ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 32914—XXXX
代替GB/T 32914-2016

信息安全技术 网络安全服务能力要求

Information security technology—Capability requirements of cybersecurity service

（征求意见稿）

（本草案完成时间：2022 年 11 月 04 日）

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。

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

国家市场监督管理总局
国家标准化管理委员会　发布

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。

本文件代替GB/T 32914—2016 《信息安全技术 信息安全服务提供方管理要求》，与GB/T 32914—2016相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 将术语“信息安全服务”更改为“网络安全服务”，并更改了定义（见3.1，2016年版的3.1）；

b) 增加了总则（见第4章）；

c) 将原第5章、第6章内容调整为“第5章 通用要求”（见第5章，2016年版的第5章、第6章）；

d) 增加了“供应链管理”要求（见5.4）；

e) 增加了“远程服务”要求（见5.7）；

f) 增加了“法律保护”要求（见5.8）；

g) 增加了“数据保护”要求（见5.9）；

h) 增加了“服务可持续性”要求（见5.10）；

i) 增加了“不同种类网络安全服务专项要求”内容（见第6章）；

j) 增加了“增强要求”内容（见第7章）；

k) 增加了“常见网络安全服务使用的工具类型”内容（见附录A）。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国信息安全标准化技术委员会（SAC/TC260）提出并归口。

本文件起草单位：中国电子技术标准化研究院、中国网络安全审查技术与认证中心、中国信息安全测评中心、国家信息技术安全研究中心、中国电子科技集团公司第十五研究所（信息产业信息安全测评中心）、杭州安恒信息技术股份有限公司、北京安信天行科技有限公司、北京神州绿盟科技有限公司、广州竞远安全技术股份有限公司、中国移动通信集团有限公司、北京信息安全测评中心。

本文件主要起草人：杨建军、何延哲、李有元、程瑜琦、陆丽、史大为、刘健、陈青民、朱雪峰、李彦峰、陈星、金达、何刚、王琰、程璐样、韦国文、邱勤、李媛、白旭东、李伟旗。

本文件及其所代替文件的历次版本发布情况为：

——2016年首次发布为GB/T 32914-2016；

——本次为第一次修订。

信息安全技术　网络安全服务能力要求

1　范围

本文件对网络安全服务机构提供网络安全服务应具备的能力提出具体要求。

本文件适用于指导网络安全服务机构开展网络安全服务能力建设，以及评价网络安全服务机构的能力水平，也可为政务部门、关键信息基础设施运营者选用网络安全服务机构时提供参考。

注：本文件所述网络安全服务不含涉及国家秘密的网络安全服务。

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 22080—2016　信息技术　安全技术　信息安全管理体系　要求

