ICS 00.000
X XX

CIIPA

团　　体　　标　　准

T/CIIPA 00001-2024

关键信息基础设施安全分析识别能力要求与评价

Capability requirements and evaluation for security analysis and identification of critical information infrastructure

（征求意见）

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技术归口和解释。

本文件起草单位：国家工业信息安全发展研究中心、中关村华安关键信息基础设施安全保护联盟、中国电子科技集团公司第十五研究所、华为技术有限公司、中国信息通信研究院、合肥天帷信息安全技术有限公司、天津恒御科技有限公司、北京国信城研科学技术研究院、中国信息安全测评中心、中国电力科学研究院有限公司、工信部教育与考试中心、国家石油天然气管网集团有限公司油气调控中心、中国联合网络通信有限公司研究院、中国联合网络通信有限公司软件研究院、杭州中尔网络科技有限公司、中国矿业大学、北京工商大学、国家广播电视总局监管中心、上海计算机软件技术开发中心、北京知道创宇信息技术股份有限公司、南方电网数字电网集团信息通信科技有限公司、广州市盛通建设工程质量检测有限公司、中国交通通信信息中心、水利部信息中心、国家基础地理信息中心、中国人民财产保险股份有限公司、成都久信信息技术股份有限公司、深圳开源互联网安全技术有限公司、北京北信源软件股份有限公司、北京启明星辰信息安全技术有限公司、北方实验室（沈阳）股份有限公司、大唐科技研究总院、中国移动通信集团有限公司。

本文件主要起草人：刘志尧、逯瑶、周呈辉、刘赫、高松、修凤洲、徐彬、张少昌、肖凡、白云波、张毅、肖红阳、许亚玲、魏启超、葛方隽、林果园、高原、郭轲、刘浩然、吕峰、王琼、张博、周映、张磊、张震、陈树辉、杜渐 贺林佳、李恒、张建宇等。

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

关键信息基础设施是经济社会运行的神经中枢，是网络安全保护的重中之重。《中华人民共和国网络安全法》第三十一条规定，关键信息基础设施在网络安全等级保护制度的基础上，实行重点保护。随着我国信息化建设的迅猛推进，网络资产数量快速增长，网络架构日趋复杂，所承载的业务系统也日益增多。关键信息基础设施正朝着大平台、大系统、大数据的方向融合发展，但这种融合也带来了网络边界模糊、攻击面增加、业务逻辑繁杂和业务间依赖加深的问题，因此亟需开展关键信息基础设施安全分析识别工作，对关键信息基础设施的业务依赖性、关键资产和风险隐患进行分析识别。

关键信息基础设施安全分析识别是《GB/T 39204-2022 信息安全技术 关键信息基础设施安全保护要求》文件中提出的关键信息基础设施安全保护六个方面环节的首要环节，是开展安全防护、检测评估、监测预警、主动防御和事件处置等活动的基础。研究制定关键信息基础设施安全分析识别能力要求和评价，一是落实《中华人民共和国网络安全法》《关键信息基础设施安全保护条例》《GB/T 39204-2022 信息安全技术 关键信息基础设施安全保护要求》等法律法规及政策标准中关于关键信息基础设施安全分析识别的要求，建立一套综合性的关键信息基础设施安全分析识别机制；二是规范关键信息基础设施安全分析识别的原则、内容、范畴等，为有关部门、关键信息基础设施运营者、网络安全服务机构有效开展关键信息基础设施安全分析识别提供参考，进而提高关键信息基础设施安全保护水平；三是实现关键信息基础设施业务链、资产和风险的全面梳理，为安全防护、检测评估、监测预警、主动防御和事件处置等后续工作提供坚实的基础。

本文件参考国家标准、行业标准及国内网络安全服务机构能力建设与评定的相关内容，结合关键信息基础设施安全保护制度及分析识别实际工作的特点，对关键信息基础设施运营者、网络安全服务机构等开展分析识别活动提出能力要求和评价标准。

关键信息基础设施安全分析识别能力要求

1 范围

本文件确立了关键信息基础设施安全分析识别的总体要求和能力模型，规定了关键信息基础设施运营者和网络安全服务机构从事关键信息基础设施安全分析识别工作应具备的基本能力要求和评价方法。

本文件适用于指导关键信息基础设施运营者、网络安全服务机构开展关键信息基础设施安全分析识别活动，以及评价安全分析识别能力水平，也可为关键信息基础设施安全分析识别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

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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 25069 信息安全技术 术语

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 20984 信息安全技术 信息安全风险评估方法

3 术语和定义

GB/T 25069、GB/T 39204、GB/T 20984 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 critical information infrastructure

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的，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。

[来源：GB/T 39204-2022，3.1]

3.2 关键信息基础设施安全分析识别 security analysis and identification for critical information infrastructure

依据国家关键信息基础设施保护制度规定，按照有关管理规范和技术标准，围绕关键信息基础设施承载的关键业务，开展业务分析识别、资产分析识别和风险分析识别的活动。

3.3 关键业务链 critical business chain

组织的一个或多个相互关联的业务构成的关键业务流程。

[来源：GB/T 39204-2022，3.3]

3.4 业务分析识别 business analysis and identification

梳理关键业务链，识别关键业务和与其相关联的外部业务，分析关键业务对外部业务的依赖性和重要性，确定支撑关键业务的关键信息基础设施分布和运营情况的过程。

3.5 资产分析识别 asset analysis and identification

识别关键业务链所依赖的资产，建立网络、系统、数据、服务和其他类资产的资产清单，分析支撑业务的重要资产，确定资产防护的优先级，并根据资产的实际情况动态更新的过程。

3.6 风险分析识别 risk analysis and identification

识别关键业务链各环节的威胁、脆弱性，确定已有安全控制措施，分析主要风险点，确定风险处置的优先级，形成安全风险报告的过程。

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）

CVSS：通用漏洞评分系统（Common Vulnerability Scoring System）

BIA：业务影响评估（Business Impact Assessment）

5 分析识别总体要求

5.1 基本原则

开展关键信息基础设施安全分析识别应遵循以下基本原则：

a）全面性原则：应覆盖关键信息基础设施的所有关键点，包括业务链、资产和风险等，确保关键业务链、关键资产和主要风险的全面梳理。

b）合规性原则：应符合网络安全领域相关法律法规、标准规范等要求，采取合法、正当的方式开展分析识别活动，避免非授权开展关键信息基础设施安全分析识别。

c）规范性原则：应采用规范化的分析识别流程、方法和文档模板，通过标准化模板记录分析识别过程和结果，确保过程和结果可追溯、可复核。

d）保密性原则：在开展安全分析识别过程中，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。

e）独立性原则：应由独立的第三方机构或内部独立部门开展安全分析识别，避免利益冲突，确保分析识别结果的客观性。

f）客观性原则：应基于真实数据与事实进行分析识别，避免主观臆断，需通过实地调查、数据验证及多源信息交叉比对确保结论的可靠性。

g）风险管理原则：应采取必要的风险管控措施，保障安全分析识别过程的可控性，避免对相关组织和个人的安全造成不良影响。

h）持续更新原则：业务链、资产和风险都不是一成不变的，应根据实际情况持续更新，当关键信息基础设施发生改建、扩建或所有人变更等较大变化时，应重新开展分析识别。

5.2 分析识别技术措施

围绕关键信息基础设施所承载的关键业务，利用分析识别技术措施，支撑分析识别工作开展，实现分析识别的一体化管理，分析识别技术措施框架图如图 1 所示：

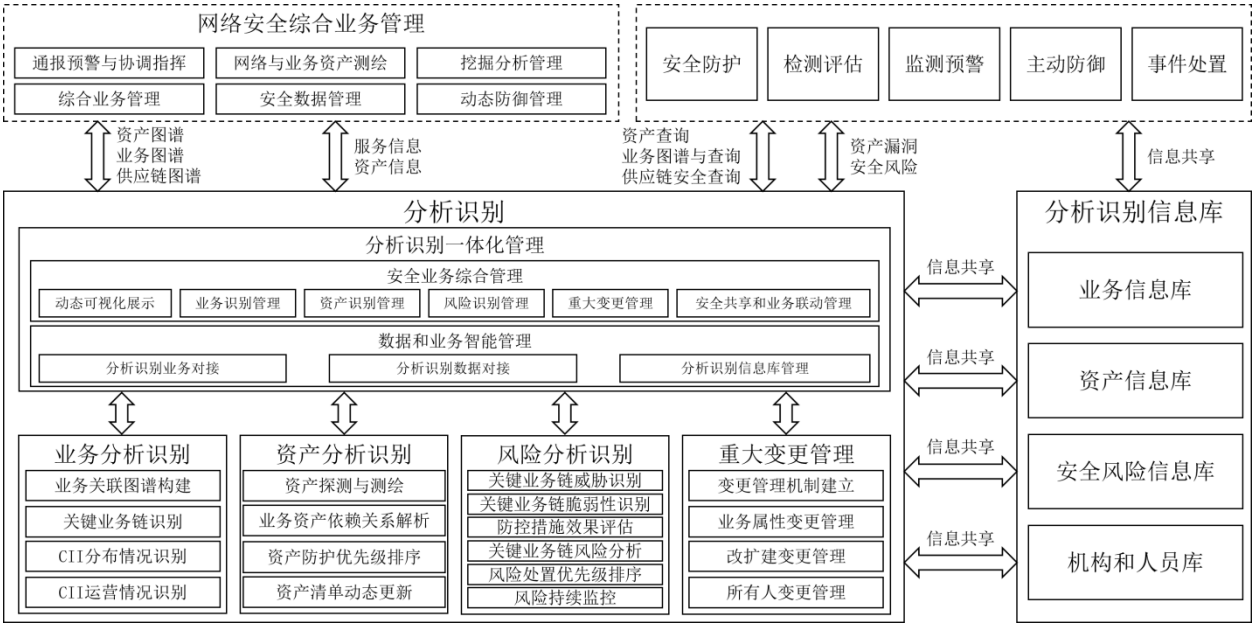

图 1 分析识别技术措施框架图

关键信息基础设施安全分析识别过程，利用分析识别技术措施，支撑分析识别工作开展，并实现分析识别业务的一体化管理，通过高效整合当前的分析识别技术资源以及探索采用的新型分析识别工具，为分析识别工作的全流程提供一站式管理服务。强调两大核心功能：

（1）安全业务综合管理。开展动态的可视化监控、精确的业务识别、资产识别、风险评估、重大变更跟踪、安全信息共享以及业务间的协同联动，实现全方位的安全业务管理。通过强化安全信息共享和业务协同机制，与“网络安全综合管控与应急指挥系统”实现数据互通和业务对接，进而在安全防护、检测评估、监测预警、主动防御以及事件处置等多个环节实现信息的共享和业务的联动。

（2）数据和业务智能管理。通过数据与业务的智能化集成，提升分析识别业务对接的效率、优化分析识别数据的对接流程，并建立健全的分析识别信息库管理体系，实现对业务接口、业务数据、资产数据、风险数据等各类信息的标准化和统一化处理。

5.3 业务分析识别过程

业务分析识别涵盖了多维度分析，包括业务关联图谱构建、关键业务链识别、CII 分布情况识别以及 CII 运营情况识别等。

5.3.1 业务关联图谱构建

业务关联图谱是一种以图形化方式展示 CII 中各项业务之间相互关系的模型。通过将业务抽象为节点，以连线表示业务之间的数据传输、流程衔接、服务调用等关联关系，直观地呈现出业务的整体架构、运行逻辑甚至是整个业务生态，能够帮助相关人员全面、清晰地理解业务的组成结构、交互方式以及依赖关系。业务关联图谱构建过程如下：

