ICS 35.240
L80

团　　体　　标　　准

T/××× ××××—××××

能源企业数字化转型能力评价
安全防护能力评价

Evaluation for digital transformation capabilities of energy enterprises
Evaluation for Capability of security protection

（征求意见稿）

XXXX-XX-XX 发布　　XXXX-XX-XX 实施

中国能源研究会　　发布

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》给出的规则编制。

本文件由中国能源研究会归口。

本文件起草单位：中国电力科学研究院有限公司、国家能源集团数据中心、北京理工大学、华北电力大学。

本文件主要起草人：张姗、张道娟、戴聿雯、胡云卿、余勇、张涛、王文辉、韩龙玺、张英杰、陈凯、吴天琦、赵宇飞、高雪芹、韩啸、武宏斌、王玉曼、费克雄、白晓雪、张悦。

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国能源研究会。

能源企业数字化转型能力评价 安全防护

1 范围

本文件规定了能源企业数字化转型安全防护能力的评价要求和方法，包括安全体系、安全技术、安全运营等。

本文件适用于能源企业自我评价及第三方服务机构开展安全防护能力评价。评价结果作为制度落实的印证以及隐患整改的依据。

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 5271 信息技术 词汇

GB/T 25069—2022 信息安全技术术语

T/CERS 0006—2023 能源企业数字化转型能力评价导则

3 术语和定义

GB/T 5271、GB/T 25069—2022、T/CERS 0006—2023界定的以及下列术语和定义适用于本文件。

3.1

能源企业 energy enterprise

从事电力、石油石化、煤炭、燃气、新能源、核能等主营业务的企业，或支撑以上主营业务开展的咨询、相关设备制造等服务的企业。

3.2

安全防护能力 security protection capability

指为应对数字化转型带来的各种安全风险和威胁所展现出的综合防护水平与效能，涵盖技术手段运用、管理制度完善及人员安全意识提升等方面。

4 缩略语

下列缩略语适用于本文件。

IaaS：基础设施服务（Infrastructure as a service）

PaaS：平台服务（Platform as a service）

SaaS：软件服务（Software as a service）

5 评价指标

5.1 指标体系

能源企业数字化转型安全防护能力评价指标体系包含一级指标三个、二级指标十四个，如图1所示。

5.1.1 一级指标

一级指标包括安全体系、安全技术、安全运营等三个方面。

5.1.2 二级指标

能源企业数字化转型安全防护能力评价二级指标共十四个。

a）安全体系评价包括安全机制、人员管理、安全建设、人才培养等四个方面。

