ICS 35.020
CCS L 05

DB11

北　京　市　地　方　标　准

DB11/T 2413—2025

信息安全技术 重要信息基础设施安全保护与评估要求

Information security technology—
Cybersecurity protection and assessment requirements for important information infrastructure

2025－06－24 发布　　2025－10－01 实施

北京市市场监督管理局　发布

目　　次

前　　言 II
引　　言 III
1 范围 1
2 规范性引用文件 1
3 术语和定义 1
4 安全保护要求 1
4.1 网络安全等级保护 1
4.2 安全通信网络 1
4.3 安全区域边界 1
4.4 安全计算环境 2
4.5 安全管理中心 2
4.6 安全管理制度 2
4.7 安全管理机构 2
4.8 安全管理人员 2
4.9 供应链安全 3
4.10 数据安全 3
4.11 安全运营 4
5 安全评估要求 5
5.1 安全评估方法 5
5.2 安全评估单元 5
5.3 安全评估判定方法 20
参　考　文　献 22

前　言

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

本文件由北京市公安局、北京市委网信办共同提出并归口。

本文件由北京市公安局、北京市委网信办共同组织实施。

本文件起草单位：北京市公安局关键信息基础设施保护中心、北京市公安局网络安全保卫总队、中共北京市委网络安全和信息化委员会办公室、公安部第三研究所、国家计算机网络应急技术处理协调中心北京分中心、公安部第一研究所、北京市大数据中心、北京市数字教育中心、北京市标准化研究院、首都信息发展股份有限公司、北京安信天行科技有限公司、深信服科技股份有限公司、国投云网数字科技有限公司、科来网络技术股份有限公司、瑞数信息技术（上海）有限公司、国网北京市电力公司、中国政法大学法治与可持续发展中心、中国法学会法治研究所。

本文件主要起草人：张帆、问闻、郭毅、杨虎、周永战、陈亮、韩国宁、李杰、邝琳、李宝彦、徐硕、陈广勇、刘宇畅、王丛妍、艾春迪、储迅潮、于跃、张志豪、迟海成、李童、贾宝刚、赵章界、陈昊、李一鸣、刘云、张益谦、安亚鹏、方莉莉、叶润国、刘佳、闫明、张卫云、关福君、赵子慧、李秋香、宫月、刘卜瑜、韩盟、周献飞、周巧霖、郝作成、刘金瑞、荣晓燕、李文静。

引　言

为落实《中华人民共和国网络安全法》相关要求，加强北京市市域内重要信息基础设施的安全保护，在国家等级保护制度和关键信息基础设施保护制度的基础上，借鉴我国相关部门在重要行业和领域开展网络安全保护工作的成熟经验，结合我国和北京市现有的网络安全保障成果，从安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员等方面，提出重要信息基础设施增强型安全保护与评估要求，切实加强重要信息基础设施安全保护。

信息安全技术 重要信息基础设施安全保护与评估要求

1 范围

本文件规定了重要信息基础设施的安全保护要求和评估要求。

本文件适用于重要信息基础设施安全保护和安全评估工作。

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 22240 信息安全技术 网络安全等级保护定级指南

GB/T 25069 信息安全技术 术语

GB/T 39204—2022 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界定的以及下列术语和定义适用于本文件。

3.1

重要信息基础设施 important information infrastructure

北京市重要信息基础设施是指北京市公共通信和信息服务、电子政务、能源、交通、金融、教育、水务、卫生健康、城市管理、广播电视等重要行业和领域中，一旦遭受攻击或者数据泄露，可能严重危害首都城市运行，直接威胁国家安全或者严重危害经济运行、社会稳定、公共健康和地区安全的网络设施、信息系统等。

4 安全保护要求

4.1 网络安全等级保护

重要信息基础设施的网络安全保护等级应不低于GB/T 22240规定的第三级，且应达到相应等级的安全保护要求。

4.2 安全通信网络

对业务连续性要求较高的，应采用至少两条不同运营商的通信线路，并实现通信线路的故障实时检测和链路自动切换。

4.3 安全区域边界

安全区域边界应符合以下要求：

a) 应依据 GB/T 39204—2022 中 10.1 要求，收敛暴露面；

b) 应采取措施保证跨网络通信双方的身份真实性，并授予最小访问控制权限；

c) 应在网络区域间采取访问控制措施，防止网络区域之间的横向攻击；

d) 应禁止将数据库服务器部署在互联网用户直接访问的网络区域。

4.4 安全计算环境

安全计算环境应符合以下要求：

a) 若设备影响重要业务连续性需求，应进行更换或升级；
b) 应实现操作系统和数据库用户的权限分离；
c) 应采用密码技术保证数据库口令在配置文件中的保密性；
d) 应实现应用程序（API）接口调用的最小权限管理，如采用限制调用频率、白名单等措施；
e) 应限制远程访问数据库、中间件、应用系统和网络等相关管理系统的网络地址；
f) 应要求用户修改应用系统的默认口令；
g) 应采用有效措施防止互联网应用被恶意篡改，如采用网页防篡改技术和第三方安全服务等方式。

4.5 安全管理中心

安全管理中心应符合以下要求：

a) 应支持采用自动化工具进行系统账户、配置、漏洞、补丁和病毒库等的集中管理；
b) 应集中收集各类安全告警、日志信息和流量监测数据等，实现所有监测数据的整合分析。

4.6 安全管理制度

安全管理制度应符合以下要求：

a) 应制定并发布适合本组织的网络安全保护计划,明确重要信息基础设施安全保护工作目标,从管理、技术和运营等方面进行规划,每年至少对网络安全保护计划进行一次评估，必要时进行修订；
b) 应制定网络安全策略，并根据重要信息基础设施面临的安全风险和威胁的变化进行相应调整，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、供应链安全管理策略、安全运维策略等；
c) 应制定网络安全管理制度,覆盖风险管理、网络安全考核及监督问责、网络安全教育培训、业务连续性管理及容灾备份、三同步(安全措施同步规划、同步建设和同步使用)和供应链安全管理等方面。

