ICS 35.030
CCS L 70

T

团　　体　　标　　准

T/TMAC ×××—202X

政务云数据中心安全运维技术规范

Technical specifications for security operation and maintenance of government cloud data centers

（征求意见稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

已授权的专利证明材料为专利证书复印件或扉页，已公开但尚未授权的专利申请证明材料为专利公开通知书复印件或扉页，未公开的专利申请的证明材料为专利申请号和申请日期。

××××-××-××发布　　××××-××-××实施

中国技术市场协会　　发布

中国技术市场协会（TMAC）是科技领域内国家一级社团，以宣传和促进科技创新，推动科技成果转移转化，规范交易行为，维护技术市场运行秩序为使命。为满足市场需要，做大做强科技服务业，依据《中华人民共和国标准化法》《团体标准管理规定》，中国技术市场协会有序开展标准化工作。本团体成员和相关领域组织及个人均可提出制修订 TMAC 标准的建议并参与有关工作。TMAC 标准按《中国技术市场协会团体标准管理办法》《中国技术市场协会团体标准工作程序》制定和管理。TMAC 标准草案经向社会公开征求意见，并得到参加审定会议多数专家、成员的同意，方可予以发布。

在本文件实施过程中，如发现需要修改或补充之处，请将意见和有关资料反馈至中国技术市场协会，以便修订时参考。

中国技术市场协会地址：北京市海淀区复兴路甲 23 号城乡华懋大厦 12 层 1217 室

邮政编码：100036　　电话：010-68270447　　传真：010-68270453

网址：www.ctm.org.cn　　电子信箱：136162004@qq.com

目　次

前　言

本文件按照 GB/T 1.1—2020《标准化工作导则 第 1 部分：标准化文件的结构和起草规则》的规定起草。

本文件由天翼云科技有限公司和北京交通大学联合提出。

本文件由中国技术市场协会归口。

本文件起草单位：天翼云科技有限公司、北京交通大学、XXXXX、XXXXX、XXXXX、XXXXX、XXXXX、XXXXX、XXXXX、XXXXX、XXXXX、XXXXX、XXXXX、XXXXX、XXXXX、XXXXX、XXXXX、XXXXX、XXXXX。

本文件主要起草人：孟坤、张亮、孟德寅、华成裕、周华春、冯博昊、XXX、XXX、XXX、XXX、XXX、XXX、XXX、XXX、XXX、XXX、XXX、XXX、XXX、XXX、XXX、XXX、XXX、XXX、XXX、XXX、XXX。

政务云数据中心安全运维技术规范

1 范围

本文件确立了政务云数据中心数据的安全运维框架，规定了安全运维技术种类及技术要求。

本文件适用于政务云数据中心安全运维

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 20984—2022 信息安全技术 信息安全风险评估方法
GB/T 20986—2023 信息安全技术 网络安全事件分类分级指南
GB/T 25069—2022 信息安全技术 术语
GB/T 34982—2017 云计算数据中心基本要求
GB/T 36626—2018 信息安全技术 信息系统安全运维管理指南
YD/T 4570—2023 政务云安全能力要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

政务云 government cloud

用于承载各级政务部门开展公共服务、社会管理的业务信息系统和数据，并满足跨部门业务系统、数据共享和交换等的需要，提供IaaS、PaaS和SaaS的云计算服务。

3.2

云数据中心 cloud computing data center

以云计算服务为主要业务的数据中心。

3.3

云数据中心安全运维 secure operation and maintenance of cloud computing data center

在云数据中心经过授权投入运行之后，确保云数据中心内各信息系统免受各种安全威胁所采取的一系列预先定义的活动。

4 政务云数据中心安全运维参考框架

政务云数据中心安全运维以网络安全防护与事件管理为核心，依托技术支撑体系，构建信息资产风险管理、日常操作及应急响应的标准化闭环流程。通过整合安全产品、工具与服务数据，实现风险精准分析与管控，达成安全目标。关键要素包括专业运维团队、支撑平台/工具及流程机制，服务提供方基于最佳实践定制服务模式与级别，满足政务云安全需求。
实施四大环节精要：

a) 识别：资产盘点、漏洞评估、情报预警、合规检查，风险趋势分析与预警。
b) 防御：漏洞识别、威胁分级、防御部署，安全加固，意识培训与云容灾体系搭建。
c) 监测：流量采集分析、实时告警、深度检测，覆盖网站安全、威胁感知与异常行为监控。

d) 响应：按“准备-诊断-抑制-根除-恢复-跟踪-优化”流程，快速处置事件，包括威胁报告、阻断取证、业务恢复、溯源分析及执法协同，配套应急预案与演练。

安全运维核心在于“风险可识、防御可筑、监测可准、响应可速”，通过风险识别、防御建设、监测分析和响应处置四个环节的协同运作保障政务云安全稳定运行，支撑政务业务连续性与数据安全，实现高效、可靠、合规的运维目标。