b）安全技术评价包括态势感知能力、安全基础资源库、工控安全、数据安全、云平台安全、密码应用、新技术应用等七个方面。

c）安全运营评价包括安全运维、实战运营、运营效率等三个方面。

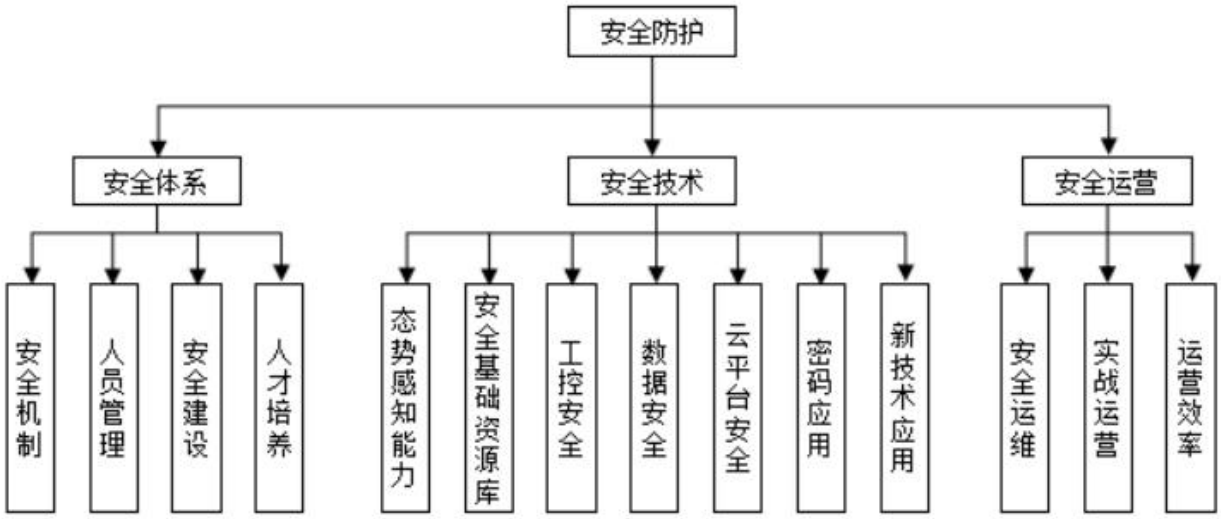

图 1 安全防护能力评价指标

5.2 评价内容

5.2.1 安全体系

5.2.1.1 安全机制

评价内容如下：

a) 优化网络安全管理体系，落实主体责任，健全安全制度，强化考核监督，应对数字化转型带来的组织和管理架构变化，为实现更高水平安全提供有力的制度体系保障；

b) 坚持源头防范和预防为主，健全数字安全防护体系，优化网络安全架构，构建覆盖业务全生命周期的“预警、监测、响应”纵深防御体系，增强企业数字化转型中应对各类网络安全风险的能力；

c) 制定网络安全防控整体策略，通过攻防演习、安全检查、风险评估等方式，综合排查分析数字化转型过程中公司面临的网络安全新风险；完善风险分级管控和隐患排查治理工作机制；

d) 制定相关方案，推进传统信息系统网络安全动态防护、云安全防护、大数据安全防护、物联网安全防护、移动安全防护、工业控制系统安全防护升级；
e) 建立健全网络安全审查机制，依法依规对供应商、安全方案、产品和服务等进行严格审查，提高产品和服务的安全性可控性。

5.2.1.2 人员管理

评价内容如下：

a) 加强人员录用、人员离岗、外部人员访问管理；
b) 定期组织安全意识教育与培训，提升企业员工网络安全意识。

5.2.1.3 安全建设

a) 推进网络安全标准化建设，保障企业数字化转型安全；
b) 建设能源数字化智能化研发创新平台，围绕能源数字化智能化安全技术创新重点方向开展系统性研究；
c) 制定对能源数字化转型安全防护技术创新的资金支持计划，形成支持能源数字化智能化发展的长效机制。

5.2.1.4 人才培养

评价内容如下：

a) 建立能源数字化网络安全人才培养机制，优化人才评价及激励政策。促进交流引进，大力吸引能源数字化智能化领域高层次人才从事科研等活动；
b) 深化能源数字化智能化领域产教融合，与院校围绕重点发展方向和关键技术共建网络安全产业学院、联合实验室、实习基地等；
c) 每年通过各种形式培养和提升员工的网络安全基本技能；
d) 建立网络安全专业人才的选拔、培养、任用机制，通过安排技术技能培训与考核、参与技能大赛和攻防演练等方式实现人才队伍技术能力及实战能力的提升。

5.2.2 安全技术

5.2.2.1 态势感知能力

评价内容如下：

a) 建设网络安全态势感知平台，完善网络安全监测预警与应急处置体系，增强事前防范、事中监测、事后应急能力，提升安全保障能力和服务水平；
b) 态势感知平台覆盖生产全过程、作业全场景、运营管理各项活动；
c) 具备监控及调度系统网络安全预警及响应处置能力，实现自动化安全风险识别、风险控制和攻击溯源。

5.2.2.2 安全基础资源库

规划建设漏洞库、病毒库、威胁情报等网络安全基础资源库，加强安全资源储备。

5.2.2.3 工控安全

制定完整的工控系统网络防护架构，确保系统具备抗攻击能力，实现网络边界安全和内部访问控制，并具备应对安全威胁与数据保障措施。采用安全可靠的信创产品和服务。5.2.2.4 **数据安全**

