ICS 35.030
CCS M 10

团　　体　　标　　准

T/ISC 0165—2026

工业互联网安全服务机构能力评价准则

Evaluation criteria for capabilities of industrial internet security service organiztions

（发布稿）

2026－10－28 发布　　2026－11－28 实施

中 国 互 联 网 协 会　　发布

目　　次

前　　言 2
1 范围 3
2 规范性引用文件 3
3 术语和定义 3
3.1 工业互联网 3
4 能力评价概述 3
5 能力评价等级 3
6 能力认定要求 4
6.1 基本条件 4
6.2 组织管理要求 4
6.3 人员素质与资质要求 5
6.4 技术能力要求 5
6.5 评估经验及业绩能力要求 6
6.6 项目管理要求 6
6.7 质量管理要求 7
参　考　文　献 8

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。

本文件由中国互联网协会归口。

本文件起草单位：中国信息通信研究院、中国电子信息产业集团公司第六研究所、西安热工研究院有限公司、江苏天创科技有限公司

本文件主要起草人：赵爽、柯皓仁、李艺、马娟、于广琛、江浩洁、董悦、杨冬梅、章永春、张亚宁、王晔、靳方略、邓楠轶、董夏昕、朱博迪、徐昊、赵历、彭高

工业互联网安全服务机构能力评价准则

1 范围

本文件规定了工业互联网安全服务机构的能力衡量与评价标准，对基本条件、组织管理、人员素质与资质、技术能力、评估经验及业绩能力、项目管理、质量管理等方面做出基线要求和细化明确。

本文件适用于工业互联网安全服务机构的能力评价认定。

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 25069 信息安全技术 术语

GB/T 42021 工业互联网 总体网络架构

3 术语和定义

GB/T 25069和GB/T 42021界定的以及下列术语和定义适用于本文件。

3.1

工业互联网

新一代信息通信技术与工业经济深度融合的新型基础设施、应用模式和工业形态，通过对人、机、物、系统等的全面连接，构建起覆盖全产业链、全价值链的全新制造和服务体系。

[来源：GB/T 42021-2022，3.1]

4 能力评价概述

工业互联网安全服务机构能力评价是对工业互联网安全服务机构的客观评价，直接反应了工业互联网安全服务机构的服务资格、技术能力和管理能力。

工业互联网安全服务机构能力评价准则是对工业互联网安全服务机构的基本条件、组织管理、人员素质与资质、技术能力、评估经验及业绩能力、项目管理、质量管理共七个维度的具体衡量和评价。

5 能力评价等级

工业互联网安全服务机构能力等级由低到高分为一级、二级、三级三个级别。在本文件中，高等级能力的评价要求涵盖了低等级能力评价要求的所有方面，符合较高等级能力评价要求时，可不经通过较低能力等级的评价，直接申请较高等级的能力评价。

符合能力评价要求中所有三级条款要求，可申请评价为三级工业互联网安全服务机构。符合能力评价要求中所有二级条款要求，可申请评价为二级工业互联网安全服务机构。符合能力评价要求中所有一级条款要求，可申请评价为一级工业互联网安全服务机构。

工业互联网安全服务机构在取得能力评价结果之后，应维持满足本等级所述的相关要求。如未达到要求的，能力评价评审机构将做出降低能力评价等级、暂停或撤销能力评价结果的决定。

6 能力认定要求

6.1 基本条件

申请工业互联网安全服务能力评价的服务机构应具备的基本条件包括：

a) 在中华人民共和国境内注册（港澳台地区除外），由中国公民、法人或国家投资的企事业单位；
b) 产权明晰，注册资金100万元以上，独立核算，无违法违规记录；
c) 机构主要负责人、服务人员均为中国公民，无犯罪记录；
d) 具备固定办公场所；
e) 原则上不从事网络安全产品开发销售、安全集成等可能影响公正性的业务（自用除外）。

