，加强对员工的个人信息安全教育。参与评估之中，员工能熟悉各种个人信息安全风险，增强处置风险的能力。

06 增强信任：对合作伙伴，组织通过评估的实际行动表明其严肃对待个人信息安全保护，并引导其能够采取适当的安全控制措施，以达到同等或类似的安全保护水平。

目录

contents

74 问：什么是数据安全事件，典型事件有哪些？

- 数据安全事件指通过技术或其他手段对数据实施篡改、假冒、泄露、窃取等导致业务损失或造成社会危害的网络安全事件。《信息安全技术网络安全事件分类分级指南（GB/T 20986—2023）》定义了12种数据安全事件：

数据篡改事件 • 指未经授权接触或修改数据。	**数据假冒事件** • 指非法或未经许可使用、伪造数据。	**数据泄露事件** • 指无意或恶意通过技术手段使数据或敏感个人信息对外公开泄露。	**社会工程事件** • 指通过非技术手段(如心理学、话术等)诱导他人泄露数据或执行行动。
数据窃取事件 • 指未经授权利用技术手段偷窃数据。	**数据拦截事件** • 指在数据到达目标接收者之前非法捕获数据。	**位置检测事件** • 指非法检测系统、个人的地理位置信息或敏感数据的存储位置。	**数据投毒事件** • 指干预深度学习训练数据集，在训练数据中加入精心构造的异常数据，破坏原有训练数据的概率分布，导致模型在某些特定条件下产生分类或聚类错误。
数据滥用事件 • 指无意或恶意滥用数据。	**隐私侵犯事件** • 指无意或恶意侵犯网络中存在的敏感个人信息。	**数据损失事件** • 指因误操作、人为蓄意或软硬件缺陷等因素导致数据损失。	**其他数据安全事件** • 指不在以上子类之中的数据安全事件。

75 问：什么是网络安全事件，如何进行事件分级？

- 依据《网络安全事件报告管理办法（征求意见稿）》：网络安全事件是指由于人为原因、软硬件缺陷或故障、自然灾害等，对网络和信息系统或其中的数据造成危害，对社会造成负面影响的事件。运营者在发生网络安全事件时，应当及时启动应急预案进行处置。

分级	基本情形	具体条件
特别重大网络安全事件	1.重要网络和信息系统遭受特别严重的系统损失，造成系统大面积瘫痪，丧失业务处理能力。 2.国家秘密信息、重要敏感信息、重要数据丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成特别严重威胁。 3.其他对国家安全、社会秩序、经济建设和公众利益构成特别严重威胁、造成特别严重影响的网络安全事件。	1.省级以上党政机关门户网站、重点新闻网站因攻击、故障，导致24小时以上不能访问。 2.关键信息基础设施整体中断运行6小时以上或主要功能中断运行24小时以上。 3.影响单个省级行政区30%以上人口的工作、生活。 4.影响1000万人以上用水、用电、用气、用油、取暖或交通出行。 5.重要数据泄露或被窃取，对国家安全和社会稳定构成特别严重威胁。 6.泄露1亿人以上个人信息。 7.党政机关门户网站、重点新闻网站、网络平台等重要信息系统被攻击篡改，导致违法有害信息特大范围传播。以下情况之一，可认定为“特大范围”： （1）在主页上出现并持续6小时以上，或在其他页面出现并持续24小时以上； （2）通过社交平台转发10万次以上； （3）浏览或点击次数100万以上； （4）省级以上网信部门、公安部门认定为是“特大范围传播”的。 8.造成1亿元以上的直接经济损失。 9.其他对国家安全、社会秩序、经济建设和公众利益构成特别严重威胁、造成特别严重影响的网络安全事件。
重大网络安全事件	1.重要网络和信息系统遭受严重的系统损失，造成系统长时间中断或局部瘫痪，业务处理能力受到极大影响。 2.国家秘密信息、重要敏感信息、重要数据丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成严重威胁。 3.其他对国家安全、社会秩序、经济建设和公众利益构成严重威胁、造成严重影响的网络安全事件。	1.地市级以上党政机关门户网站、重点新闻网站因攻击、故障，导致6小时以上不能访问。 2.关键信息基础设施整体中断运行2小时以上或主要功能中断运行6小时以上。 3.影响单个地市级行政区30%以上人口的工作、生活。 4.影响100万人以上用水、用电、用气、用油、取暖或交通出行。 5.重要数据泄露或被窃取，对国家安全和社会稳定构成严重威胁。 6.泄露1000万人以上个人信息。 7.党政机关门户网站、重点新闻网站、网络平台等被攻击篡改，导致违法有害信息大范围传播。以下情况之一，可认定为“大范围”： （1）在主页上出现并持续2小时以上，或在其他页面出现并持续12小时以上； （2）通过社交平台转发1万次以上； （3）浏览或点击次数10万以上； （4）省级以上网信部门、公安部门认定为是“大范围传播”的。 8.造成2000万元以上的直接经济损失。 9.其他对国家安全、社会秩序、经济建设和公众利益构成严重威胁、造成严重影响的网络安全事件。
较大网络安全事件	1.重要网络和信息系统遭受较大的系统损失，造成系统中断，明显影响系统效率，业务处理能力受到影响。 2.国家秘密信息、重要敏感信息、重要数据丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成较严重威胁。 3.其他对国家安全、社会秩序、经济建设和公众利益构成较严重威胁、造成较严重影响的网络安全事件。	1.地市级以上党政机关门户网站、重点新闻网站因攻击、故障，导致2小时以上不能访问。 2.关键信息基础设施整体中断运行30分钟以上或主要功能中断运行2小时以上。 3.影响单个地市级行政区10%以上人口的工作、生活。 4.影响10万人以上用水、用电、用气、用油、取暖或交通出行。 5.重要数据泄露或被窃取，对国家安全和社会稳定构成较严重威胁。 6.泄露100万人以上个人信息。 7.党政机关门户网站、重点新闻网站、网络平台等被攻击篡改，导致违法有害信息较大范围传播。以下情况之一，可认定为“较大范围”： （1）在主页上出现并持续30分钟以上，或在其他页面出现并持续2小时以上； （2）通过社交平台转发1000次以上； （3）浏览或点击次数1万以上； （4）省级以上网信部门、公安部门认定为是“较大范围传播”的。 8.造成500万元以上的直接经济损失。 9.其他对国家安全、社会秩序、经济建设和公众利益构成较严重威胁、造成较严重影响的网络安全事件。
一般网络安全事件	除上述网络安全事件外，对国家安全、社会秩序、经济建设和公众利益构成一定威胁、造成一定影响的网络安全事件。	/