4.7 安全管理机构

安全管理机构应符合以下要求：

a) 应将重要信息基础设施安全保护纳入网络安全工作委员会或领导小组重要议事日程，明确一名首席网络安全官作为高层管理人员，专职管理或者分管重要信息基础设施安全保护工作，参与重要信息基础设施重要事项决策；
b) 应明确重要信息基础设施网络安全管理工作的管理机构；
c) 应建立并实施网络安全考核及监督问责机制；
d) 应为每个重要信息基础设施明确一名安全管理责任人，并明确其安全管理职责；
e) 应保证重要信息基础设施的安全管理责任人能够参与其信息化项目立项、方案设计、方案评审和项目验收等环节的决策。

4.8 安全管理人员

安全管理人员应符合以下要求：

a) 如发生以下情形之一，应对重要信息基础设施安全管理机构的负责人和关键岗位人员实施背景审查，审查通过后方可上岗，包括：

1） 在履行岗位职责前；
2） 相关人员的身份、国籍、安全背景和家庭情况等发生变化时；
3） 岗位发生重大变化或其他必要情况下。

b） 应为重要信息基础设施相关人员提供安全意识教育和安全技能培训，重要信息基础设施相关人员年度接受网络安全培训时间应不少于 15 个学时，在此基础上，网络安全岗位人员年度还应接受专业技能培训不少于 15 个学时，其中包含数据安全相关培训内容；
c） 应明确重要信息基础设施相关人员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。

4.9 供应链安全

供应链安全管理应符合以下要求：

a） 应建立供应链安全管理策略，包括风险管理策略、供应方选择和管理策略、产品开发采购策略、安全维护策略等；
b） 应建立供应商管理制度，至少包括供应商资质审核、供应商分类分级、供应商不良行为处置等方面的管理要求；
c） 应形成年度采购的网络产品和服务清单，采购、使用的网络产品和服务应符合国家及行业合规要求；
d） 应制定软件供应链安全风险持续监测、风险评估和事件响应制度，明确不同等级安全事件的报告、处置、响应和流程机制，规定安全事件的现场处置、事件报告和后期恢复等要求；
e） 采购网络产品和服务时，在合同中应明确提供者的安全责任和义务，要求提供者对网络产品和服务的设计、研发、生产和交付等关键环节加强安全管理，要求提供者声明不非法获取用户数据、控制和操纵用户的系统和设备，或利用用户对产品的依赖性谋取不正当利益或者迫使用户更新换代；
f） 应与网络产品和服务的提供者签订安全保密协议，协议内容包括安全职责、保密内容、奖惩机制和有效期等；
g） 重要信息基础设施采购公有云服务时，应优先使用通过国家云计算服务安全评估的云平台；
h） 应当建立严格的授权机制，操作系统、数据库等最高管理员权限应由本单位人员专人负责，应当按照最小必要原则对外包单位人员进行精细化授权，在授权期满后及时收回权限。

4.10 数据安全

数据安全管理应符合以下要求：

a） 应明确数据安全管理责任，建立数据安全评价考核制度，编制数据安全保护计划；
b） 应保证数据安全管理责任人能够参与其信息化项目立项、方案设计、方案评审和项目验收等环节的决策；
c） 应基于国家标准、行业标准以及业务需求制定组织内部的数据分类分级制度，建立数据资产目录；
d） 应基于数据分类分级制定数据安全保护策略，明确重要数据和个人信息在收集、存储、使用、加工、传输、提供和公开等关键环节的安全保护要求；
e） 应采用加密、脱敏、去标识化等技术手段保护个人敏感信息安全；
f） 应采用技术措施标记敏感数据，辅助追踪数据泄露源头；
g） 应在重要信息基础设施退役废弃时，按照数据安全保护策略对存储的数据进行处置；
h） 应开展数据安全风险评估，对未落实数据安全保护策略的情况及时整改；
i） 应制定数据安全事件应急预案，并定期开展应急演练。

4.11 安全运营

4.11.1 资产识别

资产识别活动应符合以下要求：

a) 应建立重要信息基础设施资产信息清单，资产包括但不限于物理设备、虚拟设备、操作系统、数据库、中间件、应用软件、业务系统等，资产信息包括但不限于资产名称、资产类别、资产型号或版本、网络地址、用途、数量、所处位置、资产责任人、资产防护优先级等；
b) 应采取技术措施支持资产的识别和动态更新。

4.11.2 检测评估

检测评估活动应符合以下要求：

a) 应建立重要信息基础设施安全检测评估制度，包括但不限于检测评估工作流程、方式方法和周期等内容；
b) 应采取自行或者委托的方式对重要信息基础设施开展年度检测评估，并及时整改发现的问题；
c) 新建的重要信息基础设施应开展检测评估工作，通过后方可投入运行；改建或扩建的重要信息基础设施发生重大变化时，应重新开展检测评估工作并及时对发现的问题进行整改；
d) 应至少每年组织开展一次攻防演练，检测重要信息基础设施在面对实际网络攻击时的防护和响应能力；
e) 应至少半年进行一次钓鱼攻击演练，对演练过程中容易被社会工程学攻击的部门、员工进行重点安全意识培训；
f) 应积极配合安全主管部门的安全风险检测和安全专项检查工作，提供必要的材料和技术支持，针对发现的安全隐患和风险建立清单，制定整改方案，并及时整改。

4.11.3 监测预警

监测预警活动应符合以下要求：

a) 应制定监测预警和信息通报制度，明确分级别的信息报告和响应处置程序，建立常态化监测预警和快速应急响应机制；
b) 应与行业主管部门和监管部门建立网络安全信息共享机制，网络安全共享信息内容包括但不限于漏洞信息、威胁信息、最佳实践和前沿技术等，当网络安全共享信息为漏洞信息时，应符合国家关于漏洞管理制度要求；
c) 应及时响应行业主管部门和监管部门的安全预警，分析、研判事件或威胁对自身网络安全保护对象可能造成损害的程度，并将获取的安全预警信息按照规定通报给相关人员和相关部门，必要时应启动应急预案。

4.11.4 应急演练

应急演练活动应符合以下要求：

a) 应急预案中应包括特殊时期的应急响应流程；
b) 应围绕业务的可持续运行设定演练场景，定期组织开展应急演练。

4.11.5 事件处置

事件处置活动应符合以下要求：

a) 应明确网络安全事件处置的专门组织，并配备技术支撑；

b) 应建立安全事件通报机制，及时通报内部相关部门和人员，并按照规定向相关方通报安全事件；
c) 应形成年度网络安全监测预警和事件处置报告，并上报网络安全工作委员会或领导小组。