1、数据收集与调研

（1）与各业务部门进行沟通，收集各项业务的详细资料，包括业务功能描述、操作流程手册、业务报表等。

（2）与各业务部门进行调研，访谈相关业务人员，了解不同业务之间的数据交互、共享情况，以及业务流程中的上下游关系和协同工作机制。

（3）在 CII 中的关键网络节点处部署流量监测探针，收集关键网络节点处的流量数据。

2、数据整合与分析

（1）对收集的文档进行人工分析，形成业务清单，包括业务名称、功能、流转过程等内容；并绘制信息流图，展示各个业务系统之间的数据流转路径、数据流向及关键的通信协议等情况。

（2）借助流量分析设备对收集到的流量数据进行深入分析，对各业务流转过程进行验证确认，并与业务部门进行核实后更新业务清单信息和信息流图。

3、确定图谱元素

（1）设计将各项业务信息作为图谱的节点以清晰的图形表示，并在每个节点标注上该节点对应的业务名称，可为每个节点设定唯一标识符。

（2）设计不同样式（例如：实线、虚线）、颜色和箭头方向的线条来表示不同的关联关系，包括数据传输、业务流程衔接、服务调用等关系类型，并在每个线条标注该关系的说明信息。

4、构建图谱布局

（1）按照业务流程的先后顺序，从左到右或从上到下依次排列业务节点，使业务流程的走向清晰可见；对于存在并行或循环的业务流程，合理运用图形和线条进行展示，避免图谱过于复杂和混乱。

（2）按照业务功能相似、安全性相同等情况将所有业务划分为不同区域；在区域内按照业务关联紧密程度排列节点，区域之间用线条连接表示跨区域的业务关联。

以某电网公司的整体业务情况为例，构建业务关联图谱如图 2 所示：

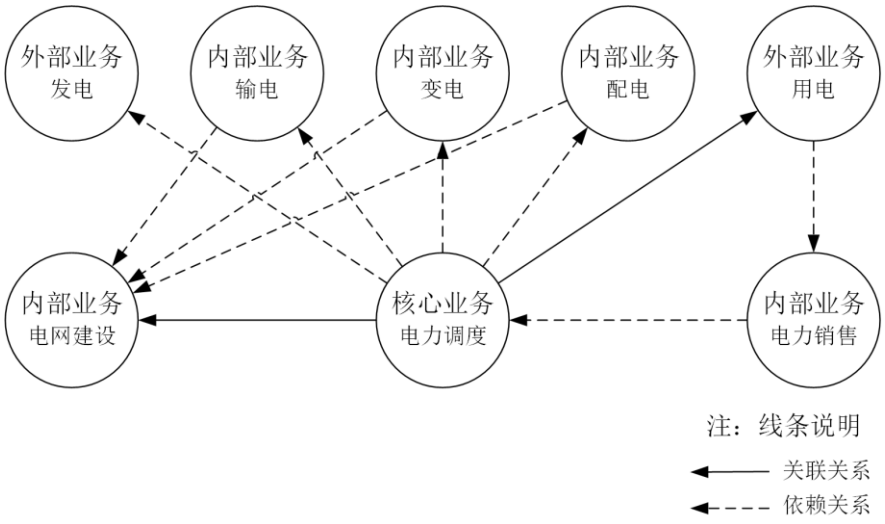

图 2 某电网公司业务关联图谱

5.3.2 关键业务链识别

关键业务链作为支持 CII 正常运行的一系列相互关联的业务流程和服务，一旦中断可能严重影响社会经济秩序或国家安全。因此需要识别出 CII 中至关重要的关键业务链条，从而确保关键业务链条在受到攻击或发生故障时能够得到及时响应与恢复。关键业务链识别过程如下：

1、关键业务识别

基于业务影响分析（BIA）对各业务流程进行重要性评估，可以从业务对企业影响、经济价值和战略重要性等方面的影响来评定优先级，再进行优先级排序，识别哪些流程对组织运营至关重要、一旦中断会对组织造成重大影响，确定为关键业务。

2、外部业务依赖性分析

（1）通过业务关联图谱，找出关键业务与外部业务的协作点，分析这些协作点在关键业务整个流程中是否作为输入点，从而确定关键业务是否依赖外部业务系统或服务提供服务。

（2）若关键业务依赖外部业务系统或服务提供服务，则深入分析关键业务对外部业务系统或服务的依赖程度，形成外部业务依赖性信息，包括外部业务名称、业务提供方名称、依赖程度、稳定性、替代方式等内容。

（3）还可以研究关键业务在整个行业产业链中的位置，分析其对上游业务的依赖性。

3、外部业务重要性分析

（1）通过业务关联图谱，找出关键业务与外部业务的协作点，分析这些协作点在关键业务整个流程中是否作为输出点，从而确定关键业务是否服务于外部业务系统或服务。

（2）若关键业务对外部业务系统或服务提供服务，则深入分析关键业务对外部业务系统或服务的重要程度，可以从服务范围、服务对象、服务能力、社会影响和经济损失等方面进行分析，形成外部业务重要性信息。

（3）还可以研究关键业务在整个行业产业链中的位置，分析其对下游业务的重要性。

4、关键业务链梳理

根据关键业务识别、外部业务依赖性分析、外部业务重要性分析的结果，明确关键业务链上的关键业务、其他业务以及相互关系，梳理出完整的关键业务链，形成关键业务链的图谱或记录文档。

5.3.3 CII 分布情况识别

关键信息基础设施分布情况识别是指对 CII 的物理位置分布、网络逻辑分布、行业领域分布等进行详细调查和记录，以便于后续的安全管理和应急响应。CII 分布情况识别过程如下：

1、物理位置分布

识别 CII 的物理位置分布情况，重点是数据中心、服务器机房或网络节点等的分布情况，明确其地理区域（如不同城市、国家或区域）。

2、业务逻辑分布

（1）根据整个业务关联图谱和网络拓扑结构，绘制网络拓扑图，标识出网络设备（如路由器、交换机、防火墙、负载均衡器等）的位置及其连接关系，网络拓扑应涵盖内网与外网、数据中心之间的网络链路、核心业务系统和互联网的连接等。

（2）识别 CII 的业务逻辑分布情况，重点是关键业务、关键网络节点的分布情况，明确其逻辑区域（如核心、接入、边界等）。

（3）分析信息流动路径，记录不同组件之间的数据流向，尤其是对于跨区、跨云的业务部署。

3、行业领域分布

（1）跨行业关联分布：识别 CII 在不同行业领域的分布情况，例如：电力、石油、天然气等能源行业的 CII 为多个其他行业提供能源供应保障，可能分布在其他行业合作伙伴和客户等多个节点。

（2）上下游产业分布：识别 CII 在产业链上下游中的分布情况，可能分布在供应商、合作伙伴和客户等多个节点。

5.3.4 CII 运营情况识别

关键信息基础设施运营情况识别是保障关键业务持续稳定运行的核心步骤。通过洞察 CII 的运行状态、性能表现、安全态势等运营情况，可以及时发现潜在的风险、优化资源配置。CII 运营情况识别过程如下文所示：

1、数据采集

要洞察 CII 的运营情况，需要全面、准确的数据支持。可以构建统一的数据采集平台，实现跨系统、跨平台的数据整合与关联，包括生产数据、运维数据、网络数据、安全数据等多维度信息的集成。通过数据仓库和大数据处理技术，对数据进行清洗、整理和分析，为后续洞察提供数据基础。

2、实时监控与告警

建立基于 IT 基础设施监控的业务管理系统，实现对 CII 状态的实时监控，直观展示业务的健康度、关键指标以及告警信息，使运维团队能够迅速响应潜在问题。同时将网络安全态势感知纳入 CII 运营情况识别体系，实时监测网络攻击、恶意入侵等安全事件，通过安全日志分析、流量监测等手段，及时发现并处置潜在的安全威胁，确保 CII 的网络安全。

a）运营状态监控：通过实时监控系统，收集和分析关键信息基础设施的运行数据，识别出设备、网络、应用等的健康状况；

b）异常行为检测：对关键信息基础设施的运营数据进行异常行为分析，及时发现潜在攻击流量或内部安全风险。

5.4 资产分析识别过程

在识别关键业务和业务链的基础上，深入分析识别关键业务链所依赖的各类资产，包括网络、系统和服务等，并建立与之相关的详细资产清单。根据资产的类别、重要性和对业务的支撑程度，对资产进行排序，确定其防护的优先级。通过采用资产探测与测绘技术，根据业务链所依赖资产的实时情况，动态更新资产清单。资产分析识别包括资产探测与测绘、业务资产依赖关系解析、资产防护优先级管理及资产清单动态更新等内容。

5.4.1 资产探测与测绘

资产探测与测绘是指通过一系列技术手段和方法，对目标区域或系统中的各类资产进行全面、细致的查找、识别、定位和信息收集，并以可视化或数据化的方式呈现出来的过程。资产探测与测绘过程如下：

1、准备工作

（1）收集信息：收集与目标资产相关的已有资料，如网络拓扑图、资产清单、系统文档等，为后续工作提供基础数据。

（2）选择工具和技术：根据目标资产的特点和探测需求，选择合适的探测工具和技术方法，如网络扫描工具、指纹提取工具、流量分析平台、地理信息系统（GIS）技术、数据库查询工具等。

2、资产探测

（1）通过资产指纹对比的技术手段实现网络设备组件的识别，识别信息包括设备类型、设备厂商、设备品牌、设备型号等属性；

（2）通过 IP 路径信息、路由器配置文件、BGP 路由表等数据还原得到网络拓扑结构，实现网络拓扑的还原与分析；

（3）通过应用指纹识别方式自动化识别 Web 服务器软件、Web 脚本语言、服务类型及相应版本型号等应用组件的属性；

（4）通过数据库管理工具、数据目录系统等，对组织内的数据资产进行梳理，包括数据库的结构、数据量、数据类型、数据所有者等信息。

3、资产测绘

（1）根据资产探测数据，绘制精确的资产地图，以可视化的方式展示资产的分布情况、关系结构等，如网络拓扑图、资产位置分布图、数据资产关系图等；

（2）基于资产探测数据，深入融合 DNS 信息、漏洞库、IP 地理信息库等资源，建立资产多层级的关联模型，推断网络资产的业务类型，实现业务识别和网络资产多维度画像；

(3)应建立关键业务链相关的网络、系统、数据、服务和其他类型的资产清单，从连通关系和逻辑关系的角度建立关键业务链实体之间多维度、多层次的拓扑结构图，为制定资产管理策略提供依据。

5.4.2 业务资产依赖关系解析

业务资产依赖关系解析是指通过一系列方法和技术，对业务流程中涉及的各种资产之间的相互依存、相互影响的关系进行识别、分析和明确的过程。业务资产依赖关系解析过程如下：

1、准备工作

（1）通过描绘各个环节、步骤、活动的输入、输出和关键节点确定进行业务流程建模；

（2）根据资产测绘得到的资产地图建立全面的资产清单。

2、依赖关系分析

（1）针对每个业务流程环节明确所依赖的具体资产实现业务流程与资产的映射关系；

（2）通过分析业务流程、系统架构、数据流动等手段识别出关键业务链和资产的依赖关系；

3、关系建模与可视化呈现

（1）建立依赖关系模型：根据分析结果，使用合适的建模方法和工具，建立业务资产依赖关系模型，以图形化或数据化的方式表示资产之间的依赖关系，例如使用有向图表示资产之间的依赖链路，节点表示资产，边表示依赖关系；