76 问：什么是应急预案，涉及哪些法律要求?

- 数据安全事件应急预案是组织为应对数据安全事件而制定的一系列预先定义的响应措施和程序。这个预案旨在最小化数据安全事件对组织运营、声誉和利益造成的损害，并确保在事件发生时能够迅速、有效地恢复正常运营。

《网络安全法》

第二十五条　网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，**立即启动应急预案**，采取相应的补救措施，并按照规定向有关主管部门报告。

第三十四条　除本法第二十一条的规定外，关键信息基础设施的运营者还应当履行下列安全保护义务:

（一）设置专门安全管理机构和安全管理负责人，并对该负责人和关键岗位的人员进行安全背景审查；

（二）定期对从业人员进行网络安全教育、技术培训和技能考核；

（三）对重要系统和数据库进行容灾备份；

（四）**制定网络安全事件应急预案，并定期进行演练**；

（五）法律、行政法规规定的其他义务。

《数据安全法》

第二十三条 国家建立数据安全应急处置机制。发生数据安全事件，有关主管部门应当依法启动应急预案，**采取相应的应急处置措施**，防止危害扩大，消除安全隐患，并及时向社会发布与公众有关的警示信息。

《个人信息保护》

第五十一条　个人信息处理者应当根据个人信息的处理目的、处理方式、个人信息的种类以及对个人权益的影响、可能存在的安全风险等，采取下列措施确保个人信息处理活动符合法律、行政法规的规定，并防止未经授权的访问以及个人信息泄露、篡改、丢失:

……

（四）合理确定个人信息处理的操作权限，并定期对从业人员进行安全教育和培训；

（五）**制定并组织实施个人信息安全事件应急预案**；

《网络安全等级保护条例（征求意见稿）》

第三十二条**【应急处置要求】**第三级以上网络的运营者应当按照国家有关规定，**制定网络安全应急预案，定期开展网络安全应急演练**。
发生重大网络安全事件时，**有关部门应当按照网络安全应急预案要求联合开展应急处置**。

第四十二条【涉密网络预警通报要求】涉密网络运营者应建立健全本单位涉密网络安全保密监测预警和信息通报制度，发现安全风险隐患的，**应及时采取应急处置措施**，并向保密行政管理部门报告。

第五十九条【行业监督管理】
行业主管部门应当监督管理本行业、本领域网络运营者依照网络安全等级保护制度和相关标准规范要求，落实网络安全管理和技术保护措施，组织开展网络安全防范、**网络安全事件应急处置、重大活动网络安全保护等工作**。

《网络数据安全管理条例(征求意见稿)》

第十一条 数据处理者应当建立数据安全应急处置机制，**发生数据安全事件时及时启动应急响应机制**，采取措施防止危害扩大，消除安全隐患。安全事件对个人、组织造成危害的，数据处理者应当在三个工作日内将安全事件和风险情况、危害后果、已经采取的补救措施等以电话、短信、即时通信工具、电子邮件等方式通知利害关系人，无法通知的可采取公告方式告知，法律、行政法规规定可以不通知的从其规定。安全事件涉嫌犯罪的，数据处理者应当按规定向公安机关报案。

第二十八条 重要数据的处理者，应当明确数据安全负责人，成立数据安全管理机构。数据安全管理机构在数据安全负责人的领导下，履行以下职责:

……

（二）制定实施数据安全保护计划和数据安全事件应急预案；

77 问：什么是数据安全应急演练，有哪些演练类型？

- 数据安全应急演练是一种预先设计的模拟活动，旨在通过模拟数据安全事件的发生，来测试和评估组织的应急响应计划、团队协作、技术能力和流程有效性。其核心目的在于通过这种实战模拟，提高组织应对真实数据安全事件的能力，确保在发生实际安全威胁时，组织能够迅速、有效地采取应对措施，最大程度地减少潜在的损失和影响。