评价内容如下：

a) 落实国家法律法规要求，建立数据安全合规管理体系，推动数据安全合规管控能力建设；
b) 建立数据安全监管机制，梳理数据资产，进行分类分级，规范数据使用；
c) 制定数据安全技防架构，加强数据采集、传输、存储、使用、共享、销毁等各个环节的保护措施；
d) 开展数据安全保护能力落地，推广数据安全保护产品应用；
e) 应用能源数据安全共享及多方协同等技术，实现敏感数据泄露监测、敏感数据泄露溯源分析、数据异常流动分析等技术保障及分析能力。

5.2.2.5 云平台安全

构建云安全防护体系，全面覆盖云边界、应用系统区域、主机、容器等层次，实现公有云、私有云、混合云多云架构环境下网络安全的深度融合，形成IaaS、PaaS、SaaS层级的云安全防护能力。

5.2.2.6 密码应用

评价内容如下：

a) 建立密码应用标准体系，推动重要业务系统国产密码算法应用改造；
b) 对使用商用密码进行保护的重要网络与信息系统，应明确要求同步规划、同步建设、同步运行商用密码保障系统，并定期进行商用密码应用安全性评估。

5.2.2.7 新技术应用

评价内容如下：

a) 推进内生安全等新技术在能源系统网络安全领域的应用，提升网络安全智能防护技术水平；
b) 建立新技术应用安全评估体系，动态评估新技术应用存在的安全风险。

5.2.4 安全运营

5.2.4.1 安全运维

评价内容如下：

a) 从规划、设计、建设、运行、管理等全生命周期加强安全运行管理，提高安全运营效率，产生高质量的安全运营成果；
b) 强化数字化转型安全风险综合研判和监督评估，增强应对各类安全风险的风险预警、防控机制和能力建设；
c) 强化合规管理，推进安全审计，强化安全生产监督和考核；
d) 实施安全防护精准治理，加快重点隐患治理，强化应急处置效能，防范和化解各种安全风险，以高水平安全运营保障数字化转型高质量发展。

5.2.4.2 实战运营

评价内容如下：

a) 建设网络安全仿真验证环境，具备网络安全仿真实验、分析推演能力；
b) 定期开展攻防演习，检验企业网络安全防护水平；
c) 制定网络安全应急预案，具备突发网络安全事件应急处置和协同联动能力。

5.2.4.3 运营效率

评价内容如下：

a) 有效控制攻击者破坏企业信息资产或网络的次数（安全事件发生率），避免对组织的资产或数据造成实际的损失；

b) 对突发安全事件能够快速响应和处置；

c) 安全漏洞和隐患能够及时进行修补或评估可能的影响后进行修补。

6 安全防护能力评价分级

6.1 评价形式

能源企业数字化转型安全防护能力评价形式包括两种：

a) 企业自评：由企业自行对安全防护情况进行评价。通过自评，掌握本组织安全防护现状，并针对薄弱环节采取有效改进措施，最终达到改善和提高本企业字化转型安全防护能力的目的；

b) 外部评价：由外部组织（例如，网络安全服务机构）按照评价标准对企业安全防护情况进行评价，最终达到为能源企业提供更客观、更专业的安全防护能力的目的。

6.2 评分细则

能源企业数字化转型安全防护能力评分细则见附录A。对附录A给出的每项评价指标，按以下方法给予单项指标得分：

a) 如果该项指标规定的全部要求都得到满足，给予该项指标的全部分值；

b) 如果有充分理由证明该项指标对该企业不适用，给予该指标项的全部分值；

c) 如果该项指标规定的全部要求都未得到满足且不满足b)情况，该指标项得0分；

d) 该项指标规定的要求部分满足且不满足b)情况，按具体满足情况给予该指标部分分值。

6.3 指标权重分配

能源企业数字化转型安全防护能力各项指标的权重分配如表1所示。

表 1 指标权重分配表

序号	评估指标	权重值
1	安全体系	30%
2	安全技术	40%
3	安全运营	30%

6.4 评分计算方法

计算企业安全防护能力总得分，见公式（1）：

$$S = \sum_{i=1}^{3} \left(\frac{E_i}{T_i} \times W_i \times 100 \right) \quad (1)$$

