ICS 00.000
X XX

CIIPA

团　　体　　标　　准

T/CIIPA 00006—2024

关键信息基础设施安全服务能力要求

Capability requirements for security service of critical information infrastructure

（征求意见稿）

20XX-XX-XX 发布　　20XX-XX-XX 实施

中关村华安关键信息基础设施安全保护联盟　发布

目　　次

前　言

本文件按照《中关村华安关键信息基础设施安全保护联盟标准管理办法（暂行）》的要求，依据 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。

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。

本文件由中关村华安关键信息基础设施安全保护联盟提出。

本文件由中关村华安关键信息基础设施安全保护联盟网络安全标准专业委员会归口和解释。

本文件起草单位：本文件起草单位：国网思极网安科技（北京）有限公司、中关村华安关键信息基础设施安全保护联盟、中国工商银行股份有限公司、中国电力科学研究院有限公司、国家广播电视总局监管中心、国家工业信息安全发展研究中心、教育部教育管理信息中心、北京北信源软件股份有限公司、中国信息安全测评中心、中邮信息科技（北京）有限公司、大唐科技研究总院、中国建设银行股份有限公司、中国电信集团有限公司、深圳万物安全科技有限公司、四川北斗弘鹏科技有限公司、湖南浩基信息技术有限公司、中科信息安全共性技术国家工程研究中心有限公司、甘肃赛飞安全科技有限公司、杭州中尔网络科技有限公司、工信部教育考试中心、水利部信息中心、中国移动通信集团有限公司、中国民生银行股份有限公司、南京众智维信息科技有限公司、银行卡检测中心（北京银联金卡科技有限公司）、成都久信信息技术股份有限公司。

本文件主要起草人：夏颖、乔淑娟、逯瑶、姜帆、杨阳、刘正坤、李永刚、任磊、尹琴、祁剑、于越、宫春江、靳喜军、聂君、石天浩、王文路、许科展、于俊杰、伊玮珑、孙滢、肖红阳、李炎、郑世涛、孙娅苹、李威、林皓、杨华、李洪典、邸丽清、李聃、谢凌云、吕博、钟国辉、郎颂、王文军、邹远辉、李晓芳、胡建勋、刘元、杜建斌、谢占斐、陈傲晗、葛方隽、孙茂增、王天昊、徐子龙。

本文件首次发布。

本文件在执行过程中的意见或建议反馈至中关村华安关键信息基础设施安全保护联盟（地址：北京市海淀区板井路 69 号世纪金源商务中心 607，100097，网址：http://www.ciipa.com，邮箱：guanbaolianmeng@cnciipa.com）。

引　言

关键信息基础设施安全保护自身具有实战引领、服务为先和业务融合的特点，从安全服务入手，以风险治理为根，以安全运营为翼，了解业务方能定制安全，专业安全服务先行是做好关键信息基础设施安全保护工作的核心要义。在当今数字化时代，关键信息基础设施的安全问题日益凸显，其安全服务能力的标准化、专业化已成为行业发展的迫切需求。为此制定《关键信息基础设施安全服务能力要求》团体标准，旨在规范网络安全服务机构的服务行为，提升其安全服务能力，确保关键信息基础设施的稳健运行。

本标准围绕关键信息基础设施安全服务机构的核心能力进行深入剖析，主要包括两大方面：一是安全服务保障能力，在网络安全服务机构自身综合保障层面，从基本条件、组织管理、项目管理、供应链管理、服务工具管理、远程服务、法律保障、数据安全保护、质量管理、保密管理、教育培训、服务可持续性、可持续性发展、服务机构行为规范性等多个角度出发，设定严格的标准和要求，以强化网络安全服务机构内部的安全管理和风险防范。二是安全服务供给能力，在网络安全服务机构对外提供安全服务的能力层面，旨在从经验积累、专业人员、专业工具三个方面，明确提出了服务能力要求，以确保网络安全服务机构能够为关键信息基础设施运营者提供管理、技术、运营等不同维度高效、专业的安全服务。

通过实施本标准，期望能够提升关键信息基础设施网络安全服务机构的整体服务质量和水平，进一步筑牢关键信息基础设施安全防线，为数字经济的健康发展提供有力支撑。

关键信息基础设施安全服务能力要求

1 范围

本文件确立了关键信息基础设施安全服务框架、总体要求、能力模型，规定了网络安全服务机构提供关键信息基础设施安全服务应具备的能力要求。

本文件适用于指导网络安全服务机构开展关键信息基础设施安全服务，以及评价网络安全服务机构的能力水平，也可为关键信息基础设施安全服务需求方选择网络安全服务机构时提供参考。

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 信息安全技术 信息安全风险评估方法

GB/T 22080 信息技术 安全技术 信息安全管理体系 要求

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 25069 信息安全技术 术语

GB/T 25070 信息安全技术 网络安全等级保护安全设计技术要求

GB/T 30271 信息安全技术 信息安全服务能力评估准则

GB/T 30283—2022 信息安全技术 信息安全服务 分类与代码

GB/T 32914—2023 信息安全技术 网络安全服务能力要求

GB/T 35274 信息安全技术 大数据服务安全能力要求

GB/T 37973 信息安全技术 大数据安全管理指南

GB/T 37988 信息安全技术 数据安全能力成熟度模型

GB/T 38631 信息技术 安全技术 GB/T 22080 具体行业应用 要求

GB/T 38674 信息安全技术 应用软件安全编程指南

GB/T 39204 信息安全技术 关键信息基础设施安全保护要求

GB/T 39477 信息安全技术 政务信息共享 数据安全技术要求

GB/T 39786 信息安全技术 信息系统密码应用基本要求

GB/T 41479 信息安全技术 网络数据处理安全要求

GB/T 42446 信息安全技术 网络安全从业人员能力基本要求

GB/T 42461 信息安全技术 网络安全服务成本度量指南

GB/T 43207 信息安全技术 信息系统密码应用设计指南

T/CIIPA 00007 关键信息基础设施安全检测评估能力要求

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）

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）

3 术语和定义

GB/T 25069、GB/T 32914、GB/T 39204 界定的以及下列术语和定义适用于本文件。

3.1

关键信息基础设施安全服务 cybersecurity service of critical information infrastructure

根据服务协议，基于服务人员、技术、工具、管理和资金等资源，提供保障关键信息基础设施运行安全、网络信息安全等服务的相关过程。

注：简称“安全服务”。

3.2

关键信息基础设施安全服务需求方 cybersecurity service acquirer

获取外部所提供的网络安全服务，以满足关键信息基础设施安全保护需求，实现自身业务目标的组织或个人。

注：简称“服务需求方”。

3.3

网络安全服务机构 cybersecurity service provider

按照服务协议，通过专业的网络安全人员提供网络安全服务的组织或个人。

注：简称“服务机构”。

4 缩略语

下列缩略语适用于本文件。

CII：关键信息基础设施（Critical Information Infrastructure）

CMMI：能力成熟度模型集成（Capability Maturity Model Integration）

CISP：注册信息安全专业人员（Certified Information Security Professional）

IOC：失陷指标（Indicators of Compromise）

IP：网际协议（Internet Protocol）

PE：可移植的可执行文件（Portable Executable）

5 安全服务框架

关键信息基础设施安全服务框架见图 1，主要包括以下几方面内容：

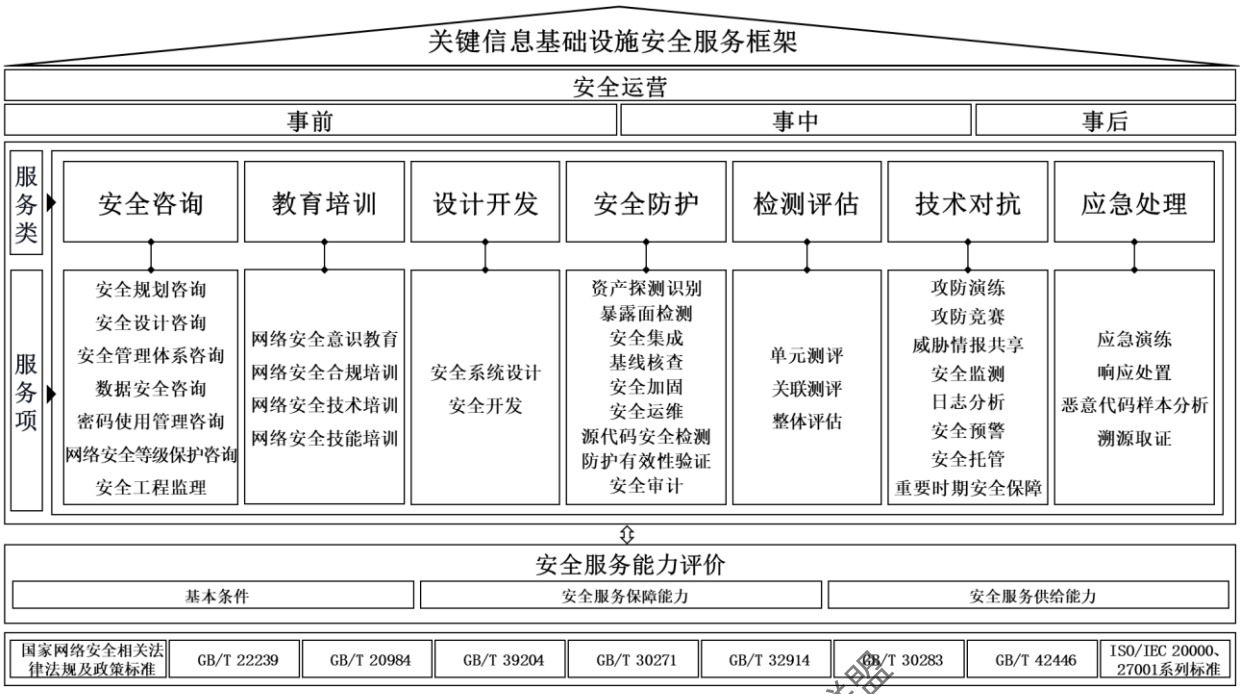

图1 关键信息基础设施安全服务框架

a） 安全服务划分为服务类，并进一步划分为服务项；服务需求方根据自身实际和关键信息基础设施安全保护需求，对服务类或服务项进行组合，形成安全服务实例；安全服务可以服务实例的形式，由一个或多个服务类或者服务项构成；可包含本文件不涉及的其他扩展的服务；

b） 服务类包括关键信息基础设施安全咨询、教育培训、设计开发、安全防护、检测评估、技术对抗、应急处理等；其中，安全咨询服务划分为安全规划咨询、安全设计咨询、安全管理体系咨询、数据安全咨询、密码使用管理咨询、网络安全等级保护咨询、安全工程监理等服务项；教育培训服务划分为网络安全意识教育、网络安全合规培训、网络安全技术培训、网络安全技能培训等服务项；设计开发服务划分为安全系统设计、安全开发等服务项；安全防护服务划分为资产探测识别、暴露面检测、安全集成、基线核查、安全加固、安全运维、防护有效性验证、源代码安全检测、安全审计等服务项；检测评估服务划分为单元测评、关联测评、整体评估等服务项；技术对抗服务划分为攻防演练、攻防竞赛、威胁情报共享、安全监测、日志分析、安全预警、安全托管、重要时期安全保障等服务项；应急处理服务划分为应急演练、响应处置、恶意代码样本分析、溯源取证等服务项；安全服务内容、关键活动和交付成果见附录 A，安全服务类别与 GB/T 30283-2022 服务类别（代码）的对应关系见附录 B；

c） 服务机构开展安全服务，应符合网络安全有关法律、行政法规的规定以及国家和行业相关标准的要求；

d） 服务机构开展安全服务，应遵循第 6.1 条的基本原则，满足第 6.2 条的基本条件，具备第 8 章、第 9 章规定的相关能力；

e） 可通过安全服务评价对服务机构综合安全服务能力或专项安全服务能力进行能力评价，评价方法可参照第 7 章规定的安全服务能力模型开展。

6 总体要求

6.1 基本原则

网络安全服务机构向服务需求方提供关键信息基础设施安全服务，应满足 GB/T 32914 的要求，同时遵循以下基本原则：

a） 合规性原则：应采取合法、正当的方式开展安全服务活动，应采取明确合理的控制措施确保安全服务不超出服务需求方的需求范围，避免非授权开展安全服务，不得损害国家安全、社会公共利益或者他人合法权益；

b） 风险管理原则：应采取必要的措施，保障安全服务过程的可控性，应避免对相关组织和个人的安全造成不良影响；服务机构宜采取现场服务形式提供安全服务，不推荐以远程服务的方式开展安全服务相关关键活动；

c） 保密性原则：在服务过程中，应严格保密相关信息，防止敏感数据泄露，维护关键信息基础设施的数据安全；

d） 持续改进原则：在服务过程中，应具备持续改进的能力，及时更新安全服务工具与技术，改进安全服务管理机制。

6.2 基本条件

服务机构应具备以下基本条件：

a） 在中华人民共和国境内注册成立，由中国公民、法人投资或者国家投资的企事业单位；

b） 产权关系明晰，注册资金 500 万元以上，独立经营核算，无违法违规记录；

c） 法定代表人、董事、合伙人以及高层管理人员、服务人员仅限中华人民共和国境内的中国公民，且无犯罪记录；

d） 从事网络安全服务 2 年以上；

e） 具有网络安全相关工作经历的技术和管理人员不少于 15 人，岗位职责清晰，且人员相对稳定；

f） 具有固定的办公场所，配备满足安全服务需要的服务工具和实验环境等；

g） 具有完备的安全服务流程与保密管理、项目管理、质量管理、人员管理、档案管理和培训教育等规章制度。

7 安全服务能力模型

7.1 模型组成

关键信息基础设施安全服务能力模型见图 2，主要包括以下几方面内容：

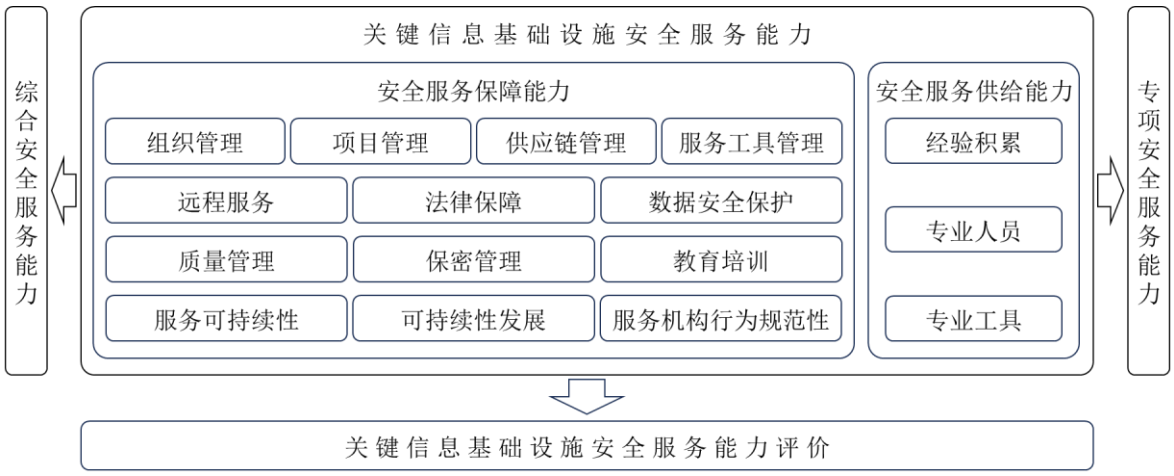

图2 关键信息基础设施安全服务能力模型

a） 关键信息基础设施安全服务能力主要包括安全服务保障能力和安全服务供给能力两方面核心能力；其中，安全服务保障能力侧重于描述服务机构自身综合保障能力，即服务机构确保安全服务能够正常配置部署、有效实施并持续改进的内部安全管理和风险防范综合能力，主要包括组织管理、项目管理、供应链管理、服务工具、远程服务、法律保障、数据安全保护、质量管理、保密管理、教育培训、服务可持续性、可持续性发展、服务机构行为规范性等能力；安全服务供给能力侧重于描述服务机构对外提供高效、专业安全服务的能力，即在协助服务需求方应对关键信息基础设施安全威胁和风险时，所能提供的资源、工具、技术和方法的综合能力；

b） 关键信息基础设施安全服务能力评价可根据服务机构自身业务需求选择第 5 章第 b）条的安全咨询、教育培训、设计开发、安全防护、检测评估、技术对抗、应急处理服务中专项安全服务能力进行评价；在专项安全服务能力评价基础上，可对服务机构的综合安全服务能力进行评价；对于本文件不涉及的其他扩展服务，可参照本文件设计评价指标及评价方法进行评价。

7.2 评价指标

关键信息基础设施安全服务能力评价指标见附录 C，主要包括：

a） 基本条件，合规项 7 项，必要项 6 项；

b） 安全服务保障能力，包括组织管理能力、项目管理能力、供应链管理能力、服务工具管理能力、远程服务能力、法律保障能力、数据安全保护能力、质量管理能力、保密管理能力、教育培训能力、服务可持续性能力、可持续性发展能力、行为规范性能力，合规项 78 项，必要项 41 项；

c） 安全服务供给能力；其中，安全咨询服务能力合规项 46 项，必要项 12 项；教育培训服务能力合规项 20 项，必要项 5 项；设计开发服务能力合规项 15 项，必要项 4 项；安全防护服务能力合规项 59 项，必要项 17 项；检测评估服务能力评价指标应符合 T/CIIPA 00007 相关要求；技术对抗服务能力合规项 59 项，必要项 17 项；应急处理服务能力合规项 27 项，必要项 8 项。