GB/T 25069—2022　信息安全技术　术语

GB/T 36626—2018　信息安全技术　信息系统安全运维管理指南

GB/T 36957—2018　信息安全技术　灾难恢复服务要求

GB/T 36959—2018　信息安全技术　网络安全等级保护测评机构能力要求和评估规范

GB/T AAAA—XXXX　信息安全技术　网络安全服务成本度量指南

GB/T BBBB—XXXX　信息安全技术　网络安全从业人员能力基本要求

3　术语和定义

GB/T 25069—2022界定的以及下列术语和定义适用于本文件。

3.1

网络安全服务 cybersecurity service

根据服务协议，基于服务人员、工具、管理体系等技术资源，向网络安全服务需求方（3.3）提供服务的过程。

注1：常见的网络安全服务包括检测评估、安全运维、安全咨询、灾难恢复等。

注2：网络安全服务通常以供需双方的服务项目形式进行。

3.2

网络安全服务机构 cybersecurity service provider

通过专业的网络安全人员提供网络安全服务（3.1）的组织。

注：包括企事业单位、非法人组织等，简称服务机构。

3.3

网络安全服务需求方 cybersecurity service acquirer

获取外部所提供的网络安全服务（3.1），以满足网络安全需求，实现自身业务目标的组织或个人。

注：简称服务需求方。

3.4

服务协议 service contract

服务开始前供需双方共同签署的约定，并在服务过程中共同遵守。

注：服务协议形式上可以是服务合同及其附属的工作说明书。

3.5

服务级别 service level

在服务协议中对服务交付成果明确约定、可测量和文档化的一系列服务指标。

3.6

服务要素 service factors

规划和实施服务所需的服务人员、服务流程、服务环境、服务方法、服务工具、服务保障等关键要素，以及其他服务所需的资源。

3.7

服务方案 service plans

基于服务目标，对服务各阶段中所需执行的过程、任务、活动以及相关服务要素、服务级别进行详细描述的文档。

3.8

服务变更 service change

任何可能对服务产生影响的新增、修改或解除的活动。

注：服务变更可能涉及服务范围、服务目标、服务依据、服务内容、服务级别、服务价格、服务要素（3.6）等。

4 总则

网络安全服务机构开展网络安全服务，应满足第5章通用要求，以及第6章中与其服务类型相对应的专项要求。面向对网络安全服务有更高要求的服务需求方，如政务部门、关键信息基础设施运营者等，网络安全服务机构开展网络安全服务时，还应满足第7章的增强要求。

5 通用要求

5.1 基本条件

网络安全服务机构应具备以下条件：

a) 在中华人民共和国境内注册；

b) 法定代表人、董事、合伙人以及高层管理人员无犯罪记录；

注1：以公司为例，高层管理人员通常是指经理、副经理、财务总监、技术总监、安全总监等。

c) 未被列入失信被执行人、重大税收违法案件当事人名单和政府采购严重违法失信行为记录名单等严重失信名单，以及其他可能影响网络安全服务的负面清单；

d) 独立经营核算，具有依法缴纳税收和社会保障资金的良好记录。

5.2 组织管理

5.2.1 信息安全管理

网络安全服务机构的信息安全管理应满足GB/T 22080-2016中第4章至第10章、附录A的要求。

5.2.2 服务人员管理

网络安全服务机构对服务人员的管理应满足以下要求：

a) 设置与网络安全服务规模相适应的专业技术部门或团队，建立并维护服务人员清单；

b) 网络安全服务项目负责人具备2年以上相应网络安全服务项目经验；

c) 建立服务人员档案，包括服务人员的资格证明、培训/考核记录、技术方向和能力水平、从业经历、实际参与项目及分工等信息，档案至少保存至服务人员离职后5年，有关法律法规、行业管理另有规定的除外；

d) 根据服务人员工作岗位，按照GB/T BBBB—XXXX中第5章及第6章的知识和技能要求，制定岗前培训计划，开展岗前培训，并经考核评定合格后上岗；

注 1：例如，服务人员取得网络安全等级测评师证书后，持证开展网络安全等级测评工作。

注 2：岗位涉及使用安全服务工具的，培训及考核内容中需包含网络安全服务工具实操部分，网络安全服务使用的常见工具类型见附录 A。

e) 与服务人员签订保密协议，并定期进行保密教育。

5.2.3 资源配置

网络安全服务机构应对资金、人员、工具等资源进行调配，根据服务需求方需要以书面承诺等方式向服务需求方说明资源配置、保障情况。

5.3 项目管理

5.3.1 服务价格

网络安全服务机构应按照GB/T AAAA—XXXX对每项网络安全服务成本进行度量后，确定服务价格。

5.3.2 服务方案

网络安全服务机构编制网络安全服务方案应满足以下要求：

a) 在服务项目实施前编制网络安全服务方案，并得到服务需求方的认可；

b) 在服务方案中明确网络安全服务范围、服务目标、服务依据、服务内容及服务级别（或服务成果）；

c) 应明确服务人员（包括项目负责人、项目实施人员的职责等）、服务流程（包括计划或进度等）、服务环境、服务方法、服务工具、服务保障（包括资源保障、质量管理、保密管理、风险控制等）等服务要素。