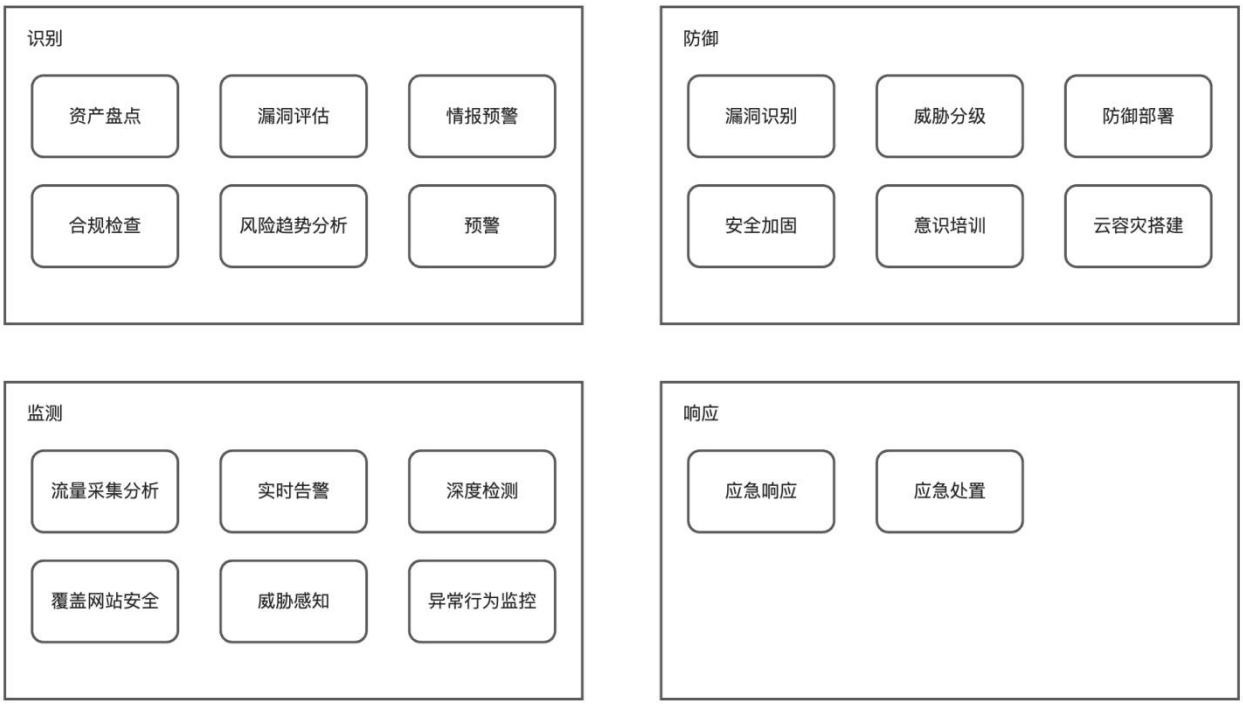

图 1 参考框架

5 云数据中心安全运维模式

云数据中心安全运维模式主要包括以下三类：

a) 自主网络安全运维模式：对安全性和数据保护的要求较高，具备足够的安全资源投入，能够持续有效网络安全运维的组织、机构和设施，选择自主建设安全运维中心。此类组织、机构和设施具备完善的安全运维人员配置、管理机制和人才培养机制，自主建立安全运维中心（SOC），整合安全防护技术、安全运维工具与平台和人员等要素，建立网络安全监测、分析、处置、应急等网络安全运维流程；

b) 联合网络安全运维模式：网络安全运维需求方联合网络安全运维提供方共同建立安全运维中心，并为网络安全运维需求方提供驻场托管式网络安全运维；

c) 托管网络安全运维模式：MSS主要依靠网络安全运维提供方建立的安全运维中心（SOC），通过云平台或远程管理系统，管理组织IT 资产的安全信息、管理安全工具、监测和改善组织的安全状况，识别、检测、分析和响应组织所面临的网络安全事件。以满足对安全人员、技术和流程外包的需要。