7.3 评价方法、流程及形式

关键信息基础设施安全服务能力评价方法、流程及形式包括：

a） 根据参评机构的类型以及评价指标的可获取性、方法可实现性，结合评价目的和需求、评价周期等因素选择适用的评价方法；

b） 评价时可根据各项评价指标在参评机构安全服务能力中的作用差异，调整各项指标的权重；

c） 评价时应根据各项评价指标进行加权和赋值，便于实现评价结果的定量化表达；

d） 评价流程一般包括确定评价目的、制定评价方案、收集评价信息、遴选评价专家、综合分析评价、形成评价结果等基本步骤；

e） 评价形式可采用自评估或第三方评估的形式；

f） 评价活动应明确评价报告的格式，至少包含以下内容：参评机构与评价主体的基本信息、评价活动基本情况、各项评价指标的权重、各项评价指标的赋值方法、评价专家与评价主体的意见、评价专家与评价主体的签字或盖章等；

g） 对于评价结果应明确其作用范围与时效性。

7.4 评价准则

关键信息基础设施安全检测评估能力评价应符合 T/CIIPA 00007 相关要求；安全咨询、教育培训、设计开发、安全防护、技术对抗、应急处理服务能力评价应首先判断必要项的满足情况，如出现必要项不满足，整体的结论为不通过；其次，必要项全部满足情况下，再对合规项进行评价，根据合规率×权重的算法计算得出整体分值；分值大于等于 65 分整体结论为通过，分值低于 65 分为不通过。具有相关服务经验或资质的人员在同一服务类不同服务项中可以复用，在不同服务类中复用的情况不能超过 3 个服务类。

表 1 服务机构的专项安全服务能力评价表

评价结论	服务机构的专项安全服务能力评分标准	
	合规项加权计算分值	必要项评价
通过	$\sum_{i=1}^{15}\left(\frac{\text{单合规项满足数}}{\text{单合规项总数}}\times\text{权重}\times 100\right)_i \geqslant 65$	全部满足
不通过	$\sum_{i=1}^{15}\left(\frac{\text{单合规项满足数}}{\text{单合规项总数}}\times\text{权重}\times 100\right)_i < 65$	全部满足
不通过	N/A	存在不满足情况

8 安全服务保障能力要求

8.1 组织管理

服务机构的组织管理能力应满足以下要求：

a） 应制定完备的、符合自身特点的安全服务项目管理流程，主要应包括服务工作的组织形式、工作职责、服务各阶段的工作内容和管理要求等，可参考 GB/T 30271 规定的安全服务过程制定；

b） 应制定人员管理制度，包括人员录用、考核、日常管理以及离职等方面的内容和要求；应建立并保存服务人员的人员档案，包括人员基本信息、社会背景、工作经历、培训记录、专业资格、奖惩情况等，保障人员的稳定和可靠；

c） 应设置满足安全服务工作需要的岗位，如安全服务技术员、安全服务项目负责人、技术主管、质量主管、保密安全员、设备管理员和档案管理员等，岗位职责明确，人员稳定；

d） 具有胜任安全服务工作的专业技术人员和管理人员，大学本科（含）以上学历所占比例不低于 70%；

e） 应指定一名具有大学本科（含）以上学历的人员担任技术主管，全面负责安全服务方面的技术工作；

f） 至少有 1 名服务人员接受过系统的项目管理培训，并获得过项目管理相关权威机构的认证，掌握开展相关安全服务的目的、流程、关键活动、交付成果等要求；

g） 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 30%；

h） 在项目实施前，服务机构应对服务人员进行安全背景审查，通过审查的人员方能上岗；

i） 当服务人员离岗时，服务机构应及时终止离岗人员的所有访问权限，收回服务需求方提供的资料、安全服务活动生成的数据和记录、安全服务交付成果等所有服务资料；

j） 应制定申诉、投诉及争议处理制度，明确包括服务机构各岗位人员在申诉、投诉和争议处理活动中相应的职责，建立从受理、确认到处置、答复等环节的完整程序。

8.2 项目管理

8.2.1 服务方案

服务机构的关键信息基础设施安全服务方案应满足以下要求：

a） 应在深入调研服务需求方现状后，根据服务需求方的实际情况编写服务方案；

b） 在服务方案中应明确服务计划进度等，并明确服务过程中的各类交付成果；

c） 在服务方案中明确服务工具清单，明确服务过程中可能存在的各类风险以及应对措施；

d） 在服务方案中明确具体的服务验收标准。

8.2.2 成本控制

服务机构的安全服务成本管理应满足以下要求：

a） 应在项目实施前按照 GB/T 42461 对安全服务项目的成本进行度量后合理确定服务报价；
b） 应明确项目所需的人员、设备、技术等资源，确保资源配置合理，满足项目目标需求和预算要求；
c） 应建立项目成本监控机制，定期审核项目预算和实际支出，防止成本超支。

8.2.3 服务实施

服务机构在服务实施过程中应满足以下要求：
a） 应在服务过程中指定专人与服务需求方进行沟通，确保沟通渠道畅通，应向服务需求方定期汇报项目进度、进展以及存在的问题与解决方案建议等；
b） 服务实施前，服务机构和服务人员应与服务需求方签署保密协议；
c） 应根据安全服务工作流程，有计划、有步骤地开展安全服务工作，并保证安全服务活动的每个环节都得到有效的控制。

8.2.4 进度管理

服务机构在项目实施过程中的进度管理应满足以下要求：
a） 应制定详细的服务计划；应在服务计划中设定明确的项目里程碑，确保每个关键时间节点能够按期完成阶段任务；
b） 服务机构的安全服务项目负责人应定期召开项目进度会议，记录会议纪要并追踪进展，确保所有服务人员都能及时了解项目进展和潜在风险；
c） 应针对项目实施过程中存在的风险做好应对措施，避免项目进度受到影响。

8.2.5 变更管理

服务机构进行服务变更应满足以下要求：
a） 服务变更前应书面告知服务需求方变更带来的风险、影响以及补救措施，经过服务需求方评估同意并做好变更记录后，确保服务变更以受控的方式得到评估、批准和实施；禁止开展未授权的服务活动；
b） 变更的服务内容不应影响整体服务的服务水平。

8.2.6 风险控制

服务机构在服务过程中的风险控制应满足以下要求：
a） 应充分估计安全服务可能给服务需求方带来的风险，风险包括但不限于服务机构由于自身能力或资源不足造成的风险、安全服务活动可能对服务需求方关键业务和信息系统正常运行造成影响的风险、服务工具接入可能对服务需求方关键业务和信息系统正常运行造成影响的风险、服务过程中可能发生的服务需求方关键业务和信息系统重要信息（如网络拓扑、IP 地址、业务流程、安全机制、安全隐患和有关文档等）泄露的风险等；
b） 应通过多种措施对上述服务需求方关键业务和信息系统可能面临的风险加以规避和控制。

8.2.7 成果交付

服务机构交付服务成果应满足相关规范性要求，并通过必要的评审。

8.3 供应链管理

服务机构的供应链管理应遵照服务需求方的供应链管理相关制度进行管理与执行，应满足以下要求：
a） 应建立供应链安全管理制度和策略，明确供应链安全管理目标；建立供应商评价制度，定期对供应商进行评价，以便在服务过程中优先选择评价结果更好的供应商；

b） 如果在服务过程中，使用引入服务机构自身能力之外的人员、软件、系统、工具时，应提前告知服务需求方；服务机构在服务过程中需要引入供应商人员的，按照第 8.1 条相关要求对相关人员进行筛选、考核和管理，同时应为引入的人员提供服务过程所必需的软硬件资源，并在服务过程中以及服务结束后，开展检查和审核；

c） 在提供服务过程中必须使用获得授权的正版商业软件，严禁使用盗版商业软件。

8.4 服务工具管理

服务机构在服务过程中使用服务工具应满足以下要求：

a） 应制定服务工具管理制度，包括服务机构人员在服务工具管理中的相关职责，以及服务工具的购置、使用和运行维护的各项规定等；

b） 服务工具属于网络关键设备和网络安全专用产品的，应当按照相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求；

c） 在服务开始前，服务机构应就服务工具清单与服务需求方进行确认；服务工具应具备全面的功能列表且不存在功能列表之外的隐蔽功能；在服务过程中，如果确需使用服务工具清单之外的工具的，应在使用前通过恶意代码检测等测试，并与服务需求方进行沟通，得到服务需求方审批授权后方可使用，严禁使用未授权工具；

d） 使用的服务工具不应对服务需求方的业务稳定性、网络性能、系统的安全性带来影响。

8.5 远程服务

服务机构确实需要远程提供服务的，应满足 GB/T 32914—2023 第 5.7 条要求。

8.6 法律保障

服务机构在法律保障方面应满足 GB/T 32914—2023 第 5.8 条要求。

8.7 数据安全保护

服务机构对服务过程中获取的数据（包括原始数据和加工分析产生的数据等），应满足以下要求：

a） 在开展服务前，应通过合同条款或者保密协议等方式，明确服务机构和服务需求方各自在数据安全保护的责任和义务；

b） 应具备完善的数据安全管理制度，并采取技术手段保护数据安全，防范发生数据泄露；

c） 在服务过程中若涉及敏感数据或核心数据的操作或加工，应在服务需求方指定的设备上进行；

d） 应制定文档管理制度，包括服务机构人员在服务文档管理中的相关职责、档案借阅、保管直至销毁的各项规定等；

e） 在服务过程中获取的数据只能用于维护服务需求方关键信息基础设施安全的需要，不得用于其他用途。

8.8 质量管理

8.8.1 管理体系建立

服务机构建立安全服务管理体系应满足以下要求：

a） 应建立、实施和维护符合关键信息基础设施安全服务工作需要的文件化的管理体系，确保服务机构各级人员能够理解和执行，并获得信息技术服务管理体系及相关领域质量管理体系认证资质；

b） 应制定相应的质量目标，不断提升自身的检测评估质量和管理水平；

c） 应指定一名质量主管，明确其质量保证的职责；质量主管不应受可能有损工作质量的影响或利益冲突，并有权直接与服务机构管理层沟通。

8.8.2 管理体系维护

服务机构维护安全服务管理体系应满足以下要求：

a） 应保证管理体系的有效运行，发现问题及时反馈并采取纠正措施，确保其有效性；

b） 应严格遵守申诉、投诉及争议处理制度，并应记录采取的措施；

c） 应建立并实施内部管理体系审核和反馈处理机制，以验证管理体系的符合性及有效性，确保在管理体系运行过程中发现的问题及时得到解决；执行审核的人员应独立于被审核部门。

8.8.3 质量监督

服务机构应指定监督员对全体服务人员开展监督，监督内容包括现场安全服务活动、服务过程规范性和交付成果的规范性、准确性等。

8.9 保密管理

服务机构应满足以下保密管理要求：

a） 应根据国家有关保密规定制定保密管理制度，制度中应明确保密对象的范围、人员保密职责和义务、服务过程保密管理各项措施与要求、奖惩机制、离岗后的脱密期限等内容，确保服务需求方提供的资料、安全服务活动生成的数据和记录、安全服务交付成果等所有服务资料安全；

b） 应指派安全服务保密工作负责人，并明确安全服务各岗位保密要求；

c） 应与全体服务人员签订保密责任书，规定其应当履行的保密义务和承担的法律责任，定期对服务人员进行保密培训和考核；

d） 服务机构和服务人员应保守在安全服务活动中知悉的国家秘密、工作秘密、商业秘密、个人隐私等。

8.10 教育培训

服务机构的教育培训应满足以下要求：

a） 应建立网络安全服务知识技能教育培训制度，包括培训计划的制定、培训工作的实施、培训的考核与上岗以及人员培训档案建立等内容和要求；

b） 应定期对全员开展安全意识培训；应根据服务人员的工作岗位职责和培训需求，制定详细和有针对性的培训计划，对服务人员进行专业培训并进行岗位培训、考核和评定，并保存培训和考核记录；

c） 应安排具有 2 年以上网络安全工作经验、具有安全服务项目经历的专家作为讲师进行培训；

d） 服务人员应参加并通过服务机构安排的各类培训，获得行业认可的安全服务领域专业资质证书，每年的培训时长累计不少于 40 学时，其中安全保密培训不少于 8 学时。

8.11 服务可持续性

服务机构保障服务可持续性应满足 GB/T 32914—2023 第 5.10 条和第 6.7 条要求。

8.12 可持续性发展

服务机构在可持续性发展方面应满足以下要求：

a） 应根据自身情况制定战略规划，通过不断地投入保证自身的持续建设和发展；

b） 应定期对管理体系进行评审并持续改进，不断提高管理要求；设定中、远期目标，通过目标的实现，逐步提升质量管理能力；

c） 应跟踪国内外新技术、新应用的发展，通过专项课题研究和实践，确保服务能力与当前的技术发展和业务发展的同步性和先进性。

8.13 服务机构行为规范性

服务机构不得从事以下活动：

a） 影响服务需求方关键业务和信息系统正常运行，危害服务需求方关键业务和信息系统安全；
b） 故意隐瞒服务过程中发现的安全问题，或者在服务过程中弄虚作假，未如实提供安全服务交付成果；
c） 非授权占有、使用和安全服务相关资料及数据文件；
d） 分包或转包安全服务项目；
e） 限定服务需求方购买、使用其指定的网络安全产品；
f） 其他危害国家安全、社会秩序、公共利益以及服务需求方利益的活动。

9 安全服务供给能力要求

9.1 安全咨询

9.1.1 安全规划咨询

服务机构开展安全规划咨询服务应满足以下能力要求：

a） 应在近 3 年内具有不少于 3 个安全规划咨询服务案例；
b） 应获得信息安全管理体系认证资质和信息安全风险评估二级及以上服务资质，或同级别认证资质；
c） 具有 5 年以上网络安全从业经验，且参与过 2 个以上安全规划咨询服务项目的服务人员不少于 2 人；
d） 具有获得 CISP 认证或同级别认证的服务人员不少于 2 人；
e） 服务人员掌握 GB/T 42446 规定的网络安全管理类人员相关的知识和技能要求，熟悉关键信息基础设施安全保护相关法律、行政法规和标准规范；
f） 具备支撑开展网络安全前瞻性技术研究的实验条件；
g） 具备以服务需求方实际需求为导向，提供定制化、可操作的具有全面性和前瞻性的安全规划或计划方案的能力，具备每年开展不少于 1 个安全规划咨询服务项目的实施能力。

9.1.2 安全设计咨询

服务机构开展安全设计咨询服务应满足以下能力要求：

a） 应在近 3 年内具有不少于 3 个安全设计咨询服务项目实施经验；
b） 应获得信息安全管理体系认证资质和信息安全风险评估二级及以上服务资质，或同级别认证资质；
c） 具有 5 年以上网络安全从业经验，且参与过 2 个以上安全设计咨询服务项目的服务人员不少于 2 人；
d） 具有获得 CISP 认证或同级别认证的服务人员不少于 2 人；
e） 服务人员掌握 GB/T 42446 规定的网络安全管理类人员相关的知识和技能要求，熟悉关键信息基础设施安全保护相关法律、行政法规和标准规范；
f） 具备支撑开展网络安全前瞻性技术研究的实验条件；
g） 具备开展安全框架、安全策略、安全技术体系结构、安全管理体系结构等方面的设计能力，具备每年开展不少于 1 个安全设计咨询服务项目的实施能力。

9.1.3 安全管理体系咨询

服务机构开展安全管理体系咨询服务应满足以下能力要求：

a） 应在近 3 年内具有不少于 3 个安全管理体系咨询服务项目实施经验；

b） 应获得信息安全管理体系认证资质和信息安全风险评估二级及以上服务资质，或同级别认证资质；
c） 具有 5 年以上网络安全从业经验，且参与过 2 个以上安全管理体系咨询服务项目的服务人员不少于 2 人；
d） 具有获得 CISP 认证或同级别认证的服务人员不少于 2 人；
e） 服务人员掌握 GB/T 42446 规定的网络安全管理类人员相关的知识和技能要求，熟悉 GB/T 22080、GB/T 38631 相关安全管理体系要求，熟悉关键信息基础设施安全保护相关法律、行政法规和标准规范；
f） 具备安全管理风险评估，以及安全管理制度和安全策略方案设计能力，具备每年开展不少于 1 个安全管理体系咨询服务项目的实施能力。

9.1.4 数据安全咨询

服务机构开展数据安全咨询服务应满足以下能力要求：
a） 应在近 3 年内具有不少于 3 个数据安全咨询服务项目实施经验；
b） 应获得信息安全管理体系认证资质和信息安全风险评估二级及以上服务资质，或同级别认证资质；
c） 具有 5 年以上网络安全从业经验，且参与过 2 个以上数据安全咨询服务项目的服务人员不少于 2 人；
d） 具有获得 CISP 认证或同级别认证的服务人员不少于 2 人；
e） 服务人员掌握 GB/T 42446 规定的网络安全管理类、网络安全建设类人员相关的知识和技能要求，熟悉数据安全保护相关法律、行政法规，GB/T 41479、GB/T 35274、GB/T 37988、GB/T 37973、GB/T 39477 及其他相关标准规范；
f） 具有数据安全评估、风险评估等服务工具；
g） 具备提供覆盖数据全生命周期的安全服务的能力，包括数据分类分级、数据脱敏、数据加密、数据泄露防护等，具备每年开展不少于 1 个数据安全咨询服务项目的实施能力。

9.1.5 密码使用管理咨询

服务机构开展密码使用管理咨询服务应满足以下能力要求：
a） 应在近 3 年内具有不少于 1 个商用密码应用安全性评估服务项目实施经验；
b） 应通过国家密码管理部门组织的商用密码检测机构（商用密码应用安全性评估业务）资质审查；
c） 具有 5 年以上网络安全从业经验，且参与过 1 个以上商用密码应用安全性评估服务项目的服务人员不少于 2 人；
d） 具有获得密码技术应用员职业资格，并通过国家密码管理部门组织的商用密码应用安全性评估从业人员考核的服务人员不少于 2 人；
e） 服务人员掌握 GB/T 42446 规定的网络安全建设类人员相关的知识和技能要求，熟悉密码相关法律、行政法规，GB/T 39786、GB/T 43207 及其他相关标准规范，密码学理论基础扎实，熟悉各种密码算法、协议和标准；
f） 服务过程及解决方案中所涉及的商用密码技术、产品和服务应符合国家密码管理有关要求；
g） 具备提供覆盖密码生成、存储、分发、使用、销毁全生命周期的咨询服务能力，具备每年开展不少于 1 个密码使用管理咨询服务项目的实施能力。

9.1.6 网络安全等级保护咨询

服务机构开展网络安全等级保护咨询服务应满足以下能力要求：
a） 应在近 3 年内具有不少于 3 个网络安全等级保护咨询服务项目实施经验；
b） 应获得网络安全等级测评与检测评估机构服务认证资质或同级别认证资质；

c） 具有 5 年以上网络安全从业经验，且参与过 2 个以上网络安全等级保护咨询服务项目的服务人员不少于 2 人；
d） 具有网络安全等级保护高级测评师不少于 1 人；
e） 服务人员掌握 GB/T 42446 规定的网络安全建设类人员相关的知识和技能要求，熟悉网络安全等级保护相关法律、行政法规和 GB/T 22239、GB/T 25070 等标准规范；
f） 具备提供覆盖信息系统定级、备案、建设整改、等级测评、监督检查全流程的咨询服务能力，具备每年开展不少于 1 个网络安全等级保护咨询服务项目的实施能力。