01 桌面演练

特点：通过讨论形式进行，不涉及实际的系统操作或技术干预。

目的：主要用于评估和讨论应急响应计划、流程和决策过程，强调团队沟通和决策能力。

02 功能演练

特点：模拟实际操作环境，但不影响生产系统，重在测试特定功能或响应能力。

目的：检验特定应急响应功能（如通知流程、数据备份恢复）的有效性。

03 全面演练

特点：最为复杂和真实的演练形式，可能涉及真实系统的操作，需要广泛的资源和人员参与。

目的：全面检验组织在实际操作环境下的响应能力，包括技术、物理和逻辑响应。

04 走查测试

特点：通过逐步走查应急响应流程来进行，侧重于逐步检查每个步骤的准确性和可行性。

目的：确保应急响应计划的每个步骤都是清晰和可执行，发现并修正流程中的任何遗漏或错误。

05 模拟攻击

特点：模拟真实的攻击场景，如使用红队（攻击方）对蓝队（防御方）进行模拟攻击。

目的：测试组织对于突发安全事件的检测、反应和恢复能力，同时提升安全团队的技能和协作。

06 红蓝对抗

特点：更高级的模拟攻击形式，红队模拟攻击者角色，而蓝队负责防御。

目的：通过对抗演练深入检验组织的侦测、防御和应对策略的有效性。

78 问：应急演练的流程及常见演练方法？

准备

目标设定：明确演练的目的和预期成果。
场景设计：根据目标设计演练场景。
角色分配：确定参与演练的团队和成员。
资源准备：准备所需的资源和工具。
沟通计划：制定演练期间沟通计划。

执行

启动演练：根据设计的场景模拟数据安全事件的发生。
角色扮演：参与者根据各自的角色和职责执行响应任务。
实时监控：实时监控演练的进展。
调整反馈：根据演练实际情况适时调整演练计划。

评估

总结会议：演练结束后，召开总结会议。
性能评估：评估演练的效果，与预设目标进行对比，识别差距和不足之处。
详细报告：编写详细的演练报告，包括演练过程、发现的问题、改进建议等。

改进

制定改进计划：根据评估结果和报告中的建议，制定具体的改进措施和计划。
执行改进措施：落实改进计划，对应急响应计划、技术控制、流程等进行必要的修改和优化。
跟踪和复审：定期跟踪改进措施的实施情况。

演练方法

情景讨论

- 参与者围绕一个或多个具体的安全事件情景进行讨论。

角色扮演

- 参与者根据事先分配的角色（如安全管理员、技术支持、管理层等）参与模拟事件的处理。

沙盘推演

- 使用模型或图形工具模拟网络环境和事件场景，参与者根据模拟环境进行决策和响应。

实战演习

- 在控制的环境中进行真实操作，可能涉及到实际系统和网络的操作。

79 问：什么是数据泄露，企业应如何准备应对数据泄露事件?

- 数据泄露是指敏感、受保护或机密信息被未经授权的个人访问、查看或窃取的事件。这种情况可能发生在各种环境中，包括个人、企业、政府机构等，且可能涉及从个人身份信息到国家安全信息等各种类型的数据。数据泄露可能是由于安全漏洞、人为错误、内部恶意行为或外部攻击等原因造成的。

如何应对数据泄露

更多精彩内容点击→

80 问：如何建立跨部门的数据泄露响应团队？

确定团队领导	组建跨部门团队	定义具体职责	建立指挥链和决策流程

- 选择具有领导决策能力和跨部门协调能力的人担任团队领导，通常这个人应该具备足够的权威和经验来指导团队应对紧急情况。
- 组建跨部门数据泄露响应团队这个过程旨在确保快速、协调一致的应对措施，以最小化数据泄露可能造成的影响。
- 每个团队成员应该有明确的职责和行动指南，确保在数据泄露事件发生时能够迅速、有效地采取行动。
- 明确在数据泄露响应过程中的指挥链和决策流程，确保在紧急情况下能够快速做出决策并采取行动。

81 问：如何有效地通知受数据泄露影响的个人？

- **通知内容的核心要素：**

■ **事件概述：**提供数据泄露事件的基本信息，包括何时、如何发现泄露，以及初步判断的泄露原因。

■ **受影响的数据类型：**明确列出受影响的数据类型，如个人识别信息（PII）、财务信息、健康记录等，以便个人了解哪些具体信息可能已泄露。

■ **潜在影响：**说明数据泄露可能对受影响个人造成的潜在影响，如身份盗窃风险、财务损失等。

■ **已采取的措施：**介绍企业已经采取或计划采取的措施来应对数据泄露并减轻其影响，如增强安全措施、与执法机构合作调查等。

■ **对受影响者的建议：**提供给受影响个人的建议和指导，帮助他们保护自己免受数据泄露的进一步影响。

■ **获取帮助的途径：**提供受影响者可以获得更多信息和帮助的渠道，如专门的客服热线、电子邮件地址等。

■ **表达歉意和承诺改进：**对所发生的数据泄露事件表达诚挚的歉意，并承诺采取措施防止未来类似事件的发生。

82 问：如何评估数据泄露的影响和损害？

确定泄露数据的敏感性

- **数据类型：**分析泄露数据的类型，如个人身份信息、健康记录、财务信息等，以及这些数据的保密性、完整性和可用性要求。
- **敏感性评估：**评估数据的敏感程度和保护需求，高敏感度数据的泄露将导致更严重的影响。