（2）可视化呈现：将建立的依赖关系模型通过可视化工具进行展示，如绘制业务资产依赖关系图、系统架构图、数据流程图等，使依赖关系更加直观、清晰，便于理解和沟通。

5.4.3 资产防护优先级排序

资产防护优先级排序是指根据资产的价值、重要性、面临的风险程度以及对业务的影响等因素，对组织内的各类资产进行综合评估，确定其在安全防护工作中的优先顺序，以便合理分配安全资源，集中力量对高优先级资产进行重点防护，最大限度地降低资产遭受威胁的可能性，保护组织的核心利益和业务连续性。资产防护优先级排序过程如下：

1、 资产分类

制定组织内部的资产分类方法，依据分类方法结合资产清单对资产进行分类整理，资产类别通常可划分为：信息系统、数据资源、通信网络，也可根据组织自身的资产特点自行定义分类标准。

2、资产重要性评估

（1）确定评估指标：建立资产价值评估指标体系，通常包括资产重要性、数据敏感性等方面，资产重要性可依据资产在保密性、完整性和可用性方面的综合评定等级确定；

（2）评估方法选择：采用合适的评估方法，可以根据自身的特点，选择对资产保密性、完整性和可用性最为重要的一个属性的赋值等级作为资产的最终赋值结果；也可以根据资产保密性、完整性和可用性的不同等级对其赋值，再进行加权计算得到资产的最终赋值结果，加权方法可根据组织的业务特点确定；

（3）重要性评估：按照确定的评估指标和方法，对各类资产进行重要性评估，计算最终赋值结果。

3、支撑业务的重要性评估

（1）制定组织内部的业务分类方法，依据分类方法对业务系统进行分类整理，业务分类方法通常包括：按业务实时性（实时业务、准实时业务、非实时业务）、按业务数据一致性要求（强一致性业务、弱一致性业务、无需一致性业务）、按业务风险（高风险业务、中风险业务、低风险业务）、按业务流量或负载（高并发业务、中等并发业务、低并发业务）；

（2）业务的重要性可根据业务的优先级、风险、性能需求等因素确定。业务重要性等级通常可划分为：核心业务、重要业务、普通业务，也可根据组织自身的资产特点自行定义。

4、资产防护优先级确认

（1）依据资产类别、资产重要性和支撑业务的重要性三方面细化评估关键指标，设定明确的评分标准和规则；

（2）根据评分标准和规则计算每一个资产的分数值，依据分数值进行排序，形成资产防护优先级清单。

5.4.4 资产清单动态更新

资产清单动态更新是指随着组织内外部环境的变化以及资产自身状态的改变，对记录组织各类资产信息的清单进行实时或定期的修改、补充和完善，以确保资产清单能够准确、全面地反映组织资产的最新情况，为资产的有效管理、决策制定以及风险防控等提供可靠依据。资产清单动态更新过程如下：

1、 建立资产变更监测机制

利用各种技术工具和管理手段对资产进行监测，资产管理软件、网络监控工具、系统日志分析工具等技术工具，定期的资产巡检、员工反馈机制等管理手段，通过这些工具和方法，及时发现资产的变化情况。

2、 资产定位

采用资产定位等技术手段，监控并追踪关键信息基础设施资产的位置和转移情况。

3、 动态更新

（1）采用自动机制识别关键信息基础设施中新增的非授权软件、硬件或固件组件，通过技术手段和资产管理工具根据关键业务链所依赖资产的实际情况进行动态调整，实现资产清单的及时动态更新。

（2）对资产的运行状态和使用情况进行跟踪，在资产发生变化时及时更新资产信息。在配置信息出现变化、接入新设备、移除旧设备等情况发生时，通过自动化管理工具感知变化。

5.5 风险分析识别过程

聚焦关键信息基础设施所承载的关键业务链，对其进行深入的风险分析识别，形成详细的安全风险报告。风险分析识别包括关键业务链风险识别、安全风险关联分析、风险处置优先级排序、风险持续监控以及防控措施效果评估等内容。

5.5.1 关键业务链威胁识别

关键业务链威胁识别旨在识别可能影响 CII 业务连续性、资产可用性、完整性和保密性的外在威胁。通过全面分析业务流程、信息系统架构和关键数据流向，确保所有可能影响关键业务稳定运行的威胁得到识别。关键业务链威胁识别过程如下：

1、分析威胁主体

（1）先根据威胁主体的属性进行分类，分为人为和环境两类；

（2）再根据威胁主体所具备的资源和影响程度进行分级，人为可以分为国家、组织团队和个人，环境则可以分为一般、较为严重和严重的自然灾害。

2、分析威胁动机

根据人为的威胁主体不同的动力和原因，将威胁动机分为恶意和非恶意，其中因为金钱利益、政治利益和名誉权利等进行攻击、破坏、窃取等行为的属于恶意，而因为好奇心、自负、无意的错误或遗漏等导致业务、资产产生影响的属于非恶意。

3、分析威胁时机

（1）当社会活动按照既定规则平稳运行、相对稳定，则处于普通时期，例如和平发展时期；

（2）当社会活动偏离既定规则、发生重大事件和显著变化，则处于特殊时期，例如战争时期、疫情时期；

（3）不以人的意志为转移、客观存在的必然现象，则属于自然规律，例如四季轮转、自然灾害。

4、分析威胁频率

根据组织、行业和区域有关的统计数据，结合经验对各种威胁出现的频率进行等级评定，威胁出现的频率越高，等级数值越大，从而得出不同的威胁频率等级。

5、分析威胁能力

根据组织和业务所处的地域和环境，结合不同的威胁来源所具备的资源和综合素质对威胁能力进行等级判定，威胁能力越强，等级数值越大，从而得出不同的威胁能力等级。

6、开展威胁赋值

基于威胁行为，根据上述得出的频率等级和能力等级，并结合威胁发生的不同时机对威胁频率进行调整，进行综合评价，得出不同评价等级，根据评价等级的高低为威胁赋值。

5.5.2 关键业务链脆弱性识别

关键业务链脆弱性识别旨在发现关键业务链内在可被威胁利用的薄弱点。关键业务链脆弱性识别过程如下：

1、技术层面脆弱性识别

通过配置核查、漏洞扫描、渗透测试等技术手段，分析关键业务链中存在的技术层面安全薄弱点。

2、管理层面脆弱性识别

通过人员访谈、文档查阅及现场核查等手段，分析关键业务链中存在的管理层面安全薄弱点。

5.5.3 防控措施效果评估

防控措施效果评估是指对 CII 中实施的各项安全防护措施的有效性进行综合评估的过程。防控措施效果评估过程如下：

1、梳理安全防护情况

梳理当前的安全防护措施，以及安全防护措施设置的访问控制策略、加密策略、审计策略等具体安全防护策略配置，形成安全防护措施清单和安全策略配置清单。

2、制定评估指标

从技术、管理和业务应用等多方面制定防控措施效果评估的指标。例如，技术方面考察系统漏洞数量、数据加密强度等，管理方面考察安全管理制度的完善性、人员安全培训的覆盖率等，业务应用方面考察系统的可用性、数据完整性、服务中断时间等。

3、选择评估方法

可以采用漏洞扫描、风险评估工具检测、人工检查、模拟攻击测试、问卷调查、访谈等方法。例如，通过模拟黑客攻击来测试系统的防御能力，或通过问卷调查了解员工对安全制度的知晓度。

4、开展评估分析

（1）合规性分析：检查关键信息基础设施的防控措施是否符合相关法律法规、行业标准和监管要求。如是否符合网络安全等级保护制度的要求。

（2）性能分析：根据收集的数据，分析系统的性能指标，评估防控措施对系统性能的影响。例如，分析加密措施是否导致系统响应时间过长，影响业务操作效率。

（3）效果对比分析：与历史数据或同行业类似设施的防控效果进行对比，评估自身防控措施的优势和不足。

5.5.4 关键业务链风险分析

关键业务链风险分析旨在通过识别、连接并分析不同安全事件之间的关联性或相关性，从而发现潜在的威胁、漏洞和风险趋势。这种分析方法不仅关注单一安全事件，而且将多个事件联系起来，形成对安全态势的整体感知。关键业务链风险分析过程如下：

1、风险识别

（1）在完成威胁识别、防控措施效果识别、脆弱性识别后，采用适当的方法与工具确定威胁利用脆弱性导致安全事件发生的可能性。

（2）综合安全事件所作用的关键业务链及其资产的重要程度、价值及脆弱性的严重程度，判断安全事件造成的损失和对组织的影响。可以参考行业内外类似业务链安全事件，利用沙盘推演可能的攻击模式及其对业务的潜在影响。

2、风险分类

将识别出的风险整理成风险清单，包括风险名称、描述、潜在影响、可能原因等。根据关键业务链各节点重要性、风险发生的可能性及产生的影响程度，将识别到的风险进行分类（如业务类、数据类风险、物理类风险等）。

5.5.5 风险处置优先级排序

风险处置优先级排序是指根据风险的严重程度、发生可能性、潜在影响等因素，对已识别的安全风险进行分类和优先级排序，以便合理分配资源，优化处置流程，确保最紧急和最重要的风险得到优先处理。风险处置优先级排序过程如下：

1、风险评估

对于已经识别到的风险进行风险评估，包括每个风险的潜在影响，包括对机密性、完整性和可用性的影响。确定风险暴露的范围和被攻击难易度，需要考虑暴露在互联网的设备、开放端口、外部依赖等客观因素。

2、风险量化

应用定量模型（如：CVSS 评分）或定性模型为每个风险打分，综合考虑其严重性、发生概率、影响范围等因素。根据量化得分或分类结果，进行风险的优先级排序，确保高风险项获得优先处置。

5.5.6 风险持续监控

风险持续监控是指通过技术手段、流程管理和人员协作，实时或周期性地对已识别的安全风险进行动态跟踪和状态更新，及时捕获风险变化及其对系统、业务的潜在影响，以便采取有效应对措施。网络安全风险管理是一个整体性工作，也是一个持续的流程。开展风险持续监控对于发现新的威胁和脆弱性至关重要。风险持续监控过程如下：

1、残余风险监控

对已识别的风险开展风险处置后，为确保安全措施的有效性，对关键业务链风险进行再评估，以判断实施安全措施后的风险是否已经降低到可接受的水平；若残余风险的结果仍处于不可接受的风险范围内，则考虑是否替代合适的安全措施或增加相应的安全措施。

2、新风险识别和监控

（1）通过各类网络安全监测和控制措施对 CII 关键节点进行实时监控，并结合威胁情报数据，更新威胁分析结果。

（2）通过漏洞扫描、漏洞挖掘等技术和工具定期对 CII 关键资产进行脆弱性评估，更新脆弱性分析结果。

（3）根据更新的威胁分析和脆弱性分析结果，重新对关键业务链风险进行评估，发现新风险，并针对新风险进行风险处置，确保新风险已降低到可接受的水平。

5.6 重大变更管理过程

关键信息基础设施的重大变更管理涵盖了多个方面，包括但不限于关键信息基础设施的大规模调整、业务属性的改变、改扩建变更以及所有人变更等。当这些关键要素发生显著变化时，例如网络拓扑结构的重大调整、关键业务链或关键业务属性的更改、业务服务范围的实质性扩展或缩减等，需要重新启动识别流程，确保对所有相关变更的全面了解和管理。