注 1：涉及项目实施人员及职责的，具体到个人身份，并提供联系方式。

注 2：涉及服务流程中计划或进度的，至少具体到月份。

注 3：服务方法通常包括：人员访谈、资料查看、配置检查、漏洞扫描、渗透测试、源码分析、日志分析、系统监测等。

5.3.3 服务实施

网络安全服务机构在服务过程中应满足以下要求。

a） 根据服务方案组织项目实施，定期通过通知、例会、报告（如周、月报）等多种形式与服务需求方沟通反馈。

b） 建立服务变更管理流程，变更前与服务需求方就具体事项主动沟通，经服务需求方同意后，确保服务变更以受控的方式得到评估、批准和实施；服务变更后对服务目标、服务质量和效率、服务需求方信息系统和业务造成影响的，应进行针对性的改进、补救或恢复。

c） 建立项目沟通与应急处置机制，确定双方的接口人，及时处理服务实施过程中产生的投诉、争议、突发事件等，并形成处置结论或解决方案。

d） 在服务过程中发现网络安全事件，及时向服务需求方报告，并记录事件相关内容；如网络安全服务涉及安全事件处置，协助其根据《国家网络安全事件应急预案》及相关规定处置，并对事件处置情况进行完整记录，在服务需求方本地服务器等存储媒介妥善留存，记录内容包括但不限于：事件原因、事件经过、事件影响、处置结果等。

注 1：网络安全事件包括有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件和其他事件等。

注 2：记录内容的具体格式见 GB/T 36643—2018 中 6.3。

e) 在服务过程中发现产品（含硬件、软件）的网络安全漏洞时，及时向服务需求方报告。涉及通用产品、其上游产品或者组件的，应根据《网络产品安全漏洞管理规定》和相关国家标准要求进行报告和协助处置。

注 3：通用产品是指已公开销售或开放授权，且被广泛应用的产品。

注 4：网络安全漏洞管理过程见 GB/T 30276—2020。

f） 对服务过程中的关键活动和原始数据进行记录，主要包括：

1） 接收数据、资料的记录；

2） 进行补丁更新、系统加固的记录；

3） 与关键人员沟通访谈的记录；

4） 引入的供应商产品（包括标识、版本）、服务人员（名单）；

5） 与漏洞、安全事件有关的原始数据等。

g） 网络安全服务不得转包，服务协议中涉及分包的，原则上分包比例不超过40%；分包部分通过服务协议将网络安全服务的原则、目标、要求和责任有效传递到涉及的供应商，并对其履约情况进行监督。

5.3.4 风险控制

网络安全服务机构在服务过程中应采取以下措施对风险进行控制：

a) 根据服务范围、服务内容，以及服务人员、服务流程、服务环境、服务资源等服务要素，识别服务实施过程中可能产生的风险，制定应对措施并确认其有效性；

b） 使用服务工具，有可能对服务需求方系统或平台的功能、性能，数据的保密性、完整性、可用性等造成影响的，需向服务需求方进行风险提示，在采取风险规避措施并得到服务需求方同意后方可使用；

c） 采取必要的监督、审计措施，确保服务人员对系统或数据的操作不超出服务协议及服务需求方授权的范围。

5.3.5 成果交付

网络安全服务机构交付服务成果应满足以下要求：

a） 按服务协议中所规定的关键节点，提交服务交付成果，如服务方案、服务过程文档和记录、服务报告（包括阶段报告、总结报告、验收报告等），并得到服务需求方的确认；

b） 保证所有服务交付成果的真实性、准确性和完整性，能清晰阐明其中的依据、组成、结论、措施、数据来源及支撑材料等内容；

c） 完成服务交付后，根据与服务需求方的约定，主动将持有的相关数据、资料、账号、部署的工具等进行清理、交还或卸载，并向服务需求方提供由项目负责人签字的承诺或确认函；