评估受影响用户数量

- **影响范围：**确定受影响的个人或用户群体的数量，大规模的数据泄露将导致更广泛的影响。
- **用户影响：**评估泄露数据对受影响个人的具体影响，包括潜在的身份盗窃、隐私侵犯等问题。

分析泄露对业务运营的影响

- **业务中断：**评估数据泄露是否导致关键业务流程中断或服务不可用，以及恢复正常运营所需的时间和资源。
- **客户信任：**考虑数据泄露事件对客户信任和客户关系的长期影响，以及可能的客户流失。

评估潜在的法律和财务后果

- **合规责任：**分析数据泄露事件是否违反了数据安全法规以及可能面临的法律责任和罚款。
- **财务损失：**评估直接的财务损失，如罚款、赔偿和诉讼费用，以及间接损失，如品牌损害和市场份额下降所导致的长期财务影响。

83 问：如何利用技术工具来应对数据泄露？

反恶意软件工具：针对恶意软件的专门防御，保护系统不受病毒、木马、勒索软件等威胁的侵害。

数据防泄露解决方案：专注于敏感数据的管理，防止数据通过电子邮件、网页或其他传输途径泄露。

安全信息和事件管理系统：通过实时收集和分析安全日志数据来监控网络和系统的安全状态，提供全面的安全事件监控和报警机制。

数据加密软件：确保数据在存储和传输过程中的安全，即使数据被访问也无法被未授权者解读。

防火墙和入侵检测系统：作为网络的第一道防线，监控和控制进出的网络流量，防止未经授权的访问。

84 问：在数据泄露事件中，法律义务和考量包括哪些？

监管机构：组织可能需要在特定时间内向监管机构报告数据泄露事件。
受影响个人：法规可能还要求组织通知受数据泄露影响的个人，告知泄露的性质、影响和保护措施。

合规性审查：评估数据泄露是否因违反数据安全法规而发生，可能涉及内部审计或外部调查。
法律诉讼：面临受影响个人或集体提起的法律诉讼，可能导致赔偿责任。

合同义务：检查与第三方的合同条款，确定数据泄露是否违反了与客户、供应商或合作伙伴的协议。

文档记录和保留：保留关于数据泄露发现、响应和通报过程的详细记录，以备未来审计和法律审查之用。

跨境数据传输问题：如果数据泄露涉及跨境传输，需要遵守国际数据保护法规的要求。

保险覆盖：了解组织的的保险政策是否覆盖数据泄露事件，以及如何进行理赔。

85 问：数据泄露发生后，如何进行事后分析和教训总结?

根本原因： 确定数据泄露的直接原因，如系统漏洞、策略缺失或操作失误，以及这些因素如何相互作用导致了安全事件。

02

事件影响： 概述数据泄露对个人隐私、组织运营、客户关系和品牌声誉的影响，包括短期和长期的影响。

04

教训与见解： 提炼从事件中学到的关键教训和见解，这些可能涉及组织的安全文化、内部流程、技术架构或与第三方的合作关系。

确定根本原因 → 评估安全措施效能 → 概述事件影响 → 明确改进领域 → 提炼教训与见解

01

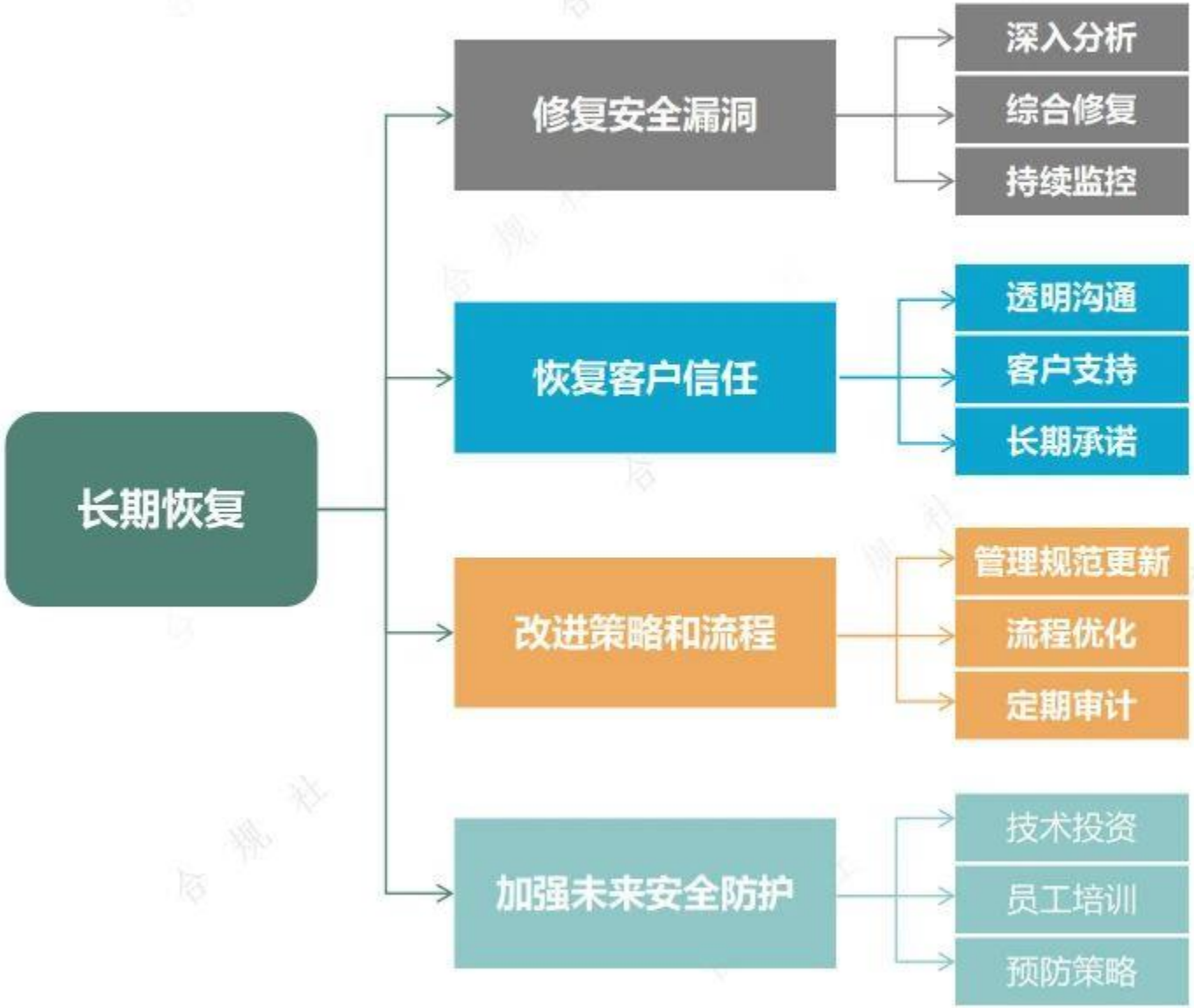
安全措施的效能： 评估现有安全控制措施在事件中的表现，识别哪些措施有效阻止或缓解了事件的影响，哪些措施未能发挥作用及其原因。