9.1.7 安全工程监理

服务机构开展安全工程监理服务应满足以下能力要求：
a） 应在近 3 年内具有不少于 3 个信息安全工程监理服务项目实施经验；
b） 应获得信息安全管理体系认证资质；
c） 具有 3 年以上信息安全工程监理服务经验的服务人员不少于 2 人；
d） 具有获得 CISP 认证或同级别认证的服务人员不少于 2 人；
e） 服务人员掌握 GB/T 42446 规定的网络安全建设类人员相关的知识和技能要求；
f） 具备提供覆盖项目准备阶段、实施阶段和验收阶段等全过程的安全工程监理服务能力，具备每年开展不少于 1 个安全工程监理服务项目的实施能力。

9.2 教育培训

9.2.1 网络安全意识教育

服务机构开展网络安全意识教育服务应满足以下能力要求：
a） 应在近 3 年内具有不少于 1 个网络安全意识教育服务项目实施经验；
b） 具有获得 CISP 认证或同等资质认证的服务人员不少于 2 人；
c） 服务人员掌握 GB/T 42446 规定的网络安全科研教育类人员相关的知识和技能要求；
d） 具有针对不同参训人员特点和需求的网络安全意识教育课程，支持通过理论授课、网络安全事件案例警示教育等多种方式提升参训人员的网络安全意识和知识水平，具备每年开展不少于 1 个网络安全意识教育服务项目的实施能力。

9.2.2 网络安全合规培训

服务机构开展网络安全合规培训服务应满足以下能力要求：
a） 应在近 3 年内具有不少于 1 个网络安全合规培训服务项目实施经验；
b） 具有 5 年以上网络安全从业经验，且熟悉关键信息基础设施安全保护相关法律、行政法规和标准规范的服务人员不少于 2 人；
c） 具有获得 CISP 认证或同等资质认证的服务人员不少于 2 人；
d） 服务人员掌握 GB/T 42446 规定的网络安全科研教育类人员相关的知识和技能要求；
e） 具有关键信息基础设施安全保护相关法律、行政法规和标准规范解读和培训相关课程，具备每年开展不少于 1 个网络安全合规培训服务项目的实施能力。

9.2.3 网络安全技术培训

服务机构开展网络安全技术培训服务应满足以下能力要求：
a） 应在近 3 年内具有不少于 1 个网络安全技术培训服务项目实施经验；
b） 具有网络攻防实战项目经历或 5 年以上网络安全从业经验，且熟悉关键信息基础设施安全保护相关法律、行政法规和标准规范的服务人员不少于 2 人；
c） 具有获得 CISP 认证或同等资质认证的服务人员不少于 2 人；

d） 服务人员掌握 GB/T 42446 规定的网络安全科研教育类人员相关的知识和技能要求；
e） 具有网络安全管理体系、风险管理、安全策略、数据安全和隐私保护、供应链管理等基本概念和方法，以及网络安全技术基础、高级网络安全技术、新技术安全防护、行业最佳实践和成功案例等相关课程，具备每年开展不少于 1 个网络安全技术培训服务项目的实施能力。

9.2.4 网络安全技能培训

服务机构开展网络安全技能培训服务应满足以下能力要求：
a） 应在近 3 年内具有不少于 1 个网络安全技能培训服务项目实施经验；
b） 具有网络攻防实战项目经历，熟练使用网络安全产品和掌握操作系统、网络设备的安全配置方法的服务人员不少于 2 人；
c） 具有获得 CISP 认证或同等资质认证的服务人员不少于 2 人；
d） 服务人员掌握 GB/T 42446 规定的网络安全科研教育类人员相关的知识和技能要求；
e） 具有可以进行技能培训的模拟仿真环境或实训平台；
f） 具有网络安全实战化知识和技术、实战训练等课程，具备每年开展不少于 1 个网络安全技能培训服务项目的实施能力。

9.3 设计开发

9.3.1 安全系统设计

服务机构开展安全系统设计服务应满足以下能力要求：
a） 从事网络安全服务 5 年以上，从事安全系统设计服务不少于 3 年，应在近 3 年内具有不少于 2 个安全系统设计服务项目实施经验；
b） 应获得软件安全开发二级及以上服务资质或同级别认证资质，并通过CMMI3 及以上级别认证；
c） 具有 5 年以上网络安全从业经验，且参与过 2 个以上安全系统设计服务项目的服务人员不少于 2 人；
d） 具有获得 CISP 认证或同级别认证的服务人员不少于 2 人；
e） 服务人员掌握 GB/T 42446 规定的网络安全建设类人员相关的知识和技能要求，熟悉关键信息基础设施安全保护相关法律、行政法规和标准规范；
f） 具备按照服务需求方应用环境特性和实际需求提出安全防护设计要求的能力，具备每年开展不少于 1 个安全系统设计服务项目的实施能力。

9.3.2 安全开发

服务机构开展安全开发服务应满足以下能力要求：
a） 从事网络安全服务 5 年以上，从事安全开发服务不少于 3 年，应在近 3 年内具有不少于 2 个安全开发服务项目实施经验；
b） 应获得软件安全开发二级及以上服务资质或同级别认证资质，并通过CMMI3 及以上级别认证；
c） 具有掌握关键信息基础设施安全保护相关法律、行政法规和标准规范要求，具备 3 年以上安全开发经验，且参与过 2 个以上安全系统设计服务项目的服务人员不少于 2 人；
d） 具有安全开发人员不少于 15 人；
e） 服务人员掌握 GB/T 42446 规定的网络安全建设类人员相关的知识和技能要求，熟悉关键信息基础设施安全保护相关法律、行政法规和标准规范；
f） 具备在需求分析、设计、编码、测试和部署等环节嵌入安全控制措施的能力，管控开发全过程安全；
g） 如果在服务过程中确需引入第三方开发机构的，第三方机构应满足安全开发服务对应的资质和人员要求；

h） 如果在服务过程中引入第三方组件或者开源代码，应征得服务需求方同意后，并通过代码审计、漏洞扫描等方式排查第三方组件或者开源代码安全风险可控后，方可引入；服务人员应详细记录第三方组件或者开源代码来源等信息，在服务交付时一并提供给服务需求方；
i） 开发的网络安全系统或产品应能通过国家有关部门或者独立第三方的安全评估与检测；
j） 具备按照服务需求方特定的安全需求和安全设计要求开发网络安全系统或产品的能力，具备每年开展不少于 1 个安全开发服务项目的实施能力。

9.4 安全防护

9.4.1 资产探测识别

服务机构开展资产探测识别服务应满足以下能力要求：
a） 应在近 3 年内具有不少于 3 个资产探测识别服务项目实施经验；
b） 应至少获得信息系统安全运维二级及以上服务资质、网络安全审计二级及以上服务资质、信息安全风险评估二级及以上服务资质中的 1 项，或同级别认证资质；
c） 具有熟练使用资产探测识别工具，具备 3 年以上网络安全从业经验，且参与过 3 个以上资产探测识别项目的服务人员不少于 2 人；
d） 具有获得 CISP 认证或同级别认证的服务人员不少于 2 人；
e） 服务人员掌握 GB/T 42446 规定的网络安全建设类人员相关的知识和技能要求，掌握 GB/T 20984 规定的资产识别方法，熟悉关键信息基础设施安全保护相关法律、行政法规和标准规范；
f） 具有自主知识产权的资产探测识别工具，具有资产信息指纹特征库，能够利用工具自动获取网络资产信息，包括服务器、计算机终端、移动设备、物联网设备、存储设备、网络设备、安全设备等；
g） 具备利用资产探测技术识别服务需求方关键业务链所依赖的网络、系统、数据、服务和其他类资产的能力，具备每年开展不少于 1 个资产探测识别服务项目的实施能力。

9.4.2 暴露面检测

服务机构开展暴露面检测服务应满足以下能力要求：
a） 应在近 3 年内具有不少于 3 个暴露面检测服务项目实施经验；
b） 应至少获得信息系统安全运维二级及以上服务资质、网络安全审计二级及以上服务资质、信息安全风险评估二级及以上服务资质中的 1 项，或同级别认证资质；
c） 具有熟练使用和配置暴露面检测工具，具备 3 年以上网络安全从业经验，且参与过 3 个以上暴露面检测服务项目的服务人员不少于 2 人；
d） 具有获得 CISP 认证或同级别认证的服务人员不少于 2 人；
e） 服务人员掌握 GB/T 42446 规定的网络安全运营类人员相关的知识和技能要求，熟悉关键信息基础设施安全保护相关法律、行政法规和标准规范；
f） 具备自主知识产权的暴露面检测工具；
g） 具备对暴露在互联网的服务、域名、IP、端口等数字资产暴露面进行发现和识别，持续监测重要网站系统异常情况，如网页篡改、敏感词、网站挂马、黑链等的能力，具备每年开展不少于 1 个暴露面检测服务项目的实施能力。

9.4.3 安全集成

服务机构开展安全集成服务应满足以下能力要求：
a） 应在近 3 年内具有不少于 3 个安全集成服务项目实施经验；
b） 应获得信息系统安全集成二级及以上服务资质或同级别认证资质；

c） 具有 3 年以上安全集成服务经验，且参与过 3 个以上安全集成服务项目的服务人员不少于 10 人；
d） 具有获得 CISP 认证或同级别认证的服务人员不少于 3 人；
e） 服务人员掌握 GB/T 42446 规定的网络安全建设类人员相关的知识和技能要求，熟悉关键信息基础设施安全保护相关法律、行政法规和标准规范；
f） 具备对服务需求方关键信息基础设施安全保护现状、差距与需求进行分析，设计整体解决方案的能力，具备每年开展不少于 1 个安全集成服务项目的实施能力。

9.4.4 基线核查

服务机构开展基线核查服务应满足以下能力要求：
a） 应在近 3 年内具有不少于 3 个基线核查服务项目实施经验；
b） 应至少获得信息系统安全运维二级及以上服务资质、网络安全审计二级及以上服务资质、信息安全风险评估二级及以上服务资质中的 1 项，或同级别认证资质；
c） 具有 5 年以上网络安全从业经验、3 年以上基线核查服务经验，且参与过 3 个以上基线核查服务项目的服务人员不少于 3 人；
d） 具有获得 CISP 认证或同级别认证的服务人员不少于 3 人；
e） 服务人员掌握 GB/T 42446 规定的网络安全运营类人员相关的知识和技能要求，熟悉关键信息基础设施安全保护相关法律、行政法规和标准规范；
f） 具备自主知识产权的基线核查工具；
g） 具备使用自动化基线核查工具进行基线核查并开展人工抽查复核的能力，能够定期、自动地进行核查和差异分析并生成详细的报告，识别重要服务器、操作系统、数据库、中间件、存储设备、网络设备、安全设备和系统等实际配置与基线标准之间的偏差，发现异常时及时告警，提供改进建议；具备详细记录和追溯能力，支持事后审计和问题定位；具备每年开展不少于 1 个基线核查服务项目的实施能力。

9.4.5 安全加固

服务机构开展安全加固服务应满足以下能力要求：
a） 应在近 3 年内具有不少于 3 个安全加固服务项目实施经验；
b） 应至少获得信息系统安全运维二级及以上服务资质、网络安全审计二级及以上服务资质、信息安全风险评估二级及以上服务资质中的 1 项，或同级别认证资质；
c） 具有 5 年以上网络安全从业经验、3 年以上安全加固服务经验，且参与过 3 个以上安全加固服务项目的服务人员不少于 3 人；
d） 具有获得 CISP 认证或同级别认证的服务人员不少于 3 人；
e） 服务人员掌握 GB/T 42446 规定的网络安全运营类人员相关的知识和技能要求，熟悉关键信息基础设施安全保护相关法律、行政法规和标准规范；
f） 具备对服务器、操作系统、数据库、中间件、存储设备、网络设备、安全设备和系统等的脆弱性进行分析和加固的能力，具备每年开展不少于 1 个安全加固服务项目的实施能力。

9.4.6 安全运维

服务机构开展安全运维服务应满足以下能力要求：
a） 应在近 3 年内具有不少于 3 个安全运维服务项目实施经验；
b） 应获得信息系统安全运维二级及以上服务资质或同级别认证资质；
c） 具有 5 年以上网络安全从业经验、3 年以上安全运维服务经验，掌握操作系统、数据库、中间件、存储设备、网络设备、安全设备和系统等功能及原理，且参与过 3 个以上安全运维服务项目的服务人员不少于 3 人；

d） 具有获得 CISP 认证或同级别认证的服务人员不少于 3 人；
e） 服务人员掌握 GB/T 42446 规定的网络安全运营类人员相关的知识和技能要求，熟悉关键信息基础设施安全保护相关法律、行政法规和标准规范；
f） 具备开展应用系统、中间件、数据库、操作系统、服务器、存储设备、网络设备、安全设备和系统等的管理、维护和安全防护，维护网络及业务系统安全运行的能力，具备每年开展不少于 1 个安全运维服务项目的实施能力。

9.4.7 源代码安全检测

服务机构开展源代码安全检测服务应满足以下能力要求：
a） 应在近 3 年内具有不少于 3 个源代码安全检测服务项目实施经验；
b） 应至少获得信息系统安全运维二级及以上服务资质、网络安全审计二级及以上服务资质、信息安全风险评估二级及以上服务资质中的 1 项，或同级别认证资质；
c） 具有 5 年以上网络安全从业经验、3 年以上源代码安全检测服务经验，且参与过 3 个以上源代码安全检测服务项目的服务人员不少于 3 人；
d） 具有获得 CISP 认证或同级别认证的服务人员不少于 3 人；
e） 服务人员掌握 GB/T 42446 规定的网络安全建设类人员相关的知识和技能要求，熟悉关键信息基础设施安全保护相关法律、行政法规和标准规范；
f） 具有源代码安全检测工具；
g） 具备对软件源代码分析识别安全漏洞或缺陷的能力，具备每年开展不少于 1 个源代码安全检测服务项目的实施能力。

9.4.8 防护有效性验证

服务机构开展防护有效性验证服务应满足以下能力要求：
a） 应在近 3 年内具有不少于 3 个防护有效性验证服务项目实施经验；
b） 应至少获得信息系统安全运维二级及以上服务资质、网络安全审计二级及以上服务资质、信息安全风险评估二级及以上服务资质中的 1 项，或同级别认证资质；
c） 具有 5 年以上网络安全从业经验、1 年以上防护有效性验证服务经验，掌握安全测试和评估方法、渗透测试方法和技术、网络攻防技术等，掌握常见安全漏洞及利用方法，且参与过 1 个以上防护有效性验证服务项目的服务人员不少于 2 人；
d） 具有获得 CISP 认证或同级别认证的服务人员不少于 2 人；
e） 服务人员掌握 GB/T 42446 规定的网络安全运营类人员相关的知识和技能要求，熟悉关键信息基础设施安全保护相关法律、行政法规和标准规范；
f） 具有防护有效性验证工具；
g） 具备通过模拟攻击行为等方法，验证单点安全策略或安全防护体系是否能够有效阻止恶意攻击的能力，具备每年开展不少于 1 个防护有效性验证服务项目的实施能力。

9.4.9 安全审计

服务机构开展安全审计服务应满足以下能力要求：
a） 应在近 3 年内具有不少于 3 个安全审计服务项目实施经验；
b） 应获得网络安全审计二级及以上服务资质或同级别认证资质；
c） 具有 5 年以上网络安全从业经验、3 年以上安全审计服务经验，掌握网络安全审计方法和技术，且参与过 3 个以上安全审计服务项目的服务人员不少于 2 人；
d） 具有获得 CISP-Auditor 认证或同级别认证的服务人员不少于 2 人；
e） 服务人员掌握 GB/T 42446 规定的网络安全审计和评估类人员相关的知识和技能要求，熟悉关键信息基础设施安全保护相关法律、行政法规和标准规范；

f） 具备评估和管理网络安全风险、出具网络安全审计报告的能力，具备每年开展不少于 1 个安全审计服务项目的实施能力。

9.5 检测评估

服务机构开展检测评估服务应符合 T/CIIPA 00007 相关要求。

9.6 技术对抗

9.6.1 攻防演练

服务机构开展攻防演练服务应满足以下能力要求：

a） 应在近 3 年内具有不少于 3 个攻防演练服务项目实施经验，近 3 年内没有出现因阶段性验收未通过或企业自身原因而废止的攻防演练服务项目；

b） 应获得信息系统安全运维二级及以上服务资质、信息安全应急处理二级及以上服务资质中的 1 项，或同级别认证资质；

c） 具有 5 年以上网络安全从业经验、3 年以上攻防演练服务经验，且参与过 3 个以上攻防演练服务项目的服务人员不少于 5 人；

d） 具有获得 CISP 认证或同级别认证、参加过关键基础设施安全防护技术和标准相关系统培训的服务人员不少于 5 人；

e） 服务人员掌握 GB/T 42446 规定的网络安全建设类、网络安全审计和评估类人员相关的知识和技能要求，熟悉关键信息基础设施安全保护相关法律、行政法规和标准规范；

f） 具有攻防演练平台类工具；

g） 具备通过多场景攻防演练，全面测试验证服务需求方的防御措施和分析溯源措施有效性的能力，具备每年开展不少于 1 个攻防演练服务项目的实施能力。

9.6.2 攻防竞赛

服务机构开展攻防竞赛服务应满足以下能力要求：

a） 应在近 3 年内具有不少于 3 个攻防竞赛服务项目实施经验，近 3 年内没有出现因阶段性验收未通过或企业自身原因而废止的攻防竞赛服务项目；

b） 应获得信息系统安全运维二级及以上服务资质、信息安全应急处理二级及以上服务资质中的 1 项，或同级别认证资质；

c） 具有 5 年以上网络安全从业经验、3 年以上攻防竞赛服务经验，且参与过 3 个以上攻防竞赛服务项目的服务人员不少于 5 人；

d） 具有获得 CISP 认证或同级别认证、参加过关键基础设施安全防护技术和标准相关系统培训的服务人员不少于 5 人；

e） 服务人员掌握 GB/T 42446 规定的网络安全审计和评估类人员相关的知识和技能要求，熟悉关键信息基础设施安全保护相关法律、行政法规和标准规范；

f） 具有攻防竞赛平台类工具；

g） 具备攻防竞赛赛制设计、赛题设计等能力，能够支撑开展赛前准备、现场部署、赛中运维、赛后收尾工作，具备每年开展不少于 1 个攻防竞赛服务项目的实施能力。

9.6.3 威胁情报共享

服务机构开展威胁情报共享服务应满足以下能力要求：

a） 应在近 3 年内具有不少于 3 个威胁情报共享服务项目实施经验；

b） 应获得信息安全风险评估二级及以上服务资质同级别认证资质；

c） 具有 5 年以上网络安全从业经验、3 年以上威胁情报共享服务经验，且参与过 3 个以上威胁情报共享服务项目的服务人员不少于 2 人；
d） 具有获得 CISP 认证或同级别认证的服务人员不少于 2 人；
e） 服务人员掌握 GB/T 42446 规定的网络安全运营类人员相关的知识和技能要求，熟悉《网络产品安全漏洞管理规定》等安全漏洞管理要求，熟悉关键信息基础设施安全保护相关法律、行政法规和标准规范；
f） 具备威胁情报获取途径和手段，建设维护百万级威胁情报库和管理技术手段；
g） 具备威胁情报收集、加工、分析、共享和处置的能力，每年开展不少于 1 个威胁情报共享服务项目的实施能力。