5 安全评估要求

5.1 安全评估方法

5.1.1 人员访谈

评估人员通过引导方式，进行有目的的、有针对性的交流，以帮助评估人员理解、澄清或取得证据的过程。

5.1.2 文档审查

评估人员通过查看制度文档、设计方案、运维报告和记录文档等各类文档，以帮助评估人员理解澄清或取得证据的过程。

5.1.3 配置核查

评估人员通过登录各类设备、各类平台和应用系统，进行安全配置查看和分析，以帮助评估人员理解澄清或取得证据的过程。

5.1.4 技术测试

评估人员通过使用测试工具（如漏洞扫描工具、渗透测试工具、抓包工具）或人工手动测试等方式，发现重要信息基础设施存在的安全漏洞，验证已有的安全措施是否有效，以帮助评估人员理解澄清或取得证据的过程。

5.2 安全评估单元

5.2.1 网络安全等级保护

该评估单元应按如下要求展开评估：
a) 评估指标：见 4.1
b) 评估对象：等级保护备案证明和等级保护测评报告等。
c) 评估实施包括以下内容：
   1) 查验是否具有等级保护备案证明，定级范围是否覆盖评估对象，安全保护等级是否不低于第三级；
   2) 审查是否按照国家法律法规要求对评估对象全部开展等级测评，查验评估对象符合率是否高于 60%，且不存在重大风险隐患。
d) 单元判定：如果 1）～2）均为肯定，则符合本评估单元指标要求；如果 1）或 2）为否定，则不符合本评估单元指标要求。

5.2.2 安全通信网络

该评估单元应按如下要求展开评估：
a) 评估指标：见 4.2
b) 评估对象：网络设计文档、网络拓扑图和网络策略配置等。

c) 评估实施包括以下内容：
   1) 核查评估对象的业务连续性要求是否较高；
   2) 核查网络拓扑中是否存在至少两条不同运营商的通信线路；
   3) 核查是否配置了通信线路的故障实时检测机制和自动切换机制。
d) 单元判定：如果 1）为否定，本评估单元指标为不适用；如果 1）为肯定，2）～ 3）均为肯定，则符合本评估单元指标要求，否则不符合本评估单元指标要求。

5.2.3 安全区域边界

5.2.3.1 安全区域边界 01

该评估单元应按如下要求展开评估：
a) 评估指标：见 4.3 a）
b) 评估对象：安全管理员、网络安全设计文档、设备资产清单和网络拓扑图等。
c) 评估实施包括以下内容：
   1) 访谈安全管理员，是否制定暴露面收敛策略或制度；
   2) 核验暴露面收敛策略或制度执行文件，是否采取暴露面收敛措施；
   3) 通过技术手段验证暴露面收敛措施是否有效。
d) 单元判定：如果 1）～ 3）为肯定，则符合本评估单元指标要求，否则不符合本评估单元指标要求。

5.2.3.2 安全区域边界 02

该评估单元应按如下要求展开评估：
a) 评估指标：见 4.3 b）
b) 评估对象：安全管理员、业务系统设计文档、网络拓扑图和通信设备等。
c) 评估实施包括以下内容：
   1) 核查业务系统设计文档和网络拓扑图，是否存在跨网络的通信；
   2) 若存在跨网络的通信，核查业务系统设计文档和通信设备，是否进行通信双方的身份真实性验证；
   3) 核查访问控制策略配置，是否授予最小访问权限。
d) 单元判定：如果 1）为否定，本评估单元指标为不适用；如果 2）～ 3）均为肯定，则符合本评估单元指标要求，否则不符合本评估单元指标要求。

5.2.3.3 安全区域边界 03

该评估单元应按如下要求展开评估：
a) 评估指标：见 4.3 c）
b) 评估对象：网络安全设计文档、网络拓扑图和访问控制设备等。
c) 评估实施包括以下内容：
   1) 根据网络区域划分情况，核查是否在每个网络区域之间部署访问控制设备；
   2) 核查访问控制设备，是否进行了有效的访问控制策略配置。
d) 单元判定：如果 1）～ 2）均为肯定，则符合本评估单元指标要求，否则不符合本评估单元指标要求。

5.2.3.4 安全区域边界 04

该评估单元应按如下要求展开评估：

a) 评估指标：见 4.3 d）
b) 评估对象：网络拓扑图、系统设计文档和网络/安全设备等。
c) 评估实施包括以下内容：
   1) 核查网络拓扑图和系统设计文档，查看数据库服务器部署位置，是否未将数据库服务器部署在互联网访问区；
   2) 核查网络/安全设备配置，是否未将数据库服务器映射到互联网。
d) 单元判定：如果 1）～ 2）均为肯定，则符合本评估单元指标要求；如果 1）或 2）为否定，则不符合本评估单元指标要求。

5.2.4 安全计算环境

5.2.4.1 安全计算环境 01

该评估单元应按如下要求展开评估：
a) 评估指标：见 4.4 a）
b) 评估对象：系统运维人员和系统运行监测系统等。
c) 评估实施：访谈系统运维人员或核查系统运行监测系统，系统设备是否满足业务连续性需求。
d) 单元判定：如果以上测评实施内容为肯定，则符合本评估单元指标要求，否则不符合本评估单元指标要求。

5.2.4.2 安全计算环境 02

该评估单元应按如下要求展开评估：
a) 评估指标：见 4.4 b）
b) 评估对象：操作系统和数据库等。
c) 评估实施包括以下内容：
   1) 核查操作系统用户和数据库用户的权限是否已进行分离；
   2) 核查操作系统用户和数据库用户的权限是否为其工作任务所需的最小权限。
d) 单元判定：如果 1）～ 2）均为肯定，则符合本评估单元指标要求，否则不符合本评估单元指标要求。

5.2.4.3 安全计算环境 03

该评估单元应按如下要求展开评估：
a) 评估指标：见 4.4 c）
b) 评估对象：应用系统连接数据库的配置文件等。
c) 评估实施包括以下内容：
   1) 核查数据库口令存储的配置文件，数据库口令在配置文件中是否进行加密存储；
   2) 测试数据库口令加密存储后，是否无法进行解密。
d) 单元判定：如果 1）～ 2）均为肯定，则符合本评估单元指标要求，否则不符合本评估单元指标要求。