注：承诺或确认函中可包含清理、卸载等操作的具体过程证据。

d） 建立、维护服务档案（包括服务交付成果和服务记录），且档案至少保存5年，有关法律法规、行业管理另有规定的除外。

5.4 供应链管理

网络安全服务机构的供应链管理应满足以下要求。

a） 建立统一的采购和供应链管理制度，对供应商的基本资格、供应过程、供应变更等进行审核、监督、管理；

b） 建立供应商筛选机制，不应选择存在以下情况的组织作为网络安全服务的供应商：

1） 被列入失信被执行人、重大税收违法案件当事人名单和政府采购严重违法失信行为记录名单等严重失信名单，以及其他可能影响网络安全服务的负面清单；

2） 未处理的网络安全服务相关行政处罚；

3） 3年内因重大网络安全服务问题被有关部门通报；

注1：重大网络安全服务问题包括但不限于以下情形：供应存在恶意代码的产品或假冒产品；在服务过程中因服务机构原因造成服务需求方系统大面积瘫痪，丧失业务处理能力，重要数据、资料被窃取、泄露；未使用可信或可控的分发、交付和仓储手段导致产品被篡改。

4） 未解决的知识产权方面纠纷；

5） 不满足服务需求方的筛选条件的；如，服务需求方要求限制从特定供应商或国家、地区采购产品或服务。

注2：不满足网络安全服务需求方筛选条件的，仅影响其在特定网络安全服务项目中被使用，不影响其进入网络安全服务机构的合格供应商清单。

c） 对长期使用的产品、服务建立合格供应商清单，同类的产品或服务宜有多个合格供应商。

d） 在服务过程中需要引入供应商人员的，应按照 5.2.2 对相关人员进行筛选、考核、管理。

e） 建立、维护供应过程档案，记录所有供应商 5 年内提供产品的名称、标识、版本、产地、生产商，服务的名称、涉及的人员名单及其简历等信息。

5.5 技术能力

网络安全服务机构应具有与所开展网络安全服务相适应的技术能力，并满足以下要求。

a） 对已开展的网络安全服务形成技术指导书（包括技术规范、操作指引、用例集等），编制技术指导书应重点关注以下内容：

1） 网络安全服务相关法律法规、国家标准、行业标准等中的规范性要求、最佳实践等内容；

2） 国内外权威机构发布的安全态势报告、漏洞公告、突发安全事件报告等中的最新安全威胁分析方法、脆弱性识别方法、安全加固指引等内容；

3） 国内外网络安全技术等的发展动向中关于安全控制、技术解决方案等最新内容。

b） 涉及网络安全事件处理服务的，根据《国家网络安全事件应急预案》及相关国家标准要求，建立网络安全事件应急处置所需的技术能力，如编制相关工作程序、开展相关技能培训、定期进行预案演练等。