式中：

S ——安全防护能力总得分；

E_i ——第 i 项指标实际评估得分；

T_i ——第 i 项指标标准分总分；

W_i ——表1中给出的第 i 项指标的权重值。

能源企业数字化转型安全防护能力评价结果见附录B。

6.5 安全防护能力分级

能源企业数字化转型安全防护能力评价时，针对安全防护得分分为基础级、发展级、成熟级、优秀级、卓越级五个等级。五个等级分级标准应符合要求如表2所示。能源企业数字化转型安全防护能力评价发现的主要问题及整改建议见附录C。

表 2 安全防护能力分级

评价分级	级别描述	分级标准
基础级	初步构建面向数字化转型的安全防护体系和能力，建立健全数据分类分级保护机制，基本建立数据安全保障能力，系统运行安全稳定。	得分≤60
发展级	网络安全体系进一步明晰，基本构建面向数字化转型的安全防护能力，安全防护体系基本完整，安全技术手段基本完整，安全运营正常可靠。	60＜得分≤70
成熟级	全面建成适应“云、大、物、移、智”等新型信息技术应用的网络安全一体化能力，形成“技术+管理”的体系化防护能力，安全防护能力与企业数字化其他能力融为一体，基本建成可信可控的网络安全和数据安全综合防控体系，全面敏捷应对多变、复杂的网络攻击和数据安全威胁，重大风险事故基本为零。	70＜得分≤80
优秀级	建成立体化、智能化的行业级安全防护体系。网络安全与数字化发展齐头并进，数字化发展水平和网络安全保障能力协调一致，数据安全保障进一步强化，防范化解风险能力得到增强，安全防护能力达到国内行业先进水平。	80＜得分≤90
卓越级	高水平建立面向全球范围重大风险的常态预防机制与应对策略，高质量建成面向网络战的态势感知和应急响应体系，安全防护总体能力基本达到国际一流水平。	得分＞90 分

附 录 A
（规范性）
能源企业数字化转型安全防护能力评分细则

能源企业数字化转型安全防护能力评分细则如表A所示。

表 A 能源企业数字化转型安全防护能力评分细则

评价方法				得分
安全体系（40分）	安全机制（15分）	a)	1）核查是否针对数字化转型带来的风险对网络安全管理体系进行优化；（1分） 2）核查网络安全管理体系是否针对数字化转型带来的组织和管理架构变化，落实主体责任，强化考核监督。（1分）	
		b)	1）核查网络安全架构方案是否针对数字化转型风险进行优化；（1分） 2）方案内容是否覆盖业务全生命周期的“预警、监测、响应”纵深防御体系。（2分）	
		c)	1）核查是否制定网络安全防控整体策略；（1分） 2）核查是否通过技术检查、攻防演习、安全检查、风险评估等方式，综合排查分析数字化转型过程中公司面临的网络安全新风险；（1分） 3）核查是否根据风险影响程度进行分级管控，完善风险分级管控工作机制；（1分） 4）核查是否针对数字化转型引入的安全隐患，完善隐患排查治理机制。（1分）	
		d)	1）核查是否制定网络安全动态防护方案；（0.5分） 2）核查是否制定云安全防护方案；（0.5分） 3）核查是否制定大数据安全防护方案；（0.5分） 4）核查是否制定物联网安全防护方案；（0.5分） 5）核查是否制定移动安全防护方案；（0.5分） 6）核查是否制定工业控制系统安全防护方案。（0.5分）	
		e)	1）核查是否制定供应链安全审查机制；（1分） 2）检查相关记录文档，核查是否对供应商、产品和服务等进行严格审查。（2分）	
	人员管理（5分）	a)	1）核查是否设置录用人员审查机制，包括对被录用人员的身份、安全背景、专业资格或资质等的审查；（0.5分） 2）核查是否与被录用人员签署保密协议，与关键岗位人员签署岗位责任协议；（0.5分） 3）核查是否建立离岗人员访问权限回收制度，及时回收各种身份证件、钥匙、徽章等以及机构提供的软硬件设备；（0.5分） 4）核查是否要求离岗人员办理严格的调离手续，并承诺调离后的保密义务后方可离开；（0.5分） 5）核查是否建立外部人员访问受控区域和受控网络的书面申请机制以及外部人员离场时的访问权限清除机制；（0.5分） 6）核查是否与获得系统访问授权的外部人员签署保密协议。（0.5分）	
		b)	1）核查是否定期组织安全意识教育和岗位技能培训；（1分） 2）核查是否定期对不同岗位的人员进行技能考核。（1分）	
	安全建设（8分）	a)	1）核查是否开展网络安全生产标准化建设工作；（1分） 2）核查是否制定数字化转型网络安全生产相关标准。（2分）	
		b)	1）核查是否应建设能源数字化智能化研发创新平台；（1分） 2）核查是否围绕能源数字化智能化安全技术创新重点方向开展系统性研究。（2分）	
		c)	核查是否具有对能源数字化转型安全防护技术创新的资金支持计划，支持能源数字化智能化发展。（2分）	