5.2.4.4 安全计算环境 04

该评估单元应按如下要求展开评估：
a) 评估指标：见 4.4 d）
b) 评估对象：安全管理员、数据库和应用程序接口配置文件等。

c) 评估实施包括以下内容：
   1) 访谈安全管理员，是否制定应用程序接口的访问控制策略；
   2) 核查应用程序接口访问控制策略，是否采用限制调用频率、白名单等措施实现应用程序接口调用的最小权限管理；
   3) 通过技术手段验证应用程序接口访问控制措施是否有效。
d) 单元判定：如果 1）～ 3）均为肯定，则符合本评估单元指标要求，否则不符合本评估单元指标要求。

5.2.4.5 安全计算环境 05

该评估单元应按如下要求展开评估：
a) 评估指标：见 4.4 e）
b) 评估对象：安全管理员，以及数据库、中间件、应用系统和网络等相关管理系统等。
c) 评估实施包括以下内容：
   1) 访谈安全管理员，是否具有数据库、中间件、应用系统和网络等相关管理系统；
   2) 查看是否限制远程访问数据库、中间件、应用系统和网络等相关管理系统的网络地址；
   3) 通过技术手段验证远程登录地址限制措施是否有效。
d) 单元判定：如果 1）为否定，本评估单元指标为不适用；1）为肯定的情况下，如果 2）～ 3）为肯定，则符合本评估单元指标要求，否则不符合本评估单元指标要求。

5.2.4.6 安全计算环境 06

该评估单元应按如下要求展开评估：
a) 评估指标：见 4.4 f）
b) 评估对象：应用系统等。
c) 评估实施包括以下内容：
   1) 核查是否采取技术措施，要求用户修改应用系统的默认口令；
   2) 通过技术手段验证是否存在默认口令。
d) 单元判定：如果 1）～ 2）均为肯定，则符合本评估单元指标要求，否则不符合本评估单元指标要求。

5.2.4.7 安全计算环境 07

该评估单元应按如下要求展开评估：
a) 评估指标：见 4.4 g）
b) 评估对象：互联网系统、应用系统开发/维护人员和第三方安全服务合同/报告等。
c) 评估实施包括以下内容：
   1) 访谈是否存在面向互联网的网站系统；
   2) 核查面向互联网的网站系统，是否通过部署网页防篡改技术措施或第三方安全服务等方式防止互联网应用被恶意篡改。
d) 单元判定：如果 1）为否定，本评估单元指标为不适用；1）为肯定的情况下，如果 2）为肯定，则符合本评估单元指标要求，否则不符合本评估单元指标要求。

5.2.5 安全管理中心

5.2.5.1 安全管理中心 01

该评估单元应按如下要求展开评估：

a) 评估指标：见 4.5 a）
b) 评估对象：安全管理平台、账户管理系统、防病毒管理系统、配置管理系统、补丁管理系统和漏洞扫描系统等。
c) 评估实施：核查是否采用支持自动化工具对系统账户、配置、漏洞、补丁和病毒库等的集中管理。
d) 单元判定：如果以上测评实施内容为肯定，则符合本评估单元指标要求，否则不符合本评估单元指标要求。

5.2.5.2 安全管理中心 02

该评估单元应按如下要求展开评估：
a) 评估指标：见 4.5 b）
b) 评估对象：网络拓扑图、网络流量监测设备、网络安全设备清单、日志综合分析平台、网络安全运营/态势/威胁感知类平台及相关设备；
c) 评估实施包括以下内容：
   1) 核查网络拓扑图，网络流量监测设备的监测范围是否覆盖每个网络区域；
   2) 核查日志综合分析平台、网络安全运营/态势/威胁感知类平台及相关设备的日志收集范围是否覆盖整个系统；
   3) 核查网络流量监测设备的功能实现和配置情况，是否能够对网络流量进行分析，是否具备异常行为检测和威胁感知能力；
   4) 核查日志综合分析平台、网络安全运营/态势/威胁感知类平台及相关设备，是否能够通过对日志和安全告警数据的集中分析，实现对网络安全攻击事件态势分析。
d) 单元判定：如果 1）～ 4）均为肯定，则符合本评估单元指标要求，否则不符合本评估单元指标要求。

5.2.6 安全管理制度

5.2.6.1 安全管理制度 01

该评估单元应按如下要求展开评估：
a) 评估指标：见 4.6 a）
b) 评估对象：网络安全保护计划/规划文件和安全管理员等。
c) 评估实施包括以下内容：
   1) 核查是否制定了网络安全保护计划；
   2) 核查网络安全保护计划是否明确了重要信息基础设施安全保护工作目标，从管理、技术和运营等方面进行规划；
   3) 核查网络安全保护计划的评估和修订记录，是否每年开展了网络安全保护计划的评估和修订。
d) 单元判定：如果 1）～3）均为肯定，则符合本评估单元指标要求，否则不符合本评估单元指标要求。

5.2.6.2 安全管理制度 02

该评估单元应按如下要求展开评估：
a) 评估指标：见 4.6 b）
b) 评估对象：网络安全策略文件等。

c) 评估实施包括以下内容：
   1) 核查是否制定了网络安全策略；
   2) 核查网络安全策略文件是否包括安全互联策略、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、供应链安全管理策略、安全运维策略等；
   3) 核查是否定期对安全策略进行评估和调整。
d) 单元判定：如果 1）～ 3）均为肯定，则符合本评估单元指标要求，否则不符合本评估单元指标要求。

5.2.6.3 安全管理制度 03

该评估单元应按如下要求展开评估：
a) 评估指标：见 4.6 c）
b) 评估对象：网络安全管理制度文件等。
c) 评估实施包括以下内容：
   1) 核查是否在等级保护基础上，制定了针对重要信息基础设施的网络安全管理制度；
   2) 核查管理制度是否覆盖风险管理、网络安全考核及监督问责、网络安全教育培训、业务连续性管理及容灾备份、三同步（安全措施同步规划、同步建设和同步使用）和供应链安全管理等方面。
d) 单元判定：如果 1）～ 2）均为肯定，则符合本评估单元指标要求，否则不符合本评估单元指标要求。