5.6.1 变更管理机制建立

变更管理机制建立是针对 CII 运行过程中涉及技术、流程、供应链等核心要素的变更行为，建立一套规范化的管理流程和风险防控体系，旨在确保变更实施后系统稳定性、数据安全性和业务连续性不受威胁，并符合国家安全及行业监管要求。变更管理机制建立过程如下：

1、 变更识别

通过监控系统和人工巡检等方式，收集关键信息基础设施的运行数据，与预设的基准数据进行对比，从而识别出变更的发生，及时了解和掌握所有可能影响 CII 安全和稳定运行的变更情况。

2、 变更分类分级标准

（1）基于在业务属性、技术、供应链、所有人等维度的变更情况制定 CII 变更分类规则，包括但不限于业务属性变更、改扩建变更、所有人变更等。

（2）基于业务影响程度（如可能导致核心业务中断、数据泄露风险）、风险等级（如国家安全威胁、经济损失规模）等多维度的变更影响分析制定 CII 变更分级规则，包括一般变更、较大变更和重大变更，明确重大变更的判定阈值。

3、 建立变更审批机制

（1）变更提出方通过标准化表单提交变更需求，包含变更目标、实施方案、预期影响及应急预案等内容，由 CII 运营单位安全部门进行初步合规性审查。

（2）CII 运营单位组织技术专家对变更方案的技术成熟性、兼容性等进行验证。

（3）不同级别的变更设置不同的审批流程，一般变更由业务部门负责人进行审批，较大变更由业务部门和安全部门负责人共同审批，重大变更由运营单位负责人进行审批，并向行业主管部门进行备案。

4、 实施变更

（1）在变更前完成关键数据的备份工作，准备详细的回滚方案和应急处置流程，以便在变更实施过程中发生问题及时恢复。

（2）按照审批通过的实施方案开展变更实施工作，一旦变更过程发生问题，根据回滚方案进行回退恢复，或根据应急处置流程进行处置。

5、 变更分析与应对

（1）在实施变更完成之后，组织专业人员对变更可能带来的风险进行详细分析，确定影响范围。

（2）根据变更分析结果，结合业务需求和战略目标，制定合理的变更应对决策，确保业务运行正常，安全风险可控。

（3）及时更新资产清单、业务图谱和风险清单等，确保相关信息的动态更新。

5.6.2 业务属性变更管理

业务属性变更管理是针对关键信息基础设施所承载的业务在功能、流程、服务水平等属性方面发生的变化进行管理的活动，以确保业务变更与基础设施的兼容性和协同性，保障业务的正常开展。业务属性变更管理过程如下：

1、 明确变更需求与目标

与变更的提出方及其他相关方进行充分沟通，了解变更的原因和期望达成的目标等信息，例如是由于业务服务对象、服务模式等原因导致的业务属性变更，还是因为组织经营方向或战略目标发生变化等，确保对变更的背景和意图有清晰的认识。

2、 业务流程梳理

对变更后的业务流程进行详细梳理，明确各个环节的输入、输出、处理逻辑和责任人，重新识别出关键业务节点和流程依赖关系。

3、 数据资产分析

确定业务属性变更对数据资产的影响，包括数据类型、数据量、数据存储位置、数据流向等方面的变化，评估数据安全风险。

4、 系统与应用评估

分析业务属性变更对相关信息系统和应用程序的功能、性能、接口等方面的影响，判断是否需要进行系统升级、改造或重新开发。

5、 关联关系识别

分析业务属性变更与关键信息基础设施中其他要素（如网络、设备、人员等）的关联关系，确定可能受到影响的范围和程度。

5.6.3 改扩建变更管理

改扩建变更管理是指对关键信息基础设施进行规模扩大、功能扩展或设施改造等活动的管理，旨在提升关键信息基础设施的性能、容量和功能，以满足业务增长和发展的需求。改扩建变更管理过程如下：

1、 明确变更需求与目标

与变更的提出方及其他相关方进行充分沟通，了解变更的原因和期望达成的目标等信息，例如是由于业务服务范围、服务对象等原因导致的改扩建，还是因为业务能力已无法满足当前需求等，确保对变更的背景和意图有清晰的认识。

2、 关键要素识别

明确改扩建涉及的关键要素，如关键设备、核心系统、重要数据接口、关键网络节点等，确定这些要素对整体关键信息基础设施的重要性和影响程度。

3、 变更分析

组织专业人员对改扩建可能带来的风险进行详细分析，包括技术风险（如新技术的兼容性问题）、安全风险（如施工过程中的数据泄露风险）、业务中断风险、环境风险等，确定影响范围。

5.6.4 所有人变更管理

所有人管理是指针对关键信息基础设施的所有权或控制权发生转移等情况进行的管理活动，包括所有权变更过程中的资产交接、信息转移、责任界定以及变更后的管理体系调整等。所有人变更管理过程如下：

明确变更需求与目标

与变更的所有人及其他相关方进行充分沟通，了解变更的原因和期望达成的目标等信息，例如是由于企业收购、重组等原因导致的所有权转移，还是为了引入新的战略投资者等，确保对变更的背景和意图有清晰的认识。

1、 变更分析

评估所有人变更可能带来的风险隐患，如数据安全风险、业务中断风险、合规风险等。例如，新所有人可能有不同的安全管理策略，可能导致数据泄露风险增加。

2、 合规性评估

依据国家法律法规、行业标准和监管要求，审查所有人变更是否符合相关规定，如金融行业对关键信息基础设施所有者的资质要求等。

6 分析识别能力模型

6.1 模型框架

关键信息基础设施分析识别能力模型如图 3 所示，包括 CII 运营者分析识别能力和网络安全服务机构分析识别能力；对应的关键信息基础设施分析识别能力评价模型如图 4 所示，包括 CII 运营者能力评价和网络安全服务机构能力评价。

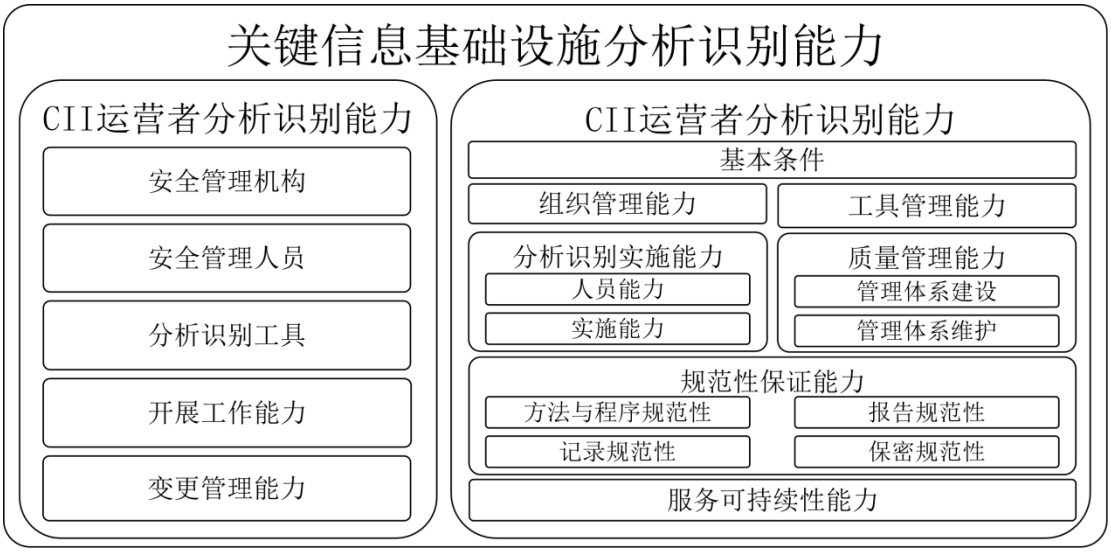

图 3 关键信息基础设施分析识别能力模型

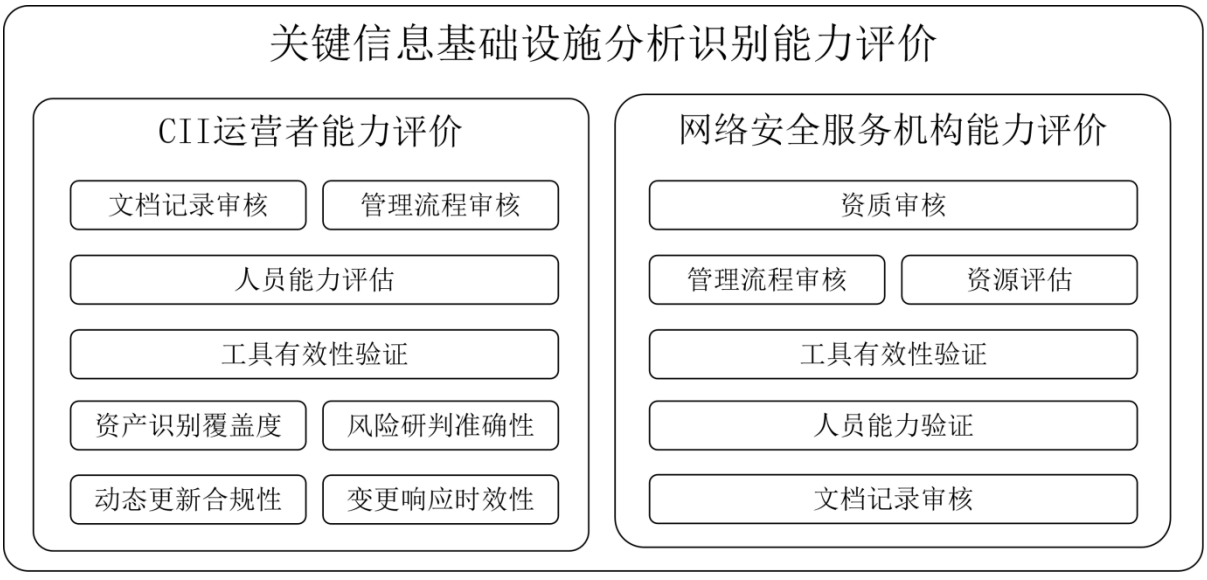

图 4 关键信息基础设施分析识别能力评价模型

6.2 模型组成

6.2.1 CII 运营者分析识别能力

CII 运营者的详细能力要求参见第 7 章，必要项总结为三个方面：

(1) 专门的管理机构、严格的人员成长与管理机制；
(2) 具备资产安全监测和变更管理机制；
(3) 常态化、自适应的风险管理体系。

6.2.2 网络安全服务机构分析识别能力

网络安全服务机构的详细能力要求参见第 8 章，必要项总结为三个方面：
(1) 有经验、有积累、有专业人员、有专业工具储备；
(2) 具备围绕关键业务链，识别业务依赖性、关键资产和风险等的能力；
(3) 具备质量控制、过程和结果规范性的能力。

6.2.3 CII 运营者分析识别能力评价

通过以下方式和方法针对 CII 运营者分析识别能力进行评价：
（1）通过文档记录审核、管理流程审核、人员能力评估等方式来评价安全管理机构和安全管理人员的管理能力和技术水平；
（2）通过工具有效性验证来评价分析识别工具的有效性；
（3）通过资产识别覆盖度、风险研判准确性来评价开展工作能力水平；
（4）通过动态更新合规性、变更响应时效性来评价变更管理能力水平。