9.6.4 安全监测

服务机构开展安全监测服务应满足以下能力要求：
a） 应在近 3 年内具有不少于 3 个安全监测服务项目实施经验，近 3 年内没有出现因阶段性验收未通过或企业自身原因而废止的安全监测服务项目；
b） 应获得信息系统安全运维二级及以上和信息安全应急处理二级及以上服务资质，或同级别认证资质；
c） 具有 5 年以上网络安全从业经验、3 年以上安全监测服务经验，熟练使用安全监测工具，熟悉各类网络安全事件的应急处置流程，且参与过 3 个以上安全监测服务项目的服务人员不少于 5 人；
d） 具有获得 CISP 认证或同级别认证的服务人员不少于 3 人；
e） 服务人员掌握 GB/T 42446 规定的网络安全运营类人员相关的知识和技能要求，熟悉关键信息基础设施安全保护相关法律、行政法规和标准规范；
f） 支持 5×8、7×8、7×24 小时等驻场值守，具备分钟级的网络安全事件发现和响应能力；
g） 服务过程中如果需要在服务需求方设备上安装服务所需的程序，应经服务需求方同意并在测试环境测试通过后方可部署；
h） 具备对被监测对象的运行状态、网络安全事件、日志与流量等数据收集、处理，分析研判整体安全态势，及时发现处置异常情况或行为的能力，具备每年开展不少于 1 个安全监测服务项目的实施能力。

9.6.5 日志分析

服务机构开展日志分析服务应满足以下能力要求：
a） 应在近 3 年内具有不少于 3 个日志分析服务项目实施经验；
b） 应获得信息系统安全运维二级及以上和信息安全应急处理二级及以上服务资质，或同级别认证资质；
c） 具有 5 年以上网络安全从业经验、3 年以上日志分析服务经验，熟练使用日志分析工具，熟悉各类网络安全事件的应急处置流程，且参与过 3 个以上日志分析服务项目的服务人员不少于 3 人；
d） 具有获得 CISP 认证或同级别认证的服务人员不少于 3 人；
e） 服务人员掌握 GB/T 42446 规定的网络安全运营类人员相关的知识和技能要求，熟悉关键信息基础设施安全保护相关法律、行政法规和标准规范；
f） 具有自主知识产权的智能化分析引擎，建设维护智能检测模型和信息资源库等；
g） 开展日志分析服务所需日志宜通过服务需求方的日志审计系统或威胁检测与告警系统获取；
h） 如果需要在服务需求方设备上安装部署客户端或者日志采集程序，应征得服务需求方的同意，并在测试环境测试通过后方可安装部署；

i） 具备提供针对行业与场景的定制化日志分析解决方案能力，具备每年开展不少于 1 个日志分析服务项目的实施能力。

9.6.6 安全预警

服务机构开展安全预警服务应满足以下能力要求：

a） 应在近 3 年内具有不少于 3 个安全预警服务项目实施经验；
b） 应获得信息系统安全运维二级及以上和信息安全应急处理二级及以上服务资质，或同级别认证资质；
c） 具有 5 年以上网络安全从业经验、3 年以上安全预警服务经验，熟悉各类网络安全事件的应急处置流程，且参与过 3 个以上安全预警服务项目的服务人员不少于 3 人；
d） 具有获得 CISP 认证或同级别认证的服务人员不少于 3 人；
e） 服务人员掌握 GB/T 42446 规定的网络安全运营类人员相关的知识和技能要求，熟悉关键信息基础设施安全保护相关法律、行政法规和标准规范；
f） 服务过程中应将威胁情报的研判、最新漏洞通告、网络告警事件研判结果等可能影响服务需求方安全的内容及时提交给服务需求方；
g） 具备综合分析研判网络安全态势形成内部安全预警信息、获取外部安全预警信息，协助服务需求方开展预警信息生成、发布、响应和解除的能力，具备每年开展不少于 1 个安全预警服务项目的实施能力。

9.6.7 安全托管

服务机构开展安全托管服务应满足以下能力要求：

a） 应在近 3 年内具有不少于 3 个安全托管服务项目实施经验；
b） 应获得信息系统安全运维二级及以上和信息安全应急处理二级及以上服务资质，或同级别认证资质；
c） 具有 5 年以上网络安全从业经验、3 年以上安全托管服务经验，熟悉各类网络安全事件的应急处置流程，且参与过 3 个以上安全托管服务项目的服务人员不少于 15 人；
d） 具有获得 CISP 认证或同级别认证的服务人员不少于 5 人；
e） 服务人员掌握 GB/T 42446 规定的网络安全运营类人员相关的知识和技能要求，熟悉关键信息基础设施安全保护相关法律、行政法规和标准规范；
f） 对于通过自建安全运营中心提供安全托管服务的，应具备独立数据中心机房且满足网络安全等级保护三级及以上要求；
g） 支持 5×8、7×8、7×24 小时驻场值守，具备分钟级的网络安全事件发现和响应能力；
h） 具备识别服务需求方托管资产、及时发现响应安全威胁与异常事件、定期提供安全报告的能力，具备每年开展不少于 1 个安全托管服务项目的实施能力。

9.6.8 重要时期安全保障

服务机构开展重要时期安全保障服务应满足以下能力要求：

a） 应在近 3 年内具有不少于 3 个国家重大活动、重大赛事、重要会议和网络安全实战演习期间等安全保障服务项目实施经验，近 3 年内没有出现因阶段性验收未通过或企业自身原因而废止的重要时期安全保障服务项目；
b） 应获得信息系统安全运维二级及以上和信息安全应急处理二级及以上服务资质，或同级别认证资质；
c） 具有 5 年以上网络安全从业经验、3 年以上重要活动或重大演习等安全保障服务经验，熟悉各类网络安全事件的应急处置流程，且参与过 3 个以上重要活动或重大演习等安全保障服务项目的服务人员不少于 5 人；

d） 具有获得 CISP 认证或同级别认证的服务人员不少于 3 人；
e） 服务人员掌握 GB/T 42446 规定的网络安全运营类人员相关的知识和技能要求，熟悉关键信息基础设施安全保护相关法律、行政法规和标准规范；
f） 具备重要时期对关键业务和信息系统进行全面的风险评估和威胁分析，制定并执行定制化安全加固方案，开展事前评估准备、事中监测防御、事后总结加固的能力，具备每年开展不少于 1 个重要时期安全保障服务项目的实施能力。

9.7 应急处理

9.7.1 应急演练

服务机构开展应急演练服务应满足以下能力要求：
a） 应在近 3 年内具有不少于 3 个应急演练服务项目实施经验；
b） 应获得信息系统安全运维二级及以上服务资质、信息安全应急处理二级及以上服务资质中的 1 项，或同级别认证资质；
c） 具有 5 年以上网络安全从业经验、3 年以上应急演练服务经验，且参与过 3 个以上应急演练服务项目的服务人员不少于 5 人；
d） 具有获得 CISP 认证或同级别认证的服务人员不少于 1 人；
e） 服务人员掌握 GB/T 42446 规定的网络安全运营类人员相关的知识和技能要求，熟悉《国家网络安全事件应急预案》等相关要求，熟悉关键信息基础设施安全保护相关法律、行政法规和标准规范；
f） 具备根据服务需求方的定制化需求与业务实际运行场景，帮助服务需求方制定、检验及完善应急预案，以及制定应急演练方案并协助实施的能力，具备每年开展不少于 1 个应急演练服务项目的实施能力。

9.7.2 响应处置

服务机构开展响应处置服务应满足以下能力要求：
a） 应在近 3 年内具有不少于 3 个应急处理服务项目实施经验；
b） 应获得信息系统安全运维二级及以上服务资质、信息安全应急处理二级及以上服务资质中的 1 项，或同级别认证资质；
c） 具有 5 年以上网络安全从业经验、3 年以上应急处理服务经验，掌握应急分析溯源技能，且参与过 3 个以上应急处理服务项目的服务人员不少于 5 人；
d） 具有获得 CISP 认证或同级别认证的服务人员不少于 2 人；
e） 服务人员掌握 GB/T 42446 规定的网络安全运营类人员相关的知识和技能要求，熟悉关键信息基础设施安全保护相关法律、行政法规和标准规范；
f） 具备制定与执行应急处置策略的能力，能够根据网络安全事件的性质和影响，设计并实施针对性的应急处置方案，包括系统恢复、数据保护和威胁消除等措施，确保事件得到有效处理；
g） 应保证 7×24 小时的服务响应，具备网络安全事件发生时快速响应的能力，能够在事件检测后立即采取初步隔离措施，防止威胁扩散，并及时向服务需求方及相关安全管理机构报告，具备每年开展不少于 1 个响应处置服务项目的实施能力。

9.7.3 恶意代码样本分析

服务机构开展恶意代码样本分析服务应满足以下能力要求：
a） 应在近 3 年内具有不少于 3 个恶意代码样本分析服务项目实施经验；
b） 应获得信息系统安全运维二级及以上服务资质、信息安全应急处理二级及以上服务资质中的 1 项，或同级别认证资质；

c） 具有 5 年以上网络安全从业经验、3 年以上恶意代码样本分析服务经验，熟练使用动态分析工具、反汇编工具、PE 分析工具、逆向工程工具、恶意软件分类与识别工具、IOC 指标收集工具、样本提取工具等，且参与过 3 个以上恶意代码样本分析服务项目的服务人员不少于 3 人；
d） 具有获得 CISP 认证或同级别认证的服务人员不少于 2 人；
e） 服务人员掌握 GB/T 42446 规定的网络安全建设类人员相关的知识和技能要求，熟悉关键信息基础设施安全保护相关法律、行政法规和标准规范；
f） 具有恶意代码样本分析工具，建设维护亿级的恶意代码样本库和管理技术手段；
g） 具备开展恶意代码样本收集、样本动态分析、静态分析、交互性分析、样本分类、修复建议等工作的能力，具备每年开展不少于 1 个恶意代码样本分析服务项目的实施能力。

9.7.4 溯源取证

服务机构开展溯源取证服务应满足以下能力要求：
a） 应在近 3 年内具有不少于 3 个溯源取证服务项目实施经验；
b） 应获得信息安全应急处理二级及以上服务资质或同级别认证资质；
c） 具有 5 年以上网络安全从业经验、3 年以上溯源取证服务经验，且参与过 3 个以上溯源取证服务项目的服务人员不少于 5 人；
d） 具有获得 CISP 认证或同级别认证的服务人员不少于 2 人；
e） 服务人员掌握 GB/T 42446 规定的网络安全审计和评估类人员相关的知识和技能要求，熟悉关键信息基础设施安全保护相关法律、行政法规和标准规范；
f） 具有攻击溯源工具；
g） 具备提供自动化的应急分析及应急溯源服务，以及对电子证据进行提取、固定、恢复、分析的能力，具备每年开展不少于 1 个溯源取证服务项目的实施能力。

附 录 A
（资料性）
安全服务内容、关键活动和交付成果

A.1 安全咨询

A.1.1 安全规划咨询

安全规划咨询服务内容、关键活动及交付成果包括：

a） 安全规划咨询主要根据服务需求方关键信息基础设施所涉及系统及其支持的业务和管理的安全需求，由服务机构结合服务需求方投资预算、网络安全现状以及发展趋势，协助服务需求方明确关键信息基础设施安全保护工作的目标，从管理体系、技术体系、运营体系、保障体系等方面进行规划，加强机构、人员、经费、装备等资源保障，设计基本要求、工作任务、具体措施等内容以形成一套指导性文件，支撑服务需求方开展关键信息基础设施安全保护建设；

b） 安全规划咨询服务包括但不限于需求分析、现状评估、投资预算分析、安全保护目标设定、管理措施建议、技术解决方案推荐、指导性文件编制、培训以及持续监控与改进等关键活动；针对服务需求方发布的关键信息基础设施安全规划或计划提供执行情况和效益评估，跟进服务需求方安全规划或计划的推行和落地情况，支撑服务需求方建立持续优化、改进机制；

c） 安全规划咨询服务交付成果包括但不限于短期安全计划、中期或长期安全规划等综合性方案，以及数据安全保护计划等专项方案等。

A.1.2 安全设计咨询

安全设计咨询服务内容、关键活动及交付成果包括：

a） 安全设计咨询服务主要是针对服务需求方关键信息基础设施所涉及系统的安全防护需求，由服务机构落实服务需求方的安全规划或计划，设计总体安全策略，制定安全建设方案和实施方案，并在此基础上形成安全框架、安全策略、安全技术体系结构、安全管理体系结构等方面设计，支撑服务需求方关键信息基础设施安全保护具体实现；

b） 安全设计咨询服务包括但不限于需求分析、安全策略设计、安全方案设计、安全体系结构设计、安全政策与标准制定、技术方案评估、持续监控与评估等关键活动；

c） 安全设计咨询服务的交付成果包括但不限于顶层设计、概要设计和详细设计等设计文档。

A.1.3 安全管理体系咨询

安全管理体系咨询服务内容、关键活动及交付成果包括：

a） 安全管理体系咨询服务主要是针对服务需求方关键信息基础设施安全管理制度建设需求，由服务机构结合服务需求方的需求和目标、安全要求、所采用的过程、规模和结构，重点考虑基于关键业务链安全需求，设计关键信息基础设施安全管理制度和安全策略，确定安全管理范围和方针，明确责任、权限和角色，采用风险评估的方法规划建设任务，协助服务需求方建立、实现、维护并持续改进安全管理制度和安全策略；

b） 安全管理体系咨询服务包括但不限于需求分析、安全管理风险评估、安全管理体系方案设计、合规性建设、持续监控与评估等关键活动；

c） 安全管理咨询服务的交付成果包括但不限于安全管理风险评估报告、安全策略与方针设计方案、安全策略与控制措施设计方案、安全管理制度设计方案、安全管理培训计划方案等；其中，

安全策略包括但不限于安全互联策略、安全审计策略、身份管理策略、入侵防范策略、数据安全防护策略、自动化机制策略（配置、漏洞、补丁、病毒库等）、供应链安全管理策略、安全运维策略等，安全管理制度包括但不限于风险管理制度、网络安全考核及监督问责制度、网络安全教育培训制度、人员管理制度、安全检测评估制度、安全监测预警和信息通报制度、网络安全事件管理制度、业务连续性管理及容灾备份制度、三同步制度（安全措施同步规划、同步建设和同步使用）、供应链安全管理制度等；

A.2 教育培训

A.2.1 网络安全意识教育

网络安全意识教育服务内容、关键活动及交付成果包括：

a） 网络安全意识教育服务主要针对服务需求方提升人员安全意识需求，由服务机构开展网络安全基础知识介绍、网络安全案例分析等服务；

b） 网络安全意识教育服务包括但不限于培训需求分析、培训课程制定、培训计划编制、培训实施与评估等关键活动；

c） 网络安全意识教育服务交付成果包括但不限于培训计划、培训资料、培训评估报告等。

A.2.2 网络安全合规培训

网络安全合规培训服务内容、关键活动及交付成果包括：

a） 网络安全合规培训服务主要针对服务需求方解读网络安全法律、行政法规和标准规范等需求，由服务机构开展针对网络安全、数据安全、个人信息保护、网络安全等级保护、关键信息基础设施安全保护、商用密码应用安全性评估、信息技术应用创新产业、资质认证等相关合规要求培训服务；

b） 网络安全合规培训服务包括但不限于培训需求分析、培训课程制定、培训计划编制、培训实施与评估等关键活动；

c） 网络安全合规培训服务交付成果包括但不限于培训计划、培训资料、培训评估报告等。

A.2.3 网络安全技术培训

网络安全技术培训服务内容、关键活动及交付成果包括：

a） 网络安全技术培训服务主要针对服务需求方提升网络安全人员能力需求，由服务机构开展网络安全攻防、网络安全设备操作、网络安全基线核查、网络安全加固、安全开发等方面培训服务；

b） 网络安全技术培训服务包括但不限于培训需求分析、培训课程制定、培训计划编制、培训实施与评估等关键活动；

c） 网络安全技术培训服务交付成果包括但不限于培训计划、培训资料、培训评估报告等。

A.2.4 网络安全技能培训

网络安全技能培训服务内容、关键活动及交付成果包括：

a） 网络安全技能培训服务主要针对服务需求方提升网络安全人员技能水平需求，由服务机构围绕网络安全、数据安全、供应链安全、商用密码应用、网络攻防、职业资格认证等方面开展实操技能培训和实战训练工作；

b） 网络安全技能培训服务包括但不限于培训需求分析、培训课程制定、培训计划编制、培训实施与评估等关键活动；

c） 网络安全技能培训服务交付成果包括但不限于培训计划、培训资料、培训评估报告等。

A.3 设计开发

A.3.1 安全系统设计

安全系统设计服务内容、关键活动及交付成果包括：

a） 安全系统设计服务主要针对服务需求方不能通过采购现有信息安全系统或产品予以满足的安全需求，由服务机构按照需求分析、概要设计、详细设计等流程设计网络安全系统，可按照GB/T 38674 提出的应用软件安全编程通用框架的要求，结合服务需求方应用环境的特性，提出安全防护设计要求，以指导后续的安全开发；

b） 安全系统设计服务包括但不限于安全实现技术框架设计、安全功能设计、性能设计等关键活动；

c） 安全系统设计服务的交付成果包括但不限于需求分析文档、概要设计文档、详细设计以及各类设计的评审记录文档等。

A.3.2 安全开发

安全开发服务内容、关键活动及交付成果包括：

a） 安全开发服务主要针对服务需求方不能通过采购现有安全系统或产品予以满足的安全需求，由服务机构在安全系统设计的基础上，按照安全要求确认、安全基线要求确定、设计要求确认、安全策略制定、威胁建模、安全编码规范设计、事件响应计划制定、最终安全评审等软件安全开发流程开发网络安全系统或产品；并可按照 GB/T 38674 提出的应用软件安全编程通用框架的要求，采取相应的措施保障网络安全系统或产品的安全性，以满足服务需求方特定的安全需求并最大程度地减少网络安全系统或产品的安全缺陷；安全开发服务也可以基于已有的网络安全系统或产品进行二次开发。