6 云数据中心安全运维实施

6.1 识别

6.1.1 资产识别

资产是对组织具有价值的信息或资源，是安全策略保护的对象。组织应对资产进行全生命周期管理，建立健全资产管理制度，对资产全流程进行跟踪和管理。资产识别内容包括：

a) 建立健全完善的资产管理制度，对资产上线、变更、下线等流程进行跟踪和管理，明确资产管理责任人及资产供应链；

b) 建立健全准确的资产台账，定期通过技术手段识别未知或新增的资产，动态更新并完善资产基本属性、安全属性、管理属性和指纹信息，识别资产间的关联性，绘制资产关联图谱。根据GB/T 20984 的方法进行分类分级和资产赋值，并在资产投入使用前完成资产纳管（即将资产

纳入统一的管理流程和系统中）。采用主动或被动资产探测技术识别资产，并动态更新；

c) 基于资产类别、资产重要性和支撑业务的重要性，确定资产防护的优先级；梳理和验证安全防护设施对资产的防护状态，同步更新资产安全防护属性信息；

d) 定期通过技术手段感知资产属性变更，根据预设规则识别变更风险，开展安全告警、通报、处置；对变更的敏感项进行记录和审核，以便事后审计和追溯；

e) 根据域名、IP、端口、中间件、应用、技术架构、变更状态、业务类型（自定义）等条件对资产进行查询、统计，以及对资产进行周期变化监控。基于最小化原则，尽可能收敛互联网暴露面。资产转移或处置时，及时完成资产清单的更新，资产管理责任人需识别可能出现的风险并予以控制，并保留相关记录。

6.1.2 威胁识别

威胁是一种对云数据中心及其资产构成潜在破坏的可能性因素或者事件。组织应识别主要涉及对系统或网络造成威胁的各种因素，并进行评估。这通常包括威胁的来源、途径和意图等，以及威胁利用脆弱性的可能性。

威胁识别内容包括：

a) 威胁识别内容：包括威胁来源、主体、动机、时机和频率等；

b) 威胁来源：对威胁分类前，识别威胁来源，包括环境、意外和人为三类。根据威胁来源的不同，将威胁划分为信息损害和未授权行为等威胁种类；

c) 威胁主体：根据人为和环境区分，人为分为国家、组织团体和个人，环境分为一般的自然灾害、较为严重的自然灾害和严重的自然灾害；

d) 威胁动机：可以分为恶意和非恶意；

e) 威胁频率：应基于经验、统计数据、安全事件报告、检测工具日志及行业威胁情报进行综合评估。

6.1.3 脆弱性识别

脆弱性是组织、系统和信息资产本身存在的，如果没有被相应的威胁利用，脆弱性本身不会对组织和信息资产造成损害。组织应针对云数据中心每一项需保护的信息资产，识别可能被威胁利用的脆弱点。应基于安全脆弱性问题可能造成的风险级别（如高、中、低），科学评定修复优先级，确保高风险脆弱点优先处置。脆弱性识别内容包括：

a) 脆弱性识别：采取问卷调查、工具检测、 人工核查、文档查阅、渗透测试等手段探测和识别资产在物理环境、网络结构、系统软件、应用中间件、应用系统、技术管理、组织管理等方面存在技术脆弱性或管理脆弱性问题；根据资产价值、类型、暴露面等维度针对资产采取不同的脆弱性探测策略；

b) 脆弱性评估：对检测发现的安全脆弱性问题进行研判和甄别，并基于资产价值、资产暴露面类型、脆弱性严重程度、脆弱性问题利用难度等维度评估可能造成安全威胁的风险级别，评定脆弱性问题修复先后次序和脆弱性利用防范方式；

c) 脆弱性管理：借助信息系统将所有安全脆弱性问题列入统一工单管理，开展通报、接收、修复、复测等工作，定期跟踪、督促修复工作进展，复测通过后关闭工单；定期或不定期组织开展安全脆弱性问题分析总结工作，调整安全策略、优化运营流程、健全并完善安全管理制度。