6.2.4 网络安全服务机构分析识别能力评价

通过以下方式和方法针对网络安全服务机构分析识别能力进行评价：
（1）通过资质审核来核查基本条件达标情况；
（2）通过管理流程审核、资源评估等方式来评价组织管理和服务可持续性的能力水平；
（3）通过工具有效性验证来评价工具管理能力水平；
（4）通过人员能力验证来评价分析识别实施能力水平；
（5）通过文档记录审核来评价质量管理和规范性保证能力水平。

6.3 评价指标

CII 运营者分析识别能力评价指标包括安全管理机构、安全管理人员、分析识别工具、开展工作能力和变更管理能力等方面，涉及合规项 41 项，必要项 15 项。评价指标详见附录 A。

网络安全服务机构分析识别能力评价指标包括基本条件、组织管理能力、工具管理能力、分析识别实施能力、质量管理能力、规范性保证能力和服务可持续性能力等方面，合规项 64 项，必要项 24 项。评价指标详见附录 B。

6.4 评价方法

CII 运营者的分析识别能力合规指标进行了权重和必要项标识，仅供运营者优化提升借鉴使用，原则上无评价结论。而网络安全服务机构的分析识别能力合规指标需要有明确的评价结论。

网络安全服务机构的分析识别能力评价方法见表 1。首先判断必要项的满足情况，如出现必要项不满足，则评价结论为不通过；在必要项全部满足的情况下，再对合规项进行评价（详见附录 B），根据权重×符合率的算法计算得出整体分值，分值大于等于 80 分则评价结论为通过，分值低于 80 分则评价结论为不通过。

表 1 网络安全服务机构分析识别能力评价表

评价结论	网络安全服务机构分析识别能力评分标准	
	合规项加权计算分值	必要项评价
通过	$\sum_{i=1}^{7}\left(\frac{\text{单合规项满足数}}{\text{单合规项总数}}*\text{权重}*100\right)_i \geq 80$	全部满足
不通过	$\sum_{i=1}^{7}\left(\frac{\text{单合规项满足数}}{\text{单合规项总数}}*\text{权重}*100\right)_i < 80$	全部满足

不通过	N/A	存在不满足的情况

注：N/A 是“Not Applicable”缩写，意为“不适用”。

7 CII 运营者分析识别能力

7.1 能力组成

CII 运营者分析识别能力评价指标项分为 5 个部分，如表 2 所示。安全管理机构占权重的 15%，包含 5 个合规项，其中必要项 2 个；安全管理人员占权重的 20%，包含 9 个合规项，其中必要项 3 个；分析识别工具占权重的 15%，包含 7 个合规项，其中必要项 2 个；开展工作能力占权重的 35%，包含 14 个合规项，其中必要项 6 个；变更管理能力占权重的 15%，包含 6 个合规项，其中必要项 2 个。

表 2 CII 运营者分析识别能力组成表

能力层面	权重	合规项	必要项
安全管理机构	15%	5	2
安全管理人员	20%	9	3
分析识别工具	15%	7	2
开展工作能力	35%	14	6
变更管理能力	15%	6	2
合计	100%	41	15

7.2 安全管理机构

CII 运营者应建立安全管理机构，要求包括以下：

a) 运营者应成立针对关键信息基础设施指导和管理的网络安全工作委员会或领导小组，由单位第一负责人担任其领导职务，明确一名领导班子成员作为首席网络安全官，专职管理或分管关键信息基础设施安全保护工作；

b) 运营者应设置专门的网络安全管理机构，明确机构的安全管理职责和安全岗位编制；

c) 运营者应建立并实施网络安全考核及监督问责机制，并通过考核和监督问责相关工作记录文档查验该机制是否正确有效运行；

d) 应为每个关键信息基础设施明确一名安全管理责任人；

e) 应将安全管理机构的主要负责人纳入本组织关键信息基础设施相关决策体系。

7.3 安全管理人员

CII 运营者应配备安全管理人员，要求包括以下：

a) 应明确安全管理机构的关键岗位，包括与关键业务系统直接相关的系统管理、网络管理、安全管理等岗位；

b) 应对安全管理机构的关键岗位人员进行安全技能考核，符合要求的人员方能上岗；

c) 关键岗位宜从内部人员中选拔，配备专人，并配备两人以上共同管理；

d) 应定期安排安全管理机构人员参加国家、行业或业界网络安全相关活动，及时获取网络安全动态；

e) 应建立网络安全教育培训制度，定期开展网络安全教育培训和技能考核，关键信息基础设施从业人员每人每年教育培训时长不得少于 40 个学时；教育培训内容应包括网络安全相关法律法规、政策标准，以及网络安全保护技术、网络安全管理等；

f) 网络安全教育培训和技能考核应根据岗位的不同而设定不同周期；

g)　应对安全管理机构的负责人和关键岗位人员进行背景调查，并留存相关的背景调查材料。当安全管理机构的负责人和关键岗位人员的身份、安全背景发生变化(例如：取得非中国国籍)或必要时，应根据情况重新按照相关要求进行安全背景审查；

h)　应在人员发生内部岗位调动时，重新评估调动人员对关键信息基础设施的逻辑和物理访问权限，修改访问权限并通知相关人员或角色。应在人员离岗时，及时终止离岗人员的所有访问权限，收回与身份鉴别相关的软硬件设备，进行面谈通知相关人员或角色；

i)　应明确人员的安全保密职责和义务，包括安全职责、奖惩机制、离岗后的脱密期限等，并签订安全保密协议。

7.4　分析识别工具

CII 运营者应配备分析识别工具，要求包括以下：

a）分析识别工具包括但不限于流量分析工具、资产探测工具、安全基线核查工具、漏洞扫描工具、入侵检测工具、渗透测试工具等；

b）分析识别工具应能覆盖关键业务链的各环节，包括业务、资产和风险三个方面的分析识别；

c）分析识别工具应通过具备资质的检测机构的测试或认证；

d）针对分析识别工具的使用和操作流程，应制定详细的标准和规范；

e）应定期评价分析识别工具的有效性和适用性，并根据评估结果进行持续改进升级；

f）具备自动化工具对资产进行识别与脆弱性评估，实现资产的安全管理；

g）具备对拒绝服务攻击、高级可持续威胁等网络攻击行为进行有效分析的自动化工具或平台。

7.5　开展工作能力

CII 运营者应具备开展分析识别工作的能力，要求包括以下：

a）应建立分析识别的制度和流程，明确分析识别的目的、范围、方法和周期等要求；

b）应组建专业的安全团队或委托专业的第三方网络安全服务机构开展分析识别；

c）业务分析识别应包括梳理业务清单、分析业务关联关系、识别关键业务链、明确支撑关键业务的 CII 定位和运营情况等，并形成业务分析识别相关文档，包括但不限于业务清单、业务关联图谱、CII 分布和运营情况表；

d）资产分析识别应包括梳理资产清单、分析业务资产依赖关系、资产防护优先级排序、资产探测自动识别和资产动态更新机制等，并形成资产清单，包含但不限于资产名称、资产类别、用途、数量、所处位置、资产责任人、资产防护优先级等信息；

e）风险分析识别应包括围绕关键业务链的各个环节开展，并形成安全风险报告，至少包含风险分析目标、范围、资产识别、威胁分析、脆弱性分析、安全控制有效性分析、风险分析和风险处置优先级等内容；

f）明确资产识别的标准和方法，对资产进行分类，从业务影响、经济价值和战略重要性等多个维度评估资产的价值和重要性，对资产防护的优先级进行排序；

g）采用定量和定性相结合的分析方法对风险的可能性和影响进行评估，确保风险分析识别结果的准确性和可靠性；

h）基于业务场景构建威胁分析模型，结合威胁情报数据和历史安全事件开展威胁分析识别，提高威胁分析识别的准确性；

i）采用渗透测试、漏洞扫描、攻防演练、沙盘推演等方式对安全控制措施有效性进行测试验证，提高安全控制措施有效性分析的准确性；

j）采用主流的资产探测、风险评估工具和技术，提高资产探测、风险评估的效率和准确性；

k）对风险分析识别中发现的安全风险，应及时进行整改并跟踪记录，形成风险整改清单文档，确保整改措施的有效实施；

l）建立有效的资产管理和风险管理机制，确保资产和风险信息及时更新；

m）建立有效的风险沟通机制，确保风险信息在组织内部和利益相关方之间得到及时和准确的传递，并报告风险分析识别的结果；

n）建立风险数据库，记录所有分析识别到的安全风险，为风险处置和决策提供数据支撑；

o）确保分析识别工作和管理过程符合相关法律法规和行业标准。

7.6 变更管理能力

CII 运营者应具备变更管理能力，要求包括以下：

a）应建立高效、灵活且全面的变更管理机制，以应对不断变化的关键信息基础设施环境；

b）具备强大的数据分析能力，能够对海量的监控数据进行快速分析和处理，从中提取有价值的信息，准确判断变更的性质和影响；

c）具备业务理解能力，能够深入理解业务的本质、目标、流程和需求，可以准确识别业务属性变更对关键信息基础设施的影响；

d）具备对信息系统、网络技术、数据处理等方面的专业知识和分析能力，能够评估变更对技术架构和系统运行的影响；

e）建立有效的变更沟通机制，确保变更信息在组织内部和利益相关方之间得到及时和准确的传递，并报告变更实施的进展情况；

f）具备风险防控能力，能够及时识别和防范变更后的各类风险，确保业务正常运行。

8 网络安全服务机构分析识别能力

8.1 能力组成

网络安全服务机构分析识别能力评价指标项分为 7 个部分，如表 2 所示。基本条件占权重的 10%，包含 8 个合规项，其中必要项 6 个；组织管理能力占权重的 8%，包含 5 个合规项，其中必要项 1 个；工具管理能力占权重的 10%，包括 7 个合规项，其中必要项 2 个；分析识别实施能力占权重的 30%，包含 14 个合规项，其中必要项 5 个；质量管理能力占权重的 12%，包含 8 个合规项，其中必要项 2 个；规范性保证能力占权重的 22%，包含 18 个合规项，其中必要项 6 个；服务可持续性能力占权重的 8%，包含 4 个合规项，其中必要项 2 个。

表 3 网络安全服务机构分析识别能力组成表

能力层面	权重	合规项	必要项
基本条件	10%	8	6
组织管理能力	8%	5	1
工具管理能力	10%	7	2
分析识别实施能力	30%	14	5
质量管理能力	12%	8	2
规范性保证能力	22%	18	6
服务可持续性能力	8%	4	2
合计	100%	64	24

8.2 基本条件

开展分析识别活动的网络安全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，且无违法违规记录；

b）产权关系明晰，注册资金 500 万元以上，独立经营核算；

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；

h）不涉及网络安全产品开发、销售或信息系统安全集成等可能影响分析识别结果公正性的业务（自用除外）。

8.3 组织管理能力

开展分析识别活动的网络安全服务机构应具备组织管理能力，要求包括以下：

a）网络安全服务机构管理者应掌握关键信息基础设施安全保护政策文件，熟悉相关的标准规范；

b）网络安全服务机构应按一定方式组织并设立相关部门，明确其职责、权限和相互关系，保证业务管理、人员管理、合同管理、项目管理、资源管理等工作的有序开展；

c）网络安全服务机构应具有胜任关键信息基础设施安全分析识别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 80%；

d）网络安全服务机构应设置满足关键信息基础设施安全分析识别工作需要的岗位，如技术员、项目组长、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，上述岗位应为专职人员，不得兼任；

e）网络安全服务机构应制定完善的规章制度，包括但不限于以下内容：

1) 保密管理制度，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、分析识别过程保密管理各项措施与要求，以及违反保密制度的罚则等内容；

