ICS 35.030
CCS L 80

# 团　　体　　标　　准

T/CIIPA 00007—2024

# 关键信息基础设施安全检测评估能力要求

**Capability requirements for security inspection and evaluation of critical information infrastructure**

2025-03-07 发布　　2025-03-09 实施

中关村华安关键信息基础设施安全保护联盟　发布
中　国　标　准　出　版　社　出版

# 目　　次

# 前　言

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

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。

本文件起草单位：中国电子科技集团公司第十五研究所、中关村华安关键信息基础设施安全保护联盟、国家工业信息安全发展研究中心、中国信息安全测评中心、国家广播电视总局监管中心、杭州安信检测技术有限公司、银行卡检测中心（北京银联金卡科技有限公司）、广州竞远安全技术股份有限公司、北京北信源软件股份有限公司、国网思极检测技术（北京）有限公司、中国电力科学研究院有限公司、中国联合网络通信有限公司研究院、大唐科技研究总院、工业和信息化部教育与考试中心、教育部教育管理信息中心、中国工商银行股份有限公司、中邮信息科技（北京）有限公司、水利部信息中心、中国民生银行股份有限公司、中国联合网络通信集团有限公司、中国电信集团有限公司、中国移动通信集团有限公司、湖南浩基信息技术有限公司、甘肃赛飞安全科技有限公司、中科信息安全共性技术国家工程研究中心有限公司、成都久信信息技术股份有限公司、四川北斗弘鹏科技有限公司、湖北珞格科技发展有限公司、杭州中尔网络科技有限公司、合肥天帷信息安全技术有限公司。

本文件主要起草人：霍珊珊、郭启全、刘健、逯瑶、张益、刘赫、刘琛、杨龙、裴帅、赵霖、孙琪、于盟、曹禹、周呈辉、王尊、杜宇鸽、邸丽清、杨波、李炎、何冠辉、叶玉杰、孙茂增、王天昊、原野、梁承东、彭世强、林皓、杨华、徐建、陶然、张仕文、吴谬、王明军、王文军、胡健勋、刘元、成嘉轩、邹远辉、刘洋、张傑、王柯龙、杨蔚、徐亮亮、杜建斌、谢占斐、陈傲晗、魏启超。

# 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。《中华人民共和国网络安全法》和《关键信息基础设施安全保护条例》对关键信息基础设施运营者开展网络安全检测和风险评估的责任和义务进行了规定。

关键信息基础设施安全检测评估是GB/T 39204—2022中提出的关键信息基础设施安全保护六个方面环节之一，检测和评估关键信息基础设施安全状况、发现存在的问题和风险，为关键信息基础设施安全整改建设和监督管理提供依据。关键信息基础设施安全检测评估是以合规测评为基础的网络安全风险和能力判定。由于关键信息基础设施通常由一个或多个等级保护对象构成，因此，关键信息基础设施安全检测评估在其所有等级保护对象开展等级测评之后进行，以便复用等级测评结果。

关键信息基础设施安全检测评估能力要求参考国家标准、行业标准及要求、检测评估机构能力建设与评价的相关内容，结合关键信息基础设施安全保护制度及检测评估实际工作特点，对关键信息基础设施运营者、网络安全检测评估机构开展检测评估活动提出基本能力要求。在此背景下，为确保有效指导提升检测评估能力，满足关键信息基础设施安全保护工作要求，特制定本文件。

# 关键信息基础设施安全检测评估能力要求

## 1 范围

本文件确立了关键信息基础设施安全检测评估总体要求、能力组成，规范了从事关键信息基础设施安全检测评估工作应具备的基本能力要求。

本文件适用于关键信息基础设施运营者、网络安全检测评估机构对关键信息基础设施开展安全检测评估的能力建设参考。

## 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 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 28448 信息安全技术 网络安全等级保护测评要求

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

GB/T 39204 信息安全技术 关键信息基础设施安全保护要求

## 3 术语和定义

GB/T 25069、GB/T 39204、GB/T 22239、GB/T 28448 和 GB/T 36959 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，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。

3.2

**检测评估 testing and evaluation**

为检测评估安全防护措施的有效性，发现网络安全风险隐患，建立相应的检测评估制度，确定检测评估的流程及内容等，开展安全检测与风险隐患评估，分析潜在安全风险可能引发的安全事件。

3.3

**访谈 interview**

检测评估人员通过引导关键信息基础设施保护相关人员进行有目的（有针对性）的交流以帮助检测评估人员理解、澄清或取得证据的过程。

3.4

**核查 examination**

检测评估人员通过对检测评估对象（如制度文档、各类设备及相关安全配置等）进行观察、查验和分

析，以帮助检测评估人员理解、澄清或取得证据的过程。

3.5

**测试　test**

检测评估人员使用预定的方法/工具使检测评估对象（各类设备或安全配置）产生特定的结果，将运行结果与预期的结果进行比对的过程。

3.6

**评估　evaluation**

检测评估人员对关键信息基础设施可能存在的威胁及其可能产生的后果进行综合评价和预测的过程。

3.7

**关键信息基础设施安全检测评估　testing and evaluation for critical information infrastructure**

检测评估机构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，对关键信息基础设施的安全保护状况进行检测评估的活动。

3.8

**单元测评　unit evaluation**

主要依据 GB/T 39204—2022 中各安全子类（包括分析识别、安全防护、检测评估、监测预警、主动防御、事件处置）以及运营者自定义的特殊安全子类的测评。

3.9

**关联测评　correlation evaluation**

在单元测评结果的基础上，结合已知的和潜在的风险集、关键信息基础设施的业务场景、所属领域已知安全事件、可能面临的威胁等，对关键信息基础设施实施的综合性安全检测评估，包括信息收集汇总、入侵痕迹分析、业务逻辑安全分析、设计模拟攻击路径及测试用例、开展渗透测试等。

3.10

**整体评估　overall evaluation**

主要包括针对运营者的网络安全管控能力评估、针对关键信息基础设施自身的网络安全保护水平评估，以及针对关键信息基础设施所承载关键业务的网络安全风险分析与评价三部分。

## 4　检测评估总体要求

### 4.1　基本原则

关键信息基础设施是指一旦遭到破坏、丧失功能或数据泄露，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和信息系统。为关键信息基础设施安全提供保障的安全检测评估工作应遵循的基本原则包括：

a）　全面性原则：安全检测评估应覆盖关键信息基础设施的所有关键点，包括网络设备、服务器、应用系统、数据库等，确保没有遗漏潜在的安全隐患；

b）　主动性原则：安全检测评估应主动进行，而不是等待问题发生后再采取措施。运营者应定期进行安全检测评估可以及时发现和修复安全漏洞，预防安全事件的发生。

c）　系统性原则：安全检测评估应采用系统化的方法，结合威胁情报、漏洞扫描、渗透测试、配置核查等多种手段，形成一个完整的检测评估体系；

d）　独立性原则：安全检测评估应由独立的第三方机构或内部独立部门进行，以确保评估结果的客观性和公正性，避免利益冲突；

e）　合规性原则：安全检测评估应符合网络安全领域国家和行业的相关法律法规、标准规范等要求，避免非授权开展关键信息基础设施安全检测评估；