5.2.7 安全管理机构

5.2.7.1 安全组织机构 01

a) 评估指标：见 4.7 a）
b) 评估对象：网络安全组织架构文件等。
c) 评估实施包括以下内容：
   1) 核查组织架构文件或相关发文，是否成立指导和管理重要信息基础设施网络安全工作的委员会或领导小组；
   2) 核查是否指定一名首席网络安全官作为高层管理人员；
   3) 核查首席网络安全官的岗位职责，是否专职管理重要信息基础设施安全保护工作，是否允许参与重要信息基础设施重要事项决策。
d) 单元判定：如果 1）～ 3）均为肯定，则符合本评估单元指标要求，否则不符合本评估单元指标要求。

5.2.7.2 安全组织机构 02

a) 评估指标：见 4.7 b）
b) 评估对象：部门职责文件或相关发文等。
c) 评估实施：核查部门职责文件或相关发文，是否明确重要信息基础设施的网络安全管理职能部门。
d) 单元判定：如果以上测评实施内容为肯定，则符合本评估单元指标要求，否则不符合本评估单元指标要求。

5.2.7.3 安全组织机构 03

a) 评估指标：见 4.7 c）

b) 评估对象：考核和问责制度、考核记录和问责记录等。
c) 评估实施包括以下内容：
   1) 核查考核和问责制度，是否明确网络安全考核及监督问责方面的内容；
   2) 核查考核记录和问责记录，是否依据考核和问责制度文件实施考核和问责。
d) 单元判定：如果 1）～ 2）均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

5.2.7.4 安全组织机构 04

a) 评估指标：见 4.7 d）
b) 评估对象：岗位职责文件或内部正式文件等。
c) 评估实施：核查岗位职责文件或内部正式文件，是否为每个重要信息基础设施明确一名安全责任人,并明确其岗位职责。
d) 单元判定：如果以上测评实施内容为肯定，则符合本评估单元指标要求，否则不符合本评估单元指标要求。

5.2.7.5 安全组织机构 05

a) 评估指标：见 4.7 e）
b) 评估对象：项目管理制度、项目建设及实施文档等。
c) 评估实施包括以下内容：
   1) 核查项目管理制度，是否要求安全管理责任人参与本组织重要信息基础设施的信息化决策；
   2) 核查项目建设及实施文档，安全管理责任人是否在信息化项目立项、方案设计、方案评审、项目验收等环节参与决策。
d) 单元判定：如果 1）～ 2）均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

5.2.8 安全管理人员

5.2.8.1 安全管理人员 01

a) 评估指标：见 4.8 a）
b) 评估对象：人员安全管理文档和人员背景审查记录等。
c) 评估实施包括以下内容：
   1) 核查人员安全管理文档,是否要求对重要信息基础设施安全管理机构的负责人和关键岗位人员在上岗前实施背景审查，包括：在履行岗位职责前；相关人员的身份、国籍、安全背景和家庭情况等发生变化时；岗位发生重大变化或其他必要情况下；
   2) 核查是否具有背景审查记录，记录是否包括审查内容和审查结果等。
d) 单元判定：如果 1）～ 2）均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

5.2.8.2 安全管理人员 02

a) 评估指标：见 4.8 b）
b) 评估对象：网络安全培训制度和网络安全培训记录等。
c) 评估实施包括以下内容：

1) 核查网络安全培训制度，是否要求针对重要信息基础设施相关人员提供安全意识教育和安全技能培训；
2) 核查网络安全培训记录文档，相关人员的年度网络安全培训时长是否不少于 15 个学时，在此基础上，网络安全岗位人员的专业技能年度培训时长是否不少于 15 个学时，其中是否包括数据安全相关培训。

d) 单元判定：如果 1）～ 2）均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

5.2.8.3 安全管理人员 03

a) 评估指标：见 4.8 c）
b) 评估对象：安全保密制度和安全保密协议等。
c) 评估实施包括以下内容：
   1) 核查安全保密制度，是否明确重要信息基础设施相关人员的安全保密职责和义务；
   2) 核查安全保密协议，安全保密协议中是否约定安全职责、奖惩机制、离岗后的脱密期限等。
d) 单元判定：如果 1）～ 2）均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

5.2.9 供应链安全

5.2.9.1 供应链安全 01

该评估单元应按如下要求展开评估：

a) 评估指标：见 4.9 a）
b) 评估对象：供应链安全管理人员和供应链安全管理策略相关文档等。
c) 评估实施包括以下内容：
   1) 访谈供应链安全管理人员，是否建立了供应链安全管理策略；
   2) 核查供应链安全管理策略相关文档，是否包含风险管理策略、供应方选择和管理策略、产品开发采购策略、安全维护策略等。
d) 单元判定：如果 1）～ 2）均为肯定，则符合本评估单元指标要求，否则不符合本评估单元指标要求。

5.2.9.2 供应链安全 02

该评估单元应按如下要求展开评估：

a) 评估指标：见 4.9 b）
b) 评估对象：供应链安全管理人员和供应商安全管理制度等。
c) 评估实施包括以下内容：
   1) 访谈供应链安全管理人员，是否建立了供应链管理制度；
   2) 核查供应链管理制度，是否包含供应商资质审核、供应商分类分级、供应商不良行为处置等方面的管理要求。
d) 单元判定：如果 1）～ 2）均为肯定，则符合本评估单元指标要求，否则不符合本评估单元指标要求。

5.2.9.3 供应链安全 03

该评估单元应按如下要求展开评估：

a) 评估指标：见 4.9 c）

b) 评估对象：供应链安全管理人员、采购的网络产品和服务清单等。
c) 评估实施包括以下内容：
   1) 访谈供应链安全管理人员，是否建立了年度采购的网络产品和服务清单；
   2) 核查年度采购的网络产品和服务清单，所采购、使用的网络产品和服务是否符合国家及行业合规要求。
d) 单元判定：如果 1）～ 2）为肯定，则符合本评估单元指标要求，否则不符合本评估单元指标要求。

5.2.9.4 供应链安全 04

该评估单元应按如下要求展开评估：
a) 评估指标：见 4.9 d）
b) 评估对象：软件供应链安全风险管理文档、软件供应链产品风险评估记录和安全风险事件响应制度等。
c) 评估实施包括以下内容：
   1) 核查软件供应链安全风险管理文档，是否包含软件供应链安全风险持续监测、风险评估和事件响应制度；
   2) 核查软件供应链产品风险评估记录，是否对软件供应链安全风险进行持续监测和风险评估；
   3) 核查安全风险事件响应制度，是否明确了不同等级安全事件的报告、处置、响应和流程机制，是否规定了安全事件的现场处置、事件报告和后期恢复等要求。
d) 单元判定：如果 1）～ 3）均为肯定，则符合本评估单元指标要求，否则不符合本评估单元指标要求。