6.2 防护

6.2.1 安全设备运维

组织应对云数据中心内的各种安全设备进行全面、细致、有效的日常维护和管理，以确保其正常运行并能够及时应对各种安全威胁。安全设备运维内容包括：

a) 可用性监控：实时监控安全设备的运行状态和性能指标，及时发现和处理设备故障或异常情况，确保设备的可用性和可靠性；

b) 设备更新和升级：根据组织机构的安全需求和设备厂商的建议，及时更新和升级安全设备，以提高设备的防护能力和安全性；

c) 安全策略管理：根据业务及安全需求，调整和修改安全设备策略，并对策略进行归并及优化；

d) 安全配置管理：定期梳理检查安全设备的配置，如访问控制配置等。对配置文件定期进行备份，并将备份文件存储在安全可靠的位置。同时，应测试配置恢复功能，确保在需要时能够快速

恢复设备配置；

e) 设备的审计和记录：对安全设备的操作进行审计和记录，包括设备的配置操作、检测和监控操作、故障处理操作等，确保设备的操作合规性和可追溯性；

f) 设备安全性管理：建立设备安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期、维修过程等方面作出规定；根据运行参数研判、预测设备故障运行隐患、安全设备的告警进行及时分析和研判；定期开展安全设备漏洞排查，经过充分测试评估后，对已有漏洞及时修补。

6.2.2 安全加固服务

组织应针对云数据中心网络设备、安全设备、操作系统、硬件设备及应用程序实施安全加固，并基于专业安全评估结果，制定差异化加固方案。例如打补丁、修改安全配置、增加安全机制等方法，合理进行安全性加强，从而保障信息系统的安全。安全加固内容包括：

a) 安全现状调查：了解资产安全现状和资产关联关系，评估安全缺陷或安全隐患的影响范围和严重程度；

b) 制定加固方案：针对发现的安全现状问题，与相关业务部门、建设部门、管理部门、运维部门等联合确认安全加固方案，包括实施时间、范围、流程、方法等，确认每项加固措施和操作方法的可行性，同步制定回退方案和应急方案；

c) 落实加固举措：安全加固前做数据备份、版本备份，分阶段、分批次有序开展安全加固举措、测试验证。针对重要资产，应先加固资产，测试无误后再小批量、分批次开展安全加固；

d) 验证加固结果：通过测试、攻击等手段，针对安全加固后的结论进行验证，根据验证结果判断是否符合加固要求，最终按需落实加固方案。

6.2.3 数据安全防护

组织应针对云数据中心存储、分析、处理的数据实施数据加密、访问控制、备份恢复、安全审计及监控等防护措施；并按照数据敏感级别（高/中/低）实施差异化防护策略；定期开展防护有效性评估和安全审计，确保措施持续有效；建立数据安全事件应急响应机制，实现快速处置与溯源。数据安全防护内容包括。

a) 数据采集过程安全防护。在数据采集过程中，API 接口需具有身份验证能力和数据来源校验能力，避免数据非法接入，同时需对数据输入输出进行验证和清洗。

b) 数据传输过程安全防护。在数据传输过程中需具有数据加密和访问控制能力。通过使用加密算法对敏感数据进行加密，并通过身份验证和访问权限管理来控制对数据的访问。加密技术可以保护数据在传输过程中的安全性，访问控制可以确保只有授权人员访问敏感数据。

c) 数据存储过程安全防护。在数据存储过程中需要具有敏感信息加密存储的能力，如个人身份信息、密钥信息等，应使用密码技术进行保护。对于加密密钥的存储和管理可使用硬件加密模块进行加密。同时，对数据库存储平台权限需采用最小权限原则进行配置，确保对数据的访问和操作权限具备合理范围的限制。

d) 数据处理过程安全防护。在数据处理过程中需具有敏感数据脱敏处理的能力，同时，需对数据的操作管理进行记录和监控，以防止数据的非法操作和篡改。此外，数据处理系统需根据存储数据的敏感程度进行不同等级的保护。

e) 数据交换过程安全防护。在数据交换过程中需具有交换数据加密传输和校验的能力，确保数据的安全性和完整性。同时，需对交换的数据进行安全检查和过滤，以防止有害数据的传入和传出。此外，应建立完善的数据交换协议和规范，确保数据交换的可靠性和合规性。

f) 数据销毁过程安全防护。在数据销毁过程中需建立完善的数据销毁规范和流程，并对销毁的存

储介质进行抽样认定，确保数据被彻底删除并无法恢复。

g） 数据安全防护措施有效性验证。定期对数据防泄漏保护机制及有效性进行安全性评估和验证。

6.2.4 云容灾能力

云容灾是针对云数据中心数据和应用进行的容灾防护措施。组织应通过识别容灾体系、建设云容灾系统、开展故障演练和故障切换等措施，确保故障场景下用户业务的连续性。满足用户对容灾能力的建设要求，提高系统的容错能力和抗灾能力，减少停机时间和数据丢失，满足用户对 RTO 和 RPO 的要求。