A.4 安全防护

A.4.1 资产探测识别

资产探测识别服务内容、关键活动及交付成果包括：

a） 资产探测识别服务主要针对服务需求方关键资产识别需求，由服务机构围绕服务需求方关键信息基础设施承载的关键业务，采用资产探测技术识别关键业务链所依赖的网络、系统、数据、服务和其他类资产，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，并根据关键业务链所依赖资产的实际情况动态更新；资产探测识别服务的适用场景可根据服务需求方需求，覆盖云网端包括但不限于服务需求方内部网络、云计算环境、物联网网络、各类终端网络等资产的探测发现和识别；

b） 资产探测识别服务包括但不限于资产发现和清点、资产分类和标记、资产信息收集和分析、脆弱性优先级支撑、资产监控和告警等关键活动；

c） 资产探测识别服务交付成果包括但不限于资产清单、资产状态报告、资产监控分析报告、脆弱性报告、脆弱性优先级报告等。

A.4.2 暴露面收敛

暴露面收敛服务内容、关键活动及交付成果包括：

a） 暴露面收敛服务主要针对服务需求方减少不必要的资产和信息暴露、降低遭受潜在攻击风险的需求，由服务机构通过暴露面扫描工具对服务需求方的暴露面进行扫描，同时根据服务需求方的实际情况，提出对应的收敛措施建议；服务过程应覆盖服务需求方关键信息基础设施中的所有潜在暴露面，包括网络、应用、设备和用户等层面的暴露面；

b） 暴露面收敛服务包括但不限于暴露面扫描、暴露面评估、暴露面收敛、应急响应、持续监控与改进等关键活动，应识别互联网和服务需求方内网资产的互联网协议地址、端口、应用服务等暴露面，以及在公共存储空间存储可能被攻击者利用的服务需求方的技术文档、内部信息等，制定有效的收敛策略，并经服务机构和服务需求方共同评估确认且在测试环境测试后方可执

行，从而减少暴露面的数量和影响范围，提升整体安全性；收敛策略中应明确暴露面收敛操作带来的影响、风险以及应对措施，如互联网出口收敛方案等；

c） 暴露面收敛服务交付成果包括但不限于暴露面资产目录、暴露面收敛报告、收敛策略与实施计划等。

A.4.3 安全集成

安全集成服务内容、关键活动及交付成果包括：

a） 安全集成服务包括安全硬件集成、安全软件集成等集成服务，主要针对服务需求方采购或租赁的安全硬件设备、安全软件和系统（包括软件构件），由服务机构根据已制定的设计方案和实施方案等集成方案，明确集成部署安装方式，按照部署环境搭建、软件集成实施（包括现场系统开发）、安装配置、现场部署、功能调试、性能测试、评测改进等工作流程规范开展集成部署工作，确保各个安全软件和子系统实现安全互联互通和高效应用；

b） 安全集成服务涉及关键信息基础设施建设、改造、升级等环节，包括但不限于网络安全基础建设、现有网络安全建设升级或改造、网络安全系统性能扩容、功能增加、定制化需求等关键活动；

c） 安全硬件集成服务的内容通常覆盖信息安全需求分析、规划设计、设备采购、集成部署、交付验收等过程；安全软件集成服务通常覆盖信息安全需求分析、设计、实施与运行、测试与改进和验收等过程；其中，集成部署环境一般有以下几种：部署在服务需求方本地机房，部署在托管数据中心，部署在云平台的虚拟资源上，或者以前面几种形式混合部署等；

d） 安全集成服务交付成果包括但不限于网络安全需求分析报告、网络安全系统设计方案、网络安全设备采购和部署建议、网络安全集成实施报告等。

A.4.4 安全工程监理

安全工程监理服务内容、关键活动及交付成果包括：

a） 安全工程监理服务主要是针对服务需求方各类信息系统工程中涉及网络安全的工程活动，由服务机构根据服务需求方委托，在工程建设的规划设计、部署实施（招标、设计、实施、验收）各阶段实施控制和管理，提供相关建议和意见，确保实现各阶段的监理目标和完成监理内容；

b） 安全工程监理服务包括但不限于安全工程项目监理、关键信息基础设施运行维护阶段的网络安全服务监理等关键活动；安全工程监理服务的内容通常覆盖项目准备阶段、项目实施阶段和项目验收阶段等，通过质量控制、进度控制、合同管理、信息管理和协调，来促使信息安全工程以科学规范的流程，在一定的成本范围内，按时保质保量地完成，实现项目预期的信息安全目标；

c） 安全工程监理服务交付成果包括但不限于监理单位的监理权利、监理机构主要成员的职能分工说明、监理单位在信息安全工程建设过程中提供的服务及相关报告输出等。

A.4.5 基线核查

基线核查服务内容、关键活动及交付成果包括：

a） 基线核查服务是针对服务需求方关键信息基础设施的关键系统和设备配置的安全性和合规性核查需求，由服务机构受服务需求方委托开展自动化核查，识别和评估偏离基线的风险，并提供修复建议和持续监控与优化；

b） 基线核查对象包括但不限于主机操作系统、数据库、中间件和网络与安全设备等，具体检查内容包括但不限于账号和口令管理、认证和授权策略、访问控制、日志审核策略、入侵防范、剩余信息保护、系统资源控制、加密管理、通信协议、路由协议、其他安全配置等；

c） 基线核查服务交付成果包括但不限于基线配置清单、基线核查报告、偏离项修复建议等。

A.4.6 安全加固

安全加固服务内容、关键活动及交付成果包括：

a） 安全加固服务主要是针对服务需求方的网络设备、操作系统、数据库和应用系统等被加固对象，由服务机构在获得服务需求方允许的前提下，按照已制定的安全加固方案，采取补丁升级，关闭不必要的端口和服务、优化访问控制策略、增加安全机制等措施对被加固对象存在的安全缺陷和漏洞进行弥补和修复，以增强被加固对象的安全性，提高其安全保护能力；

b） 安全加固服务包括但不限于对关键业务和信息系统中的主机系统、网络设备、安全设备的脆弱性进行分析并加固，对主机系统的身份鉴别与认证、访问控制和审计跟踪策略增强，建设或优化网络隔离、信息过滤、容错、数据镜像、数据备份等关键活动，可采取配置加固、应用程序加固、操作系统加固、主机服务器加固等方式；

c） 安全加固服务交付成果包括但不限于网络安全加固方案、网络安全加固实施报告、安全配置管理报告、安全监控和运行报告等。

A.4.7 安全运维

安全运维服务内容、关键活动及交付成果包括：

a） 安全运维服务主要针对服务需求方关键信息基础设施安全运维规范管理需求，由服务机构协助服务需求方制定安全运维基线，采取运维行为审批、运维操作过程记录、运维工具审核及监视、运维人员适度授权等必要手段和措施，规范安全运维活动，以降低可能带来的风险；

b） 安全运维服务可分为基础设施安全运维、应用安全运维、数据安全运维等，包括但不限于脆弱性管理、安全配置管理、合规性管理、日志管理、数据备份与恢复、恶意代码防范和处理等关键活动，使用自动化工具支持系统账户、配置、漏洞、补丁、病毒库等的管理，开展漏洞、补丁验证后及时修补；

c） 安全运维服务交付成果包括但不限于安全基线设计、安全漏洞管理报告、安全配置管理报告、合规性管理报告、备份和恢复报告、安全培训材料等。

A.4.8 防护有效性验证

防护有效性验证服务内容、关键活动及交付成果包括：

a） 防护有效性验证服务主要针对服务需求方关键信息基础设施网络安全防护措施，由服务机构协助服务需求方采取入侵与模拟攻击技术，验证网络安全防护有效性，使服务需求方能够更好地了解网络安全防护状况，及时修复漏洞，提升安全防护能力，确保关键信息基础设施运行安全；

b） 服务机构应能够开展包括但不限于模拟攻击验证、评估防护有效性、测试防护设备性能等内容；

c） 服务机构应能够交付包括但不限于模拟攻击验证报告、防护有效性评估报告、防护设备测试性能报告等成果。

A.4.9 安全审计

安全审计服务内容、关键活动及交付成果包括：

a） 安全审计服务主要是针对服务需求方的关键信息基础设施安全保护相关活动，由服务机构通过文件审核、记录检查、技术测试、现场访谈等手段，采取网络审计措施等监测、记录系统运行状态、日常操作、故障维护、远程运维等，留存相关日志数据，获得审计证据，并对其进行客观的评价，形成审计报告，确定被审计对象满足审计依据的程度，帮助服务需求方全面了解和掌握其安全保护工作的有效性、充分性和适宜性；

b） 安全审计服务包括但不限于系统安全配置审计、日志审计和分析、合规性审计、安全策略和流程审计、用户行为分析审计等关键活动；审计对象包括但不限于各类服务器和业务系统、网络、数据库和终端等；审计范围包括但不限于服务需求方关键信息基础设施安全保护目标、安全管

理制度和策略、安全管理机构的建立、安全管理人员的管理、安全事件管理、安全教育培训、通信网络安全、计算环境安全、安全建设管理、安全运维管理、供应链安全保护、数据安全防护等；

c） 安全审计服务交付成果包括但不限于安全审计报告、日志审计报告、合规性审计报告、安全事件审计报告、安全策略和安全管理制度流程审计报告等。

A.5 检测评估

检测评估服务内容、关键活动及交付成果符合 T/CIIPA 00007 相关要求。

A.6 技术对抗

A.6.1 攻防演练

攻防演练服务内容、关键活动及交付成果包括：

a） 攻防演练服务主要针对服务需求方攻防演练需求，由服务机构协助服务需求方明确攻防演练的组织架构，编制演练规划，包括演练频次、规模、形式、时间、地点、预算等，制定演练的工作方案、保障方案、评估方案等，按照演练规划和方案执行安全演练，监视、评价安全演练过程，并就演练过程中存在的问题、取得的经验教训等加以改进，使安全演练符合预期设定目标，确保演练规划得到有效执行；通过演练使服务需求方相关人员了解和掌握攻防演练的流程，检验和优化现有安全策略的有效性和适用性，增强团队协作能力，提升安全事件的响应处置能力；

b） 攻防演练服务包括但不限于信息收集、演练场景设计、演练方案编制、攻击准备、模拟攻击、防御验证、演练评估、复盘总结等关键活动，演练形式包括实网攻防演练、模拟攻防演练、桌面推演等，应围绕服务需求方关键业务的可持续运行设定演练场景，可根据演练内容分为专项演练、综合演练，根据演练目的和作用分为检验性演练、示范性演练和研究性演练；应将关键信息基础设施核心供应链、紧密上下游产业链等业务相关单位，纳入演练范畴，应针对攻防演练中发现的安全问题及风险提出整改建议，消除结构性、全局性风险；

c） 攻防演练服务交付成果包括但不限于攻防演练计划、攻防演练工作方案、攻防演练保障方案、攻防演练评估方案、演练场景设计方案、攻击脚本、参与者手册、防御报告、攻防演练记录、攻防演练评估报告、攻防演练总结报告、参与者反馈、攻防演练改进计划、安全整改方案以及培训材料等。

A.6.2 攻防竞赛

攻防竞赛服务内容、关键活动及交付成果包括：

a） 攻防竞赛服务主要针对服务需求方开展攻防竞赛需求，由服务机构协助服务需求方赛前准备、竞赛支撑、赛后总结等阶段开展攻防竞赛支撑服务；

b） 攻防竞赛服务包括但不限于环境搭建、工具准备、漏洞挖掘、攻击防御、结果分析、经验总结等关键活动；

c） 攻防竞赛服务交付成果包括但不限于环境搭建报告、工具清单、漏洞挖掘报告、攻击防御报告、竞赛总结等。

A.6.3 威胁情报共享

威胁情报共享服务内容、关键活动及交付成果包括：

a） 威胁情报共享服务主要针对服务需求方威胁情报共享需求，由服务机构协助服务需求方建立本单位及外部协同网络威胁情报共享机制，组织联动上下级单位，协同联动权威网络威胁情报机构，采用多种技术手段，通过采集大规模、多渠道的网络安全威胁数据，集中进行深度融合、归并和分析，形成网络安全威胁信息，经人工或自动化处理为结构化信息，采用通用模型来实

现对网络安全威胁信息的统一描述，批量传递给服务需求方，以实现跨组织的海量网络安全威胁信息的快速传递，进而支持对复杂网络安全威胁的应对；

b） 威胁情报共享服务包括但不限于网络安全威胁数据搜集、威胁情报信息报送、威胁情报加工、威胁情报处置、网络安全威胁信息统一描述模型构建、威胁情报数据库建设维护、威胁情报共享传递等关键活动，情报来源可以选择开源情报、商业情报服务、社区情报等多种；网络安全威胁信息的描述通常由可观测数据、攻击指标、安全事件、攻击活动、威胁主体、攻击目标、攻击方法和应对措施等要素组成；

c） 威胁情报服务交付成果包括但不限于威胁趋势分析报告、威胁情报报告、攻击者分析报告等。

A.6.4 安全监测

安全监测服务内容、关键活动及交付成果包括：

a） 安全监测服务主要针对服务需求方关键信息基础设施的环境、网络、设备、系统、应用、不同区域间流动信息等被监测对象，由服务机构采用监测工具、平台或感知节点设备现场或远程对被监测对象的网络安全事件、运行状态、脆弱性与威胁进行监测和感知，以及时发现威胁、告警、事件等异常情况或行为，其中异常行为包括 APT 攻击等新型网络攻击行为；

b） 安全监测服务包括但不限于网络安全日志收集、流量采集、数据分析、常见系统通信流量或事态模型构建、违规操作模型构建、攻击入侵模型构建、异常行为模型构建、安全事件研判，以及国内外及行业关键信息基础设施安全事件、安全漏洞、解决方法和发展趋势研判等关键活动，应采用自动化机制对关键业务所涉及的系统的所有监测信息进行整合分析，将关键业务运行所涉及的各类信息进行关联，并分析整体安全态势，通过安全态势分析结果评估安全策略和安全控制措施是否合理有效；监测对象应重点关注网络边界、网络出入口等网络关键节点，以及关键业务所涉及的系统等；

c） 安全监测服务交付成果主要包括网络安全态势报告、异常活动分析报告、安全事件分析报告等。

A.6.5 日志分析

日志分析服务内容、关键活动及交付成果包括：

a） 日志分析服务主要针对服务需求方各类设备日志中的告警信息研判需求，由服务机构通过收集、存储、分析服务需求方各类设备中的日志、流量、性能、漏洞等多类数据，采用多类专业智能化分析引擎、AI 检测模型和信息资源库，识别网络攻击、恶意软件、信息泄露等安全威胁，并提出建议采取的解决方案或措施；

b） 日志分析服务主要包括但不限于信息收集、数据处理、数据分析研判、应急响应以及持续监控等关键活动；

c） 日志分析服务交付成果包括但不限于日志分析报告、日志数据汇总与可视化图表、关联分析与攻击预测报告。

A.6.6 安全预警

安全预警服务内容、关键活动及交付成果包括：

a） 安全预警服务主要针对服务需求方关键信息基础设施的安全预警需求，由服务机构持续获取预警发布机构的安全预警信息，对网络安全共享信息和监测工具生成的报警信息等进行综合分析、研判，评估相关事件或威胁对服务需求方关键信息基础设施可能造成损害的程度，必要时协助服务需求方生成内部预警信息、启动应急预案，采取相关措施对预警进行响应；

b） 安全预警服务包括网络安全共享信息获取、数据分析、预警信息生成、通报等关键活动；

c） 安全预警服务交付成果包括但不限于安全预警和报警信息分析报告、内部预警信息等。

A.6.7 安全托管

安全托管服务内容、关键活动及交付成果包括：

a） 安全托管服务主要针对服务需求方资源或专业能力不足的情况下，由服务机构识别和预防安全威胁的需求，支撑服务需求方实现安全运营；安全托管服务由服务机构通过自建或者使用服务需求方的安全运营中心统一进行全天候监测和管理，能够为接入服务需求方的各类信息系统、网络设备和安全设备提供全面的托管服务，包括防火墙、入侵检测系统、数据加密设备等，确保整体安全环境的持续维护与管理；

b） 安全托管服务包括但不限于通过定期主动扫描与被动识别等手段，识别服务需求方托管范围内的资产类型信息，并将资产信息录入到安全运营平台中进行统一管理；服务过程中提供 7×24 小时的安全监控，及时发现并响应安全威胁与异常事件；应定期向服务需求方提供安全报告，包括安全威胁分析、安全事件统计、安全建议等，帮助服务需求方了解当前的最新安全状况，并制定和调整相应的安全防护措施；

c） 安全托管服务交付成果包括但不限于安全事件统计报告、安全防护改进建议、安全威胁分析报告等。

A.6.8 重要时期安全保障

重要时期安全保障服务内容、关键活动及交付成果包括：

a） 重要时期安全保障服务主要针对服务需求方在重要活动期间开展网络安全保障工作需求，由服务机构从备战、迎战、决战、总结四个阶段开展网络安全保障工作；

b） 重要时期安全保障服务包括但不限于资产梳理、风险评估、威胁检测、安全加固、安全监测、应急响应、溯源分析、经验总结等关键活动；

c） 重要时期安全保障服务交付成果包括但不限于资产梳理报告、风险评估报告、威胁检测报告、安全加固方案、安全加固报告、安全监测报告、应急响应报告、溯源分析保障、重要活动保障总结等。