2) 项目管理制度，网络安全服务机构应根据相关标准制定完备的、符合自身特点的分析识别项目管理程序，主要应包括分析识别工作的组织形式、工作职责，分析识别各阶段的工作内容和管理要求等；

3) 文档管理制度，应包括机构人员在分析识别文档（含电子文档）管理中的相关职责、档案借阅、保管直至销毁的各项规定等；

4) 设备管理制度，应包括机构人员在仪器设备（含分析识别设备和工具）管理中的相关职责、仪器设备的购置、使用和运行维护的各项规定等；

5) 人员管理制度，应包括人员录用、考核、日常管理以及离职等方面的内容和要求；

6) 人员培训制度，应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；

7) 申诉、投诉及争议处理制度，应明确包括网络安全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。

8.4 工具管理能力

开展分析识别活动的网络安全服务机构应具备工具管理能力，要求包括以下：

a）网络安全服务机构应配备满足关键信息基础设施安全分析识别工作需要的设备和工具，如网络协议分析、资产探测或测绘、漏洞扫描、渗透测试工具等，使用的设备和工具应经具备资格的机构安全认证合格或者安全检测符合要求，并获得正版授权；

b）网络安全服务机构应具备满足关键信息基础设施安全分析识别业务开展需要的实验环境，至少满足技术培训、模拟测试的需要；

c）网络安全服务机构自行研发或开源的设备和工具需要经过功能性、安全性和结果准确性验证后方可使用，并保留验证材料；

d）网络安全服务机构应制定设备和工具的档案、操作维护规程（作业指导书）、使用说明书、定期核查计划、日常使用记录、定期维护记录、升级记录等文档，有校准需求的设备工具在有效期内的校准报告或证书原件；

e）网络安全服务机构应确保设备和工具运行状态良好，并通过持续更新、升级等手段保证其提供准确的数据；

f）设备和工具均应有正确的标识，以表明其运行状态、资产管理等情况；

g）网络安全服务机构应建立专门的制度，对用于分析识别数据处理的计算机进行有效的运行维护，并保证计算机中数据记录的完整性、可控性。

8.5 分析识别实施能力

8.5.1 人员能力

开展分析识别活动的网络安全服务机构应具备人员能力，要求包括以下：

a）网络安全服务机构从事关键信息基础设施安全分析识别工作的专业技术人员（以下简称分析识别人员）应具有把握国家法律政策，理解和掌握相关技术标准，熟悉关键信息基础设施安全分析识别的方法、流程和工作规范等方面的知识及能力；关键信息基础设施安全分析识别人员能力要求应符合附录C 的要求；

b）网络安全服务机构应组织分析识别人员进行岗前培训，通过考核并由网络安全服务机构确认具备分析识别能力后上岗；

c）网络安全服务机构应组织分析识别技术员、分析识别项目组长和技术主管岗位人员分别进行培训考核，确保具备相应初、中、高级的分析识别人员能力，分析识别人员数量不应少于 15 人；

d）网络安全服务机构应建设专门的业务仿真实验室，实验室技术人员不少于 5 人，应具备开展特定行业业务分析、资产识别和风险评估等技术经验；

e）分析识别人员应除具备分析识别能力外，每年应参加多种形式的分析识别业务和技术培训，分析识别人员每年培训时长累计不少于 40 学时；

f）网络安全服务机构应指定一名技术主管，全面负责关键信息基础设施安全分析识别方面的技术工作；技术主管应具有大学本科（含）以上学历、具有 5 年以上网络安全工作经验；

g）在开展安全分析识别服务实施过程中，实施人员人数不得少于 4 名，其中高级和中级技术人员应各不少于 1 名。

8.5.2 实施能力

开展分析识别活动的网络安全服务机构应具备分析识别实施能力，要求包括以下：

a）业务分析识别实施能力，包括业务关联图谱构建、关键业务链识别、CII 分布情况识别和 CII 运营情况识别等方面工作指导书的开发、使用、维护及获取相关结果的专业判断；

b）资产分析识别实施能力，包括资产探测与测绘、业务资产依赖关系解析、资产防护优先级排序、资产清单动态更新等方面工作指导书的开发、使用、维护及获取相关结果的专业判断；

c）风险分析识别实施能力，包括关键业务链威胁识别、脆弱性识别、防控措施效果评估、风险分析和风险处置优先级排序等方面工作指导书的开发、使用、维护及获取相关结果的专业判断；

d）工具使用与分析能力，根据实际工作要求，开发与服务相关的工具使用指导书，借助专用设备和工具，实现资产探测、脆弱性发现与威胁识别等方面的能力；

e）风险分析能力，按照 GB/T 20984 规定的风险评估方法对关键业务链进行风险评估，并确保风险评估结果的客观性和准确性；

f）整体实施风险管控能力，充分评估分析识别工作可能给关键信息基础设施带来的风险，特别是可能影响关键信息基础设施正常运行的工作内容，包括操作失误、设备和工具接入等；

g）网络安全服务机构应依据分析识别工作流程，有计划、按步骤地开展分析识别工作，并保证分析识别活动的每个环节都得到有效的控制，具体要求分为四个阶段：

1) 工作准备阶段，收集关键信息基础设施的相关资料信息，填写规范的调查表，全面掌握CII运营者相关业务的详细情况，为分析识别工作的开展打下基础；
2) 方案编制阶段，正确合理地确定分析识别目的、对象及方法等，并依据现行有效的技术标准、规范开发分析识别方案、指导书、结果记录表格和报告模板等；分析识别方案应通过技术评审并有相关记录，分析识别指导书应进行版本有效性维护，且满足以下要求：
①符合相关的关键信息基础设施安全分析识别标准；
②提供足够详细的信息以确保分析识别数据获取过程的规范性和可操作性。
3) 现场实施阶段，严格执行分析识别方案和指导书中的内容和要求，并依据操作规程熟练地使用分析识别设备和工具，规范、准确、完整地填写结果记录，获取足够证据，客观、真实、科学地反映出关键信息基础设施关键业务链、关键资产和风险等状况，分析识别过程应予以监督并记录；
4) 报告编制阶段，客观描述CII运营者的关键业务和关联业务以及主要资产，指出关键业务链存在的脆弱性、面临的威胁，结合现有防控措施分析这些脆弱性和威胁可能导致的风险，给出风险评估结论和风险处置建议，形成风险评估报告和风险处置报告。

8.6 质量管理能力

8.6.1 管理体系建设

a）网络安全服务机构应当制定安全方针和目标，并在其指导下建立、实施和维护符合自身关键信息基础设施安全分析识别工作要求的安全管理体系，并确保体系的有效运行；

b）网络安全服务机构应当制定相应的质量目标，不断提升自身的服务质量和管理水平；

c）网络安全服务机构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，并有权直接与网络安全服务机构最高管理层沟通；

d）网络安全服务机构应指定监督员，对关键信息基础设施安全分析识别服务实施质量监督；监督员应具备丰富的安全分析识别经验、精通安全分析识别技术，并能对分析识别结果做出权威判断。

8.6.2 管理体系维护

a）网络安全服务机构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）网络安全服务机构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）网络安全服务机构应制定并严格遵守申诉、投诉及争议处理制度，包括网络安全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，并应记录采取的措施；

d）网络安全服务机构应建立并实施内部管理体系审核和管理评审机制，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。

8.7 规范性保证能力

8.7.1 方法与程序规范性

网络安全服务机构应保证分析识别方法、程序和审批过程的规范性：

a）网络安全服务机构应制定程序，保证与分析识别服务相关的所有工作程序、指导书、标准规范、工作表格、核查记录表等现行有效并便于分析识别人员获得；

b）上述文件的发布实施应履行统一的审批程序，文件的变更和修订应有授权并及时进行版本维护。

8.7.2 记录规范性

网络安全服务机构应保证分析识别服务内容和管理的规范性：

a）分析识别记录应当清晰规范，并获得被分析识别方的书面确认；

b）分析识别记录应详实、完整，不得漏记、补记、追记；

c）网络安全服务机构应具备完全保管记录的能力，所有的分析识别记录应保存三年以上。

8.7.3 报告规范性

网络安全服务机构应保证分析识别服务产出报告的规范性：

a）网络安全服务机构开展安全分析识别服务，应产出风险评估报告、风险处置报告等报告成果；

b）产出报告应依据机构统一制订的相应报告模版的格式和内容要求进行编写；

c）风险评估报告应包括所有风险评估结果、根据风险评估结果做出的专业判断以及理解和解释风险评估结果所需要的相关信息，以上信息均应正确、准确、清晰地表述；

d）风险处置报告应包括所有风险处置优先级、做出的处置措施建议以及理解和解释风险处置优先级和建议措施所需要的相关信息，以上信息均应正确、准确、清晰地表述；

e）产出报告应由分析识别项目负责人作为第一编制人，由技术主管或质量主管负责审核，机构管理者或其授权人员签发或批准。

8.7.4 保密规范性

a）网络安全服务机构应建立并保存关键信息基础设施安全分析识别工作人员的人员档案，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；

b）网络安全服务机构应重视安全保密工作，指定安全保密工作的责任人；

c）网络安全服务机构应依据保密管理制度，每年至少组织开展一次安全保密教育培训，分析识别人员应当保守在分析识别服务中知悉的国家秘密、工作秘密、商业秘密和个人隐私等；

d）网络安全服务机构应明确岗位保密要求，与全体人员签订《保密责任书》，规定其应当履行的安全保密义务和承担的法律责任，并负责检查落实；

e）网络安全服务机构应采取技术和管理措施来确保关键信息基础设施安全分析识别相关信息的安全、保密和可控，这些信息包括但不限于：

1) 被分析识别单位提供的资料；
2) 关键信息基础设施安全分析识别活动生成的数据和记录；
3) 依据上述信息做出的分析与专业判断；
4) 在分析识别服务中知悉的商业秘密、重要敏感信息和个人信息；
5) 在分析识别服务中收集掌握的安全事件、资产信息、业务流程、系统漏洞等信息。

f）网络安全服务机构应借助有效的技术手段，确保关键信息基础设施安全分析识别相关信息的整个数据生命周期的安全和保密；

g）不应擅自使用、泄露或出售关键信息基础设施安全分析识别活动中收集的数据信息、资料或报告等；

h）关键信息基础设施安全分析识别工作人员离职前，网络安全服务机构应与其签订保密协议，并保存人员档案三年。

8.8 服务可持续性能力

a）网络安全服务机构应根据自身情况制定战略规划，通过不断的投入保证网络安全服务机构的持续建设和发展；

b）网络安全服务机构应实施完善的培训制度，以确保其人员在专业技术和管理方面持续满足关键信息基础设施安全分析识别工作的需要；除常规培训外，应根据人员的工作岗位需求，制定详细和有针对性的培训计划，并进行岗位培训、考核和评定；