表 A （续）

评价指标			评价方法	得分
	人才培养（12 分）	a)	1）核查是否建立能源数字化网络安全人才培养机制，优化人才评价及激励政策。（1.5 分） 2）核查是否促进交流引进，大力吸引能源数字化智能化领域海外高层次人才从事科研等活动。（1.5 分）	
		b)	核查是否深化能源数字化智能化领域产教融合，与院校围绕重点发展方向和关键技术共建网络安全产业学院、联合实验室、实习基地等。（3 分）	
		c)	1）核查是否每年通过网络安全到基层、网络安全宣传周等形式培养和提升员工的网络安全意识；（1 分） 2）核查是否开展钓鱼邮件模拟演练等活动，提升员工防钓鱼、防社工意识；（1 分） 3）核查是否每年对网络安全人员进行基本技能培训。（1 分）	
		d)	1）核查是否建立网络安全专业人才选拔、培养、任用机制；（1 分） 2）核查是否通过安排技术技能培训与考核、参与技能大赛和攻防演练等方式实现人才队伍技术能力及实战能力的提升。（2 分）	
安全技术（50 分）	态势感知能力（9 分）	a)	1）核查是否建设网络安全态势感知平台；（1 分） 1）核查是否制定网络安全监测预警与应急处置体系，增强安全运营的态势感知能力；（1 分） 2）检查相关系统日志、事件报告，核查是否具备事前防范、事中监测、事后应急能力。（1 分）	
		b)	1）核查态势感知系统是否覆盖生产全过程;（1 分） 2）核查态势感知系统是否覆盖作业全场景;（1 分） 3）核查态势感知系统是否覆盖运营管理各项活动。（1 分）	
		c)	1）核查态势感知系统是否具备监控及调度系统网络安全预警及响应处置能力；（1 分） 2）核查态势感知系统是否具备自动化安全风险识别和风险阻断能力；（1 分） 3）检查事件报告、响应处置记录，核查是否具备攻击溯源能力。（1 分）	
	安全基础资源库（4 分）		1）核查是否规划建设网络安全基础资源库；（1 分） 2）核查是否建有网络安全漏洞库；（1 分） 3）核查是否建有网络安全病毒库；（1 分） 4）核查是否建有网络安全威胁情报库。（1 分）	
	工控安全（6 分）	a)	1）核查是否制定完整的工控系统网络防护架构；（1 分） 2）核查是否具备应对安全威胁与数据保障措施。（2 分）	
		b)	检查工控系统、芯片、操作系统、通用基础软硬件等方面使用的产品和服务，核查是否采用安全可靠的信创产品和服务。（3 分）	
	数据安全（15 分）	a)	1）核查是否建设数据安全合规管理体系；（1 分） 2）核查是否开展数据安全合规管控能力建设，比如部署数据安全合规管控相关系统；（2 分）	
		b)	1）核查是否建立数据安全监管机制；（1 分） 2）核查是否梳理数据资产并进行分类分级；（2 分）	
		c)	1）核查是否制定数据安全技防架构，明确资产的安全管理目标、原则和范围；（1 分） 2）核查是否明确各类数据全生命周期（包括并不限于数据采集、存储、处理、应用、流动、销毁等过程）的操作规范和保护措施；（2 分）	
		d)	1）核查是否开展数据安全保护能力落地；（1 分） 2）检查数据安全相关产品，核查是否推广数据安全保护产品应用；（2 分）	
		e）	1）核查是否应用能源数据安全共享及多方协同等技术，实现敏感数据泄露监测及溯源分析；（1.5 分） 2）核查是否应用能源数据安全共享及多方协同等技术，实现数据异常流动分析等技术保障能力。（1.5 分）	
			1）核查是否应用能源数据安全共享及多方协同等技术，实现敏感数据泄露监测；（1.5 分） 2）核查是否应用能源数据安全共享及多方协同等技术，实现数据异常流动分析等	