A.7 应急处置

A.7.1 应急演练

应急演练服务内容、关键活动及交付成果包括：

a） 应急演练服务主要针对服务需求方网络安全事件应急响应能力验证和评估需求，由服务机构协助服务需求方制定或评估修订网络安全事件应急预案，组织开展本组织的应急演练，组织或参加跨组织、跨地域的应急演练，监视、评价安全演练过程，并就演练过程中存在的问题、取得的经验教训等加以改进，使服务需求方相关人员了解和掌握网络安全事件应急处置的流程，提升和增强团队协作能力与团队成员的信任度，提高服务需求方在突发事件中的反应速度和处理能力；

b） 应急演练服务包括但不限于制定应急预案、制定应急演练计划、演练场景设计、演练方案编制、应急演练实施、应急演练活动评估、应急演练复盘总结等关键活动；其中，应急预案应在国家网络安全事件应急预案的框架下，根据行业和地方的特殊要求制定，应明确一旦信息系统中断、受到损害或者发生故障时，需要维护的关键业务功能，以及遭受破坏时恢复关键业务和恢复全部业务的时间，应包括非常规时期、遭受大规模攻击时等处置流程，同时包括服务需求方本组织和多个运营者间应急事件的处理，应与服务需求方内部相关计划以及其外部服务提供者的应急计划相协调，以确保连续性要求得以满足；

c） 应急演练服务交付成果包括但不限于应急演练计划、应急演练工作方案、应急演练保障方案、应急演练评估方案、应急演练场景设计方案、参与者手册、应急演练记录、应急演练评估报告、应急演练总结报告、参与者反馈、应急演练改进计划以及培训材料等。

A.7.2 响应处置

响应处置服务内容、关键活动及交付成果包括：

a） 响应处置服务主要针对影响关键信息基础设施安全的各类各级网络安全事件，由服务机构结合服务需求方的事件处置流程、应急预案等网络安全应急管理要求，在规定时间内快速进行标识、记录、分类和处理，恢复关键业务和信息系统到已知的状态，查找事件原因，提出应对措施防止关键业务和信息系统遭受再次破坏、危害或故障，及时总结事件处理活动的经验教训，为事件响应规程变更、培训以及测试等提供参考，最大程度减少损失和降低安全事件造成的消极影响；

b） 响应处置服务包括但不限于网络安全事件的准确识别、快速响应、制定与执行应急策略、系统恢复、事件总结评估等关键活动，分析网络攻击的方法、手段，制定防护策略和技术措施，采取捕获、干扰、阻断、封控、加固等多种技术手段切断攻击路径，快速处置网络攻击，提出安全策略改进建议；

c） 响应处置服务交付成果包括但不限于响应处置培训、应急处置方案、应急恢复评估报告等。

A.7.3 病毒样本分析

病毒样本分析服务内容、关键活动及交付成果包括：

a） 病毒样本分析服务主要针对病毒样本进行分析；

b） 病毒样本分析服务包括但不限于样本收集、样本动态分析、静态分析、交互性分析、样本分类、修复建议等关键活动；

c） 病毒样本分析服务交付成果包括但不限于动态分析报告、静态分析报告、修复建议方案、IOC特征、样本哈希值、修复建议等。

A.7.4 溯源取证

溯源取证服务内容、关键活动及交付成果包括：

a） 溯源取证服务主要针对网络安全相关违法犯罪活动，由服务机构根据服务需求方委托，使用符合相关技术标准和规范的取证设备和方法，确定攻击来源、攻击者身份、攻击路径、攻击目标等信息，通过技术手段收集、保全和记录电子证据，形成证据链以支持网络安全调查、分析、识别等工作；

b） 溯源取证服务包括但不限于确定调查依据、制定调查取证实施步骤、定位攻击源头，获取和保存电子证据、分析和验证证据链、溯源取证总结等关键活动，对攻击者进行画像，系统全面地分析网络攻击意图、技术与过程，提出安全策略改进建议；

c） 溯源取证服务交付成果包括但不限于攻击溯源分析报告、攻击路径可视化图表、攻击工具和技术分析文档、调查取证报告、电子证据、改进建议报告等。

附 录 B
（资料性）
安全服务类别与 GB/T 30283-2022 服务类别（代码）的对应关系

服务类	服务项	对应的服务类别（代码）
安全咨询	安全规划咨询	A01
	安全设计咨询	A02
	安全管理体系咨询	A03
	数据安全咨询	E01 E03
	密码使用管理咨询	F0106
	网络安全等级保护咨询	F0104
	安全工程监理	A04
教育培训	网络安全意识教育	A0601
	网络安全合规培训	A0602
	网络安全技术培训	A0603
	网络安全技能培训	A0603
设计开发	安全系统设计	B01
	安全开发	B02
安全防护	资产探测识别	/
	暴露面检测	D06
	安全集成	C01 C02 C99
	基线核查	/
	安全加固	D06 D10
	安全运维	D11 D13
	防护有效性验证	/
	源代码安全检测	D06 F0101
	安全审计	D12
检测评估	/	A05 D02 F01 F02 F99
技术对抗	攻防演练	D08
	攻防竞赛	D08
	威胁情报共享	D03
	安全监测	D01
	日志分析	D04
	安全预警	D07
	安全托管	E02
	重要时期安全保障	D07
应急处理	应急演练	D08
	响应处置	D07 D14
	恶意代码样本分析	/
	溯源取证	D09

附 录 C
（规范性）
服务机构安全服务能力评价指标

安全服务能力		权重	合规项指标描述	合规项数量	必要项标识
基本条件		10%	a）在中华人民共和国境内注册成立，是由中国公民、法人投资或者国家投资的企事业单位；	7	是
			b）产权关系明晰，注册资金 500 万元以上，独立经营核算，无违法违规记录；		是
			c）法定代表人、董事、合伙人以及高层管理人员、服务人员仅限中华人民共和国境内的中国公民，且无犯罪记录；		是
			d）从事网络安全服务 2 年以上；		是
			e）具有网络安全相关工作经历的技术和管理人员不少于 15 人，岗位职责清晰，且人员相对稳定；		是
			f）具有固定的办公场所，配备满足安全服务需要的服务工具和实验环境等；		是
			g）具有完备的安全服务流程与保密管理、项目管理、质量管理、人员管理、档案管理和培训教育等规章制度。		/
安全服务保障能力	组织管理	5%	a）应制定完备的、符合自身特点的安全服务项目管理流程，主要应包括服务工作的组织形式、工作职责、服务各阶段的工作内容和管理要求等，可参考 GB/T 30271 规定的安全服务过程制定；	10	/
			b）应制定人员管理制度，包括人员录用、考核、日常管理以及离职等方面的内容和要求；应建立并保存服务人员的人员档案，包括人员基本信息、社会背景、工作经历、培训记录、专业资格、奖惩情况等，保障人员的稳定和可靠；		/
			c）应设置满足安全服务工作需要的岗位，如安全服务技术员、安全服务项目负责人、技术主管、质量主管、保密安全员、设备管理员和档案管理员等，岗位职责明确，人员稳定；		/
			d）具有胜任安全服务工作的专业技术人员和管理人员，大学本科（含）以上学历所占比例不低于 70%；		是
			e）应指定一名具有大学本科（含）以上学历的人员担任技术主管，全面负责安全服务方面的技术工作；		/

安全服务能力			权重	合规项指标描述	合规项数量	必要项标识
				f）至少有 1 名服务人员接受过系统的项目管理培训，并获得过项目管理相关权威机构的认证，掌握开展相关安全服务的目的、流程、关键活动、交付成果等要求；		是
				g）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 30%；		/
				h）在项目实施前，服务机构应对服务人员进行安全背景审查，通过审查的人员方能上岗；		是
				i）当服务人员离岗时，服务机构应及时终止离岗人员的所有访问权限，收回服务需求方提供的资料、安全服务活动生成的数据和记录、安全服务交付成果等所有服务资料；		/
				j）应制定申诉、投诉及争议处理制度，明确包括服务机构各岗位人员在申诉、投诉和争议处理活动中相应的职责，建立从受理、确认到处置、答复等环节的完整程序。		/
	项目管理	服务方案	12%	a）应在深入调研服务需求方现状后，根据服务需求方的实际情况编写服务方案；	4	/
				b）在服务方案中应明确服务计划进度等，并明确服务过程中的各类交付成果；		/
				c）在服务方案中明确服务工具清单，明确服务过程中可能存在的各类风险以及应对措施；		/
				d）在服务方案中明确具体的服务验收标准。		/
		成本控制		a）应在项目实施前按照 GB/T 42461 对安全服务项目的成本进行度量后合理确定服务报价；	3	/
				b）应明确项目所需的人员、设备、技术等资源，确保资源配置合理，满足项目目标需求和预算要求；		/
				c）应建立项目成本监控机制，定期审核项目预算和实际支出，防止成本超支。		/
		服务实施		a）应在服务过程中指定专人与服务需求方进行沟通，确保沟通渠道畅通，应向服务需求方定期汇报项目进度、进展以及存在的问题与解决方案建议等；	3	是
				b）服务实施前，服务机构和服务人员应与服务需求方签署保密协议；		是
				c）应根据安全服务工作流程，有计划、有步骤地开展安全服务工作，并保证安全服务活动的每个环节都得到有效的控制。		/
		进度管理		a）应制定详细的服务计划；应在服务计划中设定明确的项目里程碑，确保每个关键时间节点能够按期完成阶段任务；	3	/
				b）服务机构的安全服务项目负责人应定期召开项目进度会议，记录会议纪要并追踪进展，确保所有服务人员都能及时了解项目进展和潜在风险；		/
				c）应针对项目实施过程中存在的风险做好应对措施，避免项目进度受到影响。		/

安全服务能力			权重	合规项指标描述	合规项数量	必要项标识
		变更管理		a）服务变更前应书面告知服务需求方变更带来的风险、影响以及补救措施，经过服务需求方评估同意并做好变更记录后，确保服务变更以受控的方式得到评估、批准和实施；禁止开展未授权的服务活动；	2	是
				b）变更的服务内容不应影响整体服务的服务水平。		/
		风险控制		a）应充分估计安全服务可能给服务需求方带来的风险，风险包括但不限于服务机构由于自身能力或资源不足造成的风险、安全服务活动可能对服务需求方关键业务和信息系统正常运行造成影响的风险、服务工具接入可能对服务需求方关键业务和信息系统正常运行造成影响的风险、服务过程中可能发生的服务需求方关键业务和信息系统重要信息（如网络拓扑、IP 地址、业务流程、安全机制、安全隐患和有关文档等）泄露的风险等；	2	是
				b）应通过多种措施对上述服务需求方关键业务和信息系统可能面临的风险加以规避和控制。		是
		成果交付		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、总结报告和验收报告等），并得到服务需求方的确认；	4	是
				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；		是
				c）完成服务交付后，根据与服务需求方的约定，主动将服务需求方提供的数据、资料、访问凭证、开通的账号和部署的工具等进行交还、清理或卸载，并向服务需求方提供由项目服务人员签字的承诺或确认函；		是
				d）交付成果应满足相关规范性要求，并通过必要的评审。		/
	供应链管理		5%	a）应建立供应链安全管理制度和策略，明确供应链安全管理目标；建立供应商评价制度，定期对供应商进行评价，以便在服务过程中优先选择评价结果更好的供应商；	3	/
				b）如果在服务过程中，使用引入服务机构自身能力之外的人员、软件、系统、工具时，应提前告知服务需求方；服务机构在服务过程中需要引入供应商人员的，按照第 8.1 条相关要求对相关人员进行筛选、考核和管理，同时应为引入的人员提供服务过程所必需的软硬件资源，并在服务过程中以及服务结束后，开展检查和审核；		是
				c）在提供服务过程中必须使用获得授权的正版商业软件，严禁使用盗版商业软件。		是
	服务工具管理		5%	a）应制定服务工具管理制度，包括服务机构人员在服务工具管理中的相关职责，以及服务工具的购置、使用和运行维护的各项规定等；	4	/

安全服务能力		权重	合规项指标描述	合规项数量	必要项标识
			b）服务工具属于网络关键设备和网络安全专用产品的，应当按照相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求；		是
			c）在服务开始前，服务机构应就服务工具清单与服务需求方进行确认；服务工具应具备全面的功能列表且不存在功能列表之外的隐蔽功能；在服务过程中，如果确需使用服务工具清单之外的工具的，应在使用前通过恶意代码检测等测试，并与服务需求方进行沟通，得到服务需求方审批授权后方可使用，严禁使用未授权工具；		是
			d）使用的服务工具不应对服务需求方的业务稳定性、网络性能、系统的安全性带来影响。		/
	远程服务	3%	a）对远程登录操作人员进行实名登记，分配仅能自用的账号；	5	是
			b）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、数字和特殊字符等三种以上的字符类型）的口令并定期更换；		是
			c）远程登录操作仅限于指定的终端及客户端（如有），并对权限范围和时间周期进行限制；		是
			d）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和完整性；		是
			e）至少留存 6 个月内远程操作的日志，定期对日志进行审计，审计过程中发现存在网络安全事件，应及时向服务需求方报告安全事件情况，并根据国家网络安全事件报告的有关规定报告安全事件。如网络安全服务涉及网络安全事件处置，应协助服务需求方根据《国家网络安全事件应急预案》及相关规定处置，并在服务需求方的服务器和终端等存储媒介妥善留存事件处置记录（包括事件原因、事件经过、事件影响、处置人员和处置结果等）和相关原始数据（如行为日志、网络数据包和有害样本程序等）。		是
	法律保障	2%	a）应有专业法务人员审核网络安全服务协议；	2	是
			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、水平、交付成果和验收等条款； ③网络安全服务的数据安全保护、项目成果知识产权归属和保密承诺等条款； ④体现因需遵循的法律法规、政策变化影响而造成服务终端、停止服务或退出市场等的相关条款及相应责任。		是
	数据安全保护	5%	a）在开展服务前，应通过合同条款或者保密协议等方式，明确服务机构和服务需求方各自在数据安全保护的责任和义务；	5	是

安全服务能力			权重	合规项指标描述	合规项数量	必要项标识
				b）应具备完善的数据安全管理制度，并采取技术手段保护数据安全，防范发生数据泄露；		/
				c）在服务过程中若涉及敏感数据或核心数据的操作或加工，应在服务需求方指定的设备上进行；		是
				d）应制定文档管理制度，包括服务机构人员在服务文档管理中的相关职责、档案借阅、保管直至销毁的各项规定等；		/
				e）在服务过程中获取的数据只能用于维护服务需求方关键信息基础设施安全的需要，不得用于其他用途。		是
	质量管理	管理体系建立	7%	a）应建立、实施和维护符合关键信息基础设施安全服务工作需要的文件化的管理体系，确保服务机构各级人员能够理解和执行，并获得信息技术服务管理体系及相关领域质量管理体系认证资质；	3	是
				b）应制定相应的质量目标，不断提升自身的检测评估质量和管理水平；		/
				c）应指定一名质量主管，明确其质量保证的职责；质量主管不应受可能有损工作质量的影响或利益冲突，并有权直接与服务机构管理层沟通。		/
		管理体系维护		a）应保证管理体系的有效运行，发现问题及时反馈并采取纠正措施，确保其有效性；	3	/
				b）应严格遵守申诉、投诉及争议处理制度，并应记录采取的措施；		/
				c）应建立并实施内部管理体系审核和反馈处理机制，以验证管理体系的符合性及有效性，确保在管理体系运行过程中发现的问题及时得到解决；执行审核的人员应独立于被审核部门。		/
		质量监督		a）服务机构应指定监督员对全体服务人员开展监督，监督内容包括现场安全服务活动、服务过程规范性和交付成果的规范性、准确性等。	1	是
	保密管理		3%	a）应根据国家有关保密规定制定保密管理制度，制度中应明确保密对象的范围、人员保密职责和义务、服务过程保密管理各项措施与要求、奖惩机制、离岗后的脱密期限等内容，确保服务需求方提供的资料、安全服务活动生成的数据和记录、安全服务交付成果等所有服务资料安全；	4	是
				b）应指派安全服务保密工作负责人，并明确安全服务各岗位保密要求；		是
				c）应与全体服务人员签订保密责任书，规定其应当履行的保密义务和承担的法律责任，定期对服务人员进行保密培训和考核；		是
				d）服务机构和服务人员应保守在安全服务活动中知悉的国家秘密、工作秘密、商业秘密、个人隐私等。		是
	教育培训		3%	a）应建立教育培训制度，包括培训计划的制定、培训工作的实施、培训的考核与上岗以及人员培训档案建立等内容和要求；	4	/

安全服务能力			权重	合规项指标描述	合规项数量	必要项标识
				b）应定期对全员开展安全意识培训；应根据服务人员的工作岗位职责和培训需求，制定详细和有针对性的培训计划，对服务人员进行专业培训并进行岗位培训、考核和评定，并保存培训和考核记录；		是
				c）应安排具有 2 年以上网络安全工作经验、具有安全服务项目经历的专家作为讲师进行培训；		/
				d）服务人员应参加并通过服务机构安排的各类培训，获得行业认可的安全服务领域专业资质证书，每年的培训时长累计不少于 40 学时，其中安全保密培训不少于 8 学时。		是
	服务可持续性		3%	a）服务终止后，可能对服务需求方系统、业务和数据等造成影响的，应在服务期限到期前向服务需求方告知；	4	/
				b）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服务机构移交相关的资料、账号、证件和令牌等；		/
				c）如确有无法提供持续服务的情况，应提前向服务需求方告知相关情况，并提出服务需求方认可的替代或交接方案，以保障服务需求方业务的持续性；		是
				d）涉及服务机构更换的，服务机构应确保网络安全服务工作顺利交接后才可退出服务。		是
	可持续性发展		2%	a）应根据自身情况制定战略规划，通过不断的投入保证自身的持续建设和发展；	3	/
				b）应定期对管理体系进行评审并持续改进，不断提高管理要求；设定中、远期目标，通过目标的实现，逐步提升质量管理能力；		/
				c）应跟踪国内外新技术、新应用的发展，通过专项课题研究和实践，确保服务能力与当前的技术发展和业务发展的同步性和先进性。		/
	服务机构行为规范性		5%	a）影响服务需求方关键业务和信息系统正常运行，危害服务需求方关键业务和信息系统安全；	6	是
				b）故意隐瞒服务过程中发现的安全问题，或者在服务过程中弄虚作假，未如实提供安全服务交付成果；		是
				c）非授权占有、使用和安全服务相关资料及数据文件；		是
				d）分包或转包安全服务项目；		是
				e）限定服务需求方购买、使用其指定的网络安全产品；		是
				f）其他危害国家安全、社会秩序、公共利益以及服务需求方利益的活动。		是
安全服务供给	安全咨询	安全规划咨询	30%	a）应在近 3 年内具有不少于 3 个安全规划咨询服务案例；	7	/
				b）应获得信息安全管理体系认证资质和信息安全风险评估二级及以上服务资质，或同级别认证资质；		是
				c）具有 5 年以上网络安全从业经验，且参与过 2 个以上安全规划咨询服务项目的服务人员不少于 2 人；		/