5.2.9.5 供应链安全 05

该评估单元应按如下要求展开评估：
a) 评估指标：见 4.9 e）
b) 评估对象：采购管理制度，网络产品和服务采购合同与合同模板等。
c) 评估实施包括以下内容：
   1) 核查采购管理制度，是否要求在采购网络产品和服务时，在合同中明确提供者的安全责任和义务；
   2) 核查现已签订的网络产品和服务采购合同与合同模板，是否明确了提供者的安全责任和义务，要求提供者对网络产品和服务的设计、研发、生产和交付等关键环节加强安全管理，要求提供者声明不非法获取用户数据、控制和操纵用户的系统和设备，或利用用户对产品的依赖性谋取不正当利益或者迫使用户更新换代。
d) 单元判定：如果 1）～ 2）均为肯定，则符合本评估单元指标要求，否则不符合本评估单元指标要求。

5.2.9.6 供应链安全 06

该评估单元应按如下要求展开评估：
a) 评估指标：见 4.9 f）
b) 评估对象：供应商安全管理制度、安全保密协议与安全协议模板等。
c) 评估实施包括以下内容：
   1) 核查供应商安全管理制度，是否要求与网络产品和服务的提供者签订安全保密协议；

2） 核查安全保密协议与安全协议模板，是否包括安全职责、保密内容、奖惩机制和有效期等内容。

d） 单元判定：如果 1）～ 2）均为肯定，则符合本评估单元指标要求，否则不符合本评估单元指标要求。

5.2.9.7 供应链安全 07

该评估单元应按如下要求展开评估：

a） 评估指标：见 4.9 g）

b） 评估对象：安全管理员和云计算服务采购合同等。

c） 评估实施：

1） 访谈安全管理员，是否采购公有云服务；

2） 核查云计算服务采购合同，云服务商是否通过了国家云计算服务安全评估。

d） 单元判定：如果 1）为否定，本评估单元指标为不适用；1）为肯定的情况下，如果 2）为肯定，则符合本评估单元指标要求，否则不符合本评估单元指标要求。

5.2.9.8 供应链安全 08

该评估单元应按如下要求展开评估：

a） 评估指标：见 4.9 h）

b） 评估对象：供应商安全管理制度和授权策略等。

c） 评估实施包括以下内容：

1） 核查供应商安全管理制度，是否建立严格的授权机制；

2） 核查授权策略，是否要求操作系统、数据库等最高管理员权限应由本单位人员专人负责，是否要求按照最小必要原则对外包单位人员进行精细化授权,在授权期满后是否及时收回权限。

d） 单元判定：如果 1）～ 2）均为肯定，则符合本评估单元指标要求，否则不符合本评估单元指标要求。

5.2.10 数据安全

5.2.10.1 数据安全 01

该评估单元应按如下要求展开评估：

a） 评估指标：见 4.10 a）

b） 评估对象：数据安全管理责任文件、评价考核制度和数据安全保护计划等相关文档。

c） 评估实施包括以下内容：

1） 核查数据安全管理责任文件，是否明确了数据安全管理责任人；

2） 核查数据安全评价考核制度，是否明确了数据安全相关考核评价内容；

3） 核查数据安全保护计划，是否明确了工作目标,管理和技术措施等。

d） 单元判定：如果 1）～ 3）均为肯定，则符合本评估单元指标要求，否则不符合本评估单元指标要求。

5.2.10.2 数据安全 02

该评估单元应按如下要求展开评估：

a） 评估指标：见 4.10 b）

b） 评估对象：信息化项目关键环节的记录表单等文档。

c） 评估实施包括以下内容：
1） 核查是否明确数据安全管理责任人参与本组织重要信息基础设施的信息化决策；
2） 核查项目建设及实施文档，数据安全管理责任人是否在信息化项目立项、方案设计、方案评审、项目验收等环节参与决策。
d） 单元判定：如果 1）～ 2）均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

5.2.10.3 数据安全 03

该评估单元应按如下要求展开评估：
a） 评估指标：见 4.10 c）
b） 评估对象：数据分类分级相关文档和数据资产目录等。
c） 评估实施包括以下内容：
1） 核查是否基于国家标准、行业标准以及业务需求制定数据分类分级相关制度；
2） 核查是否建立数据资产目录。
d） 单元判定：如果 1）～ 2）均为肯定，则符合本评估单元指标要求，否则不符合本评估单元指标要求。

5.2.10.4 数据安全 04

该评估单元应按如下要求展开评估：
a） 评估指标：见 4.10 d）
b） 评估对象：数据安全保护策略相关文件等。
c） 评估实施：核查是否根据数据分类分级方法制定数据安全保护策略，策略中是否明确了重要数据和个人信息在数据处理的关键环节中的安全保护要求。
d） 单元判定：如果以上测评实施内容为肯定，则符合本评估单元指标要求，否则不符合本评估单元指标要求。

5.2.10.5 数据安全 05

该评估单元应按如下要求展开评估：
a） 评估指标：见 4.10 e）
b） 评估对象：数据库表、数据文件、应用系统、设计文档和建设文档等。
c） 评估实施：核查是否采取技术手段（如加密、脱敏、去标识化等）保护个人敏感信息安全。
d） 单元判定：如果以上测评实施内容为肯定，则符合本评估单元指标要求，否则不符合本评估单元指标要求。

5.2.10.6 数据安全 06

该评估单元应按如下要求展开评估：
a） 评估指标：见 4.10 f）
b） 评估对象：应用系统等。
c） 评估实施：核查应用系统，对于敏感数据是否采用数字水印等技术，以辅助追踪数据泄露源头。
d） 单元判定：如果以上测评实施内容为肯定，则符合本评估单元指标要求，否则不符合本评估单元指标要求。

5.2.10.7 数据安全 07

该评估单元应按如下要求展开评估：

a) 评估指标：见 4.10 g）
b) 评估对象：数据安全管理制度和数据处置记录表单类文档。
c) 评估实施包括以下内容：
   1) 核查数据安全管理制度，是否针对重要信息基础设施退役废弃制定了数据处置策略；
   2) 核查是否具有重要信息基础设施退役废弃时的数据处置记录。
d) 单元判定：如果 1）～ 2）均为肯定，则符合本评估单元指标要求，否则不符合本评估单元指标要求。