03

改进领域： 基于事件分析，明确需要加强或改进的安全领域，这可能包括技术防护、员工培训、政策更新或事故响应流程。

05

86 问：在数据泄露事件后，长期恢复需要关注哪些关键领域？



- 彻底调查数据泄露的根本原因，识别所有相关的安全漏洞。
- 基于调查结果，制定并实施一个综合的修复计划。
- 加强安全监控措施，确保漏洞修复后系统的安全性得到持续维护。
- 通过透明、及时的沟通向客户说明发生了什么，企业采取了哪些措施来解决问题，并表达诚意。
- 提供额外的客户支持服务，如身份盗窃保护服务，帮助客户减轻数据泄露的影响。
- 展示企业对改进数据安全和保护客户信息的长期承诺。
- 根据数据泄露事件的教训，更新数据安全管理规范及指南。
- 优化数据处理流程，确保数据安全控制得到有效实施。
- 定期进行安全审计，确保策略和流程的实施与组织的安全目标保持一致。
- 投资于先进的安全技术和工具，如加强端点防护、网络监控和入侵检测系统。
- 加强对员工安全意识培训，提高识别和防范安全威胁能力。
- 发展和实施一套全面的风险管理和预防策略，以减少未来数据泄露的风险。

目录

contents

87 问：什么是个人信息，有哪些典型示例？

- 个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。

类别	举例
个人基本资料	个人姓名、生日、性别、民族、国籍、家庭关系、住址、个人电话号码、电子邮件地址等
个人身份信息	身份证、军官证、护照、驾驶证、工作证、出入证、社保卡、居住证等；
个人身份识别信息	个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等；
网络身份标识信息	个人信息主体账号、IP地址、个人数字证书等；
个人健康生理信息	个人因生病医治等产生的相关记录，如病症、住院志、医嘱单、检验报告、手术及麻醉记录、护理记录、用药记录、药物食物过敏信息、生育信息、以往病史、诊治情况、家族病史、现病史、传染病史等，以及与个人身体健康状况相关的信息，如体重、身高、肺活量等；
个人教育工作信息	个人职业、职位、工作单位、学历、学位、教育经历、工作经历、培训记录、成绩单等；
个人财产信息	银行账户、鉴别信息(口令)、存款信息（包括资金数量、支付收款记录等）、房产信息、信贷记录、征信信息、交易和消费记录、流水记录等，以及虚拟货币、虚拟交易、游戏类兑换码等虚拟财产信息；
个人通信信息	通信记录和内容、短信、彩信、电子邮件，以及描述个人通信的数据（通常称为元数据）等；
联系人信息	通讯录、好友列表、群列表、电子邮件地址列表等；
个人上网记录	指通过日志储存的个人信息主体操作记录，包括网站浏览记录、软件使用记录、点击记录、收藏列表等；
个人常用设备信息	指包括硬件序列号、设备MAC地址、软件列表、唯一设备识别码等在内的描述个人常用设备基本情况的信息；
个人位置信息	包括行踪轨迹、精准定位信息、住宿信息、经纬度等；
其他信息	婚史、宗教信仰、性取向、未公开的违法犯罪记录等。

88 问：什么是敏感个人信息，有哪些典型示例？

- 敏感个人信息是指一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，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。