a） 识别容灾体系：针对应用做分析，识别应用架构类型和重要级别。对不同应用做不同容灾架构选型。常用容灾架构选型有同城多活、同城主备、异地多活、异地主备、两地三中心等。

b） 云容灾系统建设：

1） 应能够根据实际需求、所在地域、计划防范的灾难种类和预算投入的资金量等实际情况，确定容灾系统预期达到的级别；

2） 应能够界定容灾建设的目标，能够设定各项容灾指标，例如：RTO、RPO 等；

3） 应能够满足高可用设计，例如确保云主机用户的业务连续性，应用不间断的对外提供服务，灾难发生后可快速完成业务切换；

4） 应能够满足云容灾数据安全，支持多种加密技术保证数据传输过程安全；

5） 应包括数据备份与同步的相关设计；

6） 应包括云容灾运维管理设计。

c） 故障演练：故障往往具备随机性和不确定性，所以要定期对系统做故障演练，识别应用系统是否存在缺陷；现有故障应对机制是否成熟。具体内容如下：

1） 制定年度故障演练计划，涵盖网络故障、服务器硬件故障、软件漏洞等常见场景，演练频率不少于 1 次/年；

2） 演练前详细规划，明确演练目标、流程、参与人员职责，提前通知相关业务部门；

3） 演练过程中如实记录故障现象、处理步骤、耗时等信息，结束后形成详细报告；

4） 依据演练报告总结经验，优化应急预案与运维流程，针对暴露问题及时整改。

d） 故障切换：当故障真实发生时，按照预先设定好的切换步骤执行，切换后需做好应用健康检查，判断故障切换是否成功。具体内容如下：

1） 切换策略制定：根据数据中心不同系统、业务的优先级与恢复时间目标（RTO），制定精细的故障切换策略，明确主备系统切换条件、切换顺序、回切机制等；

2） 切换技术实现：实现故障切换流程自动化，减少人工干预，降低切换错误风险。在演练中反复验证切换技术的可靠性与稳定性；

3） 切换后验证：故障切换完成后，对系统进行全面验证，确保业务正常运行，数据无丢失、无损坏，及时发现并解决潜在问题。

6.3 监测

6.3.1 网络流量监测

组织应对进出网络的流量进行采集和分析，识别出存在的安全威胁。网络流量监测服务内容包括：

a) 流量采集：通过部署网络监测设备，监测网络边界、网络出入口等关键节点的流量信息，发现网络攻击和存在的安全风险；

b) 流量分析：通过规则库和威胁情报等技术手段对采集的流量数据进行分析；

c) 流量监测：基于多种技术进行网络威胁监测，包括特征匹配、网络行为分析、机器学习、关联分析、威胁情报等；

d) 流量存储：明确采集的流量范围和类别，对监测流量采取保护措施，防止其受到未授权的访问、修改和删除，原始流量应按照法规留存时间要求进行存放和归档。

6.3.2 异常行为监测

组织应通过使用多种机器学习算法挖掘各种用户异常行为模式，检测和识别前期没有发现的安全风险，基于实际安全场景的多维度异常检测功能，提升威胁发现速度和准确率。异常行为监测服务内容包括：

a) 已知威胁监测：依靠已知特征、已知行为模式形成的攻击特征库，结合云端情报，通过预定义规则、情报匹配等方式进行威胁分析和安全处置。对全网设备日志、流数据、数据库表数据等进行采集，并对其进行数据归一化处理，针对常用协议解析的数据形成标准化日志，在标准化日志的基础之上，通过已知威胁检测，生成一次安全事件，并在一次安全事件的基础上生成威胁分析报告。

b) 未知威胁监测：通过结合静态检测、动态检测和沙箱检测等方式，识别未知恶意代码和未知高级攻击行为，及时检测、分析并阻断物理网络中存在的安全威胁。

6.3.3 终端监测

组织应通过对终端行为进行持续监测，实时收集并提取终端的威胁信息和行为数据，结合多种异常行为分析建模工具，发现存在风险的设备并进行及时响应，防范来自终端的安全威胁。终端监测服务内容包括：