c）网络安全服务机构应跟踪国内外新技术、新应用和新业态的发展，组织开展相关领域网络安全的专项课题研究和实践，确保技术能力与当前的技术发展同步；

d）分析识别服务时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，确保工作顺利交接后方可退出服务。

附 录 A
（规范性)
CII 运营者分析识别能力评价指标

表 A.1 CII 运营者分析识别能力评价指标

层面	要点	权重	合规项指标描述	合规项数量	必要项标识
安全管理机构	/	15%	a)运营者应成立针对关键信息基础设施指导和管理的网络安全工作委员会或领导小组，由单位第一负责人担任其领导职务，明确一名领导班子成员作为首席网络安全官，专职管理或分管关键信息基础设施安全保护工作。	5	
			b)运营者应设置专门的网络安全管理机构，明确机构的安全管理职责和安全岗位编制。		☆
			c)运营者应建立并实施网络安全考核及监督问责机制，并通过考核和监督问责相关工作记录文档查验该机制是否正确有效运行。		
			d)应为每个关键信息基础设施明确一名安全管理责任人。		☆
			e)应将安全管理机构的主要负责人纳入本组织关键信息基础设施相关决策体系。		
安全管理人员	/	20%	a)应明确安全管理机构的关键岗位，包括与关键业务系统直接相关的系统管理、网络管理、安全管理等岗位；	9	
			b)应对安全管理机构的关键岗位人员进行安全技能考核，符合要求的人员方能上岗；		
			c)关键岗位宜从内部人员中选拔，配备专人，并配备两人以上共同管理；		☆
			d)应定期安排安全管理机构人员参加国家、行业或业界网络安全相关活动，及时获取网络安全动态；		
			e)应建立网络安全教育培训制度，定期开展网络安全教育培训和技能考核，关键信息基础设施从业人员每人每年教育培训时长不得少于 40 个学时；教育培训内容应包括网络安全相关法律法规、政策标准，以及网络安全保护技术、网络安全管理等；		
			f)网络安全教育培训和技能考核应根据岗位的不同而设定不同周期；		
			g)应对安全管理机构的负责人和关键岗位人员进行背景调查，并留存相关的背景调查材料。当安全管理机构的负责人和关键岗位人员的身份、安全背景发生变化(例如：取得非中国国籍)或必要时，应根据情况重新按照相关要求进行安全背景审查；		

表 A.1 CII 运营者分析识别能力评价指标（续）

层面	要点	权重	合规项指标描述	合规项数量	必要项标识
安全管理人员	/	20%	h)应在人员发生内部岗位调动时，重新评估调动人员对关键信息基础设施的逻辑和物理访问权限，修改访问权限并通知相关人员或角色。应在人员离岗时，及时终止离岗人员的所有访问权限，收回与身份鉴别相关的软硬件设备，进行面谈通知相关人员或角色；	9	☆
			i)应明确人员的安全保密职责和义务，包括安全职责、奖惩机制、离岗后的脱密期限等，并签订安全保密协议。		☆
分析识别工具	/	15%	a）分析识别工具包括但不限于流量分析工具、资产探测工具、安全基线核查工具、漏洞扫描工具、入侵检测工具、渗透测试工具等；	7	☆
			b）分析识别工具应能覆盖关键业务链的各环节，包括业务、资产和风险三个方面的分析识别；		
			c）分析识别工具应通过具备资质的检测机构的测试或认证；		☆
			d）针对分析识别工具的使用和操作流程，应制定详细的标准和规范；		
			e）应定期评价分析识别工具的有效性和适用性，并根据评估结果进行持续改进升级；		
			f）具备自动化工具对资产进行识别与脆弱性评估，实现资产的安全管理；		
			g）具备对拒绝服务攻击、高级可持续威胁等网络攻击行为进行有效分析的自动化工具或平台。		
开展工作能力	/	35%	a）应建立分析识别的制度和流程，明确分析识别的目的、范围、方法和周期等要求；	14	
			b）应组建专业的安全团队或委托专业的第三方网络安全服务机构开展分析识别；		☆
			c）业务分析识别应包括梳理业务清单、分析业务关联关系、识别关键业务链、明确支撑关键业务的 CII 定位和运营情况等，并形成业务分析识别相关文档，包括但不限于业务清单、业务关联图谱、CII 分布和运营情况表；		
			d）资产分析识别应包括梳理资产清单、分析业务资产依赖关系、资产防护优先级排序、资产探测自动识别和资产动态更新机制等，并形成资产清单，包含但不限于资产名称、资产类别、用途、数量、所处位置、资产责任人、资产防护优先级等信息；		☆
			e）风险分析识别应包括围绕关键业务链的各个环节开展，并形成安全风险报告，至少包含风险分析目标、范围、资产识别、威胁分析、脆弱性分析、安全控制有效性分析、风险分析和风险处置优先级等内容；		

表 A.1 CII 运营者分析识别能力评价指标（续）

层面	要点	权重	合规项指标描述	合规项数量	必要项标识
开展工作能力	/	35%	f）应明确资产识别的标准和方法，对资产进行分类，从业务影响、经济价值和战略重要性等多个维度评估资产的价值和重要性，对资产防护的优先级进行排序；	14	
			g）应采用定量和定性相结合的分析方法对风险的可能性和影响进行评估，确保风险分析识别结果的准确性和可靠性；		☆
			h）应基于业务场景构建威胁分析模型，结合威胁情报数据和历史安全事件开展威胁分析识别，提高威胁分析识别的准确性；		
			i）应采用渗透测试、漏洞扫描、攻防演练、沙盘推演等方式对安全控制措施有效性进行测试验证，提高安全控制措施有效性分析的准确性；		
			j）应采用主流的资产探测、风险评估工具和技术，提高资产探测、风险评估的效率和准确性；		☆
			k）对风险分析识别中发现的安全风险，应及时进行整改并跟踪记录，形成风险整改清单文档，确保整改措施的有效实施；		
			l）应建立有效的资产管理和风险管理机制，确保资产和风险信息及时更新；		
			m）应建立有效的风险沟通机制，确保风险信息在组织内部和利益相关方之间得到及时和准确的传递，并报告风险分析识别的结果；		☆
			n）应建立风险数据库，记录所有分析识别到的安全风险，为风险处置和决策提供数据支撑；		
			o）应确保分析识别工作和管理过程符合相关法律法规和行业标准。		☆
变更管理能力	/	15%	a）应建立高效、灵活且全面的变更管理机制，以应对不断变化的关键信息基础设施环境；	6	☆
			b）具备强大的数据分析能力，能够对海量的监控数据进行快速分析和处理，从中提取有价值的信息，准确判断变更的性质和影响；		
			c）具备业务理解能力，能够深入理解业务的本质、目标、流程和需求，可以准确识别业务属性变更对关键信息基础设施的影响；		
			d）具备对信息系统、网络技术、数据处理等方面的专业知识和分析能力，能够评估变更对技术架构和系统运行的影响；		
			e）建立有效的变更沟通机制，确保变更信息在组织内部和利益相关方之间得到及时和准确的传递，并报告变更实施的进展情况；		☆

表 A.1 CII 运营者分析识别能力评价指标（续）

层面	要点	权重	合规项指标描述	合规项数量	必要项标识
变更管理能力	/	15%	f）具备风险防控能力，能够及时识别和防范变更后的各类风险，确保业务正常运行。	6	

附 录 B
（规范性)
网络安全服务机构分析识别能力评价指标

表 B.1 网络安全服务机构分析识别能力评价指标

层面	要点	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，由中国公民、法人投资或者国家投资的企事业单位，且无违法违规记录；	8	☆
			b）产权关系明晰，注册资金 500 万元以上，独立经营核算；		
			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；		
			h）不涉及网络安全产品开发、销售或信息系统安全集成等可能影响分析识别结果公正性的业务（自用除外）。		☆
组织管理能力	/	8%	a）网络安全服务机构管理者应掌握关键信息基础设施安全保护政策文件，熟悉相关的标准规范；	5	
			b）网络安全服务机构应按一定方式组织并设立相关部门，明确其职责、权限和相互关系，保证业务管理、人员管理、合同管理、项目管理、资源管理等工作的有序开展；		
			c）网络安全服务机构应具有胜任关键信息基础设施安全分析识别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 80%；		☆
			d）网络安全服务机构应设置满足关键信息基础设施安全分析识别工作需要的岗位，如技术员、项目组长、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，上述岗位应为专职人员，不得兼任；		

表 B.1 网络安全服务机构分析识别能力评价指标（续）

层面	要点	权重	合规项指标描述	合规项数量	必要项标识
组织管理能力	/	8%	e）网络安全服务机构应制定完善的规章制度，包括但不限于以下内容： 1)保密管理制度，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、分析识别过程保密管理各项措施与要求，以及违反保密制度的罚则等内容； 2)项目管理制度，网络安全服务机构应根据相关标准制定完备的、符合自身特点的分析识别项目管理程序，主要应包括分析识别工作的组织形式、工作职责，分析识别各阶段的工作内容和管理要求等； 3)文档管理制度，应包括机构人员在分析识别文档（含电子文档）管理中的相关职责、档案借阅、保管直至销毁的各项规定等； 4)设备管理制度，应包括机构人员在仪器设备（含分析识别设备和工具）管理中的相关职责、仪器设备的购置、使用和运行维护的各项规定等； 5)人员管理制度，应包括人员录用、考核、日常管理以及离职等方面的内容和要求； 6)人员培训制度，应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； 7)申诉、投诉及争议处理制度，应明确包括网络安全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。	5	
工具管理能力	/	10%	a）网络安全服务机构应配备满足关键信息基础设施安全分析识别工作需要的设备和工具，如网络协议分析、资产探测或测绘、漏洞扫描、渗透测试工具等，使用的设备和工具应经具备资格的机构安全认证合格或者安全检测符合要求，并获得正版授权；	7	☆
			b）网络安全服务机构应具备满足关键信息基础设施安全分析识别业务开展需要的实验环境，至少满足技术培训、模拟测试的需要；		
			c）网络安全服务机构自行研发或开源的设备和工具需要经过功能性、安全性和结果准确性验证后方可使用，并保留验证材料；		
			d）网络安全服务机构应制定设备和工具的档案、操作维护规程（作业指导书）、使用说明书、定期核查计划、日常使用记录、定期维护记录、升级记录等文档，有校准需求的设备工具在有效期内的校准报告或证书原件；		☆

表 B.1 网络安全服务机构分析识别能力评价指标（续）

层面	要点	权重	合规项指标描述	合规项数量	必要项标识
工具管理能力	/	10%	e）网络安全服务机构应确保设备和工具运行状态良好，并通过持续更新、升级等手段保证其提供准确的数据；	7	
			f）设备和工具均应有正确的标识，以表明其运行状态、资产管理等情况；		
			g）网络安全服务机构应建立专门的制度，对用于分析识别数据处理的计算机进行有效的运行维护，并保证计算机中数据记录的完整性、可控性。		
分析识别实施能力	人员能力	30%	a）网络安全服务机构从事关键信息基础设施安全分析识别工作的专业技术人员（以下简称分析识别人员）应具有把握国家法律政策，理解和掌握相关技术标准，熟悉关键信息基础设施安全分析识别的方法、流程和工作规范等方面的知识及能力；关键信息基础设施安全分析识别人员能力要求应符合附录 C 的要求；	14	☆
			b）网络安全服务机构应组织分析识别人员进行岗前培训，通过考核并由网络安全服务机构确认具备分析识别能力后上岗；		
			c）网络安全服务机构应组织分析识别技术员、分析识别项目组长和技术主管岗位人员分别进行培训考核，确保具备相应初、中、高级的分析识别人员能力，分析识别人员数量不应少于 15 人；		
			d）网络安全服务机构应建设专门的业务仿真实验室，实验室技术人员不少于 5 人，应具备开展特定行业业务分析、资产识别和风险评估等技术经验；		
			e）分析识别人员应除具备分析识别能力外，每年应参加多种形式的分析识别业务和技术培训，分析识别人员每年培训时长累计不少于 40 学时；		
			f）网络安全服务机构应指定一名技术主管，全面负责关键信息基础设施安全分析识别方面的技术工作；技术主管应具有大学本科（含）以上学历、具有 5 年以上网络安全工作经验；		
			g）在开展安全分析识别服务实施过程中，实施人员人数不得少于 4 名，其中高级和中级技术人员应各不少于 1 名。		
分析识别实施能力	实施能力		a）业务分析识别实施能力，包括业务关联图谱构建、关键业务链识别、CII 分布情况识别和 CII 运营情况识别等方面工作指导书的开发、使用、维护及获取相关结果的专业判断；		
			b）资产分析识别实施能力，包括资产探测与测绘、业务资产依赖关系解析、资产防护优先级排序、资产清单动态更新等方面工作指导书的开发、使用、维护及获取相关结果的专业判断；		