5.2.10.8 数据安全 08

该评估单元应按如下要求展开评估：

a) 评估指标：见 4.10 h）
b) 评估对象：数据安全风险评估报告和数据安全整改记录或方案等。
c) 评估实施包括以下内容：
   1) 核查是否具备数据安全风险评估报告；
   2) 核查数据安全整改记录和方案等相关文档，是否对未落实数据安全保护策略的情况及时整改。
d) 单元判定：如果 1）为否定，本评估单元指标为不符合；如果 1）～ 2）均为肯定，则符合本评估单元指标要求，否则不符合本评估单元指标要求。

5.2.10.9 数据安全 09

该评估单元应按如下要求展开评估：

a) 评估指标：见 4.10 i）
b) 评估对象：应急预案、应急演练记录和报告等文档。
c) 评估实施包括以下内容：
   1) 核查是否制定了数据安全事件应急预案；
   2) 核查是否有定期开展应急演练的记录和报告。
d) 单元判定：如果 1）～ 2）均为肯定，则符合本评估单元指标要求，否则不符合本评估单元指标要求。

5.2.11 安全运营

5.2.11.1 资产识别 01

该评估单元应按如下要求展开评估：

a) 评估指标：见 4.11.1 a）
b) 评估对象：安全管理员、资产信息清单和资产管理系统等。
c) 评估实施包括以下内容：
   1) 访谈安全管理员，是否建立了重要信息基础设施资产信息清单；
   2) 核查资产信息清单或资产管理系统，资产是否覆盖了评估对象涉及的物理设备、虚拟设备、操作系统、数据库、中间件、应用软件、业务系统等；
   3) 核查资产信息清单或资产管理系统，资产信息是否至少包括资产名称、资产类别、资产型号或版本、网络地址、用途、数量、所处位置、资产责任人、资产防护优先级等。

d) 单元判定：如果 1）～ 3）均为肯定，则符合本评估单元指标要求，否则不符合本评估单元指标要求。

5.2.11.2 资产识别 02

该评估单元应按如下要求展开评估：

a) 评估指标：见 4.11.1 b）
b) 评估对象：安全管理员、资产信息清单和资产识别系统等。
c) 评估实施包括以下内容：
   1) 访谈安全管理员，是否采用资产探测等技术手段定期识别和更新资产清单；
   2) 核查资产信息清单或资产识别系统，是否实现资产的动态更新。
d) 单元判定：如果 1）～ 2）均为肯定，则符合本评估单元指标要求，否则不符合本评估单元指标要求。

5.2.11.3 检测评估 01

该评估单元应按如下要求展开评估：

a) 评估指标：见 4.11.2 a）
b) 评估对象：安全管理员和安全管理制度文件等。
c) 评估实施包括以下内容：
   1) 访谈安全管理员，是否建立了重要信息基础设施安全检测评估制度或者相关要求；
   2) 核查安全检测评估制度，是否明确重要信息基础设施安全检查评估的工作流程、方式方法和周期等内容。
d) 单元判定：如果 1）～ 2）均为肯定，则符合本评估单元指标要求，否则不符合本评估单元指标要求。

5.2.11.4 检测评估 02

该评估单元应按如下要求展开评估：

a) 评估指标：见 4.11.2 b）
b) 评估对象：安全管理员、安全检测评估报告和问题整改报告等。
c) 评估实施包括以下内容：
   1) 核查安全检测评估报告，是否按年开展安全检测评估工作；
   2) 核查问题整改报告或者整改记录文件，是否对检测评估发现的问题制定了整改方案和整改计划，并及时整改。
d) 单元判定：如果 1）～ 2）均为肯定，则符合本评估单元指标要求，否则不符合本评估单元指标要求。

5.2.11.5 检测评估 03

该评估单元应按如下要求展开评估：

a) 评估指标：见 4.11.2 c）
b) 评估对象：安全管理员、安全检测评估报告、重要信息系统基础设施建设相关文件、安全整改报告或者记录文件等。
c) 评估实施包括以下内容：
   1) 访谈安全管理员，本单位重要信息基础设施是否存在新建、改建和扩建的情况；

2） 核查新建、改建或者扩建的重要信息基础设施安全检测评估报告和相关文件，查看其是否在上线前开展了检测评估、安全整改；

d） 单元判定：如果 1）为否定，本评估单元指标为不适用；1）为肯定的情况下，如果 2）为肯定，则符合本评估单元指标要求，否则不符合本评估单元指标要求。

5.2.11.6 检测评估 04

该评估单元应按如下要求展开评估：

a） 评估指标：见 4.11.2 d）

b） 评估对象：安全管理员、攻防演练计划和攻防演练报告等。

c） 评估实施包括以下内容：

1） 访谈安全管理员，是否定期开展攻防演练工作，且保证至少每年一次；

2） 查看攻防演练计划或者攻防演练报告，攻防演练的内容是否包括对实际网络攻击的防护情况，以及防守方的应急响应能力。

d） 单元判定：如果 1）～ 2）均为肯定，则符合本评估单元指标要求，否则不符合本评估单元指标要求。

5.2.11.7 检测评估 05

该评估单元应按如下要求展开评估：

a） 评估指标：见 4.11.2 e）

b） 评估对象：网络安全专题演练文件和安全培训记录等。

c） 评估实施包括以下内容：

1） 核查网络安全演练文件，是否至少半年开展一次钓鱼攻击演练工作；

2） 核查安全培训记录，是否对容易被社会工程学攻击的部门和员工进行了重点培训。

d） 单元判定：如果 1）～ 2）均为肯定，则符合本评估单元指标要求，否则不符合本评估单元指标要求。

5.2.11.8 检测评估 06

该评估单元应按如下要求展开评估：

a） 评估指标：见 4.11.2 f）

b） 评估对象：安全管理员、安全风险检测或者安全专项检查工作报告、整改方案或者记录等。

c） 评估实施包括以下内容：

1） 访谈安全管理员，本单位是否配合安全主管部门的安全风险检测和安全专项检查工作；

2） 核查整改方案或者记录，是否针对发现的安全隐患和风险建立了整改清单，并根据整改清单制定方案，并查看整改记录是否按照要求实施了整改工作。

d） 单元判定：如果 1）～ 2）均为肯定，则符合本评估单元指标要求，否则不符合本评估单元指标要求。

5.2.11.9 监测预警 01

该评估单元应按如下要求展开评估：

a） 评估指标：见 4.11.3 a）

b） 评估对象：安全管理员、安全制度类文档和记录表单类文档等。

c） 评估实施包括以下内容：

1） 核查安全制度类文档，是否建立监测预警和信息通报制度，并且明确了分级别的信息报告和响应处置程序；
2） 核查常态化监测预警和快速应急响应执行记录文件，是否按照建立的机制开展相关工作。