安全服务能力			权重	合规项指标描述	合规项数量	必要项标识
能力				d）具有获得 CISP 认证或同级别认证的服务人员不少于 2 人；		是
				e）服务人员掌握 GB/T 42446 规定的网络安全管理类人员相关的知识和技能要求，熟悉关键信息基础设施安全保护相关法律、行政法规和标准规范；		/
				f）具备支撑开展网络安全前瞻性技术研究的实验条件；		/
				g）具备以服务需求方实际需求为导向，提供定制化、可操作的具有全面性和前瞻性的安全规划或计划方案的能力，具备每年开展不少于 1 个安全规划咨询服务项目的实施能力。		/
		安全设计咨询		a）应在近 3 年内具有不少于 3 个安全设计咨询服务项目实施经验；	7	/
				b）应获得信息安全管理体系认证资质和信息安全风险评估二级及以上服务资质，或同级别认证资质；		是
				c）具有 5 年以上网络安全从业经验，且参与过 2 个以上安全设计咨询服务项目的服务人员不少于 2 人；		/
				d）具有获得 CISP 认证或同级别认证的服务人员不少于 2 人；		是
				e）服务人员掌握 GB/T 42446 规定的网络安全管理类人员相关的知识和技能要求，熟悉关键信息基础设施安全保护相关法律、行政法规和标准规范；		/
				f）具备支撑开展网络安全前瞻性技术研究的实验条件；		/
				g）具备开展安全框架、安全策略、安全技术体系结构、安全管理体系结构等方面的设计能力，具备每年开展不少于 1 个安全设计咨询服务项目的实施能力。		/
		安全管理体系咨询		a）应在近 3 年内具有不少于 3 个安全管理体系咨询服务项目实施经验；	6	/
				b）应获得信息安全管理体系认证资质和信息安全风险评估二级及以上服务资质，或同级别认证资质；		是
				c）具有 5 年以上网络安全从业经验，且参与过 2 个以上安全管理体系咨询服务项目的服务人员不少于 2 人；		/
				d）具有获得 CISP 认证或同级别认证的服务人员不少于 2 人；		是
				e）服务人员掌握 GB/T 42446 规定的网络安全管理类人员相关的知识和技能要求，熟悉 GB/T 22080、GB/T 38631 相关安全管理体系要求，熟悉关键信息基础设施安全保护相关法律、行政法规和标准规范；		/
				f）具备安全管理风险评估，以及安全管理制度和安全策略方案设计能力，具备每年开展不少于 1 个安全管理体系咨询服务项目的实施能力。		/
		数据安全		a）应在近 3 年内具有不少于 3 个数据安全咨询服务项目实施经验；	7	/
				b）应获得信息安全管理体系认证资质和信息安全风险评估二级及以上服务资质，或同级别认证资质；		是

安全服务能力			权重	合规项指标描述	合规项数量	必要项标识
		咨询		c）具有 5 年以上网络安全从业经验，且参与过 2 个以上数据安全咨询服务项目的服务人员不少于 2 人；		/
				d）具有获得 CISP 认证或同级别认证的服务人员不少于 2 人；		是
				e）服务人员掌握 GB/T 42446 规定的网络安全管理类、网络安全建设类人员相关的知识和技能要求，熟悉数据安全保护相关法律、行政法规，GB/T 41479、GB/T 35274、GB/T 37988、GB/T 37973、GB/T 39477 及其他相关标准规范；		
				f）具有数据安全评估、风险评估等服务工具；		是
				g）具备提供覆盖数据全生命周期的安全服务的能力，包括数据分类分级、数据脱敏、数据加密、数据泄露防护等，具备每年开展不少于 1 个数据安全咨询服务项目的实施能力。		/
		密码使用管理咨询		a）应在近 3 年内具有不少于 1 个商用密码应用安全性评估服务项目实施经验；	7	/
				b）应通过国家密码管理部门组织的商用密码检测机构（商用密码应用安全性评估业务）资质审查；		/
				c）具有 5 年以上网络安全从业经验，且参与过 1 个以上商用密码应用安全性评估服务项目的服务人员不少于 2 人；		/
				d）具有获得密码技术应用员职业资格，并通过国家密码管理部门组织的商用密码应用安全性评估从业人员考核的服务人员不少于 2 人；		/
				e）服务人员掌握 GB/T 42446 规定的网络安全建设类人员相关的知识和技能要求，熟悉密码相关法律、行政法规，GB/T 39786、GB/T 43207 及其他相关标准规范，密码学理论基础扎实，熟悉各种密码算法、协议和标准；		/
				f）服务过程及解决方案中所涉及的商用密码技术、产品和服务应符合国家密码管理有关要求；		是
				g）具备提供覆盖密码生成、存储、分发、使用、销毁全生命周期的咨询服务能力，具备每年开展不少于 1 个密码使用管理咨询服务项目的实施能力。		/
		网络安全等级保护咨询		a）应在近 3 年内具有不少于 3 个网络安全等级保护咨询服务项目实施经验；	6	/
				b）应获得网络安全等级测评与检测评估机构服务认证资质或同级别认证资质；		/
				c）具有 5 年以上网络安全从业经验，且参与过 2 个以上网络安全等级保护咨询服务项目的服务人员不少于 2 人；		/
				d）具有网络安全等级保护高级测评师不少于 1 人；		/

安全服务能力			权重	合规项指标描述	合规项数量	必要项标识
				e）服务人员掌握 GB/T 42446 规定的网络安全建设类人员相关的知识和技能要求，熟悉网络安全等级保护相关法律、行政法规和 GB/T 22239、GB/T 25070 等标准规范；		/
				f）具备提供覆盖信息系统定级、备案、建设整改、等级测评、监督检查全流程的咨询服务能力，具备每年开展不少于 1 个网络安全等级保护咨询服务项目的实施能力。		/
		安全工程监理		a）应在近 3 年内具有不少于 3 个信息安全工程监理服务项目实施经验；	6	/
				b）应获得信息安全管理体系认证资质；		是
				c）具有 3 年以上信息安全工程监理服务经验的服务人员不少于 2 人；		/
				d）具有获得 CISP 认证或同级别认证的服务人员不少于 2 人；		是
				e）服务人员掌握 GB/T 42446 规定的网络安全建设类人员相关的知识和技能要求；		/
				f）具备提供覆盖项目准备阶段、实施阶段和验收阶段等全过程的安全工程监理服务能力，具备每年开展不少于 1 个安全工程监理服务项目的实施能力。		/
	教育培训	网络安全意识教育	30%	a）应在近 3 年内具有不少于 1 个网络安全意识教育服务项目实施经验；	4	/
				b）具有获得 CISP 认证或同等资质认证的服务人员不少于 2 人；		是
				c）服务人员掌握 GB/T 42446 规定的网络安全科研教育类人员相关的知识和技能要求；		/
				d）具有针对不同参训人员特点和需求的网络安全意识教育课程，支持通过理论授课、网络安全事件案例警示教育等多种方式提升参训人员的网络安全意识和知识水平，具备每年开展不少于 1 个网络安全意识教育服务项目的实施能力。		/
		网络安全合规培训		a）应在近 3 年内具有不少于 1 个网络安全合规培训服务项目实施经验；	5	/
				b）具有 5 年以上网络安全从业经验，且熟悉关键信息基础设施安全保护相关法律、行政法规和标准规范的服务人员不少于 2 人；		/
				c）具有获得 CISP 认证或同等资质认证的服务人员不少于 2 人；		是
				d）服务人员掌握 GB/T 42446 规定的网络安全科研教育类人员相关的知识和技能要求；		/
				e）具有关键信息基础设施安全保护相关法律、行政法规和标准规范解读和培训相关课程，具备每年开展不少于 1 个网络安全合规培训服务项目的实施能力。		/
		网络		a）应在近 3 年内具有不少于 1 个网络安全技术培训服务项目实施经验；	5	/

安全服务能力			权重	合规项指标描述	合规项数量	必要项标识
		安全技术培训		b）具有网络攻防实战项目经历或 5 年以上网络安全从业经验，且熟悉关键信息基础设施安全保护相关法律、行政法规和标准规范的服务人员不少于 2 人；		/
				c）具有获得 CISP 认证或同等资质认证的服务人员不少于 2 人；		是
				d）服务人员掌握 GB/T 42446 规定的网络安全科研教育类人员相关的知识和技能要求；		/
				e）具有网络安全管理体系、风险管理、安全策略、数据安全和隐私保护、供应链管理等基本概念和方法，以及网络安全技术基础、高级网络安全技术、新技术安全防护、行业最佳实践和成功案例等相关课程，具备每年开展不少于 1 个网络安全技术培训服务项目的实施能力。		/
		网络安全技能培训		a）应在近 3 年内具有不少于 1 个网络安全技能培训服务项目实施经验；	6	/
				b）具有网络攻防实战项目经历，熟练使用网络安全产品和掌握操作系统、网络设备的安全配置方法的服务人员不少于 2 人；		/
				c）具有获得 CISP 认证或同等资质认证的服务人员不少于 2 人；		是
				d）服务人员掌握 GB/T 42446 规定的网络安全科研教育类人员相关的知识和技能要求；		/
				e）具有可以进行技能培训的模拟仿真环境或实训平台；		是
				f）具有网络安全实战化知识和技术、实战训练等课程，具备每年开展不少于 1 个网络安全技能培训服务项目的实施能力。		/
	设计开发	安全系统设计	30%	a）从事网络安全服务 5 年以上，从事安全系统设计服务不少于 3 年，应在近 3 年内具有不少于 2 个安全系统设计服务项目实施经验；	6	/
				b）应获得软件安全开发二级及以上服务资质或同级别认证资质，并通过 CMMI3 及以上级别认证；		是
				c）具有 5 年以上网络安全从业经验，且参与过 2 个以上安全系统设计服务项目的服务人员不少于 2 人；		/
				d）具有获得 CISP 认证或同级别认证的服务人员不少于 2 人；		是
				e）服务人员掌握 GB/T 42446 规定的网络安全建设类人员相关的知识和技能要求，熟悉关键信息基础设施安全保护相关法律、行政法规和标准规范；		/
				f）具备按照服务需求方应用环境特性和实际需求提出安全防护设计要求的能力，具备每年开展不少于 1 个安全系统设计服务项目的实施能力。		/
		安全开发		a）从事网络安全服务 5 年以上，从事安全开发服务不少于 3 年，应在近 3 年内具有不少于 2 个安全开发服务项目实施经验；	9	/

安全服务能力			权重	合规项指标描述	合规项数量	必要项标识
				b）应获得软件安全开发二级及以上服务资质或同级别认证资质，并通过 CMMI3 及以上级别认证；		是
				c）具有 3 年以上安全开发经验，且参与过 2 个以上安全系统设计服务项目的服务人员不少于 2 人；		/
				d）具有安全开发人员不少于 15 人；		是
				e）服务人员掌握 GB/T 42446 规定的网络安全建设类人员相关的知识和技能要求，熟悉关键信息基础设施安全保护相关法律、行政法规和标准规范；		/
				f）具备在需求分析、设计、编码、测试和部署等环节嵌入安全控制措施的能力，管控开发全过程安全；		/
				g）如果在服务过程中确需引入第三方开发机构的，第三方机构应满足安全开发服务对应的资质和人员要求；如果在服务过程中引入第三方组件或者开源代码，应征得服务需求方同意后，并通过代码审计、漏洞扫描等方式排查第三方组件或者开源代码安全风险可控后，方可引入；服务人员应详细记录第三方组件或者开源代码来源等信息，在服务交付时一并提供给服务需求方；		是
				h）开发的网络安全系统或产品应能通过国家有关部门或者独立第三方的安全评估与检测；		/
				i）具备按照服务需求方特定的安全需求和安全设计要求开发网络安全系统或产品的能力，具备每年开展不少于 1 个安全开发服务项目的实施能力。		/
	安全防护	资产探测识别	30%	a）应在近 3 年内具有不少于 3 个资产探测识别服务项目实施经验；	7	/
				b）应至少获得信息系统安全运维二级及以上服务资质、网络安全审计二级及以上服务资质、信息安全风险评估二级及以上服务资质中的 1 项，或同级别认证资质；		是
				c）具有熟练使用资产探测识别工具，具备 3 年以上网络安全从业经验，且参与过 3 个以上资产探测识别项目的服务人员不少于 2 人；		/
				d）具有获得 CISP 认证或同级别认证的服务人员不少于 2 人；		是
				e）服务人员掌握 GB/T 42446 规定的网络安全建设类人员相关的知识和技能要求，掌握 GB/T 20984 规定的资产识别方法，熟悉关键信息基础设施安全保护相关法律、行政法规和标准规范；		/
				f）具有自主知识产权的资产探测识别工具，具有资产信息指纹特征库，能够利用工具自动获取网络资产信息，包括服务器、计算机终端、移动设备、物联网设备、存储设备、网络设备、安全设备等；		/
				g）具备利用资产探测技术识别服务需求方关键业务链所依赖的网络、系统、数据、服务和其他类资产的能力，具备每年开展不少于 1 个资产探测识别服务项目的实施能力。		/
		暴露		a）应在近 3 年内具有不少于 3 个暴露面检测服务项目实施经验；	7	/

安全服务能力			权重	合规项指标描述	合规项数量	必要项标识
		面检测		b）应至少获得信息系统安全运维二级及以上服务资质、网络安全审计二级及以上服务资质、信息安全风险评估二级及以上服务资质中的 1 项，或同级别认证资质；		是
				c）具有熟练使用和配置暴露面检测工具，具备 3 年以上网络安全从业经验，且参与过 3 个以上暴露面检测服务项目的服务人员不少于 2 人；		/
				d）具有获得 CISP 认证或同级别认证的服务人员不少于 2 人；		是
				e）服务人员掌握 GB/T 42446 规定的网络安全运营类人员相关的知识和技能要求，熟悉关键信息基础设施安全保护相关法律、行政法规和标准规范；		
				f）具备自主知识产权的暴露面检测工具；		/
				g）具备对暴露在互联网的服务、域名、IP、端口等数字资产暴露面进行发现和识别，持续监测重要网站系统异常情况，如网页篡改、敏感词、网站挂马、黑链等的能力，具备每年开展不少于 1 个暴露面检测服务项目的实施能力。		/
		安全集成		a）应在近 3 年内具有不少于 3 个安全集成服务项目实施经验；	6	/
				b）应获得信息系统安全集成二级及以上服务资质或同级别认证资质；		是
				c）具有 3 年以上安全集成服务经验，且参与过 3 个以上安全集成服务项目的服务人员不少于 10 人；		/
				d）具有获得 CISP 认证或同级别认证的服务人员不少于 3 人；		是
				e）服务人员掌握 GB/T 42446 规定的网络安全建设类人员相关的知识和技能要求，熟悉关键信息基础设施安全保护相关法律、行政法规和标准规范；		/
				f）具备对服务需求方关键信息基础设施安全保护现状、差距与需求进行分析，设计整体解决方案的能力，具备每年开展不少于 1 个安全集成服务项目的实施能力。		/
		基线核查		a）应在近 3 年内具有不少于 3 个基线核查服务项目实施经验；	7	/
				b）应至少获得信息系统安全运维二级及以上服务资质、网络安全审计二级及以上服务资质、信息安全风险评估二级及以上服务资质中的 1 项，或同级别认证资质；		是
				c）具有 5 年以上网络安全从业经验、3 年以上基线核查服务经验，且参与过 3 个以上基线核查服务项目的服务人员不少于 3 人；		/
				d）具有获得 CISP 认证或同级别认证的服务人员不少于 3 人；		是

安全服务能力			权重	合规项指标描述	合规项数量	必要项标识
				e）服务人员掌握 GB/T 42446 规定的网络安全运营类人员相关的知识和技能要求，熟悉关键信息基础设施安全保护相关法律、行政法规和标准规范；		/
				f）具备自主知识产权的基线核查工具；		/
				g）具备使用自动化基线核查工具进行基线核查并开展人工抽查复核的能力，能够定期、自动地进行核查和差异分析并生成详细的报告，识别重要服务器、操作系统、数据库、中间件、存储设备、网络设备、安全设备和系统等实际配置与基线标准之间的偏差，发现异常时及时告警，提供改进建议；具备详细记录和追溯能力，支持事后审计和问题定位；具备每年开展不少于 1 个基线核查服务项目的实施能力。		/
		安全加固		a）应在近 3 年内具有不少于 3 个安全加固服务项目实施经验；	6	/
				b）应至少获得信息系统安全运维二级及以上服务资质、网络安全审计二级及以上服务资质、信息安全风险评估二级及以上服务资质中的 1 项，或同级别认证资质；		是
				c）具有 5 年以上网络安全从业经验、3 年以上安全加固服务经验，且参与过 3 个以上安全加固服务项目的服务人员不少于 3 人；		/
				d）具有获得 CISP 认证或同级别认证的服务人员不少于 3 人；		是
				e）服务人员掌握 GB/T 42446 规定的网络安全运营类人员相关的知识和技能要求，熟悉关键信息基础设施安全保护相关法律、行政法规和标准规范；		/
				f）具备对服务器、操作系统、数据库、中间件、存储设备、网络设备、安全设备和系统等的脆弱性进行分析和加固的能力，具备每年开展不少于 1 个安全加固服务项目的实施能力。		/
		安全运维		a）应在近 3 年内具有不少于 3 个安全运维服务项目实施经验；	6	/
				b）应获得信息系统安全运维二级及以上服务资质或同级别认证资质；		是
				c）具有 5 年以上网络安全从业经验、3 年以上安全运维服务经验，掌握操作系统、数据库、中间件、存储设备、网络设备、安全设备和系统等功能及原理，且参与过 3 个以上安全运维服务项目的服务人员不少于 3 人；		/
				d）具有获得 CISP 认证或同级别认证的服务人员不少于 3 人；		是
				e）服务人员掌握 GB/T 42446 规定的网络安全运营类人员相关的知识和技能要求，熟悉关键信息基础设施安全保护相关法律、行政法规和标准规范；		/