类别	典型示例
生物识别信息	个人基因、指纹、声纹、掌纹、眼纹、耳廓、虹膜、面部识别特征、步态等
宗教信仰信息	信仰的宗教、加入的宗教组织、宗教组织中的职位、参加的宗教活动、特殊宗教习俗等
特定身份信息	犯罪人员身份信息、残障人士身份信息、特定工作信息（如军人、警察）、身份证件号码等
医疗健康信息	病症、住院志、医嘱单、检验报告、检查报告、手术及麻醉记录、护理记录、用药记录、生育信息、家族病史、传染病史等
金融账户信息	银行、证券、基金、保险、公积金等账户的账号及密码，公积金联名账号、支付账号、银行卡磁道数据（或芯片等效信息）以及基于账户信息产生的支付标记信息等
行踪轨迹信息	实时精准定位信息、GPS 车辆轨迹信息、航班车票信息、特定住宿信息等
不满十四周岁未成年人个人信息	不满十四周岁未成年人的个人信息
身份鉴别信息	登陆密码、支付密码、账户查询密码、交易密码、动态口令、口令保护答案等
其他敏感个人信息	网页浏览信息、婚史、性取向、通信内容、征信信息、未公开的违法犯罪记录等

89 问：什么是敏感个人信息，如何识别敏感个人信息？

应识别为
敏感个人信息的情形

- 个人信息遭到泄露或者非法使用，容易导致自然人的人格尊严受到侵害。
- 个人信息遭到泄露或者非法使用，容易导致自然人的人身安全受到危害。
- 个人信息遭到泄露或者非法使用，容易导致自然人的财产安全受到危害。

整体具有
敏感个人信息属性的判断

- 总体考虑个人信息汇聚融合后的整体属性，如汇聚融合的个人信息遭到泄露或者非法使用容易对个人权益造成较大影响的，应判断个人信息整体具有敏感个人信息属性。

90 问：处理敏感个人信息有哪些基本要求？

- 处理敏感个人信息应具有特定的目的和充分的必要性，取得个人的单独同意，应在满足GB/T35273—2020要求的基础上，在收集、存储、使用、加工、传输、提供、公开、删除等处理的各个环节采取严格保护措施。

具有特定的目的	具有充分的必要性	取得个人的单独同意	采取严格保护措施

91 问：收集敏感个人信息前，应采用哪种告知方式?

- 参考《信息安全技术 敏感个人信息处理安全要求》，个人信息处理者在收集敏感个人信息前，应采用以下告知方式：

增加形式告知	• 在收集敏感个人信息前，应采用增强形式向个人进行告知； 注：如通过**单独弹窗**、**短信**、**填写框**、**动画**、**转至单独提示界面**等方式告知个人信息主体。
持续提示或间隔提示	• 利用App持续收集敏感个人信息的，应提供持续提示或间隔提示机制； 注：持续收集指在用户使用服务期间不间断的连续收集用户信息，**如录音、录像、连续的位置轨迹等**。 注：如出行导航类需持续收集个人信息主体地理位置信息，以**浮窗、弹窗、语音或振动等**形式间隔一定时间提醒个人信息主体当前地理位置正在被使用。
告知内容	• 应向个人信息主体告知个人信息处理者的身份和联系方式等基本情况，敏感个人信息的处理目的、处理方式以及必要性，敏感个人信息的种类、保存期限以及对个人权益的影响，个人信息主体行使个人信息权利的方式和途径；
紧急情况下的例外	• 紧急情况下为保护自然人的生命健康和财产安全无法及时向个人告知的，个人信息处理者应在紧急情况消除后及时告知；
终止时的告知	• 所提供的服务明确不再收集敏感个人信息时或不承担敏感个人信息保护责任时，应对个人信息主体进行提示。

92 问：收集敏感个人信息前，如何获得用户同意？

- 参考《信息安全技术 敏感个人信息处理安全要求》，个人信息处理者在收集敏感个人信息前，有以下获得同意的方式：

01 事先同意

■ 基于个人同意进行处理的，个人信息处理者应在处理敏感个人信息前，取得个人信息主体的单独同意。

02 书面同意

■ 在法律法规另有明确规定时取得个人信息主体的书面同意。

03 单独同意

■ 多项敏感个人信息处理活动，应按处理目的为个人信息主体提供单独同意机制。

04 同意撤回

■ 基于个人同意处理敏感个人信息的，个人信息处理者应为个人提供便捷的撤回同意的方式，同时宜向个人说明撤回同意可能对个人产生的影响。

05 处理已公开的敏感个人信息的单独同意

■ 个人信息处理者处理已公开的敏感个人信息，经评估对个人权益有重大影响的，应取得个人的单独同意。

06 公开场所收集时的单独同意

■ 在公共场所安装图像采集、个人身份识别设备的，应设置显著的提示标识，除取得个人信息主体单独同意以外，所收集的个人图像、身份识别信息类敏感个人信息原则上只能用于维护公共安全的目的，不应用于其他目的。

07 处理不满十四周岁未成年个人信息的同意规则

■ 个人信息处理者基于个人同意处理不满十四周岁未成年人个人信息的，应取得未成年人的父母或者其他监护人的同意。

93 问：敏感个人信息应遵循哪些安全保护措施？

- **参考《信息安全技术 敏感个人信息处理安全要求》，个人信息处理者在收集敏感个人信息前，应遵守以下要求：**

01 应遵循所约定的处理目的、处理方式开展敏感个人信息处理活动，并对处理情况进行记录；

记录处理情况

02 应在个人信息接收方的个人信息保护能力不低于个人信息处理者的条件下传输敏感个人信息；

对接收方的要求

03 互联网传输敏感个人信息时，应至少采用通道加密方式进行传输，宜采用通道加密与内容加密两种加密方式结合进行，通道加密和内容加密算法应符合有关行业技术标准与行业主管部门有关规定要求；