c） 建立网络安全服务管理系统，网络安全服务的基本情况和5.3.3d）-f）涉及的数据可录入系统并进行自动化管理，且系统可支持通过接口方式共享相关记录。

d） 开展网络安全服务过程中，涉及使用密码的，应满足国家密码管理有关规定和相关标准要求。

注：密码应用过程见 GM/Y 5001-2020。

5.6 服务工具

网络安全服务机构应具备与所开展网络安全服务相关的服务工具（包括设备、平台、软件、模板、知识库等，常见工具类型见附录 A），并满足以下要求：

a) 应选用未被有关部门通报存在问题的产品作为服务工具，已经使用的工具被通报存在问题的，应立即停止使用直至问题被修复；

注：经证明产品的版本不属于通报问题的版本且问题不存在的除外。

b) 服务工具为《网络关键设备和网络安全专用产品目录》中的，应获得安全认证或者安全检测符合要求；

c) 应确保工具的合法版权且授权在有效期内，运行状态良好，并持续更新、升级；

d) 应明确服务过程中工具的使用方法，对工具使用人员进行培训，避免因不当操作对业务造成影响或损害；

e) 应定期检验工具的安全性，包括对工具进行杀毒、对工具产生的网络流量进行分析等，避免工具存在有害功能，以及隐蔽的链接、协议或端口；

f) 应关注工具及其组件的安全漏洞公告和相关信息，在发现漏洞被披露时，应第一时间评估漏洞的影响，采取更新补丁、下线工具等措施，保证不影响服务涉及的系统或平台。

5.7 远程服务

网络安全服务机构需要远程提供服务的（例如远程操作服务工具、登录服务需求方系统等），应满足以下要求：

a） 服务人员、工具处于可信的物理、网络环境；

b） 对远程登录操作人员进行实名登记，分配仅能自用的实名账号；

c） 对远程登录操作人员进行身份鉴别，为账号设置复杂度高（如长度不少于12位，包含大写字母、小写字母、数字、特殊字符等三种以上的字符类型）的口令并定期更换；

d） 限制远程登录操作的网络地址、终端、时间周期；

e） 远程登录操作时，采用密码技术建立安全的信息传输通道，保证通信过程中数据的保密性、完整性；

f） 留存5年内远程登录操作的日志，定期对日志进行审计，审计过程中发现存在网络安全事件的按照5.3.3d）要求处置。

5.8 法律保障

网络安全服务机构应为网络安全服务建立法律保障机制，并满足以下要求。

a） 应由专业法务人员审核网络安全服务协议。

b） 应在服务协议中明确以下内容：

1） 服务机构与服务需求方双方的责任边界；

2） 网络安全服务的范围、内容、目标、节点、级别、交付成果、验收等条款，并采用服务目录的方式确定服务内容和服务形式；

3） 网络安全服务的保密承诺、数据保护、项目成果知识产权归属等条款；

注：数据保护条款具体见5.9a）。

4） 体现因受管辖国家及需遵循的法律法规、政策变化影响而造成服务中断、停止服务或退出市场等的相关条款及相应责任。

c) 网络安全服务实施过程中，宜按行业管理或服务需求方的要求，通过安全监理、安全审计等方式来监督和确认服务协议的执行情况。

5.9 数据保护

网络安全服务机构应对服务过程中获取的数据（包括原始数据、加工分析产生的数据等）进行安全保护，并满足以下要求：

a） 在服务实施前，应与服务需求方明确约定数据保护的相关条款，包括服务过程中涉及的个人信息（如身份信息等）、业务数据、系统数据、安全数据、文本资料等的保护要求，以及数据的使用目的和周期、最小处理范围、最小特权访问、事后处置等保护措施；

注 1：约定数据保护的条款的方式包括在服务协议中专门体现或签署单独的数据保护协议。

注 2：现场提供网络安全服务的，明确项目相关资料是否能被外带的要求。

注 3：涉及纸质资料的，明确是否可被电子化。

b） 处理网络安全服务过程中获取的各类数据，应遵守法律、法规要求，履行数据安全保护义务，承担社会责任，不应危害国家安全、公共利益，不得损害个人、组织的合法权益；

c） 不应将网络安全服务过程中获取的数据变更目的使用，不应向第三方提供或进行公开，服务协议中明确授权或经服务需求方同意的除外；

d） 应采取必要的安全措施，如加密、完整性校验、备份等，保证所获取数据的真实性、准确性，未经服务需求方同意，不应更改、删除、销毁原始数据；

e） 因服务所需向境外提供、传输网络安全服务过程中获取的各类数据，应在事前向服务需求方单独告知出境目的、数据种类、数量、周期、接收方等情况，取得服务需求方书面同意。同时，还应遵守数据出境管理相关法律法规的要求；