表 B.1 网络安全服务机构分析识别能力评价指标（续）

层面	要点	权重	合规项指标描述	合规项数量	必要项标识
分析识别实施能力	实施能力	30%	c）风险分析识别实施能力，包括关键业务链威胁识别、脆弱性识别、防控措施效果评估、风险分析和风险处置优先级排序等方面工作指导书的开发、使用、维护及获取相关结果的专业判断；	14	☆
			d）工具使用与分析能力，根据实际工作要求，开发与服务相关的工具使用指导书，借助专用设备和工具，实现资产探测、脆弱性发现与威胁识别等方面的能力；		☆
			e）风险分析能力，按照 GB/T 20984 规定的风险评估方法对关键业务链进行风险评估，并确保风险评估结果的客观性和准确性；		
			f）整体实施风险管控能力，充分评估分析识别工作可能给关键信息基础设施带来的风险，特别是可能影响关键信息基础设施正常运行的工作内容，包括操作失误、设备和工具接入等；		☆
			g）网络安全服务机构应依据分析识别工作流程，有计划、按步骤地开展分析识别工作，并保证分析识别活动的每个环节都得到有效的控制，具体要求分为四个阶段： 1)工作准备阶段，收集关键信息基础设施的相关资料信息，填写规范的调查表，全面掌握 CII 运营者相关业务的详细情况，为分析识别工作的开展打下基础； 2)方案编制阶段，正确合理地确定分析识别目的、对象及方法等，并依据现行有效的技术标准、规范开发分析识别方案、指导书、结果记录表格和报告模板等；分析识别方案应通过技术评审并有相关记录，分析识别指导书应进行版本有效性维护，且能够提供足够详细的信息以确保分析识别数据获取过程的规范性和可操作性； 3)现场实施阶段，严格执行分析识别方案和指导书中的内容和要求，并依据操作规程熟练地使用分析识别设备和工具，规范、准确、完整地填写结果记录，获取足够证据，客观、真实、科学地反映出关键信息基础设施关键业务链、关键资产和风险等状况，分析识别过程应予以监督并记录； 4)报告编制阶段，客观描述 CII 运营者的关键业务和关联业务以及主要资产，指出关键业务链存在的脆弱性、面临的威胁，结合现有防控措施分析这些脆弱性和威胁可能导致的风险，给出风险评估结论和风险处置建议，形成风险评估报告和风险处置报告。		☆

表 B.1 网络安全服务机构分析识别能力评价指标（续）

层面	要点	权重	合规项指标描述	合规项数量	必要项标识
质量管理能力	管理体系建设	12%	a）网络安全服务机构应当制定安全方针和目标，并在其指导下建立、实施和维护符合自身关键信息基础设施安全分析识别工作要求的安全管理体系，并确保体系的有效运行；	8	
			b）网络安全服务机构应当制定相应的质量目标，不断提升自身的服务质量和管理水平；		
			c）网络安全服务机构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,并有权直接与网络安全服务机构最高管理层沟通；		☆
			d）网络安全服务机构应指定监督员，对关键信息基础设施安全分析识别服务实施质量监督；监督员应具备丰富的安全分析识别经验、精通安全分析识别技术，并能对分析识别结果做出权威判断。		
	管理体系维护		a）网络安全服务机构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）网络安全服务机构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）网络安全服务机构应制定并严格遵守申诉、投诉及争议处理制度，包括网络安全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，并应记录采取的措施。		
			d）网络安全服务机构应建立并实施内部管理体系审核和管理评审机制，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。		
规范性保证能力	方法与程序规范性	22%	a）网络安全服务机构应制定程序，保证与分析识别服务相关的所有工作程序、指导书、标准规范、工作表格、核查记录表等现行有效并便于分析识别人员获得；	18	☆
			b）上述文件的发布实施应履行统一的审批程序，文件的变更和修订应有授权并及时进行版本维护。		
	记录规范性		a）分析识别记录应当清晰规范，并获得被分析识别方的书面确认；		☆
			b）分析识别记录应详实、完整，不得漏记、补记、追记；		
			c）网络安全服务机构应具备完全保管记录的能力，所有的分析识别记录应保存三年以上。		
	报告规范性		a）网络安全服务机构开展安全分析识别服务，应产出风险评估报告、风险处置报告等报告成果；		☆
			b）产出报告应依据机构统一制订的相应报告模版的格式和内容要求进行编写；		☆

表 B.1 网络安全服务机构分析识别能力评价指标（续）

层面	要点	权重	合规项指标描述	合规项数量	必要项标识
规范性保证能力	报告规范性	22%	c）风险评估报告应包括所有风险评估结果、根据风险评估结果做出的专业判断以及理解和解释风险评估结果所需要的相关信息，以上信息均应正确、准确、清晰地表述；	18	
			d）风险处置报告应包括所有风险处置优先级、做出的处置措施建议以及理解和解释风险处置优先级和建议措施所需要的相关信息，以上信息均应正确、准确、清晰地表述；		
			e）产出报告应由分析识别项目负责人作为第一编制人，由技术主管或质量主管负责审核，机构管理者或其授权人员签发或批准。		
	保密规范性		a）网络安全服务机构应建立并保存关键信息基础设施安全分析识别工作人员的人员档案，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；		
			b）网络安全服务机构应重视安全保密工作，指定安全保密工作的责任人；		☆
			c）网络安全服务机构应依据保密管理制度，每年至少组织开展一次安全保密教育培训，分析识别人员应当保守在分析识别服务中知悉的国家秘密、工作秘密、商业秘密和个人隐私等；		
			d）网络安全服务机构应明确岗位保密要求，与全体人员签订《保密责任书》，规定其应当履行的安全保密义务和承担的法律责任，并负责检查落实；		☆
			e）网络安全服务机构应采取技术和管理措施来确保关键信息基础设施安全分析识别相关信息的安全、保密和可控，这些信息包括但不限于： 1)被分析识别单位提供的资料； 2)关键信息基础设施安全分析识别活动生成的数据和记录； 3)依据上述信息做出的分析与专业判断。 4)在分析识别服务中知悉的商业秘密、重要敏感信息和个人信息； 5)在分析识别服务中收集掌握的安全事件、资产信息、业务流程、系统漏洞等信息。		
			f）网络安全服务机构应借助有效的技术手段，确保关键信息基础设施安全分析识别相关信息的整个数据生命周期的安全和保密；		
			g）不应擅自使用、泄露或出售关键信息基础设施安全分析识别活动中收集的数据信息、资料或报告等；		

表 B.1 网络安全服务机构分析识别能力评价指标（续）

层面	要点	权重	合规项指标描述	合规项数量	必要项标识
规范性保证能力	保密规范性	22%	h）关键信息基础设施安全分析识别工作人员离职前，网络安全服务机构应与其签订保密协议，并保存人员档案三年。	18	
服务可持续性能力	/	8%	a）网络安全服务机构应根据自身情况制定战略规划，通过不断的投入保证网络安全服务机构的持续建设和发展；	4	
			b）网络安全服务机构应实施完善的培训制度，以确保其人员在专业技术和管理方面持续满足关键信息基础设施安全分析识别工作的需要；除常规培训外，应根据人员的工作岗位需求，制定详细和有针对性的培训计划，并进行岗位培训、考核和评定；		☆
			c）网络安全服务机构应跟踪国内外新技术、新应用和新业态的发展，组织开展相关领域网络安全的专项课题研究和实践，确保技术能力与当前的技术发展同步；		
			d）分析识别服务时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，确保工作顺利交接后方可退出服务。		☆

附 录 C
（规范性)
关键信息基础设施安全分析识别人员能力要求

表 C.1 关键信息基础设施安全分析识别人员能力要求

等级	具体人员能力要求
初级	1）从事网络安全行业或相关领域工作 3 年以上；
	2）了解关键信息基础设施安全保护的相关法律法规、政策标准；
	3）熟悉网络安全基础知识；
	4）熟悉分析识别工具，了解其功能、特点和操作方法；
	5）熟悉资产探测方法，能够精准地识别出关键资产；
	6）熟悉风险评估方法，能够根据评估指导书客观、准确、完整地获取各项评估证据。
中级	1）从事网络安全行业或相关领域工作 5 年以上；
	2）熟悉关键信息基础设施安全保护的相关法律法规、政策标准；
	3）正确理解关键信息基础设施安全保护标准体系和主要标准内容，能够跟踪国内、国际网络安全相关标准的发展；
	4）掌握网络安全基础知识，熟悉网络安全风险评估方法，具有网络安全技术研究的基础和实践经验；
	5）具有较丰富的项目管理经验，熟悉风险评估项目的工作流程和质量管理方法，具有较强的组织协调和沟通能力；
	6）能够独立开发风险评估指导书，熟悉风险评估指导书的开发、版本控制和评审流程；
	7）能够根据关键信息基础设施的业务属性和行业特点，编制风险评估方案；
	8）具有综合分析和判断的能力，能够依据风险评估报告模板要求编制风险评估报告，整体把握风险评估报告结论的客观性和准确性，具备较强的文字表达能力；
	9）熟悉特定行业特定领域的业务，能够准确、完整地梳理各条业务信息流；
	10）能够针对中发现的安全风险，提出合理化的风险应对措施。

表 C.1 关键信息基础设施安全分析识别人员能力要求（续）

等级	具体人员能力要求
高级	1）从事网络安全行业或相关领域工作 7 年以上；
	2）熟悉和跟踪国内、国际网络安全的相关政策、法规及标准的发展；
	3）对关键信息基础设施安全保护标准体系及主要标准有较为深入的理解；
	4）具有网络安全理论研究的基础、实践经验和研究创新能力；
	5）具有丰富的质量体系管理和项目管理经验，具有较强的组织协调和管理能力。

参 考 文 献

[1] GA/T 2182-2024 关键信息基础设施安全测评要求

[2] T/CIIPA 00006-2024 关键信息基础设施安全服务能力要求

[3] T/CIIPA 00007-2024 关键信息基础设施安全检测评估能力要求

[4] 中华人民共和国网络安全法[2016年11月7日第十二届全国人民代表大会常务委员会第二十四次会议通过，中华人民共和国主席令(第53号)].

[5] 关键信息基础设施安全保护条例(2021年4月27日国务院第133次常务会议通过，中华人民共和国国务院令第745号).

[6] 贯彻落实网络安全等保制度和关键信息基础设施安全保护制度的指导意见(2020年7月22日公安部公网安〔2020〕1960号文公布).