			技术保障能力。（1.5 分）	

表 A （续）

评价指标			评价方法	得分
	云平台安全（4 分）		1）核查是否构建云安全防护体系；（1 分） 2）核查安全防护体系是否全面覆盖云边界、应用系统区域、主机、容器等层次；（1 分） 3）核查是否实现公有云、私有云、混合云多云架构环境下网络安全的深度融合，形成 IaaS、PaaS、SaaS 层级的云安全防护能力。（2 分）	
	密码应用（6 分）	a)	1）核查是否建立密码应用标准体系；（1 分） 2）核查是否开展重要业务系统国产密码算法应用改造工作。（2 分）	
		b)	1）检查使用商用密码进行保护的重要网络与信息系统的设计文档，核查是否明确要求同步规划、同步建设、同步运行商用密码保障系统；（1 分） 2）核查是否定期进行商用密码应用安全性评估。（2 分）	
	新技术应用（6分）	a)	核查是否推进内生安全等新技术的研究应用，提升网络安全智能防护技术水平。（3 分）	
		b)	1）核查是否建立新技术应用安全评估体系；（1 分） 2）核查是否动态评估新技术应用存在的安全风险。（2 分）	
安全运营（35 分）	安全运维（15分）	a)	核查是否从规划、设计、建设、运行、管理等全生命周期各环节加强安全运行管理。（3 分）	
		b)	1）核查是否开展数字化转型安全风险综合研判和监督评估工作；（1 分） 2）核查是否增强应对各类安全风险的风险预警、防控机制和能力建设。（2 分）	
		c)	1）核查是否加强合规管理，推进安全审计工作；（1.5 分） 2）核查是否强化安全生产监督和考核工作。（1.5 分）	
		d)	实施安全防护精准治理，加快重点隐患治理，强化应急处置效能，防范和化解各种安全风险，以高水平安全运营保障数字化转型高质量发展.（3 分）	
	实战运营（10分）	a)	检查网络安全仿真验证环境，核查是否具备网络安全仿真实验、分析推演能力。（3 分）	
		b)	1）核查是否定期开展攻防演习，检验企业网络安全防护水平；（2 分） 2）核查是否每年开展攻防演习。（2 分）	
		c)	1）核查是否制定网络安全应急预案；（1 分） 2）检查相关事件报告，核查是否实现突发网络安全事件应急处置和协同联动能力。（2 分）	
	运营效率（10分）	a)	攻击者从未成功实现的攻击行为，安全事件发生率为 0。（4 分）	
		b)	突发安全事件时，能够 24 小时内进行快速响应和处置。（3 分）	
		c)	发现安全漏洞和隐患时，能够 24 小时内进行修补。（3 分）	

附 录 B

能源企业数字化转型安全防护能力评价结果明细

能源企业数字化转型安全防护能力评价结果明细如表B所示。

表 B 能源企业数字化转型安全防护能力评价结果明细

评价指标	权重	标准分	实得分	得分	评级级别
安全体系	30%	40 分			
安全技术	40%	50 分			
安全运营	30%	25 分			

附 录 C

能源企业数字化转型安全防护能力评价发现的主要问题及整改建议

能源企业数字化转型安全防护能力评价发现的主要问题及整改建议如表C所示。

表 C 能源企业数字化转型安全防护能力评价发现的主要问题及整改建议

评估人：

评价指标	应得分	实得分	存在问题	整改建议