f） 因处理外国司法或执法机构的要求提供数据时，应遵守国家有关法律法规要求，上报有关主管机关批准后方可提供；

g） 在服务实施完成之后，应按服务需求方和服务协议的要求，进行数据的脱敏、移交、清理、销毁等处置；服务需求方对处理情况提出核验或审计的，应予以充分配合。

5.10 服务可持续性

网络安全服务机构应采取措施保障服务的可持续性，并满足以下要求：

a） 应针对自身服务中断、服务机构更换等制定应急处置方案采取必要措施防止造成服务需求方业务中断、安全防护水平下降或其他影响；

b） 服务期限到期前，如需继续向服务需求方提供服务的，应提前与服务需求方沟通协商，避免因服务中断、资源保障不到位等对服务需求方产生影响；

c） 涉及服务机构更换的，应根据服务需求方要求向指定的其他网络安全服务机构移交相关的资料、账号、证件、令牌等，直至网络安全服务工作平稳过渡后才可退出服务；

d） 若确有无法提供持续服务的情况，应提前3个月向服务需求方说明相关情况，并提出服务需求方认可的替代、交接方案。

6 不同种类网络安全服务的专项要求

6.1 检测评估服务

检测评估服务应满足以下要求：

a） 服务机构应具备基本的检测评估相关服务工具研发能力或二次开发能力；

注：例如，利用脚本语言编写测试代码等可认为是基本研发能力的体现。

b） 服务内容涉及网络安全等级保护测评的，服务机构应能满足GB/T 36959—2018中第4章的相关能力要求；

c） 服务内容涉及风险评估的，服务机构应能按照GB/T 20984—2022对风险进行识别、定性或定量分析、评价；
d） 开展漏洞扫描、渗透测试等可能对服务需求方系统、平台、数据等造成影响的，就可能产生的风险、应对措施向服务需求方单独告知，经其同意后采取影响最小的方式实施；
e） 服务需求方要求使用测试环境进行检测评估时，分析测试环境与真实环境（如生产环境）的区别，向服务需求方说明检测评估结果的适用范围；
f） 针对检测评估所发现的安全问题、风险等提出安全整改建议，并在服务需求方完成整改后验证整改效果，服务需求方无相关需求的除外；
g） 留存5年内对服务交付成果内部评审、批准，以及服务需求方签收或确认的记录。

6.2 安全运维服务

安全运维服务应满足以下要求：
a） 需要安全运维服务人员长期驻场（半年以上）服务的，服务机构应向服务需求方提供其背景审查、人事关系等材料供服务需求方审核，服务需求方确认后服务人员才可进场工作；
b） 通过绩效管理等措施维持安全运维服务团队的稳定性，驻场服务人员每年或单个项目服务期间更换比例原则上不超过20%；
注 1：如更换比例超过 20%，向服务需求方说明更换服务人员的原因，以及采取何种保障措施确保服务质量不会下降。
c） 按照GB/T 36626-2018中第7章界定服务人员及其工作职责，并按照GB/T 36626-2018中第8章的规程开展安全运维服务；
d） 应对运维工作记录进行汇总，定期向服务需求方提供安全运维工作简报，简报的形式和提交时间应在服务协议或方案中明确，包括日报、周报、月报、季报、年报等形式；
e） 通过可量化的方法衡量安全运维的服务水平和用户满意度；
注 2：例如，通过安全运维服务平台的反馈信息进行统计以体现运维事件响应、事件关闭的效率来量化服务水平。
f） 服务交付成果中应包含服务周期内的安全运维总结报告，总结报告内容包括安全运维工作的基本情况、处置的安全事件、采取的改进措施、服务水平评价数据等。

6.3 安全咨询服务

安全咨询服务应满足以下要求：
a） 明确安全咨询过程中服务需求方需要提供的具体资料和数据，并说明理由；
b） 将安全咨询过程中使用的资料、数据形成清单，并将被访谈人员、访谈经过，资料、数据的提供人、提供时间等进行记录，保证资料、数据获取、使用情况可追溯。