a) 终端数据采集：通过技术手段采集终端数据，主要包含服务、进程、端口、注册表、计划任务等；

b) 终端威胁监测：通过终端威胁检测技术对终端进行监测，包含恶意代码检测、暴力破解检测、流量攻击检测、异常行为检测等；

c) 终端监测技术：基于多种技术进行终端威胁检测，包括 IOA 行为检测、IOC 特征匹配、机器学习、关联分析、威胁图谱等。

6.3.4 数据监测

组织应通过数据库审计、数据防泄漏等技术手段对数据采集、存储、传输、使用等过程进行监控，及时发现并阻断对数据进行的窃取、篡改和销毁等恶意行为。数据监测服务内容包括：

a) 数据库监测：通过对数据库运行状态和操作行为进行监测，及时发现数据库的异常状态和异常操作行为等并定位问题；

b) 管理策略监测：对数据管理策略落实情况进行监测，确保数据的保密性、完整性符合管理要求，

保障数据传输、存储和使用的安全；

c) 敏感数据监测：对敏感数据流转情况进行监测，及时发现和处置数据泄露威胁；

d) 监测信息保存：对监测信息采取保护措施，防止其受到未授权的访问、修改和删除，监测信息的保存应按照法规留存时间要求进行存放和归档。

6.4 响应

6.4.1 应急响应

应急响应服务主要是对于安全事件的事前、事中、事后的预防、分析、取证及提供解决方案等工作。应急响应服务内容包括：

a) 事前准备：包括制定应急预案，定期演练等。应急预案应基于组织的需求和特定情况，包括对可能发生的紧急情况进行风险评估和针对性的预防措施。定期演练是为了确保员工和相关部门了解应急程序，并能熟练应对各种紧急情况。

b) 事件识别和报告：建立有效的事件识别机制，以及与员工和相关利益相关者进行有效沟通的渠道，对紧急事件及时发现和报告。

c) 应急响应启动：在实施应急响应工作前，现场应急处置人员应第一时间与相关技术人员取得联系，了解事件发生情况。技术人员根据事件类型判断是否需要启用应急响应服务。现场威胁分析发现入侵事件，由现场应急人员初步判断事件类型，确定事件发生情况，根据 GB/T 20986-2023 与相关人员确定是否启动应急响应服务。

d) 事件分析和系统恢复：在网络安全事件发生后，需要进行事件分析，确定存在的安全漏洞并采取必要的措施来修复漏洞，以防止类似事件的再次发生。在分析完成后，需要将被破坏的系统进行恢复，确保系统的完整性和可用性。

e) 溯源取证：遵循严格的法律程序和技术规范，以确保取证数据的真实性和完整性，为后续的应急响应和安全分析提供有力的支持。

6.4.2 应急处置

应急处置是指安全技术人员在遇到突发事件后所采取的紧急措施和行动，恢复业务到正常服务状态；调查安全事件发生的原因，在需要司法机关介入时，提供法律认可的数字证据，避免同类安全事件再次发生。应急处置服务内容包括：

a) 应急响应处置：在判断事件类型可能为安全事件，启用应急响应后，根据 GB/T 20986-2023 标准，技术人员通过现场或非现场等方式进行信息收集工作，详细了解掌握事件发生的始末、现状、可能的影响，对事件进行详细分析，提供事件处置建议，并协助相关人员解决事件。

b) 复盘总结：待事件处理结束后，应急人员整理事件分析、事件处理的过程记录和相关资料，撰写应急响应服务记录报告并提交。对于大型、复杂的应急响应过程还需进行整体的事件处理汇报工作，同时，依据现场情况，召集必要相关人员发起会议，对本次应急响应事件的发生进行复盘，提升优化应急效率，并根据复盘结果，完善运营方案，在安全管理制度、流程上做同步完善。

c） 事件归档：应急响应结束，输出应急响应报告及相关取证材料，同步交付作为事件归档。

参 考 文 献

[1]GB/T 20984—2022 信息安全技术 信息安全风险评估方法

[2]GB/T 20986—2023 信息安全技术 网络安全事件分类分级指南

[3]GB/T 25069—2022 信息安全技术 术语

[4]GB/T 34982—2017 云计算数据中心基本要求

[5]GB/T 36626—2018 信息安全技术 信息系统安全运维管理指南

[6]YD/T 4485—2023 云数据中心服务器技术要求

[7]YD/T 4570—2023 政务云安全能力要求

[8]YD/T 2584—2013 互联网数据中心安全防护要求