安全服务能力			权重	合规项指标描述	合规项数量	必要项标识
				f）具备开展应用系统、中间件、数据库、操作系统、服务器、存储设备、网络设备、安全设备和系统等的管理、维护和安全防护，维护网络及业务系统安全运行的能力，具备每年开展不少于 1 个安全运维服务项目的实施能力。		/
		源代码安全检测		a）应在近 3 年内具有不少于 3 个源代码安全检测服务项目实施经验；	7	/
				b）应至少获得信息系统安全运维二级及以上服务资质、网络安全审计二级及以上服务资质、信息安全风险评估二级及以上服务资质中的 1 项，或同级别认证资质；		是
				c）具有 5 年以上网络安全从业经验、3 年以上源代码安全检测服务经验，且参与过 3 个以上源代码安全检测服务项目的服务人员不少于 3 人；		/
				d）具有获得 CISP 认证或同级别认证的服务人员不少于 3 人；		是
				e）服务人员掌握 GB/T 42446 规定的网络安全建设类人员相关的知识和技能要求，熟悉关键信息基础设施安全保护相关法律、行政法规和标准规范；		/
				f）具有源代码安全检测工具；		/
				g）具备对软件源代码分析识别安全漏洞或缺陷的能力，具备每年开展不少于 1 个源代码安全检测服务项目的实施能力。		/
		防护有效性验证		a）应在近 3 年内具有不少于 3 个防护有效性验证服务项目实施经验；	7	/
				b）应至少获得信息系统安全运维二级及以上服务资质、网络安全审计二级及以上服务资质、信息安全风险评估二级及以上服务资质中的 1 项，或同级别认证资质；		是
				c）具有 5 年以上网络安全从业经验、1 年以上防护有效性验证服务经验，掌握安全测试和评估方法、渗透测试方法和技术、网络攻防技术等，掌握常见安全漏洞及利用方法，且参与过 1 个以上防护有效性验证服务项目的服务人员不少于 2 人；		/
				d）具有获得 CISP 认证或同级别认证的服务人员不少于 2 人；		是
				e）服务人员掌握 GB/T 42446 规定的网络安全运营类人员相关的知识和技能要求，熟悉关键信息基础设施安全保护相关法律、行政法规和标准规范；		/
				f）具有防护有效性验证工具；		/
				g）具备通过模拟攻击行为等方法，验证单点安全策略或安全防护体系是否能够有效阻止恶意攻击的能力，具备每年开展不少于 1 个防护有效性验证服务项目的实施能力。		/

安全服务能力			权重	合规项指标描述	合规项数量	必要项标识
		安全审计		a）应在近 3 年内具有不少于 3 个安全审计服务项目实施经验；	6	/
				b）应获得网络安全审计二级及以上服务资质或同级别认证资质；		是
				c）具有 5 年以上网络安全从业经验、3 年以上安全审计服务经验，掌握网络安全审计方法和技术，且参与过 3 个以上安全审计服务项目的服务人员不少于 2 人；		/
				d）具有获得 CISP-Auditor 认证或同级别认证的服务人员不少于 2 人；		/
				e）服务人员掌握 GB/T 42446 规定的网络安全审计和评估类人员相关的知识和技能要求，熟悉关键信息基础设施安全保护相关法律、行政法规和标准规范；		/
				f）具备评估和管理网络安全风险、出具网络安全审计报告的能力，具备每年开展不少于 1 个安全审计服务项目的实施能力。		/
	检测评估		/	服务机构开展检测评估服务应符合 T/CIIPA 00007 相关要求。	/	/
	技术对抗	攻防演练	30%	a）应在近 3 年内具有不少于 3 个攻防演练服务项目实施经验，近 3 年内没有出现因阶段性验收未通过或企业自身原因而废止的攻防演练服务项目；	7	/
				b）应获得信息系统安全运维二级及以上服务资质、信息安全应急处理二级及以上服务资质中的 1 项，或同级别认证资质；		是
				c）具有 5 年以上网络安全从业经验、3 年以上攻防演练服务经验，且参与过 3 个以上攻防演练服务项目的服务人员不少于 5 人；		/
				d）具有获得 CISP 认证或同级别认证的服务人员不少于 5 人；		是
				e）服务人员掌握 GB/T 42446 规定的网络安全建设类、网络安全审计和评估类人员相关的知识和技能要求，熟悉关键信息基础设施安全保护相关法律、行政法规和标准规范；		/
				f）具有攻防演练平台类工具；		/
				g）具备通过多场景攻防演练，全面测试验证服务需求方的防御措施和分析溯源措施有效性的能力，具备每年开展不少于 1 个攻防演练服务项目的实施能力。		/
		攻防竞赛		a）应在近 3 年内具有不少于 3 个攻防竞赛服务项目实施经验，近 3 年内没有出现因阶段性验收未通过或企业自身原因而废止的攻防竞赛服务项目；	6	/
				b）应获得信息系统安全运维二级及以上服务资质、信息安全应急处理二级及以上服务资质中的 1 项，或同级别认证资质；		是

安全服务能力			权重	合规项指标描述	合规项数量	必要项标识
				c）具有 5 年以上网络安全从业经验、3 年以上攻防竞赛服务经验，且参与过 3 个以上攻防竞赛服务项目的服务人员不少于 5 人；		/
				d）具有获得 CISP 认证或同级别认证的服务人员不少于 5 人；		是
				e）服务人员掌握 GB/T 42446 规定的网络安全审计和评估类人员相关的知识和技能要求，熟悉关键信息基础设施安全保护相关法律、行政法规和标准规范；		/
				f）具有攻防竞赛平台类工具；		/
				g）具备攻防竞赛赛制设计、赛题设计等能力，能够支撑开展赛前准备、现场部署、赛中运维、赛后收尾工作，具备每年开展不少于 1 个攻防竞赛服务项目的实施能力。		/
		威胁情报共享		a）应在近 3 年内具有不少于 3 个威胁情报共享服务项目实施经验；	7	/
				b）应获得信息安全风险评估二级及以上服务资质同级别认证资质；		是
				c）具有 5 年以上网络安全从业经验、3 年以上威胁情报共享服务经验，且参与过 3 个以上威胁情报共享服务项目的服务人员不少于 2 人；		/
				d）具有获得 CISP 认证或同级别认证的服务人员不少于 2 人；		是
				e）服务人员掌握 GB/T 42446 规定的网络安全运营类人员相关的知识和技能要求，熟悉《网络产品安全漏洞管理规定》等安全漏洞管理要求，熟悉关键信息基础设施安全保护相关法律、行政法规和标准规范；		/
				f）具备威胁情报获取途径和手段，建设维护百万级威胁情报库和管理技术手段；		/
				g）具备威胁情报收集、加工、分析、共享和处置的能力，每年开展不少于 1 个威胁情报共享服务项目的实施能力。		/
		安全监测		a）应在近 3 年内具有不少于 3 个安全监测服务项目实施经验，近 3 年内没有出现因阶段性验收未通过或企业自身原因而废止的安全监测服务项目；	8	/
				b）应获得信息系统安全运维二级及以上和信息安全应急处理二级及以上服务资质，或同级别认证资质；		是
				c）具有 5 年以上网络安全从业经验、3 年以上安全监测服务经验，熟练使用安全监测工具，熟悉各类网络安全事件的应急处置流程，且参与过 3 个以上安全监测服务项目的服务人员不少于 5 人；		/
				d）具有获得 CISP 认证或同级别认证的服务人员不少于 3 人；		是
				e）服务人员掌握 GB/T 42446 规定的网络安全运营类人员相关的知识和技能要求，熟悉关键信息基础设施安全保护相关法律、行政法规和标准规范；		/

安全服务能力			权重	合规项指标描述	合规项数量	必要项标识
				f）支持 5×8、7×8、7×24 小时等驻场值守，具备分钟级的网络安全事件发现和响应能力；		/
				g）服务过程中如果需要在服务需求方设备上安装服务所需的程序，应经服务需求方同意并在测试环境测试通过后方可部署；		/
				g）具备对被监测对象的运行状态、网络安全事件、日志与流量等数据收集、处理，分析研判整体安全态势，及时发现处置异常情况或行为的能力，具备每年开展不少于 1 个安全监测服务项目的实施能力。		/
		日志分析		a）应在近 3 年内具有不少于 3 个日志分析服务项目实施经验；	9	/
				b）应获得信息系统安全运维二级及以上和信息安全应急处理二级及以上服务资质，或同级别认证资质；		是
				c）具有 5 年以上网络安全从业经验、3 年以上日志分析服务经验，熟练使用日志分析工具，熟悉各类网络安全事件的应急处置流程，且参与过 3 个以上日志分析服务项目的服务人员不少于 3 人；		/
				d）具有获得 CISP 认证或同级别认证的服务人员不少于 3 人；		是
				e）服务人员掌握 GB/T 42446 规定的网络安全运营类人员相关的知识和技能要求，熟悉关键信息基础设施安全保护相关法律、行政法规和标准规范；		/
				f）具有自主知识产权的智能化分析引擎，建设维护智能检测模型和信息资源库等；		/
				g）开展日志分析服务所需日志宜通过服务需求方的日志审计系统或威胁检测与告警系统获取；		/
				h）如果需要在服务需求方设备上安装部署客户端或者日志采集程序，应征得服务需求方的同意，并在测试环境测试通过后方可安装部署；		是
				i）具备提供针对行业与场景的定制化日志分析解决方案能力，具备每年开展不少于 1 个日志分析服务项目的实施能力。		/
		安全预警		a）应在近 3 年内具有不少于 3 个安全预警服务项目实施经验；	7	/
				b）应获得信息系统安全运维二级及以上和信息安全应急处理二级及以上服务资质，或同级别认证资质；		是
				c）具有 5 年以上网络安全从业经验、3 年以上安全预警服务经验，熟悉各类网络安全事件的应急处置流程，且参与过 3 个以上安全预警服务项目的服务人员不少于 3 人；		/
				d）具有获得 CISP 认证或同级别认证的服务人员不少于 3 人；		是
				e）服务人员掌握 GB/T 42446 规定的网络安全运营类人员相关的知识和技能要求，熟悉关键信息基础设施安全保护相关法律、行政法规和标准规范；		/

安全服务能力			权重	合规项指标描述	合规项数量	必要项标识
				f）服务过程中应将威胁情报的研判、最新漏洞通告、网络告警事件研判结果等可能影响服务需求方安全的内容及时提交给服务需求方；		/
				g）具备综合分析研判网络安全态势形成内部安全预警信息、获取外部安全预警信息，协助服务需求方开展预警信息生成、发布、响应和解除的能力，具备每年开展不少于 1 个安全预警服务项目的实施能力。		/
		安全托管		a）应在近 3 年内具有不少于 3 个安全托管服务项目实施经验；	8	/
				b）应获得信息系统安全运维二级及以上和信息安全应急处理二级及以上服务资质，或同级别认证资质；		是
				c）具有 5 年以上网络安全从业经验、3 年以上安全托管服务经验，熟悉各类网络安全事件的应急处置流程，且参与过 3 个以上安全托管服务项目的服务人员不少于 15 人；		/
				d）具有获得 CISP 认证或同级别认证的服务人员不少于 5 人；		是
				e）服务人员掌握 GB/T 42446 规定的网络安全运营类人员相关的知识和技能要求，熟悉关键信息基础设施安全保护相关法律、行政法规和标准规范；		/
				f）对于通过自建安全运营中心提供安全托管服务的，应具备独立数据中心机房且满足网络安全等级保护三级及以上要求；		/
				g）支持 5×8、7×8、7×24 小时驻场值守，具备分钟级的网络安全事件发现和响应能力；		/
				h）具备识别服务需求方托管资产、及时发现响应安全威胁与异常事件、定期提供安全报告的能力，具备每年开展不少于 1 个安全托管服务项目的实施能力。		/
		重要时期安全保障		a）应在近 3 年内具有不少于 3 个国家重大活动、重大赛事、重要会议和网络安全实战演习期间等安全保障服务项目实施经验，近 3 年内没有出现因阶段性验收未通过或企业自身原因而废止的重要时期安全保障服务项目；	6	/
				b）应获得信息系统安全运维二级及以上和信息安全应急处理二级及以上服务资质，或同级别认证资质；		是
				c）具有 5 年以上网络安全从业经验、3 年以上重要活动或重大演习等安全保障服务经验，熟悉各类网络安全事件的应急处置流程，且参与过 3 个以上重要活动或重大演习等安全保障服务项目的服务人员不少于 5 人；		/
				d）具有获得 CISP 认证或同级别认证的服务人员不少于 3 人；		是
				e）服务人员掌握 GB/T 42446 规定的网络安全运营类人员相关的知识和技能要求，熟悉关键信息基础设施安全保护相关法律、行政法规和标准规范；		/

安全服务能力			权重	合规项指标描述	合规项数量	必要项标识
				f）具备重要时期对关键业务和信息系统进行全面的风险评估和威胁分析，制定并执行定制化安全加固方案，开展事前评估准备、事中监测防御、事后总结加固的能力，具备每年开展不少于 1 个重要时期安全保障服务项目的实施能力。		/
	应急处理	应急演练	30%	a）应在近 3 年内具有不少于 3 个应急演练服务项目实施经验；	6	/
				b）应获得信息系统安全运维二级及以上服务资质、信息安全应急处理二级及以上服务资质中的 1 项，或同级别认证资质；		是
				c）具有 5 年以上网络安全从业经验、3 年以上应急演练服务经验，且参与过 3 个以上应急演练服务项目的服务人员不少于 5 人；		/
				d）具有获得 CISP 认证或同级别认证的服务人员不少于 1 人；		是
				e）服务人员掌握 GB/T 42446 规定的网络安全运营类人员相关的知识和技能要求，熟悉《国家网络安全事件应急预案》等相关要求，熟悉关键信息基础设施安全保护相关法律、行政法规和标准规范；		/
				f）具备根据服务需求方的定制化需求与业务实际运行场景，帮助服务需求方制定、检验及完善应急预案，以及制定应急演练方案并协助实施的能力，具备每年开展不少于 1 个应急演练服务项目的实施能力。		/
		响应处置		a）应在近 3 年内具有不少于 3 个应急处理服务项目实施经验；	7	/
				b）应获得信息系统安全运维二级及以上服务资质、信息安全应急处理二级及以上服务资质中的 1 项，或同级别认证资质；		是
				c）具有 5 年以上网络安全从业经验、3 年以上应急处理服务经验，掌握应急分析溯源技能，且参与过 3 个以上应急处理服务项目的服务人员不少于 5 人；		/
				d）具有获得 CISP 认证或同级别认证的服务人员不少于 2 人；		是
				e）服务人员掌握 GB/T 42446 规定的网络安全运营类人员相关的知识和技能要求，熟悉关键信息基础设施安全保护相关法律、行政法规和标准规范；		/
				f）具备制定与执行应急处置策略的能力，能够根据网络安全事件的性质和影响，设计并实施针对性的应急处置方案，包括系统恢复、数据保护和威胁消除等措施，确保事件得到有效处理；		/
				f）应保证 7×24 小时的服务响应，具备网络安全事件发生时快速响应的能力，能够在事件检测后立即采取初步隔离措施，防止威胁扩散，并及时向服务需求方及相关安全管理机构报告，具备每年开展不少于 1 个响应处置服务项目的实施能力。		/

安全服务能力			权重	合规项指标描述	合规项数量	必要项标识
		恶意代码样本分析		a）应在近 3 年内具有不少于 3 个恶意代码样本分析服务项目实施经验；	7	/
				b）应获得信息系统安全运维二级及以上服务资质、信息安全应急处理二级及以上服务资质中的 1 项，或同级别认证资质；		是
				c）具有 5 年以上网络安全从业经验、3 年以上恶意代码样本分析服务经验，熟练使用动态分析工具、反汇编工具、PE 分析工具、逆向工程工具、恶意软件分类与识别工具、IOC 指标收集工具、样本提取工具等，且参与过 3 个以上恶意代码样本分析服务项目的服务人员不少于 3 人；		/
				d）具有获得 CISP 认证或同级别认证的服务人员不少于 2 人；		是
				e）服务人员掌握 GB/T 42446 规定的网络安全建设类人员相关的知识和技能要求，熟悉关键信息基础设施安全保护相关法律、行政法规和标准规范；		/
				f）具有恶意代码样本分析工具，建设维护亿级的恶意代码样本库和管理技术手段；		/
				g）具备开展恶意代码样本收集、样本动态分析、静态分析、交互性分析、样本分类、修复建议等工作的能力，具备每年开展不少于 1 个恶意代码样本分析服务项目的实施能力。		/
		溯源取证		a）应在近 3 年内具有不少于 3 个溯源取证服务项目实施经验；	7	/
				b）应获得信息安全应急处理二级及以上服务资质或同级别认证资质；		是
				c）具有 5 年以上网络安全从业经验、3 年以上溯源取证服务经验，且参与过 3 个以上溯源取证服务项目的服务人员不少于 5 人；		/
				d）具有获得 CISP 认证或同级别认证的服务人员不少于 2 人；		是
				e）服务人员掌握 GB/T 42446 规定的网络安全审计和评估类人员相关的知识和技能要求，熟悉关键信息基础设施安全保护相关法律、行政法规和标准规范；		/
				f）具有攻击溯源工具；		/
				g）具备提供自动化的应急分析及应急溯源服务，以及对电子证据进行提取、固定、恢复、分析的能力，具备每年开展不少于 1 个溯源取证服务项目的实施能力。		/