6.4 灾难恢复服务

网络安全服务机构应按照 GB/T 36957—2018 相关要求开展灾难恢复服务。

7 增强要求

网络安全服务机构应满足以下增强要求。
a） 根据服务协议中的服务内容建立相对独立的服务团队，配备专用的工具、服务管理平台，指定一名高层管理人员作为网络安全服务负责人。
b） 确保实施网络安全服务的人员是持有相关技术资格证明的正式员工，并对其进行过背景审查（如无犯罪证明记录等），调查结果应长期留存并可供服务需求方查看，根据有关部门要求服务人员已备案的除外。

c） 在服务过程中需要引入供应商产品或服务的，应优先选择合格供应商清单中供应渠道可靠，受政治、贸易、外交等因素导致供应中断可能性小的产品或服务。

d） 确保市场采购的服务工具取得安全认证，或按照相关标准通过安全检测。

注 1：如选用具有自主知识产权、可被重构的工具等。

e） 关键服务工具为非市场采购的服务工具（包括但不限于定制开发工具、自研工具、可免费下载使用或试用的工具）的，应通过第三方机构的安全检测。

注 2：关键服务工具通常是指 24h 内不使用就会对服务需求方的系统、数据的保密性、完整性、可用性等产生影响。

f） 建立关键服务工具清单，并为关键服务工具进行备份，包括但不限于：

1） 服务工具的储备充足，可随时启用备份的工具；

2） 同类用途的主备服务工具来自不同供应商；

注3：定制开发工具、自研工具和市场采购的服务工具可认为来自不同的供应商。

3） 定制开发工具、自研工具的核心研发人员存在主备方案。

g） 在获知安全事件信息或威胁信息后，对供应链中相关产品、组件、服务进行风险分析，提出更新、中止、替换等针对性的应急措施，并更新合格供应商清单。

h） 提供服务过程中，对使用的服务工具产生的网络流量进行监测或审计，保证所有网络流量均为提供服务所必需的流量；涉及出境流量的，应按照5.9e）的要求处置。

i） 具备对网络攻击行为进行主动发现、分析、提出防护建议，并按照5.3.3d）的要求进行记录和留存的能力。

注 4：发现方式主要包括日志分析、异常文件分析、异常进程分析、异常流量分析、威胁源分析等。

j） 具备对不同厂商安全设备产生的日志进行整合分析，以及对5.3.3f）中记录的、服务需求方所掌握的、以及从其他渠道获知的网络安全事件信息进行汇总、研判的能力。

k） 与国家、行业等建立的网络安全信息共享机制进行联动，将共享机制中相关机构提供的、或从国家备案的漏洞库等渠道获取的漏洞信息、威胁信息等向服务需求方进行共享。

l） 在服务协议中明确服务机构持续服务的义务。例如，在服务期内不得单方面停止对服务需求方的服务。

m） 对服务过程中获取的数据，应与其他数据分离存储，并按照重要数据相关法律法规和标准的要求予以保护。

n） 除仅用于服务所需目的外，不应对服务过程中获取的数据进行二次加工、分析。

附 录 A
（资料性）
网络安全服务使用的常见工具类型

A.1 检测评估服务可配备的工具类型

漏洞挖掘工具：针对系统或单个产品进行安全性检测分析，通过自动化构造的测试用例，检测分析系统的源码、目的代码、运行内存和通讯状态等，发现系统或产品的未知安全漏洞，并能给出初步分析，从而帮助提高系统或产品的安全性的工具。

配置核查工具：基于安全配置要求实现对资产（如服务器、网络设备、安全产品、操作系统、数据库、应用系统等）的安全配置检测和合规性分析，生成安全配置建议和合规性报告，目的是发现并指导消除资产中因安全配置不当导致的安全隐患的工具。

软件成分分析工具：通过分析软件包含的一些信息和特征来实现对该软件的识别、管理、追踪的工具，具备使用基于人工智能（AI）的分析引擎发现所有的三方组件漏洞，精确、详细地反馈漏洞信息，以及问题组件的引用位置的能力。

交互式应用安全检测系统：交互式应用程序安全测试，通过代理、虚拟专用网络（VPN）或者在服务端部署 Agent 程序，收集、监控 Web 应用程序运行时函数执行、数据传输，并与扫描器端进行实时交互，高效、准确的识别安全缺陷及漏洞，同时可准确确定漏洞所在的代码文件、行数、函数及参数。