通道加密传输

04 应定期评估或验证敏感个人信息传输方式的安全状况,网络环境发生重大变化时，应及时调整安全策略；

定期评估

05 经过加密、去标识化处理后的敏感个人信息应与解密密钥、其他个人信息等分开存储；

分开存储

06 对敏感个人信息的访问、修改、删除、导出等操作，应在对角色权限控制的基础上，按照业务流程的需求触发操作授权，定期针对敏感个人信息的访问、修改、删除、导出等操作进行日志审计；

日志审计

07 敏感个人信息存储环境应建立异常监测和分析能力，对出现的异常情况进行及时响应，动态调整安全保护措施，按照就高从严原则设定安全保护措施；

异常监测

08 对敏感个人信息的处理活动应建立异常监测预警和响应机制，对超出业务正常需求的异常操作（如频繁、大量敏感个人信息浏览查询、下载、打印，非工作时间操作等）应采取中断操作，并通过邮件、消息、弹窗等形式进行告警，开展分析调查，提前排除隐患；

预警响应

09 敏感个人信息展示界面宜添加包括访问主体标识、访问时间等内容的水印，宜默认禁用复制、打印、截屏等功能；

界面展示要求

10 应定期评估敏感个人信息删除或匿名化处理效果，确保已删除或匿名化处理的敏感个人信息不具备还原能力；

不具备还原能力

11 应定期梳理应用及API资产清单，定期针对应用及API传输敏感个人信息情况进行审计；

定期梳理应用及API资产清单

12 应建立敏感个人信息过期自动删除机制，法律、行政法规规定需要留存敏感个人信息的，应在到期后及时删除。

定期删除

94 问：哪些情形下，处理个人信息时需向个人进行告知？

- 依据《信息安全技术 个人信息处理中告知和同意的实施指南（GB/T 42574—2023）》，告知的适用情形包括：

收集个人信息	通过个人填写、勾选、上传等方式收集个人信息	通过软件程序或硬件设备等自动采集个人信息	与个人交互并记录个人的行为	第三方间接获取个人信息
	从非完全公开渠道获取个人信息	从与个人相关的他人账号收集个人信息	使用大数据、人工智能等技术分析、关联或生成个人信息	
提供、公开个人信息	向其他个人信息处理者提供个人信息	向境外提供个人信息	在一定范围内或向不特定范围公开个人信息	因合并、分立、解散、被宣告破产等原因转移个人信息
处理活动等发生变更	个人信息的处理目的、处理方式发生变更	处理的个人信息种类发生变更	因合并、分立、解散、被宣告破产等原因转移个人信息，接收方变更原先的处理目的、处理方式的	向其他个人信息处理者提供其处理的个人信息，接收方变更原先的处理目的、处理方式的
	公开的范围发生变更，如从一定范围内公开变为向不特定范围公开	个人信息的保存期限延长	个人信息处理者的名称或者姓名和联系方式发生变更	个人行使其权利的方式和程序发生变更
事后处理	两个及以上的个人信息处理者共同决定个人信息的处理目的和处理方式的	在产品或服务中接入需处理个人信息的其他个人信息处理者的产品或服务的	处理的个人信息涉及该个人以外的其他人的	处理已公开的个人信息，对个人权益有重大影响的
	停止运营某类业务功能，或停止运营产品或服务时	个人行使权利，可能对其权益产生影响的	发生或者可能发生个人信息泄露、篡改、丢失等安全事件时	其它情形处理个人信息的，采取适当方式向个人进行告知（履行合同、法定、公共卫生事件、公共利益、合理范围等）

95 问：个人信息告知和同意过程中应遵循哪些基本原则？

- 依据《信息安全技术 个人信息处理中告知和同意的实施指南（GB/T 42574—2023）》，告知的适用情形包括：

个人信息处理者在实施告知时需考虑以下基本原则：

01 **公开透明：**公布处理个人信息的种类、目的、方式、安全措施等处理规则，不采取故意遮挡、隐藏等方式诱导个人略过告知内容。

02 **有效传达：**尽可能通过交互式界面、邮件、电话或短信等方式向相关个人进行告知。

03 **适时充分：**在收集、提供、公开等个人信息处理活动发生之前或同时，对个人进行充分告知。

04 **真实明确：**告知个人信息的处理种类、目的、方式等规则与实际情况一致，且需结合实际业务功能，不使用笼统、宽泛的表述。

05 **清晰易懂：**告知文本符合个人的语言习惯，使用通用且无歧义的语言、数字、图示等。

个人信息处理者在取得个人同意时需考虑以下基本原则：

01 **告知一致：**增强告知的内容需浓缩一般告知的关键规则，突出展示个人最关心的内容，语言简洁、精炼，方便阅读。

02 **自主选择：**增强告知的方式需凸显与一般告知方式的差异，其告知内容更加容易。

03 **时机恰当：**涉及发生停止运营某类业务功能，或停止运营产品或服务、涉及合并、分立、解散、被宣告破产等特殊情形的，宜通过邮件。

04 **避免捆绑：**涉及可能对个人权益产生重大影响的个人信息处理活动时，还可选择使用电话、语音提示等方式进一步进行增强告知，以确保告知内容能够送达。

96 问：实施告知和同意过程中，应考虑哪些要素？

- 依据《信息安全技术 个人信息处理中告知和同意的实施指南（GB/T 42574—2023）》，个人信息处理者在实施告知和同意时宜考虑以下要素，优化告知和同意的方案和机制：