6.2 组织管理要求

6.2.1 一级

a) 具有专门从事工业互联网安全服务的部门或团队；
b) 建立人员管理程序，明确服务岗位与职责；
c) 具有专门制定和宣贯保密制度的部门或团队，对项目实施过程中涉及处理商业秘密信息的全过程有明确且行之有效的控制手段；
d) 具有相关投诉服务制度、应急响应服务制度并妥善执行。

6.2.2 二级

a) 具有专门从事工业互联网安全服务职责的部门或团队需成立3年以上；
b) 建立人员管理程序，明确服务岗位与职责；
c) 具有专门制定和宣贯保密制度的部门或团队，对项目实施过程中涉及处理商业秘密信息的全过程有明确且行之有效的控制手段；
d) 具有相关投诉服务流程、应急响应服务流程并妥善执行。

6.2.3 三级

a) 具有专门从事工业互联网安全服务职责的部门或团队需成立5年以上；
b) 建立人员管理程序，明确服务岗位与职责；
c) 具有专门制定和宣贯保密制度的部门或团队，对项目实施过程中涉及处理商业秘密信息的全过程有明确且行之有效的控制手段；
d) 具有相关投诉服务流程、应急响应服务流程并妥善执行。

6.3 人员素质与资质要求

6.3.1 一级

a) 了解国内外工业互联网安全情况、网络安全法律法规要求、安全保障机制，承接过网络安全相关服务项目或撰写过网络安全相关研究报告；
b) 从事工业互联网安全相关工作人员至少15名，相关人员应取得工业互联网安全相关证书，其中高级人员不少于1人，中级人员不少于5人；
c) 专职从事工业互联网安全评估的人员定期参加培训。每年保证不少于20学时，有人员、学时、日期、课程名称等详细过程记录。

6.3.2 二级

a) 了解国内外工业互联网安全情况、网络安全法律法规要求、安全保障机制，承接过网络安全相关服务项目或撰写过网络安全相关研究报告；
b) 从事工业互联网安全相关工作人员至少20名，相关人员应取得工业互联网安全相关证书，其中高级人员不少于1人，中级人员不少于8人；
c) 专职从事工业互联网安全评估的人员定期参加培训。每年保证不少于30学时，有人员、学时、日期、课程名称等详细过程记录。

6.3.3 三级

a) 了解国内外工业互联网安全情况、网络安全法律法规要求、安全保障机制，承接过网络安全相关服务项目或撰写过网络安全相关研究报告；
b) 从事工业互联网安全相关工作人员至少25名，相关人员应取得工业互联网安全相关证书，其中高级人员不少于1人，中级人员不少于10人；
c) 专职从事工业互联网安全评估的人员定期参加培训。每年保证不少于40学时，有人员、学时、日期、课程名称等详细过程记录。

6.4 技术能力要求

6.4.1 一级

a) 具备开展工业互联网安全服务所需的研发或模拟测试环境，通过实物或虚拟界面模拟的方式，对研发或测试效果进行直观呈现；
b) 具备开展工业互联网安全服务所需的设备或软件，包括但不限于符合性评测工具、漏洞扫描工具、渗透测试工具等；
c) 具备切实可行的应急服务方案，包括但不限于事件监测与报告机制、应急响应流程、隔离止损与恢复措施等。

6.4.2 二级

a) 具备面向不少于3个行业开展工业互联网安全服务所需的研发或模拟测试环境，通过实物或虚拟界面模拟的方式，对研发或测试效果进行直观呈现；
b) 具备开展工业互联网安全服务所需的设备或软件，包括但不限于符合性评测工具、漏洞扫描工具、渗透测试工具等；

c） 具备切实可行的应急服务方案，包括但不限于事件监测与报告机制、协调联动机制、应急响应流程、隔离止损与恢复措施等。

6.4.3 三级

a） 具备面向不少于5个行业开展工业互联网安全服务所需的研发或模拟测试环境，通过实物或虚拟界面模拟的方式，对研发或测试效果进行直观呈现；
b） 具备开展工业互联网安全服务所需的设备或软件，包括但不限于符合性评测工具、漏洞扫描工具、渗透测试工具等；
c） 具备切实可行的应急服务方案，包括但不限于事件监测与报告机制、协调联动机制、应急响应流程、隔离止损与恢复措施等。