流量分析工具：针对网络或者被测试系统的交互流量能够拦截、重放、修改的分析工具。

风险评估与管理工具：此类工具实现了对风险评估全过程的实施和管理，包括:被评估信息系统基本信息获取、资产信息获取、脆弱性识别与管理、威胁识别、风险计算、评估过程与评估结果管理等功能。评估的方式可以通过问卷的方式，也可以通过结构化的推理过程，建立模型、输入相关信息，得出评估结论。通常这类工具在对风险进行评估后都会有针对性地提出风险控制措施。

安全审计工具：用于记录网络行为，分析系统或网络安全现状;它的审计记录可以作为风险评估中的安全现状数据，并可用于判断被评估对象威胁信息的来源。

拓扑发现工具：通过接入点接入被评估网络，完成被评估网络中的资产发现功能，并提供网络资产的相关信息，包括操作系统版本、型号等。拓扑发现工具主要是自动完成网络硬件设备的识别、发现功能。

资产信息收集系统：通过提供调查表形式，完成被评估信息系统数据、管理、人员等资产信息的收集功能，了解到组织的主要业务、重要资产、威胁、管理上的缺陷、采用的控制措施和安全策略的执行情况。此类系统主要采取电子调查表形式，需要被评估系统管理人员参与填写，并自动完成资产信息获取。

A.2 安全运维服务可配备的工具类型

安全运维服务包括但不限于安全巡检、安全加固、应急保障，可配备的工具类型有：

漏洞挖掘工具：针对系统或单个产品进行安全性检测分析，通过自动化构造的测试用例，检测分析系统的源码、目的代码、运行内存和通讯状态等，发现系统或产品的未知安全漏洞，并能给出初步分析，从而帮助提高系统或产品的安全性的工具。

配置核查工具：基于安全配置要求实现对资产（如服务器、网络设备、安全产品、操作系统、数据库、应用系统等）的安全配置检测和合规性分析，生成安全配置建议和合规性报告，目的是发现并指导消除资产中因安全配置不当导致的安全隐患的工具。

入侵检测系统：入侵检测系统通过部署检测引擎，收集、处理整个网络中的通信信息，以获取可能对网络或主机造成危害的入侵攻击事件;帮助检测各种攻击试探和误操作;同时也可以作为一个警报器，

提醒管理员发生的安全状况。

应急响应辅助系统：为应急响应提供计算机辅助，目的是实现应急响应的半自动化支持。能对紧急事件或安全事件发生时的影响分析；应急响应的概要设计或详细制定；应急响应的测试与完善。

源代码审计产品：本类产品是针对系统开发过程中的源代码进行安全审计检测，检测缓冲区溢出、代码注入、跨站脚本、输入验证、应用协议接口（API）误用等缺陷，检测编码规范性，目的是对源代码安全问题进行分析和验证。

流量分析工具：针对网络或者被测试系统的交互流量能够拦截、重放、修改的分析工具。

参 考 文 献

[1] GB/T 30271—2013 信息安全技术 信息安全服务能力评估准则

[2] GB/T 30276—2020 信息安全技术 网络安全漏洞管理规范

[3] GB/T 31168—2014 信息安全技术 云计算服务安全能力要求

[4] GB/T 34942—2017 信息安全技术 云计算服务安全能力评估方法

[5] GB/T 36637—2018 信息安全技术 ICT 供应链安全风险管理指南

[6] GB/T 36643—2018 信息安全技术 网络安全威胁信息格式规范

[7] GM/Y 5001—2020 密码标准应用指南

[8]国家网络安全事件应急预案(2017 年 1 月 10 日 中央网络安全和信息化领导小组办公室〔2017〕4 号公布)

[9] 网络产品安全漏洞管理规定(2021 年 7 月 12 日 工业和信息化部 国家互联网信息办公室 公安部〔2021〕66 号公布)

[10] 网络关键设备和网络安全专用产品目录(第一批)(2017 年 6 月 1 日 国家互联网信息办公室 工业和信息化部 公安部 国家认证认可监督管理委员会〔2017〕01 号公布)