01 友好展示

- **友好展示：**使用友好、生动、形象的方式编辑告知内容，优化告知内容组织形式，以促进个人理解。

02 适配媒体

- **适配媒体：**告知内容、展示形式、取得同意的方式等可根据告知媒体的种类、界面特点进行适应性设计，如适宜的字型大小、字体颜色、额外的震动和语音提示等。

03 考虑影响

- **考虑影响**：设计告知和同意方案时，可考虑个人信息处理活动对个人权益的影响程度以及个人的体验、习惯、合理预期等因素。

04 区分阶段

- **区分阶段：**根据个人使用产品或服务的不同阶段及交互场景，选用个人信息保护政策、弹窗提示、文字说明等不同的告知和同意方案。

05 安全制度体系建立与发布

- **兼顾差异：**考虑复杂多样的网络条件、软硬件差异、个人的知识水平和理解能力、身体机能差异等，使用可广泛适用且兼顾特定群体的告知和同意方案。

97 问：人脸识别数据收集有哪些要求？

收集人脸识别数据的要求

- **告知同意**
  - **收集人脸识别数据时，应向数据主体告知人脸识别数据的相关事项**，包括但不限于数据处理者的名称和联系方式、个人信息保护负责人的姓名和联系方式、处理规则、必要性依据等，并征得数据主体单独同意或书面同意；**未取得数据主体单独同意收集的人脸图像应立即删除并确保不可恢复。**
- **不应拒绝**
  - **数据主体不同意收集人脸识别数据的，不应拒绝数据主体使用基本业务功能；**
- **持续告知**
  - **应采用需要数据主体主动配合的措施收集人脸识别数据；**应在识别过程中持续告知数据主体验证目的，并通过语言、文字等向数据主体进行提示。
- **最小最少**
  - **应仅收集生成人脸特征所需的最小数量、最少图像类型的人脸图像。**
- **安全措施**
  - **应采取安全措施保证人脸识别数据的真实性、完整性和一致性，防止人脸识别数据在收集过程中泄漏或篡改。**

参考：《信息安全技术 人脸识别数据安全要求（GB/T 41819-2022）》

98 问：人脸识别数据存储有哪些要求？

- **数据处理者存储人脸识别数据的要求如下：**

分别存储

➢ 应采用物理或逻辑隔离方式分别存储人脸识别数据和个人身份信息等。

加密存储

➢ 应采取加密存储等安全措施存储人脸识别数据。

数据主体可删除

➢ 数据主体个人所有且具备人脸识别功能的信息技术产品，包括但不限于移动智能终端、智能家居设备等，应将人脸识别数据存储在信息技术产品中，并可由数据主体删除。

参考：《信息安全技术 人脸识别数据安全要求（GB/T 41819-2022）》

99 问：人脸识别数据使用有哪些要求？

数据处理者使用人脸识别数据的要求

识别后立即删除

- **应在使用人脸识别数据识别自然人身份后立即删除用于识别的人脸图像。**

优先使用本地人脸识别

- **在本地和远程人脸识别方式均适用时，应优先使用本地人脸识别；**
- 注:本地人脸识别是在终端设备中进行人脸识别数据收集、使用等处理活动的过程，该方式中人脸识别数据的处理均在终端设备完成。远程人脸识别是在终端设备收集人脸识别数据，在服务器端使用人脸识别数据的过程，该方式中人脸识别数据的处理在终端设备和服务器端分别进行。

可更新、不可逆、不可链接

- **人脸特征应具有可更新、不可逆、不可链接的特性；**
- 注:可更新指当特定人脸特征泄漏或作废时，同一人脸图像可提取与该特征不同的人脸特征；不可逆指无法从人脸特征恢复出对应的人脸图像。不可链接指同一人脸图像提取的不同人脸特征之间不具备关联性。

使用审计

- **应对人脸识别数据使用行为进行审计。**

参考：《信息安全技术 人脸识别数据安全要求（GB/T 41819-2022）》

100 问：人脸识别数据传输有哪些要求？

- 数据处理者应采取双向身份鉴别、数据完整性校验、数据加密等措施保障人脸识别数据传输安全。

双向身份鉴别

- 通常通过密码、数字证书、生物识别或者多因素认证方法来实现，确保只有授权的用户或系统才能参与数据的传输，从而减少了冒名顶替或未授权访问的风险。

数据完整性校验

- 数据完整性校验确保在数据的创建、存储、传输或处理过程中数据不被未授权修改、删除或破坏，对于保护数据可靠性和准确性至关重要，通常通过哈希函数、数字签名、密钥来实现。

数据加密

- 数据加密通常通过公钥基础设施、对称密钥加密或其他加密算法来实现。加密确保了即使数据在传输中被拦截，未授权者也无法解密并读取数据内容。

参考：《信息安全技术 人脸识别数据安全要求（GB/T 41819-2022）》