d） 单元判定：如果 1）～ 2）均为肯定，则符合本评估单元指标要求，否则不符合本评估单元指标要求。

5.2.11.10 监测预警 02

该评估单元应按如下要求展开评估：

a） 评估指标：见 4.11.3 b）
b） 评估对象：安全管理员、安全制度类文档和记录表单类文档等。
c） 评估实施包括以下内容：
1） 访谈安全管理员，是否建立了与行业主管部门和监管部门的网络安全信息共享机制；
2） 核查安全管理制度类文件、行业主管和监管部门联系记录表、工作沟通过程文档，是否开展了网络安全信息共享工作；
3） 核查网络安全共享信息是否包括漏洞信息、威胁信息、最佳实践和前沿技术等；
4） 核查对漏洞信息的共享是否符合国家关于漏洞管理制度的要求。
d） 单元判定：如果 1）～ 4）均为肯定，则符合本评估单元指标要求，否则不符合本评估单元指标要求。

5.2.11.11 监测预警 03

该评估单元应按如下要求展开评估：

a） 评估指标：见 4.11.3 c）
b） 评估对象：安全管理员、应急预案类文档和记录表单类文档等。
c） 评估实施包括以下内容：
1） 访谈安全管理员是否接收行业主管部门和监管部门的安全预警，并及时响应；
2） 核查应急预案类文档是否具有对行业主管部门和监管部门安全预警的管理和处置要求，明确要求分析、研判事件或威胁对自身网络安全保护对象可能造成损害的程度，以及启动应急预案的条件，是否按照规定将获取的安全预警信息按照规定通报给相关人员和相关部门；
3） 核查记录表单类文档是否按照要求执行安全预警、应急响应和预警通告工作。
d） 单元判定：如果 1）～ 3）均为肯定，则符合本评估单元指标要求，否则不符合本评估单元指标要求。

5.2.11.12 应急演练 01

该评估单元应按如下要求展开评估：

a） 评估指标：见 4.11.4 a）
b） 评估对象：应急预案及相关文档等。
c） 评估实施包括以下内容：
1） 核查网络安全应急预案，是否包含特殊时期的应急响应流程；
2） 核查是否具有针对特殊时期的应急演练或应急响应记录文档。
d） 单元判定：如果 1）～ 2）均为肯定，则符合本评估单元指标要求，否则不符合本评估单元指标要求。

5.2.11.13 应急演练 02

该评估单元应按如下要求展开评估：

a) 评估指标：见 4.11.4 b）
b) 评估对象：应急演练方案和应急演练报告等。
c) 评估实施：核查应急演练方案和应急演练报告，是否定期围绕业务的可持续性设定演练场景，组织开展应急演练工作。
d) 单元判定：如果以上测评实施内容为肯定，则符合本评估单元指标要求，否则不符合本评估单元指标要求。

5.2.11.14 事件处置 01

该评估单元应按如下要求展开评估：

a) 评估指标：见 4.11.5 a）
b) 评估对象：安全管理员和应急预案等。
c) 评估实施：核查应急预案，是否明确了事件处置的组织和技术支撑。
d) 单元判定：如果以上测评实施内容为肯定，则符合本评估单元指标要求，否则不符合本评估单元指标要求。

5.2.11.15 事件处置 02

该评估单元应按如下要求展开评估：

a) 评估指标：见 4.11.5 b）
b) 评估对象：安全管理员、事件处置记录和应急预案等。
c) 评估实施包括以下内容：
   1) 核查应急预案，是否建立了安全事件通报机制，是否明确了通报的相关部门、人员及相关方；
   2) 核查是否有事件处置相关的执行记录。
d) 单元判定：如果 1）～ 2）均为肯定，则符合本评估单元指标要求，否则不符合本评估单元指标要求。

5.2.11.16 事件处置 03

该评估单元应按如下要求展开评估：

a) 评估指标：见 4.11.5 c）
b) 评估对象：年度网络安全监测预警和事件处置报告等。
c) 评估实施包括以下内容：
   1) 核查是否形成年度网络安全监测预警和事件处置报告；
   2) 核查是否具有报告上报的记录。
d) 单元判定：如果 1）～ 2）均为肯定，则符合本评估单元指标要求，否则不符合本评估单元指标要求。

5.3 安全评估结果的形成规则

安全评估结果以安全保护能力等级表示，安全保护能力等级根据评估对象符合率、等级保护测评结论以及安全漏洞存在情况综合评价为优、良、中、差，表1给出了安全保护能力等级判定依据。

表 1 安全保护能力等级判定依据

安全保护能力等级	优	良	中	差
评价依据	符合率[a]≥90%，且等级保护测评结论为符合，且不存在高风险安全问题	80%≤符合率<90%，且等级保护测评结论为符合或基本符合，且不存在高风险安全问题	60%≤符合率<80%，且等级保护测评结论为符合或基本符合，且不存在高风险安全问题	符合率<60%，或等级保护测评结论为不符合，或存在高风险安全问题

[a] $符合率 = \frac{符合的评估单元总数}{评估单元总数-不适用评估单元数} \times 100\%$

参 考 文 献

[1] GB/T 20984—2022 信息安全技术 信息安全风险评估方法
[2] GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求
[3] GB/T 28448—2019 信息安全技术 网络安全等级保护测评要求
[4] GA/T 2182—2024 信息安全技术 关键信息基础设施安全测评要求
[5] GB/T 30285—2013 信息安全技术 灾难恢复中心建设与运维管理规范
[6] GB/T 31506—2022 信息安全技术 政务网站系统安全指南
[7] GB/T 45577—2025 数据安全技术 数据安全风险评估方法
[8] GB/T 37046—2018 信息安全技术 灾难恢复能力评估准则