6.5 评估经验及业绩能力要求

6.5.1 一级

a） 具备1年以上的工业互联网安全评估业务实践经验；
b） 具有3次以上工业互联网安全评估服务经验，且项目终验通过；
c） 近3年没有出现因各阶段验收未通过或机构自身原因而废止的工业互联网安全评估服务项目。

6.5.2 二级

a） 具备3年以上的工业互联网安全评估业务实践经验；
b） 近3年间具有5次以上工业互联网安全评估服务经验，且项目终验通过；
c） 近3年没有出现因各阶段验收未通过或机构自身原因而废止的工业互联网安全评估服务项目。

6.5.3 三级

a） 具备5年以上的工业互联网安全评估业务实践经验；
b） 近3年间具有10次以上工业互联网安全评估服务经验，且项目终验通过；
c） 承接过行业主管部门委托的工业互联网安全评估相关任务；
d） 近3年没有出现因各阶段验收未通过或机构自身原因而废止的工业互联网安全评估服务项目。

6.6 项目管理要求

6.6.1 一级

a） 具备符合相关项目管理标准的工业互联网安全评估项目管理办法，在项目执行过程中能有效控制质量、进度，提供符合客户预期的评估服务；
b） 项目管理过程记录完整、可追溯。

6.6.2 二级

a） 具有工业互联网安全评估项目管理体系，建立项目管理机制，配备专职人员推广培训项目管理知识，有专职人员负责项目具体执行；
b） 项目管理体系应明确划分组织结构、人员职责与权利，明晰项目管理流程与要求，确保整体过程安全可控，记录准确、有效、可追溯。

6.6.3 三级

a) 具备完善的工业互联网安全评估项目管理制度，对立项、审批过程进行明确规定，有专职部门或人员实行规范管理；
b) 项目管理制度应包含设立项目实施流程与标准，明确建立项目管理计划，在项目实施过程中执行进度管理、质量管理、变更管理、风险管理、文档管理等实践要求；
c) 落实项目管理制度应确保记录完整、清晰可查，包括但不限于会议记录、过程文档等资料。

6.7 质量管理要求

6.7.1 一级

a) 应指定专职或兼职质量责任人，制定并发布质量管理办法或服务规范，明确质量目标；
b) 每年应开展不少于一次服务质量自评估，重点检查评估流程是否符合基本规范、核心文档是否完整，评估结果记录在案，列出不足项；
c) 应建立服务产品质量监控清单，并对关键交付物进行内部审查。

6.7.2 二级

a) 应设立专职质量管理部门或明确质量负责人，建立覆盖项目全生命周期的质量保证体系；
b) 每年应组织不少于2次质量管理培训，培训内容涵盖工业互联网安全评估相关规范、文档编写、风险识别、沟通协作等；
c) 应建立客户满意度收集机制，每个评估项目结束后主动获取反馈，将反馈意见纳入下一次服务改进的参考依据。

6.7.3 三级

a) 应设立专职质量管理部门或明确质量负责人，建立覆盖项目全生命周期的质量保证体系；
b) 每年应组织不少于2次质量管理培训，培训内容涵盖工业互联网安全评估相关规范、文档编写、风险识别、沟通协作等；
c) 应针对每个项目进行风险等级划分，针为高风险项目制定动态质量控制方案，针对关键控制点进行预警提醒和动态调整，确保在项目变更、环境迭代时仍能保质交付；
d) 应建立客户满意度收集机制，每个评估项目结束后主动获取反馈，将反馈意见纳入下一次服务改进的参考依据。

参 考 文 献

[1] GB/T 45389-2025 数据安全技术 数据安全评估机构能力要求
[2] YD/T 3503-2019 互联网新技术新业务安全评估服务